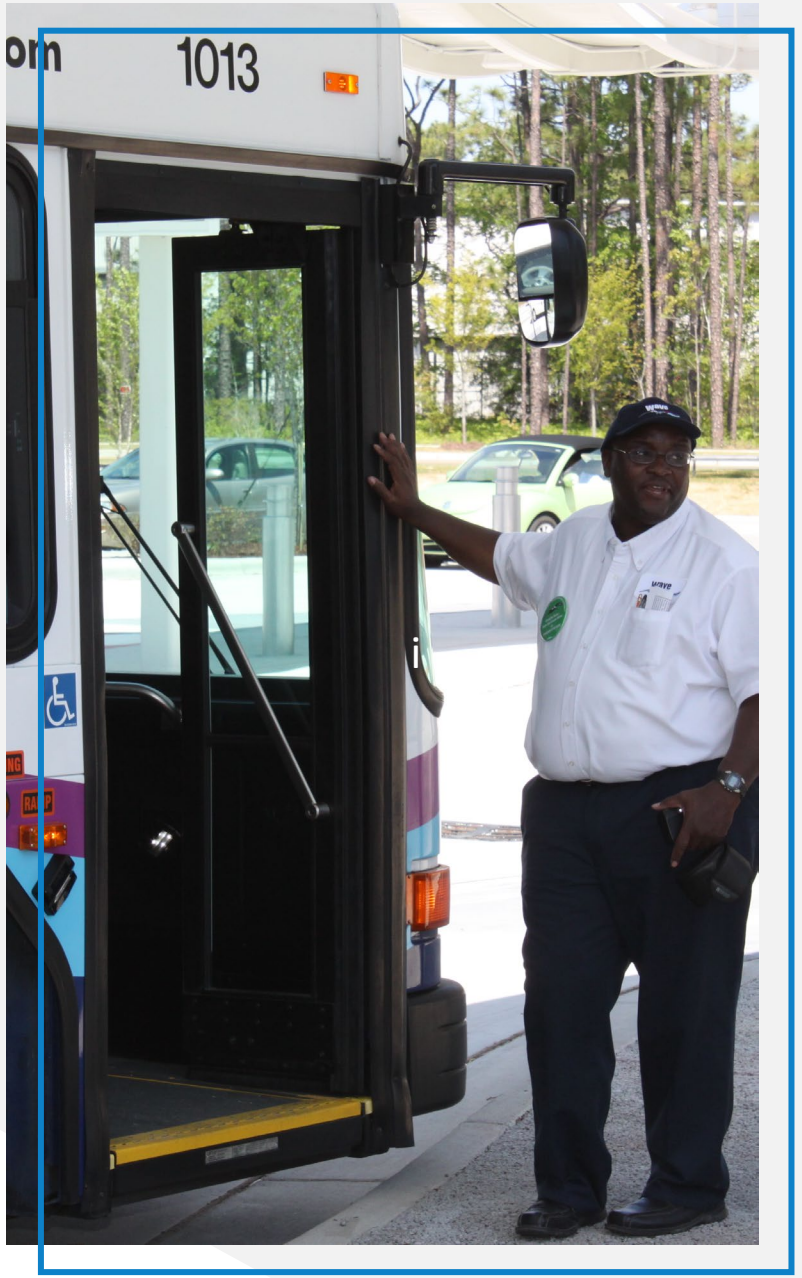
Cybersecurity Awareness for Transit Agencies Webinar



Federal Transit Administration

Office of Transit Safety and Oversight

U.S. Department of Transportation
Federal Transit Administration

Agenda

1. Cybersecurity Resources
2. Transit Agency Speakers
   - Thomas Littleton, PhD (OST)
   - Tim Coogan (RTD Denver)
   - Dr. Julius Smith (DART)
   - Tariq Habib (MTA)
3. Q&A
4. Closing

Cybersecurity Resources for Transit Agencies – FTA Website

Cybersecurity Resources for Transit Agencies

https://bit.ly/3AQQWqe

Cybersecurity Assessment Tool for Transit (CATT)

FTA published an open-source CATT tool on February 10, 2023, which assists small and mid-sized transit agencies in self-assessing their cybersecurity preparedness

CATT has three primary components:

- Data collection form
- Resulting report produced given data input from transit agency
- Resource guide on how to begin practices

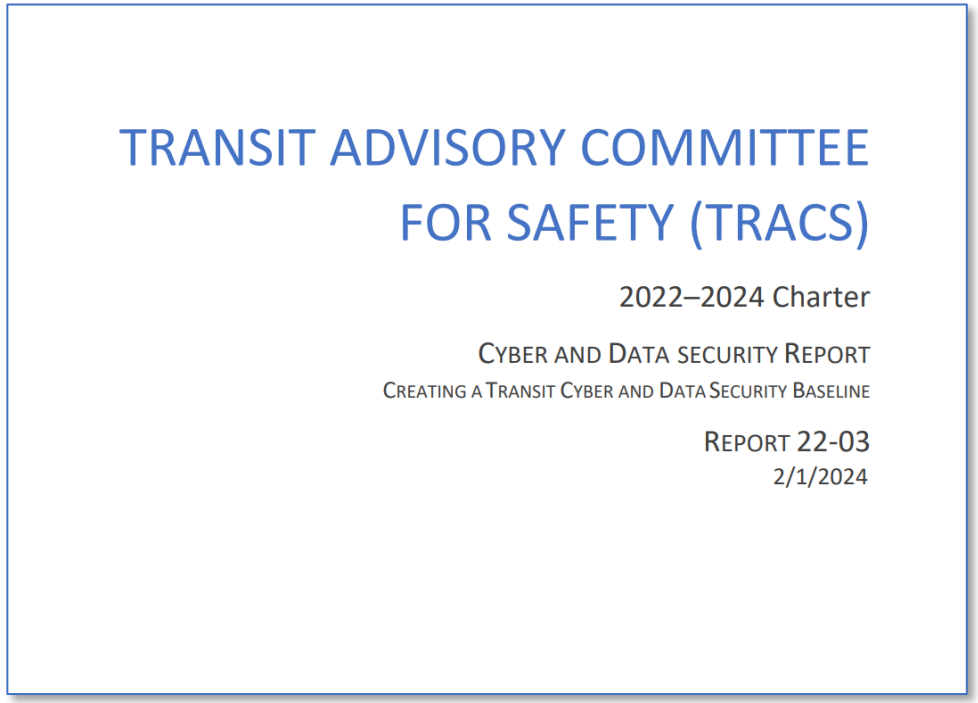
CATT provides an on-ramp for agencies to identify key practices of a modern cybersecurity program with a self-assessment that uses Department of Homeland Security's Cyber Resilience Review as a basis and aligns with National Institute of Standards and Technology framework

Cybersecurity Resources for Transit Agencies

Transit Advisory Committee for Safety (TRACS) Cyber and Data Security Recommendations

- In February 2024, the TRACS Cyber and Data Security sub-committee released a Cyber and Data Security Report to aid FTA and USDOT leadership in improving cyber and data security.

- The report details seven recommendations, including implementation suggestions, to improve the cybersecurity hygiene for transit agencies.



Thomas Littleton, PhD

Associate Chief Information Officer for Sector Cyber Coordination, Office of the Secretary

U.S. Department of Transportation
Federal Transit Administration

Cybersecurity Best Practices for Transit Agencies

Tim Coogan – Chief Information Security Officer

Timothy Coogan
Colorado’s Regional Transportation District

Backed by a 24-year career in technology and cybersecurity, Tim has been the head of cybersecurity for multiple public sector transportation agencies including Denver International Airport and currently Colorado's Regional Transportation District.

Tim’s experience with the intersection between technology and public transportation systems gives him a unique perspective on protecting our nation’s critical infrastructure and transportation systems.

Cybersecurity Best Practices Strategy and Direction

- **Risk Management to the Rescue!**
  Modern enterprises face highly sophisticated cyber threats in environments where technology is pervasive and supporting every business process. Risk Management is a time-proven and effective practice for prioritizing limited resources to align an organization's technology risk with its enterprise risk tolerance.

- **Metrics That Matter**
  By defining and measuring enterprise aligned and leading key risk indicators, you can discover and treat small issues before they become large ones.

- **Hope for the Best, Prepare for the Worst**
  As cyber-attacks affecting both information technology (IT) and operational technology (OT) environments continue to increase, being prepared to respond and recover will minimize impact when an organization becomes a victim. Manage and prioritize your technical service inventory, and create partnerships with legal, emergency management, and public relations.

Cybersecurity Best Practices
Emerging Threats

- **Phishing, The Artificial Intelligence (AI) Battleground**
  Attackers are using AI to create and automate phishing attacks. Don't bring a butter knife to a gun fight - use AI to stop the bad guys in their tracks! (and other useful ways to use AI).

- **Multi-Factor Authentication Must Be Upgraded**
  Basic multifactor authentication is used to safeguard against credential theft and other identity attacks, but now the thieves are stealing MFA tokens too. MFA must be upgraded to phishing resistant methods.

- **Recent Shifts in Ransomware Dwell Time Requires a 24 x 7 Response**
  The amount of time between initial access and ransomware execution has recently decreased by an order of magnitude from weeks or months to hours or days. This shift requires ransomware detection and response around-the-clock.

Thank you.

rtd-denver.com

National Cyber Security Awareness Month

Federal Transit Administration
October 29, 2024

Dr. Julius Smith
VP & Chief Information Officer

Security is everyone's responsibility

DART let's go.

Julius Smith

VP & CIO, DART

Dr. Julius Smith is the Vice President and Chief Information Officer for the Dallas Area Rapid Transit (DART). In this role, he oversees DART's technology systems' leadership and strategic direction.

He identifies opportunities to support the Agency's expansive transit network through the applications of innovation, cybersecurity, digital technology, data science and governance, and enhancing the employee and customer experience.

He has served as Chief Information Security Officer in his career. Before joining DART, he held leadership roles in the Department of Defense.

Introduction

- Protecting Assets
- Training
- Responding to Incidents

Security is everyone's responsibility

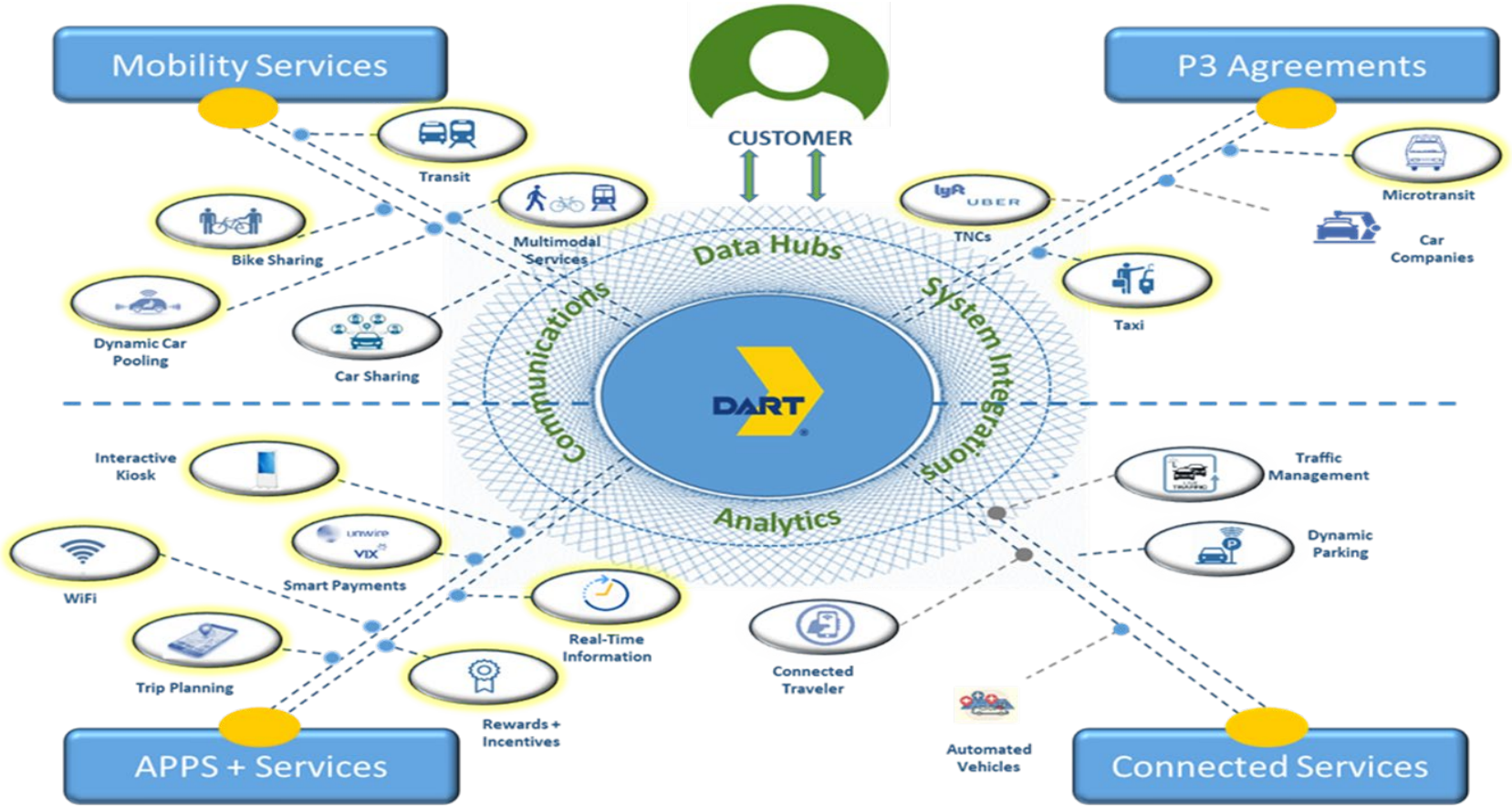
Mass Transit Sector Cybersecurity

"Cybersecurity Threats to the Transit Industry"

- As transit systems increase dependence on digital technology, the risk of cyberattacks increases
- Malware is the most common type of cyberattack
- Criminals are leveraging innovation and moving at a pace security vendors cannot possibly match

DART let's go.

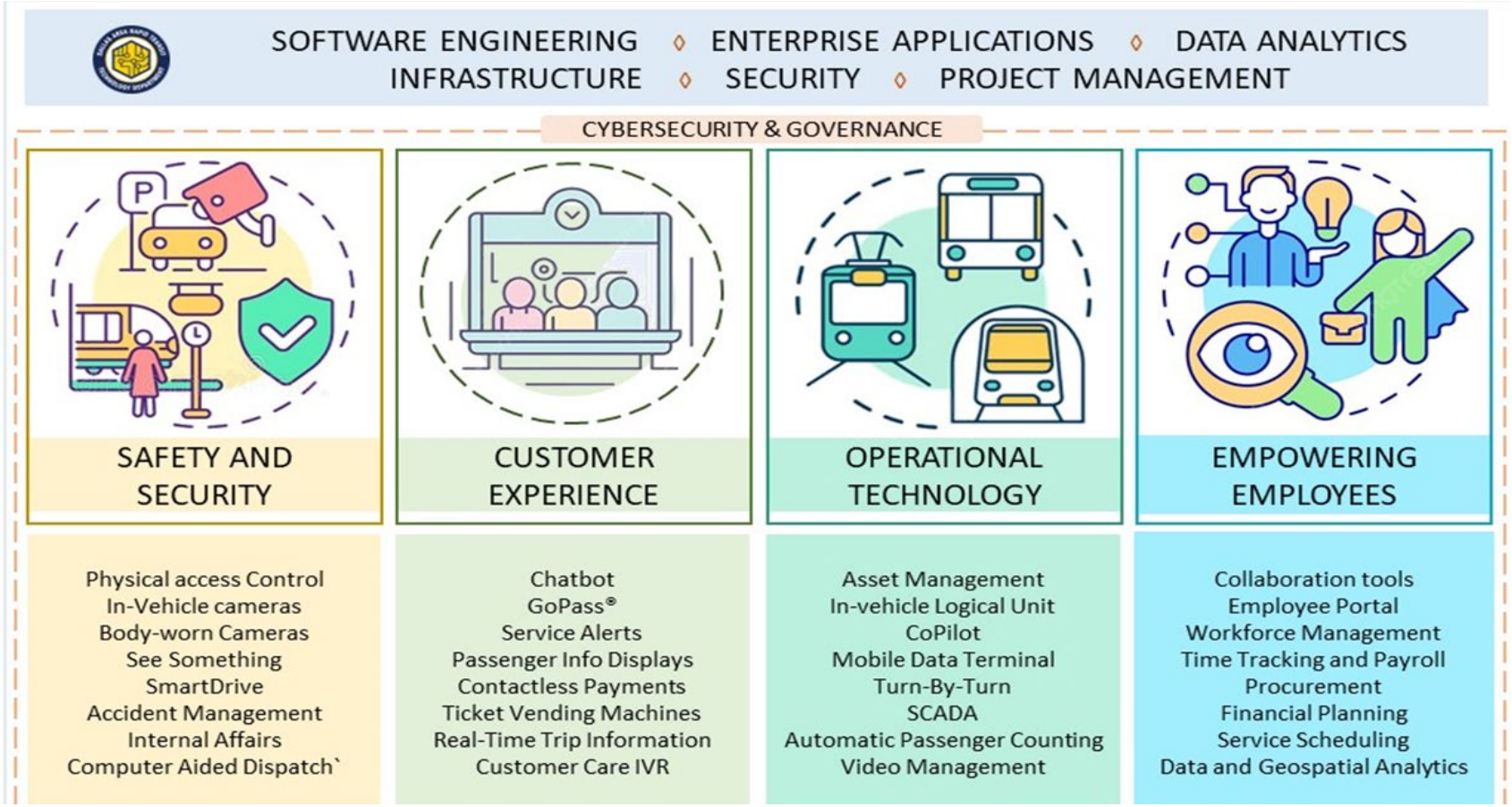
Cybersecurity Complexities



DART let's go.

Security is everyone's responsibility

Cybersecurity, People, Processes, and Technology



DART let's go.

Security is everyone's responsibility

Cybersecurity Training is Crucial for Organizations and Individuals

- Protection Against Cyber Threats
- Safeguarding Sensitive Data
- Compliance with Regulations
- Mitigating Human Error
- Building a Security-First Culture
- Reducing Financial Losses
- Enhancing Incident Response
- Protecting Brand Reputation

DART let's go.

Security is everyone's responsibility

Cybersecurity Awareness Training Enhancements

Baseline Testing to assess the Phish-prone percentage of users through a simulated phishing attack.

Train Users with interactive modules, videos, games, posters and newsletters.

Phish Users with fully automated simulated phishing attacks.

See the Results

Phish Alert Button

Social Engineering Indicators

AI-Driven Phishing and Training Recommendations

DART let's go.

Security is everyone's responsibility

Cyber Security Training and Traveling

INCREASED EXPOSURE TO UNSECURED NETWORKS

PHYSICAL SECURITY OF DEVICES

AWARENESS OF SOCIAL ENGINEERING ATTACKS

SECURING DATA TRANSFERS

REMOTE ACCESS MANAGEMENT

COMPLIANCE AND DATA PROTECTION

INCIDENT RESPONSE AWARENESS WHILE TRAVELING

REDUCING THE RISK OF CONNECTING WITH UNVERIFIED DEVICES

Security is everyone's responsibility

DART let's go.

Incident Response

Recognize and Report
- Recognize and Report the Incident

Contain
- Contain the Incident

Notify
- Notify Key Stakeholders

Assist
- Assist with Incident Investigation

Follow
- Follow Technology/Security Team Instructions

Verify
- Verify Systems Are Secure

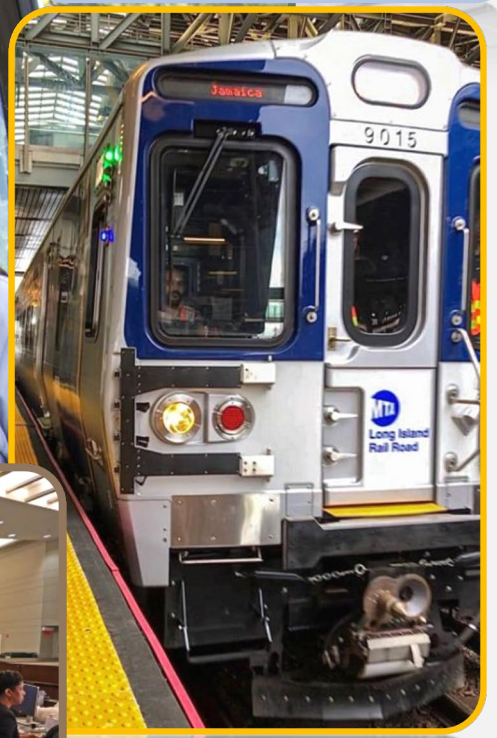
Participate
- Participate in Post-Incident Review

Refresh
- Refresh Training and Awareness

DART let's go.

Thank You

Dr. Julius Smith
APTA Chair, Enterprise Cyber Security Working Group (ECSWG)
Vice President & Chief Information Officer
Office of the CIO - Technology
Dallas Area Rapid Transit (DART) |1401 Pacific Avenue | Dallas, TX 75202
Office: 214-749-3093 | Email: JKSmith@dart.org



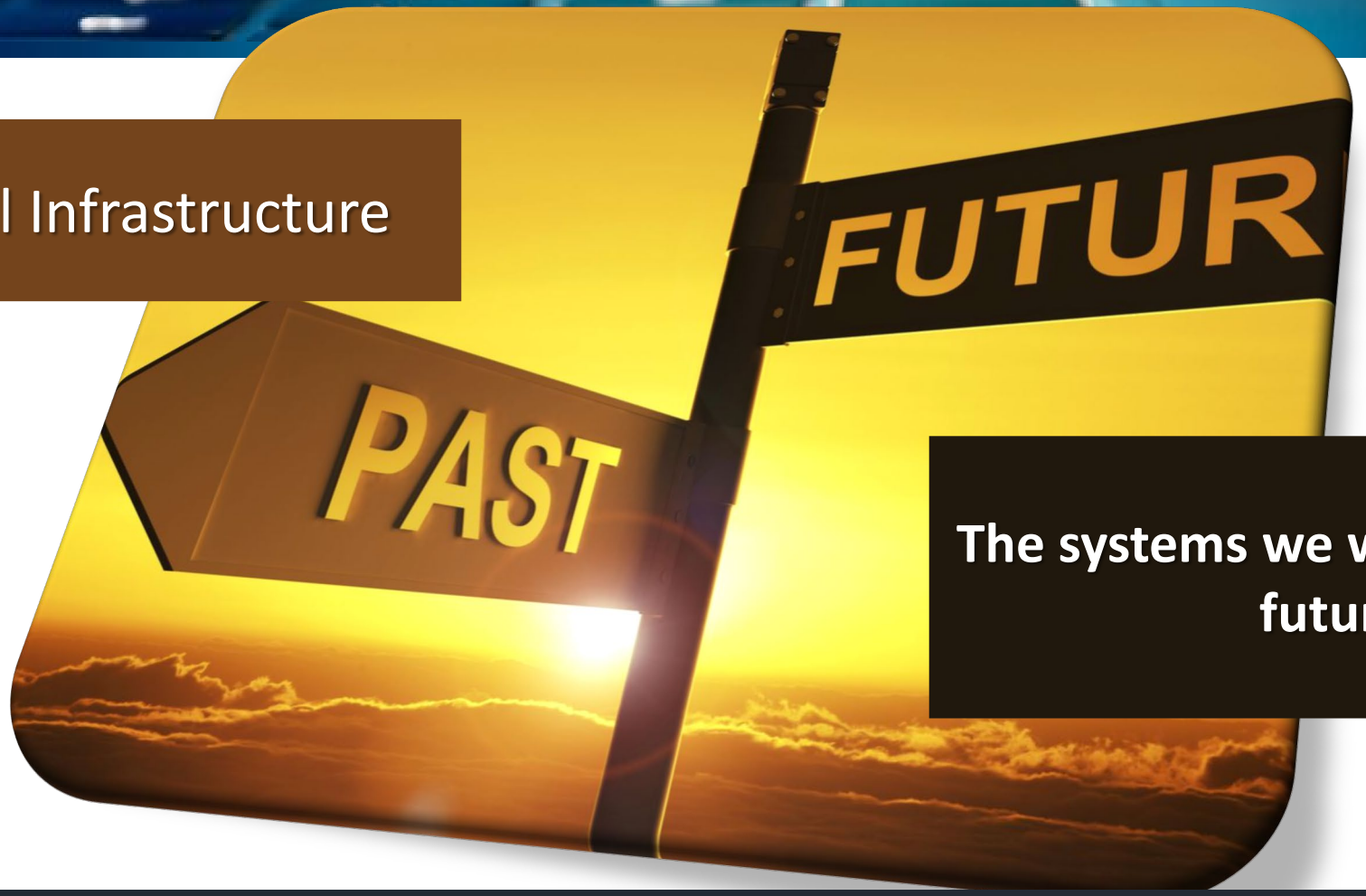
Cybersecurity

Tariq Habib

Tariq.Habib@MTAHQ.ORG

What is the Priority?

Legacy Rail Infrastructure



The systems we will have in the future

What should we be mostly concerned about?

Operational Technologies (OT) Security

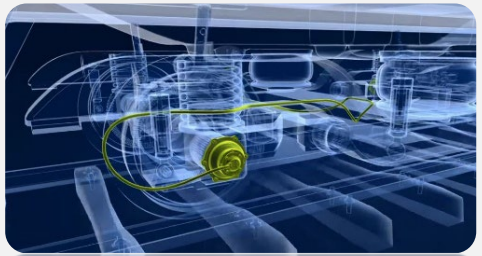
Stations

Command Center

Trains

Signals

Lift Span



Traction

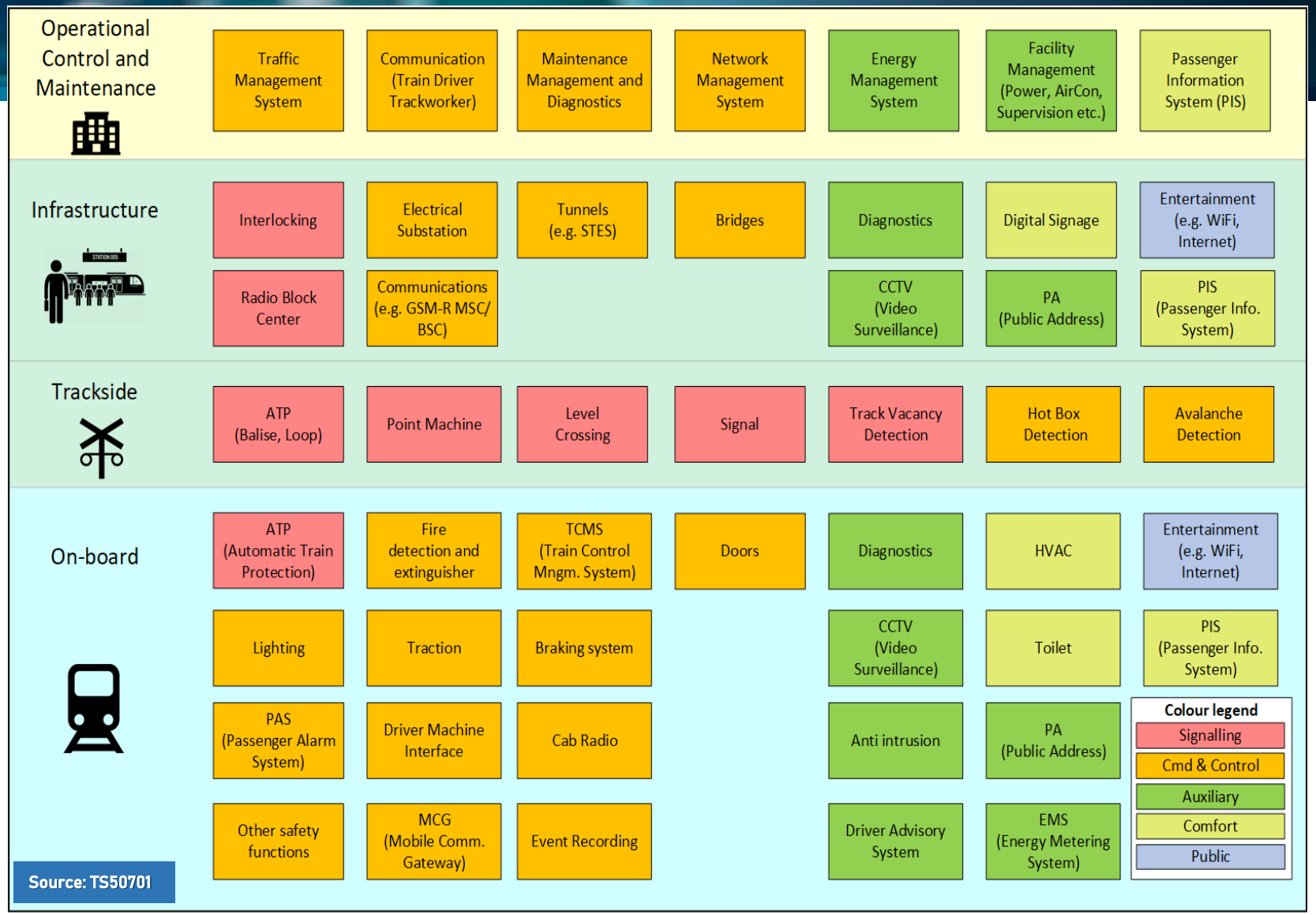
Buses

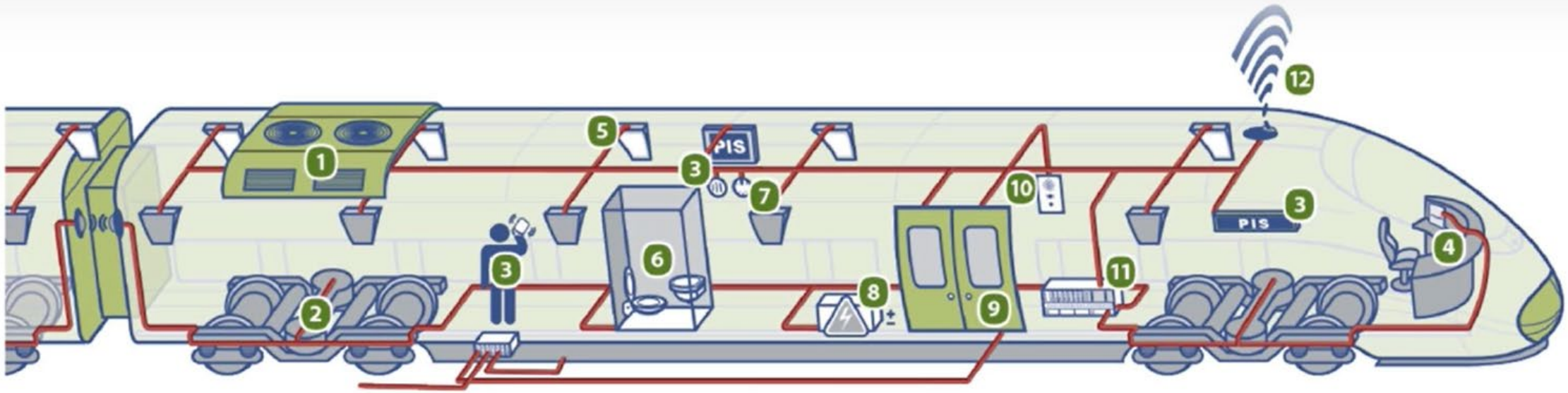
Substations

Securing Rail Assets is a Complex Challenge

→ Over 40 technologies and systems are required to run a rail operation

→ Failure in one area can cause service disruptions and safety challenges





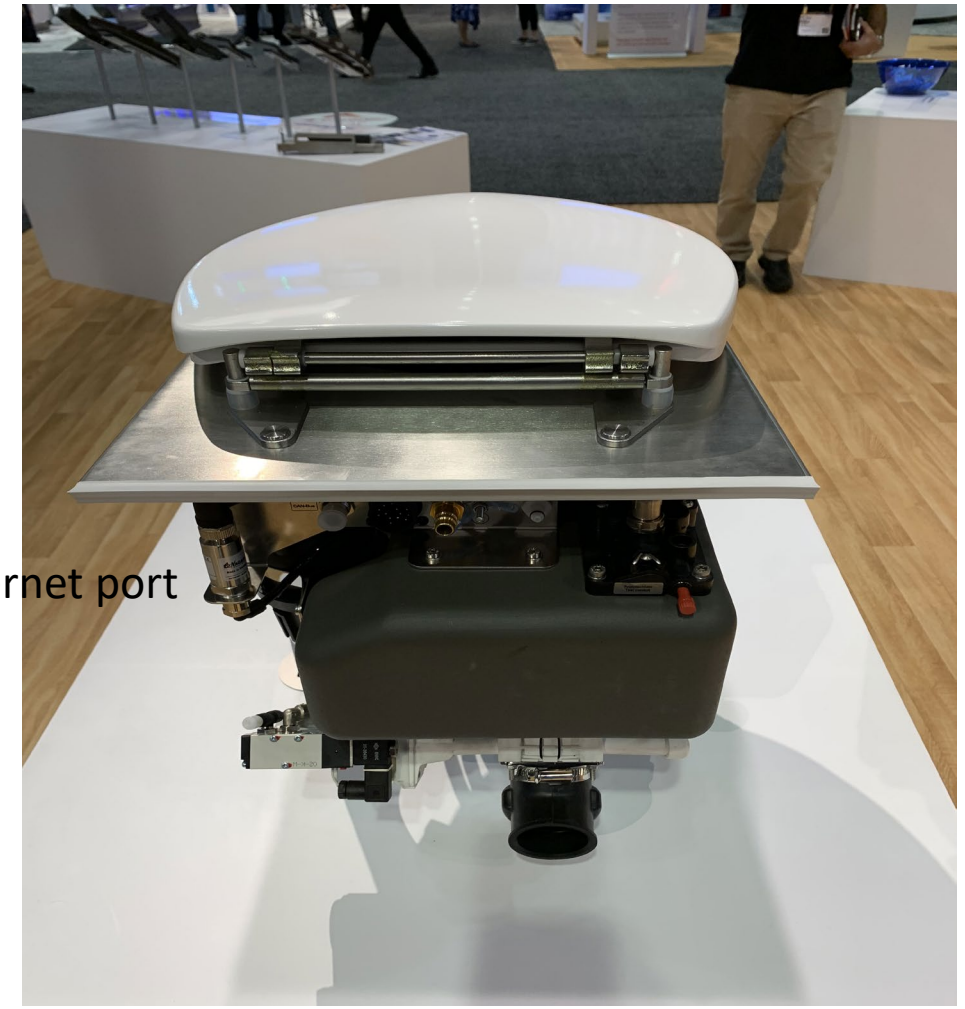
TCMS, FOR THE MONITORING, CONTROL AND AUTOMATION OF:

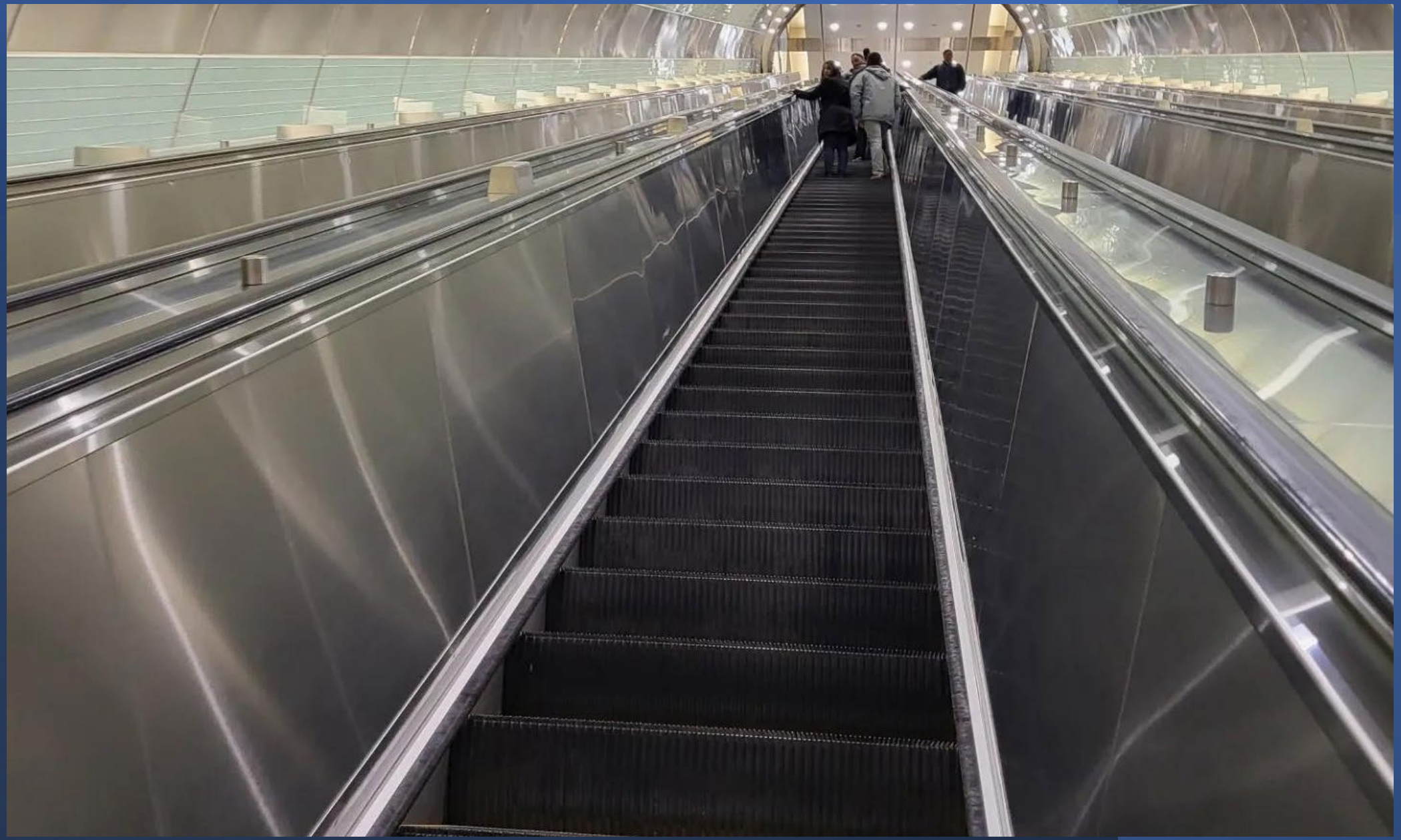
1. HVAC
2. Bearing temperature
2. Speed measurement
2. Lateral vibration
2. Brakes
2. Traction
3. PIS
4. Driver Controls
5. Lights
6. Water tanks
7. Surveillance Cameras
8. Batteries
9. Doors
10. Emergency communications
11. Vehicle Control Unit
12. Train-To-Wayside communications

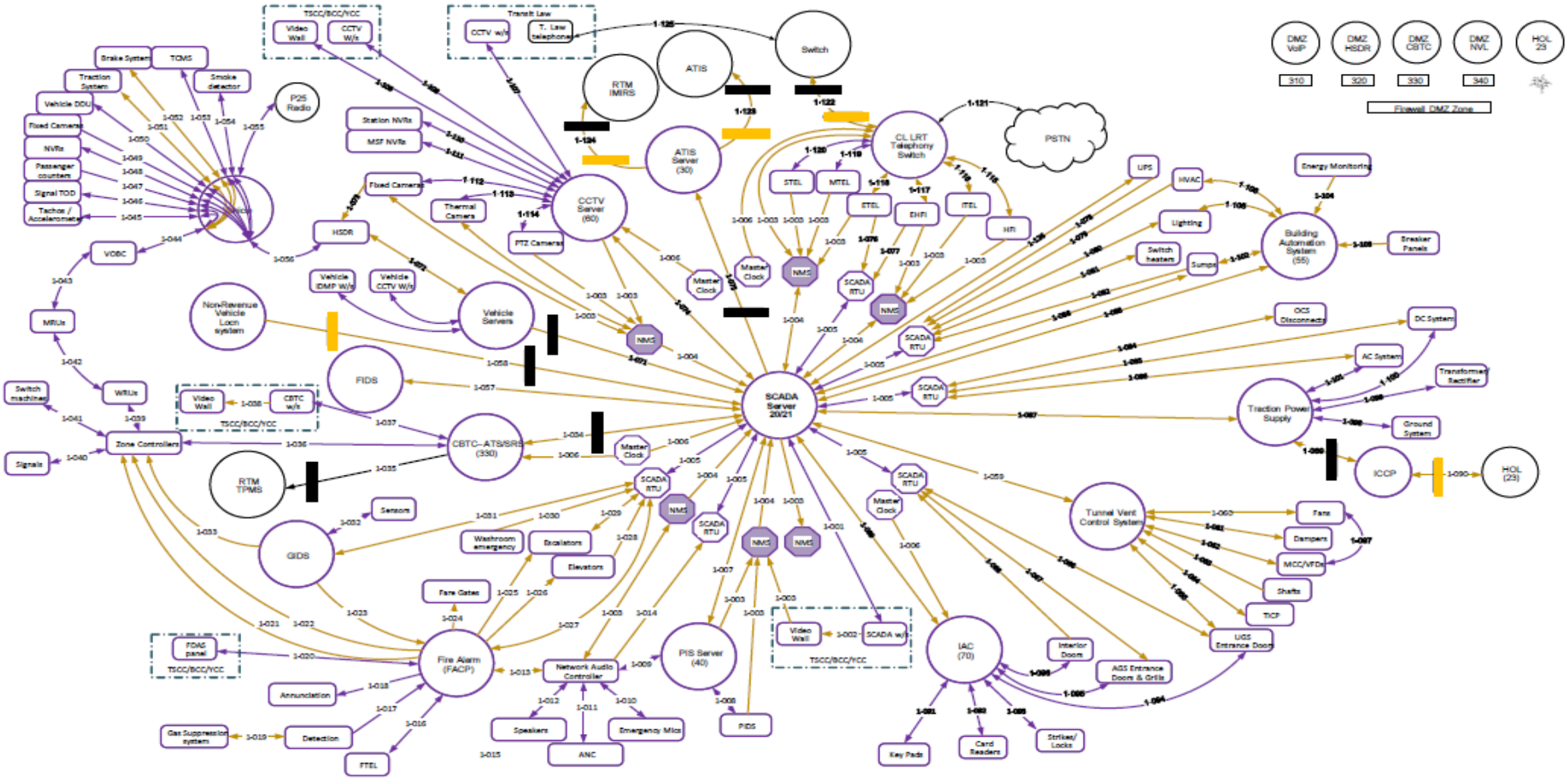
Train cars have many onboard systems – IoT

Toilet Vacuum System – Ethernet Connected TCM

Ethernet port







Interconnected, problem in one area can lead to impacting the entire system

Legacy technical debt over the decades

Generalized

Legacy System

Default Configuration

Less/No Updates (patches)

Less/No Encryption

No Governance (Policies & Procedures)

Less/No Segmentation

Latency Concerns

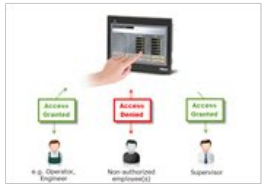
Removable Media

Remote Access

Software & Equipment Vulnerabilities

Email Phishing and attachments

Guest Networks Unprotected Sockets



Lack of Access Controls

3rd Parties (Contractors)

A product or system must enhance security & integrate with the current cyber ecosystem

Most rail systems are operated by engineering and operations teams

- **Their primary focus is safety, reliability, and on-time**
- **Have plans for every situation except for Cyber**
  - **Cyber is an invisible threat to rail/bus operation – no experience or encounter**

Engineers and operators do not fully understand IT – different operating models

- **Imagine if CrowdStrike was present in Rail Operations**

Cyber teams are not fully embedded into the operations

- **They are trying to get attention**
- **Directives are not yet enforced**

Product suppliers and integrators have not demonstrated that they understand what needs to be in place before the system is handed over to the Operations and Engineering team

What every rail operation must have in place?
Is this sufficient to defend against advanced attacks?

Doable

- ✓ **Control remote access – We know who is connecting from outside**
- ✓ **Isolation from the Internet - Make it difficult to attack Operations from anywhere**
- ✓ **Strengthening corporate security – Advanced defensive capabilities are in place**
- ✓ **Establish visibility – Ability to detect incidents in parts of operational areas**
- ✓ **Improve monitoring processes – Train cyber staff to know crown jewels, have use cases**
- ✓ **Segmentation – To limit the impact of attack, segment critical systems**
- ✓ **Incident Response and Recovery – Response and recovery are documents**
- ✓ **Procurement controls to ensure cyber requirements are part of all contracts**
- ✓ **Defined vulnerability and patch management process**
- ✓ **Account management – AAA wherever you can****
- ✓ **Improve physical security of cyber assets**

Regulators want security controls that are costly to incorporate in legacy systems

Unfunded mandates	
1	Multi-step authentication - MFA
2	Privileged access – Manage access for people who can impact the service
3	Strong access and authentication – Enable similar practices in Operations
4	Password controls – Hard to require passwords in Operations
5	Full visibility – Know all your assets and ability to detect cyber attacks
6	Recovery – Have a business recovery plan
7	Hardening and vulnerability management – Build security controls on top of legacy infrastructure

Prioritize your crown jewels

Top Priority Areas

- Signaling systems
- Network Communication
- Power
- Command Centers
- CBTC Systems
- Public Information Systems
- Revenue Collection

Cybersecurity Program

- Improve organizational readiness to cybersecurity threats and incidents - critical systems incident response plans
- Access controls, system hardening
- Asset information, detection of cyber incidents
- Expand and improve on the Cybersecurity awareness and training program
- Patch management process to secure systems – in progress

- Reduce the risk originating from partners and contractors that can impact operations and processes
- Improve application and cloud security practices
- Enable operational technology teams to assist in cyber improvement – provide resources, infrastructure, and support
- Engage with your Procurement, Capital Program Management teams

Everyone agrees cybersecurity is important, but the priorities differ

We must continuously work to bring all the stakeholders together

Cybersecurity will work when stakeholders are aligned

Supply Chain & Operators

Suppliers

- Product Security
- Project Delivery
- Sales
- Security SME?
- Legal

Integrators

- Project Delivery
- Sales
- Technical
- Legal
- Security SME?

Agencies

- Planning, Design
- Procurement
- Legal
- IT
- Cyber
- Project Delivery
- Operations & Maintenance

Government and Industry Organizations

National – US

- TSA
- FRA
- FTA
- CISA
- FBI

Whitehouse

- Cyber directorate
- National Security Office

Industry

- APTA
- UITP
- Consortium
- ISA/IEC
  - 62443
  - 21434 / R155

Align everyone to make our world defensible

Questions

Jeremy Furrer

jeremy.furrer@dot.gov

FTASystemSafety@dot.gov

U.S. Department of Transportation
Federal Transit Administration