APTA STANDARDS PROGRAM

WHITE PAPER

APTA SS-ECS-WP-007-26

First Published: March 23, 2026

Transit Cybersecurity Working Group

Cybersecurity Considerations for Systems Safety and Security Professionals

Abstract: This white paper shares considerations for public transit safety and security personnel regarding the inclusion of cybersecurity threats and risks in their hazard analysis and threat assessment processes. Further, the document provides guidance on how and when an agency's primary cybersecurity coordinator should be involved in the assessment process and/or in incident response/investigation. The document is composed of guidance from various industry sources including but not limited to the APTA Operational Technology Cybersecurity Maturity Framework (OT-CMF), APTA's recommended practice "Safety and Security Certification" (APTA SS-ISS-RP-008-24), other applicable APTA recommended practices, the National Institute of Standards and Technology (NIST) Special Publications 800-30 and 800-82, NIST Cybersecurity Framework, and other industry best practices to support efforts associated with risk assessment, mitigation strategies, system resiliency and redundancy, and incident management.

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

Summary: To drive system efficiencies, improve customer experience and support enhanced use of transit infrastructure, public transportation is becoming increasingly connected. The operational technologies systems of the past, which had been relatively isolated, are increasingly being connected to agency networks for a variety of reasons. Not least of these are greater operational efficiencies and customer visibility in fleet operations. Despite the benefits, this connectivity increases risks to operations, which agencies must understand prior to allowing for communication between security zones. Each additional pathway of communication results in an increase in the potential attack surface of OT. This contributes to increased risks to OT systems in public transportation, with the potential to impact the safety and security of agency employees and the traveling public. Further, disruptions of the operations of these systems and the resources they support could have potentially cascading effects on the societies that depend on them. Given these factors, cybersecurity is a vital component in ensuring system safety.

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.

Table of Contents

List of Figures and Tables

Participants

The American Public Transportation Association greatly appreciates the contributions of the Transit Cybersecurity Working Group (TCSWG), which provided the primary effort in the drafting of this document. The Primary Author and Working Group Lead: **Matthew Dimmick**, STV Incorporated. Sub-group members included Jack Odom, Vivian Papen, Dave Teumim, Tri Le, and Hillman Mitchell, Ahmed Idrees, Mike Echols.

At the time this White Paper was completed, the Transportation Cybersecurity 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

Ahmed Idrees, *Sound Transit*
Matthew Dimmick, *STV Inc.*
Abayomi Muse, *Safety Transit Solutions*
Justin K. Smith, *Amtrak*
Paul Braunschweig, *TSA*
Jessie Gill, *British Columbia Rapid Transit District*
Patrick Guest, *NICTD*
Yoav Levy, *Cervello*
Kenneth Blackwell, *Vallley Transit Authority*
Rafi Khan, *New Jersey Transit*
Giampaolo Orrigo, *Alstrom Group*
Shaked Kafzan, *Cervello*
Christopher Heil, *Hatch*
Michael Godfrey, *WDG Consulting*
Alan Jones, *Lextran*
Dave Teumim, *Teumim Consulting*
Hillman Mitchell, *CICSC*
Rachel Dean, *Transit Safety Solutions*
Paul Townsend, *TSA*
Susan Howard, *Michael Baker International*
Dr. Jerry Joyce, *Hatch LTD*
Juan Degree-Hayes, TSA
Mark Johnston, *TriMet*
Tri Le, *Armand*
Mark Curry, *Secheron SA*
Jack Oden, Parsons Government Services
Edward B. Taylor, *TSA*
Kevin Harnett, IO Active
Catarina Tran, *TSA*
Anthony Candarini, *Google Mandiant*
Ryan Brumley, *Sonoma-Marin Area Rail Transit*
Mike Shifman, *Cylus*
David Moskowitz, *Charlotte Area Transit System*
Chris McKay, *TSA*
Vamsikrishna Gutta, *Alstom*
Todd Ellis, *Hatch LTD*

Project team

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

Introduction

This introduction is not part of APTA SS-ECS-WP-007-26, "Cybersecurity Considerations for Systems Safety and Security Professionals."

APTA recommends the use of this document by:

- individuals or organizations that operate public transit systems;
- individuals or organizations that contract with others for the operation of public transit systems; and

- individuals or organizations that influence how public 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 paper is intended to educate and inform the reader 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.

Cybersecurity Considerations for Systems Safety and Security Professionals

1. Overview

With today's increasing automation and interconnectivity of systems, cybersecurity plays a critical role in ensuring system safety. The cybersecurity threat landscape is highly dynamic and evolves continuously over the extended life of a transportation system or project. For this reason, cybersecurity should be integrated into the project/system during the earliest stages of planning, and the in an agency's operations throughout the life cycle of the system or asset(s). This white paper offers reasonable and prudent considerations for agencies and personnel who are responsible for implementing programs relating to transit safety that may be impacted by cybersecurity risk

Transit agencies recognize the growing concern of cybersecurity, and they are increasingly taking action to reduce operational, safety and financial risks resulting from cybersecurity risks. With the unprecedented pace and complexity of cyberattacks occurring globally and across many verticals, transit agencies must take the necessary steps to be proactive, adopting a holistic cybersecurity approach to protect their critical information and fulfill their obligation to customers. Cybersecurity vulnerabilities are most often identified and exploited in information technology systems, potentially enabling access to the agency's OT systems if adequate segmentation is not in place.

Transportation faces increasingly sophisticated threats that often evolve more rapidly than the defensive updates or mitigations designed to protect the affected networks, systems, and devices. The threats that transportation faces continue to grow in sophistication and often evolve at speeds that are exponentially faster than networks, systems and devices can be updated or enhanced to compensate for them. Hence, mitigating cybersecurity risks to the greatest extent practicable requires that an agency's cybersecurity strategy be tightly woven into the organization's fabric at all levels. It is not possible to mitigate all cybersecurity risks. That stated, a whole-of-agency, risk-based approach to cybersecurity, resilience and redundancy is required to maintain the promise of safe and reliable transportation that has been made to transit customers throughout the United States. Responsible agencies can no longer consider cybersecurity only an IT or Operating Department problem. Cybersecurity threats have the potential to directly impact system safety and security and thus have grown into an issue that requires active involvement at the highest level of leadership.

APTA has developed several working groups to address agency concerns about cybersecurity. The mandate of these working groups is to produce guidance in maintaining adequate cybersecurity that all transit agencies, large or small, can utilize and implement. This document is a supplement to the family of specific cybersecurity-related recommended practices developed by these working groups. It is meant to provide awareness and an overview of cybersecurity considerations for safety and security certification and ongoing safety programs. Other APTA standards that transit agencies can adopt and tailor for their immediate use are linked and referenced throughout.

1.1 Public Transportation Cybersecurity Regulatory Brief

Transit is classified as critical infrastructure, and like other elements of America's critical infrastructure it provides essential services that underpin American society and serve as the backbone of our nation's

economy, security and health. The dependence on and seamless integration of technology into everyday activities and operations has exposed the critical need to address cybersecurity. APTA understands the real cybersecurity threats against transit infrastructure and agencies across the nation. Cybersecurity threats have become an increasingly potent concern, prompting the federal government to identify cybersecurity, associated oversight and enhanced regulations as an important priority.

In its ongoing efforts to shore up the nation's critical infrastructure, the White House and representative Cabinet-level agencies have taken measures to promote cybersecurity throughout critical infrastructure with a heavy focus on the transportation of goods, materials and people throughout the country. This has resulted in the following guidance and directives specific to transportation being issued by TSA and FRA:

1. The TSA Security Directives identified below were reissued as of October 24, 2023. The TSA reissued them because they were set to expire, and they need to be valid to interview agencies and determine compliance. APTA expects that the requirements within these SDs will be codified in the future, making compliance to cybersecurity requirements a consideration in granting agency funding requests. This belief is bolstered by the release of Advanced Notice of Proposed Rulemaking for Enhancing Surface Cyber Risk Management in November 2022, which offered "an opportunity for interested individuals and organizations, particularly owner/operators of higher-risk pipeline and rail operations, to help TSA develop a comprehensive and forward-looking approach to cybersecurity requirements." Further, while these security directives are only currently applicable to a small number of agencies on a non-voluntary basis, APTA expects to see the list of agencies required to address these SDs expand over time.
2. SD 1580-21-01 was the first directive issued by the TSA impacting all freight and railroad carriers (Owners/Operators) described in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads. This SD required agencies to:
    a. Designate a cybersecurity coordinator who will be responsible for reporting cybersecurity incidents to CISA, managing the implementation of cybersecurity program and countermeasure implementations, and be the principal point of contact for the TSA.
    b. Report cybersecurity incidents to CISA.
    c. Develop a Cybersecurity Incident Response Plan (CSIRP) and conduct regular exercises to test the efficacy of the plan.
    d. Conduct a cybersecurity vulnerability assessment (CVA) utilizing the form provided by the TSA.
3. SD 1580-82 has requirements for agencies and has an effective date of May 3, 2025:
    a. Establish and implement a TSA-approved Cybersecurity Implementation Plan:
        i. Covers access control, segmentation, continuous monitoring and detection, and patching systems. For greater detail on these requirements, agencies should refer to TSA Security Directive 1580/82-2022-01D (or latest) FAQs.
        ii. Discusses both physical and logical controls. The physical security piece is not well-defined in the directive, likely because it is assumed that this is known after so many years of safety and security regulation.
    b. Establish a cybersecurity assessment program:
        i. Consider engagement with CISA's Cyber Hygiene Services to see what they can provide and how much of this requirement can be met at no cost.
        ii. Information developed and shared as part of this program must be protected under a sensitive security information (SSI) program.
        iii. Architectural design review must be conducted within the first 12 months and again every two years.

   c. Documentation that may be requested by the TSA to determine compliance includes:
      i. Hardware/software asset inventory
      ii. Firewall rules
      iii. Network diagrams, switch and router configurations, architecture diagrams
      iv. Policy and procedures
      v. Snapshot of activity between OT and IT systems (logs, packet captures)
4. FTA Safety Advisory SA-22-2:
   a. Recommends that state safety oversight agencies direct transit agencies to address at a minimum:
      i. Wayside signal components insufficiently maintained
      ii. Vehicle signal components insufficiently maintained
      iii. Signal system design insufficiency
      iv. Signal system not present.
   b. The remainder of the document is a listing of voluntary/consensus standards, FTA guidance and other resources that may be applicable.

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

2. Cybersecurity frameworks, standards and recommended practices

The following are frameworks that can benefit safety and security professionals.

"Operational Technology Cybersecurity Maturity Framework Overview"

This recommended practice (APTA SS-CCS-RP-006-23) presents an overview and guidance to assist transit agencies in maturing their OT cybersecurity programs. The guidance walks through the six levels of maturity starting with Level 0, which is an on-ramp to launch an OT cybersecurity program. This document sets minimum requirements for control security within the transit industry, helps to standardize control and operations system practices, and promotes the adoption of voluntary industry best practices in control security.

APTA cybersecurity recommended practices

APTA develops standards for public transit system control and communications security. The Control and Communications Security Working Group began its work in 2007 and in 2010 published Part I of the APTA recommended practice "Securing Control and Communications Systems in Transit Environments" (APTA SS-CCS-RP-001-10). Part I is an introductory guide for transit agency cybersecurity and is focused on general principles such as describing transit system networks, organizing a cybersecurity program and performing a cybersecurity risk assessment. Part I is limited in its cybersecurity scope and does not address the specific use of cybersecurity technologies for prevention of attacks once cybersecurity risks are identified. Part II (APTA SS-CCS-RP-002-13) focuses on defining and applying security controls applied to high-risk/consequence and vital systems (safety-critical signaling systems, etc.) and medium-risk/consequence systems (such as SCADA, traction power systems, etc.), while laying out these security controls in the context of a transit agency security plan.

NIST SP 800-53 and 800-82

The Commerce Department's National Institute of Standards and Technology (NIST) is a nonregulatory U.S. federal agency responsible for developing standards and guidelines, including minimum requirements, and for

providing adequate information security for all agency operations and assets. The SP 800 series provides guidance, description, details, and standards in establishing and implementing information security programs. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways that enhance economic security and improve our quality of life.

NIST Cybersecurity Framework

In 2024, NIST released Version 2.0 of its Cybersecurity Framework to help organizations charged with helping the nation's financial, energy, healthcare and other critical systems better protect their information and physical assets from cyberattack. The framework provides a structure that organizations, regulators and customers can use to create, guide, assess or improve comprehensive cybersecurity programs.

Cyber Resilience Review Supplemental Resource Guides

The Cyber Resilience Review Supplemental Resource Guides were developed by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency to help organizations implement practices identified as considerations for improvement during a cybersecurity resilience review, which is an interview-based assessment process. This process is intended to collect information leading to the qualitative measurement of an organization's cyber resilience. Any organization interested in implementing or maturing cyber resilience capabilities may find these guides useful. The implementation guide series includes 10 domains as identified below:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

While all these guides may be useful to personnel responsible for system safety agencies, Guide #7, Risk Management, may be the most informative of the references.

ISA/IEC 62443

The 62443 family of standards has been developed through a consensus-based development process and is internationally recognized as the IEC standard and adopted by the United Nations as its recommended standards for the securing of industrial control systems (ICS). These standards promote the safety, integrity, availability and reliability of ICS as the foundation for cybersecurity program development. The ISA/IEC 62443 standards have not been widely adopted in rail and public transit as of the writing of this white paper. However, the information contained in these documents may be valuable when evaluating safety risks, particularly in assessments where vital processors, programmable logic controllers (PLCs), programmable automation controllers (PACs) and field-level communications are being considered.

IEC 63452

Rail System Cybersecurity is a pending international standard as of this writing. This document aims to create a strong, clear and implementable framework that will enhance the cybersecurity of rail and public transit systems across rolling stock, fixed installations, management systems and additional services.

3. Cybersecurity in the safety and security certification process

There are varying schools of thought on the placement of cybersecurity-related incidents within the safety and security realm, particularly during the safety and security certification process. It is likely that this discussion will be resolved in the future by regulators including the TSA, FTA and FRA. As these discussions continue, agencies and the organizations that support them in safety and security certification may consider the following viewpoints and determine which is most applicable to the process they have undertaken.

Cybersecurity as part of the threat and vulnerability assessment: This school of thought carries the concept forward that cybersecurity attacks by their nature are initiated by threat actors (person-made incidents) and as such fall under the auspices of a TVA. APTA SS-ISS-RP-008-24, "Safety and Security Certification," identifies cybersecurity alongside its physical security counterpart, indicating that the TVA may be the preferred placement of cybersecurity and associated vulnerabilities.

Cybersecurity as an extension of the preliminary hazard analysis: The secondary school of thought centers around the impact of the cybersecurity incident being another pathway for a potential hazard to manifest in the form of loss of visibility, loss of control or the disruption of a process. Many cybersecurity-related risks may be addressed by applying engineering-grade solutions.

In a recent panel discussion, "The Imperative of Cybersecurity in Safety Systems," this question was posed to panelists were comprised of agency safety and security personnel, agency information systems personnel, and contractors providing services in both areas. The consensus of the group was that cybersecurity is ingrained in both the TVA and the PHA in varying aspects. The person-made aspects of cybersecurity threats are the primary consideration for inclusion in the TVA. The potential risks that manifest from these incidents impact systems that are being analyzed as part of the PHA. The anchoring of these documents (what ties them together) is the Critical Elements List (CEL), which makes this the ideal point in the process to first engage with cybersecurity personnel to elicit input. This elicitation process and recommended areas of responsibility are covered shortly.

3.1 Considering cybersecurity in safety and security certification

The purpose of this paper is to inform the reader about the importance of considering cybersecurity elements as a factor when managing and monitoring the safety and security certification (SSC) process of transportation systems and changes to system elements. While cybersecurity has not traditionally been central to the certification process, this supplement offers practical considerations for agencies and personnel involved in the SSC process in response to growing cybersecurity risk.

APTA's recommended practice on these subject states: "Safety and security certification is a process to monitor the work by planners, developers, procurers, and implementers to ensure that a transportation system can demonstrate that the system (or system change) is safe and secure. Safety-critical systems have the potential to cause significant harm or damage if the subsystems and components do not meet safety and security objectives and requirements. For this reason, transit agencies that provide passenger services should adopt a formal top-down approach to managing safety and security risks. This ensures that the physical, functional and operational characteristics of structures, systems, components (including software) and existing facilities are properly identified, changes are controlled, and implementation status is recorded."

Given the current threat environment, acceleration in the capability to conduct cyberattacks against critical infrastructures such as transportation assets, and the limited information provided in this recommended

practice and the Handbook for Transit Safety and Security Certification, the following considerations are provided:

- Personnel implementing SSC should familiarize themselves with the concepts and implementation of a security PHA review[1] or an equivalent method (CyberPHA, Mil Std 882E, etc.) to include cybersecurity risks in the TVA and/or PHA as determined by the agency's program requirements. During this process, the primary focus should be in determining if the system component or element is susceptible to a cybersecurity attack (i.e., hackable).
- All hackable system components should have safeguards implemented to reduce the vulnerabilities of those systems to a level that is as low as reasonably practicable (ALARP). Where practical, non-hackable safeguards should be considered to limit the potential for an attack pathway to be exploited in a manner that causes a system failure or other safety incident.
- Agencies must understand that the cybersecurity threat environment is very dynamic and will often change multiple times during the extended life of a transportation project. For this reason, cybersecurity should be integrated into the overall operations of the project, system and agency throughout the life cycle of the asset. SSC is not intended to provide for cybersecurity throughout the life cycle. It promotes thoughtful consideration during design elements that may reduce the attack surface of the system at the time of its development.
- Agencies should consider including aspects of cybersecurity in the Operational Hazard Analysis (OHA), Safety and Security Management Plan (SSMP), and/or other applicable plans. The OHA should include cybersecurity considerations identified during walk-throughs, through operator and control center operator feedback, through communications and signals reviews, and through safety committee concerns.
- Agencies should consider developing a Cybersecurity Committee as part of their continual cybersecurity risk management processes. This committee may support ongoing hazard/vulnerability tracking resolution. The committee should consist of the transit agency executive management, chief engineer or equivalent, operations director or equivalent, chief safety and security officer, and system safety/security and may have the authority to allocate the resources to perform hazard analysis/vulnerability analysis for the identified hazard/vulnerability and identify the mitigation measure. New projects and proposed changes potentially impacting OT should be brought to the committee for review.

3.2 Responsibility assignment matrix using RACI

Agencies should develop a RACI (responsible, accountable, consulted, informed) model for the safety and security certification process and include the agency's designated cybersecurity coordinator (per TSA Security Directive 1580-21-01) in the appropriate role on all matters relating to cybersecurity. The suggested placement for this individual within the RACI chart is provided in **Figure 1**.

[1]. Marszal & McGlone, Security PHA Review for Consequence-Based Cybersecurity, International Society of Automation, 2019. https://www.isa.org/getmedia/99890f41-45a9-4269-a20c-db97390300f8/SecurityPHA_Marszal-McGlone_Chapter_4.pdf

Figure 1
Primary Cybersecurity Coordinator's Role in SSC

RACI Chart Cybersecurity in Safety and Security Certification			
Position →	Safety Certification Professional	Security Certification Professional	Cybersecurity Coordinator
Tasks ↓			
Certifiable Elements List	R	I	I
Preliminary Hazard Analysis (PHA)	R	I	C
Threat and Vulnerability Assessment (TVA)	A	R	C
Criteria Conformance Checklist	R	C	I

R Responsible – The individual(s) who must complete the task or deliverable (direct contributors).

A Accountable – Ensure accountability to project deadlines and completion (key stakeholders)

C Consulted – Key opinions that weigh heavily on successful project completion (legal, cybersecurity, compliance, finance, etc.).

I Informed – Represent individuals that should be kept in the loop on project progress, changes, etc. but do not have a specific decision-making authority or specialty required for the project to be successfully completed

3.3 Potentially applicable industrial cybersecurity risk assessment standards

There are a wide variety of standards and methodologies that may be used in the assessment of cybersecurity-related risks. The list provided below is for general reference. For ease of consideration, it has been broken down into three categories, transit-specific, general cybersecurity risk assessment and other risk assessment methodologies.

3.3.1 Transit-specific

1. Cybersecurity Assessment Tool for Transit (CATT): This tool assists public transit agencies in formalizing and developing their cybersecurity programs. The CATT and supporting documents were developed to assist small and midsized transit agencies in assessing their cybersecurity preparedness and resilience. More about the program can be found at https://www.transit.dot.gov/research-innovation/cybersecurity-assessment-tool-transit-catt.

3.3.2 General cybersecurity risk assessment

1. Cyber Security Evaluation Tool (CSET): This is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate ICS and IT network security practices. More about this tool can be found at https://www.cisa.gov/downloading-and-installing-cset.
2. NIST 800-30: This standard provides guidance for conducting risk assessments of federal information systems and organizations and may be modified to conduct assessments of agency IT systems and OT systems. See https://csrc.nist.gov/pubs/sp/800/30/r1/final.

3. ISA/IEC 62443-3-2, “Security Risk Assessment for Design”: Provides an ICS-specific approach to conducting risk assessments for the industrial process sector, building automation, medical devices, transportation sectors, electrical production and other users of ICS systems. An overview can be found at https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies.
4. Cyber PHA
5. Control hazard and operability study (CHAZOP)
6. Cyber hazard and operability study (Cyber HAZOP)

3.3.3 Other risk assessment methodologies (not a comprehensive list)

1. MIL-STD 882E, Department of Defense Standard Practice, System Safety. https://mail.system-safety.org/Documents/MIL-STD-882E.pdf
2. ISO/IEC 31010, Risk Assessment Techniques. https://www.iso.org/standard/72140.html
3. ISO/IEC 31000, Risk Management — Guidelines. https://www.iso.org/standard/65694.html
4. British Standards Institute (BSI) 100-3, Risk Analysis based on IT-Grundschutz. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-3_e_pdf.html
5. CENELEC Guide 32, Guidelines for Safety Related Risk Assessment and Risk Reduction for Low Voltage Equipment. https://boss.cenelec.eu/media/bs0h2qaf/clc_guide32_implementation_example.pdf
6. Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework. https://insights.sei.cmu.edu/library/operationally-critical-threat-asset-and-vulnerability-evaluation-octave-framework-version-10/

3.4 Cybersecurity at key phases of safety and security certification

Safety personnel should encourage engineers to apply concepts relating to Consequence-Driven Cyber-Informed Engineering (CCE) and Cyber-Informed Engineering (CIE) where practical to reduce risks associated with cybersecurity incidents. The goal should be to apply non-hackable safeguards, where reasonable and prudent, to limit the potential for adversary exploits of OT systems to result in operational disruptions. Where this is not possible, safety personnel should engage with agency and/or third-party cybersecurity personnel to assist in the evaluation of threats/hazards and identifying relevant controls to mitigate the identified risks where practical. The integration of cybersecurity into key phases of the SSC process as identified above is provided for the certifying personnel to act as a guide for engagement with the appropriately trained systems personnel.

3.4.1 Certifiable Elements (CEL) /Certifiable Items List (CIL) Development

It is not practical to provide a comprehensive list of all assets within all types of transportation systems that may have cybersecurity vulnerabilities and/or pose cybersecurity-related risks. What follows are key system elements that safety and security personnel should consider as potentially having cybersecurity exposures that will require mitigation.

1. Positive train control (PTC) systems
2. Centralized traffic control (CTC) systems
3. Communications-based train control (CBTC) systems
4. Real-time vehicle location (RTVL) systems
5. Train and onboard systems
6. Balise modules
7. Other wayside sensors/devices
8. Network hosts, servers and communications systems elements

9. Supervisory control and data acquisition (SCADA) systems
10. Wireless systems

Each project and each system are unique. As stated, the above is not a comprehensive list of items (systems or subsystems) that may be impacted by cybersecurity-related threats. As a guide for certifying personnel, if a device within the system being evaluated communicates with other devices, then system safety and security professionals should consult with agency cybersecurity staff to understand these communications and associated risks.

3.4.2 Develop and manage conformance to safety and security design criteria

The FTA and APTA cover a variety of inputs that should be considered by personnel conducting safety and security certification for transit projects. Some of the primary inputs are references to standards and codes that should be evaluated to determine what must be included in the design criteria. This white paper contains references to multiple cybersecurity standards, frameworks and best practices that should be considered during the design criteria development. For any items that have been identified as requiring cybersecurity controls, the safety and security certification personnel should engage with the agency's primary cybersecurity coordinator or their designee who is familiar with the applicability of cybersecurity controls to transit projects. Further, these individuals should be consulted on how these references, standards and codes might apply to the specific project.

3.4.3 Test program

Safety and security certification personnel should engage with the primary cybersecurity coordinator and/or their designee to facilitate the inclusion of cybersecurity requirements and specifications into design qualification tests, production verification tests, construction inspection tests and installation verification tests, as appropriate. Where multiple systems are integrated and/or there are interfaces between multiple elements, cybersecurity-related elements should be confirmed for both the individual elements and the overall integrated system.

3.4.4 Manage open items

As part of the SSC program there must be a process in place to ensure that the safety and security components (including cybersecurity controls) designed into the system are present, functional and validated for the project. The primary cybersecurity coordinator or their designee should be informed throughout this process of the status of all cybersecurity controls being implemented. If controls that are expected to be implemented are not present, are not functional or cannot be validated during this process, the requirement should be escalated and the primary cybersecurity coordinator and/or their designee should be consulted.

3.4.5 Verify operational readiness

Verifying operational readiness has a variety of activities, including but not limited to:

- Develop operations, maintenance, emergency readiness and other plans, policies and procedures.
- Develop and accept operator's manuals for all systems, equipment, facilities, etc.
- Develop individual and agency-level training, and have all responsible personnel complete it.
- Conduct training exercises (walk-through, tabletop, drills, functional and full scale).

Each of the above areas may have cybersecurity requirements included in the deliverables and/or final product. As an example, an agency may implement an asset inventory and vulnerability management platform. This platform should be supported by the development of the above materials and an associated

training program. The response to an identified vulnerability would be addressed in the agency's procedures for the system, and the response protocol might also be tested through means of a training exercise.

3.5 Overview of cybersecurity assessments in safety systems

The purpose of this paper is to inform the reader about the importance of cybersecurity assessments of rail operations safety systems.

For those that are not familiar with safety systems, it is important to understand that such systems ensure the safety of everyone associated with the operational systems. In rail operations, for example, engineers and other rail operations personnel may be injured or killed if the safety systems fail to reduce speed or shut down operation of the train in the event that safety parameters are exceeded. While rail operations personnel have some control over the train operation and may override systems to restore safe operation, safety systems are there to assist the operators. In a similar way, the safety of rail passengers and the public near rail operations are equally at stake, but they have little to no control.

Rail safety systems are often directly connected to the physical systems of the train using serial, also known as twisted pair, communications. They monitor speed, orientation, track and wayside activity, as well as many other critical factors, and they are connected to engine power, braking, and other speed and rail control devices. These are all local, physical safety control systems. In addition to being connected to physical systems, they are becoming more and more connected to train-wide, wayside, station and central (i.e., remote from the train) control communications. These connections are usually radio and may be cellular. The signals are coded using industry protocols. The radio communications are easily detected and the information received by anyone with a properly tuned radio. The signals can be disrupted, and the coding can be intercepted, modified and transmitted to the receiver. These are of course intentional malicious actions. Such actions can cause unintended results to occur and/or prevent appropriate safety results from taking place. Thus, they are of critical concern.

The purpose of cybersecurity assessments is to identify threats to rail operations, including the potential types of malicious actors, and the attack vectors they may use. These assessments also evaluate vulnerabilities within rail communications infrastructure stemming from hardware, firmware, and software flaws, misconfigurations, or design weaknesses that could be exploited by malicious actors. Communications may be unencrypted, cross over between the open internet, corporate enterprise networks, personal networks, or other rail operations and may lack sufficient controls to isolate and protect against these vulnerabilities. In some instances, user accounts may still rely on default credentials or weak authentication mechanisms, providing malicious actors with low-effort entry points to rail operation and safety systems.

Generally, cybersecurity should be assessed for each safety subsystem and factor. The level of assessment may vary in granularity. In some cases, it can be determined that a system has limited exposure due to its isolation within the system architecture. In other cases, a more thorough evaluation may be necessary due to interconnections with other networks, or other exposure factors. These determinations should be clearly documented, along with any corresponding actions taken or planned, to ensure traceability and transparency in risk treatment Transportation Cybersecurity Information Sharing Network (T-CISN)

The Transportation Cybersecurity Information Sharing Network (T-CISN) will be formed to support the sharing of cybersecurity resources and knowledge throughout the industry to contribute to our collective defense. The group will be run by a small staff of volunteer leaders from APTA who are familiar with the diverse systems used by agencies to keep vehicles, people and communities moving.

3.6 Physical security of operational technologies

Personnel with high-level access to IT and OT systems may pose multiple risks to the operations and mission of the transit agencies. This is often referred to more broadly as insider risk, where individuals with authorized access intentionally or unintentionally compromise system security, safety, or operations. Insider risk is particularly difficult to manage, as it involves trusted individuals operating within the scope of their legitimate access. Labor rules, access privileges, and challenges in identifying at-risk personnel all contribute to the difficulty of managing this risk. These factors can significantly increase system vulnerability and the potential for exploitation, particularly where personnel have direct physical access. Due to the nature of these threats, the TSA, FTA and FRA are beginning to require that the physical OT nodes, rooms, closets and equipment be protected from unauthorized physical access. Current requirements in this area from regulators remains sparse. That stated, personnel that are responsible for securing OT systems (SCADA, distributed control systems, etc.) can lean on some of the experience and expertise of the North American Electric Reliability Corporation by referring to its Critical Infrastructure Protection (CIP) standards. The NERC CIP standards are an effective security compliance baseline that support thoughtful protection of information and OT systems throughout the North American electrical infrastructure. They can be found at www.nerc.com/pa/Stand/Pages/Default.aspx.

Personnel responsible for the physical protection of OT systems should pay particular attention to the following standards:

1. CIP 005-7, Electronic Security Perimeters
2. CIP 006-6, Physical Security of BES Cyber Systems
3. CIP 014-3, Physical Security

Other beneficial NERC CIP standards relating to cybersecurity include the following:

1. CIP 002-5.1a, Cyber Security — BES Cyber System Categorization
2. CIP 003-8, Cyber Security — Security Management Controls
3. CIP 004-6, Cyber Security — Personnel & Training
4. CIP 007-6, Cyber Security — System Security Management
5. CIP 008-6, Cyber Security — Incident Reporting and Response Planning
6. CIP 009-6, Cyber Security — Recovery Plans for BES Cyber Systems
7. CIP 010-4, Cyber Security — Configuration Change Management and Vulnerability Assessments
8. CIP 011-2, Cyber Security — Information Protection
9. CIP 012-1, Cyber Security — Communications between Control Centers
10. CIP 013-2, Cyber Security — Supply Chain Risk Management

The most recent standards will be listed as subject to enforcement in the One Stop Shop on the NERC website.

4. Additional standards, resources and tools

APTA has identified industry standards, resources and tools for transit agencies to utilize and reference in developing specific information security programs tailored to individual agencies. These references are not exhaustive and are meant only to serve as a guide. Safety professionals interested in learning more about cybersecurity, its impact and its implementation may wish to review the following guidelines and standards.

CISA Cyber Essentials

A guide for leaders of small businesses and small local governments to develop an actionable understanding of where to start implementing organizational cybersecurity practices. https://www.cisa.gov/cyber-essentials

Critical Infrastructure Cyber Community (C3) Voluntary Program

Pointers to resources aligned to the NIST Cybersecurity Framework, including geographically specific resources, hands-on support for critical infrastructure, Cybersecurity Advisors (CSAs), Protective Security Advisors (PSAs), and the Critical Infrastructure Partnership Advisory Council (CIPAC) Framework. https://www.dhs.gov/ccubedvp

National Security Agency (NSA)/Central Security Service (CSS)

Includes cybersecurity advisories, technical guidance, threat intelligence and assessments, cybersecurity education, and cybersecurity products and services. https://www.nsa.gov/about/central-security-service/

National Initiative for Cybersecurity Education (NICE)

The National Initiative for Cybersecurity Education (NICE) has evolved from the Comprehensive National Cybersecurity Initiative and extends its scope beyond the federal workplace to include civilians and students in kindergarten through postgraduate school. The goal of NICE is to establish an operational, sustainable and continually improving cybersecurity education program encouraging sound cybersecurity practices that will enhance the nation's security. https://www.nist.gov/itl/applied-cybersecurity/nice

NICE will be represented by four components:

1. **Component 1:** National Cybersecurity Awareness. Lead: DHS
2. **Component 2:** Formal Cybersecurity Education. Co-leads: Department of Education (DOE) and National Science Foundation (NSF)
3. **Component 3:** Cybersecurity Workforce Structure. Lead: DHS, supported by the Office of Personnel Management (OPM)
4. **Component 4:** Cybersecurity Workforce Training and Professional Development. Tri-Leads: Department of Defense (DOD), Office of the Director of National Intelligence (ODNI), DHS.

Definitions

automatic train protection (ATP): A wayside and/or onboard train system to apply emergency brakes if a signal is missed by the train operator.

automatic train supervision (ATS): Provides advanced functionalities of train control, typically including advanced automatic routing and automatic train regulation.

certifiable elements: Project elements that can affect the safety of transportation agency passengers, employees, contractors, public safety personnel, or the general public (e.g., stations).

certifiable Elements List (CEL): A list of certifiable elements.

certifiable items: Individual items/components that make up the certifiable elements. Each item of a certifiable element must be verified before the element as a whole can be verified.

certifiable Items List (CIL): A list of certifiable items.

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.

communications-based train control (CBTC): A continuous, automatic train control system that relies on wayside data communications and/or GPS for position sensing and uses the "moving block" principle for safe train separation rather than fixed blocks with track circuits.

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.

fail-safe: Describes a device that fails in a manner that protects the safety of personnel and equipment.

interlocking: An arrangement of railway signals and signal appliances so interconnected that their movements must succeed one another in proper sequence.

malware: Short for malicious software. Such software is created and used by people, usually with bad intentions, to disrupt computer operations or obtain, without consent, confidential information.

NIST SP 800-53: NIST Special Publication 800-53, titled "Recommended Security Controls for Federal Information Systems and Organizations." Rev. 5, dated January 2020, was used in preparing this document.

NIST SP 800-82: NIST Special Publication 800-82, titled "Guide to Industrial Control Systems (ICS) Security." The May 2015 final version was used in preparing this document.

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.

programmable logic controller (PLC): An industrial computer used for automation of mechanical processes.

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, and 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.

track circuit: An electrical circuit designed to indicate the presence or absence of a train in a specific section of track.

traction power: A network supplying power to electrically powered railways.

trusted (network): Network of an organization that is within the organization's ability to control or manage. Further, it is known that the network's integrity is intact and that no intruder is present.

vector (for cyberattack): The path an attacker takes to attack a network.

vital: A term applied within rail safety to denote fail-safe operation. (Derived from IEEE Standard 1483, 2000 glossary, "vital function: A function in a safety-critical system that is required to be implemented in a fail-safe manner.")

vital programmable logic controller (vital PLC): A PLC with fail-safe functions intended for safety-critical signaling and interlocking applications in rail transit.

vital signaling: The portion of a railway signaling network that contains vital equipment.

Abbreviations and acronyms

ALARP as low as reasonably practicable
CBTC communications-based train control
CCE Consequence-Driven Cyber-Informed Engineering
CE certifiable element
CEL Certifiable Elements and Sub-Elements List
CIE Cyber Informed Engineering
CIL Certifiable Items List
CIP Critical Infrastructure Protection
CIPAC Critical Infrastructure Partnership Advisory Council
CISA Cybersecurity and Infrastructure Security Agency
CSA Cyber Security Advisor
CSIRP Cybersecurity Incident Response Plan
CSS Central Security Service
CTC Centralized Traffic Control
CVA cybersecurity vulnerability assessment
DHS Department of Homeland Security
DOT Department of Transportation

FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INFOSEC	Information Security
IT	information technology
ISO	International Organization for Standardization
NICE	The National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OHA	Operational Hazard Analysis
OPM	Office of Personnel Management
OT	operational technologies
PTC	positive train control
RACI	responsible, accountable, consulted, informed
RTVL	real-time vehicle location
SCADA	supervisory control and data acquisition systems
SD	security directive
SSC	Safety and Security Certification
SSI	sensitive security information
SSMP	Safety and Security Management Plan
T-CISN	Transportation Cybersecurity Information Sharing Network
TSA	Transportation Security Administration
TVA	Threat and Vulnerability Assessment

Document history

Document Version	Working Group Vote	Public Comment/ Technical Oversight	CEO Approval	Policy & Planning Approval	Publish Date
First published	May 30, 2025	July 31, 2025	Oct. 26, 2025	Nov. 28, 2025	Mar. 23, 2026

