SAFETY4RAILS Newsletter – April 2022

Message of Stephen CRABBE – SAFETY4RAILS Coordinator

SAFETY4RAILS is a ambitious project with many partners, a short duration, technologies starting with varying level of readiness and extra challenges caused by the COVID-19 pandemic. March 2022 marked the three-quarter point of its duration. Since its start only 18 months ago SAFETY4RAILS has covered much of the ground foreseen on its journey. This reflects the skills, commitment and support of the SAFETY4RAILS multi-disciplinary team, including rail and metro operators. The team completed the requirements, specifications and architecture for the SAFETY4RAILS information (S4RIS) platform, including its contributory tools. Based on this it also carried out the developments, first integrations and planning to enable the initial demonstration of the S4RIS platform in a simulation exercise with Madrid metro in February 2022. A further important stage in the project's journey was the passing of the European Commission's external project review in November 2021.

Currently, SAFETY4RAILS is implementing further developments, extending integration and preparing the next demonstration in Ankara in April 2022. Further demonstrations are planned in Rome and Milan before September 2022. Hand in hand with the demonstration exercises are the evaluations of the project results. In the next months also activities connected with disseminating and preparing the implementation of project results will come even more into focus. We're looking forward to share these results with you later this year.

SAFETY4RAILS Innovation Results

Over the last couple of months, a significant number of crucial developments has been achieved. The list below gives an overview of the most relevant SAFETY4RAILS outputs:

Monitoring Methods for S4RIS – Detection, Forecasting, Response and Recovery:

The partners worked together to develop and improve monitoring components for the S4RIS in terms of detection, forecasting, response or recovery functionalities for cyber-physical vulnerabilities and threats. Blockchain technology as tamperproof shared storage system was investigated for resilience improvements. Holistic situational awareness was addressed by analysing cascading effects and going beyond the view of single events. Common definitions and an automated integration between the S4RIS' monitoring components and the S4RIS' decision support engine was achieved by close collaboration.

Simulation methods – Prevention, Preparedness and Risk Mitigation

The Work package dedicated to the Simulation methods contributed to the MDM simulation exercise through the presentation of various tools especially in the 'prevention phase' of the scenario. The iCrowd tool by NCSRD simulated passengers trapped in the impacted metro station and predicted critical passenger densities with an agent-based approach. The CaESAR simulation environment by Fraunhofer presented the results of impact propagation in the MDM metro grid along with criticality of stations, resilience assessment and the comparison of some initial mitigation measures.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.

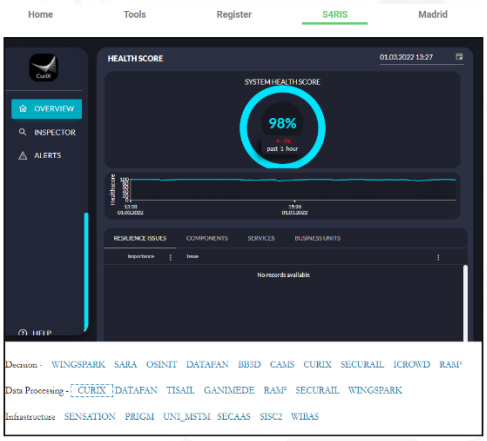
Policy Planning and investment measures of prevention-detection-response mitigation

In the S4RIS platform, CAMS (Central Asset Management System) acts as a financial tool. Within the project, some new features have been introduced and also tested during the MDM simulation exercise. The railway module is now part of the tool, which has been expanded to asset classes belonging to the railway environment and to digital and soft assets. The tool presents an outcome in terms of the predictive cost in normal degradation condition (prevention phase) and in case of emergency repairs (recovery phase). It helps to move from past practice based on reactive year-to-year planning to a new philosophy of predicting the capital expenditure of deteriorating infrastructure.

The S4RIS Platform core enabling technology:

The core enabling technology to allow for communication between tools has been developed based on web applications. It uses HTML, CSS, PHP and JavaScript technologies. Three platform structures were considered. Based on the project requirements, architecture and usability, the structure that applies an iFrame with three layers was selected to date. It is based on three layers namely: Infrastructure, Data processing and Decision support. Currently, of the 18 tools, 4 are fully integrated. In the next 3 month, all web-compatible tools will be fully integrated.

An important part in the process of integration between S4RIS tools is the definition of tools and technologies that allow intra messaging between various tools in the S4RIS platform. The technology being used for intercommunication in the S4RIS platform is Distributed Messaging System (DMS) based on Apache Kafka. The first step to access the private area S4RIS platform is the registration process. The user must fill a form with login details and email. A secure password is required for the process.



Simulation Exercise Metro de Madrid

The Simulation Exercise was co-organised by Metro de Madrid (MDM) and ETRA on 9-10 February 2022. The event brought together around 60 representatives from the SAFETY4RAILS consortium participating physically in Madrid and online. Among these participants, representatives from 8 end-users were attending: MDM (Metro de Madrid), EGO (Ankara Metro), RFI (Rail Infrastructure Manager in Italy), PRORAIL (Rail Infrastructure Manager in the Netherlands), TCDD (State Railway in Turkey), FGC (Rail operator in Barcelona) and UIC (the Worldwide Rail Organisation).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.

The main objective of this event was to demonstrate how the SAFETY4RAILS Information System (S4RIS), together with its main tool components, can help rail and metro operators manage a **combined cyber-physical attack** targeting a metro station based on a simulation scenario taking place in Madrid. Even though the attack focused on a specific metro station, S4RIS applied a holistic approach with mitigation measures considering the Smart City paradigm, public authorities, interconnected infrastructures and cascading effects across the whole metro system.

The simulation exercise was organised around resilience stages: **Prevention** (activities performed before the incidents, this includes the combination of the resilience phases identification and protection), **Detection & Response** (activities performed during the incident), **Recovery** (activities performed to ensure MDM services come back to normal operations and improve long-term resilience).

The S4RIS, with a combination of 11 tools addressing the scenario, was demonstrated leveraging operational data relevant to each resilience stage. **13 technical partners**, led by ETRA, coordinated their efforts to tackle novel emerging threats: ETRA, FRAUNHOFER, ELBIT, STAM, TREE, INNO, WINGS, RINA, RMIT, ERARGE, NCSRD, IC, UNEW.

During the prevention stage, the capabilities of 8 tools were showcased:

- BB3d (BomBlast3d): the tool provided bomb blast simulation to evaluate out-door bomb blasts and how they affect buildings and metro structures. This is intended to help the experts from the civil construction department for building more resilient physical structures.
- CAMS (Central Asset Management System): Based on maintenance data, CAMS spotted the most damaged assets/components (due to ageing degradation), i.e. the ones which would be most affected from a hazardous event. Assets from both the cyber and physical domain were evaluated. Analysis should improve the preparedness and help proactive planning for the maintenance department.
- SecuRail (Security Risk Analysis of railways infrastructures) was used to perform an off-line risk analysis of the infrastructure in order to understand the risk level of each critical component in the metro system. The results should provide the security managers with information on where and what more attention needs to be paid (e.g., by introducing more appropriate security measures).
- TISAIL (Threat Intelligence Service for the Railway sector) identified existing vulnerabilities in the cyber domain in the railway infrastructure. The tool monitored the network and found vulnerabilities, related to CCTV systems and spear-phishing campaigns. After analysing the threats, extracting some Indicators of Compromise (IoC's) and enriching the information, an alert was created in order to warn Infrastructure Managers about them.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.

- DATAFAN (Data Artificial InTelligence-based Analysis Forecasting and ReliAbility EvaluatioN) was used to run a set of what-if scenarios to understand the flow of passengers in the station, as well as possible delays. This information was then shared in the CAESAR tool, described below, to in order to identify critical stations.
- CAESAR (CAscading Effect Simulation in Areas for increasing Resilience) was used to assist security operators in providing a resilience overview based on the simulation scenario with the unavailability of certain stations and how different mitigation measures could improve the network e.g. by the closing of transportation hubs..
- iCrowd simulated different crowd movement scenarios to optimise camera's location and reduce blind spots in the station during the evasion of a malicious actor. It also generated crowd congestion and pressure levels after an explosion close to a station. For this, bomb blast results generated by BB3d were used (e.g. damage on structures and people).
- RAM^2 (Risk Assessment Monitoring & Management and Decision Support System) provided the security operator with a complete picture of the identified vulnerabilities and security gaps in the infrastructure. Identified vulnerabilities were accompanied with suggested mitigation actions to fix them and increase the resilience level of the metro infrastructure.

During the simulated detection & response stage, several tools enabled **enhanced situational awareness** thanks to the added-value provided by their alerts: TISAIL/OSINT detected a spear-phishing campaign and CCTV camera vulnerability using open internet sources, CuriX (Cure infrastructure in XaaS) detected anomalies in the sound intensity levels, in the state of the doors, electrical energy consumption and also malware operating patterns on the system, WINGSPARK (WINGS Big Data and Predictive analytics tool) detected anomalies in train speed and identified overcrowded areas, DATAFAN detected an anomaly regarding the passenger flow in the station.

All events were presented to the operator in the S4RIS (RAM2 GUI), where correlation between existing and incoming alerts were performed and details of the alerts presented. The Security Coordinator received the warnings and took immediate action, supported by the **advanced crisis management** capabilities of S4RIS Decision-Support System (RAM2).

During the response stage, the tools helped to decide which stations should be closed, considering the trade-off between security and business continuity. Based on station closures, DATAFAN was used to inform the mitigation engine (CAESAR) regarding the predicted change in passenger flow in real-time, taking into account passenger load for surrounding stations. CAESAR produced a ranking of best mitigation measures based on cascading effects computation, which helped the security operator decision-making.

For the impact analysis, iCrowd provided estimates of the consequences of the incident on the passengers, leveraging the information regarding the passenger flow in the station and the status of key assets affecting mobility (e.g. doors, turnstile...).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.

Finally, during the recovery stage, S4RIS evaluated (through CAMS) the fragility of physical and IT assets after the incident. This allowed the operators to define budgetary measures to improve resource deployment and control financial loss in the future. Furthermore, BB3d informed the civil construction department to create countermeasures to improve the resilience of structures – such as protective hardening, safety distance.

These 2 days were very fruitful and very useful for the end-users to understand the possibilities of the tools and the added value of their combination and integration in the S4RIS platform.

The next exercise will be focused on the Ankara metro operator – EGO - organised by ERARGE (R&D Centre in Istanbul) with EGO and the support of TCDD (State Railway in Turkey) in the second quarter of 2022. In the meantime, feedback from the end-users will help to improve the tools and take a further step with another set of operational data and even more tools integrated in S4RIS platform.

Workshops with the end-users and the members of the advisory board

During the period, SAFETY4RAILS organised 3 workshop gathering security experts from railways and metro companies, authorities, an EU agency as well as ethical experts. The workshops gave the opportunity to exchange views on the results and get feedback from the end-users with the objective to ensure that solutions developed within SAFETY4RAILS meet their needs and requirements.

The first workshop held on 14-15 December focused on understanding current threats faced by railways and metro stakeholders.
The second workshop held on 15 March 2021 focused on validation and prioritisation of end-user requirements for the S4R Information System.

The third Project workshop held on 29 April 2021 focused on specific requirements for inter-city and intra-city railway and metro systems. The workshop was composed on three sessions: crisis management, crisis communication towards the public and resilience of transport hubs from the Smart city point of view.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.

Past events:

SAFETY4RAILS has contributed to shaping policy related to the protection and resilience of critical infrastructure by participating to a number of high-level events and international conferences:

Conference name	Location and date	Audience
UIC Cyber Security Solutions platform	Online, 08/02/2021	Railway Cybersecurity experts
EU Rail Passenger Security platform	Online, 16/02/2021	European Transport authorities
ER-ISAC General Assembly	Online, 26/02/2021	Rail Cybersecurity experts
Project to policy kick off seminar (P2PKOS) for security research organised by REA	Online, 22-23/03/2021	Policy makers, 33 EU projects representatives
CERIS DRS Workshop Multi hazards disaster risk management organised by DG HOME	Online, 05/05/2021	Policy makers, industry, research centres
4SECURAIL workshop	Online, 08/06/2021	Rail Cyber security experts
UIC Security platform - Meeting of the SIA (Sabotage/intrusion/attack) working group	Online, 06/05/2021	Railway Security experts
CERIS DRS Synthesis & InfoDay organised by DG HOME	Online, 14/06/2021	Policy makers, industry, research centres
Workshop organised by KEMEA to Greek security companies	23/06/2021	Policy makers, industry, research centres
Meeting DG MOVE SECURITY/ EOS (IBS and ST CIP WG)	Online, 10/09/2021	Policy makers, industry
14th IWGLTS Annual Meeting 2021 (International Working Group on Land Transport Security)	Online, 29/09/2021	Policy makers
ER-ISAC General Assembly	Online, 30/09/2021	Rail Cybersecurity experts

Next steps

Monitoring Methods – Detection, Forecasting, Response and Recovery

Conclude with last implementation and integration efforts of the monitoring components to the S4RIS.

Simulation methods – Prevention, Preparedness and Risk Mitigation

The next steps and the mentioned tools involve the preparation of upcoming exercises. Further, additional communication channels through the DMS will be defined and established between the tools, such as between iCrowd and CaESAR. Also, more mitigation measures will be considered in the predictive simulation environments to enhance the decision support.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.

Policy Planning and investment measures of prevention-detection-response mitigation

As the next steps for CAMS, to make the analysis even more accurate, the incident intensity measure will be introduced in the system. The event intensity measure, combined with the current condition of the asset will give a more precise asset condition rating post-event and, consequently a more accurate budget estimation.

Next Simulation Exercises:

April 2022: Ankara (EGO and TCDD) Series of cyber-attacks and physical attacks targeting sensitive devices and sensors.

June 2022: Roma (RFI) Physical attack – Potential terrorist attack via IED carried via baggage or by a terrorist using firearms inside a railway station.

July 2022: Milan (CDM) Natural Disaster - Flooding in the city during a major event.

Upcoming events

The SAFETY4RAILS final Conference will be held on the 28th of September 2022 at UIC headquarters in Paris.

List of public deliverables available on the website

D2.2 Report on pas failure analysis and lessons learnt

D2.3 System's specifications

D2.4 System architecture

D3.3 Definition of the interface between RA tool and S4RIS

D4.3 Cyber-physical threat detection with capabilities matrix intelligence

D9.1 SAFETY4RAILS Ethical Compliance Framework (ECF)

D10.1 Dissemination and Communication Plan

D10.2 First update of the dissemination and communication plan

D10.4 Project Brochures – first version

D10.5 Project Brochures – second version

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883532.