SAFETY4RAILS Information System platform demonstration at Madrid Metro simulation exercise.

This paper was published in the form of proceedings “Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)” Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson.

doi: 10.3850/978-981-18-5183-4_S06-14-470-cd

SAFETY4RAILS Information System platform demonstration at Madrid Metro simulation exercise

Stephen Crabbe, Katharina Roß, Corinna Köpke, Katja Faist

Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, Germany. E-mail: Stephen.Crabbe@emi.fraunhofer.de, Katharina.Ross@emi.fraunhofer.de, Corinna.Koepke@emi.fraunhofer.de, Katja.Faist@emi.fraunhofer.de

Eduardo Villamor Medina

ETRA, Spain. E-mail: evillamor.etraid@grupoetra.com

Uli Siebold, Eros Cazzato

CuriX AG, Switzerland. E-mail: uli.siebold@curix.ai, eros.cazzato@curix.ai

Anett Mádi-Nátor

Cyber Services Plc., Hungary. E-mail: anett.madi-nator@cyber.services

Eli Ben-Yizhak, Ido Peled

Elbit Systems C4I & Cyber, Israel. E-mail: eli.ben-yizhak@elbitsystems.com, ido.peled@otorio.com

Alper Kanak, Niyazi Ugur, S.Halit Ergun, Salih Ergun

Ergünler Co. R&D Center, Erarge, Turkey. E-mail: alper.kanak@erarge.com.tr, niyazi.ugur@erarge.com.tr, halit.ergun@erarge.com.tr, salih.ergun@erarge.com.tr

Marco Tiemann

Innova Integra Ltd., UK. E-mail: marco.tiemann@innovaintegra.com

Marie-Hélène Bonneau

International Union of Railways, France. E-mail: bonneau@uic.org

Kaci Bourdache, Jari Savolainen

Laurea University of Applied Sciences, Finland. E-mail: kaci.bourdache@laurea.fi; Jari.Savolainen@laurea.fi

Stelios C. A. Thomopoulos, Christos Kyriakopoulos, Konstantinos Panou

National Center for Scientific Research "Demokritos", Greece. E-mail: scat@iit.demokritos.gr, ckyriak@iit.demokritos.gr, kpanou@iit.demokritos.gr

Antonio De Santiago Laporte

Metro de Madrid, Spain. E-mail: antonio.desantiago@metromadrid.es

Emmanuel Matsika, Raphael David

Future Mobility Group – NewRail, Newcastle University, UK. E-mail: emmanuel.matsika@newcastle.ac.uk, raphael.david@newcastle.ac.uk

Emiliano Costa

RINA, Italy. E-mail: emiliano.costa@rina.org

Proceedings of the 32nd European Safety and Reliability Conference
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
 Published by Research Publishing, Singapore
ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_esrel2022-paper

Giulia Siino

RMIT Europe, Spain. E-mail: giulia.siino@rmit.edu.au

Sujeeva Setunge, Mojtaba Mahmoodian

RMIT University, Australia. E-mail: sujeeva.setunge@rmit.edu.au, mojtaba.mahmoodian@rmit.edu.au,

Nader Naderpajouh

The University of Sydney, Australia. E-mail: nader.naderpajouh@sydney.edu.au

Davide Ottonello

Stam S.r.l., Italy. E-mail: d.ottonello@stamtech.com

Tatiana Silva, Alejandro Prada

Tree Technology, Spain. E-mail: tatiana.silva@treetk.com, Alejandro.prada@treelogic.com

Andreas Georgakopoulos, Eleni Giannopoulou, Michalis Mitrou, Vera Stavroulaki

WINGS ICT SOLUTIONS, Greece. E-Mail: andgeorg@wings-ict-solutions.eu, nellygiannopoulou@wings-ict-solutions.eu, mmitrou@wings-ict-solutions.eu, VERAS@wings-ict-solutions.eu

SAFETY4RAILS is the acronym for the European Union Horizon 2020 co-funded innovation project entitled: "Data-based analysis for safety and security protection for detection, prevention, mitigation and response in trans-modal metro and railway networks" which started in October 2020. Its focus is to support the increase of security and resilience against combined cyber-physical threats including natural hazards to railway and metro systems. Its objectives target capabilities to support the characteristics of resilient systems; resilience represented by cycles containing phases of identification, protection, detection, response and recovery (Department of Communications 2019) (*or similarly named phases*). An ESREL paper in 2021 introduced the SAFETY4RAILS project and the SAFETY4RAILS Information System platform as well as some of the tools that are included in the platform. This paper will describe the architectural solution implemented for the platform in the last year and the demonstration of representative capabilities from the first simulation exercise with Madrid Metro at the beginning of 2022.

Keywords: Risk, resilience cycles, resilience engineering, mitigation, railway, metro, multi-modal.

1. Introduction

In SAFETY4RAILS capabilities to support resilient trans-modal metro and railway networks are being achieved through the increase in the Technology Readiness Levels (TRLs) of, presently, eighteen tools and their combination in an overall platform: the SAFETY4RAILS Information System (S4RIS) platform (SAFETY4RAILS 2022, Miller et al. 2021). Further tools could be added in the future. S4RIS aims at improving both functions available to end-users and the overall accuracy and precision of insights presented to them. No tool features directly overlap as implemented to date. The main users targeted are in command and control centers, security/resilience planners and high-level management.

Section 2 describes the S4RIS platform architecture and the contributory tools applied in the Madrid Metro simulation exercise. Section 3 describes the aims and methodology for the simulation exercise. Section 4 describes the results. Section 5 describes the initial evaluation of the results by end-users and section 6 presents the conclusions.

2. S4RIS and contributory tools for Madrid

2.1. S4RIS platform architecture

The S4RIS platform employs a fully modular approach allowing for various tools to integrate together in a seamless manner. The architecture is broken down in various layers that facilitate separation of concerns between various components of the platform (Figure *1*).

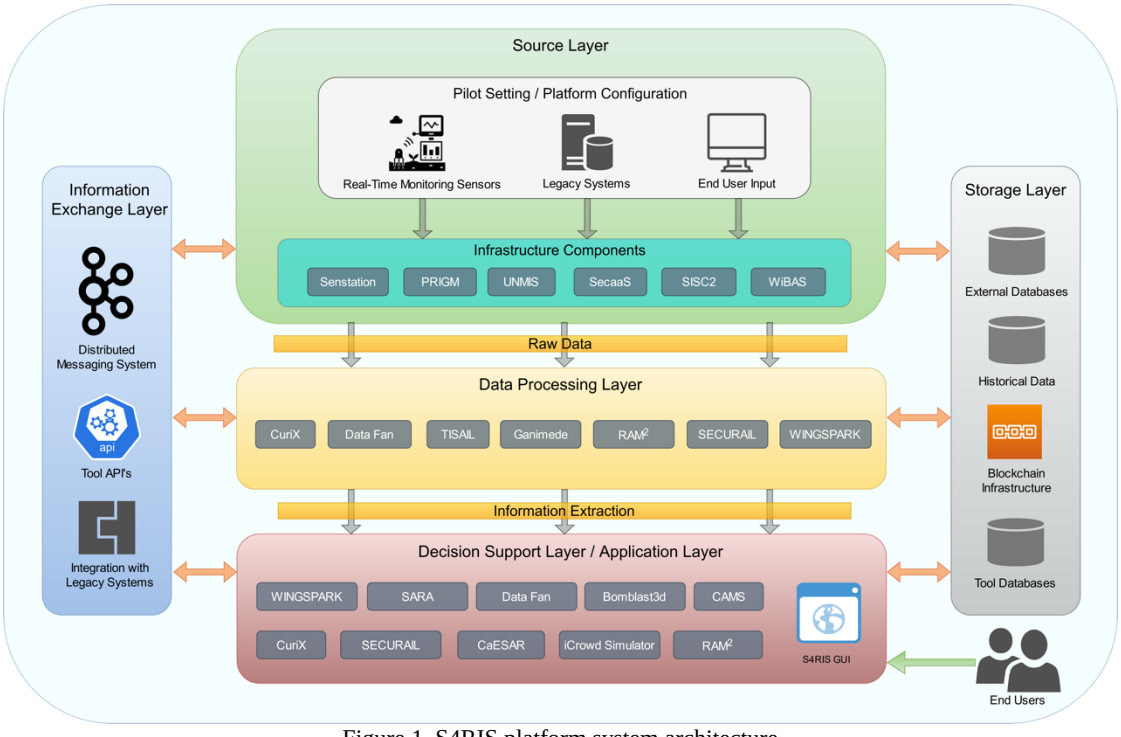

Figure 1. S4RIS platform system architecture

Core to the approach followed is a Distributed Messaging System (DMS) which is part of the Information Exchange Layer and enables heterogeneous tools to integrate consistently. DMS is based on Apache Kafka a well-known stream processing platform that follows the publish and subscribe pattern (Foundation 2022).

Information in DMS is classified using topics and various tools can publish information to topics as well as subscribe to others for retrieving available information. DMS minimizes the duplication of data in the platform since tools only need to share important information once before it becomes available for other tools. The S4RIS platform architecture is centered around continuous information exchange through DMS. Data flows from sources such as sensors into real time monitoring tools which in turn apply further processing using intelligence techniques such as anomaly detection and then share their results through DMS with decision support tools. Employing such a flexible architecture approach allows various tools and data sources to be integrated effortlessly and effectively.

2.2. Contributory tools applied in Madrid

Eleven of the S4RIS contributory tools were applied in Madrid.

2.2.1. BB3d (TRL5 at project start)

The BomBlast3d (BB3d) is a tool capable to fast predict blast loading due to high-explosive bomb attack and the consequent damage on people and structures (Costa 2018). Experimental data is its basis (Defence 2008, Gilbert 1994).

2.2.2. iCrowd (TRL6 at project start)

iCrowd is a general purpose, agent-based modeling platform that provides an abstract, domain-agnostic simulation framework. It can simulate large scale crowds in indoor and outdoor areas, focusing on behavior modeling.

2.2.3. CAMS (TRL6 at project start)

CAMS gives an innovative approach to long-term asset management of infrastructure systems (Mohseni 2017). With the understanding of the range of deterioration scenarios for the systems, asset condition data is captured to support risk identification and budget allocation forecasting.

2.2.4. SecuRail (TRL6 at project start)

SecuRail is a quantitative risk assessment tool for prevention of cyber-physical threats in railway

and metro network. SecuRail allows facility and security managers to model their own railway infrastructure and conduct tailored risk analysis to evaluate likelihood and potential impact of a set of possible threat scenarios, including impacts caused by the cascading effect.

2.2.5. TISAIL/OSINT (TRL 5 at project start)

TISAIL is a threat intelligence platform for the railway sector. TISAIL incorporates three different stages as part of the threat intelligence process: i) uses automated processes for discovering potential threats using threat intelligence feeds, malware repositories, vulnerability reports and detection rules; ii) Carries out malware analysis processes; and iii) Extracts Indicators of Compromise (IoC) and enriches the gathered information in order to generate threat data and notifications for use by other S4RIS tools.

2.2.6. PRIGM and SENSTATION (TRL6 at project start)

End-to-end holistic security in critical railway infrastructures requires sophisticated cryptographic tools enabling both node and person authentication and the security of data both at-storage and in-transit. PRIGM and SENSTATION present a point-to-point secure channel between the edge nodes where data is generated (e.g. by sensor measurements) and the central systems where the railway infrastructure and services are managed (e.g. Operational Control Center - OCC). PRIGM is a multi-purpose and high-throughput Hardware Security Module (HSM) that is installed at central systems presenting functionalities such as symmetric and asymmetric encryption, true random number generation, node and person authentication, and hashing. SENSTATION is a high-throughput secure IoT gateway with wired and wireless interfaces to edge systems (or nodes) through WiFi, GPRS, 4G, CANbus and Ethernet (Miller et al. 2021).

2.2.7. DATA FAN (TRL2 at project start)

DATA FAN targets enabling the user to analyze sequential data such as time series using machine learning algorithms to detect anomalies, e.g. abnormal high passenger loads in trains or metros in the rush hour or after a sporting event.

2.2.8. CaESAR (TRL 5 at project start)

CaESAR evaluates the impact of disruptions on single, or coupled, critical infrastructures. The tool identifies critical components, and also investigates mitigation strategies, providing a ranked list as well as performance time curves.

2.2.9. WINGSPARK (TRL3-4 at project start)

WINGSPARK is a platform which provides active monitoring, forecasting and anomaly detection mechanisms, delivering insights to the operational condition of the environment it supervises. Currently, WINGSPARK has three primary components: i) Time-series based anomaly detection utilizing train speed measurements retrieved from IoT sensors, ii) Time-series based anomaly detection utilizing energy consumption measurements; and iii) Detection of overcrowded situations in the monitored railway infrastructure, based on video acquired through CCTV cameras.

2.2.10. CuriX (TRL4 at project start)

CuriX is a commercial tool to monitor technical devices (e.g., IT, OT) in real-time. It monitors the system behavior, learns normal behavior based on statistical and machine learning methods, and informs the users about deviations.

2.2.11. RAM^2 (TRL6 at project start)

RAM^2 is an industrial digital and cybersecurity platform for risk monitoring, assessment and management. It integrates with a wide variety of security and industrial systems to collect and correlate data and events, to provide complete asset inventory visibility, identify vulnerabilities, evaluate the security posture, and detect suspicious patterns. RAM^2 prioritizes and alerts on risks and provides clear risk mitigation steps, which are feasible within the operational constraints. It simplifies the OT cybersecurity operations management, and enables operators, security teams and executives to ensure safe, reliable and efficient operations.

3. Madrid simulation exercise organization

3.1. Aims

The main aims of the simulation exercise were to: i) demonstrate how the S4RIS with some of its main tool components, can help rail and metro

operators increase the resilience of their services to combined cyber-physical attacks; and ii) receive evaluation from the rail and metro operators observing the exercise for future S4RIS development and evaluation iterations.

3.2. Methodology

The Madrid Metro simulation exercise was the first of four simulation exercises planned within the end-user evaluation and validation methodology for the S4RIS. The next three are in Ankara, Rome and Milan. (SAFETY4RAILS 2021, Bonneau M-H. 2022).

Combined cyber-physical attacks were simulated for a Madrid metro station and its surroundings; in the attackers *modus operandi* both cyber and physical attacks were launched as part of their overall attack plan. Despite the attack being focused on a specific 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. We do not present the scenario details because of the sensitivity of the security issues.

The simulation exercise was organized around the combined cyber-physical attacks in the scenario and a reduced and simplified set of resilience phases: prevention; detection & response; and recovery.

For the prevention and recovery phases the capabilities of relevant individual tools were presented in workshops. Their results were targeted to demonstrating how evidence can be provided to help decide on the need for further mitigation measures and to compare them.

For the detection & response phase a "live" simulation exercise was carried out demonstrating the capabilities of relevant individual tools and their overall correlation, enabled through the S4RIS architecture with its DMS, for managing on-going attacks. For this simulation exercise, the Postman tool (Inc. 2022) was used to publish messages, prepared in advance of the simulation, primarily for subscription by the RAM^2 tool. The structure and content of the JSON messages matched those that the individual tools generate.

Representatives from eight end-user organizations attended the simulation exercise: 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 Catalonia) and UIC (the Worldwide Rail Organization).

The end-user participants evaluated the simulation of each resilience phase via questionnaire. Further evaluation will follow through group-based techniques after further simulation exercises (SAFETY4RAILS 2021, Bonneau M-H. 2022).

4. Madrid simulation exercise results

4.1. Prevention

4.1.1. BB3d

Assigned the bomb attack location and mass charge and using the distribution of people computed by the iCrowd tool around the location, BB3d provided the structural damage level of buildings and underground tunnels as well as the number of casualties and injured people.

4.1.2. iCrowd

iCrowd was used to predict evacuation times and detect bottlenecks in the studied environment. Using the locations and movement patterns of cameras and guards, it was also used to detect blind-spots with the goal to improve the effectiveness of CCTV systems.

4.1.3. CAMS

With the input from the list of components of the infrastructure system (assets and their quantity) and the related condition inspections data, deterioration curves were provided for normal aging coupled with the impact of a sudden extreme event (Izaddoost 2021). This information was paired with the predicted cost to maintain the system to a targeted level.

4.1.4. SecuRail

Starting from the network topology and others data concerning the infrastructure and services (e.g. people flows recorded by turnstiles and economic figures of asset), SecuRail provided Metro de Madrid managers with detailed risk indicators for a set of scenarios generated by the initial threat. Furthermore, comparing two configurations of the same use-case but with different security countermeasures applied, it was possible to identify those that significantly reduce the risk of the considered threats.

4.1.5. PRIGM and SENSTATION

PRIGM and SENSTATION were not directly applied in the simulation exercise because of their nature, requiring actual physical integration (see section 2.2.6). Instead the benefit that they could bring as low-level countermeasures to MdM's considering the highest resilience against cyber-attacks. Nevertheless, the system could still be improved by addressing potential attacks, mainly at a low level, which can be prevented by the use of secure gateways and high-throughput HSMs

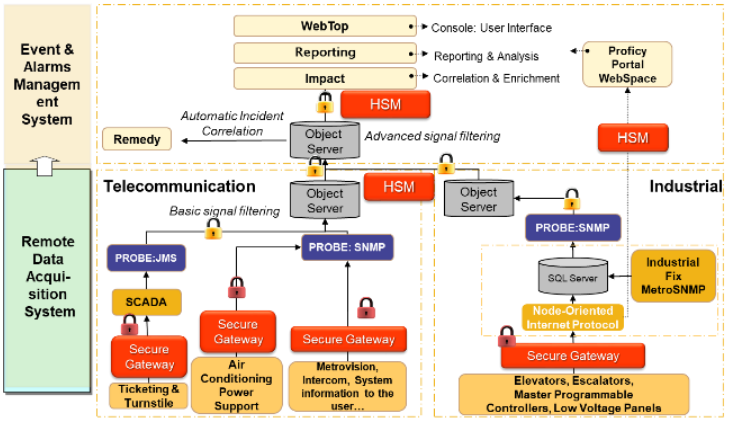

Figure 2. COMMIT System in Madrid Metro

Center for Operational Maintenance and Monitoring of Installations and Telecommunications (COMMIT) System was analyzed.

As illustrated in Figure 2, COMMIT is composed of two layers. The first layer, the Remote Data Acquisition System constitutes industrial and telecommunications infrastructure. Ticketing and turnstile, a part of the telecommunication system, are connected to an Object Server via SCADA system and Java Management System. Similarly, air conditioning systems, power support systems, Metrovision, Intercom and monitoring systems are also connected to the Object Server via Simple Network Management Protocol (SNMP). The industrial backend that is composed of elevators, escalators, low voltage panels, Master Programmable Controllers and similar subsystems are first connected to a SQLServer via the Node Oriented Internet Protocol and then the SQL Server is connected to an Object Server at a higher level. The second layer is the Event and Alarms Management System which is capable of monitoring the services, alarms, incident management, tele-maintenance and knowledge management enriched with effective event handling mechanisms, reporting and impact assessment utilities.

A detailed security assessment, identified that COMMIT itself is already designed by enabled via PRIGM and SENSTATION. The red boxes in Figure 2 illustrate where such hardware-based countermeasures could be applied to assure end-to-end security within the entire cyber-physical system.

4.1.6. DATAFAN

DATA FAN calculated the passenger load of train and metro stations and the free capacity of surrounding stations to support the user in planning the re-direction of passengers in different what-if-scenarios.

4.1.7. CaESAR

Based on a developed topology model including system components and related conditions for impact propagation, CaESAR provided resilience curves highlighting the system's performance. It gave an overview of resilience indicators and insight into the vulnerability to cascading effects for the specific event of the unavailability of certain stations and how different mitigation measures could improve the network exemplified by the closing of transportation hubs.

4.2. Detection & Response

4.2.1. iCrowd

By simulating an evacuation, iCrowd detected bottlenecks and offered aids in the improvement of evacuation protocols.

4.2.2. TISAIL/OSINT

TISAIL detected a spear-phishing campaign targeting the staff of MdM, through an email. In this email hackers pretended to be someone from MdM and convinced an employee to download a malicious file that exploited a vulnerability in the operative system. An alert about this attack was created by TISAIL and sent to RAM^2. By monitoring the assets connected to the MdM network, TISAIL also detected and alerted the vulnerability in a CCTV camera.

4.2.3. DATAFAN

DATA FAN calculated the passenger load of train and metro stations and detected and alerted anomalies such as blocked turnstiles. The tool also gave information on the reliability of the predictions.

4.2.4. CaESAR

Identifying critical components, CaESAR supported the detection of the most vulnerable network structures, here certain stations. CaESAR supported the evaluation of response strategies by comparing the impact of different mitigation strategies on the network resilience which has been presented exemplarily for the manual closure of transportation hubs in the metro network.

4.2.5. WINGSPARK

WINGPARK detected and alerted anomalies in the train speed and overcrowding on platforms.

4.2.6. CuriX

CuriX analyzed simulated time-series of network flows, sound pressure levels and power consumption. Based on this data, CuriX detected and alerted about signs of port scans, an explosion, and a power outage.

4.2.7. RAM^2

RAM^2 integrated with the S4RIS DMS Kafka queue and ingested events that were reported by all the participating tools.

The events were processed to generate alerts, which were connected to relevant assets. Risk was calculated automatically for each of the alerts for prioritization.

RAM^2 provided a complete mitigation plan for each of the alerts. Based on RAM^2's "insights" engine, alerts were correlated to identify risk scenarios that provided more context and focused the users on top priority issues. The correlation of events provided users with insight into the overall attack and its progression.

An example of such insight was detection of an abnormal event at the metro station with potential impact on crowd safety. This insight correlated and grouped together events (from the other tools just described in this section) including detection of a spear-phishing campaign based on OSINT, an explosion based on high noise, reports regarding overcrowded areas based on CCTV video feed, abnormally high passenger flow in turnstile, blocked turnstile and a closed station door at an unusual time.

4.3. Recovery

4.3.1. BB3d

Analyzing many blast scenarios around the station and assessing the numerical results in term of structural and people damage, mitigation countermeasures could be put in place and post-attack interventions could be optimized.

4.3.2. CAMS

Assessment of cost to restore the service after an extreme event was provided considering the assets damaged.

5. Initial end-user evaluation

Questionnaires covered the topics: exercise organization, tool functionalities, value of their outputs and graphical user interface user-friendliness. Most of the questionnaires' contents applied the Likert scale (McLeod 2019).

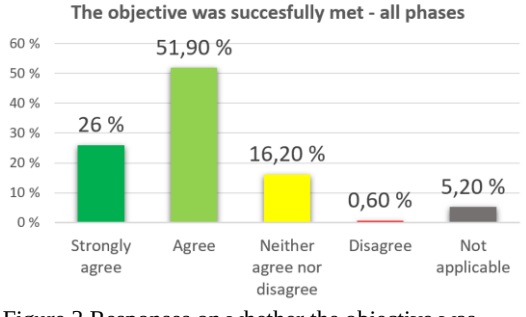

Figure 3 Responses on whether the objective was successfully met, regarding all phases

Core was to determine how far the end-users evaluated the set of requirements for each tool and the overall S4RIS were met; the "objective" (SAFETY4RAILS 2021). Overall for all tools and resilience phases evaluation was very positive

with over 75% agreeing that on an initial evaluation the "objective" was met (Figure 3). The questionnaires also had open questions for more extended answers. These mainly provided short comments of approval or acknowledgements, though some also highlighted points for improvement, which will be looked into in more depth in the next steps of the evaluation. Most importantly the end-users signaled their agreement that a platform such as S4RIS could help them to continually improve the resilience of their services.

6. Conclusions

The S4RIS platform was tested against the platform and individual tool requirements defined earlier in the project. Overall for all tools and resilience phases the initial end-user evaluation was very positive. The Postman tool was used to publish tool messages in this simulation exercise. Observations and evaluations will be used for development iterations and preparing the next three simulation exercise. Future simulation exercises foresee increased integration of tools within the S4RIS.

Acknowledgement

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532. The information appearing in this paper has been prepared in good faith and represents the views of the authoring organizations. Neither the Research Executive Agency, nor the European Commission are responsible for any use that may be made of the information it contains.

References

Bonneau M-H., Petersen L., Havarneau G., Crabbe S. 2022. "SAFETY4RAILS EU project: Protecting railway and metro infrastructure against combined cyber-physical attacks." *World Congress on Railway Research (WCRR) 2022*. Preprint.

Costa, E. 2018. "Implementation of an empirical tool for fast prediction of bomb airblast loading." *International Journal of Protective Structure.*

Defence, United States Department of. 2008. "Unified Facilities Criteria (UFC) 3-340-02, Structure to Resist the Effects of Accidental Explosions."

Department of Communications, Climate Action & Environment, NIS Compliance Guidelines for Operators of Essential Service (OES). 2019. "NIS Compliance Guidelines for Operators of Essential Service (OES)."

ENISA, European Union Agency for Cybersecurity. 2020. "RAILWAY CYBERSECURITY Security measures in the Railway Transport Sector." Technical.

Foundation, Apache Software. 2022. *Apache Kafka.* https://kafka.apache.org/.

Gilbert, S. M., F. P. Lees and N. F. Scilly. 1994. "A Model Hazard Assessment of the Explosion of an Explosives Vehicle in a Built-Up Area." *Minutes of the 26th US Department of Defense Explosives Safety Board Seminar.* Miami.

Inc., Postman. 2022. *What is Postman.* https://www.postman.com/product/what-is-postman/.

Izaddoost, A., Naderpajouh, N., & Heravi, G. 2021. "Integrating resilience into asset management of infrastructure systems with a focus on building facilities." *Journal of Building Engineering, 44, 103304.*

McLeod, S. 2019. *Likert Scale Definition, Examples and Analysis.* https://www.simplypsychology.org/likert-scale.html.

Miller, N., Y. Satsrisakul, K. Faist, M. Fehling-Kaschek, S. Crabbe, M. Poliotti, N. Naderpajouh, et al. 2021. "A Risk and Resilience Assessment Approach for Railway Networks." *Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021).* Singapore: Research Publishing Services. 2071-2078.

Mohseni, H., Setunge, S., Zhang, G., & Wakefield, R. 2017. "Markov process for deterioration modeling and asset management of community buildings." *Journal of Construction Engineering and Management, 143(6), 04017003.*

SAFETY4RAILS. 2022. https://safety4rails.eu/.

SAFETY4RAILS. 2021. "Deliverable D8.1 Evaluation Methodology."