SAFETY4RAILS

Data-based analysis for SAFETY and security protection, FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS

Goal

To increase resilience against combined cyber-physical threats including natural hazards to railway infrastructure.

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

Topic H2020 SU-INFRA01:
prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe.
Grant Agreement No: 883532
Total Budget: 9.5 Million €
Start Date: 01/10/2020
End date: 30/09/2022

SCOPE

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 critical infrastructures turns metro, railway and other related intermodal transport operators into attractive targets for cyber and/or physical attacks.
The SAFETY4RAILS project will deliver methods and systems to increase the safety, security and recovery of track-based inter-city railway and intra-city metro transportation.

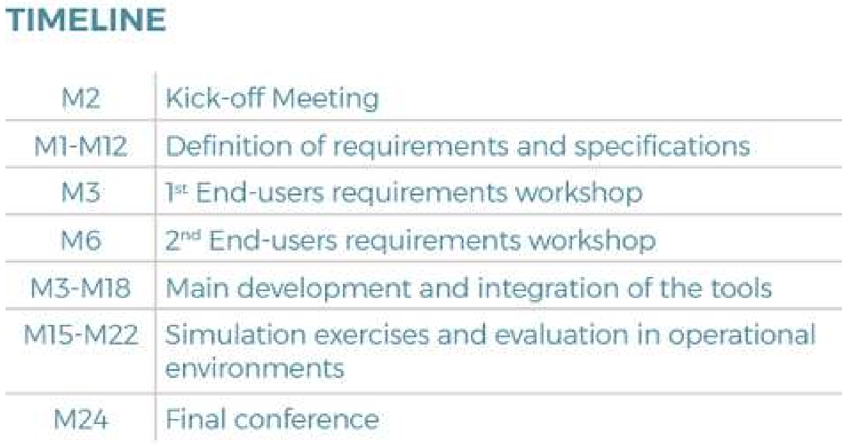
It addresses both cyber-only attacks (such as impacts from WannaCry infections), physical-only attacks (such as the Madrid commuter train bombing in 2004) and combined cyber-physical attacks, which is an important emerging scenario given the increase in the IoT infrastructure integration.

When an incident occurs during heavy usage, metro and railway operators have to consider many aspects to ensure passenger safety and security. SAFETY4RAILS will improve the handling of such events through a holistic approach.

DESCRIPTION OF THE WORK

MAIN STEPS OF THE PROJECT
The project starts by the analysis of end users' needs and requirements. In parallel and based on these requirements, at least 18 different existing tools will be adapted, further developed and implemented in an overall SAFETY4RAILS Information System platform (S4RIS). Within a resilience cycle approach, S4RIS will focus on risk assessment, risk reduction, threat prevention, threat detection, stakeholder response to incidents and system recovery.

S4RIS will then be tested and evaluated by the end-users within 2 series of simulation exercises based on different use cases. This will ensure the applicability of S4RIS in an operational environment.



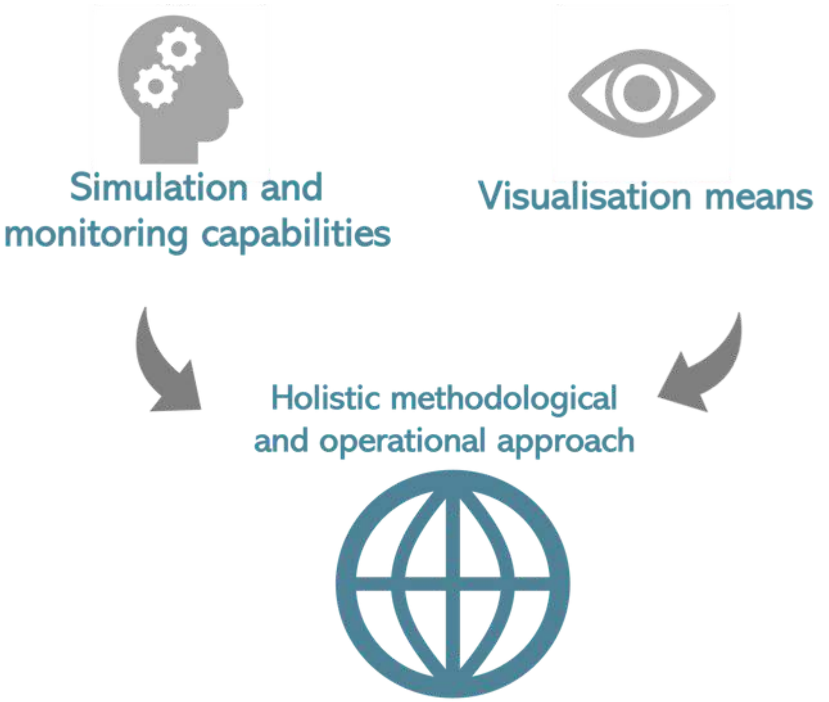
TIMELINE

M2	Kick-off Meeting
M1-M12	Definition of requirements and specifications
M3	1st End-users requirements workshop
M6	2nd End-users requirements workshop
M3-M18	Main development and integration of the tools
M15-M22	Simulation exercises and evaluation in operational environments
M24	Final conference

EXPECTED RESULTS AND ADDED VALUE

AN INNOVATIVE SOLUTION: SAFETY4RAILS INFORMATION SYSTEM (S4RIS)

S4RIS will combine **simulation and monitoring capabilities as well as visualisation means** to detect, prevent, respond, mitigate and recover in case of cyber and physical threats in a **holistic methodological and operational approach** resulting in a collaboration between cyber-physical security technologies and actors.


Simulation and monitoring capabilities
Visualisation means
Holistic methodological and operational approach

S4RIS will support managers of railways, metro, and other critical infrastructures

by identifying critical components in railway systems regarding combined cyber-physical hazards, which are addressed separately;

by developing strategies and providing decision making support to overcome weaknesses;

by decreasing possible impact caused by failures in critical components based on past experiences to foresee possible future threats.

MID-TERM ACHIEVEMENTS: Definition of requirements and specifications

THREAT/RISK OVERVIEW

Based on past failures analysis and end-users consultation, an overview of threats and risks faced by railways and metro operators was generated based on the identification of type of incidents, involved or concerned stakeholders and segments and assets targeted or impacted during both railways and metro incidents.

From the analysis of past failures, the following key trends were derived:

A rise in the proportion of cyber-attacks amongst the incidents, especially those with criminal motivation.

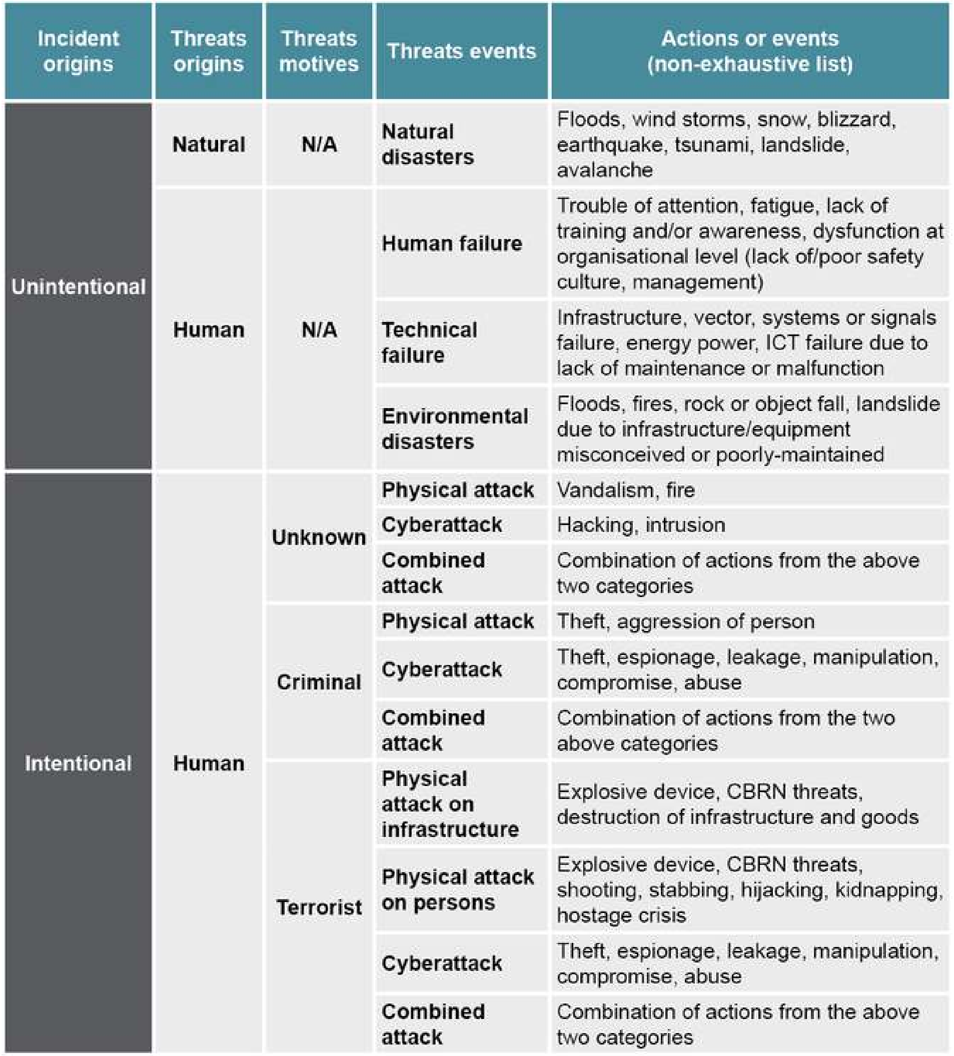
The railway and metro sector experience the same increasing convergence between logical and physical security, that is observed in other OT-related environments.

The nature of the systems applied in the sector and the typical incidents will require a special attention towards interdependencies and cascading effects.

From a security aspect, the human factor, due to a lack of awareness, is the weakest link and related requirements need to be defined within the project.

In a nutshell, threats and risks considered within SAFETY4RAILS project are divided into three main categories: physical, cyber and combined (physical-cyber) incidents.

The below table summarises the typology of threats identified within SAFETY4RAILS project framework:



Incident origins	Threats origins	Threats motives	Threats events	Actions or events (non-exhaustive list)
Unintentional	Natural	N/A	Natural disasters	Floods, wind storms, snow, blizzard, earthquake, tsunami, landslide, avalanche
	Human	N/A	Human failure	Trouble of attention, fatigue, lack of training and/or awareness, dysfunction at organisational level (lack of/poor safety culture, management)
			Technical failure	Infrastructure, vector, systems or signals failure, energy power, ICT failure due to lack of maintenance or malfunction
			Environmental disasters	Floods, fires, rock or object fall, landslide due to infrastructure/equipment misconceived or poorly-maintained
Intentional	Human	Unknown	Physical attack	Vandalism, fire
			Cyberattack	Hacking, intrusion
			Combined attack	Combination of actions from the above two categories
		Criminal	Physical attack	Theft, aggression of person
			Cyberattack	Theft, espionage, leakage, manipulation, compromise, abuse
			Combined attack	Combination of actions from the two above categories
		Terrorist	Physical attack on infrastructure	Explosive device, CBRN threats, destruction of infrastructure and goods
			Physical attack on persons	Explosive device, CBRN threats, shooting, stabbing, hijacking, kidnapping, hostage crisis
			Cyberattack	Theft, espionage, leakage, manipulation, compromise, abuse
			Combined attack	Combination of actions from the above two categories

END-USERS NEEDS AND REQUIREMENTS

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

Six majors trends were derived from this list of 64 high-level end-users 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 and collaborate with other stakeholders (for instance, law enforcement or first responders).

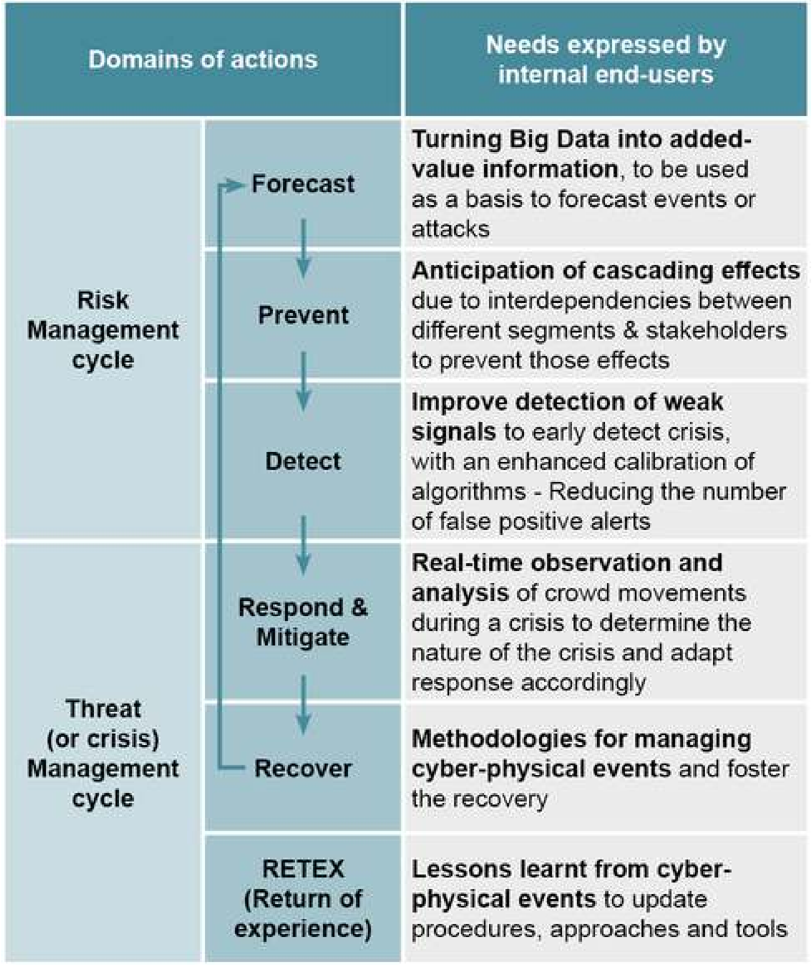
2 Secure systems and assets, as a critical infrastructure railways and metro operators must ensure safety of passengers and goods transported via their infrastructures security (management of security services, securitisation of access to systems and assets, encryption procedures and techniques to ensure data protection and security).

3 Closer cooperation with authorities is a key element of crisis and incident management, via, for instance, operational information exchanges faciliated by dedicated systems, coordination of measures and actions implementation, joint training.

4 Advanced monitoring and detection capabilities, as a condition to collect necessary information for continuous situational awareness updates aiming as much as possible to close to real-time.

5 Simulation for anticipation, prevention and/or impact mitigation of an incident that should be desgined 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 capabilities to address properly risks and threats before they occur or when the crisis is emerging.



Domains of actions		Needs expressed by internal end-users
Risk Management cycle	Forecast	**Turning Big Data into added-value information**, to be used as a basis to forecast events or attacks
	Prevent	**Anticipation of cascading effects** due to interdependencies between different segments & stakeholders to prevent those effects
	Detect	**Improve detection of weak signals** to early detect crisis, with an enhanced calibration of algorithms - Reducing the number of false positive alerts
Threat (or crisis) Management cycle	Respond & Mitigate	**Real-time observation and analysis** of crowd movements during a crisis to determine the nature of the crisis and adapt response accordingly
	Recover	**Methodologies for managing cyber-physical events** and foster the recovery
	RETEX (Return of experience)	**Lessons learnt from cyber-physical events** to update procedures, approaches and tools

MID-TERM ACHIEVEMENTS:
MAIN DEVELOPMENT AND INTEGRATION OF THE TOOLS

THE OVERALL TOOL: S4RIS

DESCRIPTION

The main output of the project is the SAFETY4RAILS Information System (S4RIS) platform, which will integrate and extend 19 tools to support rail and metro operators to manage cyber and physical risks. Most of the tools are already at TRL 5-6.

They will be further developed to meet the scope and objectives of the project. An evaluation of their performance will then be carried out at selected end-user pilot sites.

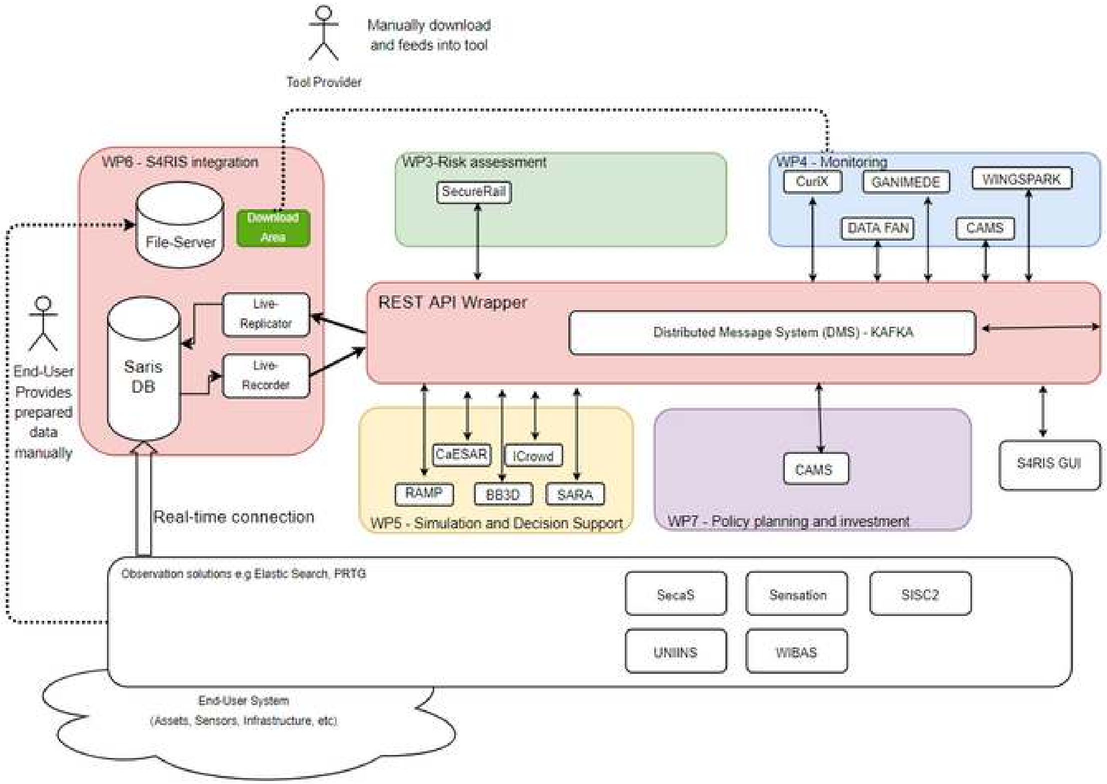
The software tools on the S4RIS platform are listed below:

- 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 that 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 a station.

ARCHITECTURE OF S4RIS

The S4RIS is a web-based decision support platform under development for SAFETY4RAILS. Between the S4RIS tools and web user interface, there is a broker that ensures effective communication and interoperability.

The added value of this configuration is increased reliability and simplicity. To further improve reliability, a store option may be added to form a 'store and forward' interface.



THE INDIVIDUAL TOOLS (1)

RISK ASSESSMENT

The SecuRail 2.0 tool will be provided within SAFETY4RAILS with the purpose of evaluating a quantitative and qualitative analysis for railway infrastructures and networks. The risk analysis will enable the identification and management of risk in advance of potential incidents.

It could also be exploited for early warning when it performs real-time analysis. The main functionalities of SecuRail are:

- Possibility to model the railway infrastructures, including assets, areas and countermeasures, through the graphical user interface;
- Modelling of connections and interdependences between different components of the infrastructures to consider cascading effects;
- Offline manual risk assessment;
- Real-time automatic Risk Assessment based on warnings from sensors and surveillance systems;
- Cost-benefits analysis to compare risk reduction with cost of security measures.

MONITORING METHODS

SAFETY4RAILS will provide tools and methods to help railways and metro operators to detect anomalies in the behaviour of technical systems, to estimate crowd concentration in case of an attack, to predict passenger load at surrounding stations, failures in IT infrastructure and cascading effects in interdependent infrastructure, to analyse video content, such as for detecting abandoned baggage, and audio content, such as for detecting gunshots. It will also provide a non-tamperable shared storage system using blockchain technology, which can also verify the integrity of anomaly detection methods, as well as open source intelligence related to cyber-physical vulnerabilities and threats.

First, the functionalities of the various solutions were identified and elaborated to design the architecture of the real-time platform components. In the next step, the solutions will be adapted, integrated and implemented with the real-time monitoring features in the S4RIS to deliver real-time information for supporting decision making of rail and metro operators against cyber-physical threats.

THE INDIVIDUAL TOOLS (2)

SIMULATION METHODS

SAFETY4RAILS incorporates a variety of simulation tools to gain a full understanding of the risk and resilience of the railway networks. This includes an agent-based simulator to model crowd behavior during different events, a predictive cascading effects simulator that investigates the effect of node failure and how the failure flows to other areas of the network, and a decision support simulation tool to aid response teams in the event of a cyber-physical attack.

Currently, these tools are being developed with specific use cases in mind, such as a combined attack with a bomb at a busy station, and a cyber attack of the signalling system of the railway infrastructure. Base models are developed, such as a 3D model of the station, or a topology model of the entire network, to be utilized in the simulations. To support the tools, a risk and vulnerability taxonomy, as well as a mitigation actions taxonomy is created.

POLICY PLANNING & INVESTMENT MEASURES

For an optimised life cycle management and proactive intervention on assets, it is crucial to know the infrastructure condition. CAMS (Central Asset Management System) can predict future damage condition based on the present asset state. The rail and metro end-user will be provided with the deterioration trajectory of each asset due to aging and to extreme events, which is fundamental for an adequate maintenance plan and budget allocation forecast.

The tool will also predict the cost for asset maintenance and repair, providing the user with an investment plan so as to comply with performance expectations. This prediction supports the asset manager’s decisions on when and where to invest to minimise the risk and maximise the profit. The end-users will also be able to analyse different scenarios of shocks and calculate the damage to asset by performing realistic predictions of the damage after the extreme event.

NEXT STEPS - EXERCISES & EVALUATION

In parallel with the development of the S4R tools, the test scenarios (four in total) are being identified and further detailed, then the simulation exercises will be described (configuration, adequate scenario description/development, different roles and tasks such as player, observer).

An evaluation methodology development is also ongoing. It will detail the process for evaluation, making use of existing established end-user evaluation methods, taking into account aspects such as usability, sustainability, technical aspects, efficiency, and other factors.

From January 2022 until July 2022, two series of simulation exercises will be performed and both attended and evaluated by the end-users based on operational scenarios according to the methodology described above. The iterative end-user validation process will help ensure uptake by end-users.

SIMULATION EXERCISES

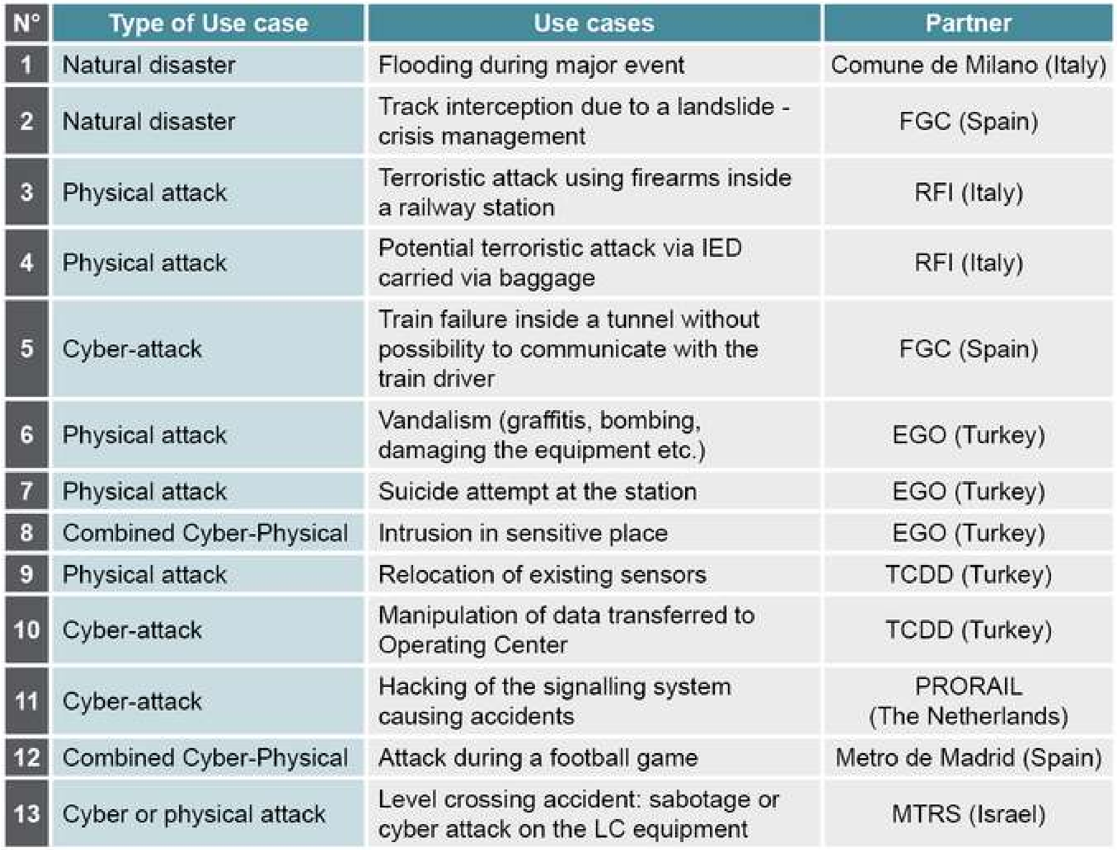
Madrid (Metro de Madrid)
Combined Cyber-Physical attack at the metro station close to the stadium during a football game.

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

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

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

LIST OF USE-CASES



N°	Type of Use case	Use cases	Partner
1	Natural disaster	Flooding during major event	Comune de Milano (Italy)
2	Natural disaster	Track interception due to a landslide - crisis management	FGC (Spain)
3	Physical attack	Terroristic attack using firearms inside a railway station	RFI (Italy)
4	Physical attack	Potential terroristic attack via IED carried via baggage	RFI (Italy)
5	Cyber-attack	Train failure inside a tunnel without possibility to communicate with the train driver	FGC (Spain)
6	Physical attack	Vandalism (graffitis, bombing, damaging the equipment etc.)	EGO (Turkey)
7	Physical attack	Suicide attempt at the station	EGO (Turkey)
8	Combined Cyber-Physical	Intrusion in sensitive place	EGO (Turkey)
9	Physical attack	Relocation of existing sensors	TCDD (Turkey)
10	Cyber-attack	Manipulation of data transferred to Operating Center	TCDD (Turkey)
11	Cyber-attack	Hacking of the signalling system causing accidents	PRORAIL (The Netherlands)
12	Combined Cyber-Physical	Attack during a football game	Metro de Madrid (Spain)
13	Cyber or physical attack	Level crossing accident: sabotage or cyber attack on the LC equipment	MTRS (Israel)

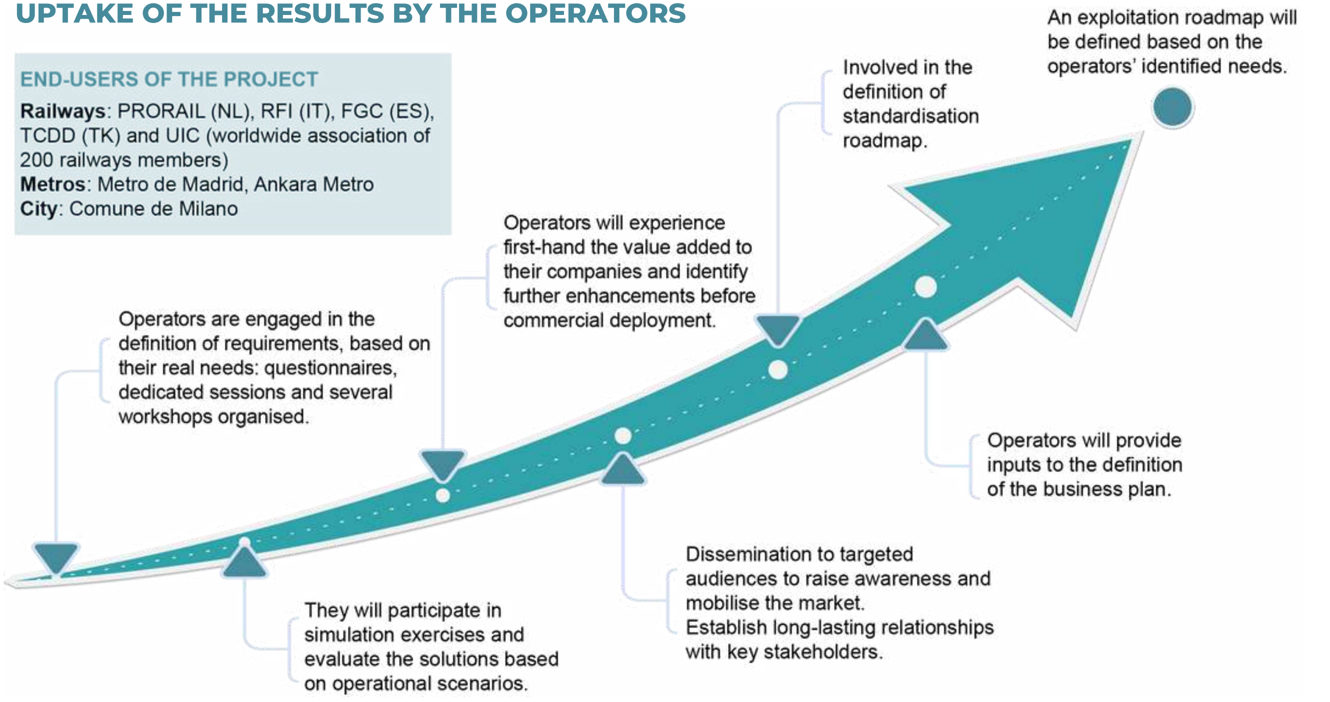
The list of use-cases above has been identified by the end-users in a first stage and will be adapted in a second stage as part of the exercises to be held in Madrid, Ankara, Roma and Milan.

Operators will experience first-hand the added value S4RIS brings to their companies and be able to identify further enhancements before commercial deployment.

This will ensure the applicability of S4RIS in an operational environment and contribute to the success of the main output of the project, which aims at improving resilience of railways particularly with a combined cyber-physical attack.

NEXT STEPS - EXPLOITATION OF THE RESULTS

UPTAKE OF THE RESULTS BY THE OPERATORS



END-USERS OF THE PROJECT

Railways: PRORAIL (NL), RFI (IT), FGC (ES), TCDD (TK) and UIC (worldwide association of 200 railways members)
Metros: Metro de Madrid, Ankara Metro
City: Comune de Milano

Operators are engaged in the definition of requirements, based on their real needs: questionnaires, dedicated sessions and several workshops organised.

They will participate in simulation exercises and evaluate the solutions based on operational scenarios.

Operators will experience first-hand the value added to their companies and identify further enhancements before commercial deployment.

Dissemination to targeted audiences to raise awareness and mobilise the market.
Establish long-lasting relationships with key stakeholders.

Involved in the definition of standardisation roadmap.

Operators will provide inputs to the definition of the business plan.

An exploitation roadmap will be defined based on the operators' identified needs.

COMMUNICATION ON THE RESULTS

Communication is an important feature of the project. Beyond the end-users who are engaged from the start of the project, national authorities and policy makers are also an important target audience identified in the dissemination strategy: they are involved in the advisory board.

Moreover, dissemination actions are planned in media provided by the European Commission and also in relevant events gathering representatives from member states, for example LANDSEC meetings, ERA and ENISA events, etc. Training activities and information material will also be developed to increase crisis managers and decision-makers knowledge.

GO-TO-MARKET ROADMAP: INDUSTRIALISATION OF RESULTS AND ENGAGEMENT WITH EU BUYERS

Bridging the gap between the project results and full commercial deployment can be only supported by sound business and exploitation plans.

The project will perform an in-depth characterisation of the Key Exploitable Results and investigate the exploitability and business feasibility.

A Plan for the Use and Dissemination of Foreground (PUDF) will be also defined to manage the exploitation objectives, aiming to take all the project outputs to the market.

CONTRIBUTION TO STANDARDISATION

SAFETY4RAILS project first identified the framework relevant for safety and security of railway systems, taking into consideration relevant legal texts at EU level, international standards adopted by industry and European norms.

SAFETY4RAILS is fully in line with the CER and NIS2 directive proposals and in fact the tools delivered therein will help rail operators to implement the requirements of both directives at national level.

Then, a feasibility study of the extension of safety certification schemes with security aspects, including risk assessment, risk management strategies and the impact on current certification schemes will be prepared.

CONSORTIUM

The SAFETY4RAILS Consortium is led by Fraunhofer-EMI and composed of 31 partners from 13 different countries (Germany, France, Spain, Turkey, Italy, Belgium, Switzerland, United Kingdom, Greece, Finland, Hungary, Israel and the Netherlands).

They represent railway operators, railway infrastructure managers, research centres, academia and industry suppliers and bring a range of complementary skills required for this multidisciplinary project.

1 GERMANY

Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V. (Fraunhofer), Coordinator, represented by its Institute for High-Speed Dynamics, Ernst-Mach-Institut (Fraunhofer EMI)

2 FRANCE

Union Internationale des Chemins de fer (UIC - the worldwide railway organisation)

3 SPAIN

Metro de Madrid (MdM)
Royal Melbourne Institute of Technology (RMIT)
ETRA Investigacion y Desarrollo (ETRA)
Tree Technology (TREE)
Universidad Miguel Hernandez de Elche (UMH)
Ferrocarrils de la Generalitat de Catalunya (FGC)

4 TURKEY

Ankara Elektrik, Havagazi ve Otobusisletme Muessesesi (EGO)
Ergunler Insaat Petrol Urunleri Otomotiv Tekstil Madencilik su Urunler Sanayi ve Ticaret (ERARGE)
TAŞIMACILIK A.Ş GENEL MÜDÜRLÜĞÜ (TCDD)

5 ITALY

Rete Ferroviaria Italiana (RFI)
Leonardo (LDO)
Stam srl (STAM)
Rina Consulting spa (RINA-C)
Alpha-Cyber srl (AC)
Comune Di Milano (CdM)

6 BELGIUM

Compagnie Européenne d'Intelligence Stratégique (CEIS)
European Organisation for Security (EOS)

7 SWITZERLAND

IC Information Company (IC)

8 GREECE

National Center for Scientific Research "Demokritos" (NCSRD)
Wings ICT Solutions Information & Communication Technologies (WINGS)
Intracom SA Telecom Solutions (ICOM)

9 UNITED KINGDOM

The University of Reading (UREAD)
University of Newcastle Upon Tyne (UNEW)
Innova Integra Limited (INNO)

10 FINLAND

Laurea-Ammattikorkeakoulu oy (LAU)

11 HUNGARY

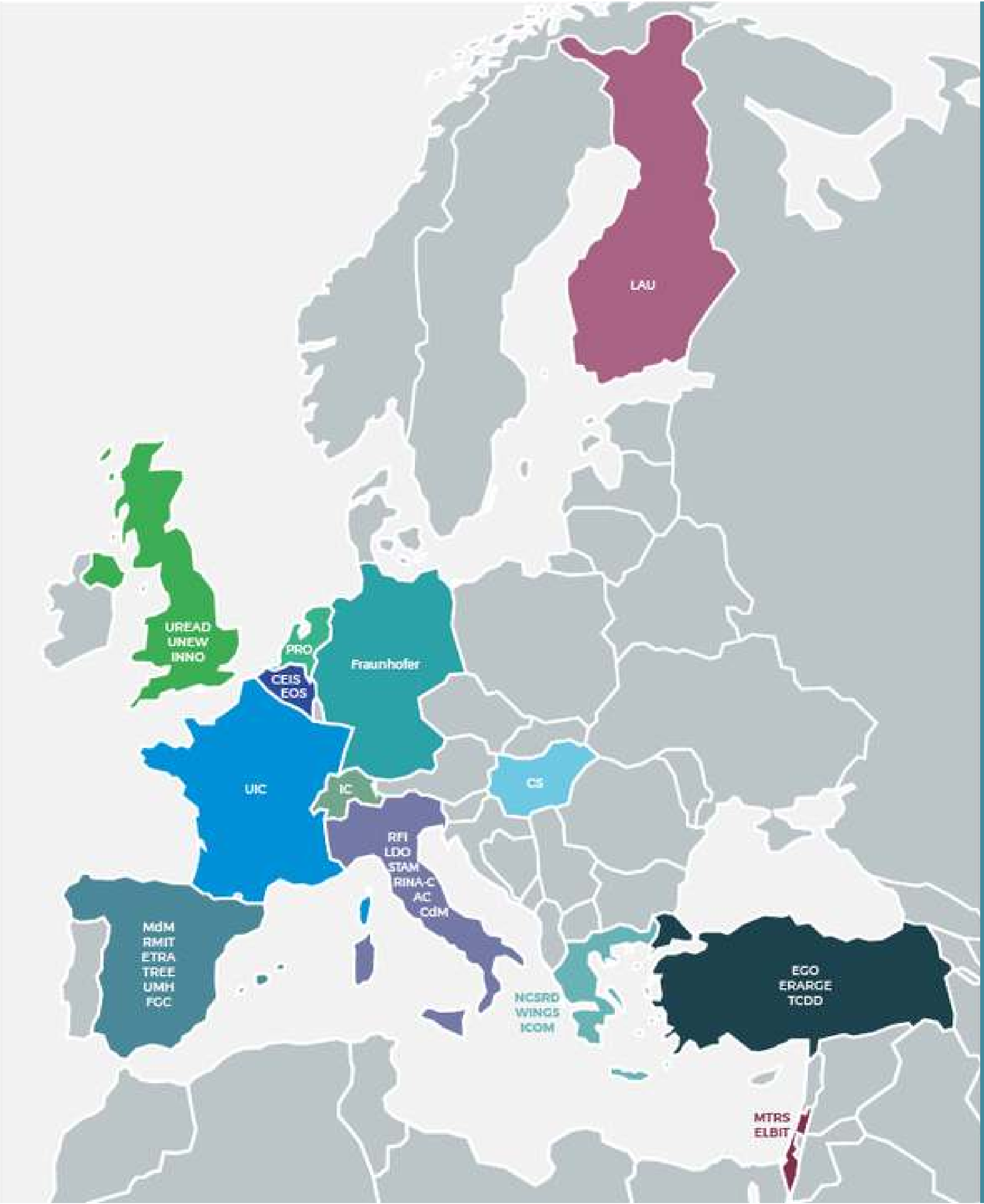
Cyber Services Zartkoruen Mukodo Reszvenytarsasag (CS)

12 ISRAEL

M T R S 3 Solutions and Services (MTRS)
Elbit Systems C4I and Cyber (ELBIT)

13 NETHERLANDS

Prorail BV (PRO)



ADVISORY BOARD

The consortium is reinforced through an Advisory Board which ensures that the SAFETY4RAILS outcomes meet the needs of railway and metro operators.

About 20 advisors from a range of sectors: rail, metro, public transport, cyber, transport ministries, and security, covering 10 countries: Belgium, France, Bulgaria, Poland, Spain, Sweden, Germany, Netherlands, Switzerland and Turkey.

The Advisory Board is being extended throughout the life of the project through a permanent recruitment process of new members.

SAFETY4RAILS has already gone social!
Make sure to follow us:

safety4rails.eu

Safety4Rrails EU Project

@safety4r

Coordinator:
Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., represented by its Institute for High-Speed Dynamics, Ernst-Mach-Institut (Fraunhofer EMI)

End User Coordinator:
International Union of Railways (UIC)

Technical coordinator:
IC Information company

Fraunhofer EMI
uic
Metro
Metro de Madrid
EGO
EGO Genel Müdürlüğü
RFI
RETE FERROVIARIA ITALIANA
GRUPPO FERROVIE DELLO STATO ITALIANE
LEONARDO
FGC
Ferrocarrils de la Generalitat de Catalunya

ProRail
ceis
avisa partners
STAM
MASTERING EXCELLENCE
IC Information company
LAUREA
TCDD
RMIT UNIVERSITY

University of Reading
etra I+D
RINA
DEMOKRITOS
NATIONAL CENTRE FOR SCIENTIFIC RESEARCH
WINGS
ICT SOLUTIONS

Newcastle University
EOS
IN Innova Integra
CybeServices
MADE IN EUROPE
UNIVERSITAS
Miguel Hernández

erGE
MTRS
INTRACOM
TELECOM
TREE
TECHNOLOGY
Elbit Systems
C4I and Cyber
Comune di Milano

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