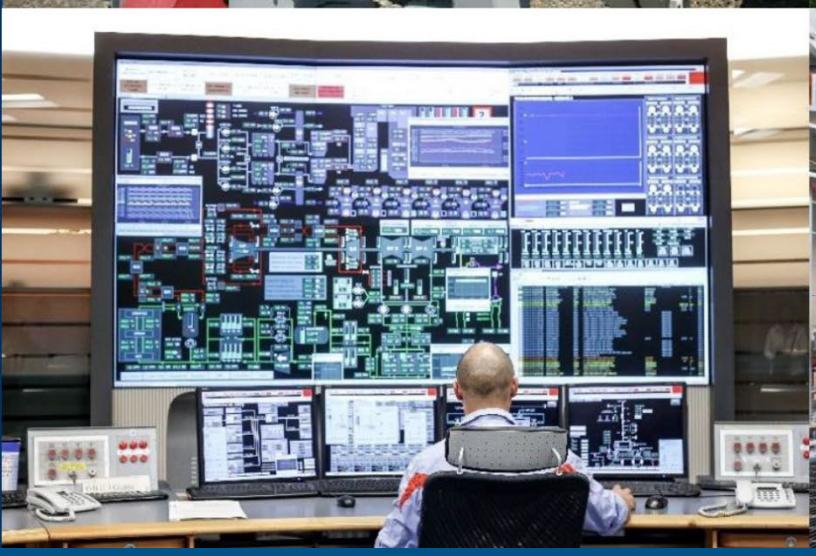





# Cybersecurity OT Smart Practices Guide

Transportation Security Administration (TSA)

July 2025

# TABLE OF CONTENTS

# TABLE OF FIGURES

# EXECUTIVE SUMMARY

The Transportation Security Administration (TSA) is responsible for regulating and ensuring the safety and security of transportation systems throughout the United States, including airports, trains, buses, and light rail. In today's increasingly volatile digital landscape, TSA and the transportation industry it regulates must also address domestic and international cyber threats to protect its passengers, employees, critical infrastructure systems, and industrial control systems (ICS).

As cyber threats become more sophisticated and continue to cause significant disruptions such as system outages, data breaches, and even physical harm, the transportation industry must rely on multiple layers of defense—known as “defense-in-depth”—to mitigate and prevent attacks. It is essential for transportation industry owners and operators to leverage defense-in-depth principles and other defense measures to help protect against today’s ever-evolving cyber threats.

Cyber and physical threats continue to evolve, and change. The tactics, techniques and procedures mutate with the changing threats. Industry defensive postures, response plans, and mitigating controls must have a regular evaluation schedule ensuring appropriate response to the evolving threat landscape. We must continue to ensure our tools for monitoring, measuring and managing risks evolve.

Defense-in-depth is a layered approach to security that involves multiple cyber and physical security measures designed to protect against a variety of threats. Defense-in-depth as a concept originated as a military strategy to construct barriers designed to impede the progress of intruders while monitoring their progress and developing and implementing responses to repel them. In the cybersecurity paradigm, Defense-in-depth correlates to detective and protective measures designed to impede the progress of a cyber intruder while enabling an organization to detect and respond to the intrusion, with the goal of reducing and mitigating the consequences of a breach.

The defense-in-depth approach to cybersecurity is critical in the transportation industry. Defense-in-depth ensures where one security measure fails, other measures are in place to mitigate the risk and help sideline an attack. Some examples of defense-in-depth measures include firewalls, intrusion detection systems, encryption, and access controls.

ICS are an integral part of critical infrastructures, helping facilitate operations in vital industries such as electricity, oil and gas, water, transportation, manufacturing, and chemical manufacturing. The growing importance of cybersecurity, and its impact on ICS, highlights fundamental risks to the Nation’s critical infrastructure. Efficiently addressing ICS cybersecurity issues requires a clear understanding of the current security challenges and specific defensive countermeasures. A holistic approach—one that uses specific countermeasures implemented in layers to create an aggregated, risk-based security posture—helps to defend against cybersecurity threats and vulnerabilities. Defense-in-depth provides a flexible, useable framework for improving cybersecurity protection when applied to control systems.

**The concept of defense-in-depth is not new—many organizations already employ the defense-in-depth measures discussed in this document within their information technology (IT) infrastructures; however, they do not necessarily apply it to ICS operations. … Due to the increasing convergence of IT and ICS architectures, recent high-profile intrusions have highlighted the increased risk to control systems.**

The concept of defense-in-depth in technology is not new. Many organizations already employ the defense-in-depth measures discussed in this document within their information technology (IT) infrastructures—however, they do not necessarily apply it to ICS operations. Historically, most organizations simply did not see a need to employ defense-in-depth principles: legacy ICS used obscure protocols and were largely considered "hack proof" due to their separation from IT, in combination with robust physical protection measures.

Due to the increasing convergence of IT and ICS architectures, recent high-profile intrusions have highlighted the increased risk to control systems while the number of cyber-based incidents across critical infrastructure sectors has risen. In response, both government agencies and sector-specific regulatory authorities have issued cybersecurity guidance and imposed sanctions for noncompliance.

The threat of an intrusion by malicious actors on critical infrastructure using computer-based exploits has also grown. Several recent noteworthy incidents have increased awareness of this threat, as well as the individuals and groups who pursue it with malicious intent. The availability of ICS-specific security solutions has not kept up with the mounting threat, so organizations must deploy a robust defense-in-depth solution—making their systems unattractive targets to would-be attackers.

**This recommended practice document provides guidance for developing mitigation strategies for specific cyber threats and direction on how to create a defense-in-depth security program for control system environments.**

This recommended practice document provides guidance for developing mitigation strategies for specific cyber threats and direction on how to create a defense-in-depth security program for control system environments. The document presents this information in four parts:

1. "Background and Overview" outlines the current state of ICS cybersecurity and provides an overview of what defense-in-depth means in a control system context.
2. "ICS Defense-in-Depth Strategies" provides strategies for securing control system environments.
3. "General Strategies for Securing ICS" covers security and risk standards.
4. "TSA's Tools and Services supporting ICS defense-in-depth" provides a list of no cost options.

Additionally, this document addresses considerations related to Internet of Things (IoT) and Industrial Internet of Things (IIOT) technologies, which continue to grow in capability and scale across critical infrastructure. This is a living document that provides a compendium of the current state of critical infrastructure and ICS security practices.

In addition to defense-in-depth, owners and operators must implement other cybersecurity measures, such as regular security assessments, Cybersecurity Implementation Plans (CIP), employee training on cybersecurity smart practices, and incident response plans. Security assessments can help identify vulnerabilities in systems and processes, while employee training can help prevent human error that could lead to a security breach. Incident response plans can help organizations respond quickly and effectively to a cyberattack and minimize damage.

Artificial Intelligence (AI) is poised to revolutionize the cybersecurity landscape for ICS by fortifying defense-in-depth strategies. By leveraging advanced machine learning models, AI can simulate sophisticated cyberattacks, enabling organizations to proactively identify vulnerabilities and strengthen their defenses. This technology enhances anomaly detection, automates threat analysis, and provides real-time insights into potential risks, making it a powerful tool against evolving cyber threats. As ICS environments become increasingly interconnected, generative AI offers a dynamic and adaptive approach to safeguarding critical infrastructure, ensuring resilience against both known and emerging challenges. As AI matures generative AI will enable

creating new content or simulating scenarios, allowing for proactive security measures. For example, generative AI can model system interdependencies, simulate sophisticated cyberattack scenarios, and assess asset criticality, enhancing planning and resilience. While traditional AI is excellent for real-time detection and response, generative AI adds a layer of strategic foresight, making both technologies complementary in building robust defense-in-depth frameworks.

Our transportation industry—as the critical infrastructure sector that connects our Nation—must strive to achieve a multilayered, resilient cybersecurity posture to remain secure, reliable, and operational. By leveraging the defense-in-depth principles and the recommended cybersecurity defense measures referenced in this document, owners and operators can help protect against persistent and ever-evolving cyber threats to ensure the safety and security of passengers, employees, and our critical infrastructure across the industry and our Nation.

## Keywords

- Cybersecurity
- data diodes
- Defense-in-depth
- demilitarized zones (DMZ)
- distributed control system (DCS)
- encryption
- firewall
- industrial control system (ICS)
- Industrial Internet of Things (IIoT)
- Internet of Things (IoT)
- intrusion detection system (IDS)
- intelligent electronic device (IED)
- intrusion prevention system (IPS)
- patch management
- policy and procedures
- process control
- programmable logic controller (PLC)
- security zones
- supervisory control and data acquisition (SCADA)
- zero trust

## Acronyms

| | |
|---|---|
| AI | Artificial Intelligence |
| ACL | Access Control List |
| ALDS | Application-Level Detection System |
| ARP | Address Resolution Protocol |
| AWWA | American Water Works Association |
| CD | Compact Disk |
| CSET® | Cyber Security Evaluation Tool |
| CIP | Cybersecurity Implementation Plans |
| CISA | Cybersecurity and Infrastructure Security Agency |
| DHS | U.S. Department of Homeland Security |

| | |
|---|---|
| DMZ | Demilitarized Zone |
| DOE | Department Of Energy |
| DTP | Dynamic Trunking Protocol |
| FERC | Federal Energy Regulatory Commission |
| FTP | File Transfer Protocol |
| HIDS | Host-Based Intrusion Detection System |
| HMI | Human-Machine Interface |
| HVAC | Heating, Ventilation, and Air Conditioning |
| ICS | Industrial Control System |
| ICT | Information And Communications Technology |
| IDS | Intrusion Detection Systems |
| IED | Intelligent Electronic Device |
| IIoT | Industrial Internet of Things |
| IoT | Internet of Things |
| IP | Internet Protocol |
| IPS | Intrusion Prevention Systems |
| ISP | Internet Service Provider |
| IT | Information Technology |
| LAN | Local Area Network |
| MAC | Media Access Control |
| NERC | North American Electric Reliability Corporation |
| NERC-CIP | NERC Critical Infrastructure Protection |
| NIC | Network Interface Card |
| NIST | National Institute of Standards and Technology |
| NRC | Nuclear Regulatory Commission |
| OS | Operating System |
| OSI | Open Systems Interconnection |
| OT | Operational Technology |
| PCS | Process Control System |

| | |
|---|---|
| PIN | Personal Identification Number |
| PLC | Programmable Logic Controller |
| RMP | Risk Management Process |
| RoE | Rules of Engagement |
| RTU | Remote Terminal Units |
| SCADA | Supervisory Control and Data Acquisition |
| SIEM | Security Information and Event Management |
| SIS | Safety-Instrumented Systems |
| SLA | Service-Level Agreement |
| SP | Special Publication |
| SSH | Secure Shell |
| SQL | Structured Query Language |
| TCP | Transmission Control Protocol |
| TSA | Transportation Security Administration |
| UPS | Uninterruptible Power Supply |
| USB | Universal Serial Bus |
| VADR | Validated Architecture Design Review |
| VLAN | Virtual LAN |
| VM | Virtual Machine |
| VPN | Virtual Private Network |

# 1. BACKGROUND AND OVERVIEW

Twenty-five years after its founding, TSA remains the recognized global leader of transportation security, enabled by our focus on capability innovation and threat-informed, information-driven operations. We will continue to be agile in addressing the dynamic threats posed to the transportation system. Over the next seven years, TSA will make strides to outpace and outmatch threats—both physical and cyber. By working to incorporate and complement industry advances, TSA will bolster the security of all modes of transportation, critical infrastructure, and ICS.

## Key trends impacting TSA:

- **Continuous threat:** Adversaries remain committed to causing physical and economic harm to transportation networks with low cost and sophisticated tactics.
- **Emerging/interconnected technologies:** Interconnected technologies enable an agile security model and effective operations.
- **Cyber-Physical interdependency:** Risk of intrusion or disruption from state and non-state actors to critical transportation infrastructure.
- **Passenger experience:** Passengers are demanding customized and seamless travel experiences with on-demand and convenient services.
- **Changing workforce:** The ability to recruit and retain talent with advanced technical skills, critical thinking and adaptability is increasingly difficult in a competitive labor market.
- **Transportation system and economy:** Passenger and cargo volumes are increasing with demand for new travel departure points and destinations in growing global regions.
- **Evolving technology:** Significant advances in technology bring new efficiencies to providing goods and services, however they also bring new threat vectors increasing risk.

In its approach to both physical security and cybersecurity, TSA's collaborative style drives seamless operations and sound, timely decisions. Effective integration, communication, and knowledge management has changed the way the agency thinks and responds to threats. Rapid, data-informed decisions and organizational alignment enable TSA and its partners to effectively allocate cybersecurity resources and field innovative solutions faster and with more precision.

In line with TSA's Strategy, our priorities are:

### 1. Improve Security and Safeguard the Transportation System

As a leader in the transportation security network, TSA will work to raise the global baseline of transportation security. We will lead by example by strengthening operations through powerful and adaptable detection capabilities, intelligence-driven operations, and enhanced vetting. Strong partnerships across governments and industry will be integral to success in this shared transportation security mission.

- Strengthen the effectiveness of TSA's core capabilities in critical infrastructure and ICS cybersecurity efforts.
- Improve intelligence-driven operations with increased information sharing.
- Modernize transportation vetting.
- Advance global transportation security standards.
- Promote security partnerships across surface transportation systems.

### 2. Accelerate Action

TSA will build a culture of innovation that anticipates and rapidly counters the changing threats across the transportation system. We will mature our ability to make timely, data-driven decisions and rapidly field innovative solutions. We will simplify access for our partners and stakeholders to encourage robust collaboration. By driving integration across the organization, TSA will more effectively manage risk, identify requirements, deploy resources, and assess operational outcomes.

- Improve the speed to decision.
- Reduce the time to field solutions.
- Define clear pathways to enable partnership and collaboration.
- Align TSA's organizational structure to manage risk and optimize resource allocation.

### 3. Commit to Our People

TSA's most important assets are the dedicated professionals securing our Nation's transportation system. We will foster a diverse, inclusive, and transparent work environment, establishing TSA as a federal employer of choice. TSA will utilize available tools and authorities to cultivate a skilled workforce prepared and equipped to meet the challenges of tomorrow. We will transform our organizational culture to promote an entrepreneurial spirit and operational excellence.

## Our Commitment to Critical Infrastructure and ICS Security

TSA is committed to strengthening the security of ICS within Critical Infrastructure (CI) across public and private domains. ICS share common, often interconnected attributes across IT and ICS components. Modern technologies trend towards miniaturization and increased networked connectivity to enhance productivity, reduce costs, and create business and government applications that were previously impossible.

Modern CI must continue to adhere to good practice(s) related to cyber risk management, maintaining awareness of risk associated with legacy technologies while leveraging the maximum benefit from newer technologies such as those associated with the Industrial Internet of Things (IIoT). Integration of older and newer technologies often expose mission-critical ICS to cyber threats through exploitation of existing vulnerabilities in the connected legacy components, thus increasing the organization's overall cybersecurity risk. These integration initiatives are a natural result of organizational evolution resulting from mergers and acquisitions, organizational growth, and strategic business transformation. Common communications protocols and open architecture standards are replacing the diverse and disparate proprietary mechanics for ICS. This recommended practice document provides guidance for developing defense-in-depth strategies for organizations that use ICS and IIoT technologies within their technology architecture.

Historically, physical separation between enterprise and ICS domains provided the primary means of protecting ICS; however, this division is much less common over the past few decades due to limited capabilities for data sharing, data acquisition, peer-to-peer data exchange, or other business operations. Modern control system architectures, business requirements, and cost control measures result in increasing integration of corporate and ICS IT architectures. Physical separation alone no longer provides a viable business option for managing, utilizing, or securing ICS.

# 2. ICS DEFENSE-IN-DEPTH STRATEGIES

An organization's cybersecurity strategy should protect the assets it deems critical to successful operation. A layered approach, known as defense-in-depth, is the most effective strategy for managing risk. Defense-in-depth, as mentioned above, originated in military strategy to provide barriers to impede, monitor, and respond to intruders during an event. In the cybersecurity paradigm, Defense-in-depth correlates to detective and protective measures designed to impede the progress of a cyber intruder while enabling an organization to detect and respond to the intrusion with the goal of reducing and mitigating the consequences of a breach.

Defense-in-depth is not a one-to-one exercise, where an organization deploys specific technologies to counter an equivalent risk. Defense-in-depth employs a holistic approach to protect all assets supporting the mission or business model, while taking into consideration its interconnections and dependencies, and using an organization's available resources to provide effective layers of monitoring and protection based on the business's exposure to cybersecurity risks. In order to apply defense-in-depth to ICS environments, an organization must understand the relationship of intruders (threats) and vulnerabilities to the controls (standards and countermeasures) put in place to protect the mission-critical and business-critical processes that rely on ICS technologies.

A threat actor, through intent, capability, and/or opportunity, poses a threat to an ICS by compromising an organization's systems through its operations, personnel, and/or technology and exploiting an existing weakness or vulnerability. Security countermeasures, based on good practices and standards, protect ICS critical assets through multiple layers of defense—thereby improving protection for operations, personnel, and technology. Organizations must constantly adjust and refine security countermeasures to ensure protection against known and emerging threats (see Figure 2).


*Figure 1: TSA staff working to secure our Nation's railways.*


*Figure 2: Defense-in-Depth Planning*

Because of the complexity of ICS architectures, potential vulnerabilities and/or exploits that introduce new and evolving categories of threats to the ICS environment can have lasting consequences, and without a layered, multitier strategy could result in long-term exposure without detection. The following intrusion methods could enable an advanced persistent threat that lies within the system to remain undetected for long periods of time:

- Attacks directly from Internet to Internet-connected ICS devices:
  - ⇒ Establish direct access deep into the ICS networks.
- Attacks initiated using remote access credentials stolen or hijacked from authorized ICS organization users:
  - ⇒ Establish direct access deep into the ICS networks.
- Attacks on the external business web interface:
  - ⇒ Leverage exploits to vulnerabilities existing in the web services.
  - ⇒ Pivot into the ICS historian that provides ICS data to the web server applications.

- Attacks initiated by insertion of infected mobile media into a system component:
  - ⇒ Pivot deeper into the ICS networks as threat actors find opportunity.
- Threat actors use phishing email to establish a presence on enterprise user desktop or business computers:
  - ⇒ Pivot deeper into the ICS networks as threat actors find opportunity.

IIoT technologies represent particularly complex challenges to security architecture that require asset owners to plan for sensor reliability, sensor security, data aggregator reliability and security, communications channel reliability and security, and logic integrity and security.[1]

Defense-in-depth is not one thing, but a combination of people, technology, operations, and adversarial awareness. Organizations must constantly adjust and refine security countermeasures to protect against known and emerging threats. Security countermeasures, based on smart practices and standards, protect the ICS critical assets through multiple layers of defenses, thereby improving protection for operations, personnel, and technology.

The goal is to reduce the opportunities for an adversary to take advantage of the ability to move through an entity's networks/systems. Multiple layers of defense help prevent direct attacks against critical systems and greatly increase the difficulty of creating impact on mission and business critical applications supported by ICS while providing natural areas for the implementation of intrusion detection technologies.

This section discusses some of the available and recommended solutions and strategies for defense-in-depth security, as outlined in Table 1. Organizations should use these solutions and strategies in combination to create layers of defenses, enabling ICS functionality while providing the most robust protection available for critical assets.

*Table 1: Defense-in-Depth Strategy Elements*

| Defense-in-Depth Strategy Elements | |
|---|---|
| Risk Management Program | • Identify Threats<br>• Characterize Risk<br>• Maintain Asset Inventory |
| Cybersecurity Architecture | • Standards/Recommendations<br>• Policy<br>• Procedures |
| Physical Security | • Field Electronics Locked Down<br>• Control Center Access Controls<br>• Remote Site Video, Access Controls, Barriers |

[1] NIST SP 800-183, Networks of 'Things', July 2016

| | |
|---|---|
| ICS Network Architecture | • Common Architectural Zones<br>• Demilitarized Zones (DMZ)<br>• Virtual Local Area Networks (LANs) |
| ICS Network Perimeter Security | • Firewalls/One-Way Diodes<br>• Remote Access & Authentication<br>• Jump Servers/Hosts |
| Host Security | • Patch and Vulnerability Management<br>• Field Devices<br>• Virtual Machines |
| Security Monitoring | • Intrusion Detection Systems<br>• Security Audit Logging<br>• Security Incident and Event Monitoring |
| Vendor Management | • Supply Chain Management<br>• Managed Services/Outsourcing<br>• Leveraging Cloud Services |
| The Human Element | • Policies<br>• Procedures<br>• Training and Awareness |

## Risk Management and ICS

Improving cybersecurity posture by implementing an ICS defense-in-depth strategy starts with developing an understanding of the business risk associated with ICS cybersecurity and managing that risk according to the overall business risk appetite. The individuals responsible for managing and maintaining the functionality of control systems need to know the methods to assess and determine cybersecurity risk and how to apply that knowledge to their unique environment. A clear understanding of the threats to the business, the operational processes and technology used within the organization, and its unique functional and technical requirements enables an organization to embed a layered approach for cybersecurity monitoring and defense into the day-to-day operation of their ICS.

An effective ICS security program depends on the willingness of the ICS operations staff to accept security as an enabler for all computer-oriented activities and their ability to apply security controls to their operational technology from a standpoint of acceptable risk. Designing an effective ICS security architecture requires a risk model that maps specifically to the functional requirements for these complex systems. A control system can affect the physical world, and as a result, the definition of risk as it applies to an ICS must include considerations for potential real-world consequences. Individuals at all levels within an organization should understand ICS risks and actively engage themselves in the risk management process (RMP).

## Multitiered Risk Management Integration

To integrate ICS risk management practices throughout an organization, the entity should employ a three-tiered approach that addresses risk at the organization level (Tier 1), the mission/business process level (Tier 2), and the information system level (Tier 3), as illustrated in Figure 3. This approach is adapted from NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems—A Security Life Cycle Approach; NIST SP 800-39, Managing Information Security Risk—Organization, Mission, and Information System View; and the NIST Framework for Improving Critical Infrastructure Cybersecurity.

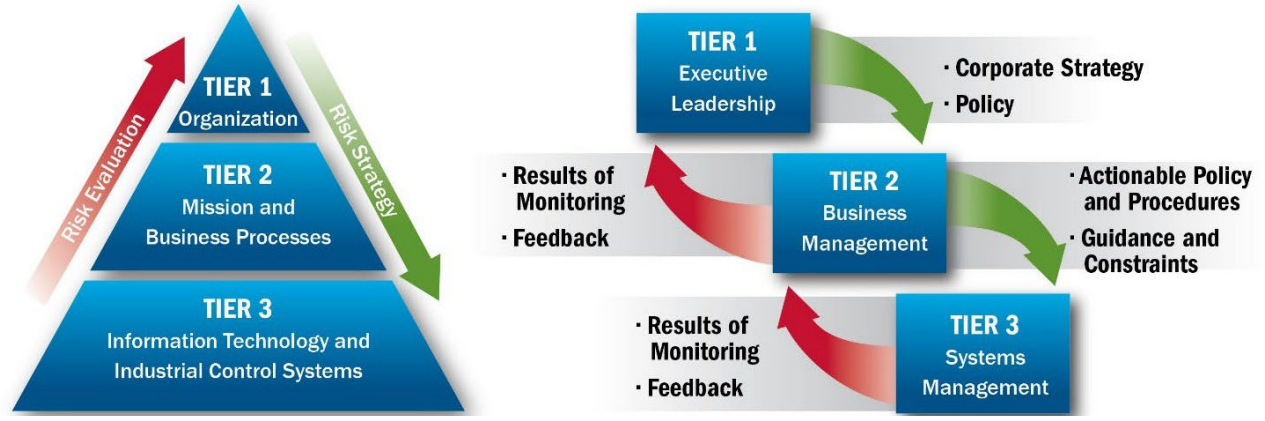



*Figure 3: Risk Management Tiers*

**Tier 1** addresses risk from an organizational perspective. At this level, the organization implements the first component of risk management—risk framing—providing the context for all risk management activities and providing the basis for risk management throughout the organization, including the operational technology (OT) space. Tier 1 activities determine:

- The techniques and methodologies used to assess information system-related security risks and other types of risk of concern from an overall business standpoint,
- The methods and procedures used to evaluate the significance of the risks identified during risk assessments,
- The types and extent of risk mitigation measures used to address identified risks,
- The level of risk the organization plans to accept (risk tolerance),
- How the organization plans to monitor risk on an ongoing basis, and
- The degree and type of oversight to ensure the risk management strategy is being effectively carried out.

**Tier 2** addresses risk from a mission/business process perspective informed by the risk context, risk decisions, and risk activities at Tier 1. Tier 2 risk management activities include:

- Defining the core ICS functions and processes that support the organization,
- Prioritizing the ICS functions and processes with respect to the overall goals and objectives of the organization,
- Defining the types of information needed to successfully execute the core ICS functions and processes and their interdependencies and information flows (information and security architecture),
- Developing an ICS information protection strategy and incorporating ICS security requirements into the operational processes, and
- Specifying the degree of autonomy regarding assessing, evaluating, mitigating, accepting, and monitoring risk.

**Tier 3** implements security at the operational level and addresses risk from an information system perspective. The risk context, risk decisions, and risk activities at Tiers 1 and 2 guide activities at this level. Tier 3 risk management activities include performing the five system-level ICS risk management functions (identify, protect, detect, respond, and recover) as part of a disciplined and structured system development life-cycle process.

Applying risk management to ICS at a practical level does not depend on having all three tiers in place. Organizations can apply risk management practices to ICS at the operational level by defining a workable RMP; ensuring systems are inventoried, categorized, and security prioritized based on their importance and impact; identifying threats and vulnerabilities and their associated mitigation strategies; and ensuring risk acceptance processes and approval hierarchies are defined and implemented as part of the ICS system life cycle.

## Risk Management Approach

The attack surface for an operation includes any and all the vectors associated with gaining access to the systems or equipment considered critical to business operations. To implement controls necessary to reduce the attack surface for critical assets, an organization must first identify the systems and components they consider business- or mission- critical. Then they must determine the criticality of the assets based on their function and importance to business operations. The business then performs a cybersecurity risk analysis of the system to identify the current threats, vulnerabilities, risks to the system and/or operations, and the potential impact should a threat be carried out. Figure 4 shows this process.


*Figure 4: Risk Management Approach*

Organizations should apply controls at the highest security level possible while enabling uninterrupted functionality. Finally, they should monitor and adjust security controls as necessary to ensure ongoing protection against emerging threats.

## Cybersecurity Architecture

For ICS security to be effective, an asset owner must first identify what needs protection. Doing so establishes a baseline understanding among the stakeholders relative to the support infrastructure (both IT and ICS). Asset owners must identify and prioritize process systems (including process equipment and operations and ICS software, networks, and personnel) and analyze interconnections and dependencies based on their business impact. Understanding the business context and the resources that support critical functions and the related business risks enables an organization to focus and prioritize its efforts consistent with its risk management strategy and business needs.

Asset identification is an important step in understanding and managing ICS risk and helps to determine the basis and priorities for applying security defenses. This is also vital in determining what specific monitoring should be considered, what countermeasures are practical, what countermeasures can impede normal system behavior, and what compensating controls asset owners can deploy if there is no applicable technical countermeasure. Unlike IT, managing cybersecurity within control system domains requires consideration of unique system nuances and realistic conditions that must be met for an adversary to compromise the system and cause process impact. Identifying all assets within the control system is vital to understanding the potential impact of cyber-related intrusion(s). Assets can include systems, information, or processes (operations).

Asset Characterization

- What asset (information) needs to be protected?
- Why must the asset be protected?
- Who has the responsibility for managing and protecting the asset (what are the roles, responsibilities, accountabilities, and authorities)?
- If the threat actor compromised the asset, what realistic worst-case scenarios would result?
- What is the value of the asset?
- What is the criticality of the process or information to the business mission?
- What are the protection levels for confidentiality, integrity, and availability?
- What interconnections are required for the systems to perform?
- What methods are currently available for user access?
- What dependencies are present for system functionality?
- How does the information flow through the system, and through what mechanisms?

The key is to identify the common thread that defines the asset, first from its mission (purpose), then to the asset itself, and finally to the supporting infrastructure and related ICS dependencies. This common thread will reveal which ICS components are more critical when applying security controls.

A current inventory that has all ICS components characterized according to their criticality to their function provides a solid basis for applying defense measures and helps to ensure asset owners miss no systems or leave no critical devices unprotected.

## Inventory Assets

A comprehensive inventory of ICS assets develops a baseline understanding among all stakeholders relative to the support infrastructure (both IT and ICS). Organizations should identify systems (including hardware, software, and supporting infrastructure technologies) and analyze dependencies to understand both the function of the asset itself and the resources required to support critical functions. Organizations should couple technical network maps for all systems with the physical inventory and an operational level of understanding of the information flows, which provide a basis for determining the protection levels for each system or subsystem and the controls to put in place to protect the system without compromising or degrading its performance. In an ICS environment, identifying both upstream and downstream dependencies is critical, as the processes involved are, many times, interdependent and potential effects subtle.

The greatest vulnerability to ICS systems occurs at any point of connection. While Internet connectivity may present the greatest vulnerability, asset owners must identify any connectivity in this step—whether connected now or connected later. To leave even one connection undiscovered could inadvertently leave the entire system and network vulnerable.

It is important to remember that running a scan on the network elements will identify only what is connected at the time of the scan; as such, the organization should also conduct a physical inventory. A physical inventory will help to determine potential future connections and/or connections that may be turned off during the time of the scan.

Generative AI can significantly enhance inventory networks and systems for ICS and Supervisory Control and Data Acquisition (SCADA) environments. Generative AI can analyze historical sales data, market trends, and external factors like seasonality to predict future demand with high accuracy. This helps businesses maintain optimal stock levels and avoid overstocking or stockouts. AI can also aid in inventory optimization; By creating dynamic models, generative AI can suggest the best inventory levels and reorder points, ensuring smooth operations while minimizing holding costs. Additionally, AI can analyze sensor data from ICS/SCADA systems to predict equipment failures, ensuring timely maintenance and reducing downtime.

## Categorize Asset Criticality

Determining asset criticality starts with identifying the information generated, processed, stored, and disseminated on and from the ICS; defining the function of the ICS asset within the overall operation (keeping in mind both upstream and downstream functional impacts); and assigning a security categorization for that asset. Asset owners should rate the security categorizations based on the potential impact (low, moderate, or high) on the organization should an event occur that jeopardizes its ability to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and/or protect individuals. The key is to identify the thread from the function (purpose) of the asset to its supporting infrastructure and ICS dependencies. This thread will reveal which ICS are more critical when it comes to applying security controls.

Generative AI provides a cutting-edge solution for categorizing asset criticality in Industrial Control Systems (ICS), strengthening defense-in-depth strategies. By analyzing complex datasets, generative AI can model system interdependencies, simulate potential failure scenarios, and assess the importance of each asset in the context of operational and cybersecurity risks. This enables organizations to prioritize resources and enhance protection for the most critical components. Furthermore, generative AI adapts to changing system configurations and evolving threat landscapes, ensuring asset categorizations remain dynamic and reflective of current challenges.

## Identify Security Risks

In order to define and articulate the risk to ICS, organizations must identify the potential threats to the ICS and the vulnerability of the system to those threats. This information provides the current security risk exposure for the ICS.

Security Risks

- Insider intentional threats—disgruntled employees, vendors, system integrators or anyone else with internal knowledge or access to the ICS
- Internal unintentional threats—inappropriate system designs, policies, architectures procedures, technologies, or testing
- External nontargeted threats—maliciously designed software viruses and worms
- Malicious actors—unethical hackers, criminals, and nation-states

The individuals most technically competent to understand the potential attack vectors and system-level consequences are typically operations line managers and operators. They understand the operational systems and the potential impact to the system should a threat actor compromise the control system. They can also help to determine the potential consequences of a system failure to the business, which may include the loss of information.

Generative AI offers a transformative approach to identifying security risks within ICS, enhancing defense-in-depth strategies. By analyzing vast datasets and modeling complex system behaviors, generative AI can uncover hidden vulnerabilities and predict potential threat scenarios. It enables the simulation of advanced cyberattacks, providing insights into how systems may respond under various conditions. Additionally, generative AI can detect patterns and anomalies that traditional methods might miss, ensuring a proactive stance against emerging risks. With its ability to adapt to evolving threats and ICS configurations, generative AI strengthens the resilience and overall security of critical infrastructure.

## Determine Potential Impact

An organization can estimate the likelihood of a threat actor carrying out a threat or exploiting a vulnerability by considering the potential channels for threat exploitation, such as whether the system is in a higher or lower security zone on the network, its access and privilege requirements, its security configuration, and identifying any exceptions to security policy. The potential impact of a threat actor compromising or making an asset unavailable (for example, financial, damage to other systems or to the public, including human safety concerns) is based on the criticality of the system or information, the visibility of the system or the exploit, and the ability to quickly remediate any damage caused by the compromise. This step identifies both direct and collateral impacts.

For ICS environments, the impacts can also be kinetic—that is, runaway processes or system failures can have physical and environmental consequences, such as the failure or disruption of a major rail junction leading to a derailment that results in a hazardous chemical spill. Asset owners should consider any impact that could present safety concerns as high impact. Figure 4 characterizes the current risk by impact and likelihood.

Generative AI can play a vital role in determining the impact of cyber incidents on ICS as part of a defense-in-depth strategy. By simulating attack scenarios and analyzing system interdependencies, generative AI can predict how a breach might propagate through ICS networks and assess the potential consequences on operations and safety. This technology enables detailed impact analyses by modeling various failure conditions and prioritizing recovery actions for the most critical components. Additionally, generative AI adapts to evolving system configurations and threat landscapes, ensuring that organizations can respond effectively and minimize disruption. By providing actionable insights, generative AI enhances preparedness and resilience in safeguarding critical infrastructure.

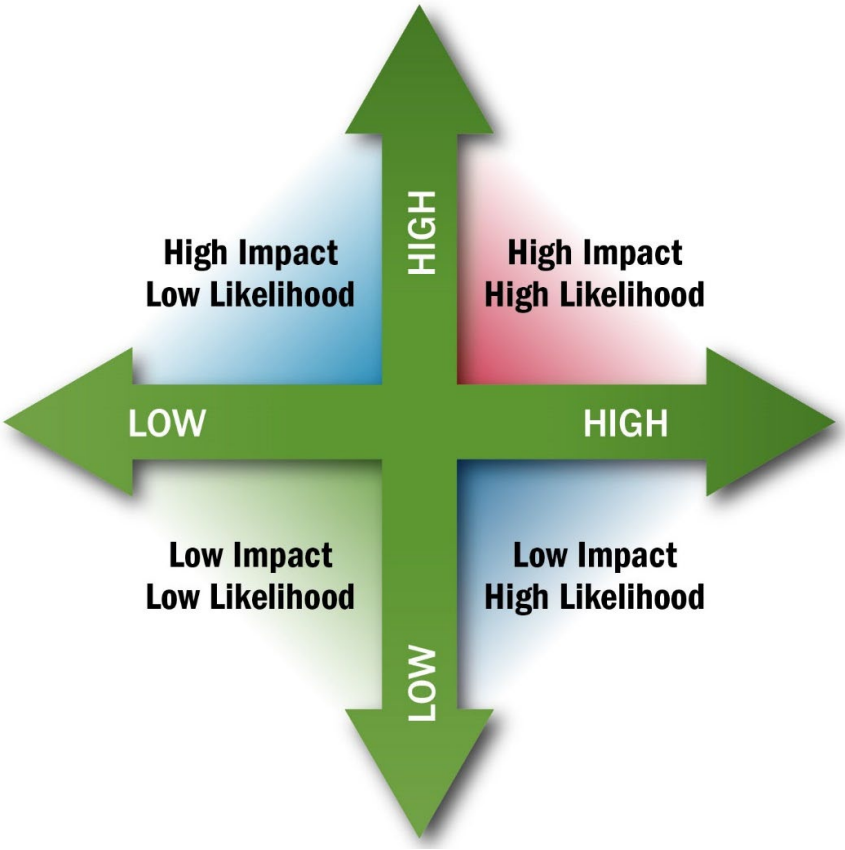



*Figure 5: Simple Qualitative Risk Analysis Chart*

## Identify and Tailor Controls

The Chief Information Security Officer or organizational equivalent usually sets baseline security controls, with input from IT and OT operations and management personnel based on the overall protection level (criticality). If the system is critical to the organization's mission (as identified in a Business Impact Assessment) or if the ICS controls a process with potential human safety consequences, it may require special consideration and additional controls.

In addition, security controls for ICS may be based on the regulatory requirements for the sector. The National Institute of Standards and Technology (NIST) has published NIST SP 800-82, Rev.2, Guide to Industrial Control Systems (ICS) Security and an updated NIST SP 800-82 Rev. 3 (Draft) for organizations wishing to protect their ICS. Organizations should gear ICS controls toward reducing risk while enabling functionality.

Asset owners should tailor security controls for a particular system based on mission needs or system functionality requirements. Control tailoring may add or subtract controls from the recommended control set. Asset owners should base tailoring on a documented business need, assessed for risk, and approved prior to system or application implementation or production release.

An important part of identifying and tailoring security controls is to remember policies and procedures are critical controls as well. Organizations should review and update policies and procedures to drive the implementation of defense-in-depth practices. Understand organization policies and procedures and ensure they are current and support ICS cyber risk reduction goals. Companies often have "unwritten policies" or rely on the expertise of their personnel to apply security controls, which leads to inconsistent applications. Asset owners should

maintain written and formalized policies and procedures and view them as a vital part of their defense-in-depth strategy.

Generative AI enhances the defense-in-depth strategies of ICS by enabling the identification and customization of security controls. By analyzing system configurations, operational data, and evolving threat landscapes, generative AI can pinpoint vulnerabilities and recommend tailored security measures that align with the unique needs of each ICS environment.

## Implement Security Controls

Apply security controls to ICS according to priority. The most critical (high impact) and most vulnerable (high likelihood) systems should be the first priority for risk reduction and mitigation activities. Pervasive vulnerabilities, such as the use of unsupported operating systems (OS), are also a good starting point for applying security controls. Regular system updates can provide far-reaching protection and reduce risk across many systems. Security controls for the human aspect of security should include cybersecurity awareness training that undergoes regular review and frequent testing. This process significantly reduces the physical business cybersecurity exposure and attack surface[2].

Asset owners should not see security controls as an "add-on" for ICS. They should integrate security considerations and processes into existing policies and procedures and consider them an integral part of the system life cycle. No system is 100% secure; however, applying security controls to the systems and environment can help reduce risk to an acceptable level. This is where organizations must apply defense-in-depth practices.

Generative AI offers a transformative approach by analyzing system configurations, operational workflows, and threat intelligence, generative AI can design and recommend tailored security controls that address specific vulnerabilities and operational needs. It can simulate various attack scenarios to test the effectiveness of proposed measures before deployment, ensuring robust protection. Additionally, generative AI supports the dynamic adaptation of security controls, enabling the continuous alignment with evolving risks and system changes. This capability strengthens ICS cybersecurity by providing precise, proactive, and adaptive security implementations.

## Variances, Waivers, and Exceptions

ICS systems may have functional or operational properties that disallow the application of a security control. In these cases, a variance, waiver, or exception to a control may be in order.

- A control variance is a request to accept a compensating control. Compensating controls apply security protection at or above the same level as outlined in the control requirement and usually do not raise risk to the security of the system.
- Control waivers are requests to tailor the control out of the baseline for the system where it does not apply to the system, system implementation, or environment.
- Control exceptions are requests made when the organization determines the control applies to the system, but they will not implement them for an established business reason.

ICS environments, unlike IT environments, usually require a good amount of control tailoring or may have many variances, waivers, or exceptions because of their specialized functionality, unique protocols, and specific operational requirements. When considering control exceptions, organizations should perform a risk assessment and ensure the appropriate personnel review and accept the risk of not implementing a security control. Organizations should consider these exceptions temporary and review them periodically to ensure they address them in a timely manner.

---

[2] Attack surface: The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment.

Generative AI can streamline the implementation of variances, waivers, and exceptions to security controls within ICS as part of a defense-in-depth strategy. By analyzing system configurations, operational constraints, and compliance requirements, generative AI can assess the feasibility and impact of deviations from established controls. It can simulate potential risks associated with these exceptions and recommend tailored compensatory measures to maintain system resilience. Additionally, generative AI enables dynamic adjustments, ensuring that variances align with evolving cybersecurity threats and operational needs.

### Monitor and Adjust

Security for any system is never a “once and done” activity. Organizations constantly change ICS environments—adjusting settings, replacing or upgrading older systems, implementing new capabilities, applying vendor patches—while the threats to ICS and operations continue to evolve. Security monitoring is critical to ensure ongoing system protection.

Asset owners should review or assess the implementation status for all security controls periodically throughout the system development life cycle. This provides an important indicator of whether the controls work as intended and reduce risk. Asset owners may need additional or compensating controls to further reduce risk, so they should revisit the control selection process and properly address identified risks. The results of these assessments or reviews will provide the organization with a determination of residual risk and provide insight into areas where they need to make security control adjustments. IIoT devices in particular must undergo thorough dynamic security testing focused on identifying vulnerabilities in off-the-shelf components, which may become critical components in the overall ICS application.

While this document discusses some of the technical controls that provide monitoring information, system monitoring only works when performed diligently and when the processes in place use the information to continually improve. Monitoring and adjustment activities such as system auditing and reviews, assessments, configuration management and change control processes, and applying lessons learned are an essential part of risk management practices.

Generative AI enhances configuration management and change control processes for ICS by analyzing system configurations and operational data, generative AI can monitor changes in real-time, ensuring adherence to established protocols and detecting unauthorized modifications. It can simulate the impact of proposed changes on ICS security, helping to mitigate risks before implementation.

## Physical Security

Physical security measures reduce the risk of accidental or deliberate loss or damage to organizational assets and the surrounding environment. The assets being safeguarded include physical assets such as tools and plant equipment, the environment, the surrounding community, and intellectual property including proprietary data such as process settings and customer information. Physical security controls often must meet environmental, safety, regulatory, legal, and other requirements, often specific to a given environment. Organizations should tailor physical security controls, like technical controls, to the type of protection needed.

Organizations must address the physical protection of the cyber components and data associated with the ICS as part of the overall security in the ICS environment. Security at many ICS facilities is closely tied to facility safety with a primary goal of keeping people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures.

Physical security controls are any physical measures, either active or passive, which limit physical access to any information assets in the ICS environment. Organizations employ these measures to prevent undesirable system impact such as the following:

- Unauthorized physical access to sensitive locations,
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations,
- Unauthorized observation of sensitive information assets through visual observation, note taking, photographs, or other means,

- Unauthorized introduction of new systems, infrastructure, communications interfaces, or other hardware,
- Unauthorized introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact such as a universal serial bus (USB) memory device, wireless access point, or Bluetooth or cellular device.

Physical Access

- Facility access control
- ICS control and server room access
- Multifactor (for example, key card, card-and-personal identification number [PIN], or biometric) authentication for physical access
- Facility monitoring using cameras, motion detectors
- Alerting for device manipulation such as power removal, device resets, cabling changes, or the addition/use of removable media devices
- Visitor escort requirements and procedures

Gaining physical access to a control room or control system components often implies gaining logical access to the process control system (PCS) as well. Likewise, having logical access to systems, such as command servers and control room computers, allows an adversary to exercise control over the physical process. If computers are readily accessible, and they have removable media drives (for example, floppy disks, compact disks [CD], digital video disks [DVD], Blu-Ray drives, external hard drives) or USB ports, organizations can fit the drives with locks or remove them from the computers and disable USB ports. Depending on security needs and risks, asset owners might also find it prudent to disable or physically protect power buttons to prevent unauthorized use. For maximum security, place servers in locked areas and protect authentication mechanisms (such as keys). Also, locate the network devices on the ICS network, including switches, routers, network jacks, servers, workstations, and controllers, in a secured area accessible only by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices.

Classic physical security considerations typically refer to a ringed architecture of layered security measures. Creating several physical barriers—both active and passive—around buildings, facilities, rooms, equipment, or other informational assets establishes these physical security perimeters. Physical security controls include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures. Most organizations include this layered model by first preventing access to the facility through the use of fences, guards, gates, and/or locked doors.

Physical access control systems should ensure only authorized people have access to controlled spaces. An access control system should be flexible. The need for access may depend on time (day versus night shift), level of training, employment status, work assignment, facility status, and a myriad of other factors. A system must verify that individuals being granted access are who they say they are (usually using something the person has, such as an access card or key; something they know, such as a PIN; or something they are, using a biometric device). Access control should be highly reliable, yet not interfere with the routine or emergency duties of personnel. Integration of access control into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity. Limit access to network and computer cabinets to only those who have a need such as network technicians and engineers or computer maintenance staff. Lock equipment cabinets and keep wiring neat and within cabinets. Consider keeping all computers in secure racks and using peripheral extender technology to connect human-machine interfaces (HMI) to the racked computers.

Access monitoring systems include still and video cameras, sensors, and various types of identification systems. Examples of these systems include cameras that monitor railway hubs, junctions, crossing loops, and multimodal interchanges. These devices do not specifically prevent access to a particular location; rather, they

store and record either the physical presence or the lack of physical presence of individuals, vehicles, or other physical entities. Provide adequate lighting based on the type of access monitoring device deployed.

Access-limiting systems may employ a combination of devices to physically control or prevent access to protected resources. Access-limiting systems include both active and passive security devices such as fences, doors, safes, gates, and guards. They often get coupled with identification and monitoring systems to provide role-based access for specific individuals or groups of individuals.

Locating people and vehicles in a large installation is important for safety reasons and, increasingly so, for security reasons as well. Asset location technologies can track the movements of people and vehicles within the plant to ensure they stay in authorized areas, identify personnel needing assistance, and support emergency response.

In addressing the security needs of the system and data, always consider environmental factors. For example, in a dusty location, place systems in a filtered environment. This is particularly important if the dust is conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, mount systems on rubber bushings to prevent disk crashes and wiring connection problems. In addition, the environments containing systems and media (for example, backup tapes and floppy disks) should have stable temperature and humidity. An alarm to the PCS should sound when environmental specifications, such as temperature and humidity, exceed the limits.

Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support personnel during normal operation and emergency situations, which could include the release of toxic substances. Organizations should carefully design fire systems to avoid causing more harm than good (for example, to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security.

Reliable power for the ICS is essential, so organizations should have an uninterruptible power supply (UPS). If the site has an emergency generator, the UPS battery life may only need to last for a few seconds; however, if the site relies on external power, the UPS battery life may need to last for several hours. It should be sized, at a minimum, so the system can be shut down safely.

Physical security for the control center/control room will reduce the potential for many threats. Control centers/control rooms frequently have consoles continuously logged onto the primary control server, where speed of response and continual view of the facility is of utmost importance. These areas will often contain the servers themselves, other critical computer nodes, and sometimes PLCs. Asset owners should limit access to these areas to authorized users only, using authentication methods such as smart or magnetic identity cards or biometric devices. In extreme cases, an asset owner could consider it necessary to make the control center/control room blast-proof, or to provide an offsite emergency control center/control room so control can be maintained if the primary control center/control room becomes uninhabitable.

Computers and computerized devices used for ICS functions (such as programmable logic controller [PLC] programming) should never leave the ICS area. Laptops, portable engineering workstations, and handhelds should be tightly secured and never used outside the ICS network.

Organizations should also address cabling design and implementation for the control network. Unshielded twisted pair communications cable, while acceptable for the office environment, is generally not suitable for an industrial environment because of its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Use industrial registered jack (RJ)-45 connectors in place of other types of twisted pair connectors to provide protection against moisture, dust, and vibration. Fiber-optic and coaxial cables are often better network cabling choices for the control network because they are immune to many of the typical environmental conditions, including electrical and radio frequency interference found in an industrial control environment. Color code and label cables and connectors to clearly delineate the ICS and IT networks and reduce the potential for an inadvertent cross-connect. Install cable runs to limit access to authorized personnel only and install equipment in locked cabinets with adequate ventilation and air filtration.

IIoT hardware is often integrated in physical locations outside the boundaries of the organization’s physical security controls. Some IIoT hardware may by integrated for applications, which require them to be unprotected by the physical security controls provided to other hardware owned by the organization. IIoT hardware may be unattended and not under observation. In these cases, tamper-proof and/or tamper-evident controls should be implemented to protect IIoT hardware in these configurations. The physical security of endpoints can include, for

example, small simple plastic devices, port locks and camera cover, which lock out USB and Ethernet ports and cover webcam apertures. Port locks help prevent unwanted malware. Some tamper-resistive approaches disable the device when it is tampered with.

As a smart practice, secure endpoint hardening likely implies a layered approach that requires attackers to circumvent a variety of obstacles designed to protect the device and its data from illicit access and use.[2]

Generative AI can significantly enhance physical security measures for ICS by analyzing data from surveillance systems, access control logs, and environmental sensors, generative AI can identify patterns, predict potential security breaches, and recommend optimized physical security protocols. It can simulate hypothetical scenarios to test vulnerabilities in facility layouts, personnel workflows, or equipment placement, ensuring proactive risk mitigation.

## ICS Network Architectures

The convergence of once-isolated ICS has helped organizations simplify the management of complex environments. Connecting these networks and incorporating IT components into the ICS domain introduces vulnerabilities asset owners must address before issues arise.

Contributing factors include:

- Insecure connectivity to internal and external networks,
- Technologies with known vulnerabilities, creating previously unseen cyber risk in the control domain, and
- Lack of a qualified business case or understanding of requirements for ICS environments.

The former isolation from external (and historically untrusted) networks allowed the organization to reduce the level of ICS security to those threats associated with having physical access to a facility or a plant floor. Most data communications in the ICS information infrastructure required limited authorization or security oversight because operational commands, instructions, and data acquisition occurred in a closed environment with trusted communications. In general, when someone sends a command or instruction via the network, they anticipate it will arrive and perform the authorized function, because only authorized operators have access to the system.

Merging a modern IT architecture with an isolated network that may not have any countermeasures in place is challenging. Using simple connectivity (that is, routers and switches) provides the most obvious way to interconnect networks; however, unauthorized access by an individual could result in unlimited access to the ICS. The diagram shown in Figure 6 depicts an integrated architecture that includes connections from external sources such as the corporate local area network (LAN), peer sites, vendor sites, and the Internet. The model comes from the International Society of Automation and provides insight into the widely accepted SP-99 (Purdue) Model of Control.

[3] NIST Special Publication 800-213: IoT Device Cybersecurity Guidance for the Federal Government

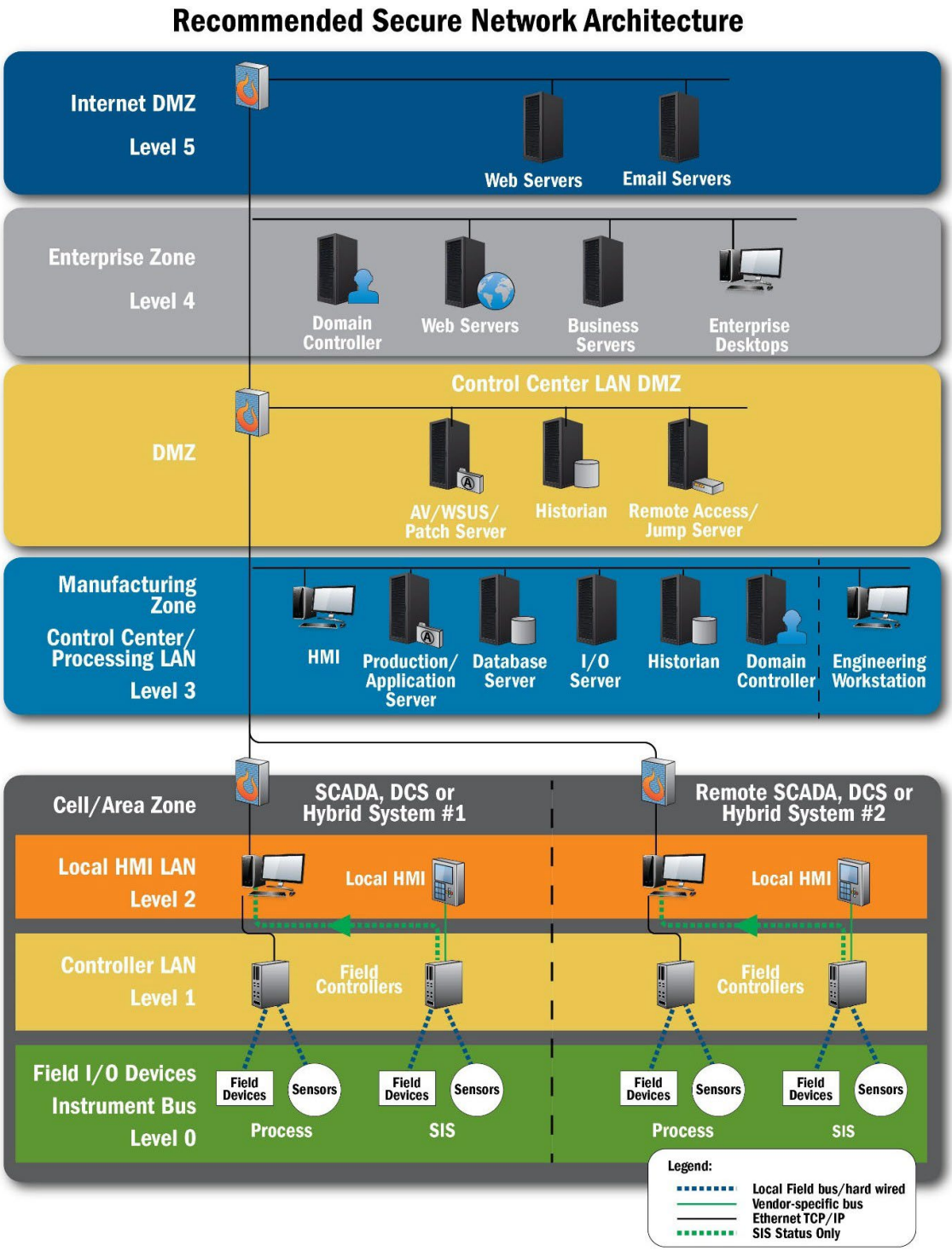



*Figure 6: Recommended Secure Network Architecture*

Integrated architectures, if compromised, could provide a threat actor with various avenues of access to critical systems—either via the corporate LAN, the control LAN, or even the communications LAN. The very nature of such architectures demands the exchange of data from disparate information sources, a factor intruders could

take advantage of. One emerging industry strategy for ICS defense-in-depth uses concepts such as the implementation of "zones and conduits" to secure communication pathways between trusted environments.[3]

## Common Architectural Zones

To create a layered defense, one must have a clear understanding of how all the technology fits together and where all the interconnectivity resides. Dividing common control system architectures into zones can assist organizations in creating clear boundaries in order to effectively apply multiple layers of defense. Understanding how to achieve network segmentation is vital to creating architectural zones and determining the best methodologies for segmenting networks within and around control system environments.

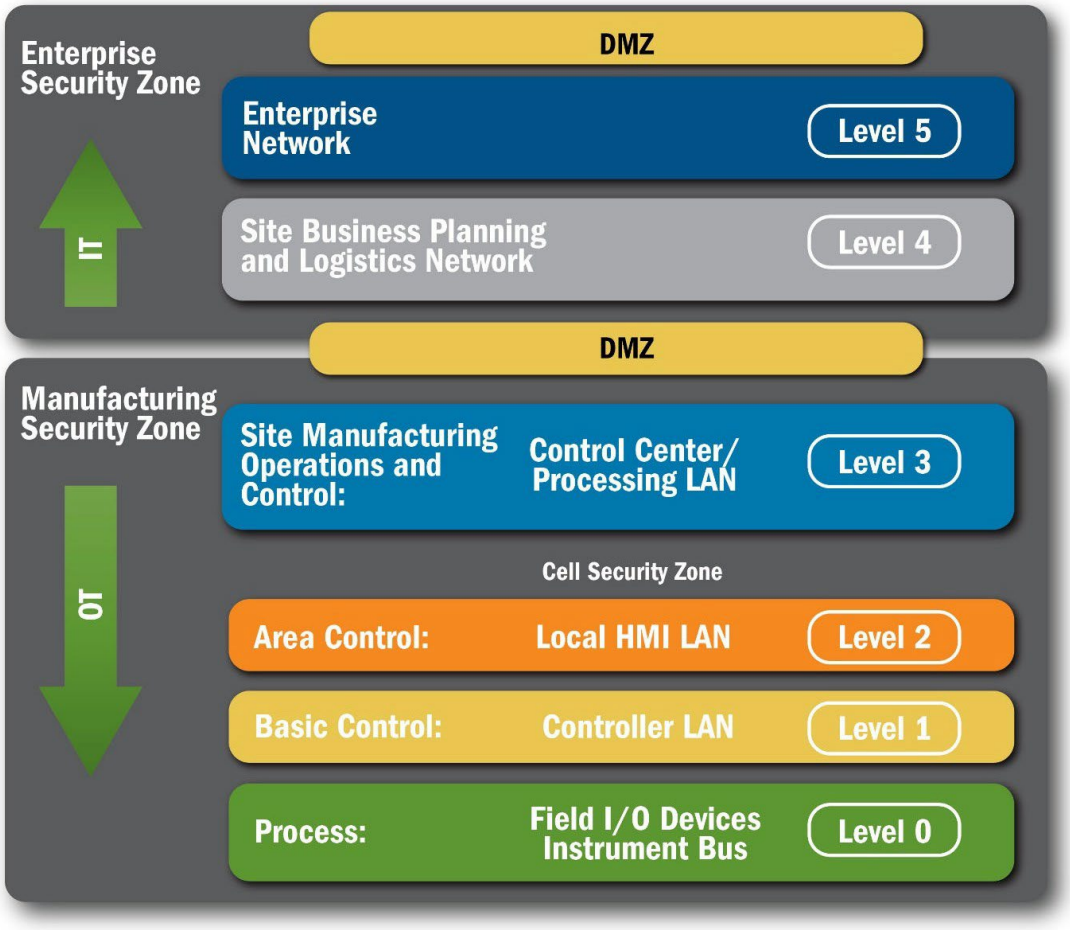



*Figure 7: Zone Segmentation of Business & ICS Architecture*

The zones depicted in Figure 7 segment business IT and OT networked information systems architecture into its basic functions:

[3] IEC 62443-3-2; Security for industrial automation and control systems—Security Risk Assessment and System Design

**Enterprise Security Zone:** The Enterprise Security Zone includes connectivity to the Internet, peer locations, and backup or remote offsite facilities (Enterprise network connectivity—Level 5) as well as the business networks that include corporate communication, email servers, Domain Name System servers, and IT business systems (Level 4). A wide variety of risks exist in this zone because of the number of systems and connectivity, and from an ICS security standpoint, one should consider this zone untrusted.

**Manufacturing Security Zone:** This zone (Level 3) contains the area of connectivity where a vast majority of monitoring and control takes place. It is a critical area for the continuity and management of a control network. Operational support and engineering management devices are in this zone, along with data acquisition servers and historians. The Manufacturing Zone is central to the operation of end devices and provides required connectivity to the Enterprise Zone. The priority of this area is high. Risks are associated with its direct connectivity to any external systems or networks.

**Cell Security Zone:** The Cell Security Zone contains systems used for local or remote area control (Level 2), such as field located HMIs, PLCs, and their controls (Level 1) and basic input/output devices such as actuators and sensors (Level 0). The priority of these zones is very high, as these are the areas where the control functions affect the physical end devices. In a modern control system network, these devices will likely have support for Transmission Control Protocol/Internet Protocol (TCP/IP) and other common protocols. It also may include safety-instrumented systems (SIS), which automatically control the safety level of an end device—elevating the risk. Ideally, one would locate the SIS on a separate network—ensuring safety systems continue to function and are not at risk of compromise in the event of an incident on the primary ICS network.

Each of these zones requires a unique security focus. A “peel-the-onion” analysis shows an intruder trying to affect a CI system would most likely go after the core control domains contained in Level 3 and below. This depends on the overall objective of the attacker. In general, complete control over core services and operational capability of the control system has high value. Manipulation of the ICS information resources can devastate an organization if this critical zone becomes compromised. In many sectors, the malicious intrusion on the control system will have real-world, physical results.

In an attack scenario, the intrusion begins at some point outside the control zone and the actor pries deeper and deeper into the architecture. Layered strategies that secure each of the core zones can create a defensive strategy with depth, offering the administrators more opportunities for information and resource control, as well as introducing cascading countermeasures that will not necessarily impede business functionality.

## Demilitarized Zones

A demilitarized zone (DMZ) (sometimes referred to as a perimeter network) is a physical and logical sub network that acts as an intermediary for connected security devices to help those devices avoid exposure to a larger and untrusted network, usually the Internet. The DMZ adds an additional layer of security to an organization’s LAN; an external intruder only has direct access to equipment within the DMZ, rather than any other part of the network.

The ability to establish a DMZ between the corporate and control networks represents a significant improvement with the use of firewalls. As shown in Figure 7, each DMZ holds one or more critical components, such as the data historian, the wireless access point, or remote and third-party access systems. Creating a DMZ requires that the firewall offers three or more interfaces, rather than the typical public and private interfaces. One of the interfaces connects to the corporate network, the second to the control network, and the remaining interfaces to the shared or insecure devices such as the data historian server or wireless access points on the DMZ network.

By placing corporate-accessible components in a DMZ, no direct communication paths are required from the corporate network to the control network; each path effectively ends in the DMZ. Most firewalls allow for multiple DMZs and can specify what type of traffic is forwarded between zones. The firewall can block arbitrary packets from the corporate network from entering the control network and can also regulate traffic from the other network zones including the control network. With well-planned rule sets, one can maintain clear separation between the control network and other networks with little or no traffic passing directly between the corporate and control networks.

The primary security risk in this type of architecture comes when a threat actor compromises a computer in the DMZ and uses it to launch an exploit against the control network via application traffic permitted from the DMZ to the control network. Organizations can reduce this risk if they make a concerted effort to harden and actively patch the servers in the DMZ, and if the firewall rule set only permits connections initiated by control network devices between the control network and DMZ. Other concerns with this architecture include the added complexity and the potential increased cost of firewalls with several ports. For more critical systems, however, the improved security should more than offset these disadvantages.

Two-zone solutions (no DMZ) are marginally acceptable, but one should only deploy them with extreme care. The most secure, manageable, and scalable control network and corporate network segregation architectures typically use a system with at least three zones, incorporating one or more DMZs.

Organizations could create multiple DMZs for separate functionalities and access privileges such as peer connections, the data historian, ICS communications protocols, the Inter Control Center Communications Protocol (ICCP) server in supervisory control and data acquisition (SCADA) systems, the security servers, replicated servers, and development servers. Multiple DMZs have proven effective in protecting large architectures composed of networks with different operational mandates. The secure flow of data into and out of the different environments is critical to operations.

One must be cautious when deploying DMZ solutions to connect otherwise logically separated domains. Do not assume the implementation of a DMZ is a panacea for preventing threat actors from penetrating deeper into critical environments. The exploitation of transitive trust across a security perimeter is a plausible intrusion vector. However, when one develops and deploys a DMZ with appropriate security, the countermeasure will increase the work effort for the adversary, provide more granular control for the asset owner, and reduce cyber risk to vital critical assets. Some high-level considerations one can use to support an effective defense-in-depth strategy utilizing DMZs are as follows:

- Asset owners should limit access to an ICS DMZ to only authorized users, applications, and services. Wherever possible, asset owners should model ingress and egress traffic to and from the DMZ so they can use additional security monitoring and anomaly detection at the payload level in addition to source/destination/service filtering.
- Access from the higher security zone (that is, from within control or operations levels) is generally to “push” data to the DMZ application and make that data available to the authorized enterprise users. Access for the enterprise user is only to pull from the DMZ application server, thereby providing further separation. It is important to create this logical separation so a threat actor cannot exploit the trust between the corporate enclaves in the DMZ to “pivot” from the DMZ into the control system. Asset owners often use DMZs for remote access. Allowing remote access creates a number of issues organizations must consider prior to documenting a policy and implementing a remote access process. Whether from the corporate network to the ICS or from the Internet to the ICS, remote access provides a serious risk to the system. An intruder can gain access to a user account at the user’s home or corporate office and use those stolen credentials to connect to critical ICS assets or allow an infected computer an access channel into the ICS networks via an established virtual private network (VPN) connection. The organization must decide what, if any, access they require from remote locations; whether a particular user truly needs that access (and if so, at what level); and how to harden the access process to reduce the risk to an acceptable level.
- Asset owners should only allow authorized external users to remotely connect to intermediary authentication servers residing in a DMZ. In addition to using multifactor authentication methods, definitive rules and connection states should be clearly identified and maintained. These servers (often referred to as “jump boxes”) provide connectivity to remote computers that are likely less secure than the jump boxes themselves. In addition to multifactor authentication and specific security related to user roles and least privileges, asset owners should harden jump boxes and any applications or services that do not support secure remote access removed.

Generative AI can strengthen DMZs for ICS, enhancing defense-in-depth strategies. By analyzing network traffic, data flows, and communication patterns, generative AI can identify vulnerabilities in DMZ configurations and recommend optimized architectures to prevent unauthorized access. It can simulate cyberattack scenarios to test the resilience of DMZs and refine rules for traffic filtering and segmentation. Additionally, generative AI adapts to evolving threats and operational changes, ensuring that DMZ configurations remain robust and

effective. This capability helps safeguard critical ICS networks by fortifying the boundaries between secure operational zones and external environments.

## Virtual LANs

A virtual LAN (VLAN) divides physical networks into smaller logical networks that consist of a single broadcast domain that isolates traffic from other VLANs. Using VLANs limits broadcast traffic and allows logical subnets to span multiple physical locations.

There are two categories of VLANs: static, often referred to as port-based, where one assigns switch ports to a VLAN so it is transparent to the end user; and dynamic, where an end device negotiates VLAN characteristics with the switch or determines the VLAN based on the IP or hardware addresses.

One must secure VLANs used in ICS environments explicitly, because default configurations and standard network configurations are not inherently secure. Virtual networking does not come without risks, because exploits known as “VLAN” hopping can create opportunities for an adversary to move between networks the asset owner has configured to be logically separated.

Many ICS network infrastructure designs deploy VLANs as part of segmenting network functions and capabilities. Current smart practices suggest that if the information infrastructure is large, then organizations should decompose each of the contributing control system domains (such as those within a plant or energy management system) into smaller and more manageable segments and zones. This methodology facilitates easier administration and can protect against unwanted traffic artifacts from “bleeding” from one network to the other. While the VLAN approach is becoming favorable in the control system community, it is equally important to understand and protect against the most prominent intrusion vectors associated with deploying virtual networks. Cybersecurity experts refer to these exploits as “VLAN hopping,” “double tagging” and “switch spoofing.” The countermeasures and defensive capabilities associated with protecting against these types of intrusions have evolved significantly over the past several years. Because the countermeasures are generally not a default component of the security architecture or the security technology used to support the information infrastructure, the effectiveness of the countermeasures often becomes a function of how one configures them.

> *“The most serious mistake that a user can make is to underestimate the importance of the Data Link layer, and of VLANs in particular, in the sophisticated architecture of switched networks. It should not be forgotten that the OSI stack is only as robust as its weakest link, and that therefore an equal amount of attention should be paid to any of its layers so as to make sure that its entire structure is sound.”*
>
> *–Virtual LAN Security Best Practices, Cisco Systems, Inc.*

The VLAN architecture needs to ensure the disabling of the Dynamic Trunking Protocol (DTP) and configure the switch ports as static access ports. This helps prevent switch spoofing exploits, because the access ports cannot handle tagged packets or become tagged ports. In addition, the unused switch ports become disabled—thus rendering them unavailable for any connectivity.

When one specifically configures the port as an access port, it cannot become a trunk port and cannot send traffic to other/multiple VLANs. If DTP is disabled, an intruder cannot use any access ports configured as dynamic to create a network relationship.

System administrators can counter double tagging by removing access ports from the default (native) and designating the native VLAN on all switched trunks to “unassigned.” Adversaries cannot match their port to one

on a different VLAN. Administrators should always select an unused VLAN as the native VLAN for all trunks. Administrators should not use this VLAN for any other purpose. They should prune VLAN 1 from all trunks and access ports that do not require it (including disconnected and shutdown ports). They also should not use VLAN 1 for in-band management traffic and should use a different, dedicated VLAN to keep management traffic separate from user data and protocol traffic.

The following is a concise set of activities that can empower the asset owner to create manageable ICS VLANs and reduce the risks associated with them:

- Control physical access by removing console-port cables and introducing password-protected console or virtual terminal access with specified timeouts and restricted access policies.
- Use a one-to-one relationship between subnets and VLANs. This requires the use of a router or multi-layer switch to join multiple VLANs. Many routers and firewalls support tagged frames so a single physical interface can route between multiple logical networks.
- Create role-based user accounts for all VLANs. Create an access-list to restrict Telnet/secure shell (SSH) access from specific networks and hosts.

Create and apply Layer 2 (L2) access control lists (ACL) and Virtual ACLs, blocking the direct communication at L2 between a potential attacker and the attacked device. Embed more intelligence into the network so it can check forwarded Address Resolution Protocol (ARP) packets for identity correctness.

- Use private VLANs to protect networks from unwanted traffic from untrustworthy devices.
- Enable port security.
- When feasible, prefer out-of-band management to in-band management.
- Limit the number of media access control (MAC) addresses used by a single port so the device traffic identification for a device is directly tied to its port of origin. Disable unused ports and assign them to an unused VLAN.
- Create and apply L3 ACLs by IP address (recommended for most static wired networks), MAC address filtering, port assignment, dynamic assignment (recommended for most wireless networks and shared switch port networks), protocols, and by applications. By default, treat only known and trusted ports as such, and configure all other ports as untrusted. This prevents attached devices from manipulating quality of service values inappropriately.
- Turn off VTP/MVRP and set DTP to “off” on all non-trusted ports. This is a smart practice for using VLANs within ICS, as it can limit (or even prevent) undesirable protocol interactions in network wide VLAN configurations. This precaution can also limit or prevent the risk of an administrator error propagating to the entire network.

Generative AI can enhance VLANs by analyzing network configurations and traffic patterns, generative AI can optimize VLAN segmentation to minimize lateral movement of cyber threats and ensure isolation of critical assets. It can simulate attack scenarios to identify vulnerabilities in VLAN setups and recommend tailored adjustments to improve security. Furthermore, generative AI can adapt dynamically to evolving ICS requirements, refining VLAN configurations to align with operational needs and emerging threats. This approach strengthens ICS cybersecurity by providing adaptive and proactive network segmentation solutions.

## ICS Network Perimeter Security

Once an organization has designed and implemented a robust network architecture, they have begun the process of establishing the security architecture for their network and systems. The security architecture includes the specific controls and their strategic placement within the network or systems to establish layers of security—defense-in-depth. Network diagrams and information flow diagrams that include all systems and their interconnections coupled with the physical inventory provide an operational-level understanding of the information flows within the network. The next step is to apply the appropriate overlay with requisite protection levels for each system or subsystem (assigned during inventory activities) to help determine the controls to put in place to protect the system without compromising or degrading its performance.

System administrators must consider the application of security controls at the network, system, application, and physical layers to provide information assurance. These include policy and security management, application

security, data security, platform security, network and perimeter security, physical security, and user security. The security architecture is where all the defensive mechanisms and controls come together and overlay the network architecture. The security architecture defines where to apply defense-in-depth measures across the organization. NIST 800-82, "Guide to Industrial Control Systems (ICS) Security," provides a community-wide ICS security controls overlay based on the NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," security controls overlay generalized concept.

Generative AI can identify vulnerabilities and recommend tailored perimeter defenses, such as optimized firewalls and IDS. It can simulate advanced cyber threats to test the resilience of perimeter security measures, enabling proactive adjustments of firewalls and IDS. Additionally, generative AI dynamically refines security protocols based on evolving risks and system changes, ensuring continuous protection against emerging threats.

## Perimeter Security

ICS perimeter security includes controls for both physical and logical security to protect the assets within those perimeters. The first consideration in logical perimeter protection is having a clear understanding of where the communications boundary exists. This requires evaluation to determine where threat actors could leverage potential intrusion vectors to infiltrate the ICS. Logical security includes controls such as authentication mechanisms, ACLs within network components, intrusion detection/prevention systems (IDS/IPS) signatures, situational awareness tools, and other means to protect the systems from a logical perspective. Physical perimeter security includes key cards to open doors, motion detection, cameras, security forces to respond to physical intrusion, and other mechanisms to protect physical assets.

## Firewalls

Network security depends on multiple components, each with specific roles. Firewalls are the first line of defense within an ICS network environment. These components keep the intruder out while allowing the authorized passage of data necessary to run the organization. Thus, the concept of network segmentation applies to the network in layers to protect assets at all levels.

Firewalls act as sentinels, or gatekeepers, between zones. When properly configured, firewalls allow only essential traffic cross security boundaries. If not properly configured, they could easily pass unauthorized or malicious users or content. Firewall rules monitor the network traffic and enable a trusted path to users and a trusted channel to other devices. This is only as effective as the accuracy of the rules with which the firewalls are configured.

The firewall Golden Rule states "that which is not explicitly allowed is denied," which means the final rule should not be "any, any," but rather "deny all."

The role of the firewall is to:

- Establish domain separation,
- Monitor (and log) system events,
- Authenticate users before they are allowed access, and
- Monitor ingress and egress traffic and disallow unauthorized communications.

There are two types of firewalls—the host firewall and the network firewall. Both host firewalls and network firewalls are crucial components in a layered cybersecurity approach.

- **Network Firewall:** The network firewall is typically a hardware device (although it can be a software solution) that sits between your internal network and the outside world (typically, the Internet). A network firewall is designed to protect a whole network rather than individual machines. It blocks or allows traffic based on a set of security rules the network administrator sets. These rules can be applied to all devices

behind the firewall. Network firewalls typically prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.

- **Host Firewall:** The host firewall is installed on individual devices or servers—hence the name "host". It is a piece of software that monitors and controls incoming and outgoing network traffic based on predetermined security rules. This means each device has its own set of rules that determine what traffic is allowed in or out. Host firewalls are particularly useful for controlling outbound connections, and they play an important role in preventing certain types of malware, such as keyloggers or botnet malware, from "phoning home" to an attacker's server.

Both types of firewalls serve a critical role in maintaining the security of networks and individual devices. They each have their strengths, and many organizations use a combination of both to achieve layered security—this way, even if an attacker can bypass one layer of defense, they will encounter another layer that could stop them.

The host firewall protects a specific host. It can be part of the OS, or it can be an appliance directly in-line with the host. The type of firewall used provides protection for the network using one of several techniques:

- Packet filtering
  - ⇒ This type of firewall filters traffic based on rules. They control traffic based on the first three levels of the open systems interconnection (OSI) model: MAC address and IP address, with some filtering based on the transport layer (port numbers).
- Circuit level gateways
  - ⇒ These types of firewalls allow only specific sessions to communicate.
- Proxy level gateways
  - ⇒ This firewall provides filtering at the application layer. In other words, it limits the types of applications and protocols that communicate across security boundaries such as File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and so forth.
- Stateful inspection
  - ⇒ Cybersecurity experts call this type of firewall stateful because it keeps track of the “state” of the connections crossing the firewall. They match the packets with the different types of connections to determine what to allow or reject.

Firewall placement should be coordinated, planned, and carefully thought through. The organization needs to ensure placement of the firewall does not enable an individual or device to bypass the security of the firewall. For example, a computer with two network interface cards (NIC), often referred to as a “dual-homed” host, introduces cyber risk when one card connects to the corporate network and the other connects to the process control network (commonly used for the convenience of Operations Managers, ICS engineers, and so forth). Even though this type of configuration eases management and reduces complexity, it effectively bypasses perimeter protection mechanisms (such as a firewall) and can create a significant vulnerability threat actors can exploit in virtual environments as well.

System administrators should layer the firewall rule set as shown in Figure 8. Smart practices apply at every level to ensure only the traffic specifically allowed at each level passes through the firewall. It is also critical to keep rules up to date, because even a slight change could reduce effectiveness against current intrusion vectors/vulnerabilities. Rule changes and rule order can affect data flow permissions, so test them to ensure the change does not negate security. Periodic reviews of firewall placement and rules will help ensure defenses are maintained.

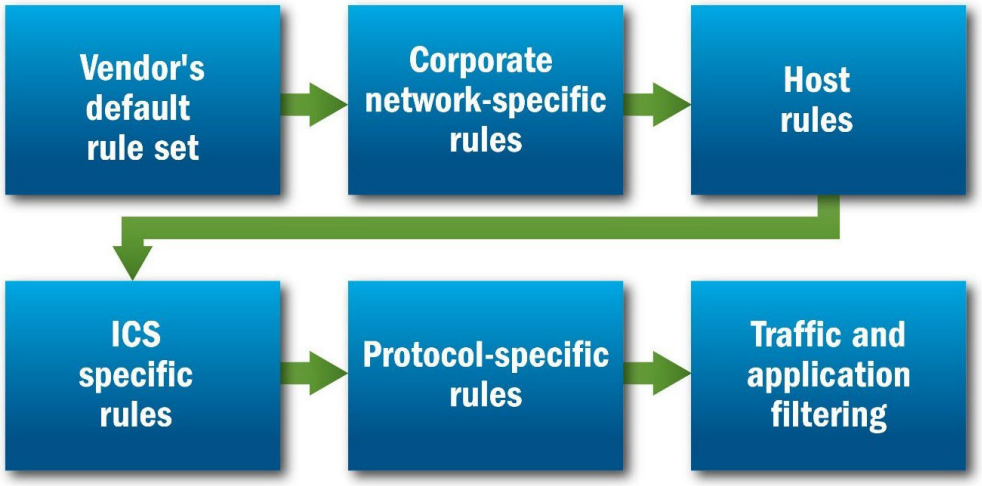



*Figure 8: ICS Firewall Rule Set Layers*

Improperly placing a firewall can result in the firewall being less effective. Bypassing the firewall, whether intentional or not, is a common occurrence. Modems that connect directly to process equipment, vendor VPNs that connect directly into the process control network, wireless access points, and dual-NIC computers all invalidate the effectiveness of the firewall.

Generative AI enhances the effectiveness of firewalls by analyzing network traffic patterns, system configurations, and potential threats, generative AI can optimize firewall rules and policies to block unauthorized access and detect malicious activities.

## Diodes

A unidirectional network device (also referred to as a unidirectional security gateway or data diode) is a network appliance or device that allows data to travel in only one direction. Users can find them most commonly in high security environments, such as defense, where they serve as connections between two or more networks of differing security classifications. This technology can now be found at the industrial control level for such facilities as nuclear power plants and electric power generation.

The physical nature of unidirectional networks only allows data to pass from one side of a network connection to another and not the other way around. The benefits for the users of the higher criticality (high-side) network, such as an ICS segment, include the ability to share data with a lower criticality (low-side) network, such as a server in a DMZ, while preventing communications access from the low-side network to the ICS network. Traditionally, when the enterprise network provides DMZ server access for an authorized user, the data are vulnerable to intrusions from the enterprise network. However, with a unidirectional network separating a high side with sensitive data and a low-side with business and Internet connectivity, one can achieve the best of both worlds, enabling the connectivity required and assuring security. This holds true even if both the low and the high network are compromised, because the traffic flow control is physical in nature.

The controlled interface that comprises the send and receive elements of a unidirectional network acts as a one-way “communications protocol break” between both two-way network domains it connects. This does not preclude the unidirectional network’s use in transferring protocols such as TCP that require communications (including acknowledgments) between sender and receiver.

The Electrical Sector has used data diodes for several years, and regulators have encouraged their use to protect equipment and processes in SISs. The Nuclear Regulatory Commission (NRC) now mandates the use of data diodes. Many other sectors, in addition to electrical and nuclear, also use data diodes effectively.

### Access and Authentication Controls

In most ICS networks, many different systems are used by a number of different users, and the systems must be accessed quickly as system operations requires. Corporate authentication, authorization, and account management practices can be problematic for ICS, because ICS are “always on,” and stopping the system for users to log out and log back in is usually not a viable option. Also, authentication processes provided by ICS suppliers may be limited. Managing many users in disparate locations becomes a challenge as one adds and removes system access and user roles change. The same authentication process may control access to many systems (HMIs, field devices, SCADA servers) and networks (remote substation LANs), which may require the use of shared credentials.

Asset owners can control access to ICS systems using either a distributed or centralized approach. Distributed access management requires that each system perform authentication separately. Each system uses a separate set of user accounts, credentials, and roles. This approach, while a good solution for small ICS implementations, does not scale well for large organizations.

Organizations normally use centralized account management to handle large numbers of users and accounts. Usually, it requires a central authentication system (for example, Active Directory or Lightweight Directory Access Protocol [LDAP]) to manage the accounts. An authentication protocol (for example, Kerberos, Remote Authentication Dial-In User Service [RADIUS], or Terminal Access Controller Access-Control System [TACACS]) communicates between the authentication server and the ICS. A centralized approach is scalable to large system implementations; however, it also introduces risk when used in ICS environments. The centralized servers must be highly secure because, if the authentication server becomes compromised, the entire ICS may be compromised. They are also required to be available in case of emergency, so one might need redundant servers, which can be expensive.

### Bring-Your-Own-Device

Operations, maintenance, and engineering personnel in ICS environments are increasingly utilizing portable computing devices such as tablets, smart phones, and laptops—a practice known as Bring-Your-Own-Device (BYOD). A number of organizations are actively promoting their use because of their popularity and the convenience of mobility while maintaining access. The problem with these devices stems from the fact the organization does not typically manage them, therefore the security policies implemented by the organization do not get implemented on the portable devices. People also use these devices to access personal email, game apps, webpages, and social media applications, so the inherent security risks of public access make BYOD inherently high risk to CI. The organization must consider the risk and enact appropriate measures, such as mobile device management (MDM) systems, to mitigate the risk associated with BYOD.

Generative AI enhances the security of BYOD policies by analyzing device behavior, network interactions, and user activity, generative AI can identify vulnerabilities and recommend tailored security measures to mitigate risks.

## Host Security

The host or workstation level implements another layer of security. Firewalls protect most devices within a network from intrusion from the outside; however, a good security model requires multitier layers of defense. This is particularly important for HMI clients that connect to the network from outside the trusted ICS network boundary, either via a VPN connection or any other means. Completely securing the network means securing all hosts as well.

Requirements for host security are well known in order to protect a machine/host while installing and using various OS and applications. The following guidelines provide some recommendations organizations should consider as part of a security policy for system operations to help keep ICS secure. In general, consider the following steps for every ICS host or device placed on the OT network, regardless of operating system:

- Install and configure a host-based firewall.

- Choose strong passwords for all accounts on the system and change any default or well-known accounts on the device (preferably, enforce strong passwords and password expiration through operating system capabilities).
- Change passwords on a pre-defined schedule—usually every 30 and not more than 90 days.
- Install screen savers with short intervals and with a password requirement to log in where possible.
- Install and keep operating system patches and hardware firmware patches current.
- Configure and monitor logs on the device.
- Disable unused services and accounts or those that are no longer necessary.
- Replace insecure services (such as Telnet, remote shell [RSH], or rlogin) with more secure alternatives such as SSH.
- Restrict access to services one cannot disable, where possible.
- Make and test backups of the system in a consistent manner if not centrally controlled.
- Secure laptops and other portable and mobile devices not continuously connected to the network.

The same requirements as stated above apply to these devices as well, where feasible, regardless of the platforms and management techniques used.

PLCs and other operational control technologies do not typically support many recommended host-based protection practices and security mechanisms. Defense-in-depth controls for those devices usually apply at the network level. However, many HMI systems are based on common platforms and administrators should lock them down (for example, disable unneeded services, disable unneeded ports, restrict access, use kernel locking) to the fullest extent possible while ensuring continued functionality. Asset owners should remove any software installed natively on the system they do not need or use. For example, an HMI used for command and control does not need standard corporate software packages such as word processing, spreadsheets, and email clients.

System configurations should be actively managed throughout the system life cycle. There are several techniques organizations can use such as creating a secure image to configure new equipment, equipment re-builds that only contain required software, and configuration of devices with only required services and ports.

Generative AI can significantly enhance host and endpoint security by analyzing endpoint activity, system logs, and threat intelligence, generative AI can detect vulnerabilities and recommend customized measures, such as enhanced malware protection, behavioral monitoring, and endpoint isolation protocols.

## Patch and Vulnerability Management

Applying patches to ICS components presents a challenge to system administrators, because system updates and patches can interfere with the ICS function. A patch to an ICS component could change the way it works, resulting in component failure or loss of functionality. System administrators should test all patches offline in a test environment that contains the same model and type of ICS to determine whether the patch has unintended consequences. Also, many ICS utilize older OS versions, which the vendor may not support.

System designers should separate any process for applying ICS patches from the corporate patch management solution, and the application of patches to ICS should occur only during planned outages. Organizations should develop a systematic patch and vulnerability management approach for ICS and ensure it reduces the exposure to system vulnerabilities while ensuring ongoing ICS operations.

Administrators should schedule software upgrades and patch management procedures at routine intervals, based on risk and criticality. The development of procedures to incorporate security patches promptly and current software recommendations on a regular basis can substantially limit opportunities for hostile parties to target newly discovered vulnerabilities, which receive wide and immediate publicity. Organizations should

institute practices to protect themselves without granting ample time for would-be intruders to apply the new knowledge against critical systems.[4]

Generative AI can revolutionize patch and vulnerability by analyzing system configurations, threat intelligence, and vulnerability databases, generative AI can prioritize critical patches and recommend tailored deployment strategies to minimize operational disruption. Additionally, generative AI enables real-time monitoring to identify emerging vulnerabilities and dynamically adapt patch management processes as threats evolve.

## Field Devices

Many field devices, such as older PLCs, remote terminal units (RTUs), and intelligent electronic devices (IEDs), are not capable of centralized management. They also may not have the security capabilities other components such as workstations may have (for example, limited password length and characters that can be used). Most often, asset owners physically protect these devices behind fences, behind locked doors, or in locked cabinets; however, they should also lock down their configuration once again to the fullest extent possible while ensuring continued functionality.

Field personnel are increasingly using portable devices such as tablets and smart phones for in-field control functionality. System administrators must secure these devices to the fullest extent possible, remove or turn off any unnecessary services (such as email capability), and keep them up to date with the latest security patches to ensure they do not introduce malicious code into the ICS. Furthermore, the organization should manage any device used to interface with the ICS to ensure it meets all corporate security standards.

Planning for IIoT components requires considerations that did not previously exist. IIoT devices are inherently interconnected and therefore require more stringent security controls. The devices are often geographically dispersed and only connected by wireless network connections not designed for updates. The acquisition strategy must address the requirement that devices be patchable or upgradable including ensuring device firmware be modifiable with the proper digital signature. An asset owner must assume a vendor may choose to discontinue support for devices in the future. Occasionally, a vendor may cease operations and therefore unable to meet any contractual obligations. Asset owners must plan for these contingencies. The full lifecycle of the IIoT device must be addressed in security planning.

Increasingly industry is looking to replace traditional IIOT devices with single board computers (SBC), which not only perform the same functions but, a lot more. Special considerations should be considered and evaluated when looking to use an SBC as an IIOT device. Many SBC's are mini-computers that run a Linux operating system (OS), in place of the traditional embedded OS variations. This IT/OT convergence of technologies, require for more traditional IT security controls to be in place to accommodate for the increased attack surface area. Such considerations could include OS hardening, deploying OS based firewalls, and security information event management (SIEM). Other considerations include supply chain. Many SBC's being introduced globally to the ICS environment originate from malicious nation states, and with OS code too originating from potentially malicious nation states could provide a backdoor, for a potential future cyber-attack.

In addition, IIoT devices should be designed to provide network connectivity with bandwidth appropriate for the intended application and not higher. This approach will limit the risk associated with IIoT devices being used for distributed denial-of-service (DDoS) attacks.

AI significantly enhances the security of field devices such as PLCs and RTUs by continuously monitoring device behavior, communication patterns, and operational data, AI can identify anomalies and potential vulnerabilities in real time. It enables rapid detection of unauthorized access or suspicious activities, supporting swift mitigation actions. Additionally, AI can analyze system configurations and recommend tailored security measures, such as firmware updates or enhanced access controls, to protect these critical devices.

---

[4] Caswell, Jayne, Survey of Industrial Control Systems Security

### Virtual Machines

Asset owners are implementing and leveraging virtual machine (VM) technology as a method of reducing capital equipment, managing device recovery, and running multiple disparate guest OS on a single physical host machine. In many industry implementations, asset owners apply inadequate user access security controls to the hypervisor host management interface—inadvertently providing a single point of entry threat actors could use to control every guest VM on the host.

- Place these interfaces in management networks with strict and logged zone access control.
- When the physical host contains both DMZ and ICS servers, administrators should harden the networks and NICs and delete all others to prevent opening a bridged scenario.
- Patching hypervisors is critical, and, when doing so, the OT and IT departments should coordinate to avoid impact to ICS processors.

## Security Monitoring

Monitoring systems and networks for changes, anomalous behaviors, or for attack signatures can be difficult in an ICS environment; however, monitoring and detection capabilities are essential to the defense-in-depth concept of protecting critical assets. Having an electronic boundary around the ICS is not sufficient to protect critical assets from unauthorized access, because for each protection put into place in a network environment, threat actors can find a method around it. The concept of defense-in-depth says a system must detect and alert an organization of an intrusion early on so they can take defensive action before critical assets are breached. Most IT organizations have some level of monitoring at the corporate level, but they rarely implement it in the ICS networks.

Without system monitoring in place, intruders could breach the system and no one would know of the intrusion before attackers achieved their objective—if it was ever detected at all. While the ICS vendor community is becoming more aware of the need for centralized monitoring of ICS security, the integration of standard monitoring capabilities into ICS is in its infancy. Asset owners can and should take action to ensure security personnel and OT operators know of changes to systems or behaviors that indicate a potential network intrusion.

Organizations can monitor networks and collect information about networks in many ways, such as:

- Utilizing centralized syslog servers for Linux and network devices and to centrally collect Windows Events using WinRM (Windows Remote Management) and WEVTUTIL (Windows event log tool) utilities. (It is important to note organizations must review these event logs).
- Security information and event management (SIEM) solutions combine security information management and security event management and can collect, log, and correlate information from multiple sources and alert on anomalous or specified activity and/or provide real-time analysis.
- Canaries and honeypots/honeynets can also flag any unauthorized intrusion, and asset owners may consider them for use in high-criticality/high-risk areas.

### Intrusion Detection and Prevention Systems

ICS environments provide a unique opportunity when considering protection mechanisms to place on the network: despite considerable network traffic, that traffic is very predictable. For example, in a typical ICS environment, the PLC communicates in a standardized way with the HMI and the historian; all applications and services on the PCS network are known (or should be); and the protocols, web traffic, and proprietary traffic are known and predictable.

Asset owners can use an IDS solution to easily monitor and create alarms for any traffic outside normal operations. An IDS is based on the passive monitoring of network traffic. Expected network traffic is deterministic, and deviations are used as triggers for alerting. Simple rules can be written to monitor for IP sources and destinations, protocols, lengths of packets, and so forth. Also, many ICS vendors can provide traffic signatures for their equipment.

IPS solutions are in-line with firewalls or ICS equipment and can act by blocking traffic that does not meet the defined rules. Many vendors and asset owners become nervous about using IPS, because it has the potential to stop a process (and therefore stop operations). However, because of the deterministic nature of ICS traffic, they can be tuned to trigger only on extreme anomalies.

IDSs/IPSs are a vital part of the defense-in-depth strategy because so many inherent vulnerabilities are within the ICS network, and an individual can only do so much to monitor unwanted traffic. An IDS/IPS provides an automated way to watch for and respond to the unexpected. However, IDS/IPSs cannot do everything, as shown in Figure 9.

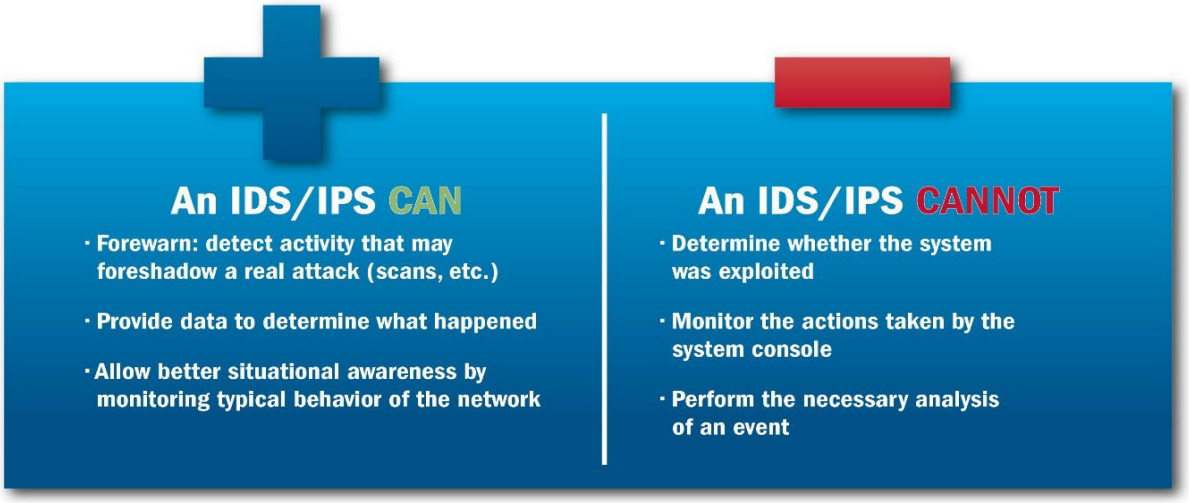



*Figure 9: IDS/IPS Limitations*

An IDS is not limited to being network-based. A host-based IDS (HIDS) monitors the state of the computer. Application-level detection systems (ALDS) monitor an application's state.

Using IDS to monitor the network and/or system is not a "silver bullet." An IDS is more of a warning or audit system. IDSs can alert to possible misconfigured systems on the network and will alert when an intruder is compromising a system using a known method. It often takes more than one method or device to provide the most complete information about an event. All methods of intrusion detection involve the gathering and analysis of information from various sources within a computer, network, and enterprise to identify threats posed by adversaries inside or outside the organization. File integrity checking tools are common in most environments.

There are a few open-source HIDS on the market that perform log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response. The main issue with any HIDS in any environment (especially ICS) is the computer resource penalty incurred to get a particular user required security level. Table 3 identifies signature versus anomaly detection and their characteristics.

*Table 2: Signature versus Anomaly-Based Detection*

| Detection Method Characteristics |
|---|

| | |
|---|---|
| Signature-based Detection: | • Watches for specific events<br>• Only looks for what it has been told to look for<br>• Can deal with any known threat<br>• Unaware of network configuration changes<br>• Highly objective inspection<br>• Predictable behavior<br>• Easy to tune manually |
| Anomaly-based Detection: | • Watches for changes in trends<br>• Learns from gradual changes<br>• Can deal with unknown threats, but any intrusion is subject to a false negative<br>• Sensitive to changes in network devices<br>• Subjective, prone to misinterpretations<br>• Unpredictable behavior<br>• Must trust the system completely |

*Table 3: Detection Basis Considerations*

| Selection Considerations | |
|---|---|
| Signature-based Detection: | • Scans network traffic (packets) for known patterns<br>• Only scans traffic on or from its home network<br>• Can scan both sides of a conversation<br>• Could be reactive and block traffic (IPS mode)<br>• Does not differentiate traffic—often does not know whether a system is Windows, Linux, or a PLC |
| Anomaly-based Detection: | • Must teach system to identify “normal” network traffic (and what if learning period includes attacks?)<br>• Detects deviations from normal behavior<br>• More difficult to spoof<br>• Needs no foreknowledge of attack signatures<br>• May raise more false positives<br>• Very hard to implement in a dynamic environment<br>• Unpredictable behavior<br>• Must trust the system completely |

Like firewalls, organizations must strategically locate IDS sensors to obtain the most value. As a general rule, they should locate them in high traffic locations and/or between security boundaries or networks with sensitive information.

Network-based IDSs/IPSs scan the network topology for “bad” traffic while HIDSs/ALDSs monitor each host and report to a central logging facility. The central logging system needs to be a very secure system to prevent bypassing and perhaps inactivating the systems. Attach a NIDS/IPS to the modem pool and wireless access points. Statistically, this is the most often forgotten entry point for “bad” traffic.

Organizations should view alerts as similar to process alarms. Process alarms alert operators to process conditions that warrant attention. Likewise, intrusion detection alarms alert network operators to network conditions that warrant attention. Use basic logic when configuring alarms and alerts. For example, if a user typically logs on between 0800 and 1600, and for any reason logs on at 0300, the IDS should detect this activity and generate an alert. Anomaly detection is difficult to implement in a typical IT network because of the dynamic nature of the environment; however, ICS networks and systems’ predictability lends itself well to the use of these technologies.

Potential complications with using IDS/IPS include that it takes a significant amount of work to write rules and requires thorough testing to ensure the rules function properly. In addition, an IPS can modify/drop legitimate packets if the rules are written improperly. This could prevent alarms from reaching the operator or configuration changes from reaching their intended destination; therefore, it may require great care and significant testing to ensure unintended consequences are not introduced into the system. Many organizations use IDS with quite sophisticated functionality for managing security zones for this purpose.

AI enhances IDS and IPS by offering advanced, adaptive capabilities for stronger cybersecurity. By analyzing network traffic, user activity, and system logs, AI can identify anomalies and emerging threats with exceptional speed and accuracy. It enables predictive threat detection, ensuring IDS can flag risks early while IPS proactively prevents malicious actions. AI-driven systems can dynamically adapt to evolving attack techniques and system changes, maintaining continuous protection. This intelligent approach significantly improves the efficiency and effectiveness of IDS and IPS, fortifying organizational resilience against sophisticated cyberattacks.

## Security Audit Logging

Security audit logs provide information about login activity, resource use, file modifications, and other security-relevant information. Without properly configured and maintained auditing and logging practices in place, incident response teams often cannot determine the significance of a potential event. Properly configured audit logs at the network, host, and application levels provide critical information for determining how an incident occurred, the impact and scope of the issue, and how best to deter future events.

Comprehensive log management and analysis policies establish the minimum requirements for devices, OS, and applications. Security control settings and user access controls enforce those requirements. When asset owners do not configure systems and applications to capture key events, they fail to capture important event data, and incident response teams may not have sufficient information to determine the cause of an event. A baseline of expected traffic and process functionality for normal and off-normal operations and system use allows security, process control, and control systems operations personnel to isolate unusual data traffic or user actions that may indicate potential security-impacting events.

Newer OS and applications provide more detailed configuration and event auditing options than their legacy counterparts; however, using the default configuration for most operating and application logs only provides minimal audit capabilities, and organizations may miss a critical event. It is important control system administrative and security personnel perform a review of all audit capabilities and configure the systems to provide the data needed to both capture all potentially relevant events and to ensure the settings do not generate unneeded logs that can overwhelm system storage capacities. Also, default configurations may allow data to be overwritten; therefore, export all logs to a central server or event management capability to ensure they are available if needed.

AI enhances security audit logging by automating and optimizing the collection, analysis, and interpretation of log data. By processing vast amounts of logs in real time, AI can identify anomalies, detect potential threats, and flag suspicious activities with greater accuracy. It simplifies the correlation of log data across systems, enabling comprehensive insights into cybersecurity events. AI also supports predictive analytics, anticipating vulnerabilities based on patterns in audit logs.

### Security Incident and Event Monitoring

SIEM technologies support the incident response process, but they can support ICS operations as well. When configured and analyzed correctly, the data can assist in predicting equipment failure, equipment capacity, and failure points as well as providing security information. Asset owners can configure them to provide alerts when a potential security intrusion occurs, and they can aggregate a vast amount of audit data that accumulates from ICS components. By providing visibility into aggregated security data, SIEMs can minimize incident response time.

A SIEM centralizes data from network devices, OS, applications, and databases within complex environments, such as control system networks. It streamlines the audit log review process, by porting logs from multiple systems into one solution that eliminates the time and effort required for manual log reviews. Organizations can set up a SIEM to integrate multiple log formats from widely distributed sources and collect the information both remotely and automatically. The SIEM can also integrate IDS/IPS information and scanning results and generate alerts on identified traffic patterns. A SIEM's analysis engine speeds data processing and formatting time, making it cheaper and easier to review functional, operational, and security data. In addition, using a SIEM provides the ability to select specific events for compliance reporting, root cause failure analysis, and incident detection.

## Vendor Management and Security

Vendors represent a special case within the framework of a strong defense-in-depth program. Over the past several years, vendors have become aware of the importance of cybersecurity in industrial control solutions and, in many cases, have incorporated security into their product life cycle to meet emerging market demands. Although not every vendor is taking this approach, many of the leading vendors are. They have seen the cyber vulnerabilities associated with ICS—especially after the publicity of exploits such as Stuxnet, structured query language (SQL) Slammer Worm, and others. One should not assume, however, that vendors always follow stringent security practices. The organization should present and address requirements for control system security in great clarity early in the procurement process. This is not only advantageous to the asset owner but also provides vendors specific guidance on what functionality they need.

Over the past several years, asset owners and vendors have benefited from a tremendous amount of work done in developing procurement guidance. This guidance has resulted in progress toward securing several vendor solutions applicable to many different sectors. The Department of Energy (DOE) developed procurement language considerations to help ensure products meet requirements. This guidance document provides baseline procurement language for use by asset owners, operators, integrators, and suppliers during the procurement process. In addition, a more generalized procurement language document for ICS is available. Asset owners from all sectors may use this procurement language for purchasing equipment, for managing and monitoring ICS security developments, and to ensure the solution meets the organization's requirements.

AI enhances vendor management and security by automating risk assessments, monitoring vendor activities, and optimizing collaboration processes. By analyzing vendor data, contracts, and compliance records, AI can identify potential vulnerabilities or risks associated with third-party relationships. It supports continuous monitoring of vendor interactions and access to critical systems, ensuring adherence to security protocols.

### Supply Chain Management

The supply chain represents a significant risk to ICS. ICS manufacturers and software developers create their products in many different locations around the world. Ensuring the security of the system or application throughout its development life cycle is impossible for most ICS operators. Purchasing commercial off-the-shelf (COTS) technologies increases the likelihood of receiving non-genuine equipment. TSA is aware of reports related to equipment with embedded unauthorized code in its firmware or operating system that provides a back door into the equipment or allows the program to "call home" once installed. To help mitigate these threats, asset owners must pay careful attention to procurement contract arrangements, quality control, and validation of

performance to specifications processes. In addition, exhaustive testing, including vulnerability scanning, is an important task to perform before installing systems in production environments.

NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations (April 2015)," defines the supply chain compromise as, "An occurrence within the Information and Communications Technology (ICT) supply chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits. An ICT supply chain compromise can occur anywhere within the system development life cycle of the product or service." (Please note, NIST 800-161 Rev.1, released May 2022, is the most current version of the above-referenced document).

Supply chain compromises have occurred in the ICS/IT environment for a number of years. A typical compromise includes some or all the following:

- Network or computer hardware with malware installed,
- Software or hardware with malware inserted by various means,
- Vulnerabilities in software applications and networks within the supply chain, and
- Counterfeit computer hardware.

Of particular concern in supply chain risk is the information regarding the operation of sensitive hardware/software vendors generally provided on their websites. Threat actors can easily find default passwords, operational instructions, vendor manuals, and information provided by the users of software and/or hardware on the Internet (in white papers, blogs, social media, and so forth). Adversaries armed with this information are well equipped to compromise these systems.

In the long term, ICS owners should work with vendors and encourage them to design ICS using attack-resilient algorithms and architectures and to design and operate control systems to survive an intentional cyber assault with no loss of critical functions. The goal should be to design systems whereby even if intruders manage to bypass some basic security mechanisms, they will still face several control-specific security devices that will minimize the damage done to the system.

AI enhances supply chain management by optimizing operations, increasing transparency, and mitigating risks. AI can predict demand trends, optimize inventory levels, and improve production planning to reduce costs and inefficiencies. It provides real-time visibility across the supply chain, enabling swift identification of disruptions and proactive responses. Additionally, AI supports risk management by identifying potential vulnerabilities, such as supplier delays or geopolitical impacts, and recommending contingency strategies.

## Managed Services/Outsourcing

Many organizations utilize managed services and/or outsourcing for functions that require highly specialized technologies and/or skills. It is common for organizations to outsource many IT security functions such as incident response forensics, cyber vulnerability assessments, risk management, supply chain management, or other functions they rarely use or those that require expertise the organizations do not have. The primary advantage of outsourcing is it is cost effective. Maintaining a full-time forensics staff, for instance, is costly due to their high level of expertise, yet an organization needs them during incident investigations.

A service-level agreement (SLA) is a common means of identifying the service requirements for the outsourced firm's responsibilities. If the firm does not meet the requirements of the SLA, the organization reserves the right to terminate the contract. When engaging with an outside entity for security services, it is important both sides agree on roles, responsibilities, incident handling and reporting, as well as the security of any interconnections, remote access policies and procedures, or interfaces a user may require. In addition to the SLA, organizations should develop a memorandum of understanding/memorandum of agreement (MOU/MOA) and interconnection security agreement (ISA) to outline the specific management and technical requirements for the services.

When engaging with an outside party to perform technical assessments or testing, all parties should establish and agree on rules of engagement (RoE). Cyber vulnerability assessments typically require some level of passive or active scanning or testing on the target systems, which means the assessors must either access or watch others access critical cyber assets within the control system environment. The assessment team lead works with their organizational counterpart to ensure testing activities do not interfere with client operations and

agree on action and notification protocols should the activity cause any problems for the organization. The RoE includes direction about what activities may take place in what systems and who may perform those activities. It includes decisions about whether testing takes place within the primary (active production) control system or some credible substitute such as a backup or secondary control system, a test network, or stand-alone system. Avoid active scanning production control systems, as they can cause operational issues or create a denial-of-service condition. Passive activities, such as network sniffing, may be adequate. If using a substitute system, compare it to the active system to ensure they are identical in operation. The assessment team and the organization will also need to agree on who will have their "hands on the keyboard" during testing—especially when active (production) control systems are the target. Local personnel should perform all tests on an active control system at the direction of the assessment team.

## Leveraging Cloud Services

Some ICS organizations are using cloud services for data storage and are considering other ways to make use of them for additional services in support of their ICS architectures. From a security perspective, any portion of any externally hosted ICS architecture must provide a level of security hardening commensurate with the criticality of the function it hosts. In addition, the organization must consider ICS information integrity, security, and confidentiality, as well as the functional and operational details associated with recovery, event/incident management, failover, forensic support, monitoring, and other operational sequences that require special support by the cloud-hosting service provider. Other areas organizations can overlook when considering shifting resources to the cloud are the reliance on Internet service provider (ISP) connections on premises and the potential bandwidth increases that can take place. Legal instruments and the use of SLAs are important because all operational support requirements must be explicitly identified to ensure the expectations for support by the cloud providers, ISP availability, and bandwidth capacity are fully covered to avoid surprises later if an operational issue arises. There are other issues to consider as well, including the effects of load balancing and other possible impacts if the cloud provider experiences a surge in the use of their available resources.

## The Human Element

Organizations face many challenges in managing the human factor within ICS organizations. Large and complex systems are susceptible to human error as well as the activities of malicious insider threats.

Insider threats are vulnerabilities posed by individuals with authorized access to sensitive or secure areas, systems, or information within the organization. Insider threats may involve employees, contractors, or trusted individuals who exploit their insider status to intentionally or unintentionally compromise the security, confidentiality, or integrity of an organization's operations, assets, or data.

Insider threats can take various forms, including:

- **Unauthorized Disclosures:** Insiders may intentionally or inadvertently disclose sensitive or classified information to unauthorized individuals or entities.
- **Sabotage:** Insiders with malicious intent may deliberately sabotage or disrupt operations, systems, or infrastructure, leading to security vulnerabilities, delays, or other negative impacts.
- **Theft or Misuse of Information:** Insiders might unlawfully access, copy, or steal sensitive information, such as passenger data, security procedures, or operational plans, for personal gain, espionage, or other malicious purposes.
- **Bribery or Corruption:** Insiders can be susceptible to bribery or coercion, compromising the integrity of security protocols, processes, or decision-making within the organization.
- **Unauthorized Access or Abuse of Privileges**: Insiders may misuse their authorized access privileges to bypass security measures, exploit vulnerabilities, or gain unauthorized access to restricted areas or systems.

## Policies

Clear, actionable policies are necessary to lay the framework for rigorous controls that secure ICS technologies and provide the governance needed to manage human factors. Policies lay the framework for detailed procedures and set the expectations of the organization with regard to the functions performed. Policies outline the rules regarding securing the ICS—stating expected rules of behavior and requiring controls. Policies outline what must and must not occur and set forth sanctions for noncompliance.

## Procedures

Historically, security management was the responsibility of the corporate IT security organization, usually governed by operating plans and procedures that protect vital corporate information assets. As ICS become part of larger conjoined network architectures, organizations must update security procedures to cover the control system domain as well.

Organizations should design procedures to state how personnel should conduct a particular process, or configure a particular system, to ensure secure functioning and provide a standard, repeatable means to accomplish a task in a safe manner. ICS security procedures also allow an organization to quickly train new personnel and to ensure they follow all required regulations and standards uniformly across the OT space. ICS security procedures also instruct ICS operators on the steps to take to protect the ICS from a cyber-based intrusion. Network-based security procedures are especially important for the ICS domain, because the use of unique vendor-specific protocols and legacy systems may hamper efforts to protect mission-critical systems.

## Training and Awareness

Many organizations overlook security training and awareness activities more often than many other areas in ICS operations. OT owners and operators rely on their intimate system and process knowledge to ensure the proper functioning of the system, and they usually allocate training time and resources only for system functionality-related purposes. As ICS become more interconnected and cyber threats and vulnerabilities rise, it is critically important for organizations to ensure they require and support ICS security-specific training. IT implementers and OT operators should know what the indicators of potential compromise look like and what steps they should take to ensure a cyber investigation succeeds. IT and ICS management should also know what they can do to make the system more secure so they can make informed decisions with regard to the cost/benefits of the protection measures they put into place.

# 3. GENERAL STRATEGIES FOR SECURING ICS

## Security and Risk Standards

An organization may need to consider one or more existing security and risk standards and guidance as a basis for securing and managing ICS depending on the CI Sector. These standards may apply as required by law or the authoritative governing body for that sector. These standards and guides may assist an organization to develop a robust ICS security and risk management program based on industry smart practices.

## NERC-CIP

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to ensure the reliability of the bulk power system in North America. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization (ERO) for North America, subject to oversight by the Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.

The NERC Critical Infrastructure Protection (NERC CIP) standards provide a set of requirements and considerations for protecting bulk power system assets, but they are also applicable to other industries as smart practices for protecting ICS.

## NIST ICS Framework

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

The NIST ICS framework provides a comprehensive set of recommendations for securing ICS. Organizations can use it alone or in conjunction with other NIST standards, such as its Special Publication (SP) series, notably:

- NIST SP 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach,"
- NIST SP 800-39, "Managing Information Security Risk – Organization, Mission, and Information System View,"
- NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and
- NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security."

## Specific Subsector Guides

Many CI subsectors have created guides to use when applying security solutions to ICS environments. These guides provide requirements and directions for protecting ICS assets that support specific functions within each sector.

## Electricity Subsector Risk Management Process

DOE developed the Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline in collaboration with NIST, NERC, and broad industry participation. The RMP is written with the goal of enabling organizations—regardless of size or of organizational or governance structure—to apply effective and efficient RMPs and to tailor them to meet their organizational requirements. Organizations can use this guideline to

implement a new program within an organization or to build on an organization's existing internal policies, standard guidelines, and procedures.

## AWWA Process Control System Security Guidance for the Water Sector

In February 2013, the American Water Works Association (AWWA) Water Utility Council initiated a project to address the absence of practical, step-by-step guidance for protecting Water Sector PCSs from cyberattacks. The goal of the AWWA guidance is to provide Water Sector utility owners/operators with a consistent and repeatable recommended course of action to reduce vulnerabilities to cyberattacks. In an effort to provide water utilities with actionable tasks, they developed a cybersecurity guidance tool to present recommended controls to users in a concise, straightforward manner. The AWWA guidance tool represents a voluntary, sector-specific approach for adopting the NIST Cybersecurity Framework as expressed by the Water Sector Coordinating Council.

## Chemical Facility Anti-Terrorism Standards

The Department of Homeland Security (DHS) has released a final rule that imposes comprehensive federal security regulations for high-risk chemical facilities. This rule establishes risk-based performance standards for the security of our Nation's chemical facilities. It requires covered chemical facilities to prepare security vulnerability assessments, which identify facility security vulnerabilities, and to develop and implement site security plans, which include measures that satisfy the identified risk-based performance standards.

# 4. TOOLS AND SERVICES SUPPORTING ICS DEFENSE-IN-DEPTH

TSA provides subject-matter expertise, tools, and inspection services to assist TSA associated organizations in the improvement of their ICS asset security posture. TSA provides assessment services at no cost to organizations. In its role as a regulatory agency, TSA consider all inspections and assessments as collaborative exercises toward a common goal—raising the cybersecurity posture of CI across the U.S.

## Validated Architecture Design Review (VADR)

A Validated Architecture Design Review (VADR) evaluates your systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. VADRs are based on standards, guidelines, and smart practices and are designed for OT and IT environments. A VADR includes:

- Architecture Design Review
- System Configuration and Log Review
- Network Traffic Analysis

## TSA Cyber Security Evaluation Tool (CSET®)

The Cyber Security Evaluation Tool (CSET®) TSA is a web-based tool that guides asset owners and operators through a systematic process of evaluating their OT and IT cybersecurity posture, addressing topics such as hardware, software, administrative policies, and user obligations. The CSET TSA tool contains an extensive collection of assessments comprised of a series of plain-language, targeted questions designed to assist users in evaluating their cybersecurity practices.

CSET TSA users answer a series of questions based on user-selected cybersecurity standards or smart practices (e.g., NIST SP 800-82, NIST SP 800-53, CFATS, NRC, NERC-CIP, etc.). The tool uses the answers to develop a report that baselines the cybersecurity posture of the target system.

A CSET TSA evaluation usually takes about 1 day. Typically, the CSET TSA assessment includes both a key requirements assessment and a component assessment. The tool uses integrated network maps to provide a visual representation of the current security state of the system, identify the component targets for the assessment, and provide guidance on where to place cybersecurity protection mechanisms to provide the most value to the organization.

CSET TSA provides:

- A framework for analyzing cybersecurity vulnerabilities associated with an organization’s overall ICS and IT architecture,
- A consistent, technically sound methodology to identify, analyze, and communicate the various vulnerabilities and consequences in an organization's threat landscape,
- The means for the user to document a process for identifying cybersecurity vulnerabilities, and
- Suggested methods to evaluate options for improvement based on existing standards and recommended practices.

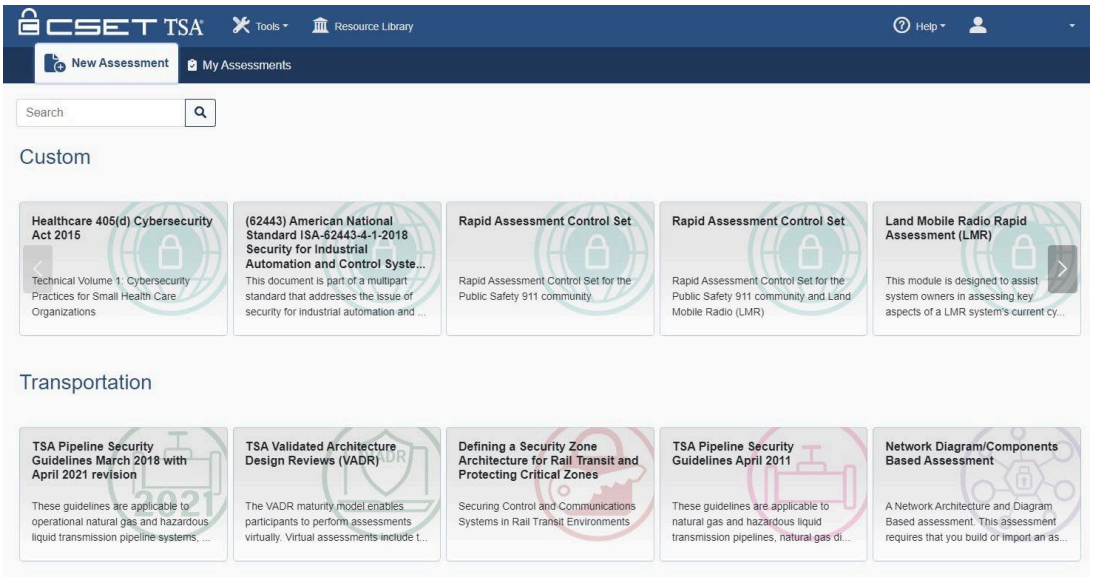



*Figure 10: CSET TSA Assessment Gallery*

## CIS 8

The CSET TSA integrated CIS Critical Security Controls (CIS Controls) are a prioritized set of safeguards to mitigate the most prevalent cyberattacks against systems and networks. They are mapped to and referenced by multiple legal, regulatory, and policy frameworks. CIS Controls v8 has been enhanced to keep up with modern systems and software. Movement to cloud-based computing, virtualization, mobility, outsourcing, Work-from-Home, and changing attacker tactics prompted the update and supports an enterprise's security as they move to both fully cloud and hybrid environments.

The CIS Controls are updated and reviewed through an informal community process. Practitioners from government, industry, and academia each bring deep technical understanding from across multiple viewpoints (e.g., vulnerability, threat, defensive technology, tool vendors, enterprise management) and pool their knowledge to identify the most effective technical security controls needed to stop the attacks they are observing.

In addition to the TSA adoption of CIS 8, the controls have been endorsed and referenced by multiple critical infrastructure authorities, including:

- NIST Cybersecurity Framework as a recommended implementation approach for the Framework.
- The European Telecommunications Standards Institute (ETSI) has adopted and published the CIS Controls and several of the Controls companion guides.
- In 2016 in her state's Data Breach Report, Kamala D. Harris, then California Attorney General, said: "The set of 20 Controls constitutes a minimum level of security – a floor – that any organization that collects or maintains personal information should meet."
- The CIS Controls are recommended by organizations as diverse as the National Governors Association (NGA) and the U.K.'s Centre for the Protection of National Infrastructure (CPNI).
- The National Highway Traffic Safety Administration (NHTSA) recommended the CIS Controls in its draft security guidance to automotive manufacturers.

## C2M2

CSET TSA has adopted and integrated the Cybersecurity Capability Maturity Model (C2M2), a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both IT and OT assets and environments.

Organizations can use the C2M2 to consistently measure their cybersecurity capabilities over time, identify target maturity levels based on risk, and prioritize the actions and investments that allow them to meet their targets. The model contains more than 350 cybersecurity practices, which are grouped by objective into 10 logical domains. Each practice is assigned a maturity indicator level (MIL) that indicates the progression of practices within a domain.

Practices within each domain are organized into objectives that can be achieved by implementing the practices in the domain. For example, the risk management domain comprises five objectives:

- Establish and Maintain Cyber Risk Management Strategy and Program
- Identify Cyber Risk
- Analyze Cyber Risk
- Respond to Cyber Risk
- Management Activities

The tool offers interactive features and help text; allows users to securely record results; and automatically generates a detailed, graphical report.

An organization can complete a self-evaluation using the C2M2 tools in as little as 1 day. If requested, DOE facilitates a free C2M2 self-evaluation for U.S. Energy Sector organizations.

## TSA Pipeline Security Guidelines

The Transportation Safety Administration (TSA) developed the Pipeline Security Guidelines with the assistance of industry and government members of the Pipeline Sector and Government Coordinating Councils, industry association representatives, and other interested parties to provide guidance for securing natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and to liquefied natural gas facility operators. In addition, the guidelines apply to pipeline systems that transport materials categorized as toxic inhalation hazards (TIH).

These guidelines are applicable to operational natural gas and hazardous liquid transmission pipeline systems, natural gas distribution pipeline systems, and liquefied natural gas facility operators. Additionally, they apply to operational pipeline systems that transport materials categorized as toxic inhalation hazards (TIH). TIH materials are gases or liquids that are known or presumed to be so toxic to humans as to pose a health hazard in the event of a release during transportation. (See the Hazardous Materials Regulations: 49 CFR parts 171-180.)

Operators of pipeline systems not included in the descriptions above are encouraged to implement the security measures contained in the Pipeline Security Guidelines to the extent appropriate to their particular system.

## American Petroleum Institute - API 1164

API 1164 refers to the American Petroleum Institute's (API) recommended practice for pipeline control room management. This document provides guidelines and smart practices for the management and operation of pipeline control rooms as central facilities responsible for monitoring and controlling pipeline operations.

API 1164 covers a range of topics related to control room management, including:

- **Roles and Responsibilities:** Outlines the qualifications, training, and certification requirements for control room operators and control room personnel (controllers, supervisors, and shift managers).
- **Alarm Management:** The document provides guidance on alarm systems and their management within the control room. It covers topics such as alarm design, documentation, prioritization, and response procedures to ensure effective handling of alarms.
- **Human Factors:** API 1164 addresses human factors considerations within the control room environment. It covers topics such as workload management, fatigue mitigation, shift handover procedures, and ergonomic design principles to optimize operator performance and reduce the risk of errors.

- **Procedures and Processes:** The document emphasizes the importance of having clear and well-documented procedures and processes for control room operations. It includes guidelines for developing and implementing procedures related to abnormal operating conditions, emergency response, and routine operations.
- **Training and Competency:** API 1164 provides recommendations for training programs and competency assessments for control room personnel. It outlines the knowledge, skills, and abilities required for different roles within the control room and emphasizes ongoing training and competency evaluation.
- **Management of Change:** The document addresses the management of change process within the control room environment. It highlights the need to assess and manage the impacts of changes to control room systems, procedures, and personnel to maintain safety and operational integrity.

API 1164 promotes standardized practices, enhances communication, and helps ensure the reliability and integrity of pipeline operations within the control room environment.

## APTA Standards Development Program

The American Public Transportation Association (APTA) is a nonprofit international association of more than 1,500 public and private sector member organizations. APTA is the only association in North America that represents all modes of public transportation, including bus, paratransit, light rail, commuter rail, subways, waterborne services, and intercity and high-speed passenger rail. More than 90% of the people using public transportation in the United States and Canada utilize APTA member systems. APTA is engaged in every aspect of the industry – from planning, designing, financing, constructing and operating transit systems to the research, development, manufacturing and maintenance of vehicles, equipment and transit-related products and services.

APTA, through its subsidiary in the North American Transit Services Association (NATSA), develops standards, recommended practices, and guidelines for the benefit of public rail transportation. These tasks are accomplished by working groups consisting of members from rail transit agencies, manufacturers, consultants, engineers, and other interested groups.

The collection of APTA-developed standards and practices adopted by TSA includes the following:

### APTA SS-CCS-RP-001-10: Securing Control and Communications Systems in Transit Environments

The intent of this practice is to provide guidance to transit agencies on securing control and communications systems for their environments. This Recommended Practice spearheads an effort within APTA to extend security smart practices to the transit industry by supplementing existing standards and regulations. This practice address specifics of equipment implementation, such as describing different types of firewalls or intrusion detection systems as well as mitigation measures.

This practice is divided into two parts:

- Part 1: Elements, Organization and Risk Assessment/Management
- Part 2: Security Plan Development, Execution and Maintenance

Part 1 addresses the importance of control and communications security to a transit agency, provides a survey of the various systems constitute typical transit control and communications systems, identifies the steps an agency would follow to set up a successful program, and establishes the stages in conducting risk assessment and managing risk.

Part 2 assumes the agency has completed the risk assessment and risk management steps of Part 1 and covers how to create the security plan with security controls/countermeasures, how to implement the security plan, and how to maintain the security plan. The final section covers continuity of operations/disaster recovery.

### APTA RT-ST-GL-001-13: Modern Streetcar Vehicle Guideline

This document provides guidelines to support specification and procurement of modern streetcar vehicles by identifying and describing important technical and operating principles relating to their application. Modern light rail and streetcar vehicles are fundamentally very similar, the differences having largely to do with how they are applied. The primary difference between the two modes is the degree of integration into the urban environment and the scale of the associated infrastructure. This difference in application makes some common light rail vehicle design features unnecessary for streetcar application but may also require the use of other features that may or may not be incorporated into a typical light rail vehicle.

The guideline includes an introduction and four chapters:

- Vehicle Configuration
- Vehicle/Platform Interface
- Vehicle/Track Interface
- Power Supply

Recognizing streetcar systems vary considerably in form and function, the document identifies and explains the underlying principles and interdependencies associated with each topic, and examines the trade-offs involved in various design approaches. Throughout, emphasis is placed on the need to treat vehicles, infrastructure, and operations as an integrated system.

## TSA Surface Transportation Cybersecurity Toolkit

The Surface Transportation Cybersecurity Resource toolkit is a collection of documents designed to provide cyber risk management information to surface transportation operators who have fewer than 1,000 employees. The materials are drawn from three primary sources:

- **National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity:** A voluntary framework for reducing cyber risks in CI. Read about the framework.
- **Stop. Think. Connect:** A national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Learn more about this campaign or email your inquiry.
- **United States Computer Emergency Readiness Team:** Responsible for improving the Nation's cybersecurity posture, coordinating cyber information sharing and managing cyber risks. Learn more and get the latest news about US-CERT.

Contact US-CERT to report a cyber incident, email the details or call (888) 282-0870.Security Directives and Information Circulars

The TSA issues Security Directives, Information Circulars, and Emergency Amendments in response to the ongoing cybersecurity threat to transportation systems and associated infrastructure.

For additional resources, see Appendix A.

# 5. ARTIFICIAL INTELLIGENCE

## Background and Overview

AI is rapidly transforming the landscape of cybersecurity, particularly in the defense of critical infrastructure systems like ICS. These systems, which are fundamental to the operation of industries such as energy, water, transportation, and manufacturing, face increasingly sophisticated cyber threats. AI introduces a new era of

defense by leveraging its capabilities for real-time data analysis, anomaly detection, and predictive modeling. By automating responses, identifying vulnerabilities in advance, and adapting to evolving threats, AI provides a robust and dynamic layer of security. However, its implementation also presents challenges, such as the risk of adversarial exploitation. As critical infrastructure becomes more interconnected, the integration of AI into cybersecurity strategies represents both an opportunity and a responsibility to fortify these essential systems against ever-advancing cyberattacks.

AI is the new “cyber-frontier”. Being a new cyber-frontier, many are still learning how to deploy AI in a secure manner. The key is to not implement AI and learn through costly mistakes, on what to do and what not to do when it comes to implementing AI in secure manner. A well thought out implementation could prevent future cyber risks. AI is a costly investment, that could become an even more costly liability if not done correctly.

Understanding the business context and the resources that support AI functions and the related business risks enable an organization to understand, focus and prioritize its efforts consistent with its risk management strategy and business needs. Identifying the AI environment establishes a baseline understanding of the environment, the stakeholders and potential impacts to the business.

AI owners should identify and prioritize their AI environments; this should consist of a detailed evaluation to include:

- Process platform
- Current posture of network and operations
- Impact to current operating software, and personnel
- Analyze interconnections and dependencies based on their business impact

The approach identified in this Overview Cybersecurity OT Smart Practice Guide, focuses heavily on the attack surface and resilience, compared to the NIST AI RMF 1.0, that focuses on the risks. There are clear overlaps between the two, and references to the NIST AI RMF will be made. At a high-level the below approach should overlap with the NIST’s “AI RMF 1.0, 5. AI Core.”:

- Govern - A culture of risk management is cultivated and present
- Map - Context is recognized and risks related to context are identified
- Measure - Identified risks are assessed, analyzed, or tracked
- Manage - Risks are prioritized and acted upon based upon projected and expected impact

To effectively defend an AI system, additional steps are needed to define, understand, and manage the attack surface area. To define the attack surface area, it requires looking at the systems directions, both the internal and external. The internal system requires the installer to look at the host AI system, define all the software, network requirements of the host system. When looking external to the AI system, identify all external systems, networks, etc. that are and could be touched by the AI system.

The AI seven-layer architecture is a conceptual framework comprised of distinct functional layers. The layers are comprised of elements from the physical hardware to the user interface. Understanding how the components work together and their specific technologies (like MLOps, RAG, etc.), provide an insight to potential attack surfaces and an understanding of where defenses may be required.

| Artificial Intelligence Model Architecture - Seven Layer | |
|---|---|
| Physical Layer<br>(Hardware Infrastructure) | Foundation, the beginning. Storage handling, high-speed computing, and distributed AI processing.<br>Includes:<br>• GPUs (NVIDIA, AMD)<br>• TPUs (Google)<br>• Edge devices<br>• Quantum computing systems |
| Data Link Layer<br>(Model Serving & API Integration) | Acting like a bridge for AI models.<br>• Model Context Protocol (MCP)<br>o Access your Google Calendar and Notion (AI assistant).<br>o Generate Web Apps (Claude Code).<br>o Connect to multiple databases or API across an enterprise.<br>o Generate 3D designs and print through 3D printer.<br>• APIs & pipelines<br>• Model orchestration (LangChain, MLflow, etc.)<br>• Agentic AI, connection to other agentic AI models. |
| Computation Layer<br>(Processing & Logical Execution) | Inference engines, real-time model execution, machine learning setups, GPU/TPU real-time processing, etc. |
| Knowledge Layer<br>(Retrieval & Reasoning Engine) | Retrieval and reasoning of stored data, enabling capabilities like Retrieval Augmented Generation (RAG) and semantic search, and contextual reasoning. |
| Learning Layer<br>(Model Training & Optimization) | Train deep learning models.<br>Fine-tune and reinforce learn to optimize the model. |
| Representation Layer<br>(Data Processing & Feature Engineering) | Transforms raw data into meaningful inputs, including feature extraction, tokenization, and creating embeddings for use by models. |
| Application Layer<br>(AI Interface & Deployment) | The top layer where end-users interact with AI through specific applications<br>• AI-powered applications (chatbots, copilots, recommendation systems)<br>• Data and information validation intercept to prevent prompt injection attacks.<br>• Deployment & monitoring of AI services<br>• Cloud + Edge AI integration |

## AI Characteristics

AI characteristics and purpose. Evaluating the characteristics and purpose can influence other factors, such as separation, segmentation, etc. A very important factor that it can influence is choosing the appropriate model(s) to ensure that they are trustworthy and not compromised.

What function(s) will the AI serve? (Augment or replace human activity?). The functions to be served should take into consideration several factors.

- Does the function introduce efficiencies to existing tasks, i.e. reduce the augmented tasks as a value-added function?
- Does the function being provided replace the need for human interaction or reduce the number of humans to perform a specific task?
- What controls are in place to monitor the AI functions, to ensure that the functions are reliable and accurate? (i.e. periodic audits, maintenance schedules, personnel monitoring daily, etc.)

- If the AI were to go down, how quickly can it be brought back up? Can humans perform the same function to keep processes working until it is brought back up?

## AI Trustworthiness

Before understanding the data that is being processed, the AI model being deployed must be trustworthy. In order to be considered trustworthy, it is suggested that referring to the NIST's "AI RMF 1.0, 3. AI Risks and Trustworthiness." Under the previously mentioned section of the NIST AI RMF 1.0, the criteria provided include:

- Safe
- Secure & Resilient
- Explainable & Interpretable
- Privacy-Enhanced
- Fair- With Harmful bias Managed
- Valid and Reliable

AI Covariate/Data Drift. When evaluating an AI model, AI data accuracy is a very important factor to consider. All AI data that is used in models, is considered point in time data. It is dependent upon all the data gathered up until the AI model was created. Deviations from that point, or changes of data from that point on will create an change in the output of an AI model, as the statistical information has changed. This change in data/statistical properties over time is considered covariate or data shift.

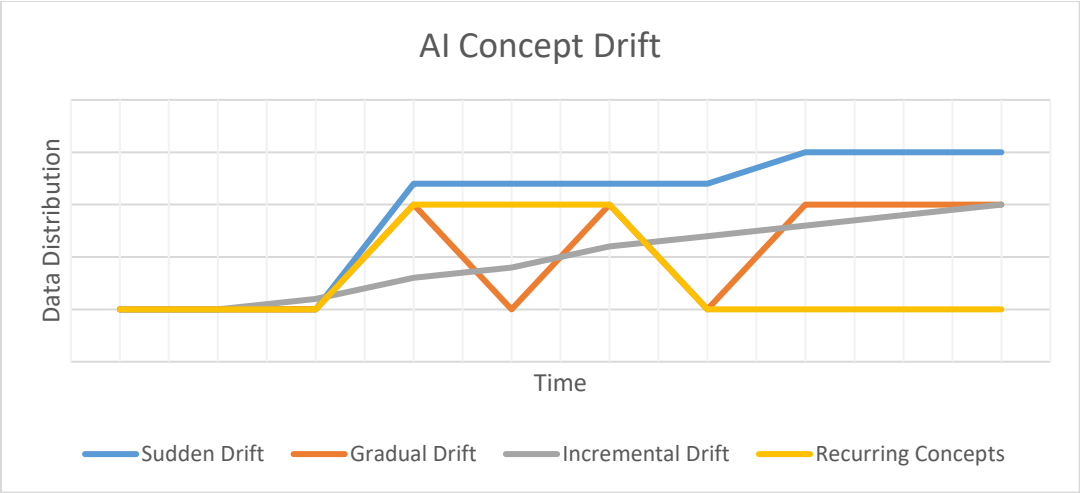
Data drift can occur due to various reasons:

- Dynamic data. Real-world data is dynamic and therefore subject to constant change. Examples are world events, cyber threats, new technologies, etc.
- Disparate data sources. New data or changing data sources and methods change the data attributes.
- Environmental changes. Changes within the environment(s) the systems or processes generating the data will impact to the data.

Concept Drift. When the data used no longer aligns to the design of a particular model, the result is a concept drift. For example, is a machine learning (ML) model is designed to identify one type of network traffic and the traffic it was designed for changes attributes or patterns, the model may no longer be able to detect what it was designed to detect.

Concept Drift can be further broken out into sub-categories.

- Sudden Drift. Changes occur in a short time period.
- Gradual Drift. Changes occur gradually over time.
- Incremental Drift. Changes occur incrementally over a period of time.
- Recurring Concepts. Changes occur for a period but, revert back to their previous state.



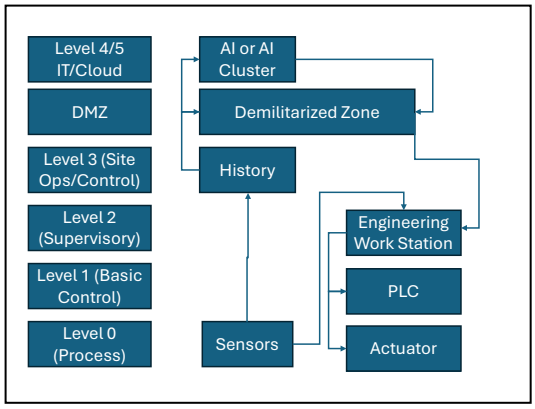

As the data drift occurs, the accuracy of the AI model too will change. The accuracy in the AI model, can have a direct impact on cost or safety. When deploying an AI model, dependent upon the models deployed, the model will require some form of monitoring to determine when and if Data or Concept drift occurs. Some subscription-based AI models such as ML based network AI tools from Cisco, account for data accuracy and can account for drift, for a premium.

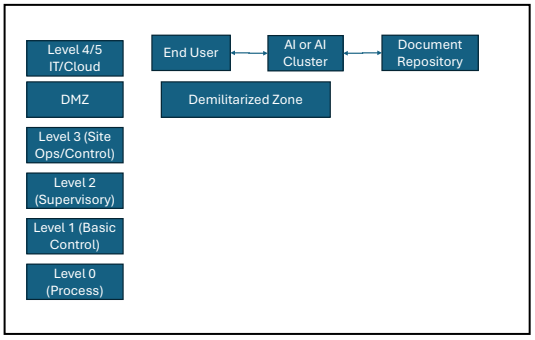
## Data and information

There are factors to consider when evaluating an AI system. It is important to know characteristics of the flow of the data, and the disposition of the data before, during and after being processed.

| Considerations | |
|---|---|
| How does the information flow through the system, and through what mechanisms? | • Understanding the flow of data, should identify the origination, the destination and everywhere in between the two, to include the AI.<br>• If the data crosses the IT and OT boundaries, ensure that it traverses the Demilitarized Zone (DMZ). If necessary, that the traffic is encrypted.<br>• A Dataflow diagram (DFD) could help identify not only the data flow but other potential attack surface areas, and necessary segmentations are employed.<br>• A data flow can add contextual knowledge to the data and can be used to validate potential outcomes of the data that flows through the AI system. |
| What are the protection levels for confidentiality, integrity, and availability? | • When looking at the CIA Triad, what controls should be put in place to protect the data?<br>• Do the protections change when processed?<br>• Are the proper policies and controls in place to protect the data? |

| | |
|---|---|
| Does the confidentiality, change once AI has completed its' processing of the information? | • Does the confidentiality change when processed through the AI model?<br>• Is the output more confidential than the input? (example: If searching a repository or historian using a general text, is it possible the information returned is sensitive and requires additional protections?) |
| Does the information processed by the AI have the potential to impact or cause harm of assets or human life? | • Is there the potential for sensors or other equipment passing information to the AI, impact other OT equipment that if processed incorrectly has the potential to cause harm to human life or equipment?<br>• If the data returned is sensitive, could it if improperly processed could impact human life? |




## Threat and Risk

After determining the characteristics of the AI and understanding the data disposition(s), and flow, we should have a better understanding of the potential threat/risks and ultimately the criticality. At this point we should understand the data flow, interactions with other systems, etc. We should have an understanding of the AI trustworthiness. After assessing potential threats and risks the reader should be able to better gauge the resources needed (e.g., staffing, funding) to achieve AI risk management goals in a cost- effective, prioritized manner.

- What methods are currently available for user access?
  - What access controls are in place?
- What internal dependencies are present for system functionality? (i.e. software, libraries, hardware, etc.)
  - Consider maintaining a list of the minimum software required to maintain functionality, with a focus on minimizing risks.
  - Consider have a test environment for pre-deployment tests, when doing updates to software.
  - Consider single 'use' servers. (i.e. limiting the attack surface area by only deploying AI servers, as only AI servers. No sharing of resources with other server types, including and especially if deploying in an AI cluster mode. Each node in the cluster should be deployed with identical configurations.)
- Are containers used?
  - What controls are put in place to ensure only approved containers are deployed?

    - Are there preventative measures in place to prevent using the daemon access to escalation of permission?
- Is Python used? Most AI deployments rely upon Python as a programming language to quickly train and control AI information. Unlike many other types of programming languages, Python is not compiled and does not rely upon binary and executable files. Python is an interpreted language, which means it the code that is executed is stored in ASCII format which is read and interpreted. This makes Python susceptible to various types of attacks that can performed without being identified, such as code injection.
    - Consider deploying a Security Information and Event Management (SIEM), for potential system level changes.
    - Consider deploying a File Integrity Monitoring (FIM) tool. Whereas SIEM's are effective tools for identifying potential Common Vulnerabilities and Exposures (CVE) and system level executions and changes, a FIM can track changes in the content, permissions, and other attributes of critical system and application files, including Python files.
    - FIMs often use hashing algorithms to create a baseline of trusted file states and compare current file states against that baseline to detect any unauthorized modifications, making code injects and file changes more identifiable.
- What data validation methods are used?
    - Current attacks allow for sensitive data to be leaked out / exfiltrated through AI implementations. In many cases models are analyzed based upon question response combinations, to fool the AI model into providing sensitive data.
    - AI models, especially LLMs, are vulnerable to hidden commands and data encoded in Unicode characters, including emojis, which can manipulate AI behavior. Emoji hijacking can unintentionally allow attackers to embed hidden data within emojis or other characters, creating security risks allowing the AI model to execute hidden commands. Consider:
        - Leveraging 'Classifiers', and 'Guardrails', to validate all data for all data prior to being accepted into the AI and prior to leaving the AI enclave.
        - When choosing an interface, chose one that allows for custom classifiers and guardrails that can enforce strict validation rules.
        - Consider enforcing allowing only ASCII text preventing hidden Unicode commands.
        - Consider implementing generative AI as a non-person entity (NPE) user and granting least privilege for all application program interfaces (APIs), and sensitive files.
    - Hallucinations. AI does not know what it does not know. A recurring issue, that can be a risk to an AI model implementation is referred to as a hallucination. To reduce the likelihood of an AI hallucination, consider:
        - Leveraging strict AI focused training when training a model.
        - Have each AI Model implementation narrowly focused to one specific area of expertise.
        - Leveraging 'Classifiers', and 'Guardrails', to validate all data for all data prior to being accepted into the AI and prior to leaving the AI enclave.
        - Ensure natural language is accepted as input and validated as outdput.

    - Recommend deploying each AI instance with firewalls, with controlled access to and from each AI server. Consider Deny by Default

## Resilience

- AI enhances the cyber resilience of ICS by strengthening defense-in-depth strategies through proactive and adaptive measures. AI enables real-time threat detection, predictive analytics, and automated incident responses to mitigate risks effectively. It facilitates dynamic network segmentation to isolate critical components and employs generative models to simulate cyberattacks for testing and training purposes. Additionally, AI continuously learns and evolves, ensuring adaptive security measures to counter emerging threats. By integrating AI into ICS cybersecurity, organizations can safeguard critical infrastructure and bolster resilience against evolving cyber challenges.

- When considering resilience, many factors must be considered.
    - What is the likelihood for the risk?
    - What are the potential costs associate with the risks?  (loss or harm to human or assets?)
    - What can be done to reduce the likelihood of the risks?
    - What is the impact to business in case of an event, cyber or physical?
    - What is an acceptable level of risks?
    - Backup and recovery procedures.
    - What is the value of the asset(s)?
        - Cost to replace?
        - Redundancy/Failover?
        - Recovery time and recovery point objectives?
    - What is the schedule to test, evaluation, verify and validate (TEVV) the AI?

# CONCLUSION

As ICS grow in complexity and connect to business and external networks, the number of potential security issues and their associated risks grows as well. Organizations cannot depend on a single countermeasure to mitigate all security issues. To effectively protect ICS from cyber-based attacks, organizations must apply multiple countermeasures at varying levels of depth—thus reducing risk using an aggregate of security mitigation techniques. Additionally, AI provides organizations with the ability to increase the good and services they provide and enhance security. However, AI also increases an organization to evolving threats who leverage AI to target vulnerabilities. When organizations plan strategies of Defense-in-depth they must account for AI to be as resilient as possible.

One should note defense-in-depth measures do not and cannot protect all vulnerabilities and weaknesses in an ICS environment. Defense-in-depth tactics are applied, primarily, to slow down attackers enough to allow IT and OT personnel to detect and respond to ongoing, persistent threats—or, alternatively, to make the effort on the attacker's side so cumbersome the reward simply is not worth the risk or effort.

Organizations that implement defense-in-depth strategies can significantly increase their cybersecurity resilience and reduce risk.

# APPENDIX A

TSA provides the following list of cybersecurity resources to the public at no cost.

American Public Transportation Association Cybersecurity Considerations for Public Transit:
This recommended practice establishes considerations for public transit chief information officers interested in developing cybersecurity strategies for their organizations. It details practices and standards that address vulnerability assessment and mitigation, system resiliency and redundancy, and disaster recovery.

American Public Transportation Association Securing Control and Communications Systems in Transit Environments:

- Part 1: Elements, Organization and Risk Assessment/Management: Addresses the importance of control and communications security to a transit agency, provides a survey of the various systems that constitute typical transit control and communication systems, identifies the steps an agency would follow to set up a successful program, and establishes the stages in conducting a risk assessment and managing risk. Read Part 1 of the recommended practice document.
- Part 2: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones: Presents Defense-in-Depth as a recommended approach for securing rail communications and control systems, defines security zone classifications, and defines a minimum set of security controls for the most critical zones.
- Part 3: Attack Modeling Security Analysis White Paper: Covers the attack modeling procedure for transit agencies and their systems integrators and vendors.

Critical Infrastructure Cyber Community Voluntary Program Kit: The Critical Infrastructure Cyber Community Voluntary Program, or C³ (pronounced "C Cubed") Voluntary Program, is an innovative public-private partnership, to help connect companies, as well as Federal, State, local, tribal, and territorial partners, to DHS and other Federal government programs and resources that will assist their efforts in managing their cyber risks.

Cyber 5N5: 5N5 is short for “five non-technical actions to consider in five days”. This cybersecurity workshop series is specifically designed for transportation Owners and Operators to learn about Department of Homeland Security resources and programs available to them, as well as non-technical policy or procedural actions that can be implemented to enhance their company or agency’s cybersecurity posture.

Cyber Hygiene Services: Describes several Cybersecurity and Infrastructure Security Agency (CISA) scanning and testing services to help organizations reduce their exposure to threats by taking a proactive approach to mitigating attack vectors.

Cyber Resilience Review Program: The Cybersecurity Evaluation program conducts a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities within CI and key resources sectors, as well as state, local, tribal, and territorial governments through its Cyber Resilience Review process.

Cyber Risk Management Primer for CEOs: Provides key cyber risk management concepts business leaders should consider to protect their organization’s systems from cyber threats.

Cybersecurity and Physical Security Convergence Guide: Describes the complex threat environment created by increasingly interconnected cyber-physical systems, and the impacts this interconnectivity has on an organization’s cybersecurity and physical security functions.

Cybersecurity Smart Practices for Industrial Control Systems: Provides recommended cybersecurity Smart Practices for ICS.

Cybersecurity Framework (CSF)**: I**ntends to provide direction and guidance to those organizations – in any sector or community – seeking to improve cybersecurity risk management via utilization of the NIST Cybersecurity Framework.

Industrial Control Systems Cybersecurity for the C-Level**:** Provides a tool to help facilitate the communication of strong, basic cybersecurity principles to organizational leadership.

Insider Threat Mitigation: Provides information and resources from CISA to will help individuals, organizations, and communities create or improve an existing insider threat mitigation program.

Law Enforcement Cybersecurity Resources**:** A list of DHS recommended support materials for the law enforcement community.

National Cyber Awareness System: Provides access to products in the National Cyber Awareness System that offer a variety of information for users with varied technical expertise.

Pipeline Security Guidelines: Provides security measures for cyber assets and a list of cybersecurity planning and implementation guidance resources.

Public Transportation Information Sharing and Analysis Center: The center collects, analyzes, and disseminates alerts and incident reports, as well as sector-specific intelligence products, and helps the government understand sector impacts.

Ransomware Guide: Provides resources a customer centered, one-stop resource with smart practices and ways to prevent, protect and/or respond to a ransomware attack.

SCRM Essentials: Provides information and strategies to assist with ensuring supply chain risk management (SCRM) is an integrated component of security and resilience planning for the Nation's infrastructure.

Shields UP: Provides up-to-date information and recommendations to help organizations prepare for, respond to, and mitigate the impact of cyberattacks.

Transportation Systems Sector Cybersecurity Framework Implementation Guidance: Provides guidance, resource direction, and a directory of options to assist a Transportation Systems Sector organization in adopting the NIST framework.