APTA STANDARDS PROGRAM

WHITE PAPER

APTA SS-TCS-WP-002-26

First Published: June 10, 2026

Transit Cybersecurity Working Group

Visibility of Digital Networks, Systems and Assets in Rail Transit Environments

Abstract: In modern rail transit systems, visibility is the foundation of both operational efficiency and cybersecurity resilience. This white paper explores the critical importance of visibility across assets, networks and systems in rail environments. It clarifies the scope of visibility focusing on comprehensive asset awareness, data flow transparency and interconnection mapping. This is presented while distinguishing visibility from detection, segmentation and other security practices. Through this focused lens, the paper presents best practices, standards alignment and practical guidance for rail operators striving to meet regulatory expectations and bolster system reliability. By addressing the visibility gaps inherent in complex operational technology and IT environments, this white paper empowers transit agencies to build a secure, adaptable and resilient foundation for their evolving digital ecosystems.

Keywords: cyber, cybersecurity assessments, cyber assets, disaster recovery, hazard analysis, operational technology (OT), preparedness, redundancy, resiliency, safety, visibility

Summary: This white paper examines the foundational role of visibility in securing modern rail transit systems. It focuses on the comprehensive identification and documentation of assets, networks and systems, which forms the bedrock of effective risk management and cybersecurity in increasingly digitalized transit environments. This document is a proactive effort to ensure that rail agencies can fully understand their operational landscapes and make informed decisions to protect them. It explores the importance of maintaining accurate and dynamic asset inventories, understanding data flows across the transit environment, and ensuring secure interfaces between IT and OT networks. By aligning these practices with the NIST Cybersecurity Framework and APTA's OT-Cybersecurity Maturity Framework (OT-CMF), it provides practical guidance for integrating visibility into the day-to-day operations of transit agencies. This paper also highlights the importance of implementing robust governance structures and continuous improvement practices. Recommendations are offered for building or refining visibility initiatives, including best practices for leveraging standards, engaging vendors and conducting periodic reviews to stay ahead of emerging threats. Visibility is not just a security function but an operational imperative. By prioritizing visibility, rail transit agencies can create the foundation for a more resilient, adaptable and secure future.

Foreword

The American Public Transportation Association is a standards development organization in North America. The process of developing standards is managed by the APTA Standards Program's Standards Development Oversight Council (SDOC). These activities are carried out through several standards policy and planning committees that have been established to address specific transportation modes, safety and security requirements, interoperability, and other topics.

APTA used a consensus-based process to develop this document and its continued maintenance, which is detailed in the manual for the APTA Standards Program. This document was drafted in accordance with the approval criteria and editorial policy as described. Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

This document was prepared by the Transit Cybersecurity Working Group as directed by the Security and Emergency Management Standards Policy and Planning Committee.

This document represents a common viewpoint of those parties concerned with its provisions, namely transit operating/planning agencies, manufacturers, consultants, engineers and general interest groups. The application of any recommended practices or guidelines contained herein is voluntary. APTA standards are mandatory to the extent incorporated by an applicable statute or regulation. In some cases, federal and/or state regulations govern portions of a transit agency's operations. In cases where there is a conflict or contradiction between an applicable law or regulation and this document, consult with a legal adviser to determine which document takes precedence.

This is a new document.

© 2026 The American Public Transportation Association. No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without prior written permission of APTA.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the **Transit Cybersecurity Working Group**, which provided the primary effort in the drafting of this document.

At the time this standard was completed, the working group included the following members:

Julius Smith, *Dallas Areas Rapid Transit*, Chair
Timothy Coogan, *Regional Transportation District*, Vice Chair
John Moore, *Phoenix Contact*, Secretary

Paul Braunschweig, *TSA*
Anthony Candarini, *Google Mandiant*
Mark Curry, *Secheron*
Terry Follmer, *CAP Metro*
Jessie Gill, *BC Rapid Transit*
Kevin Harnett, *IO Active*
Ahmed Idrees, *Sound Transit*
Mark Johnston, *TriMet*
Shaked Kafzan, *Cervello*
Tri Le, *Armand*
Yoav Levy, *Cervello*
Hillman Mitchell, *CICSCI*
John Stubbs, *TSA*
Abayomi Muse, *Transit Safety Solutions*
Jack Oden, *Parsons*
John Sheehy, *IO Active*
Miki Shifman, *Cylus*
Gutta Vamsikrishna, *Alstom*
Jessica Weiland, *IO Active*

Project team

Polly Hanson, *American Public Transportation Association*
Brian Heanue, *American Public Transportation Association*
Michael Echols, *Max Cybersecurity*

Introduction

This introduction is not part of APTA SS-TCS-WP-002-26, "Visibility of Digital Networks, Systems and Assets in Rail Transit Environments."

APTA recommends the use of this document by:

- individuals or organizations that operate rail transit systems;
- individuals or organizations that contract with others for the operation of rail transit systems; and
- individuals or organizations that influence how rail transit systems are operated (including but not limited to consultants, designers and contractors).

Scope and purpose

This document is provided for informational purposes only. It is not intended to replace or retrofit existing safety and security practices as defined by regulators or other associated industry best practices. This white paper is intended to educate and inform rail transit agencies about the importance of considering cybersecurity risks as a factor when implementing, managing and monitoring the safety and security of transportation systems and changes to system elements. It intends to encourage collaboration and information-sharing among the personnel responsible for managing system safety requirements and those responsible for securing networks, systems and devices against intrusions to maintain safety, reliability and availability of the operational infrastructure. Further, it is intended to guide users to other resources that may be beneficial for

systems safety practitioners to be familiar with when carrying out their responsibilities in our increasingly connected world.

Visibility of Digital Networks, Systems and Assets in Rail Transit Environments

1. Overview

In the evolving landscape of rail transit, visibility is the first and most essential step toward securing assets, networks and systems. Visibility means knowing what is connected, how it operates and what dependencies exist. It's about having a clear, dynamic understanding of the full operational and digital environment. This ranges from control systems and field devices to the cloud-enabled services that integrate with them.

Visibility is not just a technical requirement but a strategic safeguard. Without it, transit agencies face significant risks, including the following:

- Blind spots in asset inventories can leave critical infrastructure exposed to attacks or misconfigurations.
- Unmapped data flows may allow malicious actors to exploit gaps in network segmentation.
- Unmonitored interfaces between IT and OT environments can lead to cascading failures, especially in interconnected systems.

These vulnerabilities can jeopardize not only security but also safety, reliability and public confidence. On the other hand, a well-structured visibility program offers significant opportunities for operators to proactively identify weaknesses and prioritize investments that align with both mission and security goals. Visibility of assets, systems and networks supports compliance with federal and industry standards, reducing regulatory risk. And visibility enhances operational reliability and strengthens the foundation for future innovations, such as AI-enabled predictive maintenance.

However, building a visibility program also involves trade-offs. A robust program requires time, investment and cross-functional collaboration. It can reveal previously unknown dependencies and vulnerabilities that demand remediation. Most transit agencies have limited resources, and some may find that developing a program feels daunting. But the benefits of a visibility-first approach far outweigh the challenges.

This white paper provides a "you have to think about this" approach for rail transit leaders. It argues that visibility is not an optional add-on but a cornerstone of resilient and secure rail operations. By treating visibility as a programmatic effort rather than a one-time project, agencies can position themselves to respond to emerging threats, comply with evolving standards, and ensure safety and reliability in an increasingly complex transit environment.

1.1 Visibility and transportation cybersecurity regulation

Public transit systems are an essential part of the nation's critical infrastructure, supporting the economy, public safety and the daily lives of millions of Americans. Like other critical infrastructure sectors, transit, a subsector of the transportation sector, increasingly relies on interconnected systems and digital technologies. This reliance has heightened the need for robust cybersecurity, including comprehensive visibility of all assets, systems and data flows. A lack of visibility inhibits important components of cybersecurity resilience.

© 2026 American Public Transportation Association

Visibility is foundational to meeting regulatory and cybersecurity requirements. It enables agencies to understand what assets and systems exist, how they interconnect, and where vulnerabilities may arise. Federal agencies and key stakeholders have recognized this, elevating cybersecurity visibility to a national priority for critical infrastructure protection.

The White House and Cabinet-level agencies have underscored the urgency of improving cybersecurity across all sectors, with transportation systems singled out as a particular focus. As a result, federal agencies have issued guidance and directives that highlight the critical role of visibility in securing transit systems. These regulatory initiatives emphasize that transit agencies must not only respond to threats but must proactively identify and understand their environments to ensure compliance and maintain public trust.

Key regulatory requirements reinforcing the need for visibility include the following:

- **TSA Security Directives:**
  - **SD 1580-21-01** requires transit agencies to designate cybersecurity coordinators, report incidents, develop Cybersecurity Incident Response Plans and conduct vulnerability assessments. These activities rely on comprehensive visibility to ensure accurate reporting and risk mitigation.
  - **SD 1580/82-2022-01A,** effective October 24, 2023, further mandates the development of a TSA-approved Cybersecurity Implementation Plan. This plan covers access control, segmentation, continuous monitoring and patching—activities that hinge on knowing what assets exist and how they interact. Agencies must also establish a cybersecurity assessment program, which includes architectural reviews and network activity analysis, both of which depend on clear visibility of operational environments. Compliance documentation may include hardware/software inventories, firewall configurations, network diagrams and activity logs, all of which require accurate visibility to produce and maintain.
- **FTA Safety Advisory SA-22-2:**
  - This advisory recommends that transit agencies address signal system vulnerabilities, including insufficient maintenance or absent systems. Addressing these risks requires agencies to have a thorough understanding of their asset inventory, system configurations and maintenance practices.
- **TSA Advance Notice of Proposed Rulemaking (November 2022)**
  - The TSA has signaled its intent to codify cybersecurity requirements. Agencies that build visibility practices into their operations now will be better prepared for the evolving regulatory landscape.

While some of these directives currently apply to a limited number of agencies, APTA anticipates that they will expand in scope and be codified into regulations that impact funding decisions and operational compliance. Agencies that embrace visibility as a core element of their cybersecurity programs will be better positioned to comply with these evolving requirements and protect the public they serve.

Given the dynamic threat environment, these directives and advisories may evolve over time. Safety personnel should regularly consult TSA, CISA, FRA and FTA resources for updates and best practices. APTA's Cybersecurity Resources page can also serve as a key reference point for the latest guidance.

Visibility is no longer a luxury. It is an essential capability that underpins every aspect of regulatory compliance and operational resilience. By fostering a culture of visibility, transit agencies can strengthen their cybersecurity posture, align with federal mandates and protect the vital services that keep our nation moving.

© 2026 American Public Transportation Association

NOTE: As the cybersecurity threat environment evolves, these security directives, advisories and pending regulations may change and/or be sunsetted. Safety personnel should regularly review the websites of the TSA, CISA, FRA and FTA for updates to the requirements and/or the release of new requirements. APTA's Cybersecurity Resources page may also be used to check for the latest updates of these documents, as well as other guidance that may become available.

2. Understanding visibility

Visibility is the first step in risk-informed decision-making. Without a clear, accurate picture of their OT environment, agencies can't effectively enforce security policies, detect unauthorized changes or assign accountability for operational outcomes. Gaps in visibility mean that vulnerabilities—such as unmanaged devices, undocumented interconnections or legacy systems—remain hidden and unaddressed. These blind spots can erode trust and compromise the reliability and safety of rail transit operations.

2.1 Impact on service delivery

Both IT and OT systems directly impact service delivery and passenger safety. In today's converged environments, where IT-based analytics and digital tools are increasingly integrated with OT systems, this interplay becomes even more critical. Visibility ensures that this integration enhances performance without introducing unmonitored entry points or pathways that malicious actors can exploit. Moreover, hidden risks are not just technical concerns. They can have significant implications for regulatory compliance, incident response and public confidence. Without visibility, agencies struggle to identify potential threats early, undermining their ability to respond quickly and decisively when incidents occur. By uncovering and addressing these hidden vulnerabilities, visibility empowers agencies to make informed decisions that protect their mission, ensure reliable transit service and maintain the trust of the communities they serve.

Visibility transforms cybersecurity from a passive inventory exercise into a dynamic capability. It becomes the backbone of proactive security and operational resilience to enable agencies to detect deviations from normal operations and identify issues before they become disruptions. It also helps build the redundancy and reliability needed to adapt to future challenges.

2.1.1 IT/OT connection

Rail transit systems rely heavily on OT, including the sensors, control systems and industrial processes that keep trains moving safely and efficiently. While IT visibility has been a focus for many years, OT visibility is often overlooked or assumed to be a secondary priority. This can create critical gaps in both security and operational oversight. OT visibility isn't just about security, but also about the backbone of resilience. Without a clear understanding of how assets connect and interact, agencies can't effectively adapt to changing threats or quickly recover when something goes wrong.

Visibility empowers operators to see where vulnerabilities could be exploited, to identify interdependencies that might amplify disruptions, and to build in the redundancies needed to withstand failures and return to safe operation.

By prioritizing OT visibility, transit agencies are investing in a foundation of resilience. The goal is to develop an operational system that can absorb shocks, adapt to new threats, and continue to provide safe and reliable service to passengers even in the face of evolving challenges. Visibility provides an early warning system and supports increased system uptime.

2.2 Key visibility concepts

A lack of OT visibility isn't just a security gap; it can become a critical liability that slows recovery, hinders maintenance and exposes transit systems to avoidable risks. By prioritizing OT visibility, transit agencies can

© 2026 American Public Transportation Association

achieve better safety outcomes, improved reliability and more effective incident response. In this way, visibility transforms from a reactive discovery effort into a strategic asset that strengthens the entire transit ecosystem.

2.2.1 IT visibility

IT visibility is the ability to identify and monitor endpoints (e.g., workstations, servers, mobile devices), users, applications and data flows within the IT environment. It provides a real-time understanding of how digital assets are configured, how they communicate and how data is shared across business systems.

2.2.2 OT visibility

OT visibility is the ability to identify and monitor industrial assets, control systems, sensor inputs and actuator outputs in the OT environment. OT visibility ensures a detailed understanding of how physical processes are controlled and how field-level devices are interconnected to maintain safe and efficient transit operations.

2.2.3 System visibility

System visibility is the understanding of logical dependencies and control relationships across domains, such as how IT applications interface with OT control systems and how data moves through interconnected components. System visibility helps identify single points of failure, security gaps, and areas requiring enhanced monitoring or controls.

2.2.4 Inter-domain visibility

Inter-domain visibility is the ability to understand how IT and OT environments connect and share data, particularly over key interfaces such as supervisory control and data acquisition (SCADA) networks, human–machine interfaces (HMIs), or cloud-based applications. Inter-domain visibility ensures that agencies can monitor and secure the data and control flows that cross traditional IT/OT boundaries.

2.3 Visibility drivers

Several powerful drivers underscore the need for enhanced visibility within transit OT environments. These drivers reflect the increasing complexity and importance of OT systems in ensuring safety, reliability and regulatory compliance.

The need for visibility is driven by three core factors:

- **Criticality of OT systems:** OT assets directly control physical processes, such as train signaling, track switching and passenger safety. Gaps in visibility can translate to physical safety risks and operational disruptions.
- **Convergence of IT and OT:** Digital transformation is bringing IT tools and data analytics into OT environments. This integration offers new capabilities but also blurs traditional boundaries and exposes OT assets to IT-based threats.
- **Compliance and governance:** Federal directives such as TSA SD 1580/1582 and standards like IEC 62443 explicitly call for robust visibility across IT and OT domains. Without a foundational understanding of the need for visibility, compliance becomes superficial or incomplete.

2.4 Unique challenges to OT visibility

Despite its critical importance, achieving OT visibility comes with unique challenges that differ significantly from those in IT environments. Understanding the challenges will increase productivity and assist in identifying targeted solutions.

© 2026 American Public Transportation Association

2.4.1 Legacy systems and protocols

Rail systems were not built for today's threat landscape. Many of the OT devices and control systems were designed for reliability and performance, not for cybersecurity. They're running on legacy technology that's older than some of the people managing them, and they're communicating in languages—like Modbus, DNP3 and a multitude of rail-specific proprietary protocols—that were never meant to interface with modern security tools.

These legacy systems weren't built to handle active scans or advanced discovery tools. If pushed too hard, they could cause outages with the potential of permanently incapacitating a system, leading to downtime or serious costs. To avoid disrupting operations, agencies must be cautious, strategically using passive monitoring and external gateways to gather insights. Modernizing systems is a challenge, but visibility is the first step. It's about understanding what's there, even if it's built on foundations that predate today's cybersecurity reality.

2.4.2 Safety and availability constraints

In rail transit, safety isn't just a box to check but is the primary mission. Every decision has to protect people first. That's why visibility in OT environments isn't as simple as it is in IT. IT practitioners can scan systems, push updates overnight and hope for the best. But in OT, a careless scan can stop a train or disrupt passenger safety in real time.

Finding a balance between visibility and safety is critical. All activities should support safety and reliability for every rider, every time. Agencies must build trust and ensure that every step toward visibility supports the mission. Achieving visibility goals can never include letting safety take a back seat. That might mean using cautious, passive approaches like network taps and mirrored traffic. And it means working together with operations teams to test and validate before deploying anything new.

2.4.3 Complex and heterogeneous environments

No two rail systems look exactly alike. A signal house or traction power substation may have a hodgepodge of systems. The mix of equipment might include relays and hardwired circuits, old controllers from the '90s, new IoT sensors added last year, and proprietary gear that nobody wants to touch because it's too risky.

This mix makes visibility difficult, and one-size-fits-all tools won't be sufficient. Agencies must respect the diversity of the environment, tailoring their approach to the unique mix of protocols, vendors and operational quirks they're dealing with. The visibility approach will never be a magic bullet; the resulting architecture will emerge as a layered solution. This is a combination of passive monitoring, targeted active discovery where it's safe and a governance approach that makes sense of it all. That's how to get meaningful visibility in a system that's anything but uniform.

2.4.4 Organizational silos

Visibility isn't just about technology but about the people who comprise the stakeholder group. This effort is about building a culture that sees visibility as a shared mission. For too long, OT and IT have lived in separate worlds, where OT teams worry about keeping the trains moving and IT teams worry about data and enterprise security. Similarly, when we look at what constitutes an OT team, it's often limited to just networking and communications personnel, excluding subject matter experts from safety, engineering, operations and maintenance teams who are critical to understanding equipment and design nuances—and who can also greatly benefit from visibility improvements beyond security. Too often, those worlds don't meet until something goes wrong.

© 2026 American Public Transportation Association

If agencies are going to get serious about visibility, they must tear down those silos. That means building trust, not just policies. It means getting the operations people to see security as part of their job and getting IT to understand that OT isn't just another set of endpoints. When agencies achieve this, they will not just be protecting the system; they will be making it stronger, safer, and more reliable for everyone.

2.4.5 Evolving threat landscape

Modern threats such as ransomware and supply chain attacks specifically target OT environments, exploiting gaps in segmentation or asset management. A 2024 SANS ICS survey found that more than 60% of industrial organizations reported attempted or successful ransomware incidents targeting their OT networks in the past year alone. Even more concerning, these attacks are not random. CISA reports that supply chain vulnerabilities accounted for more than 40% of significant OT incidents in 2023.

These threats demand not just basic asset inventories, but deep, contextual visibility that can track relationships and data flows across the IT/OT boundary. Attackers exploit weak points like unmanaged connections, outdated firmware, and insecure vendor access to establish footholds that can bypass traditional perimeter defenses. Without an integrated, real-time understanding of how assets interact, what's connected to what, how data flows and where control decisions are made, agencies are effectively flying blind in a dangerous environment.

2.5 Understanding the dynamic environment

These challenges highlight why traditional IT asset management practices often fall short in OT environments. IT tools typically assume uniform systems, frequent patch cycles and easy segmentation. These assumptions don't hold in the safety-critical, real-time world of OT. In the rail sector, where even a momentary disruption can threaten lives and critical services, the stakes are even higher. To address these challenges, agencies need a visibility strategy that respects OT's unique operational and safety requirements while also building the foundation for a secure and resilient transit system. This means going beyond simple device counts and network maps by embracing passive monitoring, cross-functional governance and data-driven decision-making.

A dynamic view empowers agencies to move beyond static inventories and embrace real-time awareness. This enables them to do the following:

- Adapt to emerging threats by quickly identifying suspicious activities or abnormal behaviors in critical systems.
- Recover rapidly from incidents through a deep understanding of how systems interconnect and where the most critical impacts lie.
- Protect their mission of safe, reliable and resilient transit operations by ensuring that every action taken to secure the system is informed by accurate, up-to-date visibility.

2.6 Developing organizational resilience

Visibility in OT isn't just about what can be seen. It's about creating a living map of a system's behavior, vulnerabilities and strengths, empowering agencies to adapt to threats, recover quickly, and protect their mission of safe, reliable service. By transforming visibility from a checklist item into a living, breathing capability, agencies not only meet compliance mandates but also create the conditions for true operational resilience in an increasingly complex cyber environment.

3. Key visibility tools and processes

Achieving effective visibility in transit OT environments requires a combination of robust tools, proven processes and best practices. These elements work together to create a comprehensive, real-time view of

© 2026 American Public Transportation Association

assets, data flows and system behaviors. If done in alignment with best practices, it enables transit agencies to manage risk, comply with evolving regulations, and maintain safe and reliable operations.

3.1 Tools and techniques

A range of tools and techniques support effective visibility across both IT and OT environments:

- **For IT systems:**
  - Network scanners and endpoint agents identify devices, configurations and software versions across the network.
  - Vulnerability scanners highlight potential weaknesses in IT assets, ensuring that patching and configuration management efforts stay on track.
  - Cloud discovery tools help identify resources in hybrid environments, where critical applications may extend into third-party data centers or cloud platforms.
- **For OT systems:**
  - Passive network monitoring tools, such as deep packet inspection (DPI) tools, capture network traffic and identify connected assets without disrupting critical processes.
  - Protocol-aware asset discovery tools scan for specialized OT protocols (e.g., Modbus, DNP3, IEC 61850) and can provide real-time asset inventories.
  - Engineering diagrams like as-built schematics should be cross-referenced with digital monitoring systems to ensure that the digital state matches the physical environment.
- **Cross-domain integration:**
  - Configuration management databases (CMBDs) and enterprise asset management systems unify IT and OT asset data in a single source of truth.
  - Secure remote access gateways, with integrated monitoring and audit trails, support safe access to OT systems for maintenance and troubleshooting while maintaining complete oversight.
  - Unified data lakes or dashboards bring together these various data sources to provide a comprehensive view for decision-makers.

By leveraging these tools, agencies can ensure that visibility extends across the full spectrum of transit operations. This helps to bridge IT, OT and third-party systems in a way that is secure and transparent. Acquiring these tools is not difficult. There are a host of tools developed and sold by the private sector and some developed and provided for free by the U.S. government. These are some free tools to assist organizations with understanding their environment:

- **Cybersecurity Evaluation Tool:** CSET is a comprehensive self-assessment tool developed by CISA. It assists organizations in evaluating their cybersecurity posture across both IT and OT environments. The tool provides a systematic approach to assess security practices, identify vulnerabilities and prioritize mitigation efforts. Notably, the FHWA has adopted CSET to aid transportation authorities in enhancing infrastructure protection.
- **Cyber Hygiene services:** CISA also offers free Cyber Hygiene services designed to help organizations proactively identify and mitigate vulnerabilities in their internet-facing systems. These services include vulnerability scanning and assessments that can uncover hidden risks, such as unmanaged devices or unknown interconnections, that are crucial for maintaining trust and resilience in transit operations.
- **Cybersecurity Assessment Tool for Transit:** The FTA provides a Cybersecurity Assessment Tool tailored specifically for public transit agencies. This tool aids in developing and strengthening cybersecurity programs by helping agencies identify and mitigate risks within their systems. It serves as a foundational resource for aligning with best practices and ensuring compliance with evolving regulations.

© 2026 American Public Transportation Association

- **List of cybersecurity services and tools:** CISA has created a comprehensive list of free cybersecurity services and tools available to organizations, including those in the transportation sector. This repository includes resources for asset management, network monitoring and incident response, all aimed at enhancing visibility and security across IT and OT systems.

3.2 Asset inventory and management tools

Visibility begins with a complete inventory of all assets including hardware, software and networked devices. Automated asset discovery tools and inventory management systems provide real-time data on system components and configurations, ensuring that no asset is overlooked or left unmanaged.

The principles and benefits supporting an effective asset inventory program include the following:

- **Comprehensive and continuous:** Effective visibility requires not just a one-time snapshot, but continuous updates to manage dynamic OT environments, where devices, sensors and connections change as operations evolve. Automated asset discovery tools ensure that agencies maintain a living map of their environment.
- **Foundation for security:** Without an accurate inventory, even the best cybersecurity policies or tools can fail. Knowing exactly what assets exist is the first step in risk management. It can allow agencies to identify vulnerabilities, enforce patching and monitor unexpected changes.
- **Operational impact:** Beyond security, asset inventories help with maintenance and operational decision-making. By understanding the full range of components and their configurations, agencies can optimize maintenance schedules, plan upgrades more effectively and reduce downtime.
- **Regulatory alignment:** Federal directives such as TSA SD 1580/1582 and best practices in standards such as IEC 62443 underscore the need for comprehensive asset inventories as a foundation for compliance. Accurate inventories ensure that agencies can produce the documentation required for audits and maintain eligibility for critical funding.
- **Improved collaboration:** Up-to-date asset inventories also support collaboration with vendors and third parties. Knowing exactly what devices and systems are in place allows for clearer contracts, better security oversight, and shared responsibility for maintaining a secure and reliable transit environment.

3.3 Network monitoring tools

Continuous network monitoring is essential to identify abnormal activities and understand data flows. Tools such as intrusion detection systems (IDS) and network traffic analyzers help establish operational baselines, detect suspicious activity and respond to threats quickly. These tools should provide the following benefits to transit agencies:

- **A complete picture of data flows:** Visibility tools allow agencies to map not just asset inventories, but also how those assets communicate by uncovering data flows, identifying system interdependencies and alerting to potential bottlenecks. This capability is important because the dynamic nature of the interconnections may not be obvious in static diagrams.
- **Operational baselines:** By creating a dynamic baseline of normal data flow patterns, agencies can better understand how their environment should function, forming the foundation for all future security and reliability decisions.
- **Help in identifying interconnections:** Visibility efforts reveal how different OT and IT systems are connected, providing critical insight into where security boundaries exist and where they might need to be strengthened.

© 2026 American Public Transportation Association

- **Inform proactive decision making:** Visibility into network activity doesn't just identify what's connected; it highlights how systems are used day to day, supporting proactive maintenance, configuration updates and governance decisions.
- **Support evolving compliance requirements:** Regulatory frameworks like TSA SD 1580/1582 and IEC 62443 emphasize the need for complete visibility into network activity. Agencies that build this visibility now are better prepared to meet evolving regulatory expectations

3.4 Data logging and analysis

Rich, well-organized logs also support transparent documentation and enable agencies to clearly demonstrate operational integrity and compliance with regulatory expectations. Comprehensive logging and analysis tools, such as security information and event management (SIEM) platforms, form the backbone of operational visibility in transit OT environments. These tools capture detailed records of system events, network activity and configuration changes, providing a continuously updated view of how systems operate and interact.

Key benefits to effective logging regimens:

- **Builds an authoritative record:** Logging tools provide a historical record of how assets and systems behave, forming a trusted source of truth that agencies can rely on to inform decision-making.
- **Uncovers system relationships:** By capturing and analyzing system events, agencies gain visibility into dependencies and interactions that might not be immediately obvious in static documentation.
- **Helps maintain configuration awareness:** Logs of configuration changes and system updates highlight potential areas of misalignment with security baselines, ensuring that agencies maintain an accurate picture of their operational environment.
- **Supports governance and compliance:** Comprehensive, well-maintained logs are essential for meeting regulatory expectations around visibility and operational accountability.
- **Enables proactive improvements:** Visibility through logging helps agencies identify opportunities for operational enhancement, such as optimizing workflows or refining asset configurations.

3.5 Vulnerability management and assessment processes

Regular vulnerability assessments and patch management are critical for identifying and addressing weaknesses in OT systems. These processes go beyond simply scanning for vulnerabilities; they form the foundation for proactive risk management and regulatory compliance. Automated vulnerability scanners, tailored for OT environments, identify known and emerging vulnerabilities in software, firmware and network devices. These tools typically integrate with asset inventories to ensure that scans cover all critical components, including legacy systems and specialized OT devices. When a vulnerability is detected, it is logged in a central repository or vulnerability management platform, where it can be prioritized based on severity, potential impact on operations and exploitability.

The patch management tools complement this process by providing automated tracking, testing and deployment of security updates. These tools are configured to respect the unique demands of OT environments, including system uptime requirements and operational constraints. Before deploying a patch, OT teams typically conduct rigorous testing in a controlled environment to ensure that it does not disrupt operations or introduce new risks. Working with engineering, operations and maintenance teams to arrange for joint use of a test lab and test equipment that mirrors production can benefit multiple stakeholders and even help justify the funding of such environments. Testing often involves verifying the patch's compatibility with existing configurations and validating that no critical services will be impacted.

A well-structured vulnerability management and assessment process also involves continuous monitoring and feedback. Transit agencies should regularly review vulnerability scan results, adjust scanning schedules based

© 2026 American Public Transportation Association

on changes in operational risk, and incorporate threat intelligence to stay ahead of new vulnerabilities. They should then integrate these processes into a broader cybersecurity program that is aligned with frameworks such as NIST SP 800-82 and IEC 62443. This ensures that vulnerability management is not just a reactive exercise but a continuous improvement effort.

Ultimately, these activities help transit agencies maintain system integrity, minimize disruption from cybersecurity threats, and meet regulatory expectations from oversight bodies like the TSA and the FTA. They also foster collaboration between IT, OT and engineering teams, embedding cybersecurity considerations throughout daily operations and long-term planning.

3.6 Architectural reviews and configuration audits

Periodic architectural reviews and configuration audits are essential for evaluating how systems interconnect, where vulnerabilities may exist and how to maintain robust security. These reviews play a critical role in establishing and sustaining visibility across transit OT environments.

Visibility is not simply about knowing which assets are in place. It also requires understanding how those assets interact within complex transit ecosystems. Architectural reviews provide a structured process for mapping out these relationships, identifying critical data flows, and uncovering potential blind spots in monitoring and security coverage. These reviews include analysis of network segmentation, trust zones and data exchange points, all of which contribute to a clearer picture of potential attack paths.

Configuration audits complement these reviews by ensuring that device and system settings align with agency policies, industry best practices, engineering design drawings/documents and current regulatory requirements. Such audits verify that controls like software/firmware/application logic versions, access permissions, authentication methods and encryption settings are consistently and correctly applied across the entire architecture. This is another area where working with the engineering and maintenance teams responsible for the associated equipment is critical—and can avoid multiple teams performing the same tasks or creating separate audit data.

By integrating architectural reviews and configuration audits into a broader governance framework, transit agencies can ensure that visibility is not a one-time exercise but a continuously validated capability. These processes help identify outdated configurations, misconfigured devices or unintended changes that might reduce the effectiveness of monitoring and detection systems.

Ultimately, architectural reviews and configuration audits reinforce the agency’s commitment to safe, resilient operations. They ensure that visibility remains aligned with evolving regulatory requirements and that transit services can continue to operate securely and reliably in the face of new challenges.

3.7 Collaboration with third-party partners

Many transit agencies rely on third-party vendors and integrators to deliver and support OT systems and services. Extending visibility beyond agency boundaries is crucial for maintaining a comprehensive security posture and ensuring accountability across the entire supply chain.

Visibility in the context of third-party relationships involves more than periodic check-ins or contractual obligations. It requires establishing secure data-sharing agreements that define how vendors provide access to information about their systems, updates and security practices. These agreements should include expectations for the frequency and detail of reporting, such as vulnerability disclosures, software bills of materials (SBOMs) and any incidents that may affect transit operations.

© 2026 American Public Transportation Association

A robust documentation review process is another essential aspect of extending visibility. Agencies should regularly review vendor-supplied documentation including security architecture diagrams, testing and validation results, and patch management plans to verify that security expectations are being met. This review ensures that agencies have a clear understanding of third-party systems and can map how they integrate with transit-critical infrastructure.

Clear roles and responsibilities for security assurance must be defined in vendor contracts. This includes specifying which party is responsible for monitoring, managing and responding to vulnerabilities and threats within vendor-supplied systems. These roles should align with the agency's internal governance framework, ensuring that security gaps at the vendor level do not compromise the overall resilience of transit operations.

Extending visibility to third parties not only helps transit agencies meet regulatory requirements but also strengthens their ability to anticipate, detect and respond to emerging threats. By treating third-party visibility as an integral part of governance and operational resilience, agencies can build stronger, more transparent partnerships and uphold the trust of the communities they serve.

3.8 Integration with compliance and governance programs

Visibility efforts must align with broader compliance and governance frameworks. This integration ensures that visibility is not a standalone effort but a strategic capability that supports regulatory requirements and advances the agency's mission of safe, resilient and transparent transit operations.

Effective visibility involves not just deploying asset inventory tools and monitoring systems but embedding them into the agency's compliance and governance structures. For example, regulatory mandates such as TSA Security Directives require transit agencies to have robust processes for identifying and managing cybersecurity risks. Integrating visibility into governance programs also helps agencies establish clear accountability for the security posture. Governance frameworks such as those informed by NIST SP 800-82 and the IEC 62443 standards emphasize assigning roles, responsibilities and decision-making authority. Visibility informs governance activities by enabling informed decision-making, risk prioritization and organizational oversight.

In practice, this means that visibility tools and processes must be aligned with policies and procedures for configuration management, incident response and change control. Visibility data should be reviewed as part of routine governance meetings and used to validate that controls are effectively implemented and that any gaps are promptly addressed. This integration also enables the agency to adapt to evolving threats and regulatory changes by ensuring that visibility efforts remain aligned with the broader organizational mission.

3.9 Visibility in OT systems: Tools, collaboration and IT/OT integration

Visibility is essential for ensuring the safety, reliability and resilience of OT environments. It means having a comprehensive, real-time understanding of assets, configurations and data flows, along with the ability to monitor and respond to emerging risks. Achieving robust visibility requires more than just technical tools. It demands interdepartmental collaboration and seamless integration with IT systems.

3.9.1 Tools for visibility

Modern visibility efforts rely on a combination of specialized tools and integration methods:

- **Network discovery tools:** These tools automatically scan the OT network, identifying all connected devices and mapping their relationships. They help reveal both authorized and unauthorized assets that could introduce risk.

© 2026 American Public Transportation Association

- **Active querying:** Techniques like active scanning and protocol-specific queries provide detailed device information, including firmware versions and configurations. In OT environments, active querying must be carefully managed to avoid impacting sensitive operations.
- **Third-party system integration:** Many transit agencies rely on external vendors and integrators. APIs and secure data-sharing arrangements enable integration of vendor data. This might include asset lists, software updates and known vulnerabilities.

3.9.2 IT/OT integration

Visibility cannot stop at the OT edge. In today's converged environments, IT systems (like enterprise asset management, patch management and identity systems) contain critical data that enhances OT visibility. Effective integration of IT and OT data ensures a unified view of risk and enables coordinated cybersecurity and operational decisions.

For example, integrating IT-based asset management systems with OT network discovery tools can provide real-time updates about device locations, configurations and life cycle status. Likewise, central SIEM platforms, traditionally focused on IT, can ingest OT data to support broader threat detection and response.

3.9.3 Interdepartmental collaboration

Visibility is not solely the responsibility of facilities staff or security teams. Joint asset inventory reviews should include IT, OT and operations staff. By sharing maintenance schedules, change logs and network updates, the team can ensure that monitoring and detection systems remain current and effective. It demands active, continuous collaboration across the entire organization. Operations teams, maintenance staff, IT professionals and asset owners must all participate to ensure that visibility efforts are complete, accurate and aligned with real-world system states.

3.9.4 Dynamic processes and mutual benefits

Achieving comprehensive visibility across OT and IT systems is not just a technical goal. It's a strategic imperative for maintaining safe, resilient and efficient transit operations. The processes that support visibility must be dynamic, adapting to constant changes in OT and IT environments. Formal procedures should govern the following:

- How assets are added, updated or decommissioned.
- How data is shared across departments and with third parties.
- How visibility findings are integrated into security and operational decisions.

Collaboration and shared responsibility ensure mutual benefits: Operational teams gain confidence in the integrity and reliability of their systems, while security and IT teams get the insights they need to proactively manage risks.

3.10 Testing and functional activity

Establishing comprehensive visibility in transit environments requires a combination of functional activities and rigorous testing. While continuous monitoring and system configurations provide the foundation, targeted testing activities are equally essential to validate and strengthen visibility. Penetration testing exercises serve as controlled simulations that mirror real-world scenarios, providing agencies with practical insights into where visibility gaps exist and how they can be addressed. These testing activities not only identify technical vulnerabilities but also challenge organizational readiness, ensuring that agencies can respond effectively to evolving cybersecurity threats.

© 2026 American Public Transportation Association

3.10.1 Penetration testing to enhance visibility

Penetration testing is a proactive approach to improving visibility in transit environments. By simulating well-controlled and coordinated real-world attacks against operational systems, these tests expose vulnerabilities, misconfigurations and gaps in monitoring. Effective penetration tests assess how well OT and IT systems can detect and respond to adversarial activity, offering insights into the visibility or lack of visibility of critical assets and networks. By identifying and remediating blind spots through these tests, transit agencies can build a more accurate understanding of their risk landscape and strengthen their monitoring and detection capabilities.

3.10.2 Exercises to validate and expand visibility

Exercises, including tabletop and red team/blue team simulations, play an essential role in validating and expanding visibility. These structured scenarios force transit agencies to test detection, response and communication processes in a controlled setting. Exercises help agencies identify areas where visibility is lacking, whether due to unclear data flows, insufficient sensor coverage or misaligned response protocols. They also promote cross-functional collaboration, ensuring that engineering, operations and cybersecurity teams have a shared understanding of how to maintain continuous visibility. By integrating these exercises into regular practice, agencies can refine their visibility programs and ensure that teams remain prepared for evolving threats.

4. Implementation

Achieving comprehensive visibility in rail transit environments requires a combination of the right tools, well-defined processes and strong organizational collaboration. This section defines what effective visibility looks like and provides high-level guidance for developing an implementation plan.

4.1 What good visibility looks like

Good visibility means having a clear, accurate and up-to-date view of all systems and assets, along with their configurations, status and interactions. In IT environments, this typically involves a CMBD that documents asset ownership, patch status, life cycle data, and physical or virtual locations. Such CMDBs are integrated with patch management and endpoint monitoring tools to ensure security and operational alignment.

In OT environments, good visibility includes accurate and up-to-date SCADA maps that are tied to real-world physical layouts. These maps should be tagged and linked to asset records to provide context about system interdependencies and operational flows. Visibility at this level helps transit agencies quickly identify issues and respond to incidents in a way that respects operational priorities and physical safety.

At the integration level, mature visibility involves consolidated dashboards or data lakes that unify IT and OT data. These platforms map business systems such as maintenance management and service delivery with field infrastructure such as signaling systems and power supplies. Such integrated visibility is foundational for proactive risk management, regulatory compliance and operational efficiency.

4.2 Organizational roles and collaboration

Effective visibility is not the responsibility of the cybersecurity team alone. It requires a holistic approach that involves the following:

- **Asset management teams,** who maintain the source of truth for equipment and configurations.
- **Engineering teams,** who understand how systems are designed and deployed in the field.
- **IT operations staff,** who manage enterprise systems and ensure that integrations are properly maintained.

© 2026 American Public Transportation Association

- **Maintenance and operations teams,** who often have the most up-to-date information on field-level devices and configurations.

To ensure alignment and accountability, agencies should establish cross-functional working groups or governance boards. These groups set expectations, coordinate updates, and continuously validate that visibility efforts remain accurate and up to date.

A practical example of this collaboration is a monthly review meeting that brings together representatives from IT, OT, engineering and maintenance. This meeting focuses on reviewing any new or changed devices, validating updates to the asset inventory, and coordinating any required security or operational changes. This allows the introduction of upcoming initiatives, the sharing of observed risks and deconfliction of new organizational requirements. By formalizing these collaboration mechanisms, agencies can ensure that visibility is sustained and integrated into daily operations, rather than treated as a one-time technical project.

4.3 Roadmap to implementation

Implementing an effective visibility program in transit rail systems requires a structured and phased approach that aligns with operational priorities and regulatory expectations. The implementation roadmap below provides a clear pathway for transit agencies to enhance visibility of assets, networks and systems across OT environments, from signaling and train control systems to fare collection and communication infrastructure. This roadmap outlines sequential activities to establish a comprehensive asset inventory; strengthen network mapping; deploy continuous monitoring capabilities; and ensure that all visibility efforts support operational reliability, safety and cybersecurity resilience. By following this roadmap, agencies can build the foundational visibility needed to proactively manage risks and improve decision-making across the life cycle of transit operations.

4.3.1 Establish program governance and leadership

A strong governance structure sets the tone for a successful visibility program. By establishing leadership and defining clear roles, transit agencies ensure that visibility efforts have direction, accountability and the organizational backing needed to succeed.

- Designate a program owner (e.g., chief information security officer or director of OT security).
- Form a cross-functional working group with representatives from IT, OT, engineering, operations, maintenance and safety to ensure broad perspective and buy-in.
- Define roles and responsibilities clearly so everyone understands their contribution to maintaining visibility.

4.3.2 Conduct a baseline assessment

Understanding the agency’s starting point is critical. A baseline assessment provides the foundation for all future visibility work by identifying current capabilities, gaps and areas needing improvement across both IT and OT environments.

- Review and validate asset inventories to identify what is currently known about IT and OT systems.
- Identify known gaps in documentation, asset discovery or process visibility. This is really important in areas with outdated or incomplete records.
- Map existing physical diagrams and engineering data to digital inventories to ensure accuracy.

© 2026 American Public Transportation Association

4.3.3 Develop a comprehensive visibility strategy

A clear strategy aligns efforts with organizational priorities and external mandates. This step translates an agency's mission and regulatory requirements into a concrete plan that prioritizes risks and focuses resources where they are needed most.

- Align strategy to standards and regulations (NIST SP 800-82, IEC 62443, TSA SD 1580/1582) to ensure compliance and best practices.
- Set specific visibility goals, such as real-time network monitoring or accurate life cycle tracking of assets.
- Prioritize visibility efforts in high-risk or high-impact areas (e.g., control centers, wayside equipment or critical OT systems).

4.3.4 Select and deploy technical tools

Choosing and deploying the right technical tools is essential to achieve practical and reliable visibility. These tools must be carefully selected to match the unique needs of OT environments while ensuring compatibility and minimal operational disruption.

- Choose the right mix of tools (passive monitoring, active scanning, network discovery) to match operational needs.
- Use passive monitoring in sensitive OT environments to avoid operational impact.
- Integrate IT/OT asset data in CMDBs and asset management platforms for unified tracking.
- Secure remote access solutions to allow safe monitoring and troubleshooting of remote OT devices.
- Incorporate third-party data sources (vendor patch data, SBOMs) into monitoring platforms.

4.3.5 Integrate IT and OT data streams

Visibility efforts are strongest when IT and OT data are seamlessly integrated. This step focuses on breaking down silos and creating a unified picture of assets and systems to support comprehensive monitoring and decision-making. This may not align with the strategic cyber objectives of some organizations. However, if there is not an architectural strategy for complete separation, transit agencies should do the following to achieve visibility goals:

- Establish secure data-sharing protocols between IT and OT to avoid siloed visibility.
- Deploy unified dashboards or data lakes that present integrated views of IT and OT asset health and security status.
- Ensure that third-party and cloud-based data are captured and included in these integrations for complete context.

4.3.6 Develop and document visibility processes

Documented, repeatable processes are the backbone of sustainable visibility. This section focuses on formalizing how agencies track assets, monitor changes and validate system configurations to ensure consistent and reliable results.

- Create documented processes for inventory updates, configuration checks and architectural reviews.
- Establish consistent change tracking to ensure that asset records are updated when new devices or configurations are introduced.
- Set clear thresholds for alerts and responses to guide teams on when to escalate or investigate anomalies.

© 2026 American Public Transportation Association

4.3.7 Train stakeholders and build a collaborative culture

People are as critical as technology in achieving visibility. This step highlights the need for ongoing training and a culture of shared responsibility, ensuring that everyone understands their role in maintaining a secure and resilient environment.

- Provide targeted training for IT, OT, engineering, maintenance and operational staff to understand their roles in visibility and security.
- Use scenario-based exercises to help teams practice and validate the use of visibility data.
- Foster a culture of shared accountability so all departments see visibility as a core part of safe, secure operations.

4.3.8 Validate and test visibility controls

Even the best tools and plans require validation. This section focuses on confirming that visibility controls are functioning as intended and that they remain effective in the face of evolving operational and security challenges.

- Perform vulnerability assessments to confirm that visibility covers all critical assets.
- Conduct architectural reviews to ensure that digital models match actual field deployments.
- Test tool interoperability and validate integrations across IT and OT boundaries.

4.3.9 Establish a continuous improvement cycle

Visibility is not a one-time project—it's an ongoing effort. Establishing a continuous improvement cycle ensures that transit agencies can adapt to new risks, integrate lessons learned and remain resilient over time.

- Set a regular cadence (monthly, quarterly) for reviewing visibility processes and data integrity.
- Incorporate feedback from incidents and maintenance activities to refine visibility processes.
- Stay informed about new standards, tools and threats that could impact visibility.

4.3.10 Report and communicate progress

Transparency and accountability are key to sustaining visibility efforts. This step ensures that progress is documented and shared with stakeholders, building trust and reinforcing the agency's commitment to secure, reliable transit operations.

- Define key performance indicators (KPIs) to measure progress, such as number of assets inventoried or reduction in blind spots.
- Regularly update leadership and key stakeholders on progress and challenges.
- Document lessons learned to continuously improve visibility practices and maintain a strong security posture.

4.3.11 Safeguard artificial intelligence

As agencies work to improve visibility, it's important to recognize the dual dynamic of AI. First, AI is increasingly being deployed as a tool to support visibility. It might leverage machine learning and advanced analytics to identify anomalies and patterns that would be difficult for humans to detect alone. Second, AI can also become a source of hidden vulnerabilities, as its decision-making processes can be opaque and sometimes misaligned with operational objectives. For this reason, agencies must ensure that they have full visibility not only of their traditional OT and IT systems but also of how AI systems are making decisions, learning and adapting. Without this level of transparency, even the most sophisticated AI-enhanced visibility measures can inadvertently introduce new risks.

© 2026 American Public Transportation Association

4.4 Cohesive approach to visibility

Table 1 presents a comprehensive view of the key components of visibility within transit OT environments. It highlights the essential tools and processes that support asset discovery and monitoring, as well as the critical role of interdepartmental collaboration. This includes IT/OT integration and the dynamic nature of these processes. This table illustrates how transit agencies can build a cohesive approach to visibility, blending technical solutions, organizational roles and governance structures to ensure safe, reliable and transparent operations.

TABLE 1
Visibility Components

Visibility Element	Description	Examples	Standards and Guidance
Network discovery tools	Tools for automatically identifying connected OT assets and network paths	Passive or active scanning solutions tailored to industrial protocols (e.g., Modbus, DNP3)	NIST SP 800-82, CIS Control 1, IEC 62443-3-3, CENELEC TS 50701
Active querying	Methods to gather detailed device configuration, version and status data	Protocol-based queries (SNMP, BACnet, ICCP), firmware/patch inventory checks	NIST SP 800-82, IEC 62443-2-1, CENELEC TS 50701
Third-party system integration	Incorporation of vendor-supplied data and external monitoring capabilities	APIs and secure data-sharing agreements to integrate asset inventories, patch advisories and SBOMs from vendors	CIS Control 15 (Service Provider Management), IEC 62443-2-4, NIST CSF (Supply Chain Risk)
IT/OT integration	Coordination of IT and OT data and systems to maintain unified visibility and security posture	Linking enterprise IT asset management systems to OT monitoring tools; integrating SIEM/SOC capabilities across environments	NIST SP 800-82, CIS Control 1 & 4, IEC 62443-2-1, CENELEC TS 50701
Interdepartmental collaboration	Working across engineering, operations, maintenance, security and asset management to ensure shared visibility	Joint reviews of asset inventories, configuration audits and change management records to ensure accurate and up-to-date system views	NIST CSF (Governance and Risk), IEC 62443-2-1, CENELEC TS 50701
Configuration audits and architectural reviews	Regular assessments to confirm that system configurations and architectures align with security and operational best practices	Conducting audits of firmware/software versions, network segmentation, trust boundaries and security settings	CIS Control 4, NIST SP 800-53 CM-6, IEC 62443-2-1, CENELEC TS 50701
Dynamic processes and continuous Improvement	Regularly updating visibility processes to adapt to evolving technologies, operational changes and threats	Implementing policies for continuous inventory updates, data-sharing improvements and life cycle reviews for assets and their associated security measures	NIST CSF (Continuous Monitoring), IEC 62443-1-1, CIS Control 4

5. Case studies

Visibility is the foundation of a secure and resilient transit rail environment. These two case studies highlight the tangible impact of comprehensive visibility on asset management, risk mitigation and operational effectiveness.

© 2026 American Public Transportation Association

5.1 Case 1: Visibility of rail cars

In a recent visibility initiative, a transit agency focused on assessing rail car assets and network-connected systems. Through a detailed asset discovery and analysis process, the team identified more than 20 telematics devices that had not been previously documented in asset inventories. These devices, which provide data about rail car location, speed and condition, were found to be running outdated firmware, leaving them vulnerable to security breaches and data integrity issues.

This discovery process highlighted the critical need for robust asset management practices and the integration of automated discovery tools. By addressing these gaps, the agency not only eliminated a significant security risk but also improved the reliability of operational data used for rail car maintenance and performance tracking.

This case underscores the fact that unmanaged or "invisible" devices can pose silent but significant threats to transit systems, and it reinforces the importance of regular visibility reviews.

5.2 Case 2: Integrated visibility dashboard

Another agency faced challenges with siloed visibility across SCADA systems, asset management platforms and IT network monitoring tools. Investigations into incidents and performance issues often required switching among multiple platforms and cross-referencing data manually, which slowed response times and created confusion about the current state of systems.

To address this, the agency implemented an integrated visibility dashboard that consolidated data from these previously disconnected systems. The new dashboard provided a single, real-time view of the entire transit environment, including physical assets, control systems and IT infrastructure. As a result, investigation times for security events and system failures were reduced by 60%, dramatically improving the agency's ability to respond to issues and maintain safe, continuous service.

This approach demonstrated the power of a holistic visibility strategy that bridges traditional silos between operations, maintenance and cybersecurity teams.

5.3 Lessons learned: Visibility is not a tool, but a capability and a mindset

The key takeaway from these use cases is that visibility should not be seen as a one-time project or a standalone tool. Instead, it is a capability that must be woven into the fabric of transit agency operations. Visibility depends on a mindset that prioritizes continuous discovery, validation and collaboration across functional teams.

Effective visibility requires not only the deployment of advanced tools—such as asset discovery platforms, monitoring systems and integrated dashboards—but also a culture of accountability and curiosity. Teams must be empowered to ask difficult questions, probe blind spots, and treat visibility as an ongoing mission rather than a complete task. This mindset shift is especially important as operational technology and IT systems converge, and as agencies incorporate new technologies like AI and IoT devices into their environments. By treating visibility as a strategic capability, transit agencies can stay ahead of evolving cybersecurity threats, protect passenger safety and ensure operational excellence.

6. Transit rail visibility resources

6.1 Visibility controls

Achieving comprehensive visibility in transit rail environments requires a systematic implementation of technical and procedural controls. This includes deploying asset discovery tools to maintain accurate

© 2026 American Public Transportation Association

inventories of hardware, software and network connections; configuring continuous monitoring systems to detect anomalies; and conducting regular reviews to validate and update these controls. Equally important is integrating governance and policy frameworks to assign accountability and ensure collaboration across departments. Controls should also account for the unique challenges of OT environments, where legacy systems and physical safety considerations demand tailored visibility strategies.

By treating visibility as an ongoing effort rather than a one-time task, transit agencies can proactively manage risks and strengthen their cybersecurity posture.

6.1.1 NIST Cybersecurity Framework (especially the Identify function)

The NIST CSF's Identify function lays the groundwork for effective cybersecurity by establishing a clear understanding of the assets, systems and people within an environment. This includes developing an inventory of assets, mapping data flows and clarifying governance structures. For transit agencies, leveraging the Identify function ensures that all components of rail OT and IT systems are known and documented, forming the foundation for effective monitoring and risk management.

6.1.2 NIST SP 800-82, ICS security

NIST SP 800-82 provides guidance specifically for securing industrial control systems (ICS), such as those used in rail signaling and SCADA environments. It outlines best practices for asset identification, network architecture and continuous monitoring. By following its recommendations, transit agencies can create accurate inventories of industrial assets and control systems, improving visibility across operational processes.

6.1.3 IEC 62443, Asset Inventory and System Classification

The IEC 62443 series offers comprehensive guidelines for securing industrial automation and control systems. In the context of visibility, it emphasizes the need to identify and classify all assets and establish zones and conduits for network segmentation. These practices are essential for understanding how systems are connected and for maintaining up-to-date inventories, which directly improves visibility and control over critical assets.

6.1.4 CIS Controls 1, 2 and 12

The CIS Controls are a prioritized set of security actions. Control 1 (Asset Management) and Control 2 (Software Inventory) focus directly on asset management—identifying and tracking hardware and software assets. Control 12 (Network Infrastructure Management) extends this by ensuring that the network infrastructure is securely managed. Together these controls help transit agencies maintain detailed visibility of all assets, software and network connections that make up rail environments.

6.1.5 CENELEC TS 50701, Cybersecurity for Rail Signaling and Train Control

CENELEC TS 50701 is tailored for the rail sector, focusing on cybersecurity for signaling and train control systems. It provides guidance on identifying critical assets and system components, ensuring that transit agencies have a complete picture of their signaling environments. This visibility is crucial for managing the complex interactions among signaling, control systems and passenger safety systems.

6.1.6 ISO/IEC 27001, information security management systems

ISO/IEC 27001 sets the standard for establishing, implementing and maintaining an ISMS. While broader in scope, it requires organizations to identify their information assets, assess associated risks and establish controls. For transit agencies, this framework ensures visibility into all information flows and data stores, both IT and OT. It provides a comprehensive approach to asset management and data governance.

© 2026 American Public Transportation Association

6.2 Overview of components for visibility

Table 2 presents a comprehensive view of the key components of visibility within transit OT environments. It highlights the essential tools and processes that support asset discovery and monitoring, as well as the critical role of interdepartmental collaboration. This includes IT/OT integration and the dynamic nature of these processes. This table illustrates how transit agencies can build a cohesive approach to visibility.

TABLE 2
Standards Crosswalk

Control Area	NIST SP 800-82 References	IEC 62443 References	APTA OT-CMF Domains	Transit Rail Application
Asset Inventory & Identification	ID.AM-1, ID.AM-2, Asset Management ID.AM	SR 1.1, SR 1.2	Asset Management	Maintain inventory of rail OT assets (signaling, SCADA, fare systems)
Network Mapping & Connectivity Awareness	ID.AM-4, PR.PT-4, Network Security	SR 1.5, SR 1.6	Network Segmentation & Management	Maintain network diagrams showing asset interconnections, including third-party links
Configuration Management for Visibility	CM-8, CM-2, Configuration Management	SR 7.1, SR 7.2	Configuration Management	Keep configurations updated after changes to signaling/fare systems
Network Monitoring & Detection	DE.CM-1, DE.CM-7, Monitoring	SR 3.1, SR 3.2	Threat Monitoring & Detection	Deploy continuous monitoring and alerts for OT and IT networks
Integration with External Data Sources	ID.RA-1, Risk Assessment	SR 1.4	Third-Party Risk Management	Document and review third-party vendor connections and data flows
Use of Automated Discovery Tools	Automated asset discovery (guidance in document)	SR 3.3	Visibility & Asset Discovery	Use passive discovery tools in rail OT networks to maintain assets and connection visibility
Roles & Responsibilities	Cybersecurity governance responsibilities	IEC 62443-2-1, IEC 62443-3-3 (governance section)	Governance & Risk Management	Assign clear roles for asset tracking and visibility oversight across OT/IT teams

© 2026 American Public Transportation Association

Definitions

APTA OT-CMF: APTA's Operational Technology Cybersecurity Maturity Framework. Published by APTA in 2023, it provides guidance for assessing and improving OT cybersecurity practices in transit agencies.

asset inventory: A comprehensive list of all hardware, software and systems within the transit environment. It provides the baseline for visibility and risk management.

artificial intelligence: An application that can operate and make decisions independently, introducing potential risks if not properly governed and monitored.

CISA: The Cybersecurity and Infrastructure Security Agency is a component of the U.S. Department of Homeland Security that leads the national effort to understand, manage and reduce risk to the country's cyber and physical infrastructure.

configuration management: A practice and process of handling hardware, software and firmware changes systematically so a device or system maintains its integrity over time.

cybersecurity: The field of protecting digital computers and networks from accidental or malicious modifications.

NIST SP 800-53, Rev. 5: A NIST publication titled "Recommended Security Controls for Federal Information Systems and Organizations," which was used in preparing this white paper.

NIST SP 800-82, Rev. 3: A NIST publication titled "Guide to Operational Technology (OT) Security."

patch management: A regular, coordinated method for equipment vendors to update software and firmware fixes for their digital equipment at transit agencies in a timely and responsible manner.

recovery: The appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

risk management: The process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level.

SCADA: A control system involving a master terminal unit and remote terminal units, used for supervisory control and data acquisition.

threat monitoring and detection: Activities designed to detect and analyze potential threats within networks, systems, and operational environments.

Abbreviations and acronyms

AI	artificial intelligence
CBTC	communications-based train control
CCE	Consequence-Driven Cyber-Informed Engineering
CISA	Cybersecurity and Infrastructure Security Agency
CMBD	configuration management database

© 2026 American Public Transportation Association

CSET	Cybersecurity Evaluation Tool
FHWA	Federal Highway Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
ICCP	Inter-Control Center Communications Protocol
IEC	International Electrotechnical Commission
IDS	intrusion detection system
IoT	internet of things
ISMS	information security management system
ISO	International Organization for Standardization
IT	information technology
NIST	National Institute of Standards and Technology
OT	operational technology
SCADA	supervisory control and data acquisition systems
SD	security directive
SIEM	security information and event management
SNMP	Simple Network Management Protocol
TSA	Transportation Security Administration

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	Aug. 22, 2025	Dec. 3, 2025	April 19, 2026	May 15, 2026	June 10, 2026

© 2026 American Public Transportation Association