SAFETY4RAILS Newsletter – August 2022

### *Message of Stephen CRABBE – SAFETY4RAILS Coordinator*

SAFETY4RAILS is now in the last stage of its journey with its completion on 30 September 2022. Since our last newsletter, most technical development work packages have come to an end and there has been a focus on testing and evaluating the SAFETY4RAILS Information System (S4RIS) platform with its contributory tools in three further simulation exercises with end-users. An overview of these exercises is a core part of this newsletter. The contributory tools which were evaluated in each exercise depended on the original scenarios proposed by the end-user hosts together with their extension, where necessary, to cover those tools committed to be tested by their providers. Where possible, iterative developmental and organisational updates were implemented between the exercises. By reaching the last quarter of the project, we also had more mature content for scientific publications; those produced to date are listed later. Now, we look forward to our Final Conference to be hosted by the International Union if Railways (UIC) on 28 September 2022 in Paris, France and to the closing of the remaining project deliverables. SAFETY4RAILS has overall sixty five project deliverables. Details on the conference and those public deliverables already available come later. Further deliverables will become available following their acceptance through the European Commission's procedures. All of this has been made possible through the skills and continued commitment and support of the SAFETY4RAILS multi-disciplinary team.

SAFETY4RAILS Simulation Exercises

Following a successful first simulation exercise in Madrid in February 2022, the SAFETY4RAILS consortium held three more simulation exercises in the past few months to test the functionalities of the S4RIS platform and its main tool components to support the increase in security and resilience of rail and metro services and transportation services more broadly.

Ankara Simulation Exercise: 27-28 April 2022

The second SAFETY4RAILS simulation exercise was co-organised by ERARGE, EGO and TCDD based on a scenario in Ankara, Turkey. The event was organised online, due to travel uncertainty caused by the conflict in Ukraine, on the 27th and 28th April 2022 with 58 representatives from the SAFETY4RAILS consortium.
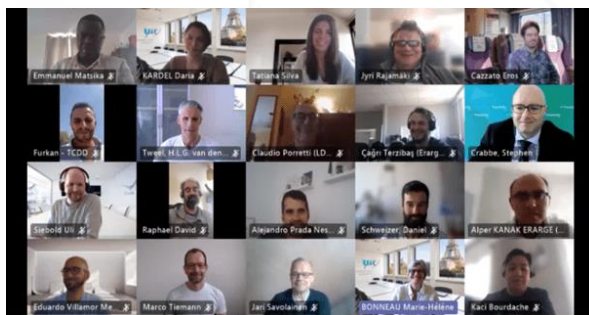
The main objective of this event was to demonstrate and evaluate the functioning of the latest version of the S4RIS platform with its contributory tools, based on a scenario of a combined cyber-physical attack on a metro station in Ankara. The simulated attack was designed around two key events: an intrusion in an important room leading to a cyber-attack and the explosion of a luggage abandoned by a terrorist.

The simulation exercise required technical capabilities to address the four stages of the resilience cycle (prevention (combining identification and protection); detection; response; recovery) and involved 9 tool providers:

- CAMS (Central Asset Management System): based on maintenance data, the tool helped to identify the most damaged assets/components of the metro system (due to ageing and degradation and also following the simulated attack). During the Ankara scenario, CAMS showcased the most affected assets, from both the physical and the cyber domains.

- iCrowd: the simulation-based situational awareness tool provided prediction of different crowd movements and behaviours in the metro station and therefore helped to detect hazardous situations, bottelnecks and malicious movements as well as to analyse risk mitigation measures. Focusing on the prevention and recovery phases, the tool identified possibilities for analysing improved CCTV systems positioning and improved evacuation routes.

- SecuRail (Security Risk Analysis of railways infrastructures): aims to support railway infrastructure managers to perform quantitative risk assessment of each critical component in the metro system in a simplified and structured manner. At the Ankara scenario, it performed an off-line risk analysis of the infrastructure. The results identified capabilities on offer to security managers in the prevention stage by providing information on which components and processes would be priorities for attention.

- CAESAR (CAscading Effect Simulation in Areas for increasing Resilience): the software was demonstrated showing capabilities to assist security managers in evaluating and mitigating the potential impact of cascading effects in their service network through the closure of a metro station.

- DATAFAN (Data Artificial InTelligence-based Analysis Forecasting and ReliAbility EvaluatioN): was used to identify the number of passengers which would be expected to be using a (closed) metro station for a given time period and the capacity for surrounding stations to take-up these extra passengers due to the initial station's closure.

- TISAIL (Threat Intelligence Service for the Railway sector) /OSINT (Open-Source Intelligence): uncovers potential threats from different services and the cyber domain in a semi-automatic manner. After analysing the threats, some Indicators of Compromise (IoC's) are extracted to enrich the information. On this basis, an alert is then created to warn infrastructure managers, railway undertakings and other SAFETY4RAILS tools. In the simulation, the risk of unauthorized access to a CCTV camera model was identified, as was a social media message reporting an explosion.

- CURIX: offers a holistic approach to prevent outages, predict critical phenomena and increase resilience in IT Operation and IT Security. During the exercise, CURIX detected the drop in the electrical power consumption (due to the terrorists manipulating an important system), which in turn triggered an alert to the security operators during the detection and response phases.

- PRIGM-SENSATION: the hardware security module was used to ensure that secure communication channels be established between physical data sensors and control centres. Connected to the SAFETY4RAILS interoperability architecture during the exercises, it enabled

the integrity of the data transferred and the detection of an intrusion to the important room through various sensors.

- GANIMEDE: as a platform used for the management of video/audio content analysis (using artificial intelligence and deep learning), it was mobilized during the scenario to provide an algorithm capable of detecting the presence of unattended objects through CCTV cameras. As it can detect and report the presence of abandoned objects, this tool is used for the purposes of detection and response phases of an incident.

During the **detection and response phase** of the simulation, several tools provided information to create situational awareness: Ganimede detected an abandoned luggage and raised an event of it, PRIGM – Sensation detected the intrusion to the important room by checking various sensors, and TISAIL/OSINT discovered the exposed CCTV and sent the event to S4RIS. CuriX detected the drop in the electric power consumption and created an event. TISAIL/OSINT also generated a social media message report regarding a reported explosion. DATAFAN performed a passenger flow analysis of the connected stations to detect possible anomalies.

The events raised 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 alerts and demonstrated immediate action to take, supported by the advanced crisis management capabilities of S4RIS Decision-Support System (RAM2).

The entire simulation was created to demonstrate the capabilities of the tools, considering actual and/or potential security threats and their combinations. However, it was not based on any previous or actual operational event(s) occurring within the organizations involved in the simulation.

After the conclusion of this exercise, end-users provided feedback to help to improve the tools demonstrated and reach a new step with another set of operational data and additional tools integrated in S4RIS platform.

Rome Simulation Exercise: 31 May – 1 June 2022

The third SAFETY4RAILS simulation exercise was organised by LDO (Leonardo) and hosted by Rete Ferroviaria Italiana (RFI) in Rome (Italy) on 31st of May and 1st of June 2022 with the participation of

around 50 representatives of the SAFETY4RAILS consortium and its Advisory Board.

The objective of this event was to demonstrate the latest version of the S4RIS platform, based on the scenario of a combined cyber-physical terrorist attack at a major Rome train station during a time with many passengers in the transport system. In this scenario, the attack began with an attempted DoS attack against the station's CCTV system. In addition to this cyber-attack, two terrorists also planted and attempted to detonate an Improvised Explosive Device (IED) inside the station and open fire against civilians.

The exercise began with a short presentation of the importance of SAFETY4RAILS for RFI's corporate security actions, followed by an overview of the project's objectives, system architecture and

capabilities provided by the Project Coordinator. LDO then gave a detailed presentation of the scenario, and the 9 tools involved in the simulation exercise across the four stages of the resilience cycle (prevention (combining identification and protection); detection; response; recovery).

Individual tool demonstrations took place across the resilience cycle, while a joint tools simulation exercise was also carried out for the detection and response phases based on the RFI scenario.

In the **prevention and recovery phase**, four tools were demonstrated:

- TISAIL: identified vulnerabilities in CCTV cameras, including a DoS vulnerability that might be exploited by a remote administrator. It provided intelligence about BotenaGO, a new malware targeting IoT and CCTV cameras.
- DATAFAN: provided information on the expected number of passengers for the station and its surrounding stations during an event of high crowd concentration.
- CAESAR: based on a grid representation of the metro network, simulated various what-if scenarios, the tool identified critical stations which could be impacted by critical combinations of threats.
- CAMS: evaluated the optimal resource deployment and financial loss control during the recovery phase based on information related to assets' final damage conditions and cost.

During **the detection and response** phase, six tools were employed:

- CuriX: detected the DoS attack against the CCTV system and raised an alarm.
- GANIMEDE: analysed video and audio sources to detect abnormal audio patterns (e.g. a gunshot) and unattended objects in a dedicated area targeted by video surveillance and raised alarms. Its algorithm also assisted with people "re-identification", reporting all the occurrences of match to assist in the detection of the attackers' location.
- SC2: as a crisis communication tool, it visualised the video analyses made by GANIMEDE and the related detection alarms and provided these alarms for further correlation in the platform.
- WINGSPARK: used CCTV input to estimate train speed anomalies, as well as crowd concentration in the station. When crowd density exceeded predefined thresholds, an alarm was raised.
- DATA FAN: provided information on the expected number of passengers for the time of the attack in the station and its surrounding stations in order to support RFI staff to re-direct the passengers according to the free capacity of the surrounding stations.
- RAM2: displayed all the alarms raised by other tools and prioritised proposed mitigation action items according to the relevant business context.

The latest version of the SAFETY4RAILS Information System (S4RIS) and its user interface were also presented. The S4RIS platform combines the different SAFETY4RAILS tools and their capabilities, also including a description of the functionalities of each tool.

At the end of the event, participants discussed how to improve the structure of simulation exercises to fully display how the different tools work together, integrated into the S4RIS platform. End-user feedback was also taken into consideration for additional improvements of the tools.

Milan Simulation Exercise: 6 July 2022

The fourth SAFETY4RAILS simulation exercise was co-organised by LDO (Leonardo) and CDM (Comune di Milano). The event took place at CDM premises in Milan (Italy) and online on 6th July 2022 with some 50 representatives of the SAFETY4RAILS consortium and its Advisory Board.

The objective of this event was to demonstrate the fourth version of the S4RIS platform, based on the scenario of a flood taking place during a major event in Milan, leading to of the need to redistribute passengers on city transport. In this scenario, the major flood was caused by torrential rain during the opening ceremony of the Olympic Games. It impacted the level of rivers close to the urban area and flooded metro and train stations – particularly at key interchange points in the city towards the north (Garibaldi station, exchange point between two metro lines, trains, trams and buses). As a consequence, the city's two major metro lines were out of service, leading to the activation of replacement transport lines.

The exercise began with a detailed presentation of the scenario by CDM, including of the city's transportation management and a mapping of systems and relevant stakeholders. The system architecture and specification of the SAFETY4RAILS Information System were then presented by the Project Coordinator. The introductory presentations were concluded by LDO who gave an overview of the foreseen implementation of the simulation exercise.

Several tool providers provided simulations of their tools' capabilities to respond to the scenario. The exercise involved the evaluation of the combination of 8 tools integrated into the SAFETY4RAILS platform.

During the exercise, SAFETY4RAILS partners presented how these tools worked together to assist end-users, that is railway and metro operators, in preventing (combining identification and protection), detecting, responding and recovering from a natural hazard. Tool providers demonstrated how end-users could access the tools in the S4RIS platform graphical user interface (GUI) and how the tools communicated with one another to efficiently support them in dealing with the attack.

In the **prevention phase**, four tools were demonstrated:

- CAESAR: identified critical stations in the Milan Railway network. The collected criticality was displayed on a georeferenced map, and what-if-scenarios were performed to analyse and compare the degradation and recovery of the network as the threat propagated across the network.
- SECURAIL: focused on computing the risk of each element of a sub-section of the Milan Railway network primarily to be affected to provide aggregated results through its dashboard.
- DATA FAN: provided a forecast of passenger loads at the Milan Porta Garibaldi and surrounding stations together with a measure of a reliability of the results with the aim of assisting end-users in redirecting passengers to alternative stations (due to the station's closure), based on their predicted capacity.

- SARA: identified the risk and losses (economic or related to human life) caused by the threat inside the flooded stations.

During the detection and response phase, four tools were also tested:

- WINGSPARK: detected anomalies in metro speed, as well as potential overcrowded areas by analysing camera footage.
- CuriX: identified the anomaly in the monitoring data indicating a blackout of electrical power supply at the Porte Garibaldi station.
- CAESAR: measured the performance of different mitigation options on the metro and rail systems' resilience.
- RAM2: displayed the detection alarms (a simulated flooding sensor, WINGSPARK, CuriX) and results of the simulation to support response actions (CaESAR) and proposed a list of mitigation actions.

During the recovery phase, S4RIS provided accurate information (through the CAMS tool) regarding the costs of recovery of assets involved in the event, considering the level of individual asset damage and cost to repair or replace the asset. A prioritisation for budget allocation was also given based on asset criticality.

To conclude, CDM representatives underlined the importance of an integration mechanism to better manage disrupting events such as flooding with the different transport operators and wider public stakeholders in the city.

The CDM exercise was the last in a series of four simulation exercises of the S4RIS platform conducted over the past six months. The last demonstration of the SAFETY4RAILS tools will take place at the project's final event, on the 28th September 2022 in Paris.

Dissemination and Communication Activities:

Over the past months, members of the SAFETY4RAILS consortium continuously engaged in dissemination and communication activities, promoting the project's activities and simulation exercises across their networks and on social media, updating the website with regular blogs and working on scientific articles and presentations to showcase the results of the project. A list of these scientific publications can be found below.

In addition, SAFETY4RAILS was presented during the European Commission's CERIS workshop on *How research supports the directive on the resilience of critical entities?* (12 July 2022), strengthening relationships with European policymakers and other projects. In addition, an update on the project was given to the LANDSEC (DGMOVE Land Transport Expert Group) meeting held on 07 July 2022.

Scientific Publications:

In the following table there is a list of scientific publications in which SAFETY4RAILS results were the focus or at least provided a contribution.

Author(s)	Title	Conference/Journal
Thomopoulos S. C. A. et al.	Anomaly detection with noisy and missing data using a deep learning architecture (Article)	Proc. SPIE 11756, Signal Processing, Sensor/Information Fusion, and Target Recognition XXX, 117560R (16 April 2021)
Rajamäki J.	Resilience Management Concept for Railways and Metro Cyber-Physical Systems (Article)	21st European Conference on Cyber Warfare and Security (ECCWS) (16-17/06/2021)
Pasino A. et al.	A Review of Single and Multi-Hazard Risk Assessment Approaches for Critical Infrastructures Protection	International Journal of Safety and Security Engineering, Aug 2021
Miller N. et al.	A Risk and Resilience Assessment Approach for Railway Networks (Article)	31st European Safety and Reliability Conference (ESREL) (19-23/09/2021)
Sathya S.U. et al.	Resilience Assessment Models for Benchmarking Rail Bridges Against Natural Hazards (Poster)	12th International Conference on Structural Engineering and Construction Management, ICSECM 2021, Dec 17-19, 2021, Kandi, Sri Lanka
John M.A. et al.	Modelling Cyber-Risk in an Economic Perspective	Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience, Virtual Conference, 2021
Bonneau M., et al.	Protecting railway and metro infrastructure against combined cyber-physical attacks	World Congress on Railway Research, WCRR 2022, Birmingham, 4-6 June 2022
Thomopoulos S. C. A. et al.	3D modeling, simulation and data exchange in cyber-physical threat assessment, multi-biometrics performance evaluation, and risk-based access control (Article)	Proc. SPIE 12122, Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI, 121221E (8 June 2022)
Thomopoulos S. C.A.	NARRATION: a platform for curation and scenario creation with application to vulnerability and risk assessment (Article)	Proc. SPIE 12122, Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI, 121220Q (8 June 2022)
Thomopoulos S. C.A.et al.	Impact assessment and mitigation strategies in rail/metro infrastructure with the use of iCrowd simulator (Article)	Proc. SPIE 12122, Signal Processing, Sensor/Information Fusion, and Target Recognition XXXI, 121221C (8 June 2022)
Siino, G. Et al.	Investment Plan and Resilience Assessment for Railway Bridges Under Extreme Conditions	11th International Conference on Bridge Maintenance, Safety and Management (IABMAS), 11-15th July 2022, Barcelona, Spain.
Crabbe S. et al.	SAFETY4RAILS Information System platform demonstration at Madrid Metro simulation exercise (Article)	32nd European Safety and Reliability Conference (ESREL) (28 August - 1 September 2022)

Roß K.	SAFETY4RAILS = Data-based analysis for safety and security protection for detection, prevention, mitigation and response in trans-modal metro and railway networks	CRITIS2022 Conference https://critis2022.comtessa.org/ross , 14-16 Sept 2022
Srivastava K. et al.	Modelling and Simulation of Railway Networks for Resilience Analysis (Article)	CPS4CIP workshop at ESORICS conference https://st.fbk.eu/events/CPS4CIP2022/, 26-30 Sept 2022
Kopke C. et al.	Methodology for resilience assessment for rail infrastructure considering cyber-physical threats (Article)	CPS4CIP workshop at ESORICS conference https://st.fbk.eu/events/CPS4CIP2022/, 26-30 Sept 2022

SAFETY4RAILS Final Conference

The SAFETY4RAILS Final Conference will be held on 28 September 2022 at the UIC headquarters in Paris, France.

This final conference will showcase the main results of the project, including a real-time joint demonstration and an interactive session with tool providers which will offer participants the opportunity to get a first-hand insight into the tools developed within the project.

It will also feature a session with recommendations and lessons learned regarding policy measures, certification, exploitation and next steps.

The conference is open to external stakeholders involved in rail and public transport security upon registration.

A preliminary agenda can be found below:

9:30 – 10:00 Registration

10:00 – 10:30 Welcome and opening session

10:30 – 11:30 Real time joint demonstration

11:30 – 13:00 Interactive session with the tool providers

13:00 – 14:00 Lunch

14:00 – 16:00 Main lessons learnt, policy recommendations and next steps.

List of public deliverables available on the website

D2.2 Report on pas failure analysis and lessons learnt

D2.3 System's specifications