SAFETY4RAILS

EXPLOITATION STRATEGY

Deliverable 10.9

Lead Author: EOS

Contributors: ETRA

CURIX, CS, ELBIT, ERARGE, INNO, ICOM, LDO, MTRS, RINA, STAM, TREE, WINGS, RMIT, Fraunhofer, NCSRD, UNEW, UREAD

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.

D10.9 EXPLOITATION STRATEGY		
Deliverable number:	D10.9	
Version:	1.1	
Delivery date:	13/01/2023	
Dissemination level:	Public	
Nature:	Report	
Main author(s)	Juliette Vieillevigne Angeliki Tsanta Elodie Reuge	EOS
Contributor(s)	Eduardo Villamor Medina	ETRA CURIX, CS, ELBIT, ERARGE, INNO, ICOM, LDO, MTRS, RINA, STAM, TREE, WINGS, RMIT, Fraunhofer, NCSRD, UNEW, UREAD
Internal reviewer(s)	Stephen Crabbe – Project Coordinator Antonio De Santiago Laporte – Security Assessment	Fraunhofer MdM
External reviewer(s)	Grigore Havarneanu	UIC not directly involved in this project work.

Document control			
Version	Date	Author(s)	Change(s)
0.1	29/09/2021	Elodie Reuge Juliette Vieillevigne	ToC release
0.2	11/05/2022	Elodie Reuge Juliette Vieillevigne	Section 3
0.3	19/07/2022	Angeliki Tsanta Juliette Vieillevigne	Section 3 updated with partner contributions and ETRA feedback.
0.4	24/08/2022	Angeliki Tsanta Juliette Vieillevigne	Section 4
0.5	13/09/2022	Angeliki Tsanta Juliette Vieillevigne	Sections 1, 2 and 5; Executive Summary and Annexes
0.6	18/09/2022	Eduardo Villamor Medina	ETRA input included in Section 3 and Annex VIII.
0.7	22/09/2022	Angeliki Tsanta Juliette Vieillevigne	Revisions made on Section 3.5 and 4 based on PC and ETRA feedback.
0.8	07/10/2022	Angeliki Tsanta Juliette Vieillevigne	Revisions made based on partial implementation of internal and external reviews.
1.0	11/10/2022	Stephen Crabbe	Creation of V1.0 from V0.8. Update of this table, very minor editing and formatting.
1.1	13/01/2023	Angeliki Tsanta Juliette Vieillevigne Atta Badii	Revised section 4.2 based on EC feedback. Typos in executive summary corrected (end of paragraph 3). Inclusion of UREAD identified required updates: Addition of UREAD to front cover and above table. Table 1 - Update of “INNO” and “UREAD” rows. Table 2 – Update of foreground Nr.4, 5 and 9 rows; introduction of new (UREAD) foreground Nr. 10 and 11 rows (Nr. 10 based on earlier Foreground Nr.33 row); renumbering of earlier foreground rows i.e. earlier row 10 becomes row 12 etc; update of foreground Nr. 16 and 21 (earlier Nr.

		14 and 19); deletion of earlier foreground Nr. 33 (covered now by Nr.10). Correction section 3.4.1.5 and PRIGM “high-throughout” to “high through-put”. Update under section 3.4.1.6 and SAFETY4RAILS Crisis communication and information sharing guidelines in first paragraph to reflect Table 2. Phrasing updates under sections 3.4.1.7 (paragraphs 1, 3 and 6 and 3.4.2.1 (paragraph 4). Section 3.4.4 addition of second sentence. Table 5 – Addition of UREAD.
	Stephen Crabbe	Update and completion of this table and footers, correction of numbering in Table 2, correction of minimal “typos” and formatting.

DISCLAIMER AND COPYRIGHT

ABOUT SAFETY4RAILS

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

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

TABLE OF CONTENT

List of tables

List of figures

Executive summary

The SAFETY4RAILS project aims to deliver methods and systems to increase the security and resilience of track-based inter-city railway and intra-city metro transportation from cyber, physical as well as combined cyber-physical attacks.

This deliverable, D10.9, presents the exploitation strategy of the SAFETY4RAILS project. This strategy is built around the individual partner exploitation plans and the joint exploitation strategy for the SAFETY4RAILS Information System (S4RIS) platform solution.

This document begins by mapping out the background intellectual property (IP) owned and brought into the project by partners, as well as the foreground IP developed during SAFETY4RAILS. It then presents up-to-date and extensive individual partner exploitation plans, including estimated timelines for the full maturity of all project results. An initial exploitation plan for S4RIS including a proposed strategy for its commercialisiation using the Pre-Commercial Procurement mechanism, is also outlined to target that the system will be commercialised within 3 years after the project end.

The strategy also identifies synergies between project results and lists the joint results of the project, including the S4RIS. A template exploitation agreement is presented to partners as a vehicle to take project results to market.

In conclusion, areas for future work are identified to ensure that all partners will undertake the necessary steps to maximise the visibility of SAFETY4RAILS scientific accomplishments and technical results, especially among end-users in order to help them use the project outcomes.

1. Introduction

1.1 Overview

The SAFETY4RAILS Description of Action (DoA) describes this deliverable as reporting:

“the actions for the joint exploitation of the project results as well as the individual exploitation plans, that will maximise the project impact”.

The main objective of this document is to develop and present an exploitation strategy that would maximise the impact of the project and ensure the uptake of all its results. This includes both individual exploitation plans pursued by each partner separately, as well as the joint exploitation efforts of the consortium.

A detailed exploitation strategy and plan developed in collaboration with all project partners is a key success factor for SAFETY4RAILS, as the vehicle for achieving the expected impacts beyond the scope of the project and ensuring that the methods, solutions and guidelines developed will be further refined and uptaken in the future, reaching metro and railway operators.

1.2 Structure of the deliverable

This document includes the following sections:

- Section 2: This section presents the methodology used to develop the SAFETY4RAILS exploitation strategy. It outlines the steps followed to gather information on all project results and determine the best course of action for their exploitation.

- Section 3: In this section, the activities for IP management during and after the end of the project are elaborated. This section lists the project’s background and foreground IP and presents partners’ individual exploitation plans (at contributory tool and/or sub-result level).

- Section 4: It proposes a joint exploitation plan for the S4RIS, while enumerating the partners interested in joint exploitation actions after the end of the project.

- Section 5: This section addresses additional actions required for joint exploitation, listing all joint results of the project and providing a template of the exploitation agreement.

- Conclusions are provided in Section 6.

2. Methodology for SAFETY4RAILS Exploitation Strategy

The SAFETY4RAILS Exploitation Strategy aims to consolidate a plan for the exploitation of the project results. As such, it relied heavily on the collaboration of all SAFETY4RAILS consortium partners to provide relevant information on their individual and joint outputs, which was then assessed and integrated. This deliverable is the result of continuous exchanges with partners (through meetings and written communication as well as questionnaires and requests for information). The step-by-step methodology used is summarised below, containing four sequential steps.

2.1 Definitions

This deliverable is built around the key concept of project exploitable result. This was defined under the T10.5 as any tangible output of the action, including software, hardware, methodologies or services, which is subject to be exploited after the project through further R&D, dissemination, commercialisation, etc.

Out of these exploitable results, the SAFETY4RAILS Exploitation Strategy prioritises the key exploitable results (KERs)[1], that is those with a "high potential to be 'exploited' downstream the value chain of a product, process or solution, or act as an important input to policy, further research or education." To select and priorities results, the EC recommends to projects to use the following criteria: "1) degree of innovation, 2) exploitability, 3) impact." These results have been selected in collaboration with project partners based on the process elaborated below.

2.2 Defining the background information

As a first step, we sought to outline the background information brought in by the partners. Indeed, the results of the project are reliant upon such background Intellectual Property (IP), such as existing patents, tools, know-how, etc.

To do so, an IP Repository was created. It included a Baseline Background IP table for SAFETY4RAILS which was distributed among consortium members. All members were requested to duly fill-in the table with the description of the background and the type of protection linked to said background. This also assisted in mapping the background needed to use the foreground, which was determined as a next step.

A template of this Baseline Background IP table can be found in Annex II.

2.3 Defining the foreground information and the individual exploitation plans

In the same IP Repository, an Exploitable Foreground table was developed. The table allowed to provide information on the owner of the foreground, the project Work Package linked to it, the type of exploitable foreground (hardware, software, guidelines and methodologies), the background needed to use such foreground (as explained above), the exploitable product (product, system, sub-system, etc.), the sector of application (for instance, some of the background brought in by partners was modified and adapted to the railway sector), the status and schedule for exploitation (starting and ending Technology Readiness Level, TRL

[1] European Commission (2020) Horizon Results Platform https://ec.europa.eu/newsroom/informatics/items/689551

as well as expected time to market), the planned IP protection strategy envisioned, as well as the other beneficiaries involved. A template of this Exploitable Foreground table can be found in Annex III.

To ensure the fruitful collaboration of all partners, a dedicated workshop was organised (by EOS and ETRA as T10.5.1 and T10.5.2 leaders respectively, M12). This enabled the clear explanation of the exercise and the collection of feedback. The slides used in this workshop are available in Annex IV.

Following this meeting, a first draft of the document was circulated to partners for their confirmation and/or additional inputs. The Exploitable Foreground Table was continuously updated throughout the project as the foreground progressed, and more detailed and accurate information became available.

At a later stage (M21), a Questionnaire was prepared for all result owners to gather and update information on all the outputs (tools, guidelines, etc.) produced or improved during the SAFETY4RAILS project. The questions referred to their plans (post-project) regarding the future development, commercialisation and exploitation of their results. A template of this questionnaire is available in Annex V.

2.4 Defining joint results, synergies and exploitation agreements

As a next step, task T10.5.2 aimed at defining the joint results and synergies among the results of the project. Result owners were therefore requested to identify any synergy with other results that could be exploited after the project (M21). They were also asked to outline the way in which ways the synergies identified could be exploited (i.e., through agreements such as further cooperation with relevant partners, Memorandums of Understanding, etc.). A template of this Synergies Table is available in Annex VI.

Based on these inputs, a cluster of results was developed. It outlines how different individual results are combined and integrated into joint results to enhance the resilience of railway and metro infrastructure.

2.5 Defining the S4RIS exploitation plan

Among the joint results, the SAFETY4RAILS Information System (S4RIS) is the main output from the project. The roadmap for its exploitation was developed in close collaboration with the leader of T10.5.1, with the objective of increasing the impact of the project in the long-term and ensure the uptake of the platform in the future.

A final questionnaire also sought to underline whom, among the project partners contributing to the S4RIS, had an interest in owning the platform and hence sharing the IPR of the platform for further exploitation in the future (M22). A template of this questionnaire is available in Annex VII.

3. Individual Exploitation Plans at Tool and System Level

3.1 IP Management

The joint exploitation and commercialisation of the SAFETY4RAILS results has as a prerequisite a clear identification of the IPR initially owned by individual partners and brought into the project, as well as of the owners of the IPR produced. For that reason, an IP Management Repository is presented in the following sections to specify the IP ownership distribution among project partners and protect both the project's background and results.

This plan takes into consideration the provisions on result ownership agreed upon in the SAFETY4RAILS Grant Agreement[2] and Consortium Agreement[3]. In summary, the rules agreed upon stipulate that:

1. IPR on background are not affected by participation in SAFETY4RAILS.
2. Project beneficiaries are only granted access rights to others' background to the extent that is necessary to implement their tasks in the project. Such access is royalty-free.
3. Results are owned by the beneficiary that generates them.
4. Joint ownership of results is possible if two or more beneficiaries "(a) have jointly generated them and (b) it is not possible to: (i) establish the respective contribution of each beneficiary, or (ii) separate them for the purpose of applying for, obtaining or maintaining their protection".
5. Partners must agree in writing the allocation and terms of exercise of their joint ownership within six months from the date of generation of such results.
6. Background and results must also be made available to other beneficiaries when necessary for exploiting their own results under fair and reasonable conditions. Such conditions may include financial terms and take into consideration the value of the results or the background.

3.2 Baseline background IP`

According to the Grant Agreement[4], 'background' means "any data, know-how or information – whatever its form or nature (tangible or intangible), including any rights such as intellectual property rights – that:

(a) is held by the beneficiaries before they acceded to the Agreement, and

(b) is needed to implement the action or exploit the results."

In order to clarify the IP baseline, a review of all partners' relevant background was conducted. This includes the description of said background, as well as the type of protection linked to it (patent, licensing, know-how, etc.) It is summarized in the table below:

TABLE 1 OVERVIEW OF PARTNER BACKGROUND

Partner	Description of relevant background	Type of protection
STAM	Experience and know-how on modelling and simulation, in particular agent-based, of complex systems	Know-how
	Experience and know-how on risk assessment of critical infrastructures and cost-benefit analysis of countermeasures	Know-how
	SecuRail - Risk Assessment and Cost-Benefit toolbox for metro and light-rail critical infrastructures	Know-how
	ABM - Agent-based 3D simulator for critical infrastructure and soft target	Know-how

[2] European Commission. SAFETY4RAILS Grant Agreement No 883532.
[3] SAFETY4RAILS Consortium Agreement Version 1.2.4 dated 8 June 2020.
[4] European Commission. SAFETY4RAILS Grant Agreement No 883532. Article 26(2).

CuriX	CuriX Anomaly Detector: univariate and multivariate time series anomaly detection	Copyright License
	CuriX Failure Predictor / CuriX Fault Localizer	Copyright License
	CuriX Heal Advice / Self-healing: Catalogue based and generic outage prediction	Copyright License
	CuriX AutoML Methods: automated organisation of machine learning methods for time-series	Copyright License
	CuriX: Cure infrastructure in XaaS. This is the overall platform integrating the above-mentioned modules	Copyright License
RMIT	Know-how of methodologies, modelling parameters and features in infrastructure projects	Know-how
	Know-how of integrating modelling into infrastructure systems and knowledge of creating an integrated software platform using that modelling	Know-how
	CAMS: Central Asset Management System	Copyright License
RINA	Knowledge, methodologies and algorithms implemented by RINA-C in relation to the fast computing of air blast load consequent to high-detonation explosive burst. Implemented software code is referred to as BomBlast3D	Know-how
	Knowledge, methodologies and algorithms implemented by RINA-C in relation to the SARA software for functional resilience assessment of a terminal asset based on the vulnerability / availability of its components	Know-how
	Engineering methodologies and knowledge owned and/or applied by RINA and/or its affiliates (RINA-S), related to the implementation of interoperability and standard related requirements, risks, resilience and vulnerability approaches and assessments	Know-how
	Background created by the area of Transport and Infrastructure (owned and/or applied by RINA) which is directly related to the project, with particular reference to the Railway, Mass Transit and Security Sector in terms of Critical Infrastructure Resilience (identification and analysis of major threat scenarios, risks and vulnerability of each CI, Definition of permanent risk clearing and mitigation actions including physical and organisational countermeasures, requirements management, operational simulations, operation and maintenance studies, dedicated safety and security analysis for system and subsystems (e.g.,	Know-how

	signalling system, communications system, permanent way, SCADA, power supply), training needs analysis, reliability, availability, maintainability and safety analyses (RAMS), EMC management, test and commissioning, bespoke innovating training and online competency management solutions, demand analysis, cost benefit and multicriteria analyses, verification and validation and competency management solutions	
	Background created by the area of Industry - Modelling and Simulation (owned and/or applied by RINA) which is directly related to the project in terms of: logistics simulations, computational fluid dynamics (CFD), debris flow modelling, blast analysis, hydrodynamic analysis, non-linear finite element analyses (FEA), electromagnetic analysis (FEM, MoM), physical system modelling, behavioural analysis and control, 3D modelling of buildings and infrastructures	Know-how
	Background created by the area of Certification (owned by RINA-S) which is directly related to the project, with respect to RINA-S being a Notified Body and Independent Safety Assessor for European and International norms on Infrastructure, Signalling, Rolling Stock, Operation, Maintenance for railway and metros. In particular, this includes Railway Independent safety assessment, Certification and Testing, Assessments and Support to Security Certification, including Design Verification Gap Analysis, In Service Support, and related aspects referenced to but not only at ISO / IEC 27001 - Information Security Management Systems, ISO / PAS 28000 - Specification for Security Management Systems for the Supply Chain, ITSEC / Common Criteria (ISO/IEC 15408) - Common Criteria for Information Technology Security Evaluation, ISO 22301 - Business Continuity Management Systems	Know-how
UNEW	SecuRail - Risk Assessment and Cost-Benefit toolbox for metro and light-rail critical infrastructures	Know-how. Note: SecuRail IP is owned by STAM and UNEW (around 85% STAM and 15% UNEW). However, the risk assessment tool being developed within SAFETY4RAILS includes only some aspects, about 5%, of SecuRail. Based on this, the IPR of UNEW on the new tool will be 5% of 15%, that is about 1%.
	Experience and know-how on risk assessment of critical infrastructures and cost-benefit analysis of countermeasures, matured also within the EU project	Know-how

	RAMPART, which produced SecuRail, jointly with UNEW and MDM	
ERARGE	PRIGM: Hardware Security Module (HSM)	Patent, Copyright License, Trademark
	Senstation: Secure sensor station and secure gateway	Know-how, Trademark
AC	Design, development, implementation and validation of data sharing infrastructures based on blockchain technologies	Know-how
	Experience on cyber-security focused on testing, design, implementation and validation of cyber-threats and detection, prevention and reaction algorithms, methodologies, infrastructures and approaches	Know-how
	Implementation of Internet of Things networks and devices by using both wireless and wired protocols, including IoT devices and network security	Know-how
	Implementation of software applications, including desktop, mobile, server and web	Know-how
ELBIT	RAM^2: Decision Support System	Patent, Copyright License
Fraunhofer	CaESAR: Cascading effect simulation to assess and increase resilience	Know-how
	DATA FAN: Anomaly Detection for time series data, Prediction of the passenger load	Know-how
LDO	Ganimede	Copyright License
	SC2: Safety & Security Control Room	Copyright License
NCSRD	iCrowd simulator is an Agent-based simulator capable of displaying small to large-scale crowds and calculate the changing status of each living component considering interactions among other entities and the environment in real time	Know-how and Copyright License
TREE	TISAIL (RAMSES)Threat Intelligence Service for Railway sector	Patent, Copyright License
ICOM	Unified Management Suite (uni|MS) software, integrated with WiBAS, which includes: Network Lifecycle Management; Radio Planner; Connected Site	Copyright License (commercial product)

	CIP & Border Surveillance (SISC2) platform	Know-how and license (commercial product)
	SecaaS is part of Intracom's Cloud Computing services (CCS)	Know-how and license (commercial product)
WINGS	WINGSPARK: WINGS Big Data and Predictive analytics tool	Know-how
INNO	Previously implemented version of an NLP analytics pipeline created for a different social media analytics application domain	Tool, know-how, copyright license for proprietary software components,
MTRS	RESTRAIL Project (FP7) - Mitigation measures for trespassing and suicide incidents SECUR-ED Project (FP7) - Development of emergency and crisis preparedness handbook	Know-how
ETRA	HYRIM Project (FP7) – Software tools for Hybrid Risk Management	Know-how
CS	Cyber Threat Intelligence (CTI) methodology	Know-how
UIC	Expert know-how in evaluating security solutions	Know-how
UREAD	Context-aware Requirements Prioritisation and Dynamic Usability, Acceptance & Social Acceptability Modelling	Know-how, Copyright
	Ethical Requirements and Ethical Compliance Assurance Management	Know-how, Copyright
	Context-aware Integrative Cyber Security & Privacy Threats Ranking and Dynamic Countermeasures Prioritisation	Know-how, Copyright
	Context-aware Data Privacy Protection Engineering	Knowhow, Copyright

3.3 Foreground IP

In addition to reviewing the background brought in by partners of the SAFETY4RAILS consortium, an assessment of the foreground coming out of the project was performed. The exercise entailed defining the owner, the type of exploitable foreground (hardware, software, guidelines and methodologies), the background needed to use such foreground (based on the Background table shown above), the exploitable product (product, system, sub-system, etc.), the sector of application, the status and schedule for exploitation, the planned IP protection strategy, as well as the other beneficiaries involved. Each partner filled in the table with regards to their respective results. The completed Foreground Table can be found below:

TABLE 2 OVERVIEW OF PROJECT FOREGROUND

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
1	RINA-C	Tool	BomBlast3d computes the loading due to the blast wave impact over structures such as buildings and supplies the main physical quantities of interest both over the wall surface of three-dimensional models (e.g.), virtually reproducing potential attractive targets for terrorists, and in air.	BomBlast 3D (know-how)	BB3d	YES	Infrastructure, Railways, blast-design, retrofitting, Security	TRL5 to TRL6 at the end of the project. 3 years until full maturity.	Know-how	None
2	AC	Tool	Block-chain based system for the exchange of sensitive information between CI. The system would be based on a REST-based interface to provide the possibility to manage heterogeneous data, coming from multiple sources,	Expert know-how of design, development, implementation and validation of data sharing infrastructures based on blockchain	Blockchain solution	NO	Critical infrastructure, railways, Security	TRL1 to TRL5 at the of the project. At least 3 additional years until full maturity.	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			and for the implementation of easy-to-use APIs.	technologies						
3	Fraunhofer	Tool	Cascading effect simulation to assess and increase resilience. Simulation tool for computing cascading effects within critical infrastructure and especially across infrastructure borders. The overall target of the CaESAR tool is to calculate cascading effects, the resilience of critical infrastructures and the influence of different mitigation on the resilience.	CaESAR (know-how)	CaESAR	YES	Critical Infrastructure, Resilience analysis and management	TRL5 to TRL7 at the end of the project. 3 additional years until technology transfer.	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
4	RMIT	Tool	Central Asset Management System supports a data driven methodology for decision making related to life cycle management of infrastructures. CAMS covers buildings, drainage assets and bridges. This is going to be expanded to asset classes belonging to the railway environment and to digital or soft assets. Further improvements of the current system will include the processing of resilience related data for assets facing extreme events such as physical and cyber-attacks.	CAMS (copyright licence)	CAMS for Rail assets	YES	Railway Infrastructure, asset management, resilience, financial strategy	TRL 3 to TRL7 at the end of the project. 1 year to reach market, with licensing or a joint venture as the preferred approach.	Copyright licensing	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
5	INNO	Tool	Citizen engagement plan for preparedness, mitigation and recovery from crisis events.	Expert know-how	Citizen engagement concept	NO	Railway crisis and disaster management	N/A – directly exploitable result	Know-how, copyright	None
6	CuriX	Tool	Cure infrastructure in XaaS (CuriX) offers a holistic approach to prevent outages, predict critical phenomena and increase resilience in IT Operation and IT Security.	CuriX (copyright licence)	CuriX	YES	SMEs and large corporations (mainly), railway systems, combined cyber-physical security.	TRL4 to TRL7 at the end of the project (for railway environment). 1 year until full maturity for SMEs and large corporations.	Copyright licensing	None
7	Fraunhofer	Tool	Data Artificial Intelligence-based Analysis, Forecasting and Reliability Evaluation. It allows to analyse different kinds of data to detect anomalies in time series training data and opens the black box of used machine	DATA FAN (know-how)	DATA FAN	YES	Railways, crisis and disaster management, security	TRL1 to TRL5 at end of project. 1-2 years until full maturity.	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			learning methods. In addition, it allows an assessment of the reliability of machine learning-based predictions. For SAFETY4RAILS, the tool DATA FAN is used to predict passenger capacity in stations and related free capacity.							
8	NCSRD	Information Exchange Subsystem	DMS (Distributed Messaging System) is an implementation of a message broker subsystem that constitutes the main interoperability subsystem for the S4RIS platform used by all S4RIS tools for information exchange.	Know-how for configuration and deployment of Apachi Kafka	DMS	NO	Information and data exchange across all S4RIS tools	TRL1 to TRL7 at the end of the project.	Open-source license	None
9	UREAD	Ethical Compliance Console as Ethical	The SAFETY4RAILS Ethical Compliance	Expertise in Ethical Compliance	Ethical Compliance Management Decision Support Pipeline from	YES	Any domain requiring Data Protection and Ethical	N/A – directly exploitable result.	Know-how, Copyright,	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
		Safeguarding Decision Support Tool	Framework has developed a systematic privacy risks responsive framework for legally-based safeguarding steps to ensure data protection compliance, comprising: i) the "Ethical Compliance Framework Console"; and ii) a Consent Form Master Template.	Assurance Management	Ethical Risks Analysis to the Legal Basis for safeguarding steps to be taken.		Compliance Management		Licensing	
10	UREAD	Tool (Security-Privacy Risks Countermeasures Prioritiser)	Context-aware Integrative Cyber-Security & Privacy Threats Ranking and Countermeasures Dynamic Prioritisation Decision Tool for Cyber-Physical Resilience Engineering	Context-aware Integrative Cyber Security & Privacy Threats Modelling and Dynamic Countermeasures Prioritisation	Integrative Cyber Security & Privacy Threat and Countermeasures Ranking and Prioritiser Tool and Generic Framework. This includes i) Decision Tool for Railways ii) Framework to customise the Tool	YES	The Decision Tools is customised for Railways and can also be exploited for other application domains; The Methodological Framework is domain and	N/A – directly exploitable result	Know-how, Copyright, Licensing	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
					for any other domain		threat type agnostic; i.e., Supports Asset Management for Resilience Engineering in any domain.			
11	UREAD	Framework and Guidelines for Context-aware Ethically Sustainability in Crisis Communications	A Methodological Framework underpinned by the S4RAILS ECFC and specifically addressing Data Privacy and Ethical Safeguarding of Citizens in deployment of Best Practice in Crisis Communications	Context-aware Data Privacy Protection Engineering Ethical Compliance Management	Operational Decision Support re the ethically safeguarded approach to be selected in executing crisis communications	YES	Applicable to any domain	N/A Decision Support Framework and Guidelines fully established	Knowhow, Copyright	None
12	LDO	Tool	Ganimede is the Leonardo platform for the large-scale analysis of live and recorded data streams based on Deep Learning. It enhances situational awareness and transforms threat detections from a manual, resource-	Ganimede (copyright licence), SC2 (copyright license)	Ganimede	YES	Infrastructure, security, safety	TRL4 to TRL7 (for railway environment) at the end of the project. 0.5 year until full maturity.	Copyright licensing	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			intensive operation into an efficient and automated process.							
13	NCSRD	Tool	The iCrowd Simulation platform is a complete domain-independent agent-based behaviour simulator. Within SAFETY4RAILS, iCrowd simulates crowd behaviour and cyber physical agents (humans, sensors, other) inside a multimodal railway system and detects, avoids or mitigates the impact of hazards for public security and safety purposes. The iCrowd platform is available as SaaS (Simulation-as-a-Service)	iCrowd (Know-how and copyright licence)	iCrowd	YES	Railways, crisis and disaster management, event planning, safe crowds and security.	TRL6 to TRL7 at the end of the project (for railway environment). 6 months to 1 year until full maturity.	Know-how, copyright licensing	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
14	MTRS	Requirements & Specifications for an Information Management System	Incident and Crisis Management Tool (ICMT) – an information management system that supports control rooms, mobile devices Apps and Web applications throughout the incident management process – control of assets, incident management and debriefing.	Expert know how - railway and metro incident and crisis management and information management system.	Incident and Crisis Management Tool (ICMT)	NO	Railway Infrastructure Manager, Railway Undertaking, Metro Operators, LRT Operators, Public Transport Authorities/Executives (PTA/PTE), Security Consulting, Emergency and Crisis Preparedness	TRL6 at the end of the project. 1-3 years until full maturity.	Know-how	None
15	CS	Guidelines and Specifications	A methodology for industry segment specific configuration & integration of an open-source tool, the Malware Information Sharing Platform (MISP). Guidelines and specifications around threat intelligence feed selection, configuration, structured data source integration	Cyber Threat Intelligence (CTI) methodology	Industry segment specific configuration & integration of an open-source tool (MISP)	NO	Railway (or other critical infrastructure) security management	TRL1 to TRL6 at the end of the project. 1 years until TRL 8.	Know-how, copyright	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			in semi-automated correlation, analysis, attribution and threat profiling.							
16	INNO	Tool	Innova Integra social media and data feed data acquisition, pre-processing, NLP analysis and analytics subsystem for use with threat repository backends.	Innova Integra NLP pipeline	Innova OS Detect Subsystem	YES	Security, safety and cybersecurity	TRL1 to TRL5-6 at the end of the project. 2-3 years until full maturity.	Know-how, copyright, licensing	None
17	ELBIT	Guidelines	The manual for crisis management and coordination of response teams describes the system features and interfaces, used by Elbit Systems to collaborate with S4RIS monitoring tools to produce relevant insights for the Operator, to address the Cyber and Cyber-	RAM² (User license)	Manual for crisis management and coordination of response teams	NO	IT and OT response centres, crisis response teams	N/A – directly exploitable result	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			Physical events for each scenario.							
18	ERARGE	Tool	Hardware Security Module (HSM) connects to SAFETY4RAILS interoperability architecture to ensure a secure communication channel is established between 'Senstation' and the control centre (or SAFETY4RAILS central system network).	PRIGM (Patent, copyright license, trademark)	PRIGM	YES	Security	TRL6 to TRL7 at the end of the project. 2 years until full maturity.	Patent, copyright licensing, trademark	None
19	ELBIT	Tool	Decision Support System RAM^2 is a cyber-physical risk assessment, monitoring and management platform, integrating with all IT, OT & IOT assets and systems.	RAM^2 (User license)	RAM^2	YES	IT & OT control centres	TRL6 to TRL7 at the end of the project (for railways environment). TRL8 to TRL9 at the end of the project (for OT & industrial security applications).	Patent, copyright licensing by Otorio Inc.	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
								1 year to reach TRL8 for this application.		
20	ETRA	Tool	Consequence cost model implemented through game-theory algorithms allowing the user to select scenarios/combination of threat scenarios and automatically compute the optimal budgetary strategy and minimise the economic consequences to the organisation when responding and recovering.	Know-how developed in the HYRIM project	Risk Assessment Planner	NO	Railway Infrastructure, asset management, resilience, financial strategy	TRL3 to TRL7 at the end of the project (for railway applications). 3 years until full maturity.	Know-how	None
21	ETRA	Guidelines	General Crisis Communication with all involved stakeholders (internal, external and clients) during and after the crisis itself – which imply response and /recovery phases in the	None	SAFETY4RAILS Crisis Communication and Information Sharing Guidelines	NO	Railway crisis and disaster management	N/A – directly exploitable result	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			resilience life-cycle, respectively.							
22	UIC	Methodology	Evaluation methodology framework to serve as a guide for evaluating security solutions demonstrated in a simulation exercise with operational data.	Expert know-how	SAFETY4RAILS Evaluation Methodology	NO	Railways, crisis and disaster management, security, cybersecurity.	N/A – directly exploitable result	Know-how	Fraunhofer
23	UNEW	Web-based Integrated tool platform	The S4RIS platform is an online platform for cyber-physical security implemented in the SAFETY4RAILS project. It is designed to integrate software tools into a single platform.	Wedpress and its application for Windows and Mac	SAFETY4RAILS Information System Platform	YES	Railways, physical and cyber security.	TRL1 to TRL7 at the end of the project. 2 years until full maturity.	Know-how, copyright licencing	ALL

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
24	RINA-C	Tool	Securestation Attack Resilience Assessment: aims to analyse a station and its equipment from a security point of view. The results of the analyses will enable the user to define, evaluate, rank and select possible countermeasures to be applied to the equipment of the station in order to reduce the effects of a terrorist attack.	SARA (know-how)	SARA	YES	Railway stations, crisis and disaster management, security	TRL5 to TRL6 at the end of the project. 1 or 2 years until full maturity.	Know-how	Pilots: Municipality of Milan (MoM) & RFI
25	ICOM	Tool	Security as a Service corresponds to innovative security services offered to Cloud customers. They are intended to provide enhanced protection to corporate assets, covering a wide range of requirements.	SecaaS (know-how & copyright license)	SecaaS	YES	Security, Cybersecurity	TRL5 to TRL7 at the end of the project (for railway environment). TRL9 (for generic infrastructures incl. telco and energy). 2-3 years until full maturity.	Know-how; licensing; copyright	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
26	STAM	Tool	Security Risk Analysis of railways infrastructures, SECURAIL 2.0 aims to safeguard metro, light rail, regional and long-distance critical infrastructures and networks which are nowadays exposed to cyber, physical, cyber-physical attacks and natural disasters. It is a risk assessment web-based application for Railway infrastructures and networks which allow to perform both quantitative and qualitative analysis.	SECURAIL (know-how)	SECURAIL	YES	Railways, crisis and disaster management, security, cybersecurity	TRL6 to TRL7 at the end of the project (for railway environment). 2 years until full maturity.	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
27	ERARGE	Tool	Secure sensor station and secure gateway: In order to provide secure data transmission between the railway physical infrastructure and the virtual cloud Senstation is planned to be realised as the combination of a secure gateway and sensor interfaces. Senstation is at client side aiming to encrypt any critical data where data is generated and assure the security of data on transit.	Senstation (know-how, trademark)	Senstation	YES	Railways, Cybersecurity, ICT, Cyber-physical systems (where available)	TRL5 to TRL6 at the end of the project. 3 years until full maturity.	Know-how, trademark	None
28	ICOM	Tool	SISC2 is a modular and scalable software integration platform for surveillance, collaboration, coordination and administration of diverse security and operations management related events. It	SISC2 (know-how and copyright licence)	SISC2	YES	Crisis and disaster management, security	TRL5 to TRL7 at the end of the project (for railway environment). TRL8 (for generic physical areas).	Know-how; licencing; copyright	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			is a comprehensive solution that gathers, processes, classifies and analyses information received from several types of detection sensors and 3rd party applications to produce meaningful intelligence.					2-3 years until full maturity.		
29	ICOM	Tool	SymbIoTe (symbiosis of smart objects across IoT environments) remedies IoT interoperability problems by providing an abstraction layer for a “unified view” about various platforms and their resources so they become transparent and standard-agnostic while ensuring data privacy and security.	SymbIoTe (know-how & copyright license)	SymbIoTe	YES	Interoperability platform	TRL5 to TRL7 at the end of the project (for railway environment). TRL8 for generic IoT ecosystems. TRL7 for e-Health services). 2-3 years until full maturity.	Know-how	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
30	TREE	Tool	Threat Intelligence Service for Railway sector provides a platform for gathering, analysing and sharing relevant Threat Intelligence for the railway sector.	TISAIL (know-how)	TISAIL	YES	Railways, crisis and disaster management, security.	TRL6 to TRL7 at the end of the project. 1 year until full commercial exploitation.	Know-how	None
31	ICOM	Tool	Unified Management Suite serves the concept of simple and unified management for networks, infrastructure and systems.	uni|MS™ (know-how and copyright licence)	uni|MS™	YES	Infrastructure, security, safety	TRL6 to TRL7 at the end of the project (for railway environment). TRL9 (for telco and energy infrastructures). 2-3 years until full maturity.	Know-how; licencing; copyright	None
32	WINGS	Tool	WINGS Big Data and Predictive analytics tool provides active system monitoring, forecasting and detection of anomalies using AI methods;	WINGSPARK (know-how)	WINGSPARK++ (working name)	YES	Infrastructure, railways, crisis and disaster management, security	TRL9 (WINGSPARK proven in an operational environment). TRL4 to TRL7 at the end of the project - system	Trademark	None

No	Owner	Type of Exploitable Foreground	Description of Exploitable Foreground	Background needed to use Foreground	Exploitable product(s)	Is this a KER (Key Exploitable Result)?	Sectors of application	Status (TRL at the start and end of the project) and schedule for exploitation	Planned IP protection strategy	Other Beneficiaries involved
			integration of various sources of data to achieve enhanced awareness; what-if analyses to assess various issues related to cyber and physical threats to the railway infrastructure; delivery of insights; visualisation of aspects of the railway infrastructure model for planning of potential measures.					prototype demonstration in operational environment (WINGSPARK ++ for railway environment, predictive analytics and anomaly detection mechanisms). 1 or 2 years until full maturity.		

3.4 Individual Partner Exploitation Plans

Each partner that has produced any type of result and IP during the project is committed to taking the necessary actions to exploit it and ensure that the impact of SAFETY4RAILS will continue after the end of the project. As such an initial exploitation of project results will take place by each partner individually.

Industrial partners already have mechanisms in place to ensure their results reach the market and will continue the development of their results using their own resources and/or public funding until they are ready for market uptake. On the other hand, academic and applied research partners plan to transfer the knowledge through scientific publications, seminars and teaching activities, as well as transferring the technology to a system integrator or spin-off.

Finally, one of the main benefits of the SAFETY4RAILS project is the participation of end-user representatives (rail and metro operators) in its consortium and Advisory Board. End-user partners are also committed to raising awareness among their networks about the SAFETY4RAILS results, hence facilitating their uptake as well as cooperating with providers to allow them to reach their markets.

3.4.1 Industrial partners

3.4.1.1 Alpha-Cyber srl

a) Partner information

Alpha-Cyber is an innovative start-up founded in late 2017 with advanced knowledge on ICT technologies and solutions. Services include consulting activities and products development, with focus on blockchain, Internet of Things and cyber-security. The mission of Alpha-Cyber is to bring technological innovation to the market in order to enhance citizen's life quality, thanks to costs and waste reduction, by lowering the environmental impact of current solutions.

b and c) Result information and Development during SAFETY4RAILS

During SAFETY4RAILS, AC evaluated the possibility of designing a **block-chain based system** for the exchange of sensitive information related to security-critical environments. The system promoted is based on a REST-based interface to provide the possibility to manage heterogeneous data, coming from multiple sources, and to allow for the implementation of easy-to-use APIs.

A proof-of-concept of this system was tested during the project. The test demonstrated that the implemented approach could eventually be integrated into the S4RIS platform, to provide added value to the whole system, guaranteeing integrity and security of stored data. As an example, the block-chain system would make it possible to quickly identify data tampering activities affecting specific source of data, by querying the blockchain to spot potential anomalies on the stored data and/or to validate data hashes.

This system was developed for SAFETY4RAILS and from a TRL1 reached TRL5 during the project.

d) Next steps

AC concluded that further study and development would be required to improve the implemented design, which would need at least 3 years to reach full maturity. For that purpose, AC will look for new funding opportunities under available R&D activities. The same team that worked on the SAFETY4RAILS proof-of-concept will continue this work after SAFETY4RAILS.

3.4.1.2 CuriX AG

a) Partner information

CuriX AG is a Swiss IT startup company founded from IC-Information Company 2021. CuriX provides an IT early warning system based on artificial intelligence and predictive big data analytics. CuriX reads weak signals based on telemetry data from IT systems, interprets them and converts them into essential information. This enables CuriX to detect unfavorable or unusual developments (events) at an early stage, localize them, rank their severity and alert accordingly. In this way, CuriX prevents possible system failures (outage prevention) and indicates possible cyber incidents at an early stage. CuriX thus prevents possible disruptions to digital business models and automates the analysis, forecasting and alerting process. On a subscription basis, CuriX AG offers its customers both, standard implementations and customer-specific solutions.

b) Result information

CuriX owns and develops a product called **CuriX (Cure Infrastructure in XaaS)** which monitors all types of IT infrastructures by means of key performance indicators. CuriX makes use of statistical and machine learning algorithms to detect anomalies, to forecast failures and locate their root causes.

CuriX is a NextGeneration Tool for system resilience: with CuriX, systems are holistically protected from threats inside or outside the system. CuriX consolidates and correlates all available numeric data. Unlike existing tools, it predicts resilience issues, which enables preventive and right on time counter measures.

CuriX® is a standard software solution offering standard connections and interfaces to the customers systems.

c) Development during SAFETY4RAILS

Commercialisation of CuriX took place during the SAFTY4RAILS project. The application has been in use in the Proof of Concept (PoC) stage since 2019 and in productive use with the first customer since early 2022.

The following improvements of the tool occurred throughout the SAFETY4RAILS project:

- Requirement CuriX_01: Cluster (log file lines) analysis (cluster methods) log file source analysis
- Requirement CuriX_02: Catalogue-Based Outage Prevention
- Requirement CuriX_03: Infrastructure Monitoring (including cyber threats)
- Requirement CuriX_04: Enhancement on user-friendly Dashboard
- Requirement CuriX_07: integration (connectors); Interface optimization and standardization
- Requirement CuriX_09: Data validation and modelling prototype enhancements

d) Next steps

Overall, through SAFETY4RAILS, the tool has evolved from TRL4 to TRL7 for the railway environment, with one year still required for reaching the market for SMEs and large corporations.

CuriX is responsible for the marketing (and market pull) as well as onboarding and enabling and supporting deployment partners. The deployment of CuriX® will be an indirect one and works via:

- System integration partners
- Software resellers
- Cloud providers

The method of deployment includes both on premise (CuriX® as a managed appliance with a yearly subscription) and CuriX® as a Service (hosted by CuriX (CuriX AG) or appropriate service providers).

The tool aims to be sold to early adopters who wish to optimise their ITOM / SIEM solution with CuriX to increase operational security and cost savings in operation. As an example, first contacts were established with a local Swiss railway to pitch the product.

Full maturity is planned for mid-year 2023 and CuriX will be provided with a licence model. To reach such maturity, the following activities linked to CuriX key modules will be implemented until mid-2023:

- Hardening of logfile analysis techniques
- Improvement of data processing / performance
- Provision of standardized integration components (controllers / connectors)
- Setup of distribution and sales channel for international businesses (currently only Swiss market addressed)
- Automatization of deployment process

Following end-user feedback, the GUI (i.e., the CuriX Dashboard) will also be made more user-friendly and the output improved to help the decision-making process even further. Likewise, more interfaces will be implemented to existing systems to gather data from there or collect feedback results to those tools.

These activities and further product development will be financed by the parent company (holding structure) as well as through the commercialization of CuriX over customer projects.

The CuriX Research and Development department (same people that joined Safety4Rails) will continue with the further development of the application as outlined above. The department is planned to increase by 30% within the next year from 6 to 8 resources.

Further R&D projects within the Horizon Europe program will also be targeted. IC aims to apply to future calls.

3.4.1.3 CYBER SERVICES PLC.

a) Partner information

Cyber Services Plc (CS) is a knowledge-based cyber security service provider interested in establishing controllable and predictable processes in the virtual space. As such, Cyber Services provides proactive cyber defence services primarily for larger commercial entities and governments internationally.

Besides traditional IT and information security consultancy and research and development solutions Cyber Services provides a holistic cyber defence life-cycle support, such as: proactive defence services; managed security services; incident response; IT risk and impact mitigation; knowledge transfer and education; and sharing cyber defence decision support information as a service.

b and c) Result information and Development during SAFETY4RAILS

CS built upon its previous Cyber Threat Intelligence (CTI) know-how to develop and implement **a methodology of adapting, configuring and integrating open-source tools in segment (railway) specific security infrastructure**. This includes guidelines and specifications around threat intelligence feed selection, configuration, structured data source integration in semi-automated correlation, analysis, attribution and threat profiling.

The Malware Information Sharing Platform (MISP), an open-source, community-driven platform for the exchange and sharing of threat intelligence and IoCs about targeted malware and attacks, was used for this exercise. The development of MISP was supported by NATO and co-funded by the EU through the Connecting European Facility, while the tool is currently used widely in order to store and exchange threat data with trust

groups, particularly in the cyber security domain. It has already been commercialised in other commercial projects of CS, unrelated to SAFETY4RAILS.

d) Next steps

The integration of this methodology in S4RIS means it has achieved a TRL6 (from TRL1 for the railway sector), as it was demonstrated in a relevant environment. Further improvements are expected to bring this methodology to TRL 8, to be ready for use in operational environment within 1 year. For this to happen, specific end-user requirements need to be considered in each individual case where the configured CTI analysis methodology is assisting infrastructure operations and management. The typical timeline for customization, validation, and testing is estimated to be 3 months per end-user. Early adopters of this methodology will be found among critical infrastructure operators, who are legally bound to implement security controls and measures to mitigate hybrid cyber-physical risks.

CS will fund these efforts through end-user contracts in B-to-B environment and own resources. The development during the project was mostly completed by the same set of experts at the company who are going to be engaged in customization and service support for prospective clients. When the tool is utilised to support more than 3 customers simultaneously, then new junior administrators need to be recruited. MISP will have to be supported by junior CTI experts. In-house training will also be considered as an option to create the relevant human capacity.

Moreover, to bring this result to the market, CS plans to begin developing its own business services through active partnerships with service provider partners, possibly through licensing and on-going support agreements from Q4 2022. Further open-source availability for a national research institute (academia sector) is scheduled from Q1 2023.

Finally, CS will build upon this result to bring impact to the market after SAFETY4RAILS, by publishing summary information on the state-of-the-art for the interested readers mostly in industry segment/security specific forums (linked-in, etc.) as well as on partner feed/portal services. Increased academic/educational impact will be achieved by utilising MISP for transportation in relevant technical trainings. MISP will also be used in future R&D projects specific to energy and transportation sectors, as CS aims to further utilise the tool in 2 other EU funded project proposals.

3.4.1.4 ELBIT SYSTEMS

a) Partner information

Elbit Systems Ltd. is an international high technology company developing and supplying defence, security and commercial systems, products and services throughout the world. The Company, which includes Elbit Systems and its subsidiaries, operates more specifically in the areas of aerospace, land and naval systems, command, control, communications, computers, intelligence surveillance and reconnaissance ("C4ISR"), unmanned aircraft systems, advanced electro-optics, electro-optic space systems, EW suites, signal intelligence systems, data links and communications systems, radios and cyber-based systems. It also focuses on the upgrading of existing platforms, developing new technologies and providing a range of support services, including training and simulation systems.

RAM²

b) Result information

Elbit Systems is the developer of the **RAM² Decision Support System tool**, which is an IT/OT cyber security platform for continuous monitoring of the operational network, risk assessment and management. It empowers industrial organizations and critical infrastructure operators to proactively reduce risks to their operational environments.

RAM² aggregates information from diverse operational and security systems to create a digital representation of the operational environment and enables organizations to quickly understand their security posture and proactively address vulnerabilities and exposures before they become breaches. With unmatched asset discovery and inventory management capabilities, RAM² allows security teams to better leverage their investment in existing technology and achieve faster ROI.

c) Development during SAFETY4RAILS

The RAM² tool was already commercialised before the start of the SAFETY4RAILS project. During the project, new plugins were developed to receive data from monitoring tools (events, assets, etc.) and generate relevant insights, together with the project's data sharing method. The tool is designated to early adapters from both the OT and IT industries, as well as long-term customers.

d) Next steps

RAM² has reached TRL7 for railway security applications through SAFETY4RAILS (from TRL6 at the start of the project) but will keep evolving to respond to market demands and new technologies. ELBIT foresees that it will take more than 12 months for the tool to reach TRL8 and be taken to the market. It is already at TRL8-9 for OT and industrial security applications. In addition, based on feedback received during the project's simulation exercise, Elbit will consider improvements to the tool's UX. Elbit plans to continue working on this tool, using the same engineering team that has been working on it so far. Cooperation in future EU R&D projects, potentially including other SAFETY4RAILS partners, is considered an option for further development.

The tool's IP will be protected through patent and copyright licensing and will be commercialised to Elbit System's customers following the incorporation of the SAFETY4RAILS results in the tool.

MANUAL FOR CRISIS MANAGEMENT AND COORDINATION OF RESPONSE TEAMS

b and c) Result information and Development during SAFETY4RAILS

In parallel to improvements made to the tool, ELBIT also updated the RAM² user manual to reflect the updates, developments and specific needs of SAFETY4RAILS end-users, developing thus a **Manual for crisis management and coordination of response teams**. This manual describes the system features and interfaces used by Elbit Systems to collaborate with S4RIS monitoring tools in order to produce relevant insights for the Operator to address the Cyber and Cyber-Physical events for each scenario.

d) Next steps

The manual is ready for direct exploitation by end-user crisis response teams. ELBIT will market this manual to railway and metro operators along with the RAM² tool.

3.4.1.5 ERARGE

a) Partner information

ERARGE is a research-oriented SME since 1975. The core research team has 3 PHDs, 2 academicians, 14 researchers working on information technologies, cryptography, chaos theory, IoT, VLSI Design, blockchain industry, machine learning, smart cards, hardware security modules, augmented reality, image processing and computer vision, embedded design, simulation technologies, trusted electronics, automation solutions, biometrics and privacy preservation.

Random Number Generators are one of the most critical components of cyber-physical security systems. The recent state of the art indicates that there is no regular and/or single method to evaluate and test the performance of randomness, reliability, the unpredictability of keys and robustness in detail. Thanks to ERARGE's method, these processes are getting standardised in the general procedure and relies on hardware-based entropy sources that guarantee the true randomness and uniqueness of crypto-keys.

ERARGE is responsible for bringing two tools to the project: **PRIGM and SENSTATION.**

PRIGM

b) Result information

As a high-throughput Hardware Security Module, PRIGM exploits the entropy source that is based on a ring oscillator, because a hardware-based source is far more resilient as compared to pseudo- or software-based entropy sources. A secure key storage is also developed at the hardware level which is protected against tampering attacks. The randomness tests are handled on the device at FPGA level as this enables the supply of sufficient amount of true random numbers whenever they are needed to generate private keys. This approach makes PRIGM compliant with high throughput IoT applications suitable for both node and person authentication, fast cryptographic functions and cryptographic verification and validation.

c) Development during SAFETY4RAILS

Throughout SAFETY4RAILS, PRIGM has been adapted to the railway sector and has progressed from TRL6 to TRL7 for railway security applications. The tool is expected to reach TRL9 for all industrial security applications (including railway security) within two years after the project ends.

d) Next steps

The tool aims to be sold to cyber-physical system owners and operators including both early adopters and long-term beneficiaries, with a specific focus on the resilience of automotive, Industry 4.0 and other critical infrastructure protection.

Amongst the entire product portfolio, ERARGE'S HSM namely PRIGM, which is equipped with a very fast hardware-based true random number generator, symmetric/asymmetric cryptographic algorithms and hashing tools can be seen as a start evolved from "question mark".

SENSTATION

b) Result information

The Senstation method presents a competitive advantage which is unique and comprehensive approach within the standardized framework. Senstation is at the client side aiming to encrypt any critical data where data is generated and assure the security of data on transit. Senstation and PRIGM work in coherence to update the required one-time passwords or any other secrets. Such a cordial work presents a low-level end-to-end and holistic cyber-physical security platform that can be adapted to any IoT-enabled system. Senstation has many wired and wireless interfaces and enables high throughput and secure data communication suitable for mission-critical systems.

c) Development during SAFETY4RAILS

Senstation is commercialized to a third-party solution provider in Turkey. This process started before the SAFETY4RAILS kick-off with requirements re-specifications and customisation of the previous work. This process got mature throughout the project and further commercialization steps have been planned.

Throughout SAFETY4RAILS, the tool has been adapted to the railway sector and has progressed from TRL5 to TRL6 for railway security applications. The tool is expected to reach TRL8 for industrial security applications (including railway security) within two years after the project ends and full maturity (TRL9) within 3 years.

d) Next steps

Like PRIGM, Senstation tool aims to be sold to cyber-physical system owners and operators including both early adopters and long-term beneficiaries, with a specific focus on the resilience of automotive, Industry 4.0 and other critical infrastructure protection.

Within 3 years, it is planned that Senstation will become a final product and get ready for the market. To do so, integration to transportation-related infrastructures and full validation that will be supported by promotional activities are needed. Existing partnerships with solution partners will be used to accelerate this process (within said 6 months after the project).

For both tools, at the software level to make them more service-oriented, ERARGE planned a series of internal tasks to adapt them in the post-project phase. The first improvements have already been finalized and even during the project, the initial phases of verification and validation will be finished.

Overall, other R&D projects from national and international resources will be used as a supporting budget, while in-house investments and joint partnerships will solution providers will be used for wider take-up. The development of these tools will be supported by ERARGE's special teams for industrialization and commercialization, working collaboratively. ERARGE has also a special motivation to employ teams in its branches abroad (namely Ergtech in Poland and now in Switzerland).

ERARGE has a strong motivation to continue with the SAFETY4RAILS consortium in future Horizon Europe or other national/international research programmes. The forthcoming areas of cooperation are expected to be, (in addition to the railway sector), automotive, integrated and multimodal transportation, critical infrastructure protection, and cyber-physical resilience in emerging areas.

ERARGE will also accelerate tandem relations with the railway sector, especially starting from the project partners and then extending to other railway operators and the Ministry of Transportation in Turkey.

Moreover, since ERARGE has positioned itself as a research-oriented SME, contribution to academia with university-public-private partnerships, publication of the results of applied research and bilateral knowledge transfer by linking S&T with industrial needs are other impactful potential areas.

3.4.1.6 ETRA Investigación Y Desarrollo S.A.

a) Partner information

ETRA Investigación y Desarrollo, S.A. (ETRA I+D) is the hi-tech unit within ETRA Group, one of the leading industrial groups in Spain. The company business focuses on the implementation and commercialisation of advanced real-time control and information management systems applied to the sectors of energy, mobility, security and public services. ETRA currently offers these solutions to its customers, mainly Public Administrations and Critical Infrastructure Operators, but the analysis and management of the massive heterogenous information streams generated and processed by those systems is becoming increasingly important and an added value that will significantly benefit the customers of ETRA.

The delivery of security solutions for public administrations and critical infrastructure operators is at the core of the technical and business interests of ETRA, which currently has an annual turnover of approximately €120M, expected to grow by a 10% per year over the next 5 years. SAFETY4RAILS is expected to have a direct impact on this business area. We see that the results from the project can be easily targeted to some of the customer segments such as metro infrastructure managers, bus fleet operators, etc.

RISK ASSESSMENT PLANNER (HOPLON)

b) Result information

During SAFETY4RAILS, ETRA built on the know-how developed in the HYRIM project to develop a **Risk Assessment Planner tool called HOPLON**. The tool is aimed at assisting railway and metro end-users with response and recovery to threats by predicting costs and calculating the optimal strategy.

c) Development during SAFETY4RAILS

A proof of concept was developed in the HYRIM project for utility networks (TRL3). In SAFETY4RAILS, the solution progressed up to TRL7 following large updates in the back-end formulation, as well as the User Interface and Experience (UI&UX). A cost-consequence model targeted to the railway sector was developed and integrated in the tool to allow the game-theory algorithms to calculate the optimal mitigation strategies.

The tool was also demonstrated with a hands-on exercise with FGC, which is also reported in D8.6[5].

d) Next steps

Following the conclusion of the project, ETRA will continue developing this tool using the same team that worked on the tool during SAFETY4RAILS. ETRA's personnel involved in SAFETY4RAILS results are experienced technology developers and business analysts. They are part of the staff to get involved in future R&D opportunities. Once the solution is fully operational, it will be transferred to the department in charge of commercial deployment.

Railway Infrastructure Managers will be the primary customer, while secondary customers will involve other critical infrastructure operators, such as utility networks.

It is currently estimated that it will take 3 years until this tool reaches full maturity. ETRA's exploitation strategy for the next three years includes:

Y1- Extend risk assessment framework.

- The consequence cost model will be expanded to include the security of the operational services of railway infrastructures.
- Non-tangible consequences of threat scenarios (e.g., reputational costs) will be included.
- The budget constraints for each action to take will be looked at.

Y2- Customisation and adaptation to end-users needs.

- Improvements and adaptations in the UI/UX will be carried out following the extension of the risk assessment framework.
- 3 iterations with the end-user will be performed to ensure usability is fully aligned with the end-user operations.

Y3- Full validation and integration within end-user premises.

- A pre-operational system will be deployed at the end-user premises to test the solution in its final configuration.
- Full validation from the end-user will be performed.

Funding for these activities is planned through further R&D projects (i.e., participation in Horizon Europe proposals and national/regional proposals) and through Pre-commercial Procurement/Public Procurement of Innovation (i.e., participation in public tenders at regional level).

[5] SAFETY4RAILS. (2022). Lessons learnt from SAFETY4RAILS for future research projects. SAFETY4RAILS project deliverable D8.6

b and c) Result information and Development during SAFETY4RAILS

ETRA also developed the SAFETY4RAILS **Crisis Communication and Information Sharing Guidelines**, a set of general guidelines for crisis communication. The guidelines are addressed to end-users and cover communication with all involved stakeholders (internal, external and clients) during and after the crisis itself, that is during the response and recovery phases in the resilience life cycle, respectively. The recommendations are summarised below:

1. Show empathy
2. Use a multi-language approach

   Ensure redundancy
3. Use visual communication
4. Be proactive
5. An internal operational ethical authority should support and provide fast clearance for any crisis communication through mass media.
6. Liaise with on-site staff
7. Use official channels only
8. Maximise key internal personnel awareness
9. Be as open as possible and as closed as necessary
10. Identify lessons learnt
11. Post-event evaluation of the crisis communication plan deployed to implement lessons learnt
12. Coordination and consistency
13. Make clients feel safe again

To develop these recommendations, ETRA built upon the experiences and objectives of end-user partners (who provided examples of existing communication frameworks, as well as their general objectives during a crisis[6]). The recommendations were also tested based on the scenario of the SAFETY4RAILS Madrid and Ankara Simulation Exercises.

c) Next steps

These Guidelines are a non-technological tool which are ready for direct exploitation and do not require any additional development. Crisis Management Offices at Railway Infrastructure Managers can directly benefit from them to improve communication mechanisms in their organisations during the response and recovery phases of a crisis.

After the end of the project, ETRA is committed to continue promoting these Guidelines in its network, but also among consortium partners and Advisory Board members to increase their impact in the field. To ensure the impact of SAFETY4RAILS, ETRA will take advantage of its work by participating in partnerships for cooperation in future relevant projects and calls; and becoming an ambassador of the solutions in other related EU R&D projects.

[6] As described in SAFETY4RAILS (2022). Guidelines for Ethically Sustainable Crisis Communications and Information Sharing. SAFETY4RAILS project deliverable D9.3.

3.4.1.7 INNOVA INTEGRA LTD

a) Partner information

Innova Integra (INNO) is a research and innovation company working in Computer Science and focusing on the application and integration of state-of-the-art Artificial Intelligence methods in real-world application scenarios. Areas of expertise include both methodological and ontological engineering as well as software systems engineering e.g. context-aware requirements analysis and privacy protection, data connectors, web services, provenance modelling and plausibility checking, privacy filtering and anonymisation, semantic sensor data fusion, machine learning, predictive modelling, decision support, crowd-sourced open data intelligence platforms and social and criminal networks analytics.

INNOVA OS DETECT SUBSYSTEM

b and c) Result information and Development during SAFETY4RAILS

I) Innova OS Detect: In SAFETY4RAILS, INNO developed a new tool, the **Innova OS Detect Subsystem**, a social media and data feed data acquisition, pre-processing, NLP processing and analytics subsystem for use with threat repository backends such as the well-known MISP repository system. The tool did not exist (and therefore was not commercialised) before the project, while at the end of SAFETY4RAILS it has reached a TRL 5-6 status.

INNO plans to market this tool towards any type of organisations who need to monitor social media and online feeds for threat information and intends to provide it as a modular plug-and-play solution to organisations using MISP repositories in the first instance.

d) Next steps

INNO foresees that it will require 2-3 years for this tool to reach full maturity, after the end of the project. Key activities required in that regard refer to further development to achieve tool robustness and ease of use; determine a marketing plan, a product packaging and the appropriate pricing. INNO will use own resources to achieve this, while the same unit will work on the technical development of the tool. A different person will be involved during the go-to-market phase.

Finally, to achieve impact in the field after SAFETY4RAILS, INNO will also cooperate in future R&D projects; and will contribute to open-source system viability through provisioning of commercial support/add-ons.

II) CITIZEN ENGAGEMENT CONCEPT

b and c) Result information and Development during SAFETY4RAILS

During SAFETY4RAILS, INNO also developed a **Citizen Engagement Concept (CEC)** that provides a framework and engagement objective-specific proposals for how to engage citizens in the context of urban transport crisis situations. This concept is one of the exploitable results of the project and is one of the non-technical tools that are offered to practitioners to improve communication with and engagement of citizens.

The CEC was developed based on a review of current best practices, goals, needs, barriers and enablers concerning general concerns of citizen engagement in the domain and concerning individual citizen engagement objectives. It includes specific guidance for preparedness prior to crisis events, the response during a crisis event and recovery following the conclusion of a crisis event.

d) Next steps

The CEC is described in a public deliverable of the SAFETY4RAILS project[7]. After the conclusion of the project, INNO is going to further develop the CEC, customise it to the needs of individual client organisations and

[7] SAFETY4RAILS (2022). Citizen's engagement concept. SAFETY4RAILS project deliverable 10.7.

integrate it with the proprietary INNO Citizens' Say participation platform in order to provide domain-specific solutions for that platform. To do so, INNO will use own-resources and the same team who worked on it during SAFETY4RAILS.

An additional option would be to convert elements of the deliverable into useful public information materials, leaflets for citizens or for citizens organisations.

3.4.1.8 INTRACOM SA TELECOM SOLUTIONS

a) Partner information

Intracom Telecom (ICOM) is the largest multinational provider of telecommunications products, and integrated ICT solutions & services in Greece with a proven track record of over 29 years of presence in Europe and more than 100 customers in the Eastern Europe, Middle East, and Asia. ICOM is rated in a top 300 of European R&D Companies and is considered amongst the largest European companies leading in R&D investments. The company operates more than 15 state-of-the-art research laboratories that drive the rapid development of high-quality, advanced telecommunication systems. Its expertise lies in the development of telecommunication products, embedded systems, and end-to-end integrated solutions, in implementing large scale turnkey projects, and in providing a wide range of engineering, consulting, and outsourcing professional services.

ICOM is a high-technology company with a vast experience in designing, developing, and producing state-of-the-art telecommunication and energy management equipment, and has combined its expertise in those two fields to meet the demands of a new evolving market. The company endorses open standards as the means to support interoperability and consumer empowerment. By actively participating in various standardization and regulation bodies (ETSI, TV Anytime, DSL Forum, WiMAX Forum, DAVIC etc.) the company seeks to continue these activities having all the necessary expertise to contribute to new standards and regulations.

In SAFETY4RAILS, ICOM provides a number of tools: **SECAAS, SISC2, UniMS and SymbIoTe.** All first three ICOM tools were already mature and commercialised at the start of the project through the Intracom Telecom brand for generic infrastructures but were further developed through the project for the railway environment. Additional features built in SAFETY4RAILS include adoption of **SymbIoTe** IoT interoperability mechanisms with possible extensions to analytics algorithms developed by other partners.

SECAAS

b) Result information

SecaaS (Security as a Service) corresponds to innovative security services offered to Cloud customers. The tool aims to provide enhanced protection to corporate assets, covering a wide range of requirements. The SecaaS portfolio encompasses dedicated virtual firewalls and web application firewalls. It can also assist organizations in strengthening their virtual private Clouds with controls applicable to their business.

c) Development during SAFETY4RAILS

While SecaaS had already reached TRL9 for generic infrastructures, including telecommunications and energy, the tool has been applied to the transport environment, including railways, and has evolved from TRL5 to TRL7 throughout the lifetime of the project.

SISC2

b) Result information

SISC2 is a modular and scalable software integration platform for surveillance, collaboration, coordination and administration of diverse security and operations management related events. It is a comprehensive solution that gathers, processes, classifies and analyses information received from several types of detection sensors and third-party applications to produce meaningful intelligence.

The SISC2 platform maximizes detection efficiency and operational effectiveness and timely produces situational awareness. It augments and expedites the operators' decision-making process by offering decision support and optimizing operation and back-office and mission plans managing available resources and tasks.

This tool is offered as part of integrated WiBAS + UniMS package (see below).

c) Development during SAFETY4RAILS

While SISC2 had already reached TRL8 for generic physical areas, the tool has been applied to the transport environment, including railways, and has in that context evolved from TRL5 to TRL7.

UNIMS

b) Result information

Network Lifecycle Management is an innovative paradigm for Wireless Transmission and Access networks offered by uni|MS™. It redefines how activities are carried out throughout Planning, Rollout, and Optimization and Maintenance phases of a network's lifecycle, offering unprecedented efficiencies. uni|MS™ provides a rich and modular set of interworking features that improves collaboration between Planners, Operators and Field Engineers and tackles complexity, from a single screen.

UniMS is part of the WiBAS offering from Intracom Telecom and in most cases, it is offered as a package. However, it might be also offered as a separate component, if required.

The tool offers a collection of capabilities in the form of Network Lifecycle Automation Applications (NLA Apps), leveraging Radio planning, Network Management and SDN control, introduces operational agility, and transforms the way that networks are being built and maintained. Eventually enhancing the value that networks produce while they remain operational.

c) Development during SAFETY4RAILS

UniMS was already deployed in railway-focused infrastructure as part of a commercial project in the past. During SAFETY4RAILS, their user interfaces and usability strategy have been adjusted to ensure accessibility, based on user needs analysis and user experiences during the project's Simulation Exercises. As a result, while UniMS had already reached TRL9 for generic infrastructures, including telecommunications and energy, it has evolved from TRL6 to TRL7 for the transport environment.

Additional features were built in, including IoT interoperability mechanisms with possible extensions to analytics algorithms developed by other partners. ICOM will proceed with employing customization options aimed at easier technical deployment of individual components.

SYMBIOTE

b) Result information

SymbIoTe (symbiosis of smart objects across IoT environments) remedies IoT interoperability problems by providing an abstraction layer for a "unified view" about various platforms and their resources so they become transparent and standard-agnostic while ensuring data privacy and security.

c) Development during SAFETY4RAILS

Based on user needs analysis and user experiences from project partners' demos/simulations, its Core Information Model (CIM) has been adjusted for compliance with IoT data exchanged among SAFETY4RAILSs project tools. As a result, the tool has evolved from TRL5 to TRL7 for the transport environment, including railways.

d) Next steps (applicable to all ICOM results)

For all tools outlined above, two or three years are expected until full commercial exploitation. For SECAAS, SISC2 and UniMS, considering that too tight lights had been identified between components, making it complex to tailor the tools to specific needs, customization options will be investigated. This will allow for an easier technical deployment of individual components. For SymbIoTe, the Core Info Model extension mechanism will be completed, the compliance with relevant IoT standards will be validated, the Message Broker interfaces will be secured and the authorization and authentication mechanisms will be enhanced for the railway sector. Extensive customization options will also be investigated in order to have easier integration with third party solutions.

SECAAS, SISC2 and UniMS are offered as licensed deployment with a one-off fee for hardware and software deployment followed by an early service and maintenance agreement. Beneficiaries include transport and transit companies, as well as companies active in the surveillance and security markets. SymbIoTe is currently expected to be licensed as COTS for integration into integrated systems hosted by service providers/operators, on a B2B per use basis.

While Intracom Telecom has already established a value chain for its tools, the links formed with SAFETY4RAILS partners during the project will be exploited to establish additional paths to access unexplored markets in other countries, e.g., in Madrid, Ankara, Rome and Milan where the Simulation Exercises took place.[8] This work will continue under the Intracom Telecom brand.

3.4.1.9 LEONARDO

a) Partner information

Leonardo is a global player in the high-tech sectors and a major operator worldwide in the Aerospace, Defence and Security sectors. Leonardo is based in Italy, has more than 46,000 employees (latest update 2018), of whom about 37% abroad, and in 2018 recorded 12.2 billion euro in revenues and received orders in the amount of 15.1 billion. Based on the dual application of technologies, Leonardo designs and creates products, systems, services and integrated solutions both for the defence sector and for public and private customers of the civil sector, both in Italy and abroad.

The wide range of defence and security solutions that Leonardo offers to Governments, private citizens and Institutions includes every possible intervention scenario: airborne and terrestrial, naval and maritime, space and cyberspace. In close contact with local customers and partners, Leonardo works every day to strengthen global security, provide essential physical protection and cybersecurity services for people, territories and infrastructure networks and supports scientific and technological research. Leonardo operates in about 20 countries with offices and industrial plants in all of the five continents and can rely on a very large network of subsidiaries, joint ventures and international partnerships, with significant industrial presence in four main markets, Italy, United Kingdom, Poland and United States and structured partnerships in the most important high potential markets in the world.

b) Result information

Within SAFETY4RAILS, Leonardo further developed **Ganimede,** an innovative, secure-by-design platform based on AI for safety and physical security, with the aim to increase the level of operational performances of customers, optimizing management and resources.

[8] Comment by project coordinator for transparency: ICOM's tools were not part of the Simulation Exercises.

Ganimede is a unique platform for large-scale video/audio analytics of live and recorded data stream. The platform:

- provides a single platform for video but also audio analysis
- has a single solution both for data centres and edge computing
- supports live video processing for real time alerts and offline recorded video analysis for investigation
- is scalable in resources and algorithms and easily configurable
- exploits existing systems and equipment safeguarding customer investment

c) Development during SAFETY4RAILS

The tool was already commercialised before the start of the SAFETY4RAILS project. However, in the past two years it was further improved through the development of new functions:

- “Man Down” detection
- Enhanced audio recognition
- Abandoned baggage detection
- People re-identification

Through the project, Ganimede has reached TRL7.

d) Next steps

Ganimede is expected to reach full maturity in half a year. To achieve this, Leonardo will need to take steps to improve the tool technically (simplifying the HMI; integrating with other VMS) and commercially (including marketing activities), also improving the HMI and ease of use of the tool.

To do so, company investments will be used and primarily the SW Engineering department will be involved in the technical part, while Marketing and Sales will work on achieving full maturity from a commercial perspective.

Ganimede can be deployed in different configuration supporting different workloads and operational contexts. At the moment, targeted customers are Rete Ferroviaria Italiana (RFI) and Azienda Trasporti Milano (ATM).

In the future, Leonardo plans to utilise the tool and build-upon the SAFETY4RAILS experience through cooperation in future R&D projects, as well as a marketing campaign targeting similar stakeholders.

3.4.1.10 MTRS3 Solution and Services Ltd.

a) Partner information

MTRS3 Solution and Services Ltd (MTRS) is an international consulting company (SME) specialising in the development of a broad range of security solutions, policies and strategies for the public transport security market. The company’s tailored solutions prevent and mitigate risks of criminal activity and terror attacks targeting the transport industry, as well as the risks and consequences of natural disasters. These solutions comprise a carefully designed blend of diverse means and measures, which are implemented to cost-effectively enhance the security of transport infrastructure, the traveling public and transport operator personnel, as well as to improve operational efficiency. The company also provides security and business consulting services to developers of technological security solutions.

b and c) Result information and Development during SAFETY4RAILS

During SAFETY4RAILS, MTRS developed an **Incident and Crisis Management Tool (ICMT)**, an information management system that supports control rooms, mobile devices Apps and Web applications throughout the incident management process – control of assets, incident management and debriefing.

This system was already commercialised: MTRS has benchmarked this concept for an 'Incident Management System' in LRT and Metro projects in Israel. During SAFETY4RAILS, MTRS added tool functionalities; integrated its operational know-how within the business process development tool; and developed a comprehensive concept of operation (CONOP) for a mainline rail and metro system. As a result, this tool reached a TRL6 within the project.

MTRS plans to market this result towards early adopters in Israel (Greenfield projects), as well as long-term customers (Brownfield railway, metro and LRT systems).

d) Next steps

MTRS will keep developing this result, after the SAFETY4RAILS project through:

- Customisation of an existing COTS
- Capacity development (product core, modules, features) of an existing COTS
- Professional services - integration and configuration in an operational environment

The same person who worked on this result during SAFETY4RAILS will continue its development.

This result is expected to reach full maturity for a solution provider with an additional product development within 1-3 years. To achieve this, MTRS will use the following funding sources:

- Greenfield projects - metro, LRT, mainline
- Brownfield projects - Railway Infrastructure Managers (IM) and Railway Undertaking (RU), Metro operators, LRT operators, Public Transport Authorities / Executives (PTA/PTE)

Finally, to achieve impact in the field, MTRS will use the following mechanisms:

- Participation in greenfield projects (metro, LRT, mainline) as lead consultant in the area of security and emergency planning
- Participation in greenfield projects brownfield projects (mainline rail, metro, LRT) s lead consultant in the area of security and emergency planning
- Business partnerships with solution providers.

3.4.1.11 RINA

a) Partner information

RINA is a global corporation that provides services across the Energy, Marine, Certification, Transport & Infrastructure and Industry sectors through a global network of 170 offices in 65 countries. Through its 3.700 talented professionals, RINA provides a wide range of high-quality tailored solutions aiming to back up the market operators across the entire life cycle of their projects.

As the engineering consultancy division of RINA, RINA Consulting provides a wide range of services covering the whole project life cycle from feasibility and specialized technical studies to conceptual and detailed design, prototyping and testing, project management, site engineering as well as operation and maintenance management. Working alongside Clients, as a trusted technical partner, RINA C provides a wide range of traditional and innovative services to critical industry sectors, including oil and gas, power, renewables, space and defence, transport and infrastructure sectors. As such, RINA-C offers high-end services to investors, promoters, operators and contractors, as well as to insurers and public administrations, to support their initiatives. Innovation is a key element in all our projects; RINA-C has a proven experience in helping its clients in developing their new products and services as well as managing their collaborative innovation processes.

Within S4R, RINA developed the **BB3d and SARA tools.**

BB3D

b) Result information

BB3D was mainly conceived and implemented to support blast designers and safety experts for carrying out studies of outdoor non-confined blast scenarios due to a high-explosive bomb attack.

The rationale of its development is based on facility of use, coupled with fast and stable computing. The assignment of data that need to be passed to BB3d is facilitated as much as possible, thus lowering the level of complexity in the setting-up of BB3d calculation, whilst the generation of free format ASCII editable outputs, such as wall blast quantities results file(s) and the number of casualties and injured people, are undemanding to manage and comprehend. In addition, BB3d computing is intrinsically stable because it is based on experimental data and not on the numerical solution.

Given these main characteristics, BB3d use is targeted to study blast scenarios for a wide range of charge possible dimensions, from a suitcase to a full van, and considering areas with an extension of a small neighbourhood or a big crucial infrastructure. It represents a good alternative to more expensive (i.e., temporary lease or perpetual purchase, maintenance) and demanding commercial software, also referred to as hydrocodes. Such tools typically need highly skilled users, powerful and expensive machines for accomplishing the complex set up of the computational case to gain outputs by performing a calculation that is quite prone to numerical instability.

c) Development during SAFETY4RAILS

Through SAFETY4RAILS, the tool's TRL has been increased to TRL6.

d) Next steps

It is expected that 3 more years are needed to reach full maturity, through performance and visualisation improvement. This will include the addition of some features related to blast wave propagation phenomena and structural damage for modern structures. Cascading effects will be looked at, as per suggestions provided by the end-users. The tool will also have to go through full validation even though this will be rather difficult to carry out due to the confidentiality of blast data of past bomb attacks. Commercially, the tool will be put in the cloud through a web application.

These improvements will be carried out with funding from other R&D projects as well as internal resources of RINA, and with the support from staff who developed BB3d so far as well as from different departments of RINA (for example IT experts, CUDA programmers, web application experts). To achieve impact in the field, the use of dissemination mechanisms such as conferences and publications will be used and cooperation in future R&D projects will be strengthened.

As far as the customer segment is concerned, the use of the BB3d tool is of interest to all people involved in designing or improving the safety and resilience of sensitive and crowded infrastructures, such as train stations and terminals. These infrastructures are typically the target of a bomb attack which aims at causing as much as possible physical damage to structures and people. To name a few, possible customers include blast experts and designers, safety experts, people in charge of the security of civil infrastructures, police, as well as national government departments and agencies interested in bomb attacks.

SARA

b) Result information

SARA is capable of making a complete risk assessment evaluation of a train station and its equipment.

The tool has the advantage of considering all the three main aspects of the loss, such as direct, indirect, and people losses.

The strong point of the tool is the possibility of simulating different mitigation actions available, such as redundancy or strengthening of physical elements. This kind of simulation gives back information on the nett gain in economic terms per each scenario (each scenario can be made up by a single mitigation action or by a plurality of them). Another fundamental point is the possibility of displaying also the information on the level of reduction of the service in terms of time losses by the users of the station.

The targets of this tool are the railway companies in charge of the managing of the train station, both at local, regional, or national scale (i.e., RFI in Italy, FNM in Lombardy, ATM in Milan Municipality).

SARA is a provision of a service model. SARA is a tool able to give support in the fields of decision making about the implementation of the risk mitigation actions and resilience improvement.

c) Development during SAFETY4RAILS

Initially created for the railway sector, SARA was further improved through SAFETY4RAILS through a better understanding of the data needed for an in-depth analysis. By the end of the project, the tool has reached TRL6.

d) Next steps

It is expected that around one to two years will be required for SARA to reach full maturity. To do so, software development will be carried out by a dedicated unit within RINA and confidentiality agreements will be pursued with infrastructure managers. Further technical analysis management will also be undertaken by staff who have already worked on the tool so far, taking into account the end-users feedback provided during the SAFETY4RAILS simulation exercises which highlighted the organisational gaps existing with regards to lack of data for proper analysis as planned. Participation in R&D projects, such as those co-financed by Horizon Europe FP will be key in achieving the latter. Publications in journals and participation in dedicated events such as workshops will simultaneously be crucial to achieve impact in the field.

3.4.1.12 STAM

a) Partner information

STAM is an engineering company that supports private and public clients, leveraging on a multidisciplinary expertise and hands-on experience across four main industrial domains, namely Security and Transport, Space and Defence, Industry, Energy and Sustainability. The company was founded in 1997, thanks to the seed funding provided by the Technology Transfer Programme of the European Space Agency (ESA) to develop an innovative gearbox system. STAM collaborates with a wide network of partners in several large research and innovation projects supported by the European Commission.

A large part of STAM's activities is currently related to security aspects of critical infrastructures. The company has matured experience in the analysis and simulation of blast effects and consequences, agent-based modelling and simulation tools of critical infrastructures operations and crisis scenarios, decision-support tools based on risk analysis and management for the security and safety of infrastructures, public spaces and citizens and the implementation of security countermeasures.

b) Result information

For the SAFETY4RAILS project, STAM brings its **SecuRail** tool for security risk analysis and builds upon it to safeguard metro, light rail, regional and long-distance critical infrastructures and networks which are nowadays exposed to cyber, physical, cyber-physical attacks and natural disasters. It is a risk assessment web-based application for Railway infrastructures and networks which allow to perform both quantitative and qualitative analysis and whose mission is to change risk management of railway and metro networks from a complex, time-consuming and costly process to a digital, easy and fast one. For this purpose, SecuRail offers tools to automatize infrastructure and service modelling, risk analysis and reporting.

As such, SecuRail's reference market is the transportation sector, especially the railway domain. SecuRail is designed to be used by railway and metro infrastructure managers/owners, providers and operators, as well as security departments.

c) Development during SAFETY4RAILS

Initially developed during the EU project RAMPART, the tool has been improved through SAFETY4RAILS since now it is a web app with an easy-to-use interface. Outside from graphical and functional upgrades, the risk computation engine has also been improved. Throughout the project, SecuRail has progressed from TRL6 to TRL7 for the railway environment.

d) Next steps

It is expected that around 2 years will be necessary to reach the full maturity of SecuRail. To do so, the product will be adapted to end-user needs, obtain full validation and be marketed. The SAFETY4RAILS simulation exercises have also shown that targeted areas of improvement are related to the implementation of specific standards used in the sector, having the possibility to have preconfigured assets/areas, and providing the user with the possibility to have more control over the values used by the tool in the computations.

The funding that is expected to be employed to fund such future improvement of the solution will come from other R&D projects and the staff currently working on the tool will be conducting the next phases of the product development.

The main mechanisms that will be used to make SecuRail achieve an impact in the field include publications, participation in workshops and knowledge transfers through collaboration in future R&D projects.

SecuRail will be offered through the selling of an annual license. This will allow the user to have a product periodically updated and improved.

3.4.1.13 TREE TECHNOLOGY

a) Partner information

Tree Technology is an R&D-performing company providing information and communication technology solutions based on Big Data and Artificial Intelligence.

Tree is divided into two branches:

1. Treelogic, the brand dedicated to digital transformation services and solutions, working under Agile methodologies.
2. R&D, exploring how advanced technologies can help customers. The technological expertise is focused on Big Data and Artificial Intelligence.

Areas of application include ICT, factories of the future, space, safety and security, health and society.

b) Result information

Under SAFETY4RAILS, TREE brings its **TISAIL** solution**,** which is a Threat Intelligence Service for the Railway sector. It provides a platform for gathering, analysing and sharing relevant Threat Intelligence for the railway sector, allowing operators to identify their vulnerabilities. TISAIL will be important for prevention and detection of attacks to the railway infrastructure.

The solution covers aspects such as the detection of a phishing attack for the railway companies, the notification of possible vulnerabilities in the components of the railway ecosystem, the alarm if one of the companies is hacked and it is published on social media, etc.

c) Development during SAFETY4RAILS

TREE had developed a prototype of TISAIL before SAFETY4RAILS, resulting from the RAMSES H2020 project. This prototype was not commercialized and went through major modifications during the SAFETY4RAILS project: the tool in itself was adapted to the needs of the railway sector and the threats identified were also adapted to the railway infrastructure, taking into account its specificities. It has evolved from TRL6 to TRL7 throughout the project.

d) Next steps

TREE foresees an additional year will be required before full maturity of the tool can be reached. To achieve this, a better understanding of stakeholders' security requirements is required to allow the integration of TISAIL with end-user premises. This point was also raised in end-user feedback during the SAFETY4RAILS simulation exercises, where TREE identified a need for cooperation with the security teams of railway stakeholders for more tailored threat intelligence.

TREE will use pre-commercial procurement, as well as its own resources for these improvements with the aim of commercializing TISAIL. The same developers' team will continue working on TISAIL, along with TREE's business unit to fully exploit the product. In terms of go-to-market and use model, the solution will be provided as a service to railway operators. It will be protected by Patent or Copyright Licensing.

TISAIL will be provided to railway, metro or transportation service companies, where they have a physical infrastructure in order to provide the service, such as railway companies, buses companies with big bus stations which could be target for an attack. A first target for TREE is making steps to sell this service to Spanish customers.

After the end of the project, TREE plans to utilise the tool and build-upon the SAFETY4RAILS improvements and feedback through cooperation in future R&D projects, as well as a marketing campaign targeting stakeholders in Spain.

3.4.1.14 WINGS ICT Solutions

a) Partner information

WINGS ICT Solutions is an SME that is focused on the development of solutions (both software and hardware) for various vertical sectors. The technology foundation comprises advanced wireless (4G/5G/B5G/WiFi), IoT, cloud and big data platforms, AI, orchestration and diagnostics, AR/VR. WINGS is proud to have cooperated from the beginning with world-class companies, in Greece, the UK, Germany and the Netherlands. Cooperation with the US has also been established, while activities for strengthening the footprints in the Middle East and in Africa are taking place.

b) Result information

Within the SAFETY4RAILS project, WINGS brings **WINGSPARK**, a Big Data and Predictive analytics tool. It provides active system monitoring, forecasting and detection of anomalies using Artificial Intelligence methods; integration of various sources of data to achieve enhanced awareness; what-if analyses to assess various issues related to cyber and physical threats to the railway infrastructure; delivery of insights; visualisation of aspects of the railway infrastructure model for planning of potential measures.

c) Development during SAFETY4RAILS

During the SAFETY4RAILS project, WINGS designed and developed an extension of the WINGSPARK platform in order to detect anomalous values in time series data and CCTV live feeds, provide useful insights regarding the status of the infrastructure and alerts in case an anomaly is detected as well as to provide potential mitigation measures (e.g., evacuation of a station in case of an incident etc.). While the overall WINGSPARK platform (with features included before the SAFETY4RAILS project) had already been proven in

an operational environment and had reached TRL9, the platform, renamed as WINGSPARK++ has been further extended and tailored to railway infrastructure, and has evolved from TRL4 to TRL7 throughout the project.

d) Next steps

WINGS foresees that an additional one or two years may be required for the tool to reach full maturity. Additional actions are required in that regard to ensure that the tool is adapted to end-user needs based on the requirements of each specific case, deployment to end-user premises and marketing activities to exploit the full potential of the solution. To achieve this, WINGS will use own resources, as well as participation in future R&D projects and commercial projects, while the work will continue by the same team that is currently working on it.

WINGS plans to provide the tool to municipalities, airports, railway stations and in general companies that act as infrastructure managers. The use model for WINGSPARK will be the provision of a service targeting railway infrastructures.

Following the conclusion of the SAFETY4RAILS project, WINGS will build upon the project conclusions and lessons-learnt to commercialise WINGSPARK. The go-to-market strategy for WINGS solutions is split in three different phases: a) Promotion and Awareness, b) Pre-sales: Customized solutions and pilots, c) Sales.

- Phase 1 “Promotion and Awareness”: Normally, the first three months after the end of the project will mainly focus on promoting the results of the project and the solution performance/innovation comparing to currently existing solutions to railway infrastructures, and other potential stakeholders/customers. This will allow WINGS to attract stakeholders’ interest and possible customers. Promotion and awareness activities will take place before the end of the Safety4Rails project.

- Phase 2 “Pre-sales: Customized solutions and pilots”: The customers attracted during the “Promotion and Awareness” phase may be interested either in the exact solutions that were designed, implemented and tested during the lifetime of SAFETY4RAILS project or to similar solutions that need to be adjusted to their needs. This phase involves all those actions that will allow the customization of the solutions to the customers’ needs. These may include but are not limited to:
    - Identification of new requirements.
    - Adjustment of monitoring, predictive and anomaly detection mechanisms.
    - Testing and validation in a lab environment.
    - Pilots of the designed mechanisms on their real environment and real users (e.g., railway facilities, municipalities, etc.).

- Phase 3 “Sales”: This phase refers to the selling of the mechanisms and the services derived both from the existing WINGSPARK solution, as well as its expansion to the railway infrastructures domain, to specific customers based on principles for licensing, business models, pricing, and distribution briefly presented above and further enhanced after the launch of the WINGSPARK+ solution.

Communication channels with broad reach (e.g., social media, project’s website, newsletters) but also workshops, webinars, conferences and other campaigns already have (during the lifetime of the project) and will be taken into consideration for the promoting activities. Social media accounts for promoting WINGSPARK solution and its functionalities, enabling stakeholders and end-users to interact, share their opinion, their concerns and their quality of experience, view news and announcements and pose questions to the project team.

3.4.2 Universities/Research Centres

3.4.2.1 Royal Melbourne Institute of Technology Spain S.L.

a) Partner information

One of Australia's original tertiary institutions, the Royal Melbourne Institute of Technology Spain S.L. (RMIT) is a global university of technology, design and enterprise. It enjoys an international reputation for excellence in education, research and engagement with industry and community.

b) Result information

As part of the project, RMIT brings forth its **Central Asset Management System (CAMS)** technology**.** Protected through copyright licence, the tool supports a data driven methodology for decision making related to life cycle management of infrastructures. CAMS covers buildings, drainage assets and bridges. Using CAMS, asset managers can capture asset condition data and obtain various analysis reports related to asset deterioration, risk and budget forecasting, allowing them to make informed decisions related to maintenance and budget allocations in regular condition and under hazardous events. Moreover, CAMS will be able to detect weak components in the system giving indication of priority of intervention and therefore delivers a good maintenance plan. An asset in good condition will have a better chance to survive an extreme event reducing out-of-service time and better allocation of financial and human resources.

c) Development during SAFETY4RAILS

The first version of the software was developed in the framework of the EU project RAMPART. Besides the graphical and functional upgrades, the risk computation engine has also been improved. Since SAFETY4RAILS, it is now a web app with an easy-to-use interface, the tool has been greatly enhanced.

Within SAFETY4RAILS, the scope of CAMS has been expanded to asset classes belonging to the railway environment and to digital or soft assets. Further improvements of the current system will include the processing of resilience related data of assets facing extreme events such as physical and cyber-attacks (i.e., through resilience modelling). The tool is therefore used to design a comprehensive asset management system for rail operators.

The tool is beneficial for railway infrastructure as well as asset management and financial strategy. Customer segments include authorities managing rail infrastructure, consultants providing asset management services to rail authorities and public-private partnerships where built operate manage agreements dictate the optimised management of Rail infrastructure.

Throughout the project, the tool has evolved from TRL3 to TRL7.

d) Next steps

It is expected that at least one year will be needed to reach pre-commissioning in a real-time project. The product will have to be adapted to meet the needs of Railways and Metro end-users, validated, as well as marketed. Following three SAFETY4RAILS simulations, areas for improvement are also related to implementing specific industry standards, establishing preconfigured assets and components, enabling End-users to have more control over the values used in calculations, and utilizing historical data recorded in previous simulations.

The funding that will be used to improve the product will come from other research and development projects, and the same team that has already worked on the product is expected to carry out the next phase of the project.

It is believed that the CAMS tools will contribute to the growth of the field via university courses and participation in academic workshops, in addition to knowledge transfer through collaborative research projects in the future.

3.4.2.2 Fraunhofer EMI

a) Partner information

The Fraunhofer-Gesellschaft is the leading organisation for applied research in Europe. Its research activities are conducted by 74 institutes and research units at locations throughout Germany.

The Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institut, EMI, is part of the Fraunhofer-Gesellschaft and studies high-speed processes in experiment and simulation. Solutions for industrial applications are approached from a physical and engineering perspective with the centre of interest on security, resilience, reliability, efficiency and sustainability of structures, systems and networks under dynamic and extraordinary loads, in particular comprising natural and man-made threats.

Throughout SAFETY4RAILS, Fraunhofer-EMI brings its **CaESAR (Cascading Effect Simulation in urban Areas to assess and increase Resilience) and DATA FAN (Data Artificial InTelligence-based Analysis Forecasting and ReliAbility EvaluatioN)** tools.

CAESAR

b) Result information

CaESAR is a software tool to evaluate and mitigate the impact of single/multiple point disruptions or crisis events on single, or coupled, critical infrastructures. This tool can simulate cascading effects for a variety of different critical infrastructures; in SAFETY4RAILS, the focus is on railway networks. The tool uses a topology and flow model of the railway network and simulates a variety of threats on the model such as natural disasters, cyber-attacks or terrorist attacks such as bombs. The models for threat (damage to the grid) and impact propagation have been implemented generically in order to accommodate a wider class of attributes. With specific knowledge of the threats and infrastructures, there is a possibility to apply the tool to a wider variety of infrastructures.

In addition, CaESAR is designed to consider attributes of the nodes, for example capacity of the nodes and computes flow through the network. CaESAR is designed as a framework and it is possible to add more models for nodes/grids/systems, threats and propagation methods, as well as its performance evaluation. The tool identifies critical components, which are components that have large cascading effects, have a high probability of failure for a specific threat, or are essential for system functionality or the vulnerability of a system. The tool will also investigate mitigation strategies, providing a ranked list as well as performance time curves. The resilience curves highlight the system's performance before the adverse event, during and the recovery after an event or attack occurs. In total, the analysis provided by the tool gives an overview of the resilience of the network and insight into the vulnerability of the network to cascading effects and how different mitigation measures improve the network.

c) Development during SAFETY4RAILS

During the SAFETY4RAILS project, additional CaESAR were developed including:

- Integration with live server
- Implementation of new visualization techniques
- Implementation of network generation scripts for open-source transportation network
- Integration with Agent-based model for passenger flow

The tool was developed for research purposes and as such, was not commercialised before SAFETY4RAILS and is planned to be provided as open source. Fraunhofer aims to provide the tool to early-adopters including other researchers (as open-source); to potentially collaborate with network providers; and to use in follow-up R&D EU projects.

Throughout the project, CaESAR has evolved from TRL5 to TRL7.

d) Next steps

It is expected that it will require three years to reach full maturity of the tool. The following activities are planned for that purpose:

- Code-optimization including parallel processing to speed-up the code
- Further inputs from end-users for adaptations and validation
- Generalization for Critical Infrastructures

In addition, based on end-user feedback during the SAFETY4RAILS Simulation Exercises, Fraunhofer is considering the following improvements:

- Provider specific mitigation options need to be implemented per use-case and further needs to be adapted (parametric tuning).
- Speed-up of the tool.
- Different models for cascades in infrastructure need to be studied and implemented/improved.

Fraunhofer aims to use other R&D projects as funding sources to further develop the tool with a research group that will include some of the same team members that have worked on it during SAFETY4RAILS.

Finally, Fraunhofer will also build further on the SAFETY4RAILS results, as they are used for teaching purposes for lectures and courses given by EMI researchers. Additional activities also include:

- A planned publication around the CaESAR tool
- Participation in the CPS4CIP workshop
- The planned release of the tool as open-source software
- The work done under S4R project is also being used in writing multiple future proposals.

DATA FAN

b) Result information

DATA FAN is a tool for anomaly detection for time series training data and prediction of the passenger load. It provides Data Artificial Intelligence-based Analysis, Forecasting and Reliability Evaluation. It allows to analyse different kinds of data to detect anomalies in time series training data and opens the black box of used machine learning methods. It offers a reliability assessment metric together with the predictions of the machine learning model. With this metric, technology acceptance is enhanced, and the end-user knows when to trust or distrust a specific prediction even if the user does not fully know the detailed algorithm. That knowledge helps the end-user minimizing uncertainty and putting decisions on a better basis.

c) Development during SAFETY4RAILS

In SAFETY4RAILS, DATA FAN is used as a prediction tool for passenger capacity in stations. The tool has not been commercialised yet as it was mainly developed within the project: the concept existed before SAFETY4RAILS, but DATA FAN was mainly developed during the project for application in the railway sector. In detail, the work for DATA FAN within SAFETY4RAILS contained the following main steps:

- Development of the ML-based algorithms for time-series analysis
- Development of the metrics for the reliability analysis as a support for the acceptance of this new technology for the practitioners and end-users
- Building a graphical user interface (GUI) that guides the end-user through the whole process of the passenger prediction

- First complete demonstrator version for a time series analysis for the passenger load prediction as well as the prediction for surrounding stations.

In this context, the TRL has been increased from 1 to 5.

d) Next steps

Fraunhofer plans to provide the tool to practitioners and end-users in the railway sector and related domains, also for doing workshops or studies for them. It will require one or two years approximately for DATA FAN to reach full maturity, while workshops, studies and reports for research requests and licensing will be used for that purpose.

Key activities required for the tool's full maturity are:

- Further technical improvement based on project feedback (approx. 6 months)
- Full validation (approx. 6 months)
- Adaptation to end-user needs (approx. 2-4 months)
- Customization & marketing (approx. 6 months)

Fraunhofer will use other research project and own resources to fund these activities, while the same team that worked on the tool during SAFETY4RAILS will continue its development.

Finally, the knowledge and work performed during SAFETY4RAILS will be used to draft a publication sharing the applied methods with the public. The outcome of the project will also be used to set-up further applications adapted to other domains like object detection or satellite data.

3.4.2.3 NCSRD

a) Partner information

The National Center for Scientific Research "Demokritos" (NCSR "Demokritos") is the largest multidisciplinary research centre in Greece, with critical mass in expertise and infrastructure in the fields of Nanotechnology, Energy & Environment, Biosciences, Particle and Nuclear Science, Informatics and Telecommunications. The National Center for Scientific Research "Demokritos" is an autonomous Legal Entity of Public Law supervised by the General Secretariat for Research and Technology (GSRT), while preserving its administrative and financial independence.

The NCSR "Demokritos" conducts world-class basic and applied research, for advancing scientific knowledge and promoting technological development in selected areas of national socio-economic interest. The Center also plays a pivotal role in graduate education and professional training and its unique infrastructure is employed for high-technology services to the Industry and the Society. NCSR "Demokritos" consists of five (5) institutes while each institute consists of different labs.

ICROWD

b) Tool information

NCSRD has contributed the **iCrowd Simulator** to the SAFETY4RAILS project, a complete general-purpose agent-based modelling platform aiming to provide an abstract, domain-agnostic simulation framework. iCrowd implements a modern, multithreaded, data-oriented simulation engine employing the latest state-of-the-art programming technologies and paradigms. It simulates crowd behaviour and cyber physical agents (humans, sensors, other) inside a multimodal railway system and detect, avoid or mitigate the impact of hazards for public security and safety purposes. The iCrowd platform is available as SaaS (Simulation-as-a-Service).

c) Development during SAFETY4RAILS

During the SAFETY4RAILS project, new functionalities and features were implemented in iCrowd. These include the intelligent use of automatic escalators by the simulated crowd, knowledge-based behaviours that model information propagation through the crowd, and CCTV monitoring system simulation, including object & agent detection as well as determination of existing “blind spots” that could be used by malicious actors for special path planning to evade detection in real time. The new features were implemented for SAFETY4RAILS but are built as independent modules that can be used for the simulation of other environments as well. The tool has evolved from TRL6 to TRL7 throughout the project.

d) Next steps

NCSRD is currently in the process of commercialising iCrowd. The tool is expected to reach full maturity and be transferred to industry within a time period of 6 months to 1 year, while NCSRD plans to use a pay-per-use model, offering iCrowd as a Simulation-as-a-Service (SaaS) tool, as well as an on-demand setup fee for space modelling and customer-specific behaviour models. This commercialisation and offering as a SaaS tool will happen through ClaRET, a spin-off SME from NCSRD.

NCSRD will provide iCrowd to security consultants in the fields of border crossing, infrastructure protection, and cyber security companies, video monitoring installers, large event and crowd protection planners, civile engineers and building designers, security personnel training, etc.

Two main actions are planned to further improve the tool:

1. Completion of the front-end photo-realistic visualizer for easier use by non-experts in simulation and for use of the simulator for training.
2. Development of the model-stitching capability that will allow the re-use and interconnection of partial models to create complex spaces without the need to re-design them from scratch.

A funding of approximately €500.000 is required to achieve these improvements. NCSRD plans to use EU projects funding that will support the existing personnel and additional personnel needed to take these actions, as well as a cooperative business scheme of a spin-off SME (Claret already established) and NCSR Demokritos as an RTO that will ensure the transfer of the tool to industry.

To achieve impact in the field, NCSRD has also published several papers in scientific journals and conference proceedings describing the operation and use of the simulator and its application in different domains of application, taking advantage of the simulations and lesson learned from the SAFETY4RAILS project.

NCSRD also plans to involve companies that provide complimentary event simulators (such as bomb blast simulators, fire simulators, vehicle simulators, etc.) that can all be integrated with iCrowd to create an extended simulation, scenario authoring, and control & command environment.

DMS

B and c) Tool information and Development during SAFETY4RAILS

The **DMS** is an implementation of a Message Broker that can be used by all tools to exchange information. One of the main advantages of using a Message Broker implementation as a means of communication between multiple systems is that whenever a system is needs to share information with two or more other systems then they can share this information through the message broker to be available for all other systems interested in the information instead of integrating with each of the interested tools separately.

The DMS chosen in SAFETY4RAILS is based on Apache Kafka technology, a well-known high-performance messaging system which is based on the publish-subscribe design pattern (i.e., parties can publish data in

specific topics and parties that are interested in the data can consume data from topics that they are interested in).

The S4RIS DMS was developed to provide a flexible framework for interoperability within the platform and enable the secure integration of external tools. In addition to the integration of tools within the S4RIS GUI (from an end-user perspective), tools must be integrated by being connected to the DMS, so that data can be exchanged between tools. To ensure coherent data handling, all tools are required to be able to read in and provide their output in JSON format.

During the project, the DMS has reached a TRL7 (from TRL1) and will be ready for exploitation as soon as all tools have been integrated to the S4RIS. It is based on Apache which is an established technology with TRL9. The framework was applied in cyber-physical events for railways for the first time.

d) Next steps

The DMS is an open-source tool, and a key component of the S4RIS platform. It cannot be exploited as a standalone tool but will be one of the main pillars of the exploitation of the platform (Section 3.5).

3.4.2.4 University of Newcastle

a) Partner information

The University of Newcastle upon Tyne (UNEW) is a UK based higher education establishment with a world-class reputation for research excellence and campuses in several other countries. UNEW strives for world-class academic excellence, working not only on the supply side of knowledge creation and dissemination, but also responding to the demand side of societal challenges. UNEW's involvement in this will be through its Centre for Railway Research (NewRail), now under the Future Mobility Group. The Future Mobility Group acts as an interface between industry and academia and provides a focus for rail transport research activities across Europe, as well as undertaking university research that are of relevance to the rail and transport industry in general.

NewRail delivers university research, information and training to meet the complex technological and managerial challenges of the transport industry, regulators, operators and customers. NewRail has a wide experience in the transfer of knowledge and international collaborative research particularly in transport applications. Since arriving in Newcastle in 2004, the group has been involved in over 40 projects both as partners and as coordinators. NewRail staff also has extensive experience as coordinators, partners, and managers of FP5, FP6, FP7 and H2020 projects and those staff allocated to this project are appropriately matched to the project aims and tasks to be delivered through their experience.

b) Result information and Development during SAFETY4RAILS

During the SAFETY4RAILS project, UNEW developed the S4RIS GUI, the UI/UX component of the S4RIS to provide the end-user with a single visualisation point. It is a web application for cyber-physical security designed to integrate software tools into a single platform. The GUI acts as an intermediate layer to the user interfaces provided; its primary objective is to provide a unified GUI for end-users to access information and different tools in the S4RIS platform.

The S4RIS is now at a TRL7 (from TRL1). It is based on Wordpress which is an established technology with TRL9.

c) Next steps

Additional actions are required for S4RIS to reach full maturity, mainly:

- Adaption to end-user requirements;

- Customisation of the interface to meet end-user needs;
- Integration to end-user premises;
- Marketing actions.

UNEW estimates that it will take 2 years for the platform to reach full maturity.

In addition, during the SAFETY4RAILS Simulation Exercises end-users identified as the biggest challenge the lack of integration of some tools that were not web compatible. Security issues were also raised regarding some tools, as linking them to the web would compromise their internal IT security. SAFETY4RAILS partners will jointly work to resolve these issues.

For that purpose, UNEW plans to use funding sources from other R&D projects, as well as launch a pre-commercial procurement process jointly with other project partners (also described in Section 3.5). UNEW has a dedicated Business Enterprise Directorate which will support the commercialisation of the platform. It must be noted that the GUI will not be commercialised as a standalone but will be one of the main pillars of the exploitation of the platform (Section 3.5).

Finally, UNEW will also build upon its work during SAFETY4RAILS to increase its academic/educational impact through the publication of journal articles and conference papers; participation in future R&I projects; and approaching companies and organisation that may be interested in S4RIS on the bilateral level.

3.4.2.5 University of Reading

a) Partner information

The Department of Computer Science at the University of Reading is part of the School of Mathematical, Physical and Computational Sciences (SMPCS). The research in the Department is organised within three main research groups and five Research Laboratories: namely AI & Data Science, Big Data Analytics, and Advanced Computing for Environmental Sciences, Computer Vision, Cyber-Physical & Embedded Data Intelligence, and Blockchain Architecture; this includes hardware accelerated real-time AI solutions, Automated ML Code Generation and model breeding. There has been a sustained pattern of large-scale collaborative projects led by the research leaders in the Department including in areas of applications of AI, and Data Science. These have included pattern discovery and multi-view data mining, cyber security and privacy-preserving technologies, and decision support, multi-modal semantic-collateral media indexing and retrieval.

b) Result information and Development during SAFETY4RAILS

I) Ethical Compliance Console as Ethical Safeguarding Decision Support Tool

During SAFETY4RAILS, UREAD engaged with the project partners to develop a systematic evidence-based framework to ensure ethical data protection compliance. This work began by mapping the SAFETY4RAILS data processing pipelines, implicated stakeholders and data types. Based on this mapping, UREAD determined the compliance measures to be planned, deployed and monitored throughout the project lifecycle.

This methodology includes:

1) Context-aware Privacy Risk Analysis Decision Table
2) Data-type and Anonymisation type specific De-Identification Decision Table3)
3) Data Controllers' Reference Compliance Decision Table (the "Ethical Compliance Framework Console", ECFC)[9], which for a given data processing context and objective assists Data Controllers in readily determining the

[9] As included in SAFETY4RAILS (2022). Ethical Compliance Framework (ECF). SAFETY4RAILS project deliverable D9.1 v1.1.

requisite compliance steps and legal basis for Compliance Assurance by selecting the relevant recommendations as indicated by the ECFC for the particular data processing pipelines as proposed by the Data Processor.

4) Consent Form Master Template, to be used to derive the appropriate Explicit Consent forms for each of the data processing purposes, as proposed by the Data Processor needed. This assisted the Partners in creating the correct consent forms together with all the requisite information to be distributed to invited data subjects prior to any data acquisition.

II) Tool (Security-Privacy Risks Countermeasures Prioritiser)

This tool takes **i)** the integrated security ontology based semantic threat model and **ii)** LINDDUN privacy threat outputs and provides **iii)** a decision network-based tool with a threat severity ranking calculus integrated with **iv)** a dynamic countermeasures prioritiser visualising the prioritisation decision process. This tool is application domain agnostic as the customisation for any application domain, workflow and threat landscape takes place merely by virtue of the threat modeller input.

Within SAFETY4RAILS this Countermeasures Prioritiser was developed to address the gap that existed in the Asset Management which is planned to include Resilience Modelling responsive to the cyber-physical attacks. As such the Countermeasure Prioritiser offers a novel methodologically guided decision framework and Calculus Tool for Intuitive Context-aware and threat based dynamic prioritisation of threats. This provides the only dynamic countermeasures priortiser providing a robust threat-responsive and current cyber resilience aware dynamic re-prioritisation of safeguarding measures and thus requisite fixes as resilience investments that need to be integrated with future generation of Asset Management systems and resilience engineering decision support tools. The current vulnerabilities and threats-based risk severity calculus essentially enables security and resilience by design both at the development stage as well for life cycle maintenance management.

c) Next steps

Within SAFETY4RAILS, the UREAD innovations I and II above have modelled the Railways System Operational Data and Ethical Protection Compliance Requirements and the Threat Landscape respectively. These tools are readily deployable to this application domain but can be applied to any other domain by simply modelling the respective ethical and privacy requirements for tool I and or threat landscape for tool II. UREAD stands ready to customise tool I and/or tool II for use in future applications through copyright protected and licensing/consultancy agreement on a case-by-case basis.

UREAD will also continue to communicate and promote this result across its network, as well as through the publication of academic articles on this topic.

III) Framework and Guidelines for Context-aware Ethically Sustainability in Crisis Communications

This is a Methodological Framework underpinned by the S4RAILS ECFC and specifically addressing Data Privacy and Ethical Safeguarding of Citizens in deployment of Best Practice in Crisis Communications. It is based on UREAD Background in context-aware Data Privacy Protection Engineering and the Ethical Framework Compliance Console (ECFC) . This is essentially a framework of decisional procedures for addressing Data Privacy and Ethical Safeguarding of Citizens in deployment of Best Practice in Crisis Communications and accordingly it offers Operational Decision Support re the ethically safeguarded approach to be selected in executing crisis communications. This framework is an essential pre-requisite for the deployment of any Crisis Communication approaches for which the prior establishment of ethically sustainable crisis communications is mandatory otherwise the organisation would expose itself to the risk of violation of legal and ethical safeguards and the citizens to serious harm and hurt.

3.4.3 End-users

The SAFETY4RAILS consortium also included eight end-users. These entities have worked together with industrial and research partners to produce the best solutions to fit their needs related to combined physical and cyber security. Their participation in the project facilitates the uptake and adaptation of the tools in order to assist their operations. As potential buyers, consortium end-users might also participate in a potential Pre-Commercial Procurement (PCP) to further develop and exploit project results.

Among end-users, those who have produced results include:

3.4.3.1 UIC

a) Partner information

The International Union of Railways (UIC) is the worldwide organisation for international cooperation among railways and promotion of rail transport at a global level. Founded in 1922, it currently gathers 200 members on all 5 continents, among them railways, rail operators, infrastructure managers, etc.

The mission of the association is to promote rail transport at world level with the objective of optimally meeting current and future challenges of mobility and sustainable development. UIC's main tasks include understanding the business needs of the rail community, launching programmes of innovation to identify solutions to meet those needs, and preparing and publishing a series of documents known as IRS that facilitate the implementation of the innovative solutions.

Within UIC, the main role of the UIC Security Division is to meet the requirements of the 200 worldwide UIC members in matters of security and, regarding technology, support/defend their needs and priorities vis à vis the supply industry. By participating in European projects, the UIC Security Division strengthens the representation of the railway sector compared to other transport sectors and helps members to look forward and develop future strategies in the area of security.

b and c) Result information and Development during SAFETY4RAILS

During SAFETY4RAILS, UIC developed an **evaluation methodology framework** to serve as a guide for evaluating security solutions demonstrated in a simulation exercise with operational data[10]. This methodology was based on the user perspective and mainly focused on the impact of the S4RIS platform in enhancing resilience against combined cyber-physical threats to railway infrastructure and metro systems.

This proposed methodology was based on: i) the validation guidance provided by the UK's Forensic Science Regulator[11] (specific Fraunhofer input to the methodology); and ii) on answering these four questions: "what, who, how and when" is relevant. The guidelines were used during the evaluation performed by the end-users of the project participating in the four simulation exercises and focused on:

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

[10] As described in in SAFETY4RAILS. (2021). Evaluation Methodology. SAFETY4RAILS project deliverable D8.1.
[11] UK Forensic Science Regulator, Guidance: Validation (FSR, Issue 2, 2020).

d) Next steps

The Evaluation Methodology is addressed to rail and metro infrastructure managers and operators who need to evaluate security solutions and are the main beneficiaries of this result. While there are currently no plans to further develop this methodology, but it will be adapted according to the priorities of each user.

Following the conclusion of the SAFETY4RAILS project, UIC will continue to communicate and promote this result among its members to ensure it achieves an impact on the field. Planned actions include:

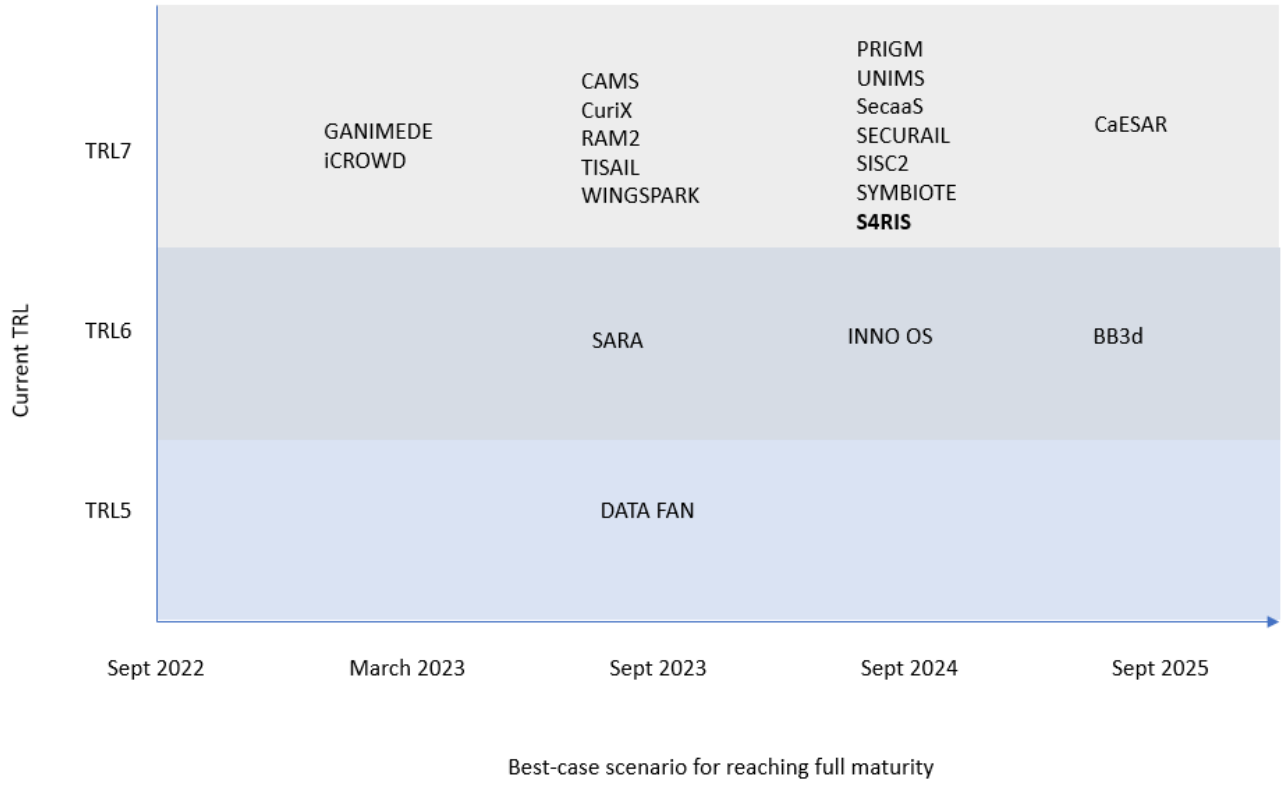
- Increasing its educational impact towards its worldwide members through publication of rail-focused articles which translate the scientific results into a way which is easy to understand by other potential end-users;
- Sharing the methodology with the rail and metro stakeholders through the UIC security platform.

3.4.4 Summary

To summarise this section, the figure below presents a timeline for the full maturity of the tools, systems and sub-systems developed during the project. This excludes the tools that are presently readily deployable and need not be further developed. These results have been grouped together according to their TRLs at the end of the project (September 2022), while the figure shows the estimated date in which they are expected to reach full maturity (in a best-case scenario).

Given the different types of SAFETY4RAILS partners, full maturity for results developed by industrial partners means reaching TRL9, while for results developed by research/academic partners the figure below takes into consideration the timeline in which they will be ready for transfer to the industry.

FIGURE 1 TECHNICAL RESULT MATURITY TIMELINE



4. S4RIS Exploitation plan

4.1 Result overview

The technical development of the SAFETY4RAILS Information System (S4RIS) platform has been the key exploitable result of the project, meant to provide railway and metro operators with a holistic solution to increase their security and recovery from cyber, physical or combined cyber-physical attacks. The platform is a combination of all project results.

As such, the S4RIS is a joint result owned by all project partners that contributed to its development and is the main object of the project's joint exploitation strategy. Each of the contributory tool owners are remaining the single owners of their contributory tools (unless otherwise identified, because of joint development). For an overview of all joint results, please see Section 5.1 below.

4.2 Proposed exploitation plan

The plan outlined in this section is one proposal that could lead to the successful exploitation of the platform as a joint result of the project – that is, including all the tools developed during SAFETY4RAILS and categorised as key exploitable results (see Table 2 for an overview of KERs and Table 4 for an overview of KERs forming the joint result of the S4RIS platform).

This plan takes into consideration the TRL and development status of each tool for the railway environment at the end of the project (September 2022). As outlined in detail in Section 3 and depicted in Table 2 and Figure 1, most tools, while already mature, have lower TRLs for the railway application: most are currently at TRL7, three tools are at TRL6 and one at TRL5. Most tool providers therefore require 2-3 years of additional funding to further develop and tailor their tools to the specific railway environment – taking also into consideration that it is a highly regulated environment with specific provisions on safety that tool providers must follow while convincing end-users of the utility of using new solutions. This is particularly true in the case of tools using Artificial Intelligence (the current regulatory framework limits their adaptation by end-users). Given the complex safety and security schemes currently implemented by end-users, the proposed plan gives them as well the time to successfully integrate the platform in their systems and allows for the necessary training to their security experts. This is why the platform as a joint result including all SAFETY4RAILS tools cannot be taken to the market immediately and requires 2 to 3 years of preparation and further tailoring to the railway segment.

It has already been established that every partner individually is looking for opportunities to commercialise its tools and is improving them based on the feedback and the evaluation received by end-users during the project. Therefore, the innovative solutions developed by SAFETY4RAILS partners will reach the market on time, while they are still "novel". It is the combination of all tools and the platform that requires further refinement.

It is worth noting here that if the consortium identified the right opportunity, the S4RIS platform in itself with the tools that are at a higher maturity level and have already been integrated (e.g., CuriX) could already be taken to the market without the need for a preparatory phase. That is because the S4RIS platform is a combination of Kafka and Wordpress – two technologies that already exist and have been successfully commercialised. The additional time foreseen in the plan below aims to ensure that interested end-users would be offered a platform with the tools that best suit their needs; and this is why the PCP route has been chosen to tailor the platform and the tools to each end user's specific needs and existing systems. At the same time, the SAFETY4RAILS consortium is constantly looking for other suitable opportunities.

This proposed exploitation plan is informed by means and mechanisms required to implement it, i.e., the funding framework described below, as well as by the individual exploitation plans of partners, considering that their tools feed into the platform.

The proposed S4RIS exploitation plan is split in three phases:

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

SAFETY4RAILS technical partners as well as end-user partners will have a key role to play in this plan, as the success of the S4RIS relies on their cooperation. End-users are foreseen to provide specifications to further refine and develop the S4RIS and its tools, as well as further disseminate the result in their networks. Technical and marketing staff in industrial partners will be crucial for the technical development and industrialisation of the platform.

The exploitation plan details activities required to take the SAFETY4RAILS solution to the market. The further development and commercialisation of the platform also depends and relies on partners' individual exploitation plans. The purpose of the activities described below (and in Section 3 above) is to improve the platform and ensure it can be integrated in end-user systems, based also on the feedback received from partner end-users during the project.

The feasibility and success of this plan is further supported by the fact that end-user partners from the SAFETY4RAILS consortium have already expressed their interest in participating in the commercialisation of the S4RIS platform. For example, MDM and TCDD are particularly interested in joining this effort, while the end-user representative of the project, UIC is regularly sharing the SAFETY4RAILS results with its members and has already gathered interest from RATP (France) and Metro de Lisbon (Portugal). UIC is frequently presenting these results to international events gathering railways and metro operators' security experts and thus, identifying new end-users/potential buyers.

YEAR 1: PREPARATION PHASE

To ensure the successful exploitation of the S4RIS, the SAFETY4RAILS consortium could take advantage of the opportunities offered through the mechanism of EU-funded Pre-Commercial Procurement (PCP)[12] to further develop and exploit the project results. This mechanism would facilitate the industrialisation of the S4RIS and ensure that it meets the specifications of end-users across Member States, as well as that it reaches more relevant stakeholders.

To begin with, SAFETY4RAILS end-users are advised to prepare and launch a PCP of the S4RIS. Actions to be undertaken in this phase include:

- Evaluation of the needs and challenges
- Launching an open-market consultation
- Drafting specifications and requirements
- Launch the tender process
- Close contracts

At the same time, SAFETY4RAILS tool providers will launch market promotion actions to engage with early adopters:

- Assess the market and customer needs

[12] European Commission (2007). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe. COM(2007) 799 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF

- Map potential interested end-users
- Review market strategy and business approach
- Review pricing strategy

YEAR 2: INDUSTRIALISATION PHASE – 1ST YEAR OF THE PCP PROJECT

Partners should be ready to launch the PCP within a year of the end of the project. The PCP would facilitate the scaling of S4RIS to a more mature prototype.

As a first step, partners would have to make the required technical improvements and adaptions of the S4RIS (including the GUI and other components) to meet the specifications and requirements of participating end-users. This would be additional to the specifications and requirements already identified within the project. Foreseen actions would include:

- Customisation and adaptation of the User Interface and User Experience to the specific end-user usability needs.
- Scale the SAFETY4RAILS solution to the management of the large volume of data linked to the assets in a railway network, including full interoperability with end-users legacy systems and facilities.
- Develop additional modules/features required by the end-users (if any).
- Perform technical verification and validation of the system.

YEAR 3: INDUSTRIALISATION PHASE – 2ND YEAR OF THE PCP PROJECT

The second year of the PCP project would focus on piloting the already developed solutions in end-user systems, as well as starting production.

- Develop and test pre-production/ installation hardware and software system at pilot demos.
- Full integration and deployment with legacy systems at the end-user premises to allow full interoperability and information exchange.
- Perform the certification of the S4RIS according to the required standards.

In parallel, SAFETY4RAILS commercial/business partners participating in the PCP project would update the customer engagement plan, and the marketing strategy and define a transferability framework to be able to deploy the solution to the largest possible number of railway operators in the EU.

Presentations, press releases and publications about the benefits of SAFETY4RAILS can bring to railway operators (compared to other available tools).

YEAR 4: COMMERCIALISATION PHASE – MARKET LAUNCH WITH EARLY ADOPTERS

- After the PCP project finalisation, the business partners selected would establish a salesforce and a marketing team to launch the solutions to the market through early adopters – those participating in the PCP. Specific procurement mechanisms would be launched from the end-user side to adopt the solution.
- A customer support and maintenance team would be established by the business partners to guarantee the uptake of the solution.
- Further training activities would be performed with the end-user to facilitate adoption.
- Demonstrations at relevant security-related events would be organised and attended by Railway Infrastructure Managers.

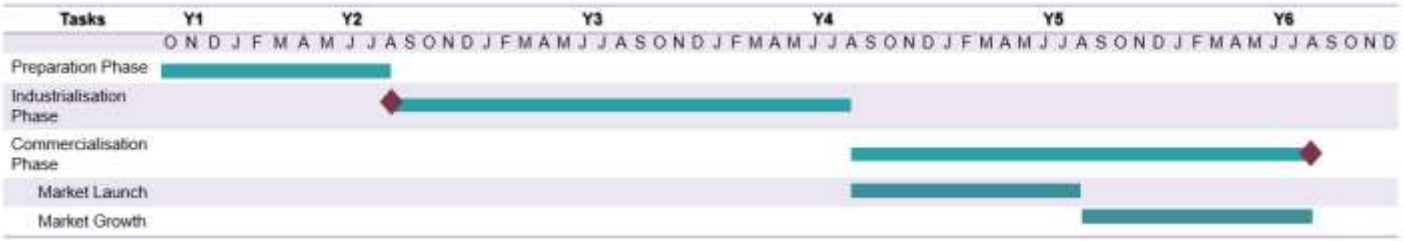
YEAR 5: COMMERCIALISATION PHASE – MARKET GROWTH AND EXPANSION THROUGH THE EU

- Launch commercial activities with Railway Infrastructure customers in other countries with high market value in Europe (according to the market analysis performed in D10.8).
- Close licensing contracts with large-scale system integrators who would leverage their network to increase the customer-base of the SAFETY4RAILS results.

- Perform commercial demos in the targeted countries and stimulate customer interest using a test version.
- Investigate other stakeholders' market (e.g., buses, ports, airports) and stimulate customers' interest using pilot demos and/or specific fairs attendance.

This exploitation plan is also outlined in the GANTT chart below:

FIGURE 2 EXPLOITATION PLAN TIMELINE



4.3 Identified opportunities

To ensure the success of this plan, the SAFETY4RAILS consortium will look for funding opportunities to support the PCP. The plan and timeline proposed are tentative and can be adapted to the available funding opportunities.

An opportunity identified early on, is the PREVENT call for tenders, a research & development (R&D) services procurement which is conducted through a PCP. PREVENT aims to improve the security of public transport through the procurement of technological solutions[13].

PREVENT could serve as a starting point for the exploitation of S4RIS components as according to the Tender Document, it seeks to provide Public Transport Operators "with solutions enhancing security situational awareness".

Several SAFETY4RAILS partners are listed in the Buyers (i.e., FGC and PRORAIL) and Preferred Partners (i.e., UIC and Metro de Madrid) groups for PREVENT. These SAFETY4RAILS partners will be taking advantage of the knowledge and expertise developed during the project to evaluate the technologies submitted. They would also be able to use their experience in the PREVENT PCP to build the SAFETY4RAILS one.

Partners have been made aware of this opportunity – however the sensitive nature of this action prevents them from disclosing any further information.

In addition, partners could seek to launch a Horizon Europe-funded PCP based on the Cluster 3 topic "Stronger grounds for pre-commercial procurement of innovative security technologies" [14] which foresees as a follow-up a PCP action to be included in the Work Programme 2023-2024. That would push the timeline for the start of

[13] PREVENT (2022) Tender Document (TD1) https://prevent-pcp.eu/wp-content/uploads/TD-1-PREVENT-PCP-CALL-FOR-TENDERS.pdf

[14] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/horizon-cl3-2022-ssri-01-03;callCode=HORIZON-CL3-2022-SSRI-01;freeTextSearchKeyword=;matchWholeText=true;typeCodes=1;statusCodes=31094501,31094502,31094503;programmePeriod=null;programCcm2Id=null;programDivisionCode=null;focusAreaCode=null;destination=null;mission=null;geographicalZonesCode=null;programmeDivisionProspect=null;startDateLte=null;startDateGte=null;crossCuttingPriorityCode=null;cpvCode=null;performanceOfDelivery=null;sortQuery=sortStatus;orderBy=asc;onlyTenders=false;topicListKey=callTopicSearchTableState

the PCP to Q3 2024 at the earliest. Such an action would allow the SAFETY4RAILS consortium to market its solutions towards an international group of procurers.

Alternatively, partners will also look into innovation procurement opportunities provided by the European Structural Investment Fund (ESIF).

4.4 Exploitation Coordination Committee

The vast majority of technical partners have confirmed their interest in taking part in the joint exploitation of the S4RIS as outlined in Section 3.5.2 above. Interested partners have also formed an Exploitation Coordination Committee which will oversee the joint exploitation approach for the SAFETY4RAILS results. Partners have designated a representative member and provided their contact details. The relevant list is kept internally within the consortium.

The table below lists the partners ready to start discussions and begin the joint exploitation process.

TABLE 3 EXPRESSION OF INTEREST FOR S4RIS JOINT EXPLOITATION

Partner name	Partner Acronym	Partner wants to have share of the IPR of the S4RIS platform	Partners wants to exploit the results/license for education purposes	Partner is interested to participate in the commercialisation of the S4RIS platform	Partner is interested to commercialise its tool/component
CuriX	CuriX	Yes	Yes	Yes	Yes
Cyber Services Plc.	CS	Yes	Yes	Yes	Yes
Elbit Systems C4I and Cyber[15]	ELBIT	Yes	Yes	Yes	Yes
Ergunler Insaat Petrol Urunleri Otomotiv Tekstil Madencilik Su Urunler Sanayi Ve Ticaret Limited STI.	ERARGE	Yes	Yes	Yes	Yes
Fraunhofer (CAESAR)	FHG	Yes	Yes	No	No
Fraunhofer (DATA FAN)	FHG	Yes	Yes	Yes	Yes
Innova Integra	INNO	Yes	No	Yes	Yes

[15] ELBIT agrees to be listed as an optional solution for S4RIS decision support system. Each relevant opportunity will be analysed separately.

Intracom S. A. Telecom Solutions	ICOM	Yes	No	No	Yes
Leonardo S.p.a	LDO	Yes	No	Yes	Yes
MTRS3 Solutions and Services Ltd.	MTRS	No	No	No	Yes
NCSR Demokritos	NCSRD	Yes	Yes	Yes	Yes
RINA Consulting S.p.A.	RINA-C	Yes	No	Yes	Yes
Royal Melbourne Institute of Technology Spain S.L.	RMIT	Yes	Yes	Yes	Yes
STAM S.r.l.	STAM	Yes	Yes	Yes	Yes
Tree Technology	TREE	Yes	Yes	Yes	Yes
University of Newcastle	UNEW	Yes	Yes	Yes	Yes
University of Reading	UREAD	Yes	Yes	Yes	Yes
WINGS ICT Solutions	WINGS	Yes	No	Yes	Yes

5. Exploitation Agreements

5.1 Joint Results

In addition to the previously identified and listed results, through their collaboration during SAFETY4RAILS, project partners also developed methods and solutions that could work together to ensure the resilience of rail and metro infrastructures. Several results work together in synergy to address different concerns of end-users.

After the project, partners will evaluate the possibility of joint exploitation and for that they can use the template in the Annex VIII for establishing the necessary agreements, also based on the Consortium Agreement.

These results, as identified by the relevant partners, are listed in the table below:

TABLE 4 LIST OF JOINT RESULTS

No	Joint Result Name	Relevant components of IP repository (TABLE 2)
1	Cyber-physical Anomaly detection for the railway sector	CURIX: #6; ELBIT: #17; ERARGE: #16, #27; LDO: #10; TREE: #30; WINGS: #32
2	Crowd monitoring, management and decision support for the railway sector	Fraunhofer: #3, #7; NCSRD: #11; WINGS: #32
3	Threat intelligence and decision support for the railway sector	ELBIT: #17; Fraunhofer: #3; TREE: #30; WINGS: #32
4	Security risk assessment for railway infrastructure	ELBIT: #17, RINA: #1, STAM: #26
5	Railway assets monitoring and management	NCSRD: #11; RMIT: #4
6	SAFETY4RAILS Information System	CURIX: #6; ELBIT: #17; ERARGE: #16; Fraunhofer: #3, #7; NCSRD: #8; RINA: #24; RMIT: #4; STAM: #26; TREE: #30; UNEW: #23; WINGS: #32

Project partners were also asked to express in which way they could work together to further exploit these joint results. All partners were open to further discussions among them through joint exploitation agreements, as well as through working together in new R&D projects. Such contracts will be defined through discussions and contact post-project with the template exploitation agreement in Annex VIII, as well as the joint exploitation strategy outlined in Section 3.5 to be used as starting points.

6. Conclusion

6.1 Summary

In this document, the SAFETY4RAILS Exploitation Strategy has been described, building upon partners' individual exploitation plans and proposing a course of action for the exploitation of joint results, focusing in particular on the S4RIS as the key marketable and innovative system developed during the project.

Section 3, has shown how, based on the background they brought into the project, in two years' time SAFETY4RAILS partners developed more than 30 key exploitable results, including technical tools and components, but also guidelines and methodologies, that are expected to make a positive impact in the field and assist railways and metro operators in improving the resilience of their infrastructures.

To ensure that the SAFETY4RAILS solutions reach the targeted market segments, in the same section, the actions that are to be undertaken by project partners individually were mapped out. Most notably, a plan for the industrialisation and commercialisation of the S4RIS has been developed based on the PCP mechanism, and

all the partners interested in joining this effort have been mapped out. This plan is a proposal regarding the strategy partners can follow to ensure the successful exploitation of the project solutions.

Finally, section 4 has highlighted other synergies identified between the project results and proposed an exploitation agreement template to be used by partners while negotiating their next steps.

6.2 Future work

It is worth highlighting that the exploitation efforts will continue after the end of the project to ensure a positive impact in the field.

To begin with, all partners are committed to undertaking additional dissemination actions to spread the results of SAFETY4RAILS – in addition to their marketing activities. Research partners in particular will continue their presentations in scientific conferences and publications in scientific journals, while all other partners will keep raising awareness in their networks, in industry-specific events and through new R&D projects[16]. Such activities will boost the visibility of results, hence facilitating their market uptake.

What is more, marketing activities will be launched to increase the opportunities for exploitation of the S4RIS and other project results among end-users. Partners also plan to be involved in new R&D projects in which they will further develop the SAFETY4RAILS solutions.

On the end-user side, in addition to the participation of SAFETY4RAILS end-users in a potential PCP call, all partners will continue to disseminate the results in relevant international meetings and across their networks.

Finally, it must be noted that UIC will continue maintaining and updating the SAFETY4RAILS website after the end of the project. In addition to information about the project and the contact details of all relevant partners, the website also includes a list of public project deliverables, facilitating thus access to information about the project's results.

[16] SAFETY4RAILS (2022). Second Update of the Dissemination and Communication Plan. SAFETY4RAILS project deliverable D10.3.

BIBLIOGRAPHY

1. European Commission. SAFETY4RAILS Grant Agreement No 883532.
2. European Commission (2020) Horizon Results Platform https://ec.europa.eu/newsroom/informatics/items/689551
3. European Commission (2007). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe. COM(2007) 799 final. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0799:FIN:EN:PDF
4. SAFETY4RAILS Consortium Agreement Version 1.2.4 dated 8 June 2020.
5. SAFETY4RAILS. (2022). Lessons learnt from SAFETY4RAILS for future research projects. SAFETY4RAILS project deliverable D8.6
6. SAFETY4RAILS (2022). Guidelines for Ethically Sustainable Crisis Communications and Information Sharing. SAFETY4RAILS project deliverable D9.3.
7. SAFETY4RAILS (2022). Citizen's engagement concept. SAFETY4RAILS project deliverable 10.7.
8. SAFETY4RAILS (2022). Ethical Compliance Framework (ECF). SAFETY4RAILS project deliverable D9.1 v1.1.
9. SAFETY4RAILS. (2021). Evaluation Methodology. SAFETY4RAILS project deliverable D8.1.
10. SAFETY4RAILS (2022). Second Update of the Dissemination and Communication Plan. SAFETY4RAILS project deliverable D10.3.
11. UK Forensic Science Regulator, Guidance: Validation (FSR, Issue 2, 2020).

ANNEXES

ANNEX I. Glossary and Acronyms

TABLE 5 GLOSSARY AND ACRONYMS

Term	Definition/description
CEC	Citizen Engagement Concept
DoA	Description of Action
DMS	Distributed Messaging System
GUI	Graphical User Interface
ICT	Information and Communications Technology
IP	Intellectual Property
IPR	Intellectual Property Rights
KER	Key Exploitable Result
PCP	Pre-Commercial Procurement
S4RIS	SAFETY4RAILS Information System
TRL	Technology Readiness Level
UI	User Interface
UX	User Experience

ANNEX II. SAFETY4RAILS Baseline Background IP Template

PARTNER	DESCRIPTION OF RELEVANT BACKGROUND	TYPE OF PROTECTION (PATENT, KNOW-HOW, ETC.)

ANNEX III. Exploitable Foreground and Exploitation Routes Template

Owner	Type of exploitable foreground	Description of exploitable foreground	Background needed to use foreground	Exploitable product(s)	Is this a KER (key exploitable result)?	Sectors of application	Status and schedule for exploitation	Planned IP protection strategy	Other beneficiaries involved
Partner name	Software, software platform, tool	Description of the main scope and objectives of the product	As per background tab	Name of the product	TBD	i.e., Railways, crisis and disaster management, security, cybersecurity, safety	Starting TRL level and target TRL level; number of years until full commercial exploitation	Copyright licensing, patenting, know-how, trade secret, trademark	TBD

ANNEX IV. IPR Management Workshop

WP10 –T10.5: Defining the exploitation roadmap – 1st session Workshop

27 September 2021

EOS&ETRA

SAFETY4RAILS

1

Workshop agenda

- Workshop objectives
- Baseline definitions
- IP repository overview
- Data required from tool providers
- Live Session with Volunteer
- Action items requested
- Next steps

2

Workshop objectives

- Present and explain the IP Repository tool (see Excel table)
- Detailed description of information needed from ALL tool providers
- Live session with 1 volunteer

3

Baseline definitions

- Result: *"Any tangible or intangible output of the action, such as data, knowledge and information whatever their form or nature, whether or not they can be protected, which are generated in the action as well as any attached rights, including intellectual property rights."* **E.g.: Hardware, software, guidelines, methodology…**
- Key Exploitable Result: *"Is an identified main interesting result (as defined above) which has been selected and prioritised due to its high potential to be 'exploited' downstream the value chain of a product, process or solution, or act as an important input to policy, further research or education. To select and prioritise results, the EC recommends to projects to use the following criteria: 1) degree of innovation, 2) exploitability, 3) impact."*
- Exploitation route: There are basically four way of exploitation: 1) A licensing agreement with a company; 2) Business start-up: get your idea to market yourself; 3) A joint venture; 4) Outright sale of your idea.

4

IP repository overview

- Show excel file live
- Explanation of what is expected on all columns

5

Data required from tool providers

- Column J, K, L to fill in (i.e: Status and schedule for exploitation, Planned IP protection strategy, Other Beneficiaries involved)
- Confirm the content of the other columns: E, F, G, I (i.e: Description of Exploitable Foreground, Background needed to use Foreground, Exploitable product(s), Sectors of application)

6

Live Session with Volunteer

- Live description of the main scope and objectives of the product
- Identification of the background needed to use the foreground
- Name of the product
- Definition of the sector of application (i.e: Railways, security, cyber…)
- TRL level at the start, TRL level targeted, number of years until fully commercial
- Planned IP protection strategy
- Involvement of other beneficiaries

7

Action items requested

ALL tool providers:

- 1) REVIEW and CONFIRM the information available for your tools at the repository.
- 2) Each tool provider to provide details on:
  - Starting TRL, expected TRL at project closure, n° of years until commercialisation/technology transfer to industry
  - Planned IP protection for the foreground (licensing, patenting, trademark, know-how,…)
  - Other beneficiaries involved in the technical development of the tools

8

Next steps

- What is next after this is completed?
  - IP repository to be circulated every 2 months
- Start the work on identification and characterisation of Key Exploitable Results

9

ANNEX V. Questionnaire

Please fill in the table below for each of the tools you have developed during the SAFETY4RAILS project. The questions refer to your plans (post-project) regarding the future development, commercialisation and exploitation of your tools as results of the project.

Q1. Partner Name	
Q2. Tool Name	
Q3. Is the tool already commercialized (no need to consider specific features and/or data developed in SAFETY4RAILS)? Please specify if this milestone occurred before or during the project.	
Q4. How is the tool developed/improved through SAFETY4RAILS (i.e., is it being adapted to the railway sector from a previous product/solution in a different sector? Is only the TRL being increased?)	
Q5. What will be the TRL of the tool at the end of the project?	
Q6. To whom will you sell/provide your tool to (early-adopters and long-term customers/beneficiaries, NOT the target market)?	
Q7. What is the timeline between the end of the project and full maturity of the tool (number of years for market launch for industrial partners or transfer to industry for research partners)? For research partners, what mechanisms do you intend to use (i.e., open-source, licensing, etc.)?	
Q8. What key activities are required to reach full maturity – both technically and commercially (i.e., customization, adaptation to end-user needs, integration with end-user premises, full validation, marketing, etc.)? Please specify a tentative timeline for each key activity.	
Q9. Considering the previous question, what funding sources will be used to do this (other R&D projects, Pre-commercial Procurement, own resources, etc.)?	
Q10. What institutional mechanism and type of personnel will support the further development of this tool (depending on your internal organization, who will work on it: the same person who worked in it so far – for SMEs for example –, a different unit – for industry –, a new spin-off entity – for research partners, etc.)?	
Q11. Based on the simulation exercises and end-user feedback, what gaps in your tool have been identified? Do you intend on adapting the tool accordingly post-project?	

Q12. How (through which mechanism) will you utilize/build-upon the tool (as a result of S4R) to achieve impact in the field? Please explain. Some relevant examples are: • Research partners: Increase academic/educational impact through the publication of journal articles, participation in workshops, update of students' curricula, knowledge transfer through collaboration in future relevant projects… • Commercial/Business partners: Cooperation in future R&D projects, contribution to standards development, etc.	

ANNEX VI. Synergies Table

Is there any synergy with other results that could be exploited after the project (clusters of results)? Please fill-in the table below and explain how you can exploit the synergies identified (how you are considering further cooperation with relevant partners etc.).

ORGANISATION	TOOL	SYNERGIES IDENTIFIED (INDICATE WITH AN 'X')	BRIEFLY EXPLAIN THE SYNERGY	HAVE YOU ALREADY ENTERED INTO DISCUSSION WITH THE OWNER REGARDING AN EXPLOITATION AGREEMENT?	WHICH TYPE OF AGREEMENT WOULD BEST SUIT YOUR INTERESTS?
RINA	BB3D				
FRAUNHOFER	CAESAR				
RMIT	CAMS				
CURIX	CURIX				
FRAUNHOFER	DATA FAN				
LDO	GANIMEDE				
NCSRD	ICROWD				
ERARGE	PRIGM				
ELBIT	RAM²				
RINA	SARA				
ICOM	SECAAS				
STAM	SECURAIL				
ERARGE	SENSTATION				
ICOM	SISC2				
TREE	TISAIL				

ICOM	UNI|MS
WINGS	WINGSPARK

OTHER : *(PLEASE SPECIFY)*

ANNEX VII. Joint Exploitation Questionnaire

Please fill in the table below indicating your interest in participating in the exploitation of the S4RIS platform. You only need to wite Yes or No to express your interest or lack thereof.

Partner name	Partner acronym	Partner wants to have share of the IPR of the S4RIS platform	Partners wants to exploit the results/license for education purposes	Partner is interested to participate in the commercialisation of the S4RIS platform	Partner is interested to commercialise its tool/component	Representative of the partner for the joint exploitation approach (member of Exploitation Coordination Committee)
		YES/NO	YES/NO	YES/NO	YES/NO	Email address

ANNEX VIII. Exploitation Agreement Template

JOINT OWNERSHIP AGREEMENT

[*Full legal name of the Party*

and

[*Full legal name of Party*]

and

[Add as necessary]

This Agreement dated _____ 202[●] is between:

(1) [●] [an academic institution incorporated *or* established under [statute *or* charter in[..],] whose [principal address *or* registered office] is at [●] and

(2) [●] [a company *or* insert relevant entity type incorporated in [•] with registration number [•],] whose [principal place of business *or* registered office] is at [•].

(3) […]

Hereinafter collectively referred to as the **"*Parties*"**, or individually as **"*Party*"**.

WHEREAS:

A. The Parties are the beneficiaries of the H2020 Project for the action entitled "*Data-based analysis for SAFETY and security protection FOR detection, prevention, mitigation and response in trans-modal metro and RAILway networkS*" ("*SAFETY4RAILS Project*").
B. The Parties have signed the grant Agreement No 883532 (the "*Grant Agreement*") for the completion of the SAFETY4RAILS Project. The Parties have also signed the "*Consortium Agreement*" specifying and supplementing binding commitments among themselves in addition to the provisions set forth in the Grant Agreement.
C. As a result of their cooperation and their obligation under the Project, the Parties have jointly developed specific software and generated certain results stemming from the work carried out jointly **("*Jointly Owned Results*").** Pursuant to Article 26.2 of the GA and Section 8.2 of the CA, the Parties agree to sign the present Joint Ownership Agreement **(the "*Agreement*")** over the above-mentioned Jointly Owned Results.

The Parties agree as follows:

1. Jointly Owned Results

1.1 In the context of the SAFETY4RAILS Project, the Parties hereto have jointly developed the following Joint Results:

1.2 [List specific items of jointly owned IP that has been generated in the project and is subject to this agreement]

2. Allocation of IP joint ownership

2.1 Each Party retains exclusive property of its background as defined in the GA and the CA.

2.2 The Parties agree that all intellectual property rights, including but not limited to patents, copyright, trademarks and trade secrets, derived or that may derive from the Jointly Owned Results of the Project in every jurisdiction.

2.3 The intellectual property rights shall be jointly shared between the Parties [in common in equal shares/or owned in shares according to their share of contribution in person months in the project/costs/background provided to the project (or however joint ownership over joint results is agreed)].

2.4 Clause 1 sets out the specific list of Jointly Owned Results in existence at the date of this Agreement. [Any jointly owned results created after the date of this Agreement may be added to this Agreement by way of an addendum in writing signed by the Parties – to be agreed and confirmed].

3. Improvements, updates and modifications

3.1 The Parties shall have the right to perform improvements, updates, upgrades and/or modifications to the Jointly Owned Results.

3.2 [Any improvements, updates and modifications made to such Jointly Owned Results after shall be owned by the Party making such improvements, updates and modifications – to be confirmed or agreed otherwise by the parties].

4. Rights of use

4.1 **Background** [amend clauses below as necessary]

4.1.1 Each Party hereby grants to the other Party the non-exclusive right to use its background free of charge, but only as strictly necessary to perform the joint ownership hereof.

4.1.2 Each Party hereby grants to the other Party a non-exclusive, royalty-free, non-transferable right to use its background, but only as strictly necessary to enable the other Party to exploit the Jointly Owned Results within the scope of its business activity.

4.1.3 No right to use any background is granted by one Party to other Parties out of the scope of this Agreement.

4.2 Jointly Owned Results

4.2.1 [Each Party shall have an unrestricted right to use the Jointly Owned Results.

OR

Each Party shall be entitled to use the Jointly Owned Results only as strictly necessary to [describe the allowed use]

OR other agreement by parties];

5. Rights of exploitation [choice of options – to be agreed by the parties]

[first option -consent required]

5.1 A Party shall not pledge, assign and/or sell Jointly Owned Results to third parties without the other Parties' prior written consent.

5.2 Licensing of Jointly Owned Results to third parties shall require written agreement between the Parties, setting out their respective rights and obligations, including but not limited to, the distribution of licensing costs and income.

[second option -consent not required]

5.1 Each Party shall have the right to license Jointly Owned Results to third parties without prior written consent from the other Parties.

5.2 The total income after deducting costs as derived from the licencing of the Jointly Owned results shall be distributed […%] to Party […] and […%] to Party […]. According to the type of license granted, said distribution ratio may be adjusted upon written agreement by the Parties.

6. Dissemination

6.1 If a Party intends to publish information and other research materials related to the Jointly Owned Results, such a party shall, prior to publication, provide […] days as examination period for the other Parties to verify whether the contents of such dissemination disclosed should be kept confidential.

7. Confidentiality

7.1 The Parties shall keep secret all non-public information, matters and materials related to the Jointly Owned Results including, but not limited to, know-how, trade secrets, vendor or supplier information, operational methods, products or product development, processes, product specifications and formulations, designs, graphics, (collectively, the "***Confidential Information***").

7.2 Confidential Information shall not be disclosed, copied, reproduced, or otherwise made available to any other third party without the consent of the other Parties. Each Party agrees to use its best efforts to maintain the confidentiality and to keep data and research materials confidential until published or until corresponding patent/trademark/copyright applications are filed.

7.3 Confidentiality obligation shall expire at the earlier of the date when the information is publicly known or […] years after the expiration or termination date of this Agreement. Each Party may request an extension to this term when necessary to protect confidential information relating to foreground not yet commercialised.

8. Protection of intellectual property rights

8.1 The Parties shall decide, by mutual agreement, whether to file, prosecute and maintain intellectual property protection of the Jointly Owned Results. The Parties shall equally bear all costs resulting from these acts.

8.2 The Parties shall agree which Party shall conduct the activities thereof in the names of and on behalf of the Parties. The elected Party shall provide a copy of relevant documents relating to the activities thereof for the other Parties examination.

8.3 If a Party declines to bear its share of the costs associated with the activities thereof, the other Parties may conduct such activities in their own name and at their own expense. The declining Party shall retain its rights of use but shall lose its rights of ownership and exploitation in respect of results.

9. Intellectual Property Rights Infringement

9.1 Each Party shall be responsible for monitoring and defending the joint intellectual property. Each Party will, however, notify the other Parties promptly if it has a reasonable basis for believing that the joint intellectual property has been infringed by a third party or if it would infringe any intellectual property rights of a third party.

9.2 The Parties shall equally bear any costs in connection with the law prosecution of third parties infringement of the Jointly Owned Results.

9.3 The Parties shall equally bear any costs in connection with third-party claims alleging that the Jointly Owned Results infringe third parties' intellectual property rights.

10. Indemnity

10.1 Each Party (the "***Indemnifying Party***") shall indemnify and keep the other Parties harmless from and against any and all damages and losses arising out of any third-party claims alleging infringement of its intellectual property rights in connection with the background used by the Indemnifying Party to build the Jointly Owned Results.

11. Assignment of Jointly Owned Results

11.1 Except as expressly provided in this clause, neither Party may assign, sell or otherwise transfer any or all of its rights over the Jointly Owned Results without the prior written agreement of the other Parties.

11.2 Each Party shall procure that before it transfers or assigns its share to any third party, such third party shall enter into an agreement with the other Parties in this Agreement.

11.3 Subject to its compliance with this clause, each Party may assign ownership of its share of any Joint IP, to an affiliate without the prior agreement of the other Parties.

12. Duration

12.1 This Agreement shall, subject to early termination in accordance with clause 13, continue in full force and effect from the date of signature until the later of:

12.1.1. in the case of any registered intellectual property right granted in respect of the Jointly Owned Results, the expiry of that registered right; or

12.1.2. 10 years from and including the date of signature of this Agreement by the Parties.

13. Governing Law and Jurisdiction

13.1 This Agreement and any non-contractual obligations arising out of or in connection with this Agreement shall be governed by and construed in accordance with the laws of […] and each Party agrees to submit to the exclusive jurisdiction of the courts of […].

14. General

14.1. *Amendments.* This Agreement may only be amended in writing signed by duly authorised representatives of the Parties.

14.2. *Entire agreement.* This Agreement form the entire agreement between the Parties relating to the joint ownership of intellectual property rights and supersedes all prior oral or written agreements, arrangements, or understandings.

14.3. *Severability*. If the whole or any part of a provision of this Agreement is or becomes illegal, invalid or unenforceable under the law of any jurisdiction, that shall not affect the legality, validity or enforceability under the law of that jurisdiction of the remainder of the provision in question or any other provision of this Agreement and the legality, validity or enforceability under the law of any other jurisdiction of that or any other provision of this Agreement.

14.4. *Costs*. Each Party shall pay its own costs in connection with or incidental to the preparation, negotiation and execution of this Agreement.

14.5. *Announcements.* Neither Party shall make any press or other public announcement concerning any aspect of this Agreement or make any use of the name of the other Party in connection with or in consequence of this Agreement, without the prior written consent of the other Party.

Agreed by the parties through their authorised signatories:

SIGNED For and on behalf of	**SIGNED** For and on behalf of
_____	_____
Signed	Signed
_____	_____
Name	Name
_____	_____
Title	Title
_____	_____

Date Date

SAFETY4RAILS

Partners:

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