TRAFICOM
Finnish Transport and Communications Agency

University level online course for railway cybersecurity

Ville Lahti
Senior Adviser (cybersecurity)
Ville.Lahti@traficom.fi

Introduction: Railway cybersecurity course

- Railway NSAs can—and should—promote cybersecurity.
- Variations in railway cybersecurity competence create a systemic risk.
- The online course can reduce the risk by increasing the understanding
- The course provides a clear starting point for continuous improvement
  - Technology, people, organisations, regulation and best practices change
  - A starting point is needed, followed by ongoing improvement.
- A good-quality online course can be delivered at a low cost.

What have we achieved so far?

- Key objectives
  - **Increase the number of professionals** with railway-specific cybersecurity competence.
  - **Strengthen the cybersecurity skills** of existing railway sector staff.
- Primary target group: cybersecurity experts and students with no prior experience in the railway domain.
  - Secondary target group: railway professionals interested in cybersecurity.
- Results
  - The total budget is **EUR ~35,000** + VAT, in addition to in-house work.
  - November 2025 around 300 students had enrolled
  - November 2025 **over 150 students** had completed the course.

What does the course contain?

- Fundamentals of cybersecurity, railway system and railway technology
- Cybersecurity governance in organisations
- Technical railway cybersecurity (new projects, radio networks)
- Railway cybersecurity in the EU
- Threat landscape for the Finnish railway sector
- In-depth: Regulatory framework (NIS2, CRA, national law and guidance)
- Overview: Standardisation (TS 50701, draft IEC 63452, IEC 62443 series)
- *Limitations: Public level information can’t contain in-depth information about technologies, vulnerabilities, solutions or processes*

2023 – Idea

Mar Discussions: Identifying the key system-level risks in the railway domain

Sep Initial idea and budget proposal

Nov Cooperation proposal to the National Emergency Supply Agency

Dec Project concept presented to universities and private sector

2024 Funds, procurement, content

Mar Background discussions with interested organisations

Apr Drafting the public procurement

May Public procurement: Request for proposal published

Jun Funding agreement concluded

Jun Submission of tenders & decision

Aug Procurement contract

Sep Kick-off meeting

Sep Initial survey for key stakeholders

Oct ERA-ENISA Conference: Presentations on trainings

Oct Ideas from the Spanish online course

Dec Railway cybersecurity seminar recorded

2025 Publication, improvement

Feb Pilot course material completed

Mar 1st Pilot course opened

Jul Feedback from the 1st round

Aug Planning of the annual update cycle

Sep 2nd round of the course

Sep IEC CDV 63452 commenting integrated with course material development

Nov CRA webinar integrated with course material development

Dec Course material update finalized

2026 Hand over

Jan 3rd round of the course - Updated version

Sep 4th round of the course starts

Dec Course ownership handed over to the university

How can we improve the model?

Finland

- Hand over to the university in Q4/26
  - Annual maintenance needed
- Adjust how we work
  - Online events to be recorded when appropriate
- Expanded to cover both physical and digital preparedness for the railway sector?
  - Finland has the long tradition on railway resilience

EU

- Need for railway cybersecurity competence
- An EU-wide, English-language online course on railway cybersecurity is feasible.
  - Hosting and maintaining the learning platform?
- Practical proposal:
  - The ERA–ENISA Railway Cybersecurity Conferences as the foundation?
  - Streamed, recorded, and integrated into study materials?
  - Voluntary contributions?

XAMK PULSE OPEN UNIVERSITY OF APPLIED SCIENCES

TRAFICOM
Finnish Transport and Communications Agency

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

Thank you for cooperation:

Mipro, WSP Finland, IC Security, FTIA, Fintraffic, Digirail, Reformo networks, Metropolitan Area Transport Ltd, Cylus, Siemens Mobility, ENISA

Cybersecurity in Rail Transport (Non-stop start, 5 credits)

https://koulutuskalenteri.xamk.fi/avoimen-amkn-kurssit/raideliikenteen-kyberturvallisuus-nonstop-aloitus-5-op/