



Securing the Digital Backbone of Public Transport

**Gothenburg Tramway system - Insights from Gothenburg's NIS2
Implementation Study**

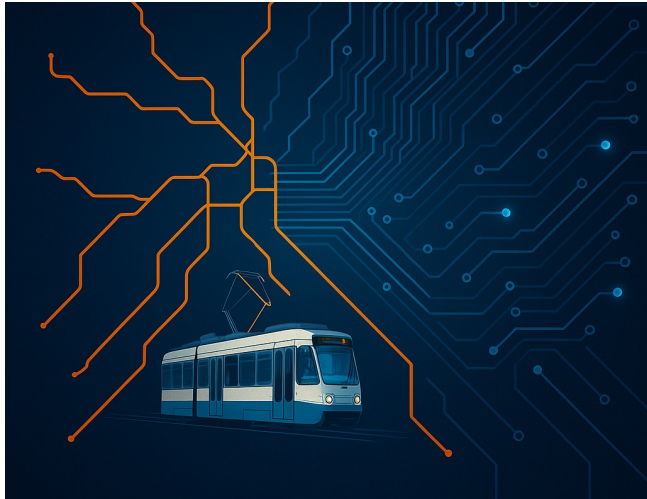
Mimmi Mickelsen

Public transport is no longer just rails and wheels – it's data, systems, and connectivity.



Göteborgs
Stad

- Digitalisation runs through every part of public transport
- Traffic management, signalling, ticketing, sensors, and infrastructure are all networked
- This creates a “digital backbone” that must be secure and resilient



The EU Framework

- NIS2 Directive (EU 2022/2555):
Cybersecurity of network & information
systems
- CER Directive (EU 2022/2557): Resilience of
critical entities
- Both apply to urban transport and public
administration as essential entities
- But this is not the only regulations that we
need to adopt to





The Gothenburg Study

Purpose: Identify what Stadsmiljöförvaltningen (SMF) must do to comply with NIS2

Method:

- GAP analysis vs ENISA's cybersecurity guidance
- Interviews with MSB (Swedish Civil Contingencies Agency)
- Benchmark with Stockholm, Lund & Norrköping
- Document and policy review

The Key Findings

Area	Current Situation	Gap Identified
Policy Framework	Fragmented	Needs central structure
Roles & Responsibility	Split SMF–GSAB	Must be clarified
Education & Awareness	Limited	Requires systematic training
Continuity Planning	Partial	Lacks cyber resilience focus
Documentation	Scattered	Needs digital system for compliance

Risk Management Requirements (NIS2 Art. 21)

Each entity must secure:

- Risk Analysis & Security Policy
- Incident Handling & Reporting
- Business Continuity
- Supply Chain Security
- Cyber Hygiene & Training
- Use of Cryptography, Access Control, MFA

These form the “**digital safety system**” of public transport.



Building Cyber Awareness



Lessons from Other Cities

Stockholm (Trafikförvaltningen):

- Assigns clear ownership & uses risk registers.

Lund & Norrköping:

- Joint municipal cyber response teams.

MSB guidance:

- Prioritise *preparedness over perfection* – implement stepwise.

Challenges for Public Transport

- Legacy systems with limited cyber maturity
- Complex ownership structures (city vs. operator)
- Dependence on suppliers and contractors
- Need to balance openness with protection
- Cybersecurity $\neq$ IT issue — it's a **governance and resilience issue.**



The Way Forward

Recommendations from the Gothenburg report:

- Establish unified policy and document hub
- Define cyber roles & accountability
- Continuous education plan
- Integrate NIS2 into existing safety frameworks
- Conduct annual self-assessment & audit



The Vision

**“From track safety to
cyber safety –
ensuring public transport
remains safe, reliable, and
resilient in a digital world.”**



Closing & Discussion

Cybersecurity is the new foundation of
public trust in transport.

**Let's build resilience – together across
Nordic cities.**

Kontakt

Mimmi Mickelsen

mimmi.mickelsen@stadsmiljo.goteborg.se

Stadsmiljöförvaltningen, Göteborgs Stad