



Virtual Vehicle & Partners

Brussels, 28 September 2026

Session 3: Artificial Intelligence & Cyber Security for Smarter Metro Operations



Co-funded by
the European Union



Co-funded by the European Union. Views and opinion expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Europe's Rail Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them. The project 'NEXUS' is supported by the Europe's Rail Joint Undertaking and its members. UK participants in this project are funded by the UKRI.

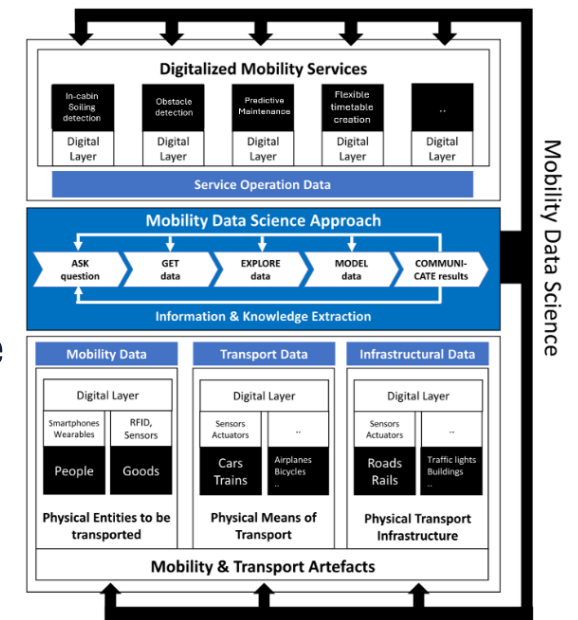


Overview

Artificial Intelligence & Cyber Security for Smarter Metro Operations

Our ambitious goals to improve Metro Operations with the help of AI

- ❖ Review IoT, Big Data, and **AI applications in future metro operations**
- ❖ Identify **use cases for AI to optimize metro operations** using data science and machine learning
- ❖ **Develop, validate and exploit AI models** and applications for future metro operations contributing to a **responsive and financially optimized system**
- ❖ Establish a proactive and comprehensive **cybersecurity framework**



We achieved valuable results in the NEXUS project documented in several Deliverables

- ❖ Passenger Demand Forecasting During Network Expansion
- ❖ Prediction of Crowding Based On Exogenous Data Sources
- ❖ Timetable Creation Using GTFS Feeds
- ❖ Anomaly Detection in the Vehicle Interior
- ❖ Potential of AI to Reduce Energy Consumption and CO₂ Emissions
- ❖ Cybersecurity Threat Identification and Management Framework





02 ————— Passenger Demand Forecasting During Network Expansion

Objectives – to validate the *Log-Linear Econometric Metro Demand Forecasting Model* developed for West Midlands for long term strategic planning:

- structural robustness;
- predictive performance; and
- practical applicability in a different context

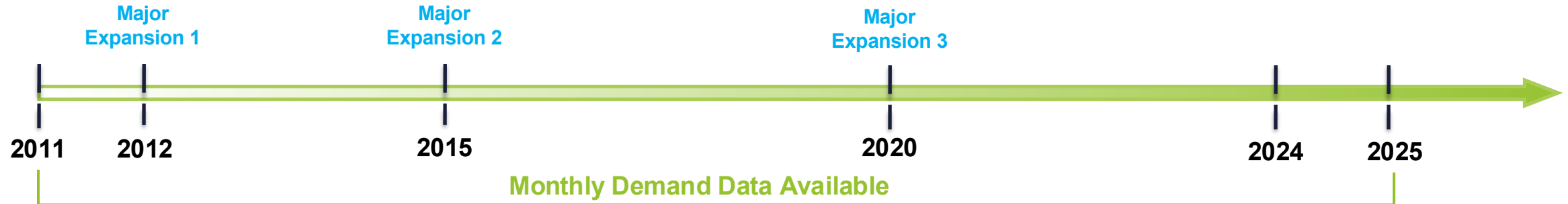
Case study: Metro Sofia, Bulgaria

Period: Feb 2011 to Dec 2024

Focus: network expansion, elasticity, transferability



Context: MetroS

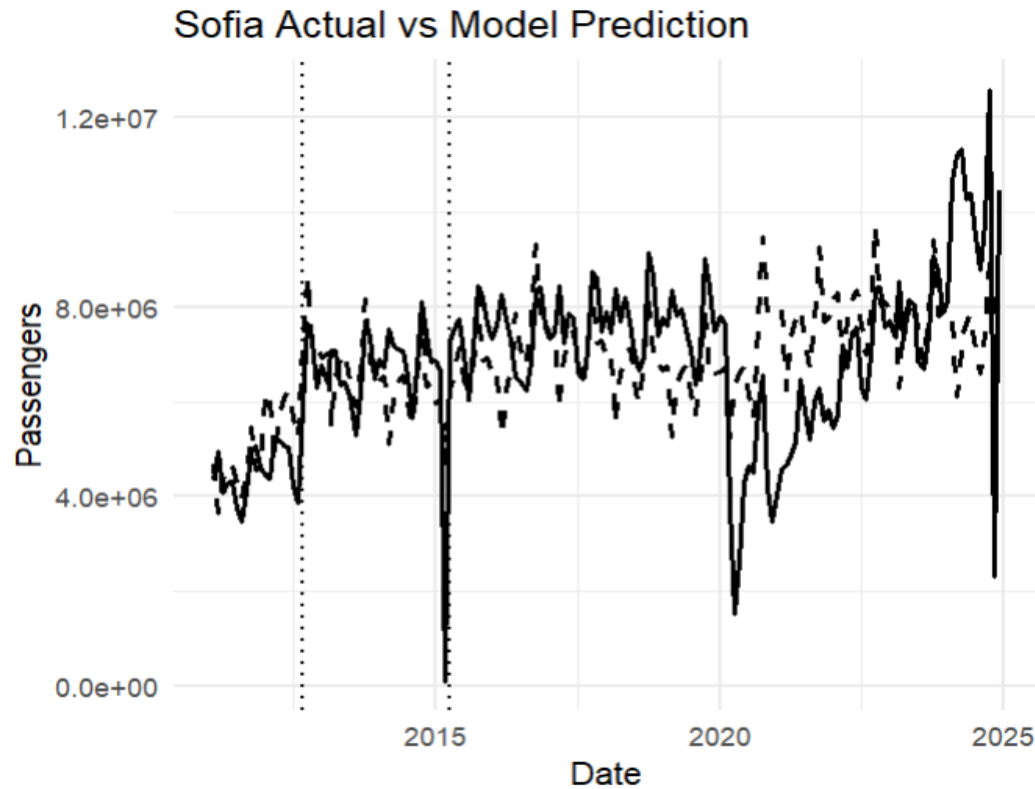


Log-Linear Model (Structural):

$$\ln(D_t) = \beta_0 + \beta_1 \ln(GDP_t) + \beta_2 \ln(POP_t) + \beta_3 \ln(NETKM_t) + \beta_4 \ln(FARE_t) + \gamma t + \delta_m + \varepsilon_t$$

Validation Approach

- Tested **three structural variants**
 - Direct transfer of West Midlands elasticities, Partial Adaptation, Full Sofia Refit
- **Event-based** reverse forecasting around expansion windows
 - Trained with pre-expansion data → Forecast post-expansion ridership → Compare observed demand
- **Metrics:** RMSE, MAE, sMAPE
- **Log-Linear Model** vs **Statistical** Benchmarks (*seasonal naïve, historical mean, trend plus season*)



Actual vs Predicted Monthly Ridership for MetroS

Key results

- *Direct Parameter Transfer* – **Poor** (sMAPE > 180%)
- *Partial Adaptation* **improved** results but underperformed statistical benchmarks
- **Full Sofia Refit** comparable to strongest benchmark (sMAPE about 19%)
- Infrastructure elasticity retained positive sign
- Macroeconomic and fare elasticities not transferable

Conclusion and Implication

- The Log-Linear form is **transferable**
- Parameter values are **context dependent**
- Infrastructure response **mechanism broadly consistent**
- **Model suitable for:**
 - Strategic planning
 - Network expansion appraisal
 - Scenario testing



03 — Anomaly Detection in the Vehicle Interior

Detect uncleanness in the Vehicle Interior

Motivation:

- Pollution in public transport, e.g. metro, should be recognised and removed as quickly as possible

Problem:

- There is too little training data for automated detection using a camera

Solution approach :

- Use of pre-trained networks for image classification
- Transfer learning with images of general pollution from open datasets
- Zero-shot transfer to metro vehicles

ResNet50 pre-trained on ImageNet1k dataset
 • Modified with replacement output-layer with only 2 classes

Open Dataset of Clean/Unclean Urban Environments (ca. 540 Bilder)

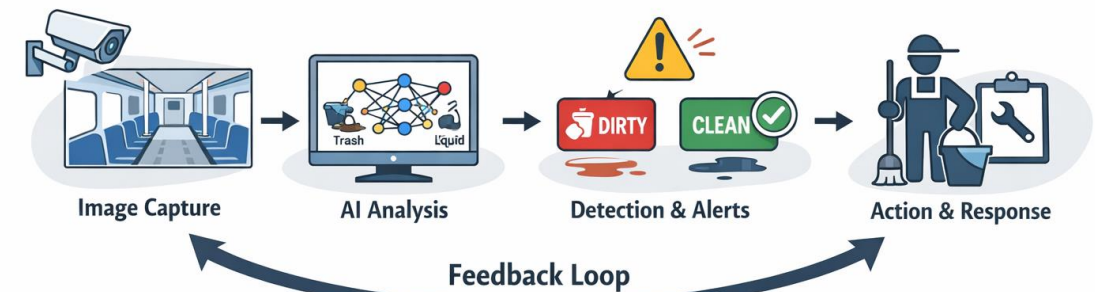


Transfer Learning

Trained to >98% validation accuracy

93% accuracy on Clean/Unclean classification in heavy rail passenger cars (50 Bilder)

Zero-Shot Transfer

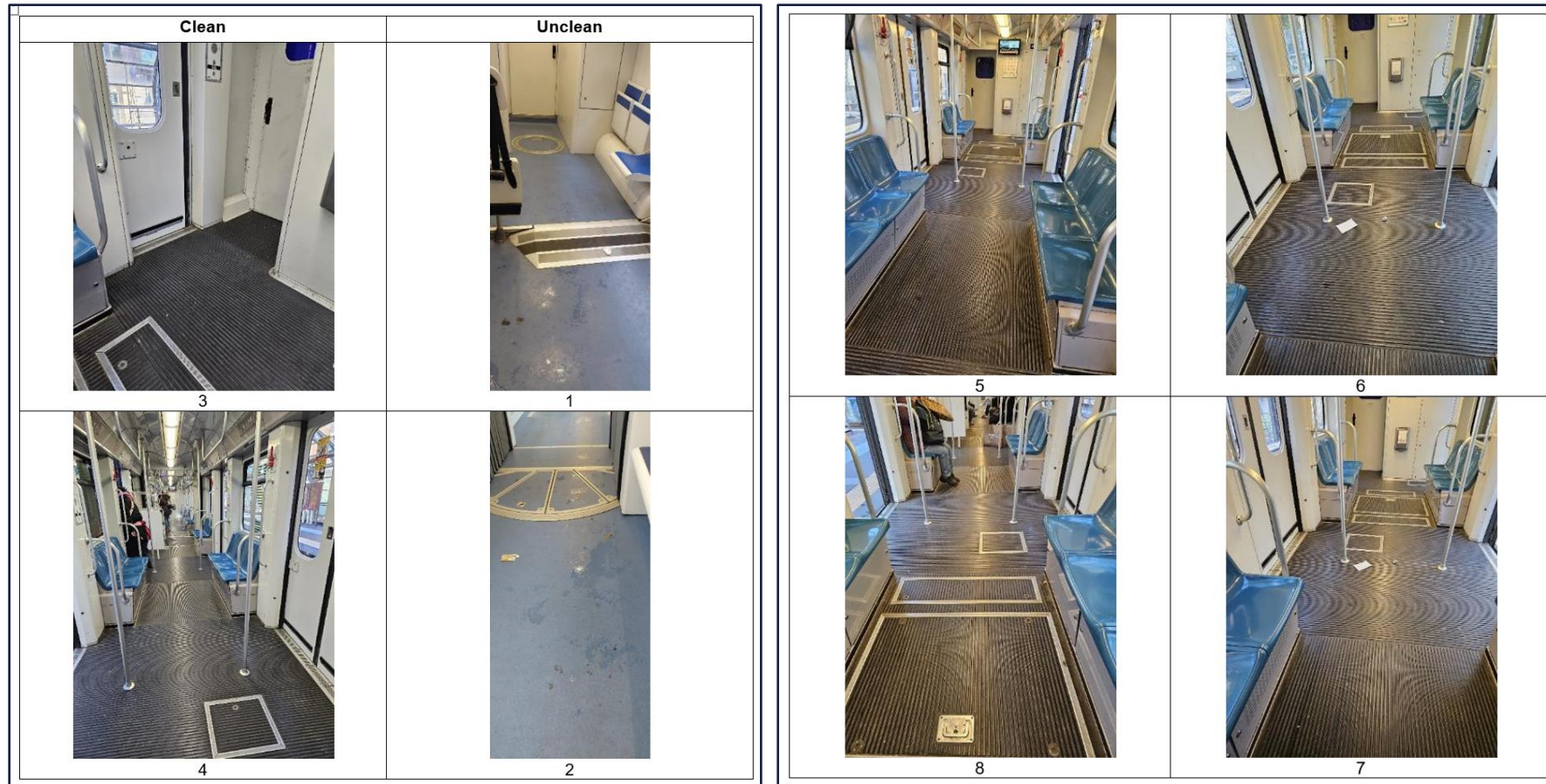


Pollution as an Anomaly Problem



Training the Modell using publicly available data

Validating the model with real-world images from the Genoa Metro



Validation of Uncleanliness Detection

❖ Summary:

- ❖ Validation under real-world operating conditions
- ❖ Recognition rates often well over 90%
- ❖ Consistent performance under varying lighting conditions
- ❖ Reliable classification in real-world Metro scenarios

❖ Operational Impact:

- ❖ Reduction in manual inspections
- ❖ Faster response
- ❖ Objective quality control
- ❖ Consistent documentation



Therefore the key question remains: can we manage cleaning in a data-driven way — by shifting from a time-based model to a condition-based model?

Limitations and Further Potential

Despite its high accuracy, there are limitations:

- ❖ new types of contamination
- ❖ extreme lighting conditions
- ❖ generalization to other vehicle types

Further potential for this approach

- ❖ Adaptation for use in stations
- ❖ Graffiti detection
- ❖ Aggression detection
- ❖ ...





04 ————— Potential of AI to Reduce Energy Consumption and CO₂ Emissions

Potential of AI and GoA4 to Reduce Energy Consumption and CO₂ Emissions

❖ Approach: automation enables new operational concept:

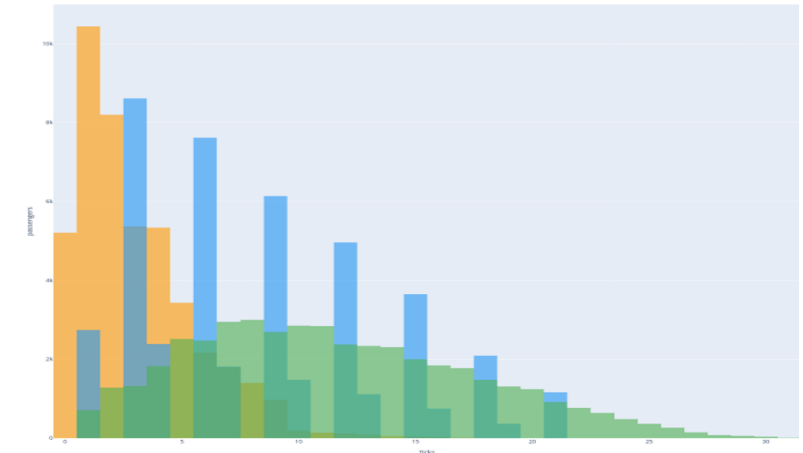
- ❖ Demand-responsive scheduling with short depot stops during low demand

❖ Objective of the study:

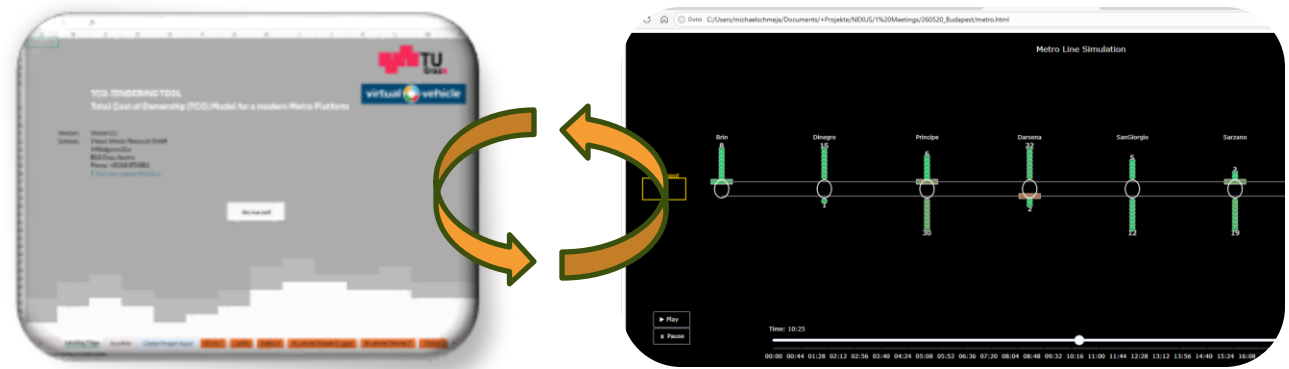
- ❖ Demonstrate new optimisation potential by coupling with TCO Tool
- ❖ Show impact on energy, CO₂, and costs
- ❖ Support future decision-making via simulation tools

❖ Key benefits:

- ❖ Short, flexible depot stays
- ❖ Dynamic adaptation to demand fluctuations
- ❖ Reduced energy consumption & CO₂ emissions
- ❖ Lower operational costs
- ❖ Efficient train utilisation



Time distributions of passenger activities (waiting times, in-vehicle journey times and trip durations)

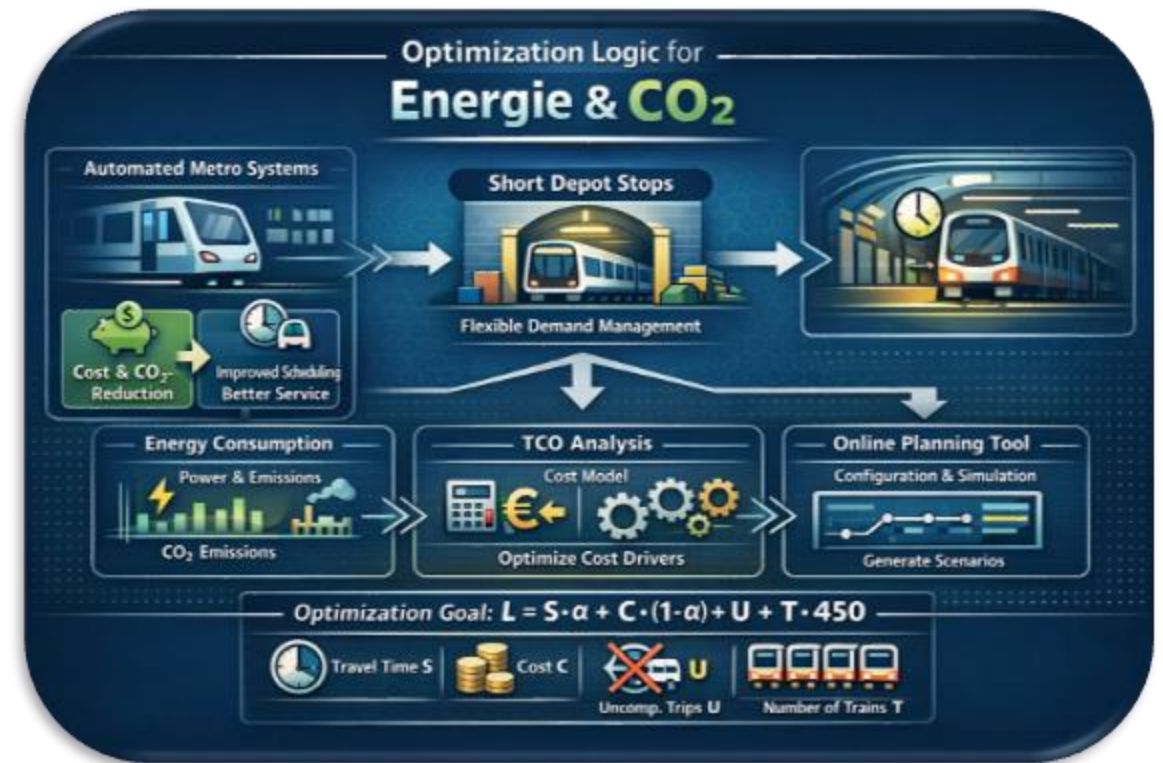


Transition to fully automated metro systems (GoA4) enables new optimisation strategies

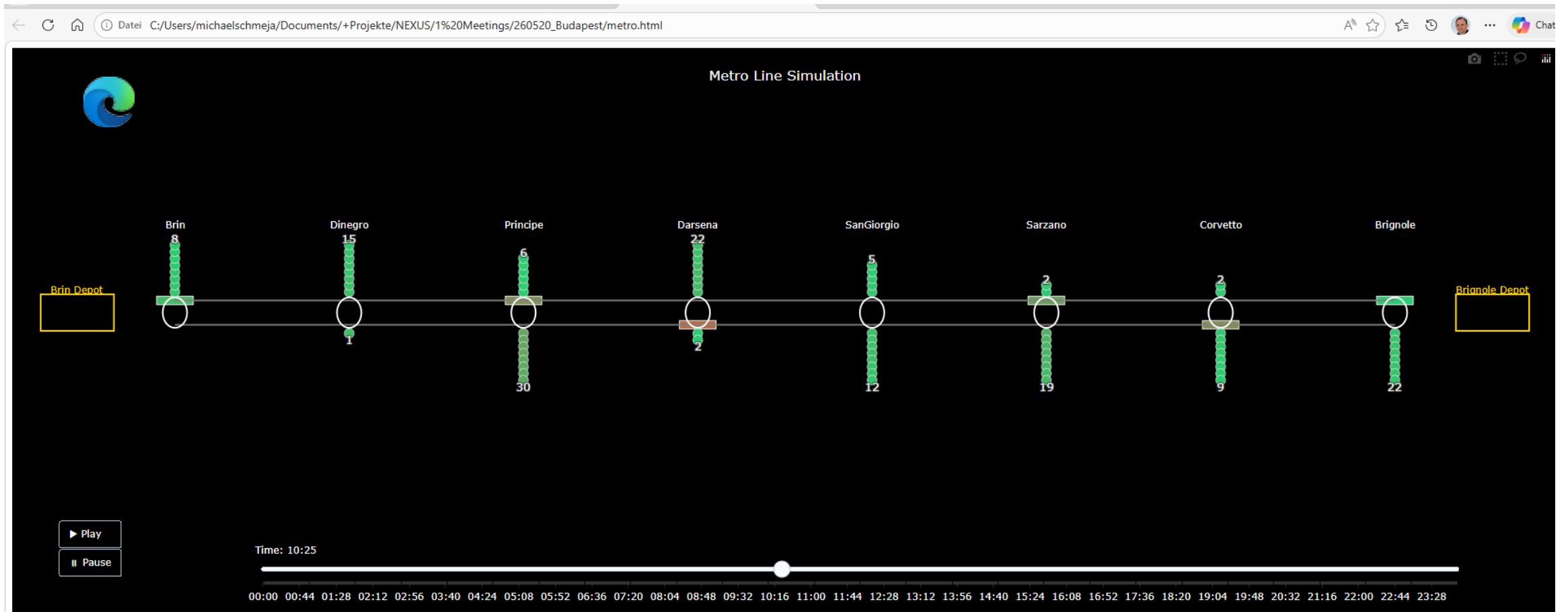
Methodology & Simulation Approach

Transition to fully automated metro systems (GoA4) enables new optimisation strategies

- ❖ **Case study: Genova metro (single-line simulation)**
- ❖ **Simulation framework:**
 - ❖ Discrete-event simulation (SimPy)
 - ❖ 45,000 synthetic passengers (realistic demand patterns)
 - ❖ Full 24-hour operation cycle
- ❖ **Integration of Total Cost of Ownership (TCO) model:**
 - ❖ Energy consumption (by operational state)
 - ❖ Power peaks and savings
 - ❖ CO₂ emissions
 - ❖ Maintenance costs
- ❖ **Key optimisation parameters:**
 - ❖ Target dwell time
 - ❖ Passenger threshold for depot entry
 - ❖ Depot check frequency
 - ❖ Number of trains
- ❖ **Multi-objective optimisation:**
 - ❖ Balance between: Passenger travel time (service quality) and Operational costs



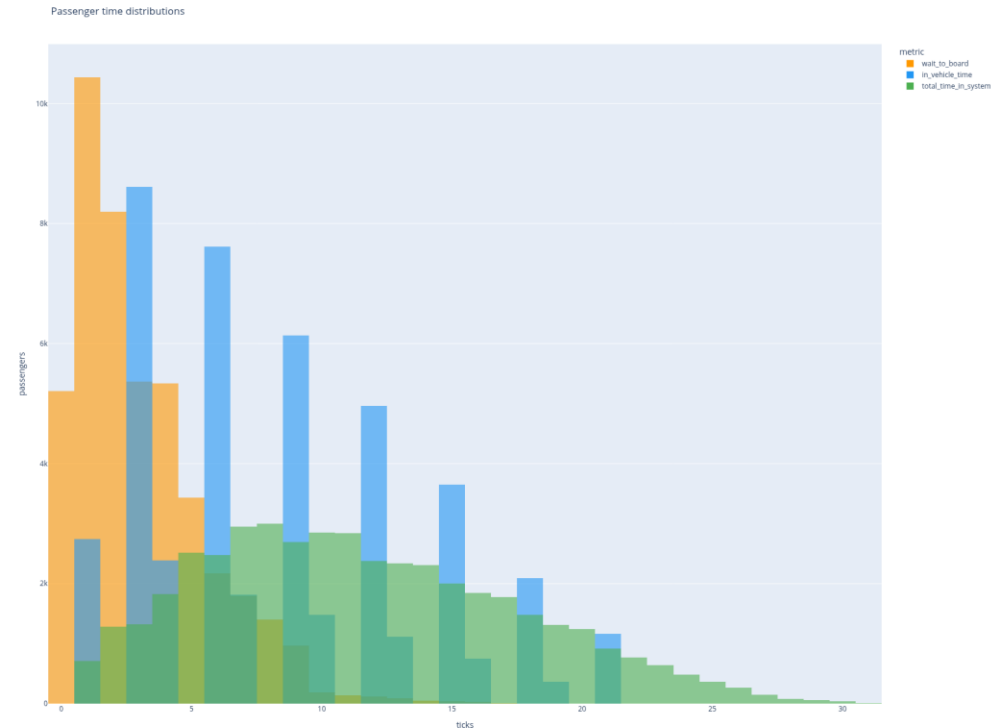
Showcase Genoa Metro



The simulation results demonstrate that when optimising for a balanced objective of operational expenditure and service quality, unconventional scheduling patterns—such as frequent, short-duration depot withdrawals—emerge as an optimal strategy.

Results & Key Insights

- ❖ **Automation enables new operational patterns:**
 - ❖ Short, flexible depot stays
 - ❖ Dynamic adaptation to demand fluctuations
- ❖ **Key benefits:**
 - ❖ Reduced energy consumption & CO₂ emissions
 - ❖ Lower operational costs
 - ❖ Efficient train utilisation
- ❖ **System performance:**
 - ❖ Stable passenger travel times (~12 minutes avg.)
 - ❖ Controlled power peaks (limited simultaneous acceleration)
- ❖ **Key insight :**
 - ❖ Optimisation naturally finds **non-intuitive but efficient strategies**
- ❖ **Conclusion:**
 - ❖ Automated metros enable adaptive, efficient, and sustainable operations
 - ❖ Simulation tool supports data-driven planning for future metro systems



Time distributions of passenger activities (waiting times, in-vehicle journey times and trip durations)

The simulation results demonstrate that when optimising for a balanced objective of operational expenditure and service quality, unconventional scheduling patterns—such as frequent, short-duration depot withdrawals—emerge as an optimal strategy.



05 — Cybersecurity Threat Identification and Management Framework

Cybersecurity Threat Identification & Management

What we did

- Assessed the **AMT cybersecurity baseline** against the **18 CIS Controls / 153 safeguards**
- Performed a **data-driven gap & exposure analysis** across metro assets and target types
- Connected identified priorities to the **rail/OT context through IEC 62443 & CENELEC TS 50701**
- Developed a **prioritised cybersecurity improvement roadmap** and **Emergency Response Plan**

What we achieved

Key priority areas identified

- Network Monitoring & Defence
- Audit Log Management
- Vulnerability Management & Penetration Testing
- Incident Response
- Security Awareness & Skills

Outcome:

A structured pathway from identified cybersecurity gaps → prioritised controls → actionable IT/OT hardening & incident readiness

From Cybersecurity Baseline to Secure AI Exploitation

Building on D6.2, D7.1 extended the framework to AI-enabled metro applications

4-step methodology:

1. AI-enabled scenario
2. Attack surface & trust boundaries
3. MITRE threat mapping
4. Safeguards & validation gates

What we achieved

- Mapped threats across the **AI/ML lifecycle** — data ingestion → training → deployment → inference
- Combined **MITRE ATLAS + ATT&CK/ICS** for AI, IT and OT threat scenarios
- Addressed AI-specific threats: **data poisoning, model tampering/theft, adversarial inputs, API abuse & prompt injection**
- Defined layered safeguards for **data, MLOps, IAM, runtime, monitoring and supply chain**
- Introduced **gating criteria** for progression from experimentation → pilot → production-like deployment

Outcome:

A reusable, model- and vendor-agnostic framework for deciding whether an AI-enabled metro application is sufficiently secure and trustworthy to progress towards operational deployment.



06 — Concluding Remarks

Artificial Intelligence & Cyber Security for Smarter Metro Operations

High Visibility

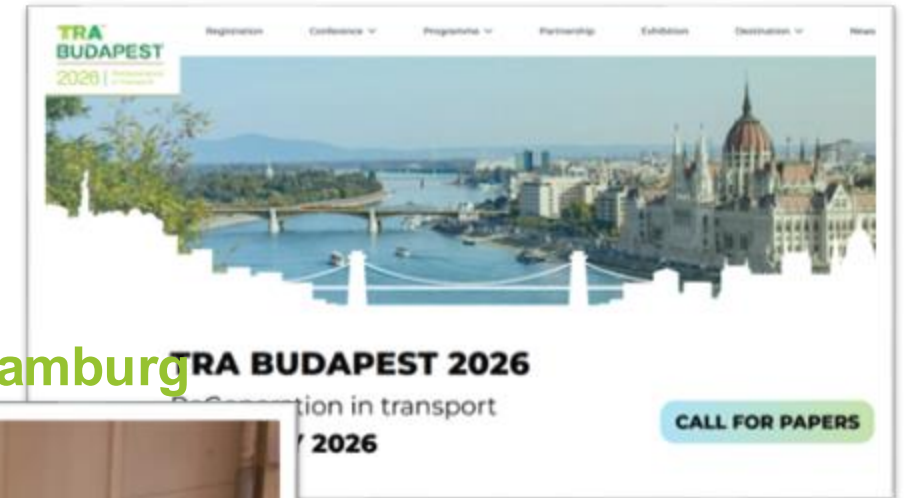
Schienenfahrzeugtagung Dresden 2026



UITP Summit in Hamburg



Transport Research Arena Budapest 2026



Concluding Remarks - Considering Acceptance and Trust

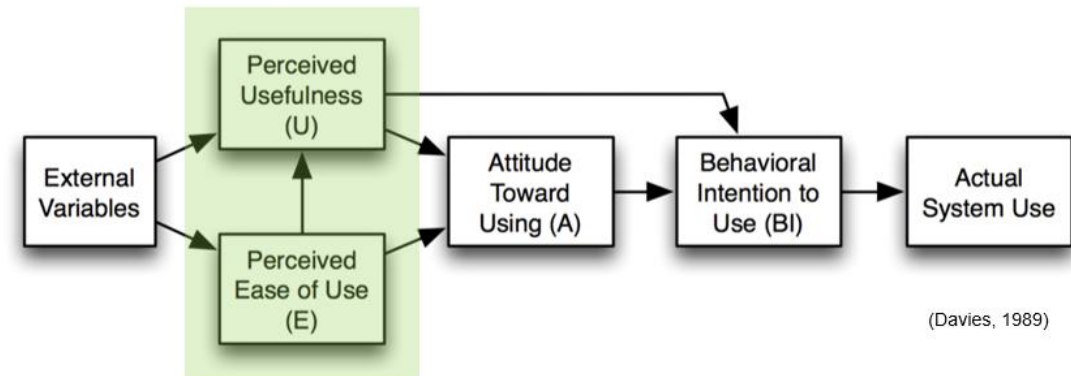


**A ship in harbor
is safe, but that
is not what ships
are built for.**

John Augustus Shedd

In addition, D6.1 further explores **research related to technology acceptance and trust in the context of AI** and data science adoption, providing a snapshot of current insights into how these factors influence the **successful implementation** of such technologies **in metro operations**.

The very first TAM (Technology Acceptance Model) from Davies



(Davies, 1989)

A Software, a tool, a new technology, which is not used by the user is useless!

THANK YOU!

Michael.Schmeja@v2c2.at

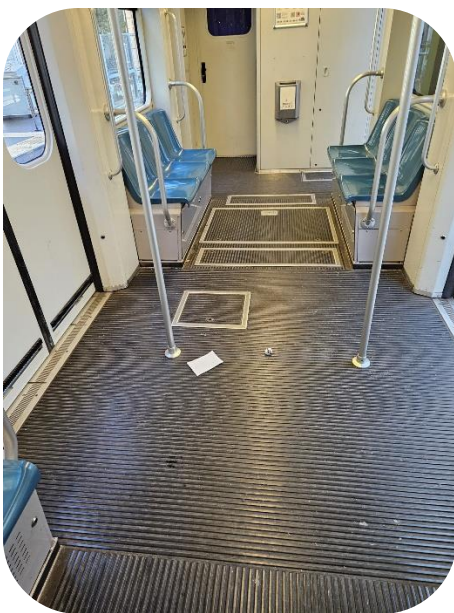
 NEXUS Project

 nexus-heproject.eu



Scientific Context - What Is New or Relevant?

- ❖ Transferring a pre-trained ResNet50 model to Metro interiors
- ❖ Zero-shot domain transfer without domain-specific retraining
- ❖ Validation under real-world operating conditions



Validation under real-world operating conditions on the Genoa Metro

The model was validated using real-world images from the Genoa Metro

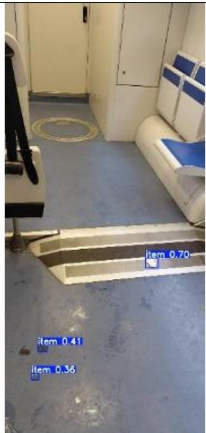
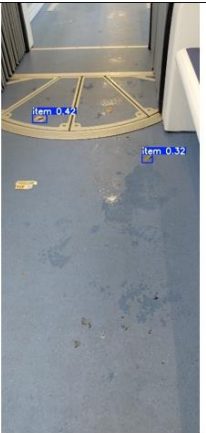
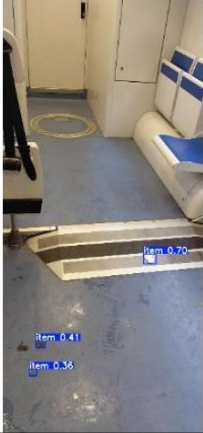
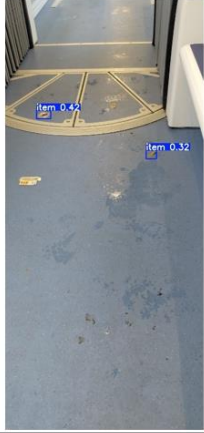
Image ID	IMAGE	Image ID	IMAGE
1		2	
6		7	

Image ID	Prediction	Correctness
1	Unclean	✓
2	Unclean	✓
3	Clean	✓
4	Clean	✓
5	Clean	✓
6	Unclean	✓
7	Unclean	✓
8	Unclean	✗

The model was validated using real-world images from the Genoa Metro

Image ID	IMAGE	Image ID	IMAGE
1		2	
6		7	

8	
---	--

The way the flap is attached throws the algorithm off