SAFETY4RAILS

Lessons learnt from SAFETY4RAILS for future research projects

Deliverable 8.6

Lead Author: UIC

Contributors: Fraunhofer, STAM, PRORAIL, MTRS, CEIS, EOS, NCSRD, LDO, RMIT, TREE, EGO, CURIX, ETRA, FGC, ICOM, WINGS, RINA-C.

Dissemination level: PU - Public

Security Assessment Control: passed

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

D8.6 LESSONS LEARNT FROM SAFETY4RAILS FOR FUTURE RESEARCH PROJECTS	
Deliverable nr.:	8.6
Version:	1.1
Delivery date:	13/10/2022
Dissemination level:	PU - Public
Nature:	Report
Main author(s)	UIC
Contributor(s) to main deliverable production	STAM, PRORAIL, MTRS, CEIS, EOS, NCSRD, LDO, RMIT, TREE, Fraunhofer, EGO, CURIX, ETRA, FGC, ICOM, WINGS, RINA-C.
Internal reviewer(s)	Fraunhofer, MdM
External reviewer(s)	Grigore Havarneanu (UIC)

Document control			
Version	Date	Author(s)	Change(s)
0.1	01/08/2022	UIC	First Draft
0.2	01/09/2022		Updated draft with contributions from STAM, PRORAIL, MTRS, CEIS, EOS, NCSRD and UIC
0.3	05/09/2022	UIC	Updated draft with contributions from LDO, RMIT, TREE, Fraunhofer, EGO, CURIX
0.4	25/09/2022	UIC	Updated draft with contributions from ICOM, ETRA, FGC, WINGS, RINA, Fraunhofer
1.0	13/10/2022	UIC	Final version prepared for submission to EC.
1.1	13/10/2022	Fraunfofer	Very minor editing and formatting.

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

SAFETY4RAILS is the acronym for the innovation project: **Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS**. Railways and Metros are safe, efficient, reliable and environmentally friendly mass carriers, and they are becoming even more important means of transportation given the need to address climate change. However, being such critical infrastructures turns metro and railway operators as well as related intermodal transport operators into attractive targets for cyber and/or physical attacks.**The SAFETY4RAILS project delivers methods and systems to increase the safety and recovery of track-based inter-city railway and intra-city metro transportation.** It addresses both cyber-only attacks (such as impact from WannaCry infections), physical-only attacks (such as the Madrid commuter trains bombing in 2004) and combined cyber-physical attacks, which are important emerging scenarios given increasing IoT infrastructure integration.

SAFETY4RAILS concentrates on rush hour rail transport scenarios where many passengers are using metros and railways to commute to work or attend mass events (e.g. large multi-venue sporting events such as the Olympics). When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security, e.g. carry out a threat analysis, maintain situation awareness, establish crisis communication and response, and they have to ensure that mitigation steps are taken and communicated to travellers and other users. **SAFETY4RAILS will improve the handling of such events through a holistic approach.** It will analyse the cyber-physical resilience of metro and railway systems and deliver mitigation strategies for an efficient response, and, in order to remain secure given everchanging novel emerging risks, it will facilitate continuous adaptation of the SAFETY4RAILS solution; this will be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENT

Executive summary

The Task T8.4 concentrates on the lessons learnt from the evaluation of the simulation exercises. This deliverable D8.6 is the main output of the task.

First, the main achievements of the project are summarised. Then the document focuses on the lessons learnt for future research projects and describes ways to improve the tools going forward. This is followed by a section on policy impact which describes how SAFETY4RAILS could contribute to compliance with EU directives and to existing standards.

A special focus is on the involvement of end-users and railroad practitioners during the whole project from the beginning in defining requirements and needs, designing and performing the scenarios and demonstrations, evaluating the software platform S4RIS and the feedback loops to the developers.

The last section addresses the go-to-market roadmap and gives insight on the industrialisation of results and the engagement with EU buyers.

The content of this deliverable is reflected in the final brochure named “Main lessons learnt” available at https://safety4rails.eu/wp-content/uploads/2022/10/Safety4Rails_Final-brochure_26SEPT22-2.pdf.

1. Introduction

The main purpose of the SAFETY4RAILS project was to provide a set of solutions to increase railway and metro security and resilience against cyber and physical incidents, including natural hazards. The resilience concept adopted in SAFETY4RAILS is a cycle which has 5 main phases: identify, protect, detect, respond and recover, as represented in the image below.

FIGURE 1 RESILIENCE PHASES

IMAGE INFORMED BY DEPARTMENT OF COMMUNICATIONS, CLIMATE ACTION & ENVIRONMENT, NIS COMPLIANCE GUIDELINES FOR OPERATORS OF ESSENTIAL SERVICE (OES), AUGUST 2019, P.8 AND P.22.

The project started by the analysis of end users' needs and requirements. In parallel and based on these requirements, the 19 tools provided by the consortium members were adapted or further developed and implemented in an overall SAFETY4RAILS Information system, abbreviated as S4RIS. S4RIS focuses on threat assessment, risk and crisis management and improvement of resilience and security. S4RIS was then tested and evaluated by the end-users within four simulation exercises based on different use cases.
This document will introduce the main lessons learnt in this whole process.

2. Main achievements

2.1 The overall tool: S4RIS

2.1.1 Description

The main output of the project is the S4RIS platform which targets the combination of multiple solutions for physical, cyber and combined cyber-physical threats to function together as one system with an efficient exchange of data and information. The aim is to support railways and metro operators to manage cyber and physical risks.

Most of the individual tools provided in SAFETY4RAILS were already at Technology Readiness Level (TRL) 5-6. They have been further developed to meet the scope and objectives of the project. The main focus of the tools on the S4RIS platform are listed below:

- 7 tools provide monitoring and infrastructure services related to security, network infrastructure and CCTV data stream analysis.
- 8 tools provide an intersection of monitoring, simulation and decision support services. These are made possible through the use of intelligent risk assessment mechanisms and provide further mitigation insights through decision support functionality.
- 4 tools provide simulation services such as agent-based crowd simulation and bomb blast simulation scenarios allowing for security and resilience assessment of stations.

2.1.2 Architecture of S4RIS

The overall architecture is described in Figure 2. This architecture is composed of 3 horizontal layers and 2 vertical layers:

The horizontal layers are as follows:

- A Source Layer where data is collected from multiple sources: real-time monitoring sensors (temperature sensors, wind sensors, network monitoring infrastructure), legacy systems or input from users.
- A layer dedicated to data processing.
- A layer providing the information for decision support to the users.

The vertical layers which are supporting the horizontal layers for the exchange of information and the storage of data are as follows:

- First, the Distributed Messaging System (DMS) is a core component of the S4RIS architecture enabling the different applications, software systems and devices to share data between them in a transparent, distributed and fault-tolerant manner: the S4RIS DMS is based on Apache KAFKA using the JSON format.
- The second vertical layer is the data storage gathering external databases, historical data, and tool databases. Within this layer is also placed solutions for guaranteeing data integrity such as through blockchain technology.

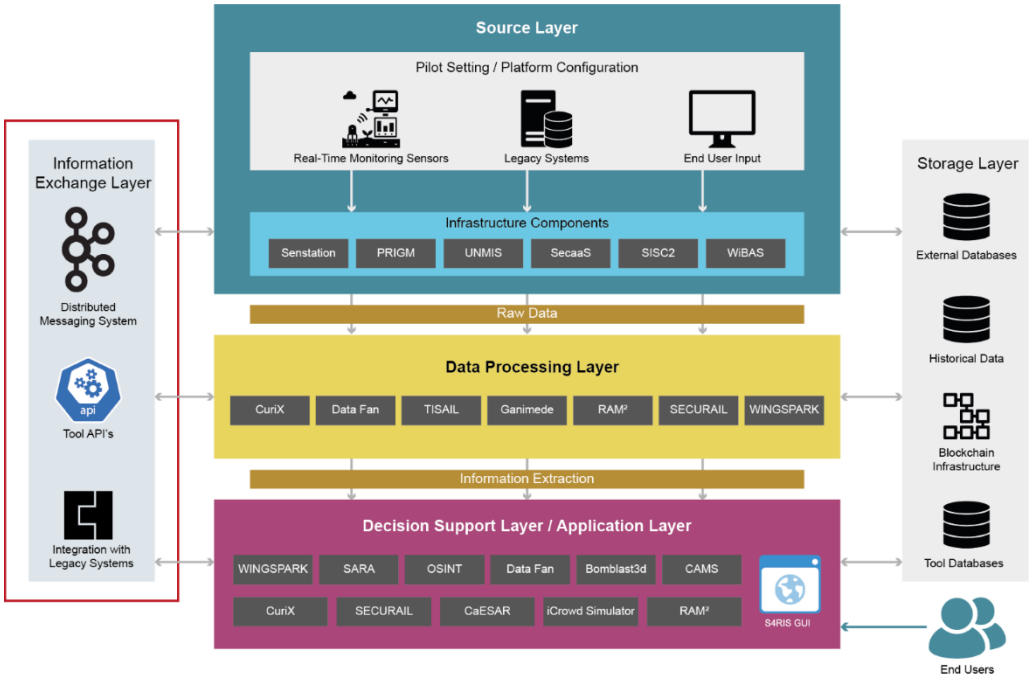

FIGURE 2 S4RIS CONCEPT ARCHITECTURE

2.1.3 User Interface

The S4RIS platform consists of information collected and processed by different tools and displayed for the end users. In this context, the Graphical User Interface (GUI) is the entire graphic structure responsible for the interactions between the users of the platform and the software. The purpose of this interaction is to intuitively allow the operation and control of other software within and/or through the S4RIS platform, while the system simultaneously feeds information into other software to assist with the operators' decision-making process.

The interface was developed considering multiple devices including mobile devices. This aimed at enabling access to the S4RIS platform and computational tools, wherever the user is, regardless of their location.

A main benefit of this integration is the ability to enable users with little or no expertise access and use of different tools to perform operational analyses.

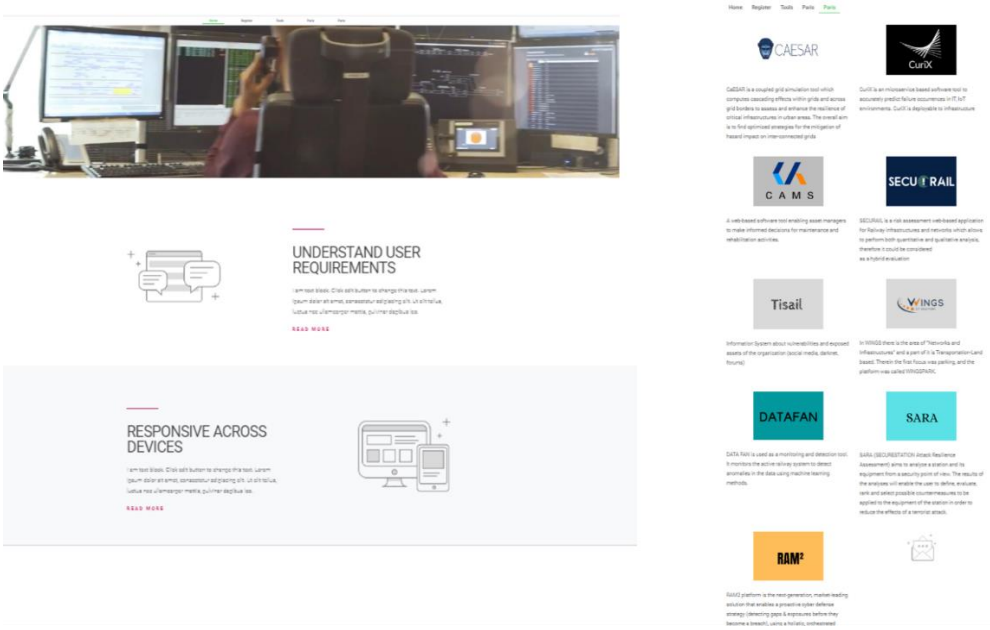

Figure 3 S4RIS GRAPHICAL USER INTERFACE (GUI)

2.2 The individual tools

This section gives a short description of the achievements per main tool. Each tool is classified in the main resilience phase that it addresses. However, as shown in Figure 4, most of the tools address several resilience phases.

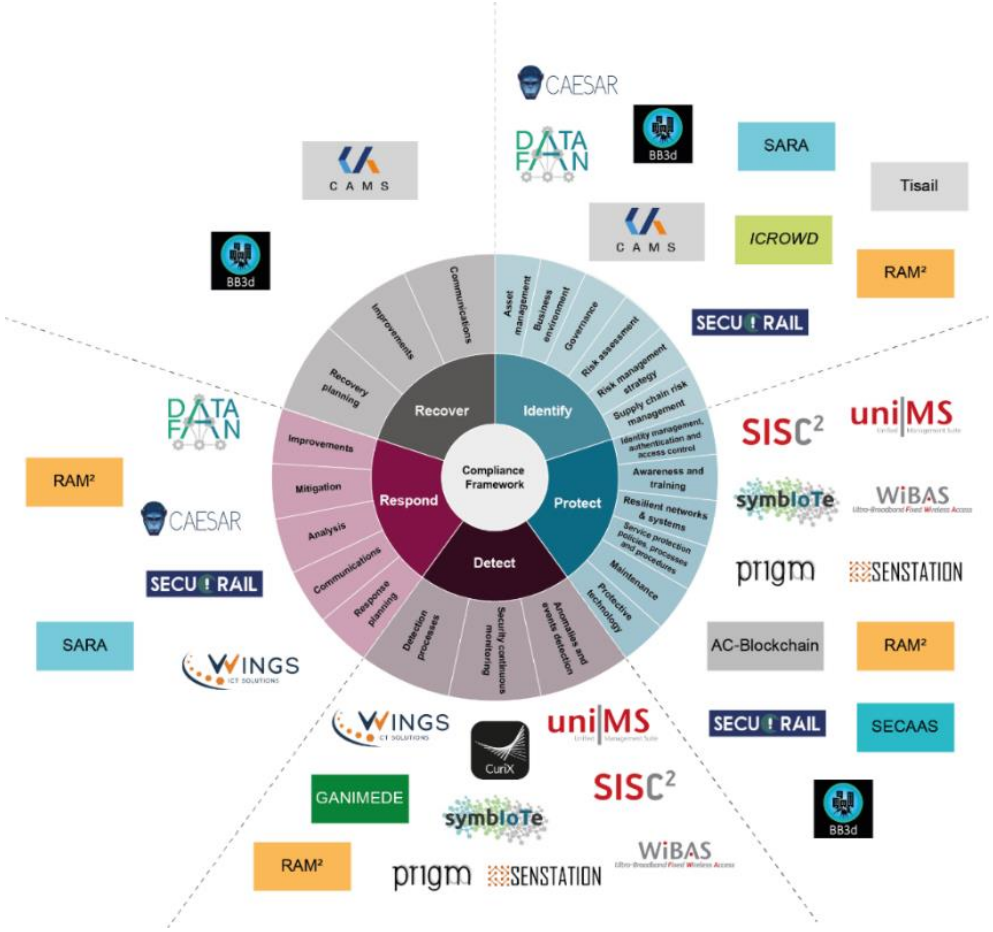

FIGURE 4 S4RIS CAPABILITIES FOR EACH RESILIENCE PHASE

Identify

1. **BBD3** is a predictive tool evaluating blast-induced adverse consequences in case of a bombing attack to help the users to identify and effectively set up the most appropriate protective strategies and countermeasures.
2. **CAESAR** is a simulation tool for computing cascading effects within critical infrastructures and especially across infrastructure borders, i.e. in interdependent infrastructures. CaESAR evaluates the vulnerability of the system in each time step and builds a resilience value. This evaluation builds the base for the identification of components which strongly contribute to the infrastructure functionality and where a failure leads to severe consequences, i.e. to a significant reduction of performance. These critical components are used for applying mitigation strategies for increasing the infrastructure resilience.
3. **CAMS** provides asset managers with recorded asset condition data and various analysis reports related to asset deterioration, risk and budget forecasting, allowing them to make informed decisions related to maintenance and budget allocations. CAMS was expanded to asset classes belonging to the railway and metro environment and to digital or soft assets within the project as well as for the inclusion of the resilience of assets facing extreme events such as terrorist attacks.
4. **DATAFAN** is a predictive tool which is based on machine learning algorithms (i.e. Deep Neural Networks). It provides time series forecasting for passenger load, based on historical passenger load for given time steps and stations. In doing this, it can e.g., predict the expected passenger load for large events such as soccer games. Furthermore, in what-if-scenarios the operator can see what the situation is if a station must be closed due to a hazardous event such as a flood and what will be the free capacity of the surrounding stations to support redirecting the passengers. Moreover, the tool gives a reliability score indicating how the results were calculated to support the practitioner's tool acceptance and to enable them to decide whether to re-run calculations with updated input parameters.

5. **iCrowd** is a general-purpose agent-based modelling platform providing an abstract, domain-agnostic crowd simulation framework. For SAFETY4RAILS, iCrowd was used as a tool to simulate crowd behaviour and cyber physical agents (humans, sensors, other) inside a multimodal railway system aiming to detect vulnerabilities and to avoid or mitigate the impact of hazards for public security and safety purposes.
6. **SECURAIL** is a risk assessment web-based application for railway infrastructures and networks which performs both quantitative and qualitative analysis. The tool provides modelling of the railway infrastructures, including assets, areas and countermeasures as well as connections and interdependences between different components of the infrastructures to consider cascading effects. It also provides the user with cost-benefits analysis to compare risk reduction with cost of security measures.
7. **SARA** is a static tool able to perform computation on threats' impact(s) on train stations. Its aim is to analyse a station from a security point of view, regarding individual equipment (e.g., ventilation, communication, power supply, etc.) based on the station description. The results of the analyses enable the user to define, evaluate, rank and select possible countermeasures to be applied to the equipment of the station in order to reduce the effects of a terrorist attack.
8. **TISAIL** is a threat intelligence platform for the railway sector based on OSINT (Open-Source Intelligence). An enhanced version of TISAIL cyber security in an OSINT platform extended in SAFETY4RAILS was integrated into the overall S4RIS platform with advanced analytics rules to extract relevant cyber security data for rail and metro operators. In addition, a new subsystem that gathers data from publicly available news feeds as well as data from social media content sources has been developed. The data gathered, evaluated, enriched, and logically represented through the OSINT analytics subsystem is communicated to the overall S4RIS platform as input data for further analytics processing and importantly also for presentation on the S4RIS decision support dashboard system.

RAM^2 (described in the response phase) also provides capabilities for the identification phase.

Protect

9. PRIGM is a Hardware Security Module (HSM), a device that is capable of performing major cryptography operations such as true random number generation, prime number generation, key generation and management, secure key storage and exchange, symmetric encryption (AES, 3DES), asymmetric encryption (RSA, ECDSA), and hashing (SHA). HSM connects to a host device (server, PC, etc.) using PCIe interface. It is enclosed in a tamper-proof enclosure.
10. Senstation is also a hardware-based cryptographic tool that enables end-to-end security in IoT-enabled cyber-physical environments together with PRIGM. The tool provides a secure channel between the HSM (PRIGM) and the IoT gateway and enable the secure collection of sensory data that can be used for time-series based anomaly detection.
11. Ultra-Broadband Fixed Wireless Access (WiBAS™), a state-of-the-art Point-to-MultiPoint (PtMP) native Ethernet microwave product line, fitting the demanding needs of railway and metro operators.
12. Unified Management Suite (uni|MS™), a state-of-the-art solution for supervising and managing modern telecommunication networks.
13. Cyber-Physical Security Information Management (SISC2), a modular and scalable software integration platform for surveillance, collaboration, coordination and administration of diverse security and operations management related events.
14. Security as a Service (SecaaS) product, a part of ICOM's cloud computing services. The SecaaS portfolio encompasses dedicated virtual firewalls and web application firewalls.
15. Symbiosis of smart objects across IoT environments (symbIoTe), an additional tool added by the partner ICOM during the project, an IoT interoperability framework which enables discovery and sharing of IoT devices and services across diverse IoT platforms and applications.

RAM^2 (described in the response phase), SECURAIL and BBD3 (described in the identification phase) also provide capabilities for the protection phase.

Detect

16. **Ganimede** is a platform for the large-scale analysis of live and recorded data streams based on Deep Learning. For SAFETY4RAILS, Ganimede was enriched with the following algorithms: abandoned object detection, people re-identification, man down detection, audio pattern detection. It enhances situational awareness and transform threat detections from a manual, resource-intensive operation into an efficient and automated process.
17. **CuriX** is a microservice based software solution with a distributed system architecture, which aims at anomaly detection and outage prediction to finally prevent service interruptions in the monitored system.
18. **WINGSPARK**: WINGS Big Data and Predictive analytics tool provides active system monitoring, forecasting and detection of anomalies using AI methods; integration of various sources of data to achieve enhanced awareness;

what-if analyses to assess various issues related to cyber and physical threats to the railway infrastructure; delivery of insights; and visualisation of aspects of the railway infrastructure model for planning of potential measures.

PRIGM, Senstation, SISC2, symbIoTe, WiBAS described in the Protection phase, also provide capabilities for the detection phase.

Respond

19. **RAM**^{2} is a Decision Support System (DSS) which aggregates the alerts received from all relevant S4RIS tools. RAM^2 generates relevant insights and mitigation procedures to help the end-users to manage the crisis and make decisions.

DATAFAN, CAESAR, SECURAIL, SARA and WINGSPARK described above, also provide capabilities for the response phase to provide decision makers with prediction data and help them to take the right decisions.

Recover

CAMS and BB3d, already described above, provide information for the recovery phase to help the decision makers to select relevant countermeasures.

2.3 Recommendations and guidelines

This section gives a brief description of the recommendations and guidelines documents that have been produced within SAFETY4RAILS project to support end-users with crisis management plans and crisis communication.

2.3.1 Incident & Crisis Management Plans

The incident and crisis tool document (Deliverable D3.5 public document[1]) provides the specifications for the development of an Incident & Crisis Management Tool (ICMT). It describes how to build on existing incident and crisis management arrangements applied by railway and metro infrastructure managers and operators. It forms an ideal set of extended requirements as a tool for crisis management. The ICMT can be integrated with the Decision Support System (DSS), to gain the benefits provided, and interfaces with existing multimedia crisis communication tools and arrangements to support efficient and safe incident and crisis management**.**

2.3.2 Crisis Communication and Information Sharing Guidelines

This Crisis Communication and Information Sharing Guidelines (Deliverable D9.3 and D10.7 public documents[2]) considered key inputs (including the main concerns in this sense) from a representative sample of railway and metro end-users in Europe and beyond. Existing gaps and needs in the field were also considered to move one step forward the current state-of-the-art. Such inputs were used to materialise more than 20 actionable recommendations that can be used to enhance crisis response and recovery by means of better communication.

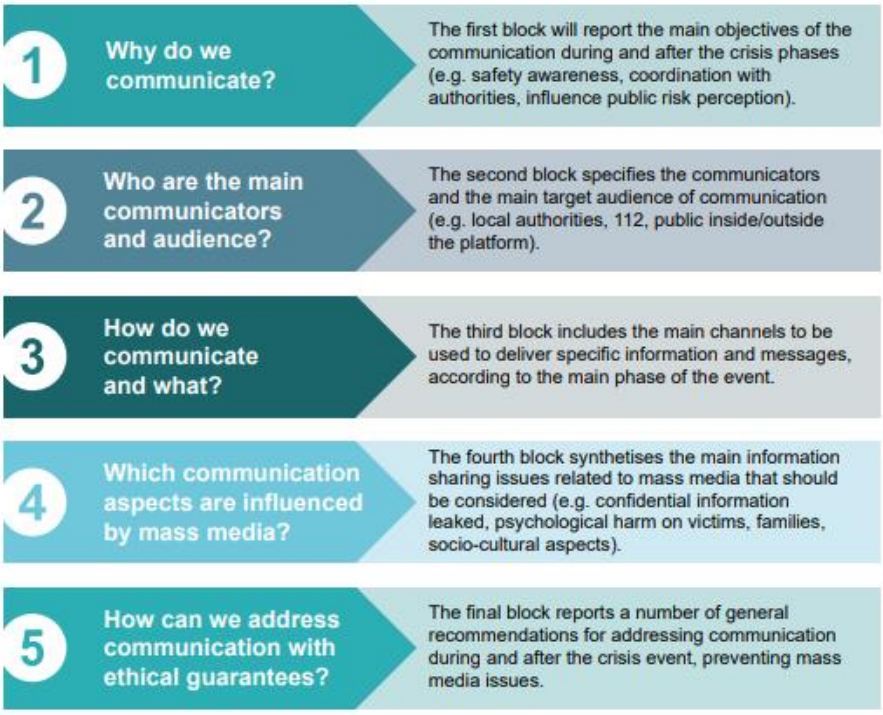

FIGURE 5 SAFETY4RAILS CRISIS COMMUNICATION GUIDELINES STRUCTURE

[1] https://safety4rails.eu/library/

[2] https://safety4rails.eu/library/

The guidelines have been applied through specific cyber-physical scenarios developed during the project using the 5 blocks of questions described in the Figure below.

3. Main lessons learnt for future research projects

This section focuses on ways to improve the tools going forward.

3.1 Overall resilience cycle

For all resilience phases, the output of the S4RIS tools is very dependent on data and also on a good knowledge of the domain addressed. The following requirements are key to achieve good quality outputs from the S4RIS tools.

DATA modelling

A solid data model capable of representing the system (infrastructure, assets, people etc.) under consideration as well as the different threats that could affect it was produced and is described in the public deliverable D3.3[3].

However, this could be taken further and better represent the complex reality of railway and metro networks by using more advanced techniques. For example, the adoption of a BIM (Building Information Modelling) model could improve the modelling and such a model could be used as the foundation for the implementation of a digital twin. The use of such advanced techniques could improve the results created by the platform and make them more reliable.

Another improvement that could be done to facilitate the modelling of the network in future projects is the adoption of a common framework, like RailTopoModel[4], to facilitate the exchange of information even with software and tools which were not developed in this project.

DATA gathering

For the simulation exercises in operational environments, and to achieve the integration of S4RIS into end user environments (e.g., operational control centres, crisis management tools), different means were used to gather data in a context where many data cannot be provided by the end-users due to their commercial and/or security sensitivity, GDPR rules or unavailability.

- Share collected data: using data which was collected before by end-users (and acquired by consortium partners or external stakeholder interactions), i.e. realistic data but from an earlier time period. Where necessary, this data can be pseudonymised or anonymised.
- Use of Open data[5].
- Generate partially artificial data: from a small sample of real data, which can be acquired from the above methods, artificial data can by generated by sampling methods, e.g., bootstrap method. This can be done individually per tool and needs to be synchronized amongst tool providers.

DATA security

Data authenticity and data integrity are needed to ensure that the original data (images, etc.) presented is complete and unaltered since time of acquisition. In SAFETY4RAILS capabilities were demonstrated with both PRIGM/Senstation and blockchain technology.

[3] Library - SAFETY4RAILS project

Guidance through the cycle

The S4RIS platform can be seen as one piece of the long journey from the development of functionalities and tools focused projects in FP7 up to tool collections and catalogues in Horizon 2020. With S4RIS the consortium partners built up a platform in which tools are not just presented to and are selectable by users, but the tools can collaborate.

One main feature that is still missing and would be recommended is continuing working on guidance to users for the platform itself. Resilience and the tools providing features to increase resilience is still a complex and sometimes complicated topic that requires domain knowledge, resilience engineering knowledge, and experience. Having means on board a platform to guide and support the end-users through the collaboration steps (or workflows) of the toolset would probably lead in the long run to more effective resilience platforms and eventually to more resilient systems.

3.2 IDENTIFICATION phase

3.2.1 Asset management

In the S4RIS platform, asset management is addressed by the CAMS tool, which is an online software application that models deterioration, assesses risks, and forecasts rehabilitation costs. The enhanced feature allows mobile solutions to be integrated into data collection, inspection, and historic data collection. CAMS-mobile inspection app will be fully functional for railway organizations. The module includes features such as asset location capture, asset condition and risk capture with images attached to each asset. Validation will be performed against historical data in order to ensure repeatability. The business intelligence platform linked to CAMS-mobile provides the inspector with reports of their performance. The administration console enables the inspector admin full control of all the inspectors and the data that is being collected in the field in real time.

The next steps for CAMS that could be addressed in future research are listed below:

- Ensure the cyber security of critical infrastructure data.
- Accurate prediction of infrastructure safety in the face of extreme events, hazardous situations, and cyber-physical incidents.
- IoT sensors and real-time monitoring of safety.
- Integration of IT into a wide range of end-user applications.
- Understanding infrastructure deterioration using IoT device information.
- An effective prediction of the interdependence of infrastructure assets, including when one asset fails.

3.2.2 Risk assessment

Risk Assessment is a complex procedure which has been performed manually for years. To date, due to the growing complexity of systems to be analysed and the increasing amount of data, performing this process in an adequate manner **requires ad-hoc tools or specific application of tool approaches to the system being assessment.**

Methodology for risk assessment

In order to improve the quality of the methodology for the risk assessment conducted with the set of the tools developed within this project some aspects could be considered. In future projects a more detailed analysis on legislative aspects could be conducted. As an example, the tool could be made compliant with risk assessment methodology standards, for example, the CEN standard recently released on Railway applications – Cybersecurity (CLC/TS 50701[6]).

The iCrowd simulator, as part of the S4RIS platform, follows a scenario-based risk assessment. An incident is detailed and implemented in the simulator. User-tailored metrics are calculated and extracted that aid in the evaluation of any resilience and mitigation strategies that are studied. The evaluation is done separately per scenario but having multiple runs of the same scenario with varying parameters is a common way of obtaining statistical data. Metrics such as the probability of detection by a CCTV camera, the probability of a

person surviving an evacuation based on its initial position, etc. required complicated implementations and extended testing, and are now available for use in future projects.

Simulation of risk scenarios

The simulation exercises conducted in the context of the SAFETY4RAILS project required 3D models of railway stations and underground metro stations, which is an expensive and time-consuming task. Thanks to the collaboration of many partners of the project (NCSRD, MDM, STAM, RINA, EGO), detailed and annotated 3D models were developed in the form of 3DMax and OBJ files. These are now available for use in future projects.

The main steps needed in order to simulate risk scenarios are in general the following:

1. Generation of risk scenarios: starting from the topology of the railway network and the modelling of related infrastructures, possible risk scenarios combining the following parameters: type of threat, severity, target, and time of occurrence need to generated.
2. Simulation of the risk scenarios: the scenarios already generated are simulated considering on one hand the effectiveness of the countermeasures, which could contrast the threat, and on the other hand the cascading effect, which can generate secondary threats. For each scenario, indeed, a possible set of outcomes is simulated.
3. Computation of the likelihood and impact of each outcome: for each outcome simulated, the likelihood of occurrence and the potential impact are computed using data-driven analysis.
4. Computation of risk: for each outcome, a quantitative risk level is computed as results of the combination between likelihood and impact.

An approach which could be explored in future project is the creation of a common template for the collection of information regarding risk scenarios which would be simulated.

The adoption of a common template could first of all facilitate the collection of information from case study owners, secondly it could make clearer for everyone how the scenario should flow. It could be useful in defining in detail which asset and element of the networks have to be considered in the railway network and how they will be affected by the threats. This could even support in the verification of the validity of the results produced by the platform.

3.2.3 Risk management strategy

Simulation and prediction tools

The complicated process of simulating a security or safety incident involving large crowds and cyber-physical assets has been largely improved in the context of the SAFETY4RAILS project.

Within the iCrowd simulator, functionalities related to the crowd movement through automatic escalators, CCTV simulation, detection evasion, and detailed collection of spatial-based data and statistics, progressed significantly. Any and all developed functionality follows an abstract implementation, agnostic to the specific domain of application, enabling its use in future projects that may be unrelated to the railway and metro sector.

The new extensions also allow for future development of iCrowd's behaviour modelling, including but not limited to guards' distraction simulation, advanced detection evasion, and knowledge-based navigation and decision making.

The mitigation measures currently proposed in the S4RIS could benefit from including, in future research projects, a cost benefit analysis directly in the asset management system. This would ensure the correct estimation of the various elements of the railway network and allow the operators to choose the mitigation measures that are the most efficient and cost-effective, based specifically on their individual network and assets found therewithin.

Regarding the prediction tool DATAFAN, main lessons learnt were:

- A reliability score of the prediction increases technological acceptance and helps the end-user in the decision-making process.
- An intuitive user-interface is crucial.
- A comprehensive manual and tutorial provide easy access for all user groups, thus improving the user experience.
- A web service as the next development step will enable a wide range of possible applications.
- In order to get realistic results and not only “what is possible if… “ it is mandatory to get real data. In SAFETY4RAILS, we got first real data that were found in the www, e.g. for the S1 in Hamburg.
- On the other hand, we got real data from the involved end-users, namely MDM, EGO, RFI and CDM. Therefore, we want to thank all these partners for providing the real historic data. We know that there are many data protection issues, and therefore, very often real data are rare.

Main feedback regarding prediction tools involved in the crisis management was that a reliability checking for the provided results by the tools is very helpful. For future projects, this reliability checking should be standardized and done for all or at least a large part of the results of the tools and not only for a few tools and results.

Policy planning and investment measures

CAMS contributed to scenarios, calculations and engagement with the railway infrastructure, and investment measures that supported the prevention, and mitigation aspects addressed in the recovery phase. Data introduced by end-users to CAMS is divided into the following categories: assets inventory (component data), topology and type and quantity of elements.

In order to determine the overall configuration of a system, it is first necessary to determine the type of element or component group that is needed. Based on the probability of the component, a rehabilitation budget can be calculated. A conceptual model determined by CAMS includes the following recommendations:

- Required cost.
- Available funding.
- Cumulative difference.

The planning and investment measures require the selection of maintenance actions every year for individual assets based on the deterioration rate of their asset groups and the damage matrix of extreme events. So, the main lesson learned for future research projects is achieving dynamic resilience by ensuring the accuracy of the component classification and developing a historical and inspection data base for infrastructure components under synergy with real time data.

3.3 PROTECTION phase

3.3.1 Monitoring method

Threat Intelligence is a crucial part of modern security programs and needs to be approached directly. There are different levels of maturity in Threat Intelligence programmes and the first step usually starts consuming Open-Source Intelligence (OSINT) feeds about threats. During the SAFETY4RAILS project, the TISAIL tool tried to bring context and tailor the threats to the railway and metro stakeholders.

However, this task was not easy since there was not much information about the IT/OT assets used by the stakeholders nor a threat model, in order to understand what parts of the railway infrastructure is more important and what threats should be monitored.

In future research projects, the importance of having further cooperation between stakeholders and Threat Intelligence providers/tools should continue to be taken into consideration. The Threat Intelligence providers need to have detail and context about the stakeholder's infrastructure to provide accurate and tailored threat intelligence.

3.3.2 Cascading effects analysis

In future research projects, the algorithm for the cascading effect analysis could be improved in various ways, one of which could be the collection of historical data concerning various type of threats in order to increase the algorithm's efficiency. Historical data would be useful in two ways:

- First, the collection of such data would be fundamental in order to create a general data set in which for each threat several historical events would be described in detail with assets and countermeasures involved. Such datasets would be fundamental in order to define several patterns of cascades specific for the railway sector.
- Second, it would allow the algorithm to conduct its analysis in advance without having to know exactly the interconnections among the elements of the railway network. This would result in a faster and more accurate algorithm capable of providing more realistic results to the end users and be even faster.

3.4 DETECTION phase

3.4.1 Anomalies and events detection

For what concerning future smart CCTV improvement related to the functions employed in Ganimede, the following lessons learned should be taken into account:

- Audio detection: the experiments were conducted in a controlled environment. The next steps are aimed at ensuring scalability in the operational environment.
- Abandoned object detection: the temporal and spatial parameter depend on the camera point of view and the FPS (Frame Per Second) and are set up with configuration files. The next steps are aimed at allowing the operator to easily configure such parameter through a GUI.
- Man down: the man down detection relies on person detection itself. If there are occlusions that prevent person detection, the man down detection is not feasible. The system is meant to raise an alarm if a person is down and nobody is there. If there is a crowd of people around the man down, no alarm is raised because occlusion prevents the system to work properly. Improvement should be done in order to minimize this effect.
- People re-identification: the functionality provides the operator a list of images of people wearing clothes similar to who is being searched. Improvements should be made to the algorithm in order to reduce the number of possible matchings which is quite high.

Regarding cybersecurity threats, TISAIL is a prevention tool that can be used also for detection. The Indicator of Compromise (IoC) and TTPs (Tactics, Techniques and Procedures) could be used for detecting Threats in security defence mechanisms such as EDRs, Firewalls or SIEMs. In future research projects, it should be addressed a better integration between Threat Intelligence and detection tools. Automation might be a very important part of this integration, but also to produce actionable intelligence, including detection signatures (Suricata, Yara, Sigma, etc) and also to have the right detection tools.

Regarding anomaly detection from time series data, WINGSPARK platform provides anomaly detection components to detect potential incidents in the railway infrastructure that could result in potential cascading effects. In order to provide more useful insights the integration of adittional data sources will be needed. Currently, the tool uses simulated time series train speed data, from 1 train. These data have been artificially augmented in order to simulate more than one trains and for a longer time period. In the future, the tool could utilise real-time train speed data coming from IoT devices (i.e., from speedometers onboard the trains), which together with the GPS location of each train could be used to enhance the tool's results. These data could be further enhanced with data from other sources such as trains timetables, number of people in each station etc. In the future, the developed anomaly detection mechanisms could be utilized in the context of a risk assessment tool, which would provide the probability of anomalies detected evolving into a cascading effect. WINGSPARK has been configured to be able to accommodate such a pipeline, which could output the probability of a hazardous incident, providing valuable information and insights, to take measures to avoid such a situation.

Furthermore, WINGSPARK can detect overcrowded situations in the monitored railway infrastructure, based on video acquired through CCTV cameras. With this input, dynamic evacuation plans can be proposed in case

of emergency. Currently, sample videos from Rome and Milan have been used in order to train the Neural Network that has been constructured as part of the tool. In the future, additional steams from CCTV cameras deployed at the stations that will provide streams in real-time could be directly integrated with WINGSPARK in order to detect potential incidents in real-time. All these mechanisms provide a holistic approach in enhancing safety and security in trans-modal metro and railway networks while their integration in the S4RIS GUI provides useful insights to the stations' operators, enabling the efficient infrastructure monitoring and timely detection of potential incidents.

3.4.2 Real time monitoring

Related to anomalies detection capabilities, within SAFETY4RAILS, the partners (in particular CuriX) partially simulated the existence of several different datasets, e.g.

- Number of turns of turnstile machines.
- Consumption of energy of the whole station (or assets).
- Status of doors (open / closed).
- Sound levels in stations.
- Meta-information of messages in Passenger Information System (e.g., average line lengths).
- Number of passengers currently in station.

For these data sets, it was simulated a sampling rate of 2 minutes in which the respective number to generate time-series out of those data was retrieved.

Detecting anomalies on those simulated data has led to the conclusion that the monitoring of the above-mentioned data would lead to further situational awareness for railway stations. The recommendation for future projects therefore would be to consider (in particular when resilience is a major topic) also the analysis of the potential of not yet existing datasets as a driving moment to develop sensors to generate such data.

3.5 RESPONSE phase

3.5.1 Crisis management

S4RIS prototype includes the RAM^2 tools which provides comprehensive visibility into the data from many of the contributory tools, turns that data into useful information, and promotes risk reduction activities based on smart prioritization and clear action plans. It serves as a Decision Support System (DSS) for helping railways and metro operators to manage incidents and crises.

The main elements needed as part of DSS are the following:

- **Alerts** indicating the severity of the issue and providing related details.
- **Vulnerabilities** Database and threat intelligence with the possibility to analyse asset information and automatically map between assets and vulnerabilities.
- **Insights**: the DSS generates insights by correlating indicators and alerts, together with known vulnerabilities, asset details, operational data, security posture, and other types of data to detect suspicious patterns.
- **Case**: to enable the creation of a case from an alert, a group of alerts or an insight. A case enables the tracking of all activities for resolution and mitigation of risk with respect to a specific scenario.

3.5.2 Crisis communication

Lessons learned regarding crisis communication include:

- Lack of academic research dedicated to this topic within the domain of railway and metros.
- Importance of taking into account the emerging emotions of passengers and station visitors associated with the crisis.
- General crisis communication guidance is applicable to cyber-attacks, with some additional considerations.

- Websites and social media are preferred by end-users for short-term crises whereas traditional mass media (TV, radio) is more appropriate for long-term crises.
- Crisis communication from rail/metro stakeholders should use a high level of security and ethical scrutiny, as these aspects affect company reputation and willingness of clients to return to the infrastructure post-crisis. This includes the handling of sensitive information and compliance with relevant legislation such as GDPR.

Suggestions for future research projects include:

- To perform academic studies on the crisis communication of rail/metro stakeholders.
- Research how rail/metro crisis communication can take into account/influence the emotions associated with a given crisis.
- Elaborate on the uniqueness of crisis communication for cyberattacks.
- Test all the SAFETY4RAILS crisis communication guideline recommendations in a controlled setting with citizens.
- Develop the pre-defined messages to be used by rail/metro stakeholders by using co-design and co-creation with the general public and vulnerable groups.
- How to improve awareness of ethical-security risks that exist in crisis communication and articulating mechanisms/methodologies to mitigate them.

3.6 RECOVERY phase

CAMS was one of the main software developments in the recovery phase. Many data exchanges could potentially be possible with other software artefacts, and some have been combined for further study, such as access and provision of asset management tool functionality to meet future end-user requirements.

Effective budgeting for investments in resilience enhancement in response to cyber-physical incidents depends on the categorization and prototyping of the various incidents. Therefore, digitising cyber-physical events can generate additional vulnerabilities information for CAMS, which can make budget charts and predictive investment models more accurate.

In the future, there should be an enhanced mobility tool included in condition survey research, such as:

- Integrated audit management functionality.
- The ability to record photos and other inspection results in the system.
- Flexible hierarchy and condition rating system.
- Data quarantining and quality assurance checks are part of the functionality of the application.

4. Policy impact

4.1 Contribution to compliance with CER and NIS directives

The SAFETY4RAILS project actively contributes to the efforts of railway and metro system operators to mitigate risks against their critical infrastructures and increase their resilience. The project has brought together in the SAFETY4RAILS Information System (S4RIS) platform a series of cutting-edge risk management tools that could assist railway and metro system operators mitigate risks posed by cyber and physical threats in five phases: Identification, Prevention, Protection, Detection, Response and Recovery.

The S4RIS platform could be used as an example of a multi-tool platform that could address operators' concerns and in particular their compliance with obligations introduced by the (soon to be adopted) Critical Entities Resilience (CER[4]) Directive and Directive for a high common level of cybersecurity (NIS 2[5]). More specifically:

- **Risk assessment**: Risk management is a prerequisite for the resilience of railway and metro infrastructures against all types of threats. As such, it is the cornerstone of the security obligations introduced by both CER and NIS2, which require operators to conduct risk assessments and take resilience enhancing measures against all relevant threats, including disaster risk reduction and climate adaption measures, and risk analysis for information system security. The S4RIS tools SECURAIL and RAM^2, for example, allow for the cyber-physical risk assessment of railway infrastructure.

- **Early detection**: Early detection and identification of threats is a crucial step to mitigating and potentially preventing a threat. The S4RIS platform has incorporated several tools to ensure that operators can enhance their resilience through threat monitoring and intelligence, including anomaly detection tools CURIX and WINGSPARK, vulnerabilities and threats alerts provided by TISAIL, object detection tool GANIMEDE.

- **Simulation and prediction**: SAFETY4RAILS supports compliance with the obligation of putting in place an effective crisis management plan through simulation and prediction tools such as BB3d, CAESAR, DATAFAN and SARA.

- **Planning and business continuity measures**: The current legislative framework requires operators to take measures for implementing the proper protocols and tools to handle a crisis, but also to recover from it and to ensure business continuity and disaster recovery. S4RIS contributes overall to resilience.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0829

[5] https://www.nis-2-directive.com/Proposal_for_a_directive_on_measures_for_a_high_common_level_of_cybersecurity_across_the_Union.pdf

4.2 Contribution to standardisation and certification

The current state of the art of the Cyber Certification in the Railway domain is based on ISO 270xx[6] family, IEC 62443[7] and CLC/TS 50 701[8].

CLC/TS 50 701 requirements are derived from the "mother" specification IEC 62443 and specialised for the railway environment. Such requirements represent the European standard approach to cybersecurity in Railway sector. The process to follow for the assessment described in the CLC/TS 50 701 has been developed following the steps of the well-known safety assessment process. In this way the two assessments have the same steps, of course with different aims. At the end of the security assessment there is a Security Case that will be maintained along the whole life cycle of the system.

The assessment process can take advantage of the tools defined in the SAFETY4RAILS project. For example, the risk assessment can be supported by SecuRail, RAM[2] and TISAIL; the early detection of threats can be supported by GANIMEDE, CURIX, WINGSPARK and iCrowd.

For future application in the railway sector, a standardisation of the true random number and cryptographic key generation schemes is needed since the Random Generation Number mechanism can be hacked. Due to the application of new technologies like Artificial Intelligence (AI) and BlockChain an additional effort in upcoming standardisation activities is required.

The cyber security certification is at the very beginning in the Railway domain. A multipurpose platform as S4RIS is a powerful tool but how this can interact with the certification process it is not easy to identify due to lack in applications.

4.3 Main SAFETY4RAILS Policy recommendations

The main policy recommendations from the project are as follows:

- Encourage operators to adopt a holistic cyber-physical approach to threats.
- Align the implementation of CER & NIS 2 Directives in Member States.
- Promote formal synergies in their enforcement.
- Promote best practices for ethical crisis communication and data management.
- Additional effort in standardisation activities to capture new technologies (e.g., AI, Block-chain) and to address specific requirements for supporting tools.

[6] https://www.iso.org/isoiec-27001-information-security.html

[7] https://www.iec.ch/blog/understanding-iec-62443

[8] https://standards.cencenelec.eu/dyn/www/f?p=CENELEC:110:441725248219701::::FSP_PROJECT,FSP_ORG_ID:67491,1257173&cs=150C0A9CE083269A7DA4B0A3E2EA7DA11

5. Lessons learnt from the stakeholders engagement

5.1 Uptake of the results by the operators

5.1.1 Introduction

Railways and metro operators had a key role in the SAFETY4RAILS project as they are the future customers / targeted final users of the S4RIS platform. Their involvement in all stages of the project has ensured that SAFETY4RAILS is of value to them.

It started with early engagement activities during the requirements definition phase to ensure they were based on their real needs: questionnaires, dedicated sessions and several workshops have been organised with the end- users who were part of the project as well as with a broader range of experts thanks to the project advisory board.

Engagement continued via participation in simulation exercises and the evaluations of the solutions based on the demonstrated operational scenarios.

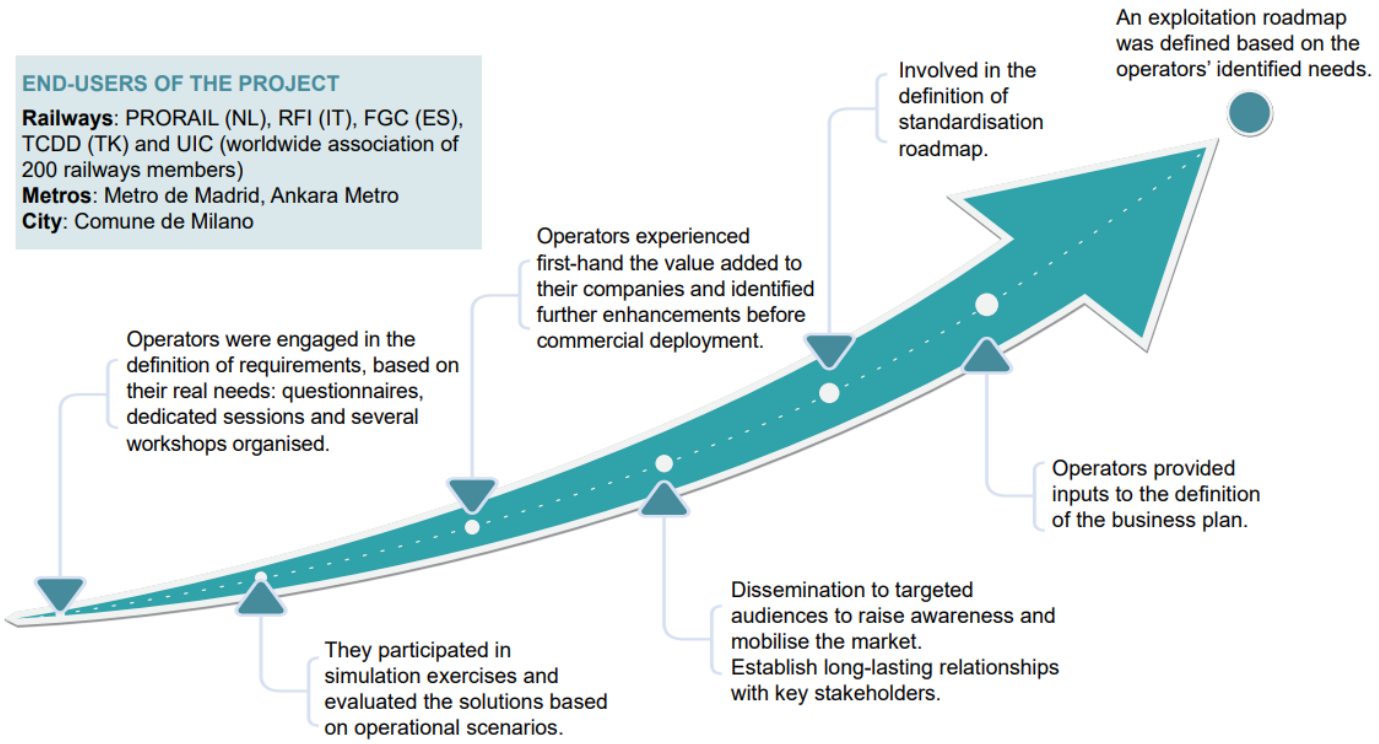

FIGURE 6 - SAFETY4RAILS UPTAKE OF RESULTS BY THE OPERATORS

5.1.2 End-user needs and lessons learnt

Based on past failures analysis and end-users consultation at the beginning of the project, an overview of threats and risks faced by railways and metro operators was generated, organised via the type of incidents, the involved or concerned stakeholders and the segments and/or assets targeted or impacted. From the analysis of past failures reviewed and co-validated with end users, the following key trends were derived:

- A rise in recent years in the proportion of cyber-attacks amongst the incidents, especially those with criminal motivation.
- The rail and metro sector experience the same increasing convergence between logical and physical security that is observed in other OT (Operational Technology)-related environments.
- Lack of awareness about security was identified as a one of the key factors in security related incidents and indicates the importance of human factors.

Thanks to collaboration with end-users, 64 high-level end user needs and requirements were formulated. Each one was described and coded with a priority rank, corresponding threats events and motives they address and the corresponding risk and threat management phase.

Six majors trends were derived from this list of 64 high-level end-user needs and requirements:

1. Improvement of both internal and external communications, in a sector where crisis management involves a large number of stakeholders - both internally within different services of the impacted transport company and externally to exchange information and collaborate with other stakeholders (for instance, law enforcement or first responders).
2. Ensure secure systems and assets. As a critical infrastructure rail and metro operators must ensure safety and security of passengers and goods transported via their infrastructures. Management of security services, securitisation of access to systems and assets, encryption procedures and techniques to ensure data protection and security are some examples of security measures.
3. Closer cooperation with authorities is a key element of crisis and incident management, via, for instance, operation information exchanges facilitated by dedicated systems, coordination of measures and actions implementation, joint trainings, harmonisation of standard operation procedures (SOPs).
4. Advanced monitoring and detection capabilities, as a condition to collect necessary information for continuous situational awareness update aiming at close as possible to real-time.
5. Use of simulation for anticipation, prevention and/or mitigating the impact of an incident that should be designed to integrate a massive amount of data and information to correctly simulate cascading effects within railways and networks and assets, characterised by their variety of interdependencies and complexity.
6. Management of data flows to support decision-making, aiming at the provision of added-value information, to improve significantly their capabilities to properly address risks and threats before they occur or when the crisis is emerging.

5.1.3 Specific requirements for multimodal transport

Multimodal transportation is also a key element of the smart city. One of the key conclusions when dealing with multi/intermodal aspects and transportation hubs is the importance of cooperation between all involved stakeholders at every stage of the resilience approach.

Main requirements that can be highlighted are the following:

1. Joint risk and threat assessment needed in a multi-modal transport hub.
2. Mutual early warning system between companies operating means of transport that are not directly connected to one another.
3. Direct and immediate security incident reporting between different stakeholders of a common transport hub.
4. Early warning system/ information exchange with cross-border partners.
5. Interoperability between stakeholders and between different critical infrastructures in a given urban area.

Beyond the identification of the requirements for multimodal aspects based on the needs of the end-users, managing of crises was identified as a key aspect with regards to the resilience of multi-modal transport systems and is also a precondition for effective crisis communication, aspects addressed in sections 5.1.1 & 5.1.2.

5.1.4 Evaluation of the S4RIS platform by the end-users

Introduction

From January 2022 until July 2022, four simulation exercises were performed based on operational scenarios as described below:

- **Madrid (Metro de Madrid):** Combined cyber-physical attack at the metro station close to the stadium during a large sporting event.
- **Ankara (EGO and TCDD):** Series of cyber and physical attacks targeting sensitives devices and sensors.
- **Roma (RFI):** Physical attack – Potential terrorist attack via IED (Improvised Explosive Device) carried via baggage and terrorist using firearms inside a railway station.
- **Milan (CDM):** Natural Disaster - Flooding in the city during a major event.

Each simulation exercise was evaluated by the end-users through questionnaires, debriefings and focus groups. The evaluation focused on two main aspects:

- The organisation of the exercise (as carried out).
- The performance of the S4RIS against pre-defined objectives related to:
    - Usability.
    - Specific requirements laid out by the end-users in SAFETY4RAILS Deliverable D1.4.
    - Scenario-based requirements/objectives identified in SAFETY4RAILS Deliverable D8.2 and in SAFETY4RAILS Deliverable D8.3 (referenced back to e.g. tool the specific requirements / specifications identified in D1.4).

Within the time between the simulations, the identified proposals for improvement of the solution and further evaluation were taken into consideration where possible. This iterative process was very useful to improve both the tools and the organisation of the exercises.

In addition, a demonstration of the Risk Management Planner tool developed by ETRA, was performed on the 12th of September with FGC as end-users. The description of this demonstration as well as the evaluation by FGC is described in ANNEX II. RISK MANAGEMENT PLANNER (D7.2) DEMONSTRATION AND END-USERS' FEEDBACK - FGC.

Main lessons learnt from the evaluation by the end-users

In general, S4RIS platform as well as the capacities of the individual tools were appreciated by the end-users, with the majority of them evaluating that the objectives were successfully met, the output useful for the related resilience phases and the GUI of the tools user friendly.

Main added value of the tools highlighted by the end-users was the following:

- **The combination of the capacities** of the tools such as detection coupled with prediction capabilities can contribute to resilience assessments of critical infrastructure in case of cyber-physical attacks. Moreover, the dashboard **grouping all the alerts** coming from the different tools addressing both cyber and physical threat provides a very good situational awareness to the end-users.

- **The simulation capacities** bring a lot of added value for managing cyber and physical risks and helping decision makers on the measures to be put in place to make rail and metro systems more resilient, e.g.:
    - The knowledge on how the detonation of an explosive device could affect the railway/metro infrastructures would help to make them more resilient in case of an attack**: this would have a clear impact on reducing deaths and injuries.**

    - Enabling off-line analysis to understand the level of risk for each critical asset during a given hazardous event **may contribute to the risk management process and help the user to compare the different measures and select them.**
    - Provision of information on the asset condition and degradation due to normal ageing or after a set of possible events may **help to plan budget and improve asset obsolescence management, especially those in OT environments.**
    - In the prevention phase, the simulation of crowd in case of different events can be used **to improve the design of the infrastructure** as well as **the implementation of CCTV** taking into account blind spots. In the response phase, it can be used **to take decision on the closure or not of the station and on the best way to evacuate the station.**
- **The detection tools** which demonstrated early detection of anomalies or vulnerabilities were appreciated by most of the responders for **anticipating situation and preventing or mitigating the consequences of cyber and physical attacks.**

The possible improvements that were mentioned are the following:

- Simulation capacities would benefit from more accurate data as well as more variables.
- The integration of the S4RIS tools with the company information systems would need to be assessed.
- The integration of tools in the S4RIS platform should be further developed.
- Inclusion of user manuals and change management schemes, adapted to each end-user, for the adequate implementation of the S4RIS platform in different environments and OT systems.

The main challenges that should be taken into account in further research projects are as follows:

- **Provision of operational data:** many SAFETY4RAILS tools are based on data and required large sets of data to make the scenarios more realistic and better assess the solutions. Given the sensitivity of data, data regulations and also the short timeframe to provide the data, the provision of real data was a challenge. Despite this, open data, artificial data as well as historical data provided by the end-users in each simulation exercise were used and allowed to demonstrate the tools capabilities and assess them in an operational context.
- **Organisation of the simulation exercises:** The simulation exercise could be designed in a more interactive way with the possibility for the participants to “play“ with the tools and have more time to discuss with the tool providers. Future simulation exercises could be organized at an actual premises of the railway stations or metro station: a test site would allow to have real sensors and to demonstrate the tools in even more realistic conditions. More stakeholders, such as authorities, other transport operators and infrastructure managers, should be participating in the exercise. This was difficult to organise in SAFETY4RAILS in the context of the covid19 crisis first and then the Ukrainian-Russian war.
- **Evaluation methodology**: It has been very challenging for the end-user representatives to evaluate the solutions for several reasons:
    - The duration of the project was very short (2 years) with a very broad scope (resilience against physical and cyber threats), many tools (19).
    - Online meetings since the beginning of the project due to the pandemic crisis make more difficult the understanding of such a large project.
    - The tools are very innovative, most of them are based on artificial intelligence which is at a very early stage within rail companies.
    - Many different areas of expertise were needed to answer the questions, so that experts from one domain were not able to answer questions pertaining to another and vice versa.
    - During the simulation exercise, the tools were presented in a relatively short timeslot. To be able to really evaluate the system, it would be worthwhile to use the system / its tools and to understand the numerous capabilities. It is accepted that this was an intrinsic challenge for SAFETY4RAILS given its starting point and duration. When planning future exercises and evaluations it will be useful to think about how this could be achieved.

5.2 Go-to-market Roadmap: Industrialisation of results and Engagement with EU buyers

SAFETY4RAILS is an Innovation Action funded under the H2020 programme, where most of the results reached at least Technology Readiness Level of 7 – System prototype demonstration in operational environment[9]. Intrinsically, a gap remains between the readiness of the project outputs and the full commercial deployment.

To bridge this gap, the project has developed a **Strategic Roadmap** for each of the project exploitable results and put a special emphasis on the Key Exploitable Results (KERs), selected among the most promising results to be marketed. Each partner owning an exploitable result, produced an individual exploitation plan defining the next steps to be conducted to **guarantee impact beyond the project**. This included required activities, milestones, resources, funding opportunities and a timeline to achieve commercialisation – in the case of commercial/business partners, and transferring the technology to the industry – in the case of research partners. The assessment of the individual exploitation plans concluded that most of the exploitable results are expected to achieve TRL9 before 2025Q4. Some are ready for exploitation now.

Apart from the individual exploitation, the Strategic Roadmap was designed to incorporate the **join exploitation of results**. A set of joint results were defined based on the open discussions of tool providers, who were eager to collaborate in the future under joint exploitation agreements, as well as through new R&D projects. Focusing on the exploitation of the SAFETY4RAILS Information System (S4RIS), the consortium identified the relevant IP, the partners to be involved, and a detailed roadmap to take the platform to the market. EU-funded Pre-Commercial Procurement was identified as a suitable mechanism to **de-risk the roadmap**. Risk reduction will be achieved thanks to unlocking the necessary resources to take the technology up to TRL8, as well as the engagement of EU buyers in the final stages of development, while taking shares over the future product commercialisation. The roadmap was designed taking into account the feedback from the end-users' validation in WP8 and is split in three phases, as defined in D10.9:

- **Phase 1 – Preparation:** at least one-year-long following the end of the project
- **Phase 2 – Industrialisation:** Years 2 & 3 after Phase 1
- **Phase 3 – Commercialisation:** Years 4 & 5 after Phase 1

In parallel, the **core business mechanisms and strategies** to take the KERs developed by commercial partners to the market were defined. Emerging business models were produced, including business model canvas, risk assessment to discover the most relevant barriers and mitigation measures, and financial viability assessment. A market analysis of railway security was used as another key input, including the size, structure, trends, drivers, economic growth and competing solutions in the sector. A competitive benchmark analysis was performed as a fundamental step for the definition of the value proposition.

Overall, while there are some mitigation measures proposed to very specific risks, the **assessment of the business feasibility is positive** from both the strategic and financial perspective. Regarding the S4RIS commercialisation, it was concluded that PCP would contribute as a key enabler of the platform exploitation.

[9] https://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

Term	Definition/description
AI	Artificial Intelligence
CCTV	Closed Circuit TeleVision, commonly known as video surveillance
CDM	City de Milan
CER directive	Critical Entities Resilience
DMS	Distributed Messaging System
DSS	Decision Support System
EDR	Endpoint Detection and Response
EGO	Ankara Metro
FPS	Frame Per Second
GUI	Graphical User Interface
HSM	Hardware Security Module
ICMT	Incident & Crisis Management Tool
IEC	International Electrotechnical Commission
IED	Improvised Explosive Device
IoC	Indicator of Compromise
IoT	Internet of Things
ISO	International Organization for Standardization
JSON	JavaScript Object Notation – It is text format for storing and transporting data.
KAFKA	open-source distributed event streaming platform
KER	Key Exploitable Result
KPI	Key Performance Indicator
LDO	Leonardo
MDM	Metro De Madrid
NIS directive	Network and Information System Security directive
OT	Operational Technology
OSINT	Open-Source Intelligence
PCP	Pre-commercial Procurement
RFI	Italian Infrastructure Manager
R&D	Research & Development
S4RIS	SAFETY4RAILS Information System
SIEM	Security Information and Event Management
SOP	Standard Operation Procedure
TCDD	Turkish railways
TRL	Technology Readiness Level
TS	Technical Specifications
TTP	Tactics, Techniques and Procedures

ANNEX II. RISK MANAGEMENT PLANNER (D7.2) DEMONSTRATION AND END-USERS' FEEDBACK - FGC

Under the scope of **D7.2: Consequence cost model various failure scenario**, ETRA developed the Risk Management Planner tool. The tool allows the railway infrastructure user to select different threat scenarios/combination of threat scenarios to automatically compute the optimal budgetary strategy and minimise the economic consequences to the organisation when responding and recovering.

The tool was technically assessed and verified for functional performance under the same deliverable, where Section 6.2 reflected that a demonstration session was planned in early September 2022 to complete the validation and gather the feedback from an end-user. The demonstration was performed on the 12th of September under the scope of WP8 with FGC as end-users – who also contributed with data to the development and is reported in the following lines of the present deliverable. The format was an online meeting via MS Teams.

FIGURE 7 RISK MANAGEMENT PLANNER – FGC DEMO ON 12TH SEPTEMBER 2022

The demonstration had as the main objective to collect feedback regarding the meaningfulness and usability of the tool. To accomplish this, a general explanation of the tool was performed, followed by a live demonstration and a hands-on session where the end-user used the tool in a set of pre-defined exercises. The objectives of the tool cover the following:

- Cover **natural, cyber, physical and cyber-physical threats** in the railway and metro environment
- Mitigation strategies in **response and recovery** against the threat
- **Prevent future impacts** on the infrastructure
- **Explore different scenarios** or combination of scenarios
- **Open and flexible model**, which allows new components to be introduced as the user wishes.

The agenda of the demonstration session included the following:

- **Objectives** (as described above)

- **Introduction to the tool**, including the main components of the risk assessment framework and the output provided to the end-user
- **Live Demonstration**, with an explanation on how the model is setup in the tool and an example scenario based on Metro de Madrid Simulation Exercise
- **Hands-on Exercise**, where the end-user is given access to the tool and operates it under specific pre-defined exercises. The user is allowed to modify some parameters in the model to understand how changes in the infrastructure can affect the consequence-cost calculation.
- **Conclusions and next steps**

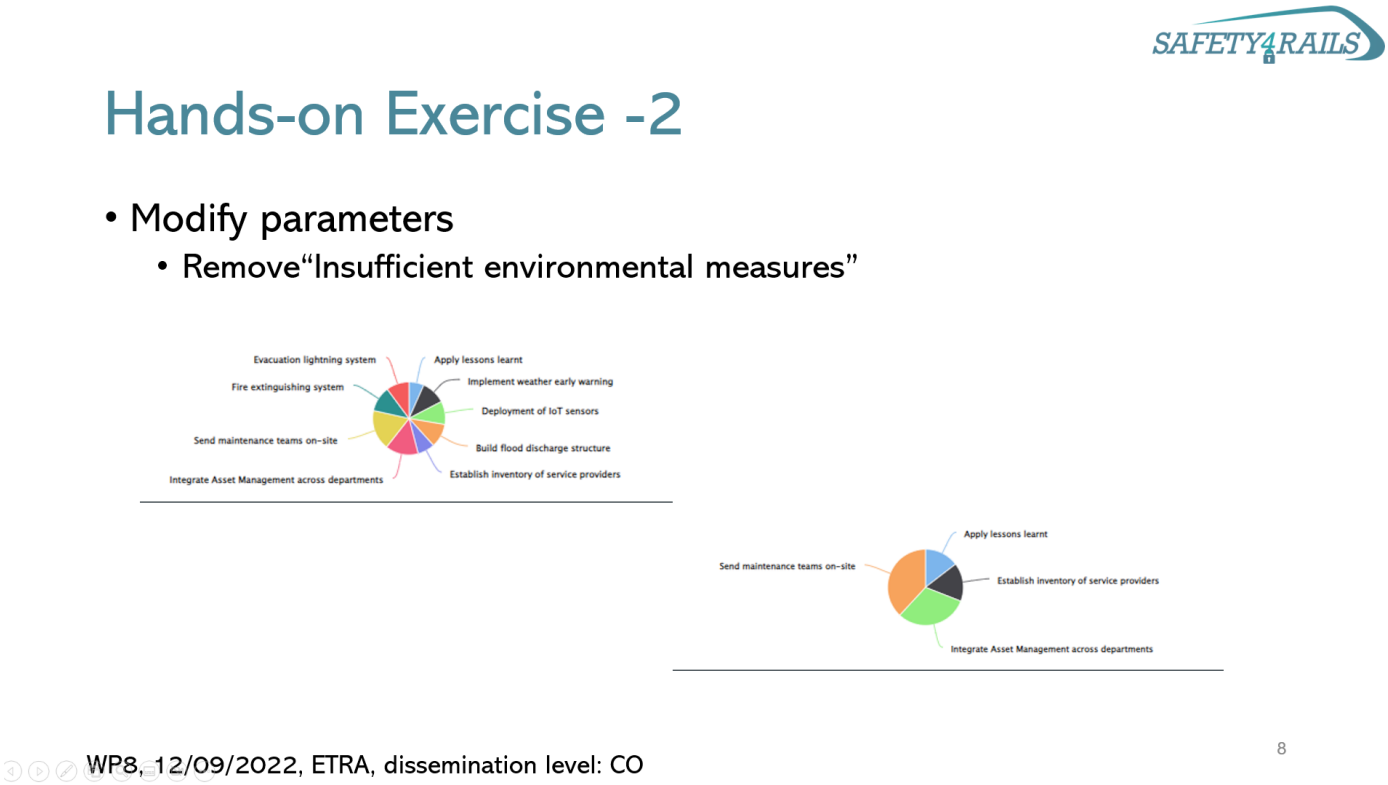

FIGURE 8 HANDS-ON EXERCISE – FGC DEMO ON 12TH SEPTEMBER 2022

As a final step, a questionnaire was sent to FGC to provide the feedback and validation of the tool. The format of the questionnaire followed the same of that used in D8.4 and D8.5. The questionnaire is reported in the next page of this Annex.

Regarding the contribution to the response phase, while it is agreed that there is no actual contribution during the response phase, the tool supports the infrastructure manager to pre-plan (before the incident) mitigation measures that could be implemented in the response phase, as described in D7.2.

S4R – HOPLON – Risk Management Planner – FGC DEMONSTRATION

Q. Were the objectives of the tool successfully met (as described in the presentation)?

a) Strongly agree
b) Agree
c) Neither agree nor disagree
d) Disagree
e) No opinion

Q. The output will help the end-user in the response phase

a) Strongly agree
b) Agree
c) Neither agree nor disagree
d) Disagree
e) No opinion

Q. The output will help the end-user in the recovery phase

a) Strongly agree
b) Agree
c) Neither agree nor disagree
d) Disagree
e) No opinion

Q. The GUI of the tool is user-friendly

a) Strongly agree
b) Agree
c) Neither agree nor disagree
d) Disagree
e) No opinion

Q. What is the added value of this tool to the response phase that you know from your current daily work?

This tool is foreseen as a planning tool to make more informed and convenient mitigation strategies to minimise the economic consequences of asset management when facing different threats. Therefore, the function of the tool happens before the incidents happen and there is no added value identified for the response phase.

Q. What is the added value of this tool to the recovery phase that you know from your current daily work?

The tool can be useful in the recovery phase in terms of planning a new strategy that addresses the potential new risks that could be detected after the incident, as well as adapting to a new situation after the incident has occurred. That is, if an incident leaves the assets in a particular status, applying the lessons learnt from the incident can lead to a new paradigm of "Overview - Context – Risk identification and analysis – Risk evaluation and treatment" which this tool could help to achieve through recalculation.

Q. How could this tool be improved in the context of the scenarios proposed?

This tool adds value when planning mitigation strategies to minimise the economic losses of asset management, hence in the prevention phase. In this case, the added value of this tool is that it provides a user-friendly GUI that helps infrastructure and operational teams to understand and calculate how to optimally spend the budget to mitigate risks.

A potential improvement, for future versions, could add the following features:

- The most significant improvement should be the addition of safety components in the calculation (on top of the economic consequences), which are the most important part of railway services, as shown in the Directive (EU) 2016/798 of the European Parliament[1].
- As mentioned in ETRA's presentation, the addition of non-tangible threats such as reputational costs is also a good improvement.
- In terms of cost calculation, it would be useful to add the feature of including the total budget for actions to take into account the budget constraint in the calculation.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0798

ANNEX III. SAFETY4RAILS Public Deliverables

All public deliverable listed below are available on the project website at https://safety4rails.eu/library/ or will become available when the European Commission officially accepts and releases them.

No	Deliverable name	Lead participant
WP2	**Requirements, specification and architecture of SAFETY4RAILS framework**	CEIS
D2.2	Report on past failure analysis and lessons learnt	CS
D2.3	System's specifications and concept architecture	NCSRD
D2.4	Specific requirements for standardisation and interoperability	RINA-C
WP3	**Development of a multilingual risk assessment tool for combined cyber-physical threats in S4RIS**	STAM
D3.3	Definition of the interface between RA tool and S4RIS	Fraunhofer
D3.4	Report on a multilingual risk assessment tool	STAM
D3.6	A specific crisis management tool	MTRS
WP4	**Monitoring Methods for S4RIS - Detection, Forecasting, Response and Recovery**	IC
D4.2	Framework and Methodology of critical components based on OSINT	INNO
D4.3	Cyber-physical threat detection with capabilities matrix intelligence	INNO
WP5	**Simulation methods for S4RIS - Prevention, Preparedness and Risk Mitigation**	Fraunhofer
D5.2	Resilience strategies for multi-modal metro and railway systems	NCSRD
D5.6	Manual for crisis management and coordination of response teams	ELBIT
WP6	**Implementation of SAFETY4RAILS Information System (S4RIS)**	UNEW
D6.1	Operational interoperability of S4RIS and logistics	Fraunhofer
D6.3	Mid-term validation and evaluation of the S4RIS system	UNEW
D6.4	Final validation and evaluation of the S4RIS system	LDO
WP7	**Policy planning and investment measures of prevention-detection-response-mitigation**	RMIT
D7.1	Investment assessment model for cost-benefit evaluation of risk mitigation and recovery	RMIT
D7.2	Consequence cost model various failure scenarios	ETRA
D7.3	Budget simulation module of S4RIS	UMH
D7.4	Resilience assessment model of optimised investment	NCSRD
D7.5	Optimised budget for a given level of resilience planning	RMIT
WP8	**Simulation Exercises and Evaluations in Operational Environments**	UIC
D8.1	Evaluation Methodology	UIC
D8.2	First version - development of a blueprint exercise handbook	LDO
D8.3	Final version of development of a blueprint exercise handbook	LDO
D8.4	First version of evaluation report	LAU
D8.5	Final version of evaluation report	LAU
D8.6	Lessons learnt from SAFETY4RAILS for future research projects	EGO/UIC
WP9	**Ethics, Legal, Privacy and Societal Aspects**	UREAD
D9.1	SAFETY4RAILS Ethical Compliance Framework (ECF)	UREAD

D9.2	Update of SAFETY4RAILS Ethical Compliance Framework (ECF)	UREAD
D9.3	Guidelines for Ethically Sustainable Crisis Communications and Information Sharing	ETRA
D9.4	Legal Framework for Certification and Standardization	RINA-C
D9.5	Data management plan	MdM
D9.6	First update of the data management plan	MdM
D9.7	Final update of the data management plan	MdM
WP10	**Communication, Dissemination, Exploitation and Training Activities**	EOS
D10.1	Dissemination and Communication Plan	LAU
D10.2	First update of the dissemination and communication plan	UIC
D10.3	Second update of the dissemination and communication plan	UIC
D10.4	Project Brochures - First version	UIC
D10.5	Project brochures - first update	UIC
D10.6	Project brochures - second update	UIC
D10.7	Citizen's engagement concept	LAU
D10.8	Market analysis and Business Plan	ETRA
D10.9	Exploitation Strategy	EOS

SAFETY4RAILS

Partners:

Fraunhofer EMI
UIC
Metro de Madrid
EGO Genel Müdürlüğü
RFI Rete Ferroviaria Italiana – Gruppo Ferrovie dello Stato Italiane
TCDD
Leonardo
ceis avisa partners
STAM Mastering Excellence
information company
RMIT University
University of Reading
etra I+D
Demokritos National Centre for Scientific Research
RINA
WINGS ICT Solutions
Newcastle University
EOS European Organisation for Security
Innova Integra
LAUREA University of Applied Sciences
CybeServices Made in Europe
erGE
FGC Ferrocarrils de la Generalitat de Catalunya
MTRS
INTRACOM TELECOM
Universitas Miguel Hernández
TREE Technology
Elbit Systems C4I and Cyber
ProRail
Comune di Milano

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