EUROPEAN UNION AGENCY FOR RAILWAYS

Moving Europe towards a sustainable and safe railway system without frontiers.

Questions and Answers

ERA-ENISA Webinar: Managing Cybersecurity Risks in Railways

25 November 2021

Q: Is there an impact on EN 5012X due cybersecurity?

A: Yes. The CENELEC series about railway applications already consider the cybersecurity risk in the EN 50126.

Q: What is ENISAs opinion about UNIFE "Cybersecurity position paper" taking into consideration that TS50701 should be used in "short term" like certification scheme and that all our legacy system should be reviewed (and new system planned) based this TS? Is this feasible in short time and what will be added value for us in railway (in comparation with using 62443 like the basis)?

A: The European Cybersecurity Act (CSA) stipulates fundamental requirements for the definition, implementation and maintenance of EU cybersecurity certification schemes. The use of these schemes is voluntary. Therefore their market take-up, as a prerequisite, requires acceptance by the ICT industry and the consumers. To this end, ENISA recently released a methodology for sectoral cybersecurity assessments, designed to be used as a preparatory step for the definition of a EU candidate certification schemes involving sectoral stakeholders. (https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment). To the best of our knowledge, such an assessment has not been conducted yet for the Railway sector.

Q: Is there a full list of Risk Treatment (Mapping NIS -NIST - TS50701) available to download?

A: Yes. The list of available risk treatment options based on NIS Directive, ISO27002, NIST Cybersecurity Framework and the CLC/TS50701 can be found at the annex of the report. https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

Q: UNIFE Paper is scoped to Signalling but headlined to “Railway”. ENISA covers all entities?!

A: For this particular report, we focused on cyber risks affecting both the IT and the OT systems of Railway Undertakings and Infrastructure Managers. ENISA supports the implementation of the NIS Directive, which aims at improving the information and network security of these two types of entities. The proposal for a new NIS Directive covers more entities, which may include the supply chain.

Q: I understand the speeches today focus on technical threats and guidelines, standards. Are there tools or information available for risk assessment on Human and Organizational Factors (with scenarios) within rail companies? If so, can those be allocated on the ERA safety culture model? Thank you in advance.

A: Unfortunately, we are not aware of such cyber risk assessment tools.

Q: Will ERA consider TS 50701 as mandatory standard, even if it is a technical specification only?

A: No. As indicated during the webinar, the TS 50701 is considered a very valuable milestone in railway cybersecurity standards but cannot be as is considered as a mandatory Standard in the EU railway regulatory framework.

Q: Can you provide the link to document please, where these threat scenarios are published and mapped?

A: https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management

Q: As transportation entities are more and more connected, in particular rail and air, should the risk assessment also include this connection instead of having only a sector specific approach? Could you please comment on this, thanks?

A: Assessing dependencies and interfaces to other entities, such as service providers, third parties or indeed other connected transport means could be considered within the risk assessment process. On the threat aspect of risk, ENISA is planning a cyber threat landscape for all transport subsectors in 2022. This will allow to observe common threats between the different modes of transport.

Q: Will be settled a common "register" to share real situation and report issues on cybersecurity and approach to solution? This will help to share knowledge and share best practices.

A: Sharing of information for the railway stakeholders to be more aware of cyber threats is indeed very important, and this is precisely an activity carried out by the European Rail - Information Sharing and Analysis Center.

Q: Would you expect that scenarios like ransomware attacks, theft, leakage of data, DDoS could lead to impacting traffic operations? Do you have any examples, possibly from other transport sectors?

A: An example would be attacks that may target the availability or integrity of passenger information systems, as they can cause confusion or inability for passengers to reach their destination. One of the most prominent examples comes from the maritime sector, where in July 2017, the cyber-attack at Maersk prevented vessels from accessing or departing ports for several weeks and destroyed the company's entire computer system, costing it over US$300 million.

Q: Are there any specific examples/templates on how the security risk assessment should be carried out? It is clear what needs to be done, but if it comes to the execution itself, it is really hard to select a proper approach and the details of the analysis.

A: Currently not, but ER-ISAC is preparing a document "Zoning and Conduits for Railways" based on EN 50701 that could be used as a guideline for performing the security risk assessment.

Q: About Risk scenario 1 (compromising CCS system to procure an accident): Is it a real risk? Have alternative simpler opportunities for a terroristic attack ever been considered vs. the complexity of hacking the trackside-onboard safety data dialogue?

A: It was pointed to us as a primary concern by the organisations participating in the study. The likelihood of such a scenario should be considered during the risk assessment, and based on the absence of previous incidents, it can be considered as low. This does not mean other attacks, such as physical attacks of lower complexity should not be considered.