SAFETY4RAILS

FIRST VERSION – DEVELOPMENT OF A BLUEPRINT EXERCISE HANDBOOK

Deliverable 8.2

Lead Authors: ETRA

Contributors: CEIS, MDM, EGO, PRO, TCDD, RINA, IC, ERARGE, ELBIT, FHG, STAM, TREE, INNO, WINGS, LDO, FGC

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.

D8.2 FIRST VERSION – DEVELOPMENT OF A BLUEPRINT EXERCISE HANDBOOK

Deliverable number:	8.2	
Version:	1.2	
Delivery date:	21/02/2022	
Dissemination level:	PU - Public	
Nature:	Report	
Main author(s)	Eduardo Villamor	ETRA
Contributor(s)	Florence Ferrando Jeroen van den Tweel Antonio de Santiago Laporte Okan Topcu İbrahim Uluçinar Emiliano Costa Uli Siebold Niyazi Ugur Eli Ben-Yizhak Natalie Miller Deborah Hugon Katharina Ross Tatiana Silva Marco Tiemann Andreas Georgakopulos Giulia Siino Chistos Kyriakopoulos Claudio Porretti Álvaro García	CEIS PRO MDM TCDD EGO RINA IC ERARGE ELBIT Fraunhofer STAM Fraunhofer TREE INNO WINGS RMIT NCSRD LDO FGC
Internal reviewer(s)	Atta Badii Stephen Crabbe Andreas Georgakopulos Uli Siebold Antonio de Santiago Laporte	UREAD Fraunhofer WINGS IC MDM
External reviewer(s)	Eva Muñoz	ETRA

Document control

Version	Date	Author(s)	Change(s)
0.1	23/06/2021	Eduardo Villamor (ETRA)	ToC release
0.2	11/08/2021	Eduardo Villamor (ETRA)	Preliminary inputs from tool providers for MDM scenario
0.3	22/11/2021	Florence Ferrando (CEIS)	Compilation of contributions & integration
0.4	25/11/2021	Florence Ferrando (CEIS)	Aggregation for EGO scenario
0.4.5	30/11/2021	Eduardo Villamor (ETRA)	1st detailed description of MDM simulation script
0.5	03/12/2021	Eduardo Villamor (ETRA)	1st MDM and EGO Simulation Handbook release
0.6	13/12/2021	Eduardo Villamor (ETRA)	Finalised sections 1,2,3 and 5.
0.7	14/12/2021	Eduardo Villamor (ETRA)	Inputs from tool providers and end-users integrated
0.8	16/12/2021	Eduardo Villamor (ETRA)	Clarifications from IC and EGO and formatting issues solved. Annexes and Executive Summary added
0.9	17/12/2021	Eduardo Villamor (ETRA)	Internal and External review comments addressed
1.0	21/12/2021	Eduardo Villamor (ETRA)	Final comments and version ready for submission
1.1	10/01/2022	Stephen Crabbe (Fraunhofer)	Update of this page, regarding security assessment control
1.2	21/02/2022	Eduardo Villamor (ETRA), Stephen Crabbe (Fraunhofer)	Editing of deliverable to produce a version for public dissemination.

DISCLAIMER AND COPYRIGHT

The information appearing in this document has been prepared in good faith and represents the views of the authors. Every effort has been made to ensure that all statements and information contained herein are accurate; however, the authors accept no statutory, contractual, or other legal liability for any error or omission to the fullest extent that liability can be limited in law.

This document reflects only the view of its authors. Neither the authors nor the Research Executive Agency nor European Commission are responsible for any use that may be made of the information it contains. The use of the content provided is at the sole risk of the user. The reader is encouraged to investigate whether professional advice is necessary in all situations.

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 CONTENTS

List of tables

List of figures

Executive summary

SAFETY4RAILS aims to develop a set of tools for increasing resilience against combined cyber-physical threats, including natural hazards, to railway infrastructure. Such tools will need to be validated with a direct involvement of metro and railways operators. To achieve this, four Simulation Exercises (SE) will be conducted during the project.

In this document, the consortium presents the analyses conducted to align all technological solutions to be demonstrated, with the relevant Use-Cases proposed by the end-users. The results served as the baseline for developing the Scenarios that will be played in each SE. Two Simulation Exercises were comprehensively developed and are reported in this deliverable (and further Confidential Annexes in an additional deliverable), namely Metro de Madrid (MDM) and Ankara Metro (EGO). The two remaining SE will be reported in D8.3.

After an introductory chapter, Section 2 provides a complete description of the final version of the Use-Cases proposed initially in D2.5, including the methodology followed. While Section 3 presents a short overview of the scenarios and a link to SAFETY4RAILS operational objectives, Section 4 provides the First Version of the Simulation Exercise Handbook available for public dissemination. This handbook contains the description of MDM SE and EGO SE with a high emphasis on the organisation and planning. RFI SE and CDM SE will be reported before the 3rd SE in deliverable D8.3.

In the first SE, planned for early February, a combined cyber-physical scenario will be played in a station of Metro de Madrid. The demonstration of the 1st version of S4RIS will involve MDM, as metro operator, and ETRA, FRAUNHOFER, ELBIT, STAM, TREE, INNO, WINGS, RINA, RMIT, ERARGE, NCSRD, IC as technological providers. LAU will support the exercise as Evaluation Manager. In this first demonstration, 11 tools will be evaluated: CAESAR, CAMS, iCrowd, PRIGM, RAM2, SecuRail, TISAL/OSINT, DATA FAN, BB3d, CuriX and WINGSPARK.

In the second SE, planned for late March, a combination of different cyber-physical threats will be evaluated at a station at Ankara Metro, considering multimodal effects with the Central Train Station (State Railways of the Republic of Turkey). The demonstration of the 2nd will involve EGO as host and TCDD as co-host, as well as ERARGE, FRAUNHOFER, LDO, IC, STAM, TREE, RMIT, INNO, NCSRD, ELBIT as technological providers. LAU will support the exercise as Evaluation Manager. In this second demonstration, 11 tools will be evaluated: CAESAR, DATA FAN, PRIGM, SecuRail, TISAL/OSINT, CAMS, iCrowd, RAM2, Ganimede, Senstation, CuriX.

Even after the submission of deliverable D8.2, the consortium will continue to refine the Exercises defined with the ultimate goal of a smooth and fruitful running and lessons learnt.

1. Introduction

1.1 Overview

In the deliverable **D2.5: Specific requirements for multimodal transport systems**, a preliminary description of the Use-Cases to be implemented by SAFETY4RAILS was described. In the present deliverable, the consortium performed an in-depth analysis of these Use-Cases, in compliance with the end-user needs, aligning them with the expected contribution from each tool provider. Following, an iterative methodology described in section 2, the consortium achieved consensus on relevant examples (Use-Cases) where S4RIS, and the capabilities offered by the tools brought to the project, could be applied. All tool providers and end-users participated actively in this process. The result of this approach is presented in section 2.2. Furthermore, the updated Use-Cases definition has been used as the foundation of the Simulation Exercises Handbook, which first version is the main output of this document.

All details related to the Simulation Exercise design, preparation, and execution have been defined in this deliverable (and further Confidential Annexes in an additional deliverable) by the partners involved in each Simulation Exercise Team. On the other hand, the details relevant to the evaluation of the simulation are provided in **D8.1: Evaluation Methodology**.

In this report, the consortium provides the first version of the Simulation Exercise Handbook, covering Simulation Exercise 1 (“MDM”) and Simulation Exercise 2 (“EGO”). The main purpose is to have a detailed planning on the execution of both exercises before their implementation in February and March. A second version, **D8.3: Final version of development of a blueprint exercise handbook** will cover the other two exercises (“RFI” and “CDM”) and will be ready before the implementation of the third Simulation Exercise.

1.2 Structure of the deliverable

This document is structured in the following sections:

- Section 1 – Introduction. This section provides a clear overview of what has been done to produce this deliverable, including its main goals, overall scope, and structure.
- Section 2 – Preliminary Analyses for Simulation Exercises. The section is the follow-up of the work carried out in D2.5 for defining SAFETY4RAILS Use-Cases and provides the basis for the definition of the simulation exercises in Section 4.
- Section 3 – Simulation Exercises Overview, providing a quick look into the simulation exercises planned during the project.
- Section 4 – Simulation Exercises Handbook (First Version). This section provides the scenarios definition, exercise scripts and many organisational details required for the simulation exercise run available for public dissemination.
- Section 5 – Conclusion.

The document also includes the following annexes:

- ANNEX I. Glossary and Acronyms
- ANNEX II. Type of exercise
- ANNEX III. Use-Cases Definition Template
- ANNEX IV. Simulation Exercises Workshop Template

2. Preliminary Analyses for Simulation Exercises

2.1 Methodology

The primary objective of Section 2 is achieving a mature definition of the Use-Cases presented in D2.5. As agreed by the consortium, a **Use-Case** is defined as a *"High-level description of the problem that needs to be addressed by means of functionalities/technology".* On the other hand, a **Scenario** is defined as *"An instance of a Use-Case/Use-cases describing the concrete set of actions to be taken".* Considering both definitions, it is a pre-condition to have the Use-Cases closed before working on the Scenarios. In fact, the finalised Use-Cases, presented in this section, will be the foundation for the definition of the Simulation Exercise Scenarios in Section 4.

To achieve the goal stated in the previous paragraph, the consortium followed a co-design approach whereby several interactions between the end-users and tool providers were performed. In this process, a special emphasis on resilience was dedicated to cover the four phases, namely prevention[1], detection, response, and recovery. The methodology used consisted of four steps to complete the Use-Cases, which are described as follows:

1) In-depth review of the Use-Cases definition in *D2.5: Specific requirements for multimodal transport systems*. Creation of a Use-Case template with the minimum set of information to be covered – which is used in section 2.2.
2) Analysis of the S4RIS capabilities/functionalities (based on specifications in answer to requirements) provided to each resilience stage for each Use-Case. A dedicated spreadsheet was generated of each Use-Case, also covering the data inputs required from the end-user, as well as from other tools; and the data outputs provided to the end-user, as well as to other tools. The template is reported in **Annex III**. The filled spreadsheet is not attached to the current deliverable due to format restrictions, however some of its content was used for the Section 4 development.
3) Based on steps 1) and 2), a draft version of the Use-Cases was developed. Tool providers and end-users have refined their contributions and expectations to align their interest. The spreadsheet in step 2 has been updated as a result.
4) Having the final integrated version of the Use-Cases, a final review was performed with the end-users to fine-tune any missing details. This review included a site survey at EGO and MDM facilities, where information was also gathered for preparing the Scenarios description in Section 4.

2.2 Use-cases final definition

As a result of the implemented methodology described in the previous section, the consortium agreed on a final set of Use-Cases, which also detail the most relevant threats for SAFETY4RAILS end-users as well as the expected value added by the S4RIS for each resilience stage. **Likelihood** and **impact** values were based on the definitions included in deliverable D2.1, and the expertise provided by the end-users. The expected contribution of each tool is outlined for each Use-Case. The use cases have been edited to allow for public dissemination. It should be noted that the original number of Use-Cases presented in D2.5 was reduced from 14 to 12 Use-Cases. The reason is that after an in-depth review of the features incorporated into S4RIS, and a site survey at EGO facilities, EGO Use-Cases were reformulated and reduced from 4 to 2. These are now described under UC-006 & UC-007 below:

[1] Prevention phase covering identification of vulnerabilities and gaps, and implementation of protection measures. Therefore, covering IDENTIFICATION and PROTECTION phases mentioned in previous project documents.

TABLE 1 USE-CASES FINAL DEFINITION (UC-001 – UC-012)

Use-Case Description	
ID	*UC – 001*
Title	**Natural Disaster - Flooding**
Main Problem Description:	A heavy torrential rain falls in the city during a major event (e.g., 2026 Olympics). Urban drainage systems cannot manage the intense rain, leading to great disturbances among transport infrastructures in the city. A massive flooding affects the metro and train stations, particularly at key interchanges, coinciding with those with most relevant visitors' flow during the event. As a result, major transport lines are stopped, and replacement transport lines are activated.
Cascading Effects Description:	The mobility of citizens and tourists is significantly reduced, which puts not only the execution of the event at risk, but also detracts from the economic benefit to the city. Stations may have to be closed off because of excess water within the station. Tracks could be damaged because of excess flooding.
Likelihood:	Likely
Impact (main problem + cascading effects):	Major
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, to be better prepared for future events. 3) Know which components are the weakest/most critical, so they can be protected. **- CuriX (DETECTION&RESPONSE):** Monitor, forecast, and maybe correlate flooding level sensors in proximity of tracks, so to decisions can be made regarding adjustments of trains systems and train schedules due to flooding. **- CAMS (PREVENTION, RESPONSE, RECOVERY)**: 1) Be well informed on the budget to allocate to repair/maintain/rehabilitate the infrastructure after unexpected hazard events, so that a proactive plan can be made. 2) Know time and cost needed to respond a crisis and restore normal functioning, so that resource deployment and quick reaction based on proactive actions can be planned. 3) Be aware of budgetary and time implication to recover the infrastructure, so that resource deployment and control of financial loss can be made. **- DATAFAN (DETECTION):** 1) Know if there are dysfunctionalities in the signalling systems caused by a natural hazard like a flooding by investigating the signal states at each time step to detect anomalies 2) If anomalies are detected countermeasures can be taken at an early stage and their effectiveness can be evaluated. 3) Know the expected number of passengers in the future for a specific station, so that passengers from affected stations could be relocated. **- iCrowd (PREVENTION&REPONSE):** Simulation of evacuation based on natural disaster scenario and crowd behaviour

	- SecuRail (PREVENTION): Perform risk analysis of the infrastructure to understand risk scenarios and related indicators**.** **- UNI|MS (DETECTION):** Offers capability to access a variety of sensors (primarily IoT ones) and controllers. It incorporates also network monitoring (developed for WiBAS and other ICOM telco HW), but could be also used for 3rd party networking devices. **- WINGSPARK (DETECTION&RESPONSE):** 1) Know if there is an overcrowded area in the facility and guide the crowd in case of emergency according to the estimated concentrations. 2) Get alerts, if there is an overcrowded area in the facility, and a guideline for the crowd in case of evacuation. **- SISC2 (DETECTION&RESPONSE):** Gathering, processing, classifying and analysing info from sensors. Producing meaningful intelligence out of diverse sensor info. **- SARA (PREVENTION&RECOVERY):** Risk assessment evaluation of train station and its equipment. Several measurements are provided: 1) Effectiveness of the station in the post-emergency phase related to service availability, 2) Measurement of the direct economic damage related to the disruption, 3) Measurement of the efficiency of the mitigation action implemented.

Use-Case Description	
ID	*UC – 002*
Title	**Natural disaster - Track Interception due to a landslide that causes an immobilization of the train**
Main Problem Description:	A major landslide, affecting various railway tracks, hinders the mobility of key transport lines, including passengers and freight. The train infrastructure is then considered damaged since the soil displacement does not allow the train to circulate and hence the service becomes unavailable. The superstructure is not strictly damaged, but it cannot be used due to the soil on top. Depending on the dimensions of the landslide, even the catenary could be affected. The incident is detected and communicated to the control centre by the train operator. Internal protocols are triggered to assess the impact and the best strategy to restore the traffic.
Cascading Effects Description:	In terms of service, the cascading effects are the following: the inability to provide regular services, delays, conflicting schedules; the need to deploy additional substitution services (e.g., shuttles, buses etc.); the need to send additional station and service agents to assist the passengers affected and announce special communications with the services affected, etc. Concerning the infrastructure, the landslide will affect the tracks, as well as create cascading effects to other infrastructure elements. The damaged infrastructure elements directly depend on the magnitude of the landslide, such the catenary and the electrical system. This leads to the need to deploy emergency maintenance procedures.
Likelihood:	Likely
Impact (main problem + cascading effects):	Moderate

S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, so that better preparation can be made for future events. 3) Know which components are the weakest/most critical, so that closer attention can be made to protect them. **- CuriX (DETECTION):** Be informed on potential track interception, based on track "throughput" data (trains/hour), so that emergency concepts can be implemented at an early stage - thus, emergency can be prevented. **- DATAFAN (PREVENTION&RESPONSE):** Know the expected number of passengers in the future for a specific station, so that passengers from affected stations could be relocated. **- RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Vulnerability and security gaps assessment. Risk assessment for each of the operational units. 2) Correlated insights for early detection of potential threats, based on data from multiple monitoring sources. 3) Risk-based prioritization of issues, case management for tracking response actions 4) Providing mitigation steps for each alert **- SISC2 (DETECTION&RESPONSE)** Gathering, processing, classifying and analysing info from sensors. Producing meaningful intelligence out of diverse sensor info

Use-Case Description	
ID	*UC – 003*
Title	**Physical Attack – Terrorist Attack using Firearms inside a Railway Station**
Main Problem Description:	A coordinated group of terrorists are planning to attack a Railway Station, they choose the date when a very crowded event will be happening in the city (e.g., sporting event). Prior to the event, they study the location and coverage of monitoring systems . During the event, two terrorists wear explosive vests and another one is carrying a Kalashnikov machine gun. They enter the station and shoot the security agents. This is not noticed due to the heavy background noise. One of the terrorists' accesses to the station and exploit his/her vest in the middle of the crowd. The panic starts and all people try to leave the station. In the meantime, the shooter is located at the exit and shooting to the crowd from a hidden place, also killing and injuring people.
Cascading Effects Description:	Based on the assumption that terrorist would choose a large station (because they want to kill as much people as possible) and choose an area in which a lot of people are gathered; the attack might possibly take place in the main station hall. That means that trains might be relatively unaffected. Explosive simulations show that the main structure of the large stations can withstand an attack (with a "normal" number of explosives). The main risk therefore would be fatalities or (fatally) wounded people. This might be directly (a consequence of an explosion) or indirectly (because of debris flying around).

Likelihood:	Unlikely
Impact (main problem + cascading effects):	Critical
S4RIS added value:	**- CuriX (DETECTION&RESPONSE):** Have an instrument to be informed on potential terroristic risks, so that potential risks can be countered by calling in security forces. **- Ganimede (DETECTION):** Recognizing specific audio pattern through AI models robust against a very noisy environment, such in a railway station. **- SISC2 (DETECTION&RESPONSE)** Gathering, processing, classifying and analysing info from sensors. Producing meaningful intelligence out of diverse sensor info.

Use-Case Description	
ID	*UC – 004*
Title	**Physical attack – Potential terrorist attack via IED carried via baggage**
Main Problem Description:	During Christmas festivity, many people travel to the city centre and buy Christmas presents to their loved ones. A lone wolf plans carefully the attack to a Railway Station. He has been radicalised during the last year and often posting hate messages in social media. He prepares an Improvised Explosive Device (IED) in advanced and selects the date with the heaviest railway traffic. The IED is hidden into a suitcase and, at 6:30pm, he arrives to the railway station. After staying for 20min, he leaves the baggage unattended in a crowded area, where security personal won't notice it. At 7:00pm, several trains arrive at the station with many people who come to buy their last Christmas presents. At 7:02pm, the IED is detonated, killing over 30 people and 50 severely injured.
Cascading Effects Description:	This might lead to a severe damage on the station structure, as well as communication systems for example.
Likelihood:	Unlikely
Impact (main problem + cascading effects):	Critical
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, so that they can be better prepared for future events. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them. **- CuriX (DETECTION):** Be informed about early warning on IED based attacks, so that intervention can start. **- Ganimede (DETECTION):** Detection of an abandoned baggage. **- UNI|MS (DETECTION):**

	Offers capability to access a variety of sensors (primarily IoT ones) and controllers. It incorporates also network monitoring (developed for WiBAS and other ICOM telco HW) but could be also used for 3rd party networking devices. **- SISC2 (DETECTION&RESPONSE)** Gathering, processing, classifying and analysing info from sensors. Producing meaningful intelligence out of diverse sensor info

Use-Case Description	
ID	*UC – 005*
Title	**Cyber-attack – Train Failure inside a tunnel without possibility to communicate with the train driver**
Main Problem Description:	After infiltrating into the railway IT system, an “important system” is hacked. Communications between the Command-and-Control Centre and a specific train line have been compromised. Thanks to this, the train is ordered to stop on a certain point in a tunnel. While communications with the C2 are hindered, the train driver is not aware that the “important systems” has been hacked.
Cascading Effects Description:	The cascading effects found in this Use Case are the following: the inability to provide regular services, delays, conflicting schedules, the need to send additional station and service agents to assist the passengers affected and announce special communications with the services affected, etc.
Likelihood:	Likely
Impact (main problem + cascading effects):	Major
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, so that they can be better prepared for future events. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them. **- CuriX (DETECTION):** Detect root causes of an incident, so that the user is able to counteract the same incidents in the future. **-RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Vulnerability and security gaps assessment. Risk assessment for each of the operational units. 2) Correlated insights for early detection of potential threats based on data from multiple monitoring sources. 3) Risk-based prioritization of issues, case management for tracking response actions 4) Providing mitigation steps for each alert **- SecaaS (DETECTION):** Anomaly detection and correlation with known cyber attract profiles. **-Blockchain (PREVENTION, DETECTION)** 1) Enable a secure and relevant usage of blockchain in the railway and metro environment by allowing only entities to the network which have a defined identity and role in the network

	2) Detecting attempts of manipulation with ingested data

Use-Case Description	
ID	*UC – 006*
Title	**Physical attack – Intrusion and bomb planted**
Main Problem Description:	During the night, a lone-wolf (terrorist) approaches the depot area in the metro infrastructure, where the rolling stocks are parked. He/she studied the patrolling protocol and selected the most suitable time for entering the facilities. The wire fences are cut, following an unauthorised access. No camera-based alerting system detected the intruder. In the intrusion, explosives are placed in the trains located in the depot area with a timer at 8am (peak hour). The intervention happens very quickly and the terrorist leaves without being noticed. In the next morning, the train is operated normally and arrives at one of the most concurrent stations in the metro system at 8am. Once the train arrives, the bomb is detonated. This leads to over 50 casualties, including children, and nearly 100 injured.
Cascading Effects Description:	Significant delays in other lines and economic losses. The explosion will also affect radio communications, high-voltage cables, SCADA, and other communications – all infrastructure in the tunnels will be affected.
Likelihood:	Unlikely
Impact (main problem + cascading effects):	Critical
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, so that they can be better prepared for future events. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them. **- TISAIL (PREVENTION, DETECTION):** 1) Be informed about vulnerabilities related to jamming as well as threat actors using jamming techniques in their campaigns. 2) Be informed about threat actors using jamming techniques in their campaigns. **- CAMS (PREVENTION, RESPONSE, RECOVERY)**: 1) Be well informed on the budget to allocate to repair/maintain/rehabilitate the infrastructure after unexpected hazard events, so that a proactive plan can be made. 2) Know time and cost needed to respond a crisis and restore normal functioning, so that resource deployment can be improved, and quick reaction based on proactive actions planned. 3) Be aware of budgetary and time implication to recover the infrastructure, so that resource deployment can be improved, and control financial loss mitigated. **- DATAFAN (RESPONSE&PREVENTION):** Know the expected number of passengers in the future for a specific station, so that passengers from affected stations could be relocated. **- iCrowd (PREVENTION):**

	1) Calculate chances of detection during infiltration/escape per configuration (camera and guard locations) 2) Estimate total time to infiltrate/escape per configuration (camera and guard locations) **- SecuRail (PREVENTION):** Risk analysis of my infrastructure to understand risk scenarios and related indicators **- CuriX (DETECTION):** 1) See hints for the upcoming cascading effects (anomaly in passenger flows of other connected stations), so that further mitigation methods can be prepared for. 2) See how passenger flows correlate with each other, so that the cascading effects analysis can be enhanced/optimised.

Use-Case Description	
ID	*UC – 007*
Title	**Physical Attack – Intrusion in Sensitive Place**
Main Problem Description:	A coordinated group of terrorists are planning to attack a Metro Station. They choose the date when a very crowded event will be happening in the city (e.g., a sporting event). They infiltrate in the station (assumed to be one with the most expected traffic) and perform an unauthorised access to an "important room". "Important systems" are all operating in the room. Typically, the room has equipment that can monitor and manage the station in case the connection with the Operational Centre is lost or broken locally due to a cyber or physical attack. Therefore, the security of the stations is directly dependant to the security of these rooms. It is assumed that (and evident from many cases in real life) such important rooms are not monitored by an intelligent system to predict possible attacks or automatically detect anomalies that may occur. After entering the important room, the attacker has many choices to disrupt the system, like tampering the servers, damaging the computers and cabinets and fire the equipment. At the same time, the terrorists send threatening messages to the people in the station. The whole situation is recorded and broadcasted through social media. Panic and chaos make the situation out of control, where people get injured during the evacuation.
Cascading Effects Description:	- Because trains are immobilised (in the detailed Use-Case description, which is confidential), this leads to major delays in the same line and in other lines, which implies heavy economic losses. - Panic is also spread to other lines and stations, also considering the use of social media. - The attacker can steal secret data about the communication infrastructure which may then cause other cyber-attacks like infiltrating to other software, passenger/personnel data compromise, etc. - Physical damage to the important rooms may cause serious effects in terms of rehabilitation and reconstruction costs and even larger disasters, like fires within the station building.
Likelihood:	Unlikely
Impact (main problem + cascading effects):	Major

S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, so that future events can be prepared for. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them. **- DATAFAN (RESPONSE&PREVENTION):** Know the expected number of passengers in the future for a specific station, so that passengers from affected stations could be relocated. **- CAMS (PREVENTION, RESPONSE, RECOVERY)**: 1) Be well informed on the budget to allocate to repair/maintain/rehabilitate the infrastructure after unexpected hazard events, so that a proactive plan can be made. 2) Know time and cost needed to respond a crisis and restore normal functioning, so that resource deployment can be optimised, and quick reactions made based on proactive actions planned. 3) Be aware of budgetary and time implication to recover the infrastructure, so that resource deployment can be improved, and control financial loss mitigated. **-RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Vulnerability and security gaps assessment. Risk assessment for each of the operational units. 2) Correlated insights for early detection of potential threats, based on data from multiple monitoring sources. 3) Risk-based prioritisation of issues, case management for tracking response actions 4) Providing mitigation steps for each alert **- iCrowd (PREVENTION&RESPONSE):** 1) Know the probability of detecting a malicious actor attempting to break into the important room, so that the effectiveness of the camera and locations can be assessed and eventually improved. 2) Estimation of the total evacuation time and distribution of evacuation times for passengers, to assess the performance of an evacuation plan and eventually improve it. 3) Know the time required to reach the important room in case of emergency, which can be affected by the crowd congestion and the evacuation process, so to calculate the time for which the important room will be compromised and in an unknown state. 4) Estimate the probability of a malicious actor getting away after compromising the important room, so that the performance of any resilience strategies can be assessed and the security of the station improved. **- Senstation (DETECTION):** 1) Receive some instant information from the important room to monitor the unauthorised physical access, to alert the security guard and the main command control (operational) centre. 2) Receive some instant information from the important room to monitor any fire, so to alert the security guard and the main command control (operational) centre. **- PRIGM (PREVENTION&DETECTION):** 1) Apply data security and management policy and GDPR regulations (including both node and person authentication) so to assure the end-to-end security and improve the cyber resilience by preventing hardware-level attacks.

	2) Observe the log data of main security operations (e.g., authentication, encryption, key exchange, etc.) to trace and detect cyber anomalies and assist other countermeasure tools for better resilience. **- SecuRail (PREVENTION):** 1) Perform risk analysis of the infrastructure to understand risk scenarios and related indicators.

Use-Case Description	
ID	*UC – 008*
Title	**Physical attack – Spoofing attack on existing sensors**
Main Problem Description:	In a high-speed line within the Railway Infrastructure, an unauthorised individual relocates “important sensors”. There is no interruption in the data transmission. However, since the sensors are relocated, data transferred to the Operating Centre (OC) is defective. The attacker is aware that the trains’ regulation depends on the sensors measurements. Given the sensors’ new location, parameters are underestimated. In the end, the train fails to conform to operational constraints due to false measurements, and this leads to the train’s derailment. Train is heavily damaged, and the derailment leads to 100 people with severe injuries.
Cascading Effects Description:	- Timetable deviations and long delays occur as a consequence. Even if measurement anomalies are detected and derailment is avoided on time, deviation from the timetable is to be expected. - Delays in the conventional lines and suburban lines- Loss of reliability and reputation of high-speed line services that may cause economic problems
Likelihood:	Unlikely
Impact (main problem + cascading effects):	Major
S4RIS added value:	- **PRIGM (PREVENTION):** Apply data security and management policy and GDPR regulations (including both node and person authentication) so that the railway operator can assure the end-to-end security and improve the cyber resilience by preventing hardware-level attacks. **- Senstation (DETECTION):** 1) Receive some instant information from sensors, so that the OC can alert the train driver. **-RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Vulnerability and security gap assessment. Risk assessment for each of the operational units. 2) Correlated insights for early detection of potential threats, based on data from multiple monitoring sources. 3) Risk-based prioritisation of issues, case management for tracking response actions 4) Providing mitigation steps for each alert

	- CuriX (DETECTION) Monitor / observe the measurement instruments for wind speed and compare the data with historical data as well as with static station data, so that it is possible to detect irregularities and cyber or physical threats and manipulations (detect irregularities and detect incidents).

Use-Case Description	
ID	*UC – 009*
Title	**Cyber-attack – Manipulation of data transferred to Operating Centre**
Main Problem Description:	In a high-speed line within a Railway Infrastructure, unauthorised persons hack the sensor-based systems used to detect the real-time site conditions. They exploit vulnerabilities of sensor and the connection to the overall infrastructure. Through such means, they have the opportunity to disable the sensor functions and block the data transmission to the Operating Centre. The hackers choose a day to make the attack and disable the sensors, endangering the High-Speed Railway operation. At the same time, they exploit the sensor vulnerabilities and infiltrate the whole Railway IT network. When the IT system becomes captive, the hackers request a huge amount of money to end their cyber-attack and return to normal operations. In the meantime, several threats are used to exacerbate the situation, including the derailment of the train.
Cascading Effects Description:	Timetable deviation and long delays occur as a consequence. Even if wind measure anomalies are detected and derailment is avoided in time, timetable failing is to be expected.
Likelihood:	Unlikely
Impact (main problem + cascading effects):	Major
S4RIS added value:	**- CuriX (DETECTION):** 1) Strengthen the measurement system by controlling its measured data (monitor / observe the measurement instruments compare the data with historical data as well as with static station data), so that it is possible to detect irregularities and cyber or physical threats (detect irregularities and detect incidents). 2) Identify critical system states for predefined subsystems, so that it is possible to take countermeasures earlier and shorten response times. **- TISAIL (PREVENTION&DETECTION):** 1) Be informed about vulnerabilities and exposed assets related to IoT sensors. Also be informed about threat actors targeting IoT sensors. 2) Be informed about threat actors targeting IoT sensors. - **PRIGM (PREVENTION&DETECTION):** 1) Apply data security and management policy and GDPR regulations (including both node and person authentication) so that the railway operator can assure the end-to-end security and improve the cyber resilience by preventing hardware-level attacks. 2) Observe the log data of main security operations (e.g., authentication, encryption, key exchange, etc.) so that the railway operator can trace and detect cyber anomalies and assist other countermeasure tools for better resilience. **- Senstation (DETECTION):**

Use-Case Description	
	1) Receive some instant information from sensors, so that the OC can alert the train driver. 2) Receive some instant information from sensors, so that the OC can tell the train driver to take the necessary precautions. **-RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Vulnerability and security gaps assessment. Risk assessment for each of the operational units. 2) Correlated insights for early detection of potential threats, based on data from multiple monitoring sources. 3) Risk-based prioritisation of issues, case management for tracking response actions 4) Providing mitigation steps for each alert **-Blockchain (PREVENTION, DETECTION)** 1) Enable a secure and relevant usage of blockchain in the railway and metro environment by allowing only entities to the network which have a defined identity and role in the network 2) -Detecting attempts of manipulation with ingested data

Use-Case Description	
ID	*UC – 010*
Title	**Cyber-attack – Hacking of the Signalling System causing accidents**
Main Problem Description:	A coordinated group of terrorists are planning to attack the Railway Infrastructure, they choose the date when a very crowded event will be happening in the city (e.g., sporting event) and many people are travelling from the nearby towns. The terrorists identify vulnerabilities in the IT network and exploit the connection with other components to infiltrate and hack the Signalling Systems. The attackers manipulate the signal and the track switch systems with the goal of rerouting two trains in the same section. The terrorists perform the attack and choose two trains with high occupancy. When the driver notices another train approaching, it is too late to turn on the brakes. The trains collide, leading to more than 50 casualties and 100 injured.
Cascading Effects Description:	-Timetable failing and strong delays occur as a consequence. - Area closed to facilitate the work of the emergency bodies, leading to inconveniencies in the neighbourhood - Panic in the neighbourhood
Likelihood:	Unlikely
Impact (main problem + cascading effects):	Major
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, to be better prepared for future events. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them.

Use-Case Description	
	- **CuriX:** 1) Monitor the access (physical and application) (Infrastructure Monitoring (including cyber threats)), so that it is possible to observe and act if no-restricted entities access a building/room or application. 2) Retrieve an alarm with information on possible upcoming incidents, so that it is possible to take action well in advance to prevent outages. 3) Detect root causes of an incident, so that it is possible to counteract the same incidents in the future. 4) Determine observed anomalies within Railway infrastructure (IT, OT), so that it is possible to identify time series irregularities to support the detection of system faults and cyber incidents. - **TISAIL (PREVENTION&DETECTION):** 1) Be informed about vulnerabilities related to signalling as well as to threat actors targeting the signalling system. 2) Be informed about Threat actors targeting the signalling system. **- DATAFAN (DETECTION):** 1) Detect a hacking of the signalling system by investigating the signal states at each time step, so that countermeasures can be taken at an early stage 2) If anomalies are detected, countermeasures can be taken at an early stage and their effectiveness can be evaluated. **- RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Vulnerability and security gaps assessment. Risk assessment for each of the operational units. 2) Correlated insights for early detection of potential threats, based on data from multiple monitoring sources. 3) Risk-based prioritisation of issues, case management for tracking response actions 4) Providing mitigation steps for each alert

Use-Case Description	
ID	*UC – 011*
Title	**Combined Cyber-Physical attack during a sporting event**
Main Problem Description:	A group of terrorists are coordinating a large-scale attack on a metro infrastructure. They are well organised and skilled at hacking and explosive preparation. The terrorists visit the place to identify vulnerabilities and attack vectors. The attack is planned for when very high occupancy is foreseen. At the day of the event, a bomb is detonated., leading to more casualties. At the same time, in the metro station this leads to avalanches of people and people trampled in the entrance hall. *Further details removed from public version.*
Cascading Effects Description:	- Immobilisation of major metro lines especially those serving the sporting location: management of crowd, activation of replacement transport lines; inconveniences and repercussions on the organisation of the event. - Impact on other transport mode: Closure of 3 main transportation hubs next to the stadium, affecting commuter trains, buses, and long-distance trains

Use-Case Description	
Likelihood:	Likely
Impact (main problem + cascading effects):	Critical
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring, to be better prepared for future events. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them. **- CAMS (PREVENTION, RESPONSE, RECOVERY)**: 1) Be well informed on the budget to allocate to repair/maintain/rehabilitate the infrastructure after unexpected hazard events, so that a proactive plan can be made. 2) Know the time and cost needed to respond a crisis and restore normal functioning, so resource deployment and quick reaction based on proactive actions can be planned. 3) Be aware of budgetary and time implication to recover the infrastructure, so that resource deployment can be improved and financial loss can be controlled. **- CuriX (DETECTION):** 1) Figure out anomalies of the observed environment / system, to enable advance response and pre-empting of an incident. 2) Monitor anomalies in monitoring data of OT systems, to observe and respond to them in advance. **- PRIGM (PREVENTION):** Be informed or to inform stakeholders about vulnerabilities and attack surfaces within the system, so that the railway operator or the relevant stakeholders can define and develop countermeasures against cyber and/or cyber-physical attacks. **- TISAIL (PREVENTION, DETECTION):** 1) Be informed about vulnerabilities and exposed assets of the organisation related to CCTV. To be informed about threat actors targeting CCTV and spear-phishing campaign targeting user mail domains. 2) Be informed about threat actors targeting CCTV systems **- iCrowd (PREVENTION, RESPONSE):** 1) Calculate chances of detection during infiltration/escape per configuration (camera and guard locations) 2) Estimate total time to infiltrate/escape per configuration (camera and guard locations) **- RAM2 (PREVENTION, DETECTION, RESPONSE AND RECOVERY):** 1) Security posture analysis. 2) Correlated insights for early detection of potential attacks based on data from multiple sources. 3) Risk assessment for each of the operational units and assets. 4) Efficient risk-based decision making according to smart prioritisation of risk within operational units. 5) Recommended prioritisation of mitigation actions for preventive risk reduction and reactive handling of on-going incidents. 6) Case management and tracking of mitigation actions.

Use-Case Description	
	- SecuRail (PREVENTION): Perform risk analysis of my infrastructure to understand risk scenarios and related indicators. **- WINGSPARK (DETECTION &RESPONSE)** 1) Know if there is an overcrowded area in the facility and guide the crowd in the case of an emergency according to the estimated concentrations. 2) Get alerts, if there is an overcrowded area in the facility, and a guideline for the crowd in case of evacuation. **- DATAFAN (PREVENTION, DETECTION & RESPONSE):** 1) Know the expected number of passengers in the future for a specific station, so that passengers from affected stations could be relocated. 2) Know the expected number of passengers in the future for a specific station, if the normal railway operation is interrupted unexpectedly (due to a station closure). Better predict time delays of trains or metros in what-if scenarios. 3) Detection of significant high passenger volume like passenger peaks before and after a football game. **- BB3D (PREVENTION, RECOVERY):** 1) Evaluate blast loading caused by a bomb attack, possible damage to structures and people, and compute the safety distance for blast design and risk assessment purposes. 2) Setup blast mitigation countermeasures (e.g., safety distance, protective hardening)

Use-Case Description	
ID	*UC – 012*
Title	**Cyber/Physical-attack – Level Crossing Accident: Sabotage or Cyber attack**
Main Problem Description:	Reports are received from the civil police at the Infrastructure Manager's Operation Control (IMOC), they had received a public emergency call, warning of a passenger train colliding with a bus on a level crossing at 'X' with a fire, fatalities, and injured civilians. The line involved has two tracks, OHL (Overhead Line) electrification and is operated using a system with movement authorities transmitted to trains. Passenger trains are 4 or 8 car EMU. The IMOC takes immediate action to ensure the safety of other train operations on the line of route. It liaises with the train operator who subsequently advises that they cannot contact the driver or any other member of the train crew onboard of the collided train. The IMOC also exchanges information with first responders to ensure they are aware/determine facts. The IMOC liaise with the Train Operating Company (TOC), who will communicate with the passengers on trains and at stations, care for those involved on site and possibly in other trains and manage staff and family issues. An investigation is carried out to understand the source of the accident. Is there a software error, human error, possible system hacking?

Use-Case Description	
Cascading Effects Description:	- Effects on buses circulation and transport. - Area closed to facilitate the work of the emergency bodies, leading to inconveniencies in the neighbourhood - Panic in the neighbourhood
Likelihood:	Likely
Impact (main problem + cascading effects):	Major
S4RIS added value:	**- CAESAR (PREVENTION, RESPONSE):** 1) Know which improvement measures will work better than others, so that they can be implemented to prevent an attack/hazard. 2) Know overall resilience of the system throughout the entire timeline of a disruptive event occurring to be better prepared for future events. 3) Know which components are the weakest/most critical, so that closer attention can be paid to protect them. **- CAMS (PREVENTION, RESPONSE, RECOVERY):** 1) Be well informed on the budget to allocate to repair/maintain/rehabilitate the infrastructure after unexpected hazard events, so that a proactive plan can be made. 2) Know time and cost needed to respond a crisis and restore normal functioning, so that resource deployment and quick reactions can be made based on proactive actions planned. 3) Be aware of budgetary and time implication to recover the infrastructure, so that resource deployment can be made and financial loss controlled.

2.3 Resilience stages coverage

Given that the focus of SAFETY4RAILS is on resilience, in the following table it is presented how all Use-Cases formulated address the different stages proposed in the project, namely PREVENTION, DETECTION, RESPONSE and RECOVERY.

USE CASE	Resilience stage	Contribution
UC - 001: NATURAL DISASTER - FLOODING	Prevention	x
	Detection	x
	Response	x
	Recovery	x
UC - 002: TRACK INTERCEPTION DUE TO A LANDSLIDE THAT CAUSES AN IMMOBILIZATION OF THE TRAIN	Prevention	x
	Detection	x
	Response	x
	Recovery	
UC - 003: PHYSICAL ATTACK - TERRORISTIC ATTACK USING FIREARMS INSIDE A RAILWAY STATION	Prevention	
	Detection	x
	Response	x
	Recovery	
UC - 004: PHYSICAL ATTACK - (POTENTIAL) TERRORISTIC ATTACK VIA IED CARRIED VIA BAGGAGE	Prevention	x
	Detection	x
	Response	x
	Recovery	
	Prevention	x

UC - 005: TRAIN FAILURE INSIDE A TUNNEL WITHOUT POSSIBILITY TO COMMUNICATE WITH THE TRAIN DRIVER	Detection	x
	Response	x
	Recovery	
UC - 006: PHYSICAL ATTACK - INTRUSION AND BOMB PLANTED	Prevention	x
	Detection	x
	Response	x
	Recovery	x
UC - 007: PHYSICAL ATTACK - INTRUSION IN SENSITIVE PLACE	Prevention	x
	Detection	x
	Response	x
	Recovery	x
UC - 008: PHYSICAL ATTACK - SPOOFING ATTACK ON EXISTING SENSORS	Prevention	x
	Detection	x
	Response	
	Recovery	
UC -009: CYBER-ATTACK - MANIPULATION ON DATA TRANSFERRED TO OPERATING SYSTEM	Prevention	x
	Detection	x
	Response	
	Recovery	
UC - 010: CYBER-ATTACK - HACKING OF THE SIGNALLING SYSTEM CAUSING ACCIDENTS	Prevention	x
	Detection	x
	Response	x
	Recovery	
UC - 011: COMBINED CYBER-PHYSICAL ATTACK	Prevention	x
	Detection	x
	Response	x
	Recovery	x
UC - 012: LEVEL CROSSING ACCIDENT: SABOTAGE OR CYBER ATTACK	Prevention	x
	Detection	x
	Response	x
	Recovery	x

2.4 Use-cases vs S4R tools

A challenge identified in this process was to incorporate the features developed by each of the S4RIS components in the Use-Cases. The following table summarises each contributory tool on each Use-Case, ensuring that all technologies to be demonstrated in a TRL7 environment are covered.

USE CASE	BB3D	Blockchain	CAESAR	CAMS	CuriX	DATA FAN	Ganimide	iCrowd	PRIGM	RAM2	SARA	SecaaS	SECURAIL	SISC2	Senstation	TISAIL/OSINT	UNI|MS	WINGSPARK
UC - 001: NATURAL DISASTER - FLOODING			x	x				x			x		x		x			
					x	x								x			x	x
			x	x	x			x						x				x
				x							x							
UC - 002: TRACK INTERCEPTION DUE TO A LANDSLIDE THAT CAUSES AN IMMOBILIZATION OF THE TRAIN			x			x				x								
					x					x				x				

			x			x				x				x				
										x								
UC - 003: PHYSICAL ATTACK - TERRORISTIC ATTACK USING FIREARMS INSIDE A RAILWAY STATION																		
					x		x							x				
					x									x				
UC - 004: PHYSICAL ATTACK - (POTENTIAL) TERRORISTIC ATTACK VIA IED CARRIED VIA BAGGAGE			x														x	
					x		x							x			x	
			x											x				
UC - 005: TRAIN FAILURE INSIDE A TUNNEL WITHOUT POSSIBILITY TO COMMUNICATE WITH THE TRAIN DRIVER		x	x							x								
		x			x					x		x						
			x							x								
										x								
UC - 006: PHYSICAL ATTACK - INTRUSION AND BOMB PLANTED			x	x		x		x		x			x			x		
					x					x						x		
			x	x		x				x								
				x						x								
UC - 007: PHYSICAL ATTACK - INTRUSION IN SENSITIVE PLACE			x	x		x		x	x	x			x					
									x	x					x			
			x	x		x		x		x								
				x						x								
UC - 008: PHYSICAL ATTACK - SPOOFING ATTACK ON EXISTING SENSORS									x	x								
					x				x	x					x			
										x								
										x								
UC - 009: CYBER-ATTACK - MANIPULATION ON DATA TRANSFERRED TO OPERATING SYSTEM		x							x	x						x		
		x			x				x	x					x	x		
										x								
										x								
UC - 010: CYBER-ATTACK - HACKING OF THE SIGNALLING SYSTEM CAUSING ACCIDENTS			x							x						x		
					x	x				x						x		
			x		x					x								
										x								
UC - 011: COMBINED CYBER-PHYSICAL ATTACK	x		x	x		x		x	x	x			x			x		
						x				x						x		x
			x	x	x	x		x		x								x
	x			x						x								
UC - 012: LEVEL CROSSING ACCIDENT: SABOTAGE OR CYBER ATTACK			x	x														
												x		x				
			x	x										x				
				x														

2.5 Limitations

In the process of refining the Use-Cases, some limitations were encountered by the tool providers. First of all, the challenges in gathering the required data from the end-users. This limitation is being currently addressed by speeding up the process of data collection and enforcing mitigation measures in case the required data is not available from the end-user side (e.g., using open-source data or generating synthetic datasets). On the other hand, issues identified regarding the development of a unified data structure are being managed in WP6.

3. Simulation exercises overview

Section 3 will provide a general overview of the Simulation Exercises (SE) to be implemented during the project. The SE will be primarily driven by the operational objectives described in the DoA, part B, which are disclosed below. In this document, the SE handbook for the first two exercises, namely MDM and EGO, have been defined (Section 4). Dedicated workshops with the tool providers and the corresponding end-users were prepared and carried out on-line for MDM, on the 13th of October, and for EGO, on the 18th of November. The templates used by each tool provider are presented in **Annex IV**. It should be noted that the information disclosed in section 4 will be subject of continuous improvements before each SE date.

3.1 Main objectives

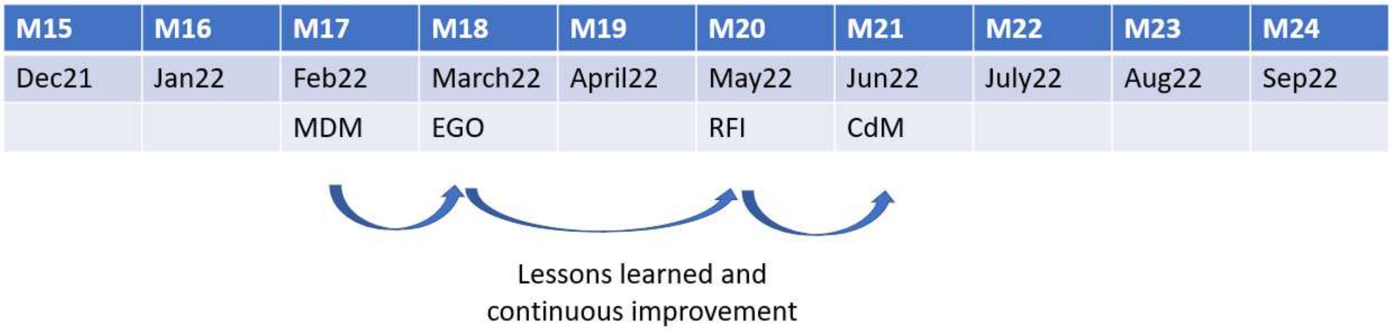
As stated in the DoA, part B, *"The overarching aim of SAFETY4RAILS is to increase resilience against combined cyber-physical threats including natural hazards to railway infrastructure. In this context, more resilient railway networks will be studied through the scenarios mentioned in Combined cyber and physical resilience of railway and metro infrastructures: Various locations where the threats can take place are considered".* In this context, the operational objectives of the project are outlined below:

- **O1: IDENTIFYING new threats:** Better understanding of potential cyber & physical threats and their possible impacts on railroad networks.
- **O2: DETECTING new threats:** Better forecast and improved detection capability of combined physical and cyber threats.
- **O3: AUTOMATING forecast & management of new threats:** Increase automation of cyber and physical anomalies forecasting and management.
- **O4: KNOWLEDGE sharing with stakeholders:** Improving information available to first responders and passengers through a secure framework as part of a holistic security scheme
- **O5: MEASURING impact of evolving cyber-physical threats:** Identifying potential blind spots in current crisis management capacities of railway operators and opportune quantification of impacts to enable appropriate reaction measures.
- **O6: SAVING response time through efficient and reliable decision support:** More accurate decision making by providing improved situational awareness to decision makers.
- **O7: INNOVATING and making response measures cost effective:** Adopting the latest generation technologies to make security the enabler rather than a cost. Strengthening the response measures to reduce the attack impact costs and to mitigate cascading effects.
- **O8: IMPROVING resilience of real-time crisis and security management:** Improving crisis management and decision-making support tools to enable real-time security management by training.
- **O9: INCREASING preparedness by a Holistic Resilience Analysis Approach for the entire multimodal infrastructure:** Extending rail transport infrastructure monitoring by considering regional and long-distance traffic aligned with smart city policies, distinguishing on transport typology and vehicles.
- **O10: TRAINING of users associated to different components of SAFETY4RAILS:** Informing practitioners on technology use, S4RIS capability and limitations, S4RIS integration in own decision processes, time required to fast reorganisation or rerouting.
- **O11: DEMONSTRATING the S4RIS operational performance and security effectiveness:** Validating the operational performance and security effectiveness of the S4RIS under realistic conditions.

These objectives are associated with KPIs defined in the DoA, and compliance with these DoA KPIs will be reported on separately in the later deliverables from WP8 and the final project report. Across the 4 Simulation Exercises planned during the project, the fulfilment of the objectives will be evaluated.

3.2 Timeline

The figure below presents the timeline of the four SE: Metro de Madrid (MDM), Ankara Metro (EGO), Rete Ferroviaria Italiana (RFI) and Comune di Milano (CDM).



M15	M16	M17	M18	M19	M20	M21	M22	M23	M24
Dec21	Jan22	Feb22	March22	April22	May22	Jun22	July22	Aug22	Sep22
		MDM	EGO		RFI	CdM			

FIGURE 1 SIMULATION EXERCISES TIMELINE

4. Simulation Exercises Handbook (First version)

4.1 Description of Simulation Exercise 1: MDM

4.1.1 Scenario

Section removed to enable public version.[2]

4.1.2 Participants[3]

The MDM Simulation Exercise (SE) team will be composed by the following participants:

- **Simulation exercise team:** ETRA, FRAUNHOFER, ELBIT, STAM, TREE, INNO, WINGS, RINA, RMIT, ERARGE, NCSRD, IC, MDM, LAU
- **SE leader: ETRA** responsible for overseeing and planning the simulation exercise.
- **Tools leaders:**
    - **FRAUNHOFER**
    - **ELBIT**
    - **STAM**
    - **TREE**
    - **INNO**
    - **WINGS**
    - **RINA**
    - **RMIT**
    - **ERARGE**
    - **NCSRD**
    - **IC**
- **Host (H): MDM** member of staff in host metro infrastructure that has access/influence on the implementation of the simulation and the seniority level to liaise with those team members having a key role/responsibility in the event.
- **Evaluation Manager (EM): LAU**, responsible of overseeing and guiding the Simulation Exercises (SE) evaluation, as well as organising the necessary material to collect feedback from the SE participants.
- **Dissemination Manager (DM):** (**LAU** responsible of organising dissemination and also and communication material for the SE runtime and after the SE.
- **Active Staff (AS):** Those actively involved during the simulation exercise. Can be staff from host metro infrastructure or from the Tools Leaders, including the named staff above and/or others.
- **Observers (O):** People within the consortium who are not actively involved during the simulation but will attend and watch it.
- **Data Controller (DC):** MDM as Project Data Controller, will be responsible for determining the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law (GDPR art4.7) (2).

4.1.3 Objectives

- **CAESAR(FHG):** One of the Simulation Exercise objectives is to test CAESAR's correct identification of weak components in the MDM infrastructure and the proposed improvement measures to prevent an

[2] Text provided to EU in an Annex to a deliverable with the dissemination level of Confidential.
[3] Individual participant names not included for public dissemination.

attack or mitigate the damages. The second objective is the evaluation of the adequacy of the proposed mitigation measures influencing resilience specific to the scenario. The simulation will give FHG a good representation of events to know if the CAESAR development is carried out in the right way thanks to the feedback of MDM as a metro infrastructure.

- **CAMS(RMIT):** Main objective of the simulation is testing friendly-user interface; completion of information developed; new features introduced (Prediction of normal deterioration due to aging and degradation of railway assets, Maintenance, and repair budget calculation for railway components, Deterioration, and budget calculation in case of extreme event). The exercise will give the chance to spot strong and weak points and gather suggestion from end-user point of view.
- **DATA FAN(FHG):** One objective is to test whether the number of predicted passengers for future time steps is an asset for redistributing passengers from the affected station to another. The second objective is to get feedback if the speed of computation is sufficient and if the presentation of the results is clear. The third objective is to evaluate whether the proposed reliability analysis for the results adds value to the end-user. If possible, the GUI of the DATA FAN tool should also be evaluated if it is clearly structured or too complex
- **RAM2(ELBIT):** Monitoring tool vendors workshop (together with CuriX) to ensure data structure and data insights, integration of testing scenarios with each monitoring data sources and recorded scenarios data for scenario simulation from monitoring tools, with all relevant event types, from each data sources.
- **CURIX(IC):** The first objective is to test CuriX to show identified anomalies in the behaviour of “MDM technical systems” from their monitoring data which could indicate a potential threat or disruption. A second objective is to test the identification of metrics and devices responsible for causing the major change in the system behaviour. Another objective is the evaluation the appropriateness of alerts and information related to content and timing as well as the health scores of the monitored technical system. A further objective is general feedback regarding the user-friendliness of the CuriX dashboard.
- **SECURAIL(STAM):** This Simulation Exercise will allow first to test SecuRail functionalities implemented in this initial release. For this purpose, SecuRail will be used to carry out an off-line risk analysis of the MDM network infrastructure under examination within the Simulation Exercise. The risk analysis will be based on a set of inputs, such as the areas and asset included within the sections and stations belonging to the infrastructure, the countermeasures with which they are equipped, the crowding levels etc. which will be entered by the user through the SecuRail UI. The simulation, indeed, will provide an overview of the core functionalities of SecuRail and it will allow end-user to identify risk level of different components of the network, as well as the most dangerous threat scenarios that can occur in its infrastructure and the consequent impact on people, assets, and services.
- **TISAIL/OSINT(TREE/INNO):** The main objective for TISAIL/OSINT in this simulation exercise is to provide cybersecurity threats that are relevant for MDM security team as well as to provide a better understanding of real threats in the railway/metro sector.
- **WINGSPARK (WINGS):** WINGSPARK tool objectives will constitute the three different phases. First to detect potentially overcrowded areas during the day of the event in the metro station, to better manage the crowd in case of emergency. Then, to detect if there are any anomalies in the metro speed, analyse them and send an alert to the system’s team. Finally, to inform, send details, during the response phase, of the detected issue in the metro speed. Alerts will be also raised in the case of overcrowded areas and guidelines in case of evacuation will be provided. Overall, WINGSPARK tool will try and identify anomalies, monitor areas in the facility and to detect if there is something that is not usual, possibly restrictions related to mobility (like forbidden areas etc.), overcrowded areas and propose measures to prevent chaos.
- **iCrowd (NCSRD):** iCrowd will be extended to provide not only the prediction of passenger flow rates and evacuation times assuming different congestion levels, but also the determination of the possible fallout from misleading information delivered by compromised digital assets. Crowd behaviours will also be refined to follow an objective-oriented approach, where instead of programming specific actions, the user will specify the objectives of a simulated agent and its actions will be determined automatically.

- **PRIGM(ERARGE):** Exchange the knowhow from previous and ongoing project for the sake of security assessment and vulnerability by (re)elicitation for the MDM data network and cyber infrastructure, identification of vulnerabilities within the network by analysing the communication and data transfer between nodes, analysis of the relations interlinking the nodes and extract the threat/attack surfaces. These objectives will be handled at low-level attack types (e.g., attack against hardware components) and will be aligned with the ENISA threat taxonomy.
- **BB3d (RINA):** based on surface burst experimental data (i.e., validated by definition), potential verification of some BB3d functionalities (e.g., casualties) by comparing numerical results with data collected considering the effects of past bomb attacks.

4.1.4 Location & Date

Event data: 8th -11th February.

Location of the event: a metro station Madrid

SE Location: Metro de Madrid Command-and-Control Centre.

4.1.5 Simulation Exercise Organisation

Event preparation (2-3 weeks before): The simulation exercise team gathers to review once again the information available in this document (D8.2), identify minor missing points (if any) and align all members on their duties. MDM will prepare the necessary internal resources identified to hold the simulation, along with the key team members required to receive relevant feedback during the demonstration and extract useful and practical lessons learned for the second round of tests.

The organisation of the Simulation Exercise has been divided into 3 phases, according to the resilience stages described before: 1) PREVENTION, 2) DETECTION&RESPONSE, 3) RECOVERY. The first and third phases are planned in a Workshop format, while the second one is planned as a Functional Simulation Exercise. Definitions for each type of exercise are provided in **Annex II.** The evaluation will be coordinated by the Evaluation Manager who will establish when and how information retrieval (e.g. questionnaires) will occur. It is expected that end-users will be able to evaluate the S4RIS and the tools at the end of each phase, therefore avoiding interruptions every time a tool contributes to the scenario.

4.1.5.1 Prevention

This phase of the demonstration will be conducted during a **Workshop**, involving the MDM personnel operating in the Command-and-Control Room and from other departments. The workshop will not be specifically oriented to the Scenario described above (Combined Cyber-physical attack), it will be focused on a pre-event phase where MDM personnel analyses main weaknesses in the infrastructure and prepare proactive mitigations. In fact, the consortium will target the analysis of weak components (cyber and physical), vulnerabilities and risk scenarios, mitigation measures, and the overall resilience of the system. Different sessions will be planned according to the MDM department involved (Civil Construction, Maintenance and Security). According to the script provided in section 4.1.1, the different activities planned for the S4RIS, and each tool are described below:

<u>Civil Construction Department</u>

1. **<u>Bomb blast 3D (BB3d)</u>**

RINA-C demonstration will be focused on the development of a complete analysis concerning a blast scenario on a discretised geometry (STL ASCII file) that has been generated before the demonstration. The main stages of the demonstration include the description of the discretised model of the asset of interest and of the input file parameters, the launch of the analysis and the visualization and description of the main results generated.

1. Simulation Information Analysis (before the SE)

- Activity 1 – Description of the generation of a discretised geometry suitable for BB3d calculation.
- Activity 2 – Introduction of the discretise geometry of the asset for the demonstration.
- Activity 3 – Introduction of the features and parameters of the input files to set for running a BB3d calculation.

2. Simulation Analysis

- Activity 1 – Run of BB3d calculation.
- Activity 2 – Brief description of the information reported on the screen.

3. Analysis of the results (supporting BB3d in prevention actions)

- Activity 1 – Overview of the output files.
- Activity 2 – Visualization of VTK files (both peak and transient data).
- Activity 3 – Description of the main data of interest reported in the output files.
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

Maintenance Department

1. Central Assets Management System (CAMS)

The demonstration will be conducted during a workshop involving the MDM personnel operating in the Asset Management Department, and it will be focused on proactive planning based on information on the budget to allocate to repair/maintain/rehabilitate the infrastructure in normal condition and after unexpected hazard events.

1. Simulation Information Analysis

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – RMIT analyses the information and prepares CAMS

2. Simulation Analysis

- Activity 1 - Evaluation of input parameters for CAMS with MDM
- Activity 2 – Evaluation of results of CAMS with MDM:
    - Results of proactive planning including degradation of the critical assets under normal condition (ageing degradation) and under the simulated event; Cost to maintenance, repair, replace

3. Analysis of the results (supporting CAMS in prevention actions)

- Activity 1 – MDM visualises the results in the GUI
- Activity 2 – MDM analyses the results and selects alternative budgetary strategies to repair/maintain/rehabilitate after the event
- Activity 3 – MDM provides feedback to RMIT (suggesting new scenarios, conditions, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met

- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

Security Department

1. SecuRail

1. Simulation Information Analysis

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2). For what concerns SecuRail, requested inputs can be collected in two manners:
    - MDM can directly enter requested data through the UI of the tool
    - STAM can provide MDM with a dedicated template (e.g., an Excel file) to collect required inputs and then STAM will enter them into SecuRail.

The first option is preferred to exploit this first Simulation exercise to evaluate easiness and clearness of SecuRail UI. The most appropriate option will be decided based on the detailed agenda of the exercise.

2. Simulation Analysis

- Activity 1 – Evaluation of SecuRail results with MDM:
    - Outputs of the risk assessment paying particular attention to the correlation between the input values and the values obtained as results.

3. Analysis of the results (supporting SecuRail in prevention actions)

- Activity 1 – MDM visualises the results in the GUI
- Activity 2 – MDM provides feedback to SecuRail (suggesting new functionalities, conditions, items to be considered during a risk assessment, etc.)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

2. TISAIL/OSINT

1. Simulation Analysis

- Activity 1 – Assessment of potential vulnerabilities

2. Analysis of the results

- Activity 1 – MDM visualises the vulnerabilities provided by TISAIL/OSINT through RAM2 GUI.
- Activity 2 – MDM adapts their security detection tools (e.g., IDS, SIEM) with some of the IoCs (Indicators of Compromise) of the vulnerabilities provided by TISAIL/OSINT.
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

3. DATAFAN

DATA FAN will focus on the reliable prediction of passenger load on specific metro stations. The Control Room Coordinator asks the user to provide reliable numbers for the passenger load to work on a plan for the worst-case scenario, for example the closure of a station due to an unexpected event. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the past passenger load (see section 4.1.8.2).
- Activity 2 – FHG analysis the information and prepares DATA FAN for this specific prediction and data pre-processing.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to MDM
- Activity 2 – Evaluation of results of DATA FAN with MDM:
    - 1) Statistical evaluation of the data set
    - 2) Prediction of passenger load for specific selected stations for future time steps
    - 3) Reliability score for the results to enhance technology acceptance

3. Analysis of the results

- Activity 1 – FHG visualises the results in the GUI
- Activity 2 – MDM analyses the results and selects strategies for improving the prediction results
- Activity 3 – FHG improves the results with refined input parameters for the calculation
- Activity 4 – MDM provides new feedback to FHG
- Activity 5 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 6 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4. CAESAR

CAESAR tool will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. The Security Coordinator asks the user to implement mitigation measures to test which of them would work better on the infrastructure. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – FHG analysis the information and prepares CAESAR
- Activity 3 – Integration of results from DATA FAN into CAESAR

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to MDM
- Activity 2 – Evaluation of results of CAESAR with MDM:
    - 1) resilience curves of performance over time throughout the adverse event (before, during and after),
    - 2) ranking of mitigation measures specific to threat
    - 3) list and ranking of critical components specific to threat, cascading effects analysis (in terms of critical components)

3. Analysis of the results (supporting CAESAR in prevention actions)

- Activity 1 – MDM/CaESAR visualises the results
- Activity 2 – MDM analyses the results and selects alternative mitigation measures (if necessary)
- Activity 3 – MDM provides feedback to FHG (suggesting new scenarios, conditions, cascading effects, mitigation measures, recovery times, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

5. iCrowd

The iCrowd simulator will focus on the simulation of infiltration/escape scenarios to better understand the chance of detection for different CCTV cameras and guards' configurations. The Security Coordinator asks the user to test different configurations to assess potential vulnerabilities in the station. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – NCSRD analyses the information and prepares iCrowd.
- Activity 3 – Integrate with other tools that provide input to iCrowd, such as BB3D and CaESAR

2. Simulation Analysis

- Activity 1 – Short presentation regarding the analysis of the input data and the scenarios that are going to be implemented to MDM
- Activity 2 – Execution of simulations and evaluation of initial results with MDM:
    - Visualize the result of a disruption or fallout of an attack, to provide a better point of view and lead to better safety measures and mitigation strategies
    - Use of final KPIs to evaluate and improve resilience/mitigation strategies
    - Observe the effect of real-time adjustments to the simulation, determine chain reactions, etc.
- Activity 3 – MDM creates a set of configurations for each simulation scenario, NCSRD runs the simulations and provides MDM with the results

3. Analysis of the results (supporting iCrowd in prevention actions)

- Activity 1 – MDM analyses the results and selects alternative mitigation measures (if necessary)
- Activity 2 – MDM provides feedback to NCSRD (suggesting new scenarios, conditions, etc…)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

6. PRIGM

PRIGM tool will focus on the threat risk analysis related to authentication and data security and privacy vulnerabilities. This will be realised by re-elicitation of the attack surfaces and mapping the vulnerabilities with respect to the ENISA threat taxonomy. PRIGM will be used mainly at security and privacy analysis phase and potential countermeasures will be proposed in accordance with the PRIGM's capabilities. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the data network infrastructure and the types of data travelling within the system
- Activity 2 – ERARGE will analyse the network topology and identify the potential vulnerabilities within the targeted data network

2. Simulation Analysis

- Activity 1 - Present a short report regarding the vulnerability analysis of the input data to MDM with respect to the ENISA threat taxonomy.
- Activity 2 – Present countermeasures to improve the resilience of the network with a special focus on authentication-related and hardware-based cryptographic solutions

3. Analysis of the results

- Activity 1 – MDM analyses the results and gives feedback about alternative countermeasures (if necessary)
- Activity 2 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 3 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

7. RAM2

RAM2 processes cyber physical assets information and events, received from S4RIS monitoring tools, for identification of vulnerabilities and provides risk assessments within the operations context.

1. Simulation Information Analysis

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2). RAM2 requires information about the operational hierarchy of MDM, process and asset criticality information, details of cyber physical assets.

2. Simulation Analysis

- Activity 1 - Evaluation of input parameters for RAM2 with MDM.
- Activity 2 - Vulnerability assessment by RAM2.

3. Analysis of the results (supporting RAM2 in prevention actions)

- Activity 1 – MDM visualises the results in the GUI and using the system reports.
- Activity 2 – MDM provides feedback to RAM2
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4.1.5.2 Detection & Response

The detection and response phases will be carried out in the same step of the exercise due to the fact they are both closely connected and can happen simultaneously during an ongoing crisis. In fact, the format of this step of the exercise will be as a **"Functional Simulation Exercise",** where activities will be driven by the scenario described in section 4.1.1 and will engage the relevant team members of Metro de Madrid. The Functional Simulation Exercise will be focused on how security operators interact with the S4RIS and the value-added by each individual tool. Therefore, the focus will be on the **alerts raised by the system** – and the usefulness of the details provided by the alerts, and the **mitigation recommendations** provided to the end-user. User interfaces from the individual tools will be presented when appropriate.

Before visualising the performance and contribution of each tool to the S4RIS, each Tool Leader will have the opportunity of performing a brief introduction (1-2min) regarding: 1) User input data, 2) User benefits (value-added to end-user) and 3) Results offered to end-user. In the following lines, the role of each tool leader and the main related activities are described:

1. **TISAIL/OSINT**

1. Simulation Analysis

- Activity 1 – Assessment of potential threats

2. Analysis of the results

- Activity 1 – MDM visualises the threats provided by TISAIL/OSINT through RAM2 GUI. The alarms could be phishing campaigns and vulnerabilities of the monitored HW and SW.
- Activity 2 – MDM adapt their security detection tools (e.g., IDS, SIEM) with some of the IoCs (Indicators of Compromise) of the threats provided by TISAIL/OSINT
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

2. **CURIX**

CuriX demonstration will be focused on: Analysing monitoring data of technical systems towards anomalous behaviour, which could indicate upcoming threats, together with information regarding health of system, or metrics and devices causing change in system behaviour by operational and functional testing of CuriX for the detection stage.

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – IC analyses the information and prepares CuriX and data

2. Simulation Analysis

- Activity 1 – Present a short report regarding the analysis of the input data to MDM
- Activity 2 – Tool leader performs simulation
- Activity 3 – If deemed appropriate, IC will present the CuriX GUI so that MDM visualises the results
- Activity 4 – Evaluation of results of CuriX with MDM:
  - 1) Number of past and current alerts on detected anomalies in the monitoring data of technical system
  - 2) List and ranking of metrics or devices causing major changes in behaviour of technical systems
  - 3) List and health scores of metrics or devices of technical systems
  - 4) Information presented in dashboard

3. Analysis of the results (supporting CuriX in detection actions)

- Activity 1 – MDM provides feedback to IC (e.g., appropriateness of alerts and results related to content and timing)
- Activity 2 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 3 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

3. DATAFAN

DATA FAN will be focused on the prediction of reliable passenger load on specific metro stations and detection of the capacities that are sufficient or have to be improved. The Control Room Coordinator asks the user to provide reliable numbers for the passenger load to work on an improved plan with modified capacities in extreme situations, e.g., after a football game. The organisation process is divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the past passenger load (see section 4.1.8.2).
- Activity 2 – FHG analysis the information and prepares DATA FAN for this specific prediction and data pre-processing

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to MDM
- Activity 2 – If appropriate, FHG will present the DATAFAN GUI so that MDM visualises the results
- Activity 3 – Evaluation of results of DATA FAN with MDM:
    - 1) Statistical evaluation of the data set
    - 2) Prediction of passenger load for specific selected stations for future time steps
    - 3) Reliability score for the results to enhance technology acceptance

3. Analysis of the results

- Activity 1 – MDM analyses the results and selects strategies for improving the prediction results
- Activity 2 – FHG improves the results with refined input parameters for the calculation
- Activity 3 – MDM provides new feedback to FHG
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4. WINGSPARK

WINGSPARK will be focused on 1) the detection of anomalies in the metro speed, analyse them and send an alert to the system's team. Detection of potentially overcrowded areas during the day of the event in the metro station, to better manage the crowd in case of emergency. 2) send details, of the detected issue in the metro speed. Alerts will be also raised in the case of overcrowded areas and guidelines in case of evacuation will be provided.

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the train speed profile and camera input for crowd concertation detection (see section 4.1.8.2).

- Activity 2 – WINGS analysis the information and prepares WINGSPARK for the anomaly detection in both components.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to MDM
- Activity 2 – Evaluation of results of WINGSPARK with MDM:
    - Results of detecting an anomaly in metro speed or an overcrowded area.

3. Analysis of the results (supporting WINGSPARK in prevention actions)

- Activity 1 – MDM get the alerts, in case of anomalies
- Activity 2 – MDM analyses the results
- Activity 3 – MDM provides feedback to WINGSPARK (suggesting new scenarios, conditions, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

5. iCrowd

The iCrowd simulator will focus on crowd behaviour during a disruption of a metro station due to a cyber-physical attack. The simulations will include the prediction of passenger flow rates and evacuation times assuming different congestion levels, the determination of the possible fallout from misleading information delivered by compromised digital assets, all based on different mitigation strategies or their parameters. Overall, iCrowd will predict the consequences of the incident on the passengers leveraging the information regarding passenger flow. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – NCSRD analyses the information and prepares iCrowd
- Activity 3 – Integrate with other tools that provide input to iCrowd, such as BB3D and CaESAR

2. Simulation Analysis

- Activity 1 - Short presentation regarding the analysis of the input data and the scenarios that are going to be implemented to MDM
- Activity 2 – Execution of simulations and evaluation of initial results with MDM:
    - Visualize the result of a disruption or fallout of an attack, to provide a better point of view and lead to better safety measures and mitigation strategies
    - Use of final KPIs to evaluate and improve resilience/mitigation strategies
    - Observe the effect of real-time adjustments to the simulation, determine chain reactions, etc.
- Activity 3 – MDM creates a set of configurations for each simulation scenario, NCSRD runs the simulations and provides MDM with the results

3. Analysis of the results (supporting iCrowd in response actions)

- Activity 1 – MDM analyses the results and selects alternative mitigation measures (if necessary)
- Activity 2 – MDM provides feedback to NCSRD (suggesting new scenarios, conditions, etc…)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

6. CAESAR

CAESAR tool will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. The Security Coordinator asks the user to implement mitigation measures to test which of them would work better on the infrastructure. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – FHG analysis the information and prepares CAESAR
- Activity 3 – Integration of results from DATA FAN into CaESAR

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to MDM
- Activity 2 – Evaluation of results of CAESAR with MDM:
  - 1) resilience curves of performance over time throughout the adverse event (before, during and after),
  - 2) ranking of mitigation measures specific to threat
  - 3) list and ranking of critical components specific to threat, cascading effects analysis (in terms of critical components)

3. Analysis of the results (supporting CAESAR in prevention actions)

- Activity 1 – MDM visualises the results
- Activity 2 – MDM analyses the results and selects alternative mitigation measures (if necessary)
- Activity 3 – MDM provides feedback to FHG (suggesting new scenarios, conditions, cascading effects, mitigation measures, recovery times, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

7. RAM2

RAM2 demonstration will be focused on orchestration of data from multiple sources, generation of alerts and correlated insights and contextualization of the information in accordance with the operational structures of MDM.

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2)
- Activity 2 – ELBIT analyses the information and prepares RAM2 and data.

2. Simulation Analysis

- Activity 1 – RAM2 processes data from available systems in the simulation
- Activity 2 – Tool leader performs simulation
- Activity 3 – ELBIT presents the RAM2 GUI and reports to MDM
- Activity 4 – Evaluation of results of RAM2 with MDM:

3. Analysis of the results (supporting RAM2 in detection actions)

- Activity 1 – MDM provides feedback to ELBIT
- Activity 2 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 3 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4.1.5.3 Recovery

This phase of the demonstration will be performed in a similar manner to the Prevention phase – through a **Workshop**. However, the workshop will be specifically targeting the recovery after the events happened in the Scenario and outcomes from the "Detection & Response" phase. Therefore, it will be a post-event evaluation to help the MDM experts to recover the infrastructure and support business continuity. Two sessions will be planned according to the MDM department involved (Maintenance & Civil Construction). According to the script provided in section 4.1.1, the different activities planned for the S4RIS, and each tool are described below:

1. **Central Assets Management System (CAMS)**

The demonstration will be conducted during a workshop involving the MDM personnel operating in the Asset Management Department, and it will be focused on: 1) Optimal resource deployment during response thanks to information related to time and cost needed to respond a crisis and restore normal functioning, 2) Optimal resource deployment and financial loss control during recovery based on information related to time, cost and performance loss.

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.1.8.2).
- Activity 2 – RMIT analysis the information and prepares CAMS

2. Simulation Analysis

- Activity 1 - Evaluation of input parameters for CAMS with MDM
- Activity 2 – Evaluation of results of CAMS with MDM:
    - Result in terms of structure resilience: performance loss assessment, cost, and time for recovery service
    - Results of optimal resource deployment to recover after the crisis including degradation of the critical assets under normal condition and under the simulated event; Cost to maintenance, repair, renew

3. Analysis of the results (supporting CAMS in recovery actions)

- Activity 1 – MDM visualises the results in the GUI
- Activity 2 – MDM analyses the results and selects alternative budgetary strategies to respond to the crisis
- Activity 3 – MDM provides feedback to RMIT (suggesting new scenarios, conditions, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

2. **Bomb blast 3D (BB3d)**

RINA-C demonstration will be focused on the analysis of the blast scenario with the asset of interest for recovery purposes.

1. Simulation Information Analysis

- Activity 1 – Description of the modifications applied to the previously presented study.

2. Simulation Analysis

- Activity 1 – Run of BB3d calculation.

3. Analysis of the results

- Activity 1 – Description of the main data and results of interest
- Activity 2 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 3 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4.1.6 Equipment/Supplies

The following table provides an overview of the technical equipment and supplies required by each tool provider during the simulation:

TABLE 2 MDM SIMULATION EXERCISE – EQUIPMENT AND SUPPLIES REQUIRED BY EACH TOOL LEADER

TOOL PROVIDER NAME	EQUIPMENT/SUPPLIES	NOTES
FRAUNHOFER (CAESAR)	PCs, laptop, ethernet connection	
FRAUNHOFER (DATA FAN)	Laptop (will be brought by us), second screen and internet connection are expected to be provided	
ELBIT	Linux server, desktop / laptop PC, ethernet connection to Kafka, internet connection …	
STAM	PCs, laptop, ethernet connection, Wi-Fi connection	SecuRail is a web application, indeed internet connection is mandatory.
TREE/INNO	Laptop, ethernet connection	Internet connection required
WINGS	Laptop, ethernet connection	WIFi
RINA	PCs, laptop, ethernet connection	PC with Paraview installed for visualising results

RMIT	PCs, laptop, ethernet connection	There is a chance that someone will be connected in remote from Australia to ease simulation run
ERARGE	-	
NCSRD	PC, stable internet connection (for remote execution)	
IC	Laptop provided by IC, power supply and WiFi connection must be provided on site	

4.1.7 Applicable Legislation/Regulation

For the performance of the S4RIS, WINGSPARK will utilise open-source/synthetic CCTV video streaming to analyse overcrowded areas. Apart from that, no personal data will be stored, accessed, or distributed in this simulation exercise for technical implementations. However, personal data will be collected for the purpose of the evaluation of the simulation (D8.1). In general terms, to comply with ethical and privacy legislation, deliverables **D9.1: SAFETY4RAILS Ethical Compliance Framework (ECF)**, **D11.1: H – Requirement No.1** (Informed Consent and Procedures) and **D11.3: POPD – Requirement No. 3** (Personal data processing) will be used as reference. The following legal, ethical and policy requirements will be also complied:

- Respect to right of access, rectification and opposition.
- The Data Controller (DC) determines the purpose and manner in which any personal data are, or are to be processed, kept and destroyed.
- Ensure the protection of privacy.
- Comply with recognized ethics.
- Not to show and disseminate internal information provided by end-users.
- Protect the rights and physical integrity of security personnel and other stakeholders.
- Project and its outcomes will attempt to protect the rights and physical integrity of people.

Ethical/privacy-related and legal requirements. The following legislation will be addressed:

- Charter of Fundamental Rights of the European Union (200/C 364/01).
- Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast).
- General Data Protection Regulation (EU) 2016/679 (GDPR).
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

4.1.8 Performance Expectations

The performance expectations of the SAFETY4RAILS Information System (S4RIS), and the each of the contributing tools, for this simulation exercise were detailed in deliverable **D8.1: Evaluation Methodology**. This deliverable was based on technical specifications elicited in the deliverable D1.4, which answered a wide set of the end-users' requirements collected in WP2. Furthermore, D8.1 has been prepared in parallel with the present document (D8.2) and takes into consideration the scenario description and organisation. As a result, the simulation success criteria were formulated based on objectives at 3 levels:

1) Usability of the S4RIS platform
2) Specific requirements of the S4RIS platform
3) Scenario-based requirements/objectives

More information can be found in the aforementioned report.

4.1.8.1 Execution

In this section, a detailed description of the **interaction between each Tool Leader and the Host** (MDM) during the simulation exercise is provided. The goal is to have a clear understanding of how the end-user and the tool leader will interact to optimise the time used and avoid confusions during the exercise. This will further enhance end-users' interpretation of the tools (and related outcomes) and therefore the lessons learned.

Furthermore, in a real scenario some tools may run or provide insights simultaneously, specially during DETECTION and RESPONSE activities. To provide a clear operational picture for the end-users, the tools will be executed in a sequence. The execution sequence for each resilience stage was described in Section 4.1.1.

CAESAR:

1. FHG explains the functionalities briefly and how MDM should interact with the tool, starting with input parameters.
2. MDM reviews and provides information to select/improve input parameters (only exemplary, for a few examples)
3. FHG user updates input parameters if necessary
4. MDM receives results about the overall resilience of the system and indicates mitigation measures
5. FHG user receives feedback and implement mitigations. Results are reported back to MDM for feedback and to the relevant tools (e.g., RAM2).
6. MDM evaluates the tool. A questionnaire is filled out at the end.

CAMS:

1. RMIT explains the functionalities briefly and how MDM should interact with the tool, starting with input parameters
2. MDM reviews and provides information to select/improve input parameters if needed and then inputs parameters
3. MDM receives info about an investment plan (cost for intervention and repair)
4. MDM reviews with RMIT the output obtained
5. RMIT asks feedback for eventual improvement of functionalities and interface. A questionnaire is filled out at the end.

DATA FAN:

1. FHG explains the functionalities briefly and how MDM could interact with the tool, starting with input parameters.

2. MDM receives results about the number of passengers for future time steps
3. FHG answers questions to the user regarding the results if any
4. MDM evaluates results and requests better results if needed
5. FHG will improve the results if deemed appropriate in step 4.
6. MDM tests and evaluates the tool. A questionnaire is filled out at the end.

RAM2:

1. Elbit explains the functionality of RAM2 and how MDM should interact with the tool.
2. End-user consumes the data through RAM2 Dashboard display.
3. The end-user follows the prioritized Insights and Alerts with mitigation steps for each of the alerts for risk reduction and responses to detection of ongoing threats.
4. MDM evaluates the tool and its results through a questionnaire prepared by Elbit.

CURIX

1. IC briefly explains the functionalities and how MDM should interact with the tool.
2. IC performs simulation.
3. MDM receives results in terms of anomalies of the behaviour of technical systems, ranking causing major changes in the behaviour of technical systems, health scores of metrics and devices. Alerts will be manually dispatched by an IC member to avoid configuring mailing connections.
4. MDM tests and evaluates the tool and its results. A questionnaire is filled out at the end.

SECURAIL

1. STAM explains the functionalities of SecuRail and how MDM should interact with the tool, starting with the entering of the required inputs.
2. MDM reviews and provides information to insert input parameters (only exemplary, for a few examples)
3. STAM updates input parameters if necessary.
4. MDM visualize results of the risk analysis and indicates potential security measures that could be implemented within the network infrastructure to mitigate risks.
5. STAM receives the feedback and implement the suggested countermeasures. Results are reported back to MDM for feedback.
6. MDM tests and evaluates the tool through a questionnaire prepared by the consortium.

TISAIL/OSINT

1. TREE/INNO explains the different threats that can be relevant for MDM.
2. MDM reviews the threat alerts for situational awareness
3. MDM use some of the information provided to update their mitigation measures (e.g., IDS, SIEMs, etc)
4. MDM tests and evaluates the alerts provided.
5. TREE/INNO receives feedback about the quality and interest of the alerts through a questionnaire. TREE/INNO will consider the feedback for future interactions/adaptations in the tool.

WINGSPARK

1. WINGSPARK explains the functionalities and how the interaction with MDM would happen, starting with input parameters.
2. MDM reviews the above information.
3. WINGSPARK user updates input parameters if necessary and try different test scenarios.
4. WINGSPARK implements anomalies scenarios. Results are reported back to MDM for feedback.
5. MDM evaluates the tool. A questionnaire is filled out at the end.

iCrowd

1. NCSRD explains the existing and possible functionalities and KPIs of iCrowd related to the MDM simulation exercise (to be done before the SE)
2. MDM explains the incidents and the resilience/mitigation strategies they would like to study using iCrowd (to be done before the SE)
3. NCSRD designs and presents the simulation scenarios that are going to be developed (to be done before the SE)
4. MDM reviews the scenarios and adjusts if necessary (to be done before the SE)
5. NCSRD implements the scenarios and showcases them, along with the inputs that MDM is required to provide.
6. MDM provides a set of configurations (input parameters).
7. NCSRD executes the available configurations, extracts the results, and shows them to MDM.
8. MDM reviews the results and extracts conclusions.
9. If more configurations are required, MDM sends new configurations to NCSRD and steps 7 and 8 are repeated. Repeat until enough results are gathered.
10. MDM evaluates the overall functionality of iCrowd and provides feedback regarding its functionality and what else they would like to achieve.

BB3d

1. RINA-C describes the main functionalities of BB3d, the rationale for its development and how the interaction with MDM would happen, starting with input parameters (e.g., coming from iCrowd computing)
2. RINA-C will set input data
3. RINA-C will launch the analysis
4. RINA-C will assess numerical results with reporting files (logs and utility files, e.g., casualties and people injured) and VTK files (visualised through the open-source visualisation tool Paraview)

PRIGM

1. ERARGE will work on the vulnerability analysis, relying on desktop studies (before the SE)
2. ERARGE will perform a presentation of the vulnerability report, together with countermeasures in relation with the capabilities of PRIGM
3. Inputs from other tool provider to protect the MDM network or improve the resilience can be incorporated by joint discussions

4.1.8.2 Data acquisition

Before the simulation, each tool provider will collect the necessary data enabling the functionalities offered to the end-user during the exercise. For specially challenging and sensitive data types described below, realistic data generated synthetically will be utilised. During the simulation, data relevant to the configuration of the tool, feedback and indications from the end-users will be used. During and after the simulation, information regarding the evaluation (reflected in D8.1, including the data acquisition methodology) will be also collected.

The data required from the end-user for setting up the tools before the simulation is described below:

TABLE 3 MDM SIMULATION EXERCISE – DATA REQUIRED FROM END-USER

TOOL NAME	DATA INPUTS REQUIRED FROM END-USER
CAESAR	System components (physical and cyber), system component attributes, system connections (internally and to external networks), system functions, dependencies between system functions, dependencies and influences of system components, threat impact to components and functions, prevention, response and recovery strategies, mitigation measures currently in use and to be tested
CAMS	At least two consecutive regular data inspections on assets; Time and cost spent in maintenance, repair, renewal. Capital value of the elements; Cost of asset maintenance under normal degradation; time allocated for maintenance of the element; Cost of asset repair under normal degradation and hazard event. Cost and time of asset rehabilitation under normal degradation and/or hazard event
CuriX	General time series data from IT infrastructure during their normal operations and, if available, disruptions of the IT systems (due to cyber and or physical incidents). The monitoring data from IT infrastructure could be from: (data that is collected from performance monitoring tools, IT operations management software, application monitoring tools, other tools from data centres, connected to security tools (firewall activities, SIEM tool activities, other tools used in (cyber) security operations centres or computer security incident response teams), network management systems,). *For a small part of the IT data set, IC can provide data set of an IT environment (also with artificial incident). This data would be of general purpose but not specific to the MDM use-case.
iCrowd	3D Model of the environment

TOOL NAME	DATA INPUTS REQUIRED FROM END-USER
	Locations of cameras, guards (and their movement patterns) (these will be adjustable, only need something as baseline)
RAM2	Operational hierarchy of MDM (operational units and related assets), Criticality of assets and operational units, mitigation measures currently in use, cybersecurity compliance and policy requirements
SecuRail	Network information (typology, number of stations, number of sections). Expected crowding level for each station. List of assets prevent in each area of the analysed stations. List of countermeasures equipped in each area of the analysed stations. Economic value of each asset. Economic value of each area. Information related to each section. Default Value of Statistical Life
TISAIL/OSINT	This includes representative examples of all levels of devices that may be susceptible to attacks or threats via technical means (e.g., station control systems, transformer equipment, CCTV cameras, networking infrastructure, information displays and display content management, station control systems, office PCs, etc).
WINGSPARK	Time series data of trains speed, especially for before reaching the station. Preferably one-year historical data to train the model. Camera stream/frames dedicated to crowd monitoring or other input info to estimate the crowd concentration, detailed plans of the infrastructure/building with dimensions and units.
DATA FAN	Number of passengers for each station/ train
BB3D	File of the three-dimensional geometry of interest (e g stadium, buildings) in ASCII STL format Bomb mass (type of explosive (e.g., C_4, TNT) and explosion' location.
PRIGM	System architecture, topology, and data flow diagrams with respect to authorised roles and priorities.

Data collection process for all the data types described in the table above is ongoing and will be finalised within a reasonable timeframe before the simulation to make the S4RIS, and the individual tools, ready for the exercise.

4.2 Description of Simulation Exercise 2: EGO

4.2.1 Scenario

Section removed to enable public version.[4]

4.2.2 Participants[5]

The EGO Simulation Exercise (SE) team will be composed by the following participants:

- **Simulation exercise team:** ERARGE, FRAUNHOFER, LDO, IC, STAM, TREE, RMIT, INNO, NCSRD, ELBIT, EGO, TCDD, LAU
- **SE leader: ERARGE** responsible for overseeing and planning the simulation exercise.
- **Tools leaders:**
  - **FRAUNHOFER**)
  - **LDO**
  - **IC**
  - **ERARGE (PRIGM & Senstation)**
  - **STAM**
  - **TREE**
  - **INNO**
  - **RMIT**
  - **NCSRD**
  - **ELBIT**
- **Host (H): EGO** member of staff in host metro infrastructure that has access to/influence on the implementation of the simulation and the seniority level to liaise with those team members having a key role/responsibility in the event.
- **Co-Host (H): TCDD** member of staff in co-host railway infrastructure that has access/influence on the implementation of the simulation and the seniority level to liaise with those team members having a key role/responsibility in the event.
- **Evaluation Manager (EM): LAU** responsible of overseeing and guiding the Simulation Exercises (SE) evaluation, as well as organising the necessary material and to collect feedback from the SE participants.
- **Dissemination Manager (DM): LAU** responsible of organising dissemination and communication material for the SE runtime and after the SE.
- **Active Staff (AS):** Those actively involved during the simulation exercise. Can be staff from host metro infrastructure or from the Tools Leaders, including the named staff above and/or others.
- **Observers (O):** People within the consortium who are not actively involved during the simulation but will attend and watch it.
- **Data Controller (DC):** MDM) as Project Data Controller will be responsible for determining the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by EU or Member State law (GDPR art4.7) (2).

[4] Text provided to EU in an Annex to a deliverable with the dissemination level of Confidential.

[5] Individual participant names not included for public dissemination.

4.2.3 Objectives

- **CAESAR(FHG):** One of the Simulation Exercise objectives is to test CAESAR correct identification of weak components in the EGO infrastructure and the proposed improvement measures to prevent an attack or mitigate the damages. The second objective is the evaluation of the adequacy of the proposed mitigation measures influencing resilience specific to the scenario. The simulation will give FHG a good representation of events to know if the CAESAR development is carried out in the right way thank to the feedback of EGO as a metro infrastructure.
- **DATA FAN(FHG):** One objective is to test whether the number of predicted passengers for future time steps is an asset for redistributing passengers from the affected station to another. The second objective is to get feedback if the speed of computation is sufficient and if the presentation of the results is clear. The third objective is to evaluate whether the proposed reliability analysis for the results adds value to the end user. If possible, the GUI of the DATA FAN tools should also be evaluated if it is clearly structured.
- **Ganimede (LDO):** The main objective will be the detection of objects and people in each frame with Convolutional Neural Networks (CNN) and their movement to determine if the object is candidate for being abandoned.
- **CURIX (IC):** The first objective is to test CuriX to show identified anomalies in the behaviour of “EGO’s technical systems” from their monitoring data which could indicate a potential threat or disruption. A second objective is to test the identification of metrics and devices responsible for causing the major change in the system behaviour. Another objective is the evaluation the appropriateness of alerts and information related to content and timing as well as the health scores of the monitored technical system. A further objective is general feedback regarding the user-friendliness of the CuriX dashboard.
- **PRIGM (ERARGE):** The main objective is to prevent cyber and cyber-physical attacks by establishing a secure data channel between end nodes (i.e., Senstation which is a secure gateway encrypting the sensor data collected from the field). This will be realised by providing point-to-point security and hardware-based cyber protection at physical layer, where data is generated. This approach will improve the resilience of the data channel between the end nodes (like sensors or systems in important rooms) and the main control centres (e.g., OCs).
- **SECURAIL (STAM):** SecuRail will be used to carry out an off-line risk analysis of the EGO network infrastructure under examination within the Simulation Exercise. The risk analysis will be based on a set of inputs, such as the areas and asset included within the sections and stations belonging to the infrastructure, the countermeasures with which they are equipped, the crowding levels etc. which will be entered by the user through the SecuRail UI. The simulation, indeed, will provide an overview of the core functionalities of SecuRail and it will allow end-user to identify risk level of different components of the network, as well as the most dangerous threat scenarios that can occur in its infrastructure and the consequent impact on people, assets, and services.
- **Senstation (ERARGE):** The main objective is to validate the functionality of the server-client/node communication by presenting a laboratory-scale implementation of sensors and Senstation. Testing and comparison with historical data acquisitions over the alternative secure data channel (digital twin of the actual system) will be realised to show how the communication between end nodes and the OC can be secured. The anomalies within the sensory data will also be detected by checking the integrity of the sensory data and applying statistical analyses to identify outlier cases within the sensor data measurements.
- **TISAIL/OSINT (TREE/INNO):** The main objective for TISAIL in this simulation exercise is to test functionally with real/realistic device and component data used in the system and to simulate the detection of vulnerable devices.
- **CAMS (RMIT):** Testing of the technical functionality in detail ahead the use-case, presentation focused on the comparison with real data if they are available and table-top exercise to evaluate the predictions produced by the tool.

- **iCrowd (NCSRD):** iCrowd will be extended to provide passenger flow rates and evacuation times assuming different congestion levels, considering the possible fallout from misleading information delivered by compromised digital assets. The simulator will be integrated with BB3D and CaESAR to receive input regarding bomb explosions and alternative transit information respectively. Crowd behaviours will also be refined to follow an objective-oriented approach, where instead of programming specific behaviours, the user will specify the objectives of a simulated agent and its actions will be determined automatically.
- **RAM2(ELBIT):** Monitoring tool vendors workshop (together with Curix IC) to ensure data structure and data insights, integration of testing scenarios with each monitoring data sources and recorded scenarios data for scenario simulation from monitoring tools, with all relevant event types, from each data sources.

4.2.4 Location & Date

Event data: 22nd -25th of March.

Location of the event: a metro station in Ankara.

SE Location: To be discussed.

4.2.5 Simulation Exercise Organisation

Event preparation (2-3 weeks before): The simulation exercise team gathers to review once again the information available in this document (D8.2), identify minor missing points (if any) and align all members on their duties. EGO will prepare the necessary internal resources identified to hold the simulation, along with the key team members required to receive relevant feedback during the demonstration and extract useful and practical lessons learned for the third round of tests.

The organisation of the Simulation Exercise has been divided into 3 phases, according to the resilience stages described before: 1) PREVENTION, 2) DETECTION&RESPONSE, 3) RECOVERY. The first and third phases are planned in a Workshop format, while the second one is planned as a Functional Simulation Exercise. Definitions for each type of exercise are provided in **Annex II.** The evaluation will be coordinated by the Evaluation Manager who will establish when and how information retrieval (e.g. questionnaires) will occur. It is expected that end-users will be able to evaluate the S4RIS and the tools at the end of each phase, therefore avoiding interruptions every time a tool contributes to the scenario.

4.2.5.1 Prevention

This phase of the demonstration will be conducted during a **Workshop**, involving the EGO personnel operating in the Operational Centre. The workshop will not be specifically oriented to the Scenario described above (Combined Cyber-physical attack), it will be focused on a pre-event phase where EGO personnel analyses main weaknesses in the infrastructure and prepare proactive mitigations through S4RIS. In fact, the consortium will target the analysis of weak components (cyber and physical), vulnerabilities and risk scenarios, mitigation measures, and the overall resilience of the system. Different sessions will be planned according to the EGO department involved (Maintenance and Security). According to the script provided in section 4.2.1, the different activities planned for the S4RIS, and each tool are described below:

<u>Maintenance Department</u>

1. **<u>Central Assets Management System (CAMS)</u>**

The demonstration will be conducted during a workshop involving the EGO personnel operating in the Maintenance Department, and it will be focused on proactive planning based on information on the budget to allocate to repair/maintain/rehabilitate the infrastructure in normal condition and after unexpected hazard events.

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2).
- Activity 2 – EGO analyses the information and prepares CAMS

2. Simulation Analysis

- Activity 1 - Evaluation of input parameters for CAMS with EGO
- Activity 2 – Evaluation of results of CAMS with EGO:
    - Results of proactive planning including degradation of the critical assets under normal condition (ageing degradation) and under the simulated event; Cost to maintenance, repair, renew

3. Analysis of the results (supporting CAMS in prevention actions)

- Activity 1 – EGO visualises the results in the GUI
- Activity 2 – EGO analyses the results and selects alternative budgetary strategies to repair/maintain/rehabilitate after the event
- Activity 3 – EGO provides feedback to RMIT (suggesting new scenarios, conditions, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

Security Department

1. SecuRail

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2). For what concerns SecuRail, requested inputs could be collected in the following way:
    - STAM can provide EGO with a dedicated template (e.g., an Excel file) to collect required inputs and then STAM will enter them into SecuRail.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2 – Evaluation of SecuRail results with EGO:
    - Outputs of the risk assessment paying particular attention to the correlation between the input values and the values obtained as results.

3. Analysis of the results (supporting SecuRail in prevention actions)

- Activity 1 – EGO visualises the results in the GUI
- Activity 2 – EGO provides feedback to SecuRail (suggesting new functionalities, conditions, items to be considered during a risk assessment, etc.)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

2. TISAIL/OSINT

1. Simulation Analysis

- Activity 1 – Assessment of potential vulnerabilities

2. Analysis of the results

- Activity 1 – EGO visualises the vulnerabilities provided by TISAIL through RAM2 GUI
- Activity 2 – EGO adapts their security detection tools (e.g., IDS, SIEM) with some of the IoCs (Indicators of Compromise) of the threats provided by TISAIL
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to dat.

3. DATAFAN

DATAFAN will focus on the reliable prediction of passenger load on specific metro stations. The Operational Centre Supervisor asks the user to provide reliable numbers for the passenger load to work on a plan for the worst-case scenario, for example the closure of a station due to an unexpected event. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the past passenger load (see section 4.2.8.2).
- Activity 2 – FHG analyses the information and prepares DATA FAN for this specific prediction and data pre-processing.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2 – Evaluation of results of DATA FAN with EGO:
  - 1) Statistical evaluation of the data set
  - 2) Prediction of passenger load for specific selected stations for future time steps
  - 3) Reliability score for the results and explaining the results to enhance technology acceptance

3. Analysis of the results

- Activity 1 – FHG visualises the results in the GUI
- Activity 2 – EGO analyses the results and selects strategies for improving the prediction results
- Activity 3 – FHG improves the results with refined input parameters for the calculation
- Activity 4 – EGO provides new feedback to FHG
- Activity 5 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 6 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4. CAESAR

CAESAR tool will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. The Operational Centre Supervisor asks the user to implement mitigation measures to test which of them would work better on the infrastructure. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2).
- Activity 2 – FHG analysis the information and prepares CAESAR.
- Activity 3 – Integration of results from DATA FAN into CaESAR

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2 – Evaluation of results of CAESAR with EGO:
    - 1) resilience curves of performance over time throughout the adverse event (before, during and after),
    - 2) ranking of mitigation measures specific to threat
    - 3) list and ranking of critical components specific to threat, cascading effects analysis (in terms of critical components)

3. Analysis of the results (supporting CAESAR in prevention actions)

- Activity 1 – EGO visualises the results
- Activity 2 – EGO analyses the results and selects alternative mitigation measures (if necessary)
- Activity 3 – EGO provides feedback to FHG (suggesting new scenarios, conditions, cascading effects, mitigation measures, recovery times, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

5. iCrowd

iCrowd tool will focus on the simulation of infiltration/escape scenarios to better understand the chance of detection for different CCTV cameras and guard configurations. The Operational Centre Supervisor asks the user to test different configurations to assess potential vulnerabilities in the station. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2).
- Activity 2 – NCSRD analyses the information and prepares iCrowd

2. Simulation Analysis

- Activity 1 - Short presentation regarding the analysis of the input data and the scenarios that are going to be implemented to EGO
- Activity 2 – Execution of simulations and evaluation of initial results with EGO:
    - Visualize the result of a disruption or fallout of an attack, to provide a better point of view and lead to better safety measures and mitigation strategies
    - Use of final KPIs to evaluate and improve resilience/mitigation strategies
    - Observe the effect of real-time adjustments to the simulation, determine chain reactions, etc.

3. Analysis of the results (supporting iCrowd in prevention actions)

- Activity 1 – EGO analyses the results and selects alternative mitigation measures (if necessary)
- Activity 2 – EGO provides feedback to NCSRD (suggesting new scenarios, conditions, etc…)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

6. PRIGM (in accordance with Senstation)

PRIGM will focus on establishing a secure alternative channel (i.e., digital twin) between the important room and the OC. PRIGM is the master device, specifically a Hardware Security Module, which protects the cyber data even if an attacker infiltrates the cyber system (e.g., man-in-the-middle). PRIGM cordially operates with Senstation (sensor stations at nodes where the sensory data is generated) and these two established point-to-point securities. Symmetric encryption will be applied to protect the data generated by the sensors or actuators mounted on Senstation. By doing so, if an attacker tries to i.e., sniff or manipulate the data channel, the critical information cannot be revealed, and the integrity checking can be realised to improve resilience. Such a point-to-point security tactic can be used for preventing many cyber and even cyber-physical attacks. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the fire alarm system and related sensor data, important room entry procedures and the electronic equipment like door switches, etc., topology information about any sensor system to protect the network infrastructure and the cyber-security protocols like authentication and authorisation policy.
- Activity 2 – ERARGE analyses the network infrastructure and the devices. This analysis will then be used to create a digital twin of the targeted system for further security assessment.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analyses of the input data to EGO
- Activity 2- Set-up the digital twin of the data channel with selected sensors mounted on the Senstation at client side (nodes). Then, set up PRIGM at server side (from ERARGE) to couple the Senstation and create the secure alternative data channel.
- Activity 3 – Compare the original channel and secure digital channel by observing how PRIGM and Senstation protect the channel against selected cyber-attacks.

3. Analysis of the results

- Activity 1 – ERARGE showcases and report the results by showing the countermeasures based on the digital twin of the system (prepared at laboratory scale)
- Activity 2 – EGO analyses the results and selects strategies for improving the resilience
- Activity 3 – ERARGE improves the results and share adaptation/extrapolation strategies with EGO for further studies
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

7. **RAM2**

RAM2 processes cyber physical assets information and events, received from S4RIS monitoring tools, for identification of vulnerabilities and provides risk assessments within the operations context.

1. Simulation Information Analysis

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.2.8.2). RAM2 requires information about the operational hierarchy of EGO, process and asset criticality information, details of cyber physical assets.

2. Simulation Analysis

- Activity 1 - Evaluation of input parameters for RAM2 with EGO
- Activity 2 - Vulnerability assessment by RAM2.

3. Analysis of the results (supporting RAM2 in prevention actions)

- Activity 1 – EGO visualises the results in the GUI and using the system reports.
- Activity 2 – EGO provides feedback to RAM2
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4.2.5.2 Detection & Response

The detection and response phases will be carried out in the same step of the exercise due to the fact they are both closely connected and happen simultaneously during an ongoing crisis. In fact, the format of this step of the exercise will be as a **"Functional Simulation Exercise"**, where activities will be driven by the scenario described in section 4.2.1 and will engage the relevant team members of EGO. The Functional Simulation Exercise will be focused on how security operators interact with the S4RIS and the value-added by each individual tool. Therefore, the focus will be on the **alerts raised by the system** – and the usefulness of the details provided by the alerts, and the **mitigation recommendations** provided to the end-user. User interfaces from the individual tools will be presented when appropriate.

Before visualising the performance and contribution of each tool to the S4RIS, each Tool Leader will have the opportunity of performing a brief introduction (1-2min) regarding: 1) User input data, 2) User benefits (value-added to end-user) and 3) Results offered to end-user. In the following lines, the role of each tool leader and the main related activities are described:

1. **TISAIL**

1. Simulation Analysis

- Activity 1 – Assessment of potential threats

2. Analysis of the results

- Activity 1 – EGO visualises the threats provided by TISAIL through RAM2

- Activity 2 – EGO adapt their security detection tools (e.g., IDS, SIEM) with some of the IoCs (Indicators of Compromise) of the threats provided by TISAIL
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

2. CURIX

CuriX demonstration will be focused on: Analysing monitoring data of technical systems towards anomalous behaviour, which could indicate upcoming threats, together with information regarding health of system, or metrics and devices causing change in system behaviour by operational and functional testing of CuriX for the detection stage.

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2).
- Activity 2 – IC analyses the information and prepares CuriX and data

2. Simulation Analysis

- Activity 1 – Present a short report regarding the analysis of the input data to EGO
- Activity 2 – Tool leader performs simulation
- Activity 3 – If appropriate, IC will present the CuriX GUI so that EGO visualises the results
- Activity 4 – Evaluation of results of CuriX with EGO:
    - 1) Number of past and alerts on current detected anomalies in the monitoring data of technical system
    - 2) List and ranking of metrics or devices causing major changes in behaviour of technical systems
    - 3) List and health scores of metrics or devices of technical systems
    - 4) Information presented in dashboard

3. Analysis of the results (supporting CuriX in detection actions)

- Activity 1 – EGO provides feedback to IC (e.g., appropriateness of alerts and results related to content and timing)
- Activity 2 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 3 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

3. DATAFAN

DATA FAN will be focused on the prediction of reliable passenger load on specific metro stations and detection of the capacities that are sufficient or must be improved. The Operational Centre Supervisor asks the user to provide reliable numbers for the passenger load to work on an improved plan with modified capacities in extreme situations, e.g., after a football game. The organisation process is divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the past passenger load (see section 4.2.8.2).
- Activity 2 – FHG analysis the information and prepares DATA FAN for this specific prediction and data pre-processing

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2 – If appropriate, FHG will present the DATAFAN GUI so that EGO visualises the results
- Activity 3 – Evaluation of results of DATA FAN with EGO:
    - 1) Statistical evaluation of the data set
    - 2) prediction of passenger load for specific selected stations for future time steps
    - 3) Information of the used algorithm and the results (“Opening the black box”)
    - 4) Reliability score for the results and explaining the results to trust

3. Analysis of the results

- Activity 1 – EGO analyses the results and selects strategies for improving the prediction results
- Activity 2 – FHG improves the results with refined input parameters for the calculation
- Activity 3 – EGO provides new feedback to FHG
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4. Ganimede

Ganimede will be focused on the detection of objects and people in each frame and their movement to determine if the object is candidate for being abandoned.

1. Simulation Preparation (before the SE)

- Activity 1 – EGO will record a video using CCTV cameras in a predefined area where a person (as an actor) will abandon a baggage
- Activity 2 – EGO will provide the video stream to LDO to be analysed by Ganimede tool

2. Simulation Analysis

- Activity 1 – Ganimede analyses the provided video and will detect the event of interest (abandoned baggage)
- Activity 2 – Ganimede raises the alarm

3. Simulation Output

- Activity 1 – Ganimede sends alarm data to RAM2 that will display the alarm.

4. Analysis of the results

- Activity 1 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 2 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

5. PRIGM-Senstation

PRIGM is the master device, a Hardware Security Module, which orchestrates the cryptographic functions, key and secret generation and data hashing. Senstation is an IoT device, a secure gateway that is installed at end nodes where sensory data is collected. Senstation has analogue and digital interfaces and can host many sensors enabling instant data monitoring at fields. Since Senstation is the device closest to the nodes, the observed data can be used for assisting the detection and response activities. The digital twin approach mentioned in Section 4.2.5.1 (see the description of and activities about PRIGM) will be used in this use case. The data collected by Senstation and secured by applying the point-to-point security scheme provided cordially by PRIGM and Senstation (client-server or node-central architecture) will be used for anomaly detection. The underlying statistical data analysis technique relies on bootstrapping which outputs the confidence intervals of the observed sensor data. If any observed data at time "t" is out of the confidence interval for a predefined duration, this may indicate that there is an anomaly. The secure alternative channel will help us to create such anomaly cases and show how these can be detected and monitored.

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the fire alarm system and related sensor data, important room entry procedures and the electronic equipment like door switches, etc.
- Activity 2 – ERARGE analyses the sensory information and extract confidence intervals by applying statistical analysis methods (bootstrapping).
- Activity 3 – ERARGE analyses the network infrastructure and the devices. This analysis will then be used to create a digital twin of the targeted system for further security assessment.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2- Set-up the digital twin of the data channel with selected sensors mounted on the Senstation at client side (nodes). Then, set up PRIGM at server side (from ERARGE) to couple the Sentation and create the secure alternative data channel.
- Activity 3 – Compare the original channel and secure digital channel by observing how PRIGM and Senstation protect the channel against selected cyber-attacks.
- Activity 4 – Present the confidence intervals and synthetically created anomalies and regarding alerts in response phase. By doing so one can see how the proposed statistical analysis technique can be used of detection and response

3. Analysis of the results

- Activity 1 – ERARGE visualises and report the results by showing the countermeasures based on the digital twin of the system (prepared at laboratory scale)
- Activity 2 – EGO analyses the results and selects strategies for improving the resilience
- Activity 3 – ERARGE improves the results and share adaptation/extrapolation strategies with EGO for further studies
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

6. iCrowd

iCrowd tool will focus on the simulation of the consequences of the incident on the passengers leveraging the information regarding passenger flow. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2).
- Activity 2 – NCSRD analyses the information and prepares iCrowd

2. Simulation Analysis

- Activity 1 - Short presentation regarding the analysis of the input data and the scenarios that are going to be implemented to EGO
- Activity 2 – Execution of simulations and evaluation of initial results with EGO:
  - Visualize the result of a disruption or fallout of an attack, to provide a better point of view and lead to better safety measures and mitigation strategies
  - Use of final KPIs to evaluate and improve resilience/mitigation strategies
  - Observe the effect of real-time adjustments to the simulation, determine chain reactions, etc.

3. Analysis of the results (supporting iCrowd in prevention actions)

- Activity 1 – EGO analyses the results and selects alternative mitigation measures (if necessary)
- Activity 2 – EGO provides feedback to NCSRD (suggesting new scenarios, conditions, etc…)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

7. SecuRail

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2). For what concerns SecuRail, requested inputs could be collected in the following way:
  - STAM can provide EGO with a dedicated template (e.g., an Excel file) to collect required inputs and then STAM will enter them into SecuRail.

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2 – Evaluation of SecuRail results with EGO:
  - Outputs of the risk assessment paying particular attention to the correlation between the input values and the values obtained as results.

3. Analysis of the results (supporting SecuRail in prevention actions)

- Activity 1 – EGO visualises the results in the GUI
- Activity 2 – EGO provides feedback to SecuRail (suggesting new functionalities, conditions, items to be considered during a risk assessment, etc.)
- Activity 3 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 4 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

8. CAESAR

CAESAR tool will focus on the analysis of weak components, mitigation measures, and the overall resilience of the system. The Security Coordinator asks the user to implement mitigation measures to test which of them would work better on the infrastructure. The organisation process in divided in 3 phases:

1. Simulation Information Analysis (before the SE)

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2)

- Activity 2 – FHG analysis the information and prepares CAESAR
- Activity 3 – Integration of results from DATA FAN into CAESAR

2. Simulation Analysis

- Activity 1 - Present a short report regarding the analysis of the input data to EGO
- Activity 2 – Evaluation of results of CAESAR with EGO:
    - 1) resilience curves of performance over time throughout the adverse event (before, during and after),
    - 2) ranking of mitigation measures specific to threat
    - 3) list and ranking of critical components specific to threat, cascading effects analysis (in terms of critical components)

3. Analysis of the results (supporting CAESAR in prevention actions)

- Activity 1 – EGO visualises the results
- Activity 2 – EGO analyses the results and selects alternative mitigation measures (if necessary)
- Activity 3 – EGO provides feedback to FHG (suggesting new scenarios, conditions, cascading effects, mitigation measures, recovery times, etc.
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

9. RAM2

RAM2 demonstration will be focused on orchestration of data from multiple sources, generation of alerts and correlated insights and contextualization of the information in accordance with the operational structures of EGO.

1. Simulation Information Analysis (before the SE)

- Activity 1 – MDM provides indicative data regarding the simulation (see section 4.2.8.2)
- Activity 2 – RAM2 analyses the information and prepares RAM2 and data.

2. Simulation Analysis

- Activity 1 – RAM2 processes data from available systems in the simulation
- Activity 2 – Tool leader performs simulation
- Activity 3 – ELBIT presents the RAM2 GUI and reports to EGO
- Activity 4 – Evaluation of results of RAM2 with EGO

3. Analysis of the results (supporting RAM2 in detection actions)

- Activity 1 – EGO provides feedback to ELBIT
- Activity 2 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 3 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4.2.5.3 Recovery

This phase of the demonstration will be performed in a similar manner to the Prevention phase – through a **Workshop**. However, the workshop will be specifically targeting the recovery after the events happened in the Scenario and outcomes from the “Detection & Response” phase. Therefore, it will be a post-event evaluation to help the EGO experts to recover the infrastructure and support business continuity. Two sessions will be planned according to the EGO department involved (Maintenance). According to the script provided in section 4.2.1, the different activities planned for the S4RIS, and each tool are described below:

1. **Central Assets Management System (CAMS)**

The demonstration will be conducted during a workshop involving the EGO personnel operating in the Asset Management Department, and it will be focused on: 1) Optimal resource deployment during response thanks to information relate to time and cost needed to respond a crisis and restore normal functioning, 2) Optimal resource deployment and financial loss control during recovery based on information related to time, cost and performance loss.

1. Simulation Information Analysis

- Activity 1 – EGO provides indicative data regarding the simulation (see section 4.2.8.2)
- Activity 2 – RMIT analysis the information and prepares CAMS

2. Simulation Analysis

- Activity 1 - Evaluation of input parameters for CAMS with EGO.
- Activity 2 – Evaluation of results of CAMS with EGO:
  - Result in terms of structure resilience: performance loss assessment, cost, and time for recovery service
  - Results of optimal resource deployment to recover after the crisis including degradation of the critical assets under normal condition and under the simulated event; Cost to maintenance, repair, renew

3. Analysis of the results (supporting CAMS in recovery actions)

- Activity 1 – EGO visualises the results in the GUI
- Activity 2 – EGO analyses the results and selects alternative budgetary strategies to respond to the crisis
- Activity 3 – EGO provides feedback to RMIT (suggesting new scenarios, conditions, etc.)
- Activity 4 - An assessment/opinion on how far the requirements/specifications tested were met
- Activity 5 - Any proposals for revisions and/or additions to the requirements and specifications defined to date

4.2.6 Equipment/Supplies

The following table provides an overview of the technical equipment and supplies required by each tool provider during the simulation:

TABLE 4 EGO SIMULATION EXERCISE – EQUIPMENT AND SUPPLIES REQUIRED BY EACH TOOL LEADER

TOOL PROVIDER NAME	EQUIPMENT/SUPPLIES	NOTES
FRAUNHOFER (CaESAR)	PCs, laptop, ethernet connection	

FRAUNHOFER (DATAFAN)	Laptop (will be brought by us), second screen and ethernet connection are expected to be provided	
Leonardo	PC and server in laboratory	
IC	Laptop provided by IC, power supply and WiFi connection must be provided on site	
ERARGE (PRIGM)	A server PC on which the PRIGM is installed	To be supplied by ERARGE and presented in the workshop
STAM	PCs, laptop, ethernet connection, etc…	
ERARGE (Senstation)	The sensors will be mounted on the Senstation to show how the system gathers the data from the important room (as the digital twin of the real system)	To be supplied by ERARGE and presented in the workshop
TREE/INNO	Laptop, ethernet connection	Internet connection required
RMIT	PCs, laptop, ethernet connection	There is a chance that someone will be connected in remote from Australia to ease simulation run
NCSRD	PC, stable internet connection (for remote execution)	
ELBIT	Linux server, desktop / laptop PC, ethernet connection to Kafka, internet connection …	Server installation according to RAM2 installation manual

4.2.7 Applicable Legislation/Regulation

For the performance of the S4RIS, personal data within CCTV video footage will be stored and processed (Ganimede), as well as personal data from social media posts (TISAIL/OSINT). Personal data will be also collected for the purpose of the evaluation of the simulation. In general terms, to comply with ethical and privacy legislation, deliverables **D9.1: SAFETY4RAILS Ethical Compliance Framework (ECF)**, **D11.1: H – Requirement No.1** (Informed Consent and Procedures) and **D11.3: POPD – Requirement No. 3** (Personal data processing) will be used as reference. The following legal, ethical and policy requirements will be also complied:

- Respect to right of access, rectification and opposition.
- The Data Controller (DC) determines the purpose and manner in which any personal data are, or are to be processed, kept and destroyed.
- Ensure the protection of privacy.

- Comply with recognized ethics.
- Not to show and disseminate internal information provided by end-users.
- Protect the rights and physical integrity of security personnel and other stakeholders.
- Project and its outcomes will attempt to protect the rights and physical integrity of people.

Ethical/privacy-related and legal requirements. The following legislation will be addressed:

- Charter of Fundamental Rights of the European Union (200/C 364/01).
- Directive 2006/54/EC on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast).
- General Data Protection Regulation (EU) 2016/679 (GDPR).
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications);
- Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.
- Turkey's legislation, namely KVKK (Personal Data Protection Rule, nr. 6698) is fully compliant with GDPR

4.2.8 Performance Expectations

The performance expectations of the SAFETY4RAILS Information System (S4RIS), and the each of the contributing tools, for this simulation exercise were detailed in deliverable **D8.1: Evaluation Methodology**. This deliverable was based on technical specifications elicited in the deliverable D1.4, which answered a wide set of the end-user requirements collected in WP2. Furthermore, D8.1 has been prepared in parallel with the present document (D8.2) and takes into consideration the scenario description and organisation. As a result, the simulation success criteria were formulated based on objectives at 3 levels:

1) Usability of the S4RIS platform
2) Specific requirements of the S4RIS platform
3) Scenario-based requirements/objectives

More information can be found in the aforementioned report.

4.2.8.1 Execution

In this section, a detailed description of the **interaction between each Tool Leader and the Host** (EGO) during the simulation exercise is provided. The goal is to have a clear understanding of how the end-user and the tool leader will interact to optimise the time used and avoid confusions during the exercise. This will further enhance end-users' interpretation of the tools (and related outcomes) and therefore the lessons learned.

Furthermore, in a real scenario some tools may run or provide insights simultaneously, especially during DETECTION and RESPONSE activities. To provide a clear operational picture for the end-users, the tools will be executed in a sequence. The execution sequence for each resilience stage was described in Section 4.2.1.

CAESAR:

1. FHG explains the functionalities briefly and how EGO should interact with the tool, starting with input parameters.
2. EGO reviews and provides information to select/improve input parameters (only exemplary, for a few examples)
3. FHG user updates input parameters if necessary

4. EGO receives results about the overall resilience of the system and indicates mitigation measures
5. FHG user receives feedback and implement mitigations. Results are reported back to EGO for feedback and to the relevant tools (e.g., RAM2).
6. EGO evaluates the tool. A questionnaire is filled out at the end.

CAMS:

1. RMIT explains the functionalities briefly and how EGO should interact with the tool, starting with input parameters
2. EGO reviews and provides information to select/improve input parameters if needed and then inputs parameters
3. EGO receives info about an investment plan (cost for intervention and repair)
4. EGO reviews with RMIT the output obtain.
5. RMIT asks feedback for eventual improvement of functionalities and interface. A questionnaire is filled out at the end.

DATA FAN:

1. FHG explains the functionalities briefly and how EGO should interact with the tool, starting with input parameters.
2. EGO receives results about the number of passengers for future time steps
3. FHG answers questions to the user regarding the results if any
4. EGO evaluates results and requests better results if needed
5. FHG will improve the results if deemed appropriate in step 4.
6. EGO tests and evaluates the tool. A questionnaire is filled out at the end.

RAM2:

1. Elbit explain the functionalities and how EGO should interact with the tool.
2. EGO reviews and provides input parameters.
3. Elbit updates the information in the system together with EGO.
4. End-user consumes the data through RAM2 Dashboard display.
5. The end-user follows the prioritized alerts and mitigation steps for each of the alerts for risk reduction and responses to detection of ongoing threats.

CURIX

1. IC briefly explains the functionalities and how EGO should interact with the tool.
2. IC performs simulation.
3. EGO receives results in terms of anomalies of the behaviour of technical systems, ranking causing major changes in the behaviour of technical systems, health scores of metrics and devices. Alerts will be manually dispatched by an IC member to avoid configuring mailing connections.
4. EGO tests and evaluates the tool and its results. A questionnaire is filled out at the end.

SECURAIL

1. STAM explains the functionalities of SecuRail and how EGO should interact with the tool, starting with the entering of the required inputs.
2. EGO reviews and provides information to select/improve input parameters (only exemplary, for a few examples)
3. STAM updates input parameters if necessary.
4. EGO visualize results of the risk analysis and indicates potential security measures that could be implemented within the network infrastructure to mitigate risks.
5. STAM receives the feedback and implement the suggested countermeasures. Results are reported back to EGO for feedback.
6. EGO tests and evaluates the tool through a questionnaire prepared by the consortium.

TISAIL/OSINT

1. TREE/INNO explains the different threats that can be relevant for EGO.
2. EGO reviews the threat alerts for situational awareness
3. EGO uses some of the information provided to update their mitigation measures (e.g., IDS, SIEMs, etc)
4. EGO tests and evaluates the alerts provided.
5. TREE/INNO receives feedback about the quality and interest of the alerts. TREE/INNO will consider the feedback for future interactions.

iCrowd

1. NCSRD explains the existing and possible functionalities and KPIs of iCrowd related to the EGO simulation exercise (to be done before the SE)
2. EGO explains the incidents and the resilience/mitigation strategies they would like to study using iCrowd (to be done before the SE)
3. NCSRD designs and presents the simulation scenarios that are going to be developed (to be done before the SE)
4. EGO reviews the scenarios and adjusts if necessary (to be done before the SE)
5. NCSRD implements the scenarios and showcases them, along with the inputs that EGO is required to provide.
6. EGO provides a set of configurations (input parameters).
7. NCSRD executes the available configurations, extracts the results, and shows them to EGO.
8. EGO reviews the results and extracts conclusions.
9. If more configurations are required, EGO sends new configurations to NCSRD and steps 7 and 8 are repeated. Repeat until enough results are gathered.
10. EGO evaluates the overall functionality of iCrowd and provides feedback regarding its functionality and what else they would like to achieve.

Ganimede

1. LDO provides information to EGO about video format expected (before de SE)
2. EGO will send the video at least 2 weeks before the date of the exercise
3. LDO will record in a video the activities made by Ganimede to detect the abandoned baggage (before the SE)

4. LDO will explain to EGO the interaction with Ganimede (during the SE)

PRIGM

1. ERARGE will explain the PRIGM functionalities, and how it is integrated with PRIGM for prevention, detection, and response activities within the use-case context (to be done before the SE)
2. EGO will share the list of critical assets in their infrastructure, and possible attack surfaces (to be done before the SE)
3. ERARGE will work on the vulnerability analysis, relying on desktop studies (to be done before the SE)
4. EGO will examine the vulnerability analysis report, including potential countermeasures, and will provide feedback (to be done before the SE)
5. Countermeasures will be reported in relation with the capabilities of PRIGM (before the SE)
6. ERARGE will establish a secure alternative data channel (digital twin) in corporation with Senstation (PRIGM at server side, and Senstation at client/node side)
7. Security assessments and vulnerability analyses will be revised for preventive actions and countermeasures.
8. Inputs from other tool provider to protect the EGO network or improve the resilience can be incorporated by joint discussions

Senstation

1. ERARGE will explain the Senstation functionalities, and how it complements PRIGM in prevention, detection, and response activities within the use-case context (to be done before the SE)
2. EGO will share sample sensory data for certain period (from important room) (to be done before the SE)
3. ERARGE will apply statistical analysis to extract confidence intervals within the real data (to be done before the SE)
4. ERARGE will establish a secure alternative data channel (digital twin) in corporation with PRIGM (PRIGM at server side, and Senstation at client/node side)
5. ERARGE will apply selected cyber-attacks to manipulate the observed sensory data and demonstrate the alerting cases
6. ERARGE will report the results
7. EGO will evaluate results and feedback

4.2.8.2 Data acquisition

Before the simulation, each tool provider will collect the necessary data enabling the functionalities offered to the end-user during the exercise. For specially challenging and sensitive data types described below, realistic data generated synthetically will be utilised. During the simulation, data relevant to the configuration of the tool, feedback and indications from the end-users will be used. During and after the simulation, information regarding the evaluation (reflected in D8.1, including the data acquisition methodology) will be also collected.

The data required from the end-user for setting up the tools before the simulation is described below:

TABLE 5 EGO SIMULATION EXERCISE – DATA REQUIRED FROM END-USER

TOOL NAME	DATA INPUTS REQUIRED FROM END-USER
CAESAR	System components (physical and cyber), system component attributes, system connections (internally and to external networks), system functions, dependencies between system functions, dependencies and influences of system components, threat impact to components and functions, prevention, response and recovery strategies, mitigation measures currently in use and to be tested
CAMS	At least two consecutive regular data inspections on assets; Time and cost spent in maintenance, repair, renewal. Capital value of the elements; Cost of asset maintenance under normal degradation; time allocated for maintenance of the element; Cost of asset repair under normal degradation and hazard event. Cost and time of asset rehabilitation under normal degradation and/or hazard event
TISAIL/OSINT	This includes representative examples of all levels of devices that may be susceptible to attacks or threats via technical means (e.g., station control systems, transformer equipment, CCTV cameras, networking infrastructure, information displays and display content management, station control systems, office PCs, etc).
Ganimede	Stream video showing a baggage that has been abandoned
DATA FAN	Number of passengers for each station/ train
iCrowd	3D Model of the environment Locations of cameras, guards (and their movement patterns) (these will be adjustable, only need something as baseline) Expected congestion (will be adjustable, need a range of values) Estimated time required to break into the important rooms Changes in the infrastructure because of the important room breach (deactivated elevators, escalators, blocked turnstiles, etc.)

CuriX	Fine-granular time-wise passenger flow data of stations (number of passengers arriving/leaving stations or even on platforms). Power consumption data in the station, considering data without anomalies for at least 2 weeks time. Static data of stations connected to passenger flows (potentially covered by SecuRail topology)
SecuRail	Network information (typology, number of stations, number of sections). Expected crowding level for each station. List of assets prevent in each area of the analysed stations. List of countermeasures equipped in each area of the analysed stations. Economic value of each asset. Economic value of each area. Information related toto each section. Default Value of Statistical Life
RAM2	Operational hierarchy and assets information including details of cyber physical assets.
Senstation	Temperature, accelerometer, light, door switch
PRIGM	Historical log data (authentication, encryption decryption, connected devices, authenticated persons or nodes access data, etc) stored during the actual use of the HSM.

Data collection process for all the data types described in the table above is ongoing and will be finalised within a reasonable timeframe before the simulation to make the S4RIS ready for the exercise.

5. Conclusion

5.1 Summary

This document has established the 1st and 2nd Simulation Exercises (SE) for the SAFETY4RAILS project. An iterative methodology has been used to know interests, wishes and expectations of the end-users (metro and railway operators) and tool providers. The methodology was divided into the following phases:

1) Analysis and refinement of the Use-Cases proposed in previous stages of the project (Deliverable 2.5).
2) Online workshop on the 13th of October 2021 for the definition of the MDM Simulation Exercise, to collect thoughts and ideas between project partners (MDM and all tool providers involved).
3) Online workshop on the 18th of November 2021 for the definition of the EGO Simulation Exercise, following the same methodology as for the MDM one.
4) Based on the previous steps, creation of narrative scenarios for both MDM and EGO SE. These included the context of the threat event, actors involved, timeline of the event, the tools to be tested and activities to be carried out. A first draft was proposed to partners, where all could easily modify and agree on the assigned roles.

This document has also provided a handbook for supporting each Simulation Exercise Team to conduct SE. Ethics should be present in all SE processes and appropriate guidelines have been provided based on available documents prepared in previous phases of the project.

5.2 Future work

While the deliverable provided detailed guidelines on how to implement the first and second SEs, the consortium will continue to refine the SE scripts and organisational frameworks to optimise the S4RIS demonstration with the end-users, and therefore, the lessons learnt to be reported in deliverables D8.4 and D8.5. In fact, it is foreseen that the 2nd SE (EGO) will implement some of the lessons learnt in the 1st one (MDM) from a technical and organisational perspective, as depicted in D8.1: Evaluation Methodology. In this sense, the project will follow an AGILE methodology where the results of the first exercises will be fed into the technical development cycle and refine the SE organisation. Such improvements will be formalised in D8.3: Final version of development of a blueprint exercise handbook, together with the detailed guidelines of the 3rd and 4th SEs.

As depicted in Section 2, SAFETY4RAILS tools are distributed across different Use-Cases. Since scenarios are based on Use-Cases, there will be some tools that are not reflected in the first and second SE, but they will be demonstrated in the third and fourth SE – based on other Use-Cases.

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 6 GLOSSARY AND ACRONYMS

Term	Definition/description
AB	Advisory Board
AS	Active Staff
CCTV	Closed-circuit television
CDM	Comune di Milano
CO	Confidential
C2	Command-and-Control Center
D	Deliverable
DC	Data controller
DM	Dissemination Manager
DoA	Description of the Action (Annex 1 to the Grant Agreement)
EC	European Commission
EGO	Elektrik-Gaz-Otobüs
EM	Evaluation Manager
ENISA	European Union Agency for Cybersecurity
GUI	Graphical User Interface
H	Host
IDS	Intrusion Detection System

IED	Improvised Explosive Device
IoCs	Input Output Control Systems
KPIs	Key Performance Indicators
LEA	Law Enforcement Agency
MDM	Metro de Madrid
MISP	Malware Information Sharing Platform
O	Observers
OC	Operating Center
RFI	Rete Ferroviaria Italiana
S4RIS	SAFETY4RAILS Information System
SE	Simulation Exercise
SIEMs	Security information and event management
TRL	Technology Readiness Level
UC	Use-Case
WP	Work-Package
WS	Workshop

ANNEX II. Type of exercise

Type of exercise		Description
WS	Workshop	Qualitative and structured exercises based on discussion within a group of experts. They aim at familiarizing experts with the specific outcomes that need to be tested in order to use them within exercise sessions. Workshops could be scenario driven (hypothetical or real) and allow gathering suggestions and feedback for the outcomes improvements from an expert perspective. A facilitator guides participants through the discussion.
FXSE	Functional Simulation Exercise	Highly specific exercises, close as possible to the reality. Lengthy exercises, which take place on location using, as much as possible, the equipment and personnel that would be called upon in a real event.
TTX	Table-Top Exercise	Discussion-based sessions within a group of stakeholders. In a classroom setting, stakeholders simulate and discuss their roles, responsibilities and actions by referring to a specific emergency scenario (hypothetical or real). A facilitator guides participants through the session. They are cost-effective tools to validate procedures, plans and capabilities.

ANNEX III. Use-Cases Definition Template

Tool provider	Tool	Resilience stage	Description of the capability/functionality provided for each resilience stage (easy to understand for end-user)	Data Inputs required from the end-user	Data Inputs required from other tools	Data outputs provided to the end-user	Data outputs provided to other tools
Partner Name	*Name of the tool*	*Select the relevant resilience stage: Prevention, Detection, Response and/or Recovery*	*High-level description of the capability/functionality your tool will provide to address each resilience stage selected before, for the indicated Use-Case. The structure should be as a user-story: As a [type of end-user], I want [a goal] so that [some reason]. e.g.: A Crisis Manager, must I want to be informed about security warnings, so that I can alert First Responders if necessary*	*List WHAT data will need to be requested/consumed from the end-user during the simulation exercise*	*List WHAT data will need to be requested/consumed from other partners during the simulation exercise*	*List WHAT data that will need to be provided/injected to the end-user during the simulation exercise*	*List WHAT data that will need to be provided/injected to the other tools during the simulation exercise*

ANNEX IV. Simulation Exercises Workshop Templates

Work Package 8: Simulation Exercises and Evaluations in Operational Environments

Scenario Template – Tool name

XX YY 2021

Organisation Name

The project leading to this application has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883532.

Capabilities/Functionalities provided to each resilience stage

PREVENTION	DETECTION	RESPONSE	RECOVERY

Proposed validation means

- ❑ Validation method for each functionality for each resilience stage
  - ❑ Please explain in detail the method/s you would use for validation (operational/functional testing, workshop, table-top exercise, etc…). Provide an outline of the activities that will be carried out with the end-user during the validation (analysis of input parameters, evaluation of results…). Explain whenever the tool is expected to be evaluated as standalone or through the S4RIS platform.
  - ❑ the same method could be apply to prevention, detection, mitigation and response).

Role expected by end-user

- ❑ Describe what the tool leader and the end-user should do during the simulation (e.g.: 1- Tool leader explains functionalities and provide input parameters, 2 – End-users reviews and provides information to fine-tune input parameters, 3- Tool leader performs simulation, 4- End-users evaluates results).
- ❑ Describe the main outcome expected (what is your tool expected to demonstrate?)

Data inputs from end-users

- ❑ List WHAT data is needed from end-users for preparing the simulation
  - ❑ Explain whether you already have it or is still missing

Data inputs/outputs from other tools

- List WHAT data is needed from other tools and what data will need to be provided to other tools, for preparing the simulation or during the simulation (if any)
  - Explain any major issues in this regard

INPUT DATA	OUTPUT DATA
TOOL NAME – DATA X, Y, Z	TOOL NAME – DATA X, Y, Z
TOOL NAME – DATA X, Y, Z	TOOL NAME – DATA X, Y, Z
TOOL NAME – DATA X, Y, Z	TOOL NAME – DATA X, Y, Z

Limitations identified up to date

❑ Explain main obstacles (if any) that would hinder the performance of your tool during the simulation

Work Package 8: Simulation Exercises and Evaluations in Operational Environments

Scenario Template – Tool name

XX YY 2021

Organisation Name

The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883532.

SAFETY4RAILS

Partners:

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