EUROPEAN UNION AGENCY FOR RAILWAYS

Making the railway system work better for society.

Questions and Answers

ERA webinar: Cybersecurity in Railways

13th November 2020

Q: Which are the milestones and foreseen dates for setting the Regulatory Framework (affecting CSM and TSIs)? When are the affected TSI and CSM regulations foreseen to be published?

A: For the methodology part, to be better consider in the Common Safety Methods, it depends on the publication of the CENELEC TS 50701 (scheduled mid 2021).
For the technical solutions to be included in the Technical Specifications for Interoperability, it depends on the availability of Shift2Rail/UNISIG inputs: a first enhancement could be the CCS TSI 2022.

Q: In the ERA presentation it was mentioned the IT Security will be included in TSIs TAF/TAP, OPE and CCS. Will there be no impact on TSI RST?

A: It should be assumed that all TSIs are reviewed to consider the need for introducing cybersecurity requirements.

Q: Please, could you specify a little more what is the rollout strategy planned at TSI level in order to introduce cybersecurity concrete measures?

A: The technical solutions to be included in the Technical Specifications for Interoperability depend on the availability of Shift2Rail/UNISIG inputs: the first TSI to include enhancements could be the CCS TSI in 2022.

Q: How do you see the new clause 6.4 (about IT services) of the EN50129:2018? How to deal with this new requirement during ISA/AsBo missions? What's the deepness expected for this assessment?"

A: It is assumed by ERA that the CENELEC TS 50701 should be used as a guidance to cope with this requirement.

Q: There are a few Recommendation for Cyber Security @Railway based on ISO27K, 62443 and NIST CS standards (UIC, S2Rail, DIN). It will be nice (good) to have a Recommendation based on prTS50701 which will tell us "how to implement measures" not only "what to be done"! It can be a challenge for UIC/ERA/ER-ISAC experts- some kind of Guidelines for implementing prTS50701.

A: ER-ISAC will be a major actor in the definition of best practices for the implementation of railway cybersecurity. Such an implementation guideline would indeed be very helpful.

Q: Could we consider Cybersecurity to be one element of the Safety Management System?
At the current state has been not an element of evaluation.

A: ERA propose, as a first step, to include an informative reference to the CENELEC TS 50701 where

the link between the cybersecurity risk assessment and the safety risk assessment is described

Q: Happy to see this cooperation between ENISA and ERA. Hope you will also be involved in Shift2Rail2?

A: ERA is already taking Shift2Rail results into account, and will also duly consider the results of Shift2Rail2.

Q: Is PKI standard X509 becoming the standard to protect digital identities of each onboard device and trackside device?

A: This point needs to be discussed in a specific Working Group before being endorsed as a technical solution.

Q: Are you aligned with UNISIG who seems to have define PKI (X509) in the KMS/PKI for ERTMS/ETCS?

A: UNISIG is one of the recognised stakeholders participating in the Working Group updating the Technical Specifications for Interoperability to enhance the robustness of ERTMS to cyber threats.

Q: Can you please link to the standard definition or recommendation about PKI "cross-certification" to ensure interoperability in ERTMS for digital identity protection?

A: This point needs to be discussed in a specific Working Group before being endorsed as a technical solution.

Q: Why public transport (namely metro/subway networks) are not essential service?

A: It is up to the Member state to identify these means of transport as essential. In fact, a few Member States have distinguished metros, tram and other light rail services (including underground services) as essential services under the rail transport subsector.

Q: Where can we find this ENISA report?

A: The ENISA report on cybersecurity can be found at: https://www.enisa.europa.eu/publications/railway-Cybersecurity

Q: TS50701 is very relevant in a system standpoint, however it doesn't cover Cybersecurity of product lifecycle, Do you plan to write a similar standard for all the secure development of a product/software for railways (including supplier requirements when you are an important manufacturer company, and the relation it may have with TS50701) ?

A: ERA is taking consideration of the developments on railway cybersecurity standards. This question should actually be better addressed to CENELEC.

Q: Does the 4th railway package prevent cooperation between RUs and IM in cybersecurity ?

A: The 4th Railway Package does not elaborate on cybersecurity. ERA is concerned about this topic to ensure that cybersecurity has no adverse effect on Railway Safety and Interoperability. Clear definition of the responsibilities and clear technical requirements for technical interoperability should ease the cooperation between RUs and IM.

Q: Have you considered / discussed the use of new EUCC Scheme for critical products with High Assurance requirements in the critical elements of railway industry ?

A: The EUCC Scheme applies to ICT products. Further analysis would be needed in order to apply the scheme to other sectors.

Q: How is the status of the TS 50701? when will it be published? Does it consider the risk approach to the railways?

A: The CENELEC TS 50701, where the link between the cybersecurity risk assessment and the safety risk assessment is described, should be available mid-2021.

Q: Having into account many Agencies, bodies are involved in cybersecurity in railways/transport, which authority is leading the whole cybersecurity topic for the sector?

A: ENISA is the competent authority for the Network and Information Security Directive and ERA is the competent authority for the Railway Safety and Interoperability Directives. A strong cooperation between the two agencies ensures that the railway sector can rely on sound requirements to tackle cybersecurity.

Q: Dear Colleagues, based on your knowledge, what is the most probably source of possible cyber danger requiring respective cyber security measures? Is it predominantly internal issue within closed railway systems (e.g. operation of RBC, etc.), or rather external, (non) intentional intervention into railway system functioning?

A: A detailed threat analysis for the railway sector has not been conducted yet. ENISA has recently published the 8th annual ENISA Threat Landscape (ETL) report, identifying and evaluating the top cyber threats for the period January 2019-April 2020. For more railway specific information, the ENISA report on Railway Cybersecurity lists known cybersecurity incidents in the sector. Until now, these attacks target the IT railway systems (e.g. Ransomware, DDoS, Phishing, Malware, Data Theft) and they match the top threats observed in the ETL report.

Q: What, if any checks should be undertaken on train systems when rail vehicles end their lease with one operator, and are then released to another operator? It could be that the original operator's systems have been unknowingly compromised and this is passed on to the second operator?

A: CENELEC TS 50701 should provide a good overview of the responsibilities of the different actors involved.

Q: Are Cybersecurity activities aligned outside the European border as well and how?

A: ENISA and ERA being EU Agencies are focusing on the EU stakeholders.

Q: EIM (railway infrastructure managers in Europe) would like to know how ENISA and ERA foresees the balance between ad-hoc cybersecurity solutions for specific railway solutions (i.e. ERTMS) and the off-the-shelf solutions dealing with cybersecurity.

A: The purpose of introducing cybersecurity requirements in the railway regulatory framework is to ensure a harmonised implementation of railway Safety and Interoperability. Some off-the-shelf solutions might not fall under this framework and more freedom for implementation can be foreseen. At the same time ENISA is supporting the development of certification schemes that could be considered for such solutions.

Q: When are the affected TSI and CSM regulations foreseen to be published?

A: For the methodology part to be better consider in the Common Safety Methods, it depends on the publication of the CENELEC TS 50701 (scheduled mid 2021) / For the technical solutions to be included in the Technical Specifications for Interoperability, it depends on the availability of Shift2Rail/UNISIG inputs: the first TSI to include enhancements could be the CCS TSI in 2022..

Q: Is there any estimate of how much cost cybersecurity adds to different systems (signalling, telecoms, energy, onboard computer, etc.)?

A: At the moment, a study quantifying the costs of cybersecurity solutions on the different railway systems is not available. ENISA is currently conducting a study on overall cybersecurity investments in the EU.

Q: Why TS 50701 does not cover radio communication devices within network zones?

A: Such detailed technical requirements should be defined directly at the telecommunication solutions level, i.e. either UIC EIRENE or FRMCS specifications.

Q: You showed that Log correlation is an immature area. Does it mean that as of today Railway operators are not using SIEM/SOAR systems at all or that the used solution haven't got enough railway specific intelligence or are focused on IT as opposed to OT?

A: From the answers received in the study, the lack of expertise and resources are identified as the main obstacle. This finding is even more pronounced for OT systems, managed more generally by IMs.

Q: Is there a possibility that 2022 TSIs will include specific cybersecurity elements within eg CCS, or elsewhere - there have been a couple of mentions at events of a potential "CEF digital"?

A: ERA received indications from UNISIG that a new Subset should be received as an input for the update of the CCS TSI in 2022.

Q: Do you have any recommendations with asset owners struggling with securing remote access and the impacts on OT?

A: No at the moment. This should be further analysed.

Q: Any directive or guideline for the setup of Cyber Security Operations Centre for Railway ??

A: ENISA is about to publish a good practice guide and information repository for setting up and improving Computer Security Incident Response Team (CSIRT) and Security Operations Centre (SOC). It is expected to be published on December 2020. It will not be a railway specific guidance, but it will contain good practices applicable to all sectors.

Q: ENISA's study points out some areas of improvement, but I don't see the "need to improve cooperation" as an important are of improvement. What is your opinion on it?

A: Cybersecurity is a shared responsibility. Both ENISA and ERA are committed to strengthen collaboration between the two agencies and with railway stakeholders.

Q: Skills and expertise within the industry was mention as one of the challenges. How is the sector working to equip itself with the technical expertise required to tackle the evolving cyber security threat?

A: The sector is already addressing this challenge by recruiting experts having both knowledge on railway

and cybersecurity, and/or developing internal trainings.

Q: When is TS50701 available?

A: The CENELEC TS 50701, where the link between the cybersecurity risk assessment and the safety risk assessment is described, should be available mid-2021.

Q: I propose to have a technical webinar and continue the discussion

A: A series of online conference jointly organised by ENISA and ERA on 16th and 17th of March will go deeper into the technical aspects.

Q: The most initiatives concerned to safety of the “front-side” what is already necessary. But the most incidents for the Railway sector (Datacentre, ioT, Cloud etc..) come from the “back-side” non-safety fields. How are these fields covered without parallel measures?

A: ENISA considers that cybersecurity measures should be applied to all railway systems following a risk based approach. The report we presented considers a minimum set of security measures that should apply to all systems that support essential railway services, regardless whether these systems are safety related or not. For the IT systems however, there are multiple good practice guides and standards to be applied. For the OT (safety related) ones, there is a gap and this is why the discussion highlighted this aspect.

Q: What is ERA/ENISA opinion on the pace of development de the ER-ISAC? Is it adequate or slow?

A: ER-ISAC is doing quite well considering its young age. ERA and ENISA continue to provide support to the ISAC to develop further. The recently published ENISA ISAC-in-a-box tool is one example of this support.

Q: What is the support that ENISA offer to the manufacturers/developers of automation/hardware equipment and software for the railway field?

A: ENISA supports the NIS directive implementation in the respective sectors. To this end, it engages with the national competent authorities and with the operators of railway essential services (via the ER-ISAC). ENISA has also recently started communications with UNIFE to engage further with the railway industry.

Q: Is SIEM a must to railway?

A: We can only recommend high level security measures and cannot endorse specific technical solutions.