Pennsylvania Turnpike Commission ITS Security Assessment

New England Intelligent Transportation Society 2025 Annual Interchange

Presented by

DRIVE ENGINEERING

Agenda

- Project Team
- PA Turnpike Cybersecurity
- Why Cybersecurity Matters
- Overview
- Asset Classification
- Risk Assessment of ITS Devices
- Risk Assessment of ITS Applications/ Systems (Penetration Test)

Project Team

PA Turnpike

- Cybersecurity is a top concern throughout the organization
- Agency Best Practices
  - Comprehensive Asset Management/ITS Inventory
  - Quarterly Patching
  - Claroty Tool
  - Extensive Maintenance Program
    - Quarterly Preventive Maintenance
  - ITS Design Checklist
- Recurrent Cybersecurity Assessments
- No Security Breaches!

Why Cybersecurity Matters

- Critical Infrastructure: Transportation systems are high-value national targets.
- Cyber-Physical Risk: Attacks can disrupt real-world safety and mobility.
- Growing Exposure: IoT, Connected Vehicles, and ITS increase vulnerabilities.
- Compliance & Trust: Agencies must protect data and maintain public confidence.

Consequences and Benefits

- **Potential Consequences of Weak Cybersecurity**
  - ITS devices manipulation → accidents and congestion
  - Ransomware → shutdown of tolling, transit, freight systems, etc.
  - Data breaches → exposure of sensitive traveler/agency info
  - Operational delays → costly disruptions to supply chains
- **Benefits of Strong Cybersecurity Programs**
  - Protects public safety and ensures system reliability
  - Supports resilience and continuity of operations
  - Builds public confidence in digital transportation
  - Reduces recovery costs and liability exposure

Overview: PTC ITS Infrastructure

Device Type	Total Devices	Notes
Roadway CCTV	92	
Security Cameras	774	Cameras installed in PTC facilities
Changeable Message Signs (CMS)	217	
Roadway Weather Information Station (RWIS)	24	
Perle Devices	55	Temperature sensors integrated with fire alarm monitoring
RTMS Traffic Monitoring Devices	12	Traffic detectors at non-tolled interchanges

Overview

- The objective of this engagement is to conduct a thorough assessment of ITS devices and applications to identify vulnerabilities and threats so that security risks can be mitigated.

- The assessment criteria adhered to the Open-Source Foundation for Application Security (OWASP) Internet of Things (IoT) assessment guidelines – OWASP ISTG.

Overview

- 4 essential tasks:
  1. Asset Classification
  2. Selection criteria for asset assessment and ITS device assessment checklist
  3. Risk Assessment of ITS Devices
  4. Risk Assessment of ITS Applications / Systems (Penetration Test)

Asset Classification

- PTC tracks ITS assets and their individual attributes using Excel spreadsheets and ServiceNow
- PTC Transportation Technologies group uses and maintains the Excel spreadsheets
- Transcore, PTC's ITS maintenance contractor, uses and maintains the ServiceNow inventory
- Observations:
  - Unify Systems: Merge Excel spreadsheets and ServiceNow into one golden asset inventory
  - Data Quality: Standardize fields, enforce data entry rules, and create a data dictionary; minimize open text fields

Asset Classification

- Observations:
  - Governance: Establish version control, regular audits, and QA/QC reviews to ensure accuracy and completeness.
  - Security & Access: Protect sensitive data (IP addresses, serial numbers) via restricted storage or passwords.
  - System Enhancements:
    - Excel: Use tables, track firmware updates, standardize device data, and add utility/firmware fields.
    - ServiceNow: Improve location standardization, consolidate assets (e.g., CMS LED modules), leverage lifecycle tracking, and separate field vs. building IT equipment.
  - Coverage Gaps: Add missing devices (Perle, RTMS) and ensure consistent asset tagging

Asset Classification

ITS Asset Type	Criticality	Inherent Risk Profile
Roadway and Security Cameras	High	High
DMS	High	High
RWIS	Medium	Medium
Perle Devices	High	High
RTMS	Low	Medium

- Potential Threats
  - Unauthorized Access
  - Malware
  - Denial of Service Attacks
  - Physical Tampering
  - Supply Chain Vulnerabilities - Hardware and Firmware

Risk Assessment of ITS Devices

- Developed a checklist to evaluate 105 devices in the field
- Checklist covered:
  - Physical interfaces
  - Cabinet enclosures
  - Internal components
  - Deployment environment
  - Environmental factors
  - Power supply
- Device-specific observations for improvement
- Six common observations for improvement

Risk Assessment of ITS Devices

- Enhanced Locking Mechanism for Technology Cabinets
- Installation of Pressure Switches for Cabinet Door Monitoring
  - Sensors can be configured to log each instance a door is opened
- Implementation of Comprehensive Temperature Control Systems for Cabinets
  - A standardized, comprehensive temperature control system will protect internal components

Risk Assessment of ITS Devices

- Regular Inspection and Maintenance for Rust and Weather Seal Integrity
- Secure Locking Mechanisms for CMS Ladders
- Install Smart Temperature Sensors with Alert Capabilities
  - Smart sensors can monitor cabinet temperatures and send real-time alerts

Penetration Test

- Test scope:
  - ATMS
  - Genetec
  - TrafficVision
  - VBrick
  - Orion
  - Vanguard
- User-Level access granted for most applications
- Attempted to gain access to other accounts / admins
  - Goal: obtain sensitive data and/or control of servers
- Attempted entry into applications without access

Critical	High	Medium	Low	Informational
0	1	102	150	147

Questions

Mario Toscano, PE, PTOE, CVP
Drive Engineering
mario@driveengineering.com
484.288.2630