【欧州】【鉄道】

Road/Railways - Cyber security of railways: 4SECURail Consortium selected for developing process and tools to achieve coordinated railway cybersecurity for European railways

Andrea Antolini Former Researcher JTTRI

【概要：Summary】

The transport sector and the entire transport supply chain remains exposed to all forms of security threats, including the risk of terrorist attacks and cyber crime. Therefore, it is important to ensure a coordinated EU approach on transport security to establish and maintain security standards. In the past years, security has become one of the political priorities of the European Commission, due to the fact that terrorist activities pose a serious and acute threat to the security of the EU, its Member States and their transport systems.

Railway infrastructures have become more connected by the internet and are also increasingly connected with other transport infrastructures. Furthermore, new passenger-centric services are introduced. The heterogeneous nature of rail systems make them vulnerable to attacks and it also poses new opportunities for cyber-criminals and terrorists. This situation leads to an increased exposure of the rail systems to new threats within the Internet of Things (IoT). Therefore, it is important to aim for specifications and recommendations to securing the modern rail systems. Exchange of experiences and best practices are crucial. While it is important to maintain or improve the security for transport users, it is also important that security is not so intrusive as to hamper travelling.

New technologies can assist in developing smooth high-security systems for the future by reducing the duration and intensity of security checks.

In January 2020, the 4SECURail project was officially launched in order to improve interoperability and safety for signalling systems, along with measures to deliver processes and tools for the coordination and improvement of cybersecurity response for European railways.

【記事：Article】

1. Latest initiatives to achieve a Security Union

On 30 October 2019, the European Commission published its progress report on the initiatives taken in some important areas of the Security Union of the European Union. The initiatives include considerations on measures to fight against terrorism, improve information exchange, countering radicalisation and cybersecurity. The report showed the progress made in the past years towards achieving an effective and genuine Security Union. The

Commission's Communication "Twentieth Progress Report towards an effective and genuine Security Union" (COM (2019) 552 final) of 30 October 2019 concluded that further efforts are still required, in particular regarding the actual implementation of EU security legislation. In the context of the terrorist attack in Christchurch, New Zealand in March 2019, the Commission also recommended to open negotiations with New Zealand on the exchange of personal data with Europol to fight serious crime and terrorism. The Commission adopted a request for authorisation to launch these negotiations for an agreement between the EU and New Zealand on the exchange of personal data.

The 20th Progress Report also provides an update on the implementation of agreed measures on cybersecurity of Fifth Generation (5G) networks, in particular on the EU Risk Assessment Report and on countering disinformation. The report identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) and a number of strategic risks. This assessment provides the basis to identify mitigation measures that can be applied at national and European level.

This report also focuses on the external dimension of the cooperation in the Security Union and on the progress made in the cooperation with third country partners on the exchange of passenger name record data, in particular, with the signing of two bilateral counter-terrorism arrangements with Albania and the Republic of North Macedonia.

The report sets out the recent progress made and a wide range of measures that the EU has been taking to address common threats in Europe and highlights areas where further action is needed. The EU has worked to counter terrorism with new rules making it harder for them to access explosives, firearms and financing, and to restrict their movements. The EU has stepped up information exchange to provide those on the frontline, police and border guards, with efficient access to accurate and complete data. Strong protection of the external borders is a precondition for security in the area of free movement without internal border controls. In March 2019, the European Parliament and the Council reached agreement on a further strengthened and fully equipped European Border and Coast Guard. The EU has provided a platform and funding for those working in local communities to exchange best practices on countering radicalisation and preventing violent extremism, as well as proposing new rules to effectively remove terrorist contents online. The EU has also addressed cybersecurity and cyber-enabled threats by putting in place a new EU cybersecurity strategy and adopting relevant legislation, and tackling disinformation to better protect elections in the EU. Regarding cybersecurity, the EU has significantly enhanced its cyber resilience and is now working to strengthen the security of the digital critical infrastructure, including reinforced cooperation on the cybersecurity of 5G networks across Europe. The 5G networks is the answer to the needs of increasingly digitised economies and societies, including in critical sectors such as energy, transport, banking, and health, as well as industrial control systems carrying sensitive information and supporting safety systems. Ensuring the cybersecurity and resilience of 5G networks is therefore essential.

The Commission also calls on the European Parliament and the Council to reach swift agreement on all pending legislative proposals on security information systems, including the technical implementation of European Travel Information and Authorization System (ETIAS) and the strengthened Visa Information System.

One specific area requiring further attention is the increasing security threat posed by drones, regarding critical infrastructure and public spaces. Complementing recent EU legislation on safe drone operations in manned airspace, and without undermining the opportunities for the beneficial use of drones, the Commission supports Member States in tracking trends in the malicious use of drones and facilitating the testing of counter measures.

2. Transport and railway security in the EU

While transport operators and authorities in the EU have been providing solutions to tackle safety risks for a long time, new and appropriate responses on security risks need to be found, as security affects all transport sectors, operators and users.

In the transport sector, security can cover anything from terrorist attacks to the prevention of vandalism. The European Commission's role is to consider measures to improve transport security at EU level. Currently, 26 million passengers board European trains every day, with rail travel projected to increase by around 80% by 2050. Protecting rail users, workers and infrastructure from ever-evolving security threats is a crucial and on-going challenge. European rail transport needs a modern rail security system that is based on risk assessment, and that allows a prompt and proportionate response to emerging threats whilst keeping rail services easily accessible. The challenges for railway security are multiple, as the railway systems are geographically dispersed and heterogeneous, which makes them more vulnerable to attacks. At the same time, railways have a limited cyber-protection and cyber-defence set of tools and practices. The collaboration with other transportation infrastructures increases the number of points for attack, while new passenger-centric services may expose rail systems to threats within the Internet of Things (IoT) environment.

After the terrorist attacks in Belgium and the attempt of an attack on a Thalys train to Paris in August 2015, security control measures have been also installed for users of Thalys (to France) and ICE trains (to Germany). However, while a general introduction of lock systems have been rejected in order not to threaten the freedom of movement, the Salisbury attack in March 2018 has demonstrated the threat that terrorists could utilise chemical, biological, radiological and nuclear substances in potential attacks on the EU's transport system. Furthermore, the terrorist risk for rail transport remains significant and any gap in the protection of rail passengers, notably cross-border rail passenger services, could be exploited.

In the EU, the Eurostar train between the UK and continental Europe is tightly controlled, mainly due to the fact that the UK is not part of the Schengen area. In the rest of Europe, only Spain and Italy are known to have security checks for long-distance trains, or conduct occasional random inspections upon boarding. Belgium enhanced security on international trains by installing x-ray scanners and metal detection security gantries in the Brussels South, Antwerp-Central and Liège train stations. However, since EU Member States consider that their rail networks are largely a domestic issue, it is more than ever necessary to consider security measures at European level. This is because measures introduced unilaterally by individual Member States could create barriers in the cross border transport of passengers within the EU. Measures introduced by individual Member States without upstream coordination could create barriers and generate costs in terms of longer travel time,

cancellations and overcrowded access to railway hubs. There is a need for equivalent levels of security for EU rail passengers across borders and transport operators. Measures at EU level to ensure cross-border coordination of all actors involved can contribute to consistent security protection across the EU. In order to deliver an increased level of security, while keeping European railways accessible and open for passengers and preventing unnecessary barriers to the internal market, Member States should improve information sharing and raise the level of awareness, preparedness and capacity to respond to terrorist incidents.

At EU level, the Commission proposed the establishment of a EU Rail Passenger Security Platform. The Platform was created by a Commission Decision on 29 June 2018 (2018/C 232/03 of 3 July 2018) in order to create an effective cooperative environment and propose recommendations to help Member States coordinate rail security actions efficiently. The Platform's task it to assist the Commission in relation to the implementation of existing Union legislation, programmes and policies. It will provide support in collecting and exchanging vital information on rail security, on optimising the security of cross-border rail services and defining a coordination mechanism to avoid unilateral decisions at national level. In addition, in close coordination with the Member States, the European External Action Service and relevant agencies, the Commission will set up annual activities, testing the efficiency of this mechanism in different scenarios.

3. The European Commission's railway security action plan

Railway infrastructures are moving towards more intelligent, connected, user-centric and collaborative systems. While this development brings many advantages for the industry and users, it also poses new opportunities for cyber-criminals and terrorists.

Since most railway operations focus more on core functionality and affordability, perhaps one of the most significant challenges is to achieve a high level of cyber-security. The cyber-security challenges and related threats in the railway sector are steadily increasing and they are not specific to technical attacks and not restricted to malware and viruses. In the railway sector, there are several pressing issues surrounding cyber-security governance, including security operations risk management and compliance monitoring activities that require near-constant attention to be able to maintain a reasonable level of maturity.

Considering the necessary actions to improve passenger rail security, the European Commission published the Fifteenth Progress Report towards an effective and genuine Security Union COM (2018) 470 final on 13 June 2018. The Commission aims at preventing possible attacks by establishing a new cooperation and coordination framework and by making recommendations to the EU Member States to coordinate rail security actions efficiently. One part of the Action Plan was to establish a EU Rail Passenger Security Platform. The Commission adopted the decision to launch the Platform on 29 June 2018. The Platform will be composed of experts from Member States and will facilitate information sharing and expertise at European and national level. The EU Rail Passenger Security Platform's activities aim at providing the Commission with advice and expertise on matters relating to the security of rail passengers in the European Union in train stations and on board trains, as well as at facilitating coordination and cooperation with and between Member States in that regard. It is expected to play a key role in the effective exchange of vital information on rail security at EU level and to provide good

practice guidance for EU Member States. In order to implement its activities, the Expert Group meetings take place four times per year. It will also help EU Member States and rail stakeholders build a mechanism to quickly assess new threats and security incidents, and to undertake an appropriate coordinated response. The European Commission will report to the European Parliament and to the Council on the implementation of the Action Plan.

4. New consortium 4SECURail selected for achieving railway cyber-security

Meanwhile, a consortium consisting of seven European specialist partners from Spain, Italy, the Netherlands and France have been selected for the delivery of the 4SECURail project, which receives funding from the Shift2Rail Joint Undertaking (JU) under the European Union's Horizon 2020 research and innovation programme. The Shift2Rail is a European rail initiative that mainly focuses on Research and Innovation (R&I) and aims at integrating new and advanced technologies through the Horizon 2020 funding for completing the Single European Railway Area (SERA). Under Grant Agreement 881775, the 4SECURail project has a budget of EUR 549,875 and will run for 24 months, from 1 December 2019 to 30 November 2021. The consortium 4SECURail was officially launched in January 2020. The consortium has been selected to deliver a new EU Shift2Rail Programme. The programme of the 4SECURail consortium is coordinated by engineering consulting firm Ardanuy Ingeniería, S.A., in collaboration with Consiglio Nazionale delle Ricerche (CNR), FIT Consulting, Hit Rail B.V., SIRTI, Tree Technology and the International Union of Railways (UIC). 4SECURail focuses on railway cyber security and safety, and it will work to deliver a co-designed collaborative process and tools for the coordination of cyber-security response across European railways. The 4SECURail consortium's main objectives are, firstly, the development of a specific railway-oriented FM demonstrator; secondly, the identification of a railway signalling subsystem, described by means of standard interfaces; and thirdly, the specification and evaluation of the cost/benefit ratio and learning curves for adopting the demonstrator in the railway environment.

The consortium members will work in partnership to deliver the co-design and testing of a model and collaboration platform for a European Railway Computer Security Incident Response Team (CSIRT). CSIRT is designed to coordinate the cybersecurity response actions of the separate railway security teams. 4SECURail addresses the development of a demonstrator for the use of Formal Methods (FM) and collaborative tools to support Computer Security Incident Response Team (CSIRT) in the railway sector. The Formal Methods Demonstrator will provide state-of-the-art Formal Methods (FM) and tools to evaluate the learning curve to perform a cost/benefit analysis of the adoption of formal methods in the railway industry. It is expected to support better interoperability of signalling systems for railway security, safety and efficiency.

The implementation of a Cyber Security Incident Response Team demonstrator in the railway sector intends to define stakeholder requirements for a European Rail CSIRT collaborative activity; to test and validate a CSIRT model for railway; to identify relevant state-of-the-art platforms to support CSIRT collaboration and, based on requirements and CSIRT model, specify and adapt to meet the railway CSIRT needs; and to test and update the CSIRT collaborative environment so as to ensure meeting user needs. The CSIRT will extend the collaboration and will be demonstrated and tested in 2020/2021 to support future consideration of the feasibility of deployment

by the Shift2Rail Joint Undertaking. The Tree Technology is in charge of the CSIRT collaborative platform, leading the development of a Threat Intelligence Platform built on top of existing state-of-the-art platforms for the CSIRTs in the railway sector to share and jointly analyse cybersecurity threats, incidents and information towards enhanced prevention and reaction to cybersecurity threats in the railway sector.

Until November 2021, the 4SECURail consortium is expected to deliver processes and tools for the coordination and improvement of cybersecurity response for European railways.

References

European Commission: EU Rail Passenger Security Platform (E03621). In: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3621, 26 Feb 2020, retrieved 24 March 2020

European Commission: European Commission puts forward action plan to improve security of rail passengers in the EU. In: https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en, 13/06/2018, retrieved 24 March 2020

EU: European Commission Presents Action Plan to Protect Rail Passengers from Terrorist Attacks. In: https://railway-news.com/eu-commission-releases-action-plan-rail-passenger-security-platform/, 18 Jun 2018, retrieved 30 March 2020

European consortium to deliver new Shift2Rail cyber-security programme. In: https://www.globalrailwayreview.com/news/97194/european-consortium-deliver-shift2rail-cyber-security-programme/, 24 February 2020, retrieved 24 March 2020

European specialists team up to deliver new Shift2Rail cyber-security programme. In: http://www.travelandtourworld.com/news/article/european-specialists-team-deliver-new-shift2rail-cyber-security-programme/, February 25, 2020, retrieved 24 March 2020

https://ec.europa.eu/transport/themes/security_en

FORMAL METHODS AND CSIRT FOR THE RAILWAY SECTOR. 4SECURAIL. In: https://cordis.europa.eu/project/id/881775, retrieved 30 March 2020

Jacob, Marc: Seven partners set to deliver new Shift2Rail '4SECURail' project for railway cybersecurity and safety. In: https://www.globalsecuritymag.fr/Seven-partners-set-to-deliver-new,20200224,96039.html, February 2020, retrieved 30 March 2020

Security Union: European Commission presents the Twentieth Progress Report. In: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6171, 30 October 2019, retrieved 28 March 2020

Seven partners set to deliver new Shift2Rail '4SECURail' project for railway cybersecurity and safety. In: https://www.realwire.com/releases/Seven-partners-set-to-deliver-new-Shift2Rail-4SECURail-project-for-railway, 24 Feb 2020, retrieved 24 March 2020

Seven partners set to deliver new Shift2Rail '4SECURail' project for railway cybersecurity and safety. In: https://digitalisationworld.com/news/58613/seven-partners-set-to-deliver-new-shift2rail-4securail-project-for-railway-cybersecurity-and-safety, 24 Feb 2020, retrieved 24 March 2020

Seven partners set to deliver new Shift2Rail '4SECURail' project for railway cybersecurity and safety. In: https://uic.org/com/uic-e-news/681/article/seven-partners-set-to-deliver-new-shift2rail-4securail-project-for-railway, 3 March 2020, retrieved 30 March 2020