Proactive Collaboration within the transport sector is needed for managing resilience and operational efficiency under NIS2 and CER Directives

Pontus Blomqvist
Swedish Transport Administration
(Member EIM Cybersecurity WG)

pontus.blomqvist@trafikverket.se

Anders Jonsson
Stockholm Public Transport Authority
(consultant, Member Enisa AHWG EUCS, Observer Enisa AHWG on the Cybersecurity Market)

anders.h.Jonsson@sl.se

Version 1.0
K1

The goal with the EU's Cybersecurity strategy is:

1. Strengthen Europe's resilience to cyber threats

- Protect networks, information systems, and critical infrastructure (energy, **transport,** health, finance, etc.).
- Ensure all Member States reach **a common high level of cybersecurity through NIS2 & CER Directives.**

2. Build collective defence and response capabilities

- **Improve cooperation** and information-sharing among EU countries, the private sector, and EU institutions.

3. Secure digital technologies and supply chains

- Promote "security by design" in digital products and services.
- Introduce the **Cyber Resilience Act (CRA)** to make hardware and software products safer.
- Reduce Europe's dependence on non-EU technologies and ensure trustworthy supply chains.

4. Develop skills, awareness, and a strong cyber ecosystem

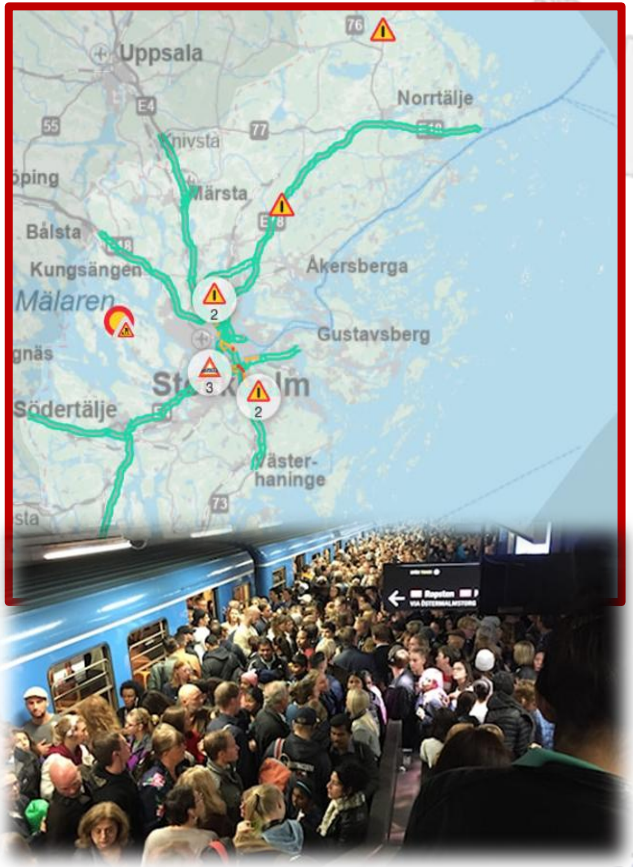
- Invest in education, training, and workforce development in cybersecurity.
- Support innovation, startups, and research through the European Cybersecurity Competence Centre (ECCC).

5. Promote a global, open, and secure internet

- Strengthen international cooperation on cyber norms, diplomacy, and cybercrime prevention.

Proactive Collaboration within the rail-bound public transport sector has been a success for mange resilience and operational efficiency in Sweden.

*”When we began working with **the directives**, we quickly recognized that rail-bound public transport, **particularly in large cities**, plays an even more critical role for functioning of other essential sectors than traditional railway services”*



Public transport in Metropolitan area of Stockholm

2.5 Miljon boarding passengers per working day - 2025

- Metro: 439 metro cars (39%)
- Bus: 2,396 vehicles (38%)
- Commuter train: 129 cars (15%)
- Tram/Local train: 120 cars (8%)
- Boat: 25 vessels + 50 chartered (<1%)

(1.5 M Saturdays - 1.2 M Sundays)

Public transport plan Stockholm 2050*
Work trips: Increase from 56% in 2015 – to 64% in 2050
Business trips: Increase from 43% in 2015 – to 57% in 2050

Large cities: The high-density of the population, concentration of workplaces and business renders public space into a scarce commodity. By consequence, public transport is the most efficient mode of transport in terms of space consumption per head.
*Public Transport Plan 2050 is the Stockholm Region's long-term plan for the development of public transport from 2030 to 2050.

Areas in scope of sector specific collaboration:

- **Collaboration on cybersecurity training** (IT/OT) and participation in various European programs/groups
- **Develop and share a common method for NIS2.** How to identifying and assessing critical functions-IT & OT services
- **Analyze incident and report hierarchy.** When is the incident critical enough to report?
- **Data-driven dynamic maintenance reduces costs.** But it can also increase resilience!
- **What can we learn from each other about AI**, share experience within our sector.
- **Collaboration to secure the supply chain** within our transport sector - CRA

Cooperation with local NSA and financed together with ENISA

Date:
February 5, 2026
09.00-16.30

Place:
Trafikförvaltningen
Stockholm
Sweden

Interested to know more
contact us or your local NSA/Enisa

The agenda included below is indicative and subject to change.

Time	Topics
0900 – 0915	Welcome and objectives: - Introduction to the seminar and expected learning outcomes - Overview of IEC 63452 and
0915 – 1015	Session 1 - Overview of IEC 63452 - Scope, terminology, structure, lifecycle - Relationship to TS 50701, IEC 62443, EN 50126, and NIS2
1015 – 1030	Coffee Break
1030 – 1145	Workshop 1 – Applying the risk-based approach - Identify assets in a simplified rail network architecture (onboard + trackside) - Define system boundaries, zones, and conduits - Perform a brief threat and risk assessment - Determine initial cybersecurity requirements
1145 – 1230	Session 2 – Integrating IEC 63452 into the rail lifecycle - Embedding cybersecurity into the system engineering lifecycle (EN 50126) - Interfacing safety with cybersecurity processes
1230 – 1315	Lunch
1315 – 1400	Session 3 – Supplier and procurement cybersecurity requirements - Translating IEC 63452 and NIS2 into supplier requirements - Setting acceptance criteria and assurance measures
1400 – 1515	Workshop 2 – Supplier risk management and validation - Review sample supplier documentation for a signaling subsystem - Identify compliance gaps against IEC 63452 and NIS2 - Propose acceptance criteria and validation steps
1515 – 1530	Coffee Break
1530 – 1615	Session 4 – Compliance roadmap - Assessing compliance gaps against IEC 63452 and NIS2 - Prioritizing remediation based on risk, criticality, and resources
1615 – 1630	Wrap-up and Q&A

Areas in scope of sector specific collaboration:

- **Collaboration on cybersecurity training** (IT/OT) and participation in various European programs/groups
- **Develop and share a common method for NIS2.** How to identifying and assessing critical functions-IT & OT services
- **Analyze incident and report hierarchy.** When is the incident critical enough to report?
- **Data-driven dynamic maintenance reduces costs.** But it can also increase resilience!
- **What can we learn from each other about AI**, share experience within our sector.
- **Collaboration to secure the supply chain** within our transport sector - CRA

Starting point for assessing critical functions, critical systems and incident reporting

Incident notification within 24h
Iincident report within 72h
Full report within 30 days

<u>Significant incident (NIS2)</u>:

An incident shall be considered to be significant if:

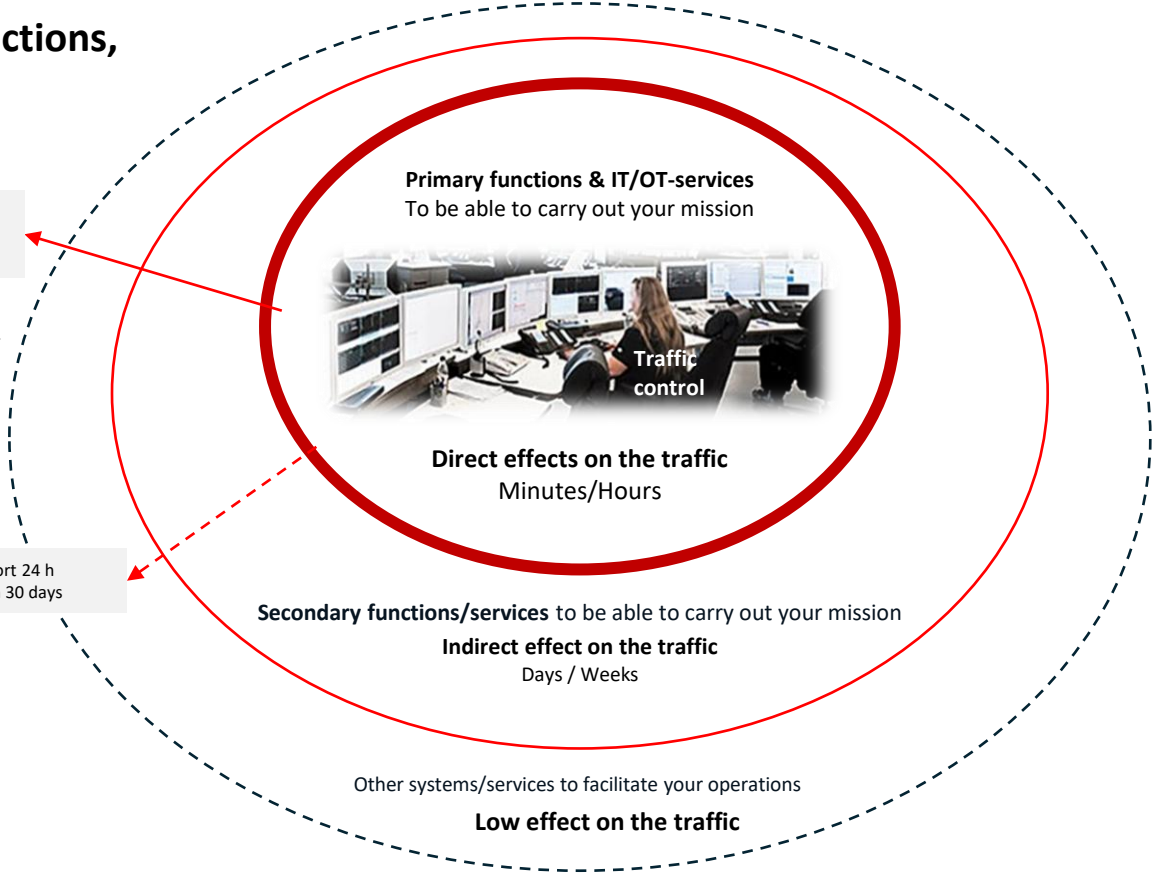
- it has caused or can cause severe operational disruption of the services (public transport) or financial loss for the entity concerned;
- it has affected or can affect other natural or legal persons by causing considerable material or non-material damage

Incident report 24 h
Full report in 30 days

<u>Significant incident/disruptive effect (CER):</u>

For significant incident, the following should be considered:

- the number of users relying on the essential service
- **the extent to which other critical sectors depend on the essential service in question**
- the duration of the disruption, and
- the geographical area affected by the disruption, considering whether the area is geographically isolated.



When is the incident “**critical enough”** to report, according to the new laws?



A critical incident within the Stockholm public transport system-SL!

SL mange 2.5 million boarding passengers per day and every ticket is valid for 75 min at all type of traffic modes!
Our conclusion is that we can only act on our planned regularity!

(Discussed proposal) §6 A significant incident that has caused serious operational disruption to the service offered is an incident where
1. the unavailability or reduced functionality of one or more sector critical systems has meant that
*a) the sector's operations can only be provided to a limited extent, corresponding to less than 95 percent of planned departures during a traffic day (24h) per traffic mode**
b) sector operations have had to use alternative traffic modes or methods to offer the service for more than six hours

** Traffic mode: Metro, Buss, Tram, local train, boat, train etc…*

CRA is necessary to secure transparency and security in the supply chain

Category - CRA	Risk level	Examples	Requirement level
Common consumer products	low	Smart home devices, apps, etc.	Self-assessment according to standards, CE
Medium risk products	medium	Operating systems, firewalls, VPN	Self-assessment according to standards, CE
High-risk products	high	SCADA, network control, cloud security	Third-party assessment, EUCC, EUCS…
Annex IV- extra critical products	critical	Smartcards, control systems, crypto HSM/KMS	Third-party assessment, EUCC, EUCS…

”90 % of the data packages are routed back to China from their electric vehicles”

All buses in Norway will be electric by 2030, 80% will be Chinese.

Norway has 660 electric Chinese buses as of June 2025, an additional 1200 are on the way.

TLP:CLEAR

Scenario 1: «Kill Switch»

Traffic sabotage, or threat of sabotage used as leverage

Scenario 2: «Lutvann»

The bus as part of a rolling surveillance network

TLP:CLEAR

Can the 2022 VDL be used for the Kill Switch scenario? NO
Can the 2022 VDL be used for the Lutvann scenario? NO

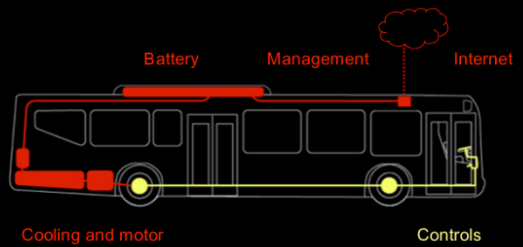
Can the 2025 Yutong be used for the Kill Switch scenario? YES
Can the 2025 Yutong be used for the Lutvann scenario? NO

Yutong – 2025 model

Critical functionality is online, direct digital access for OTA updates and diagnostics.

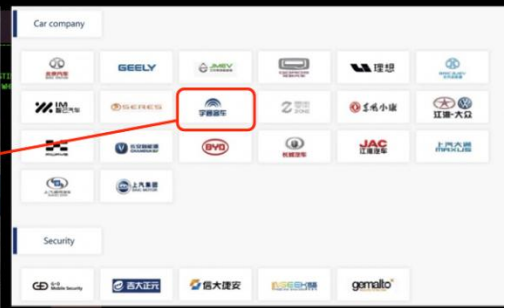
- Manufacturer has the capability to remotely disable or destroy software, **the Kill Switch scenario is possible with this bus.**

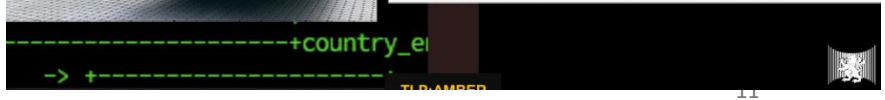
+ current system design is still simple, low degree of system intergration



TLP:CLEAR

Hack #1: OTA update platforms are a weak link





TLP:AMBER

K1

"Inside the Lion Cage" - is a good example on how we should collaborate to raise resilience in our sector!

Questions