SAFETY4RAILS

MARKET ANALYSIS AND BUSINESS PLAN

Deliverable 10.8

Lead Author : ETRA

Contributors: EOS, STAM, CURIX, TREE, ERARGE, LDO, WINGS, RINA, ELBIT, ICOM

Dissemination level: PU

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.

D10.8 MARKET ANALYSIS AND BUSINESS PLAN		
Deliverable number:	D10.8	
Version:	1.0	
Delivery date:	07/10/2022	
Dissemination level:	Public	
Nature:	Report	
Main author(s)	Eduardo Villamor Eva Muñoz	ETRA
Contributor(s)	Angeliki Tsanta Juliette Vieillevigne Davide Ottonello Philipp Sick Tatiana Silva Alper Kanak Claudio Porretti Andreas Georgakopoulos Fabio Bolletta Emiliano Costa Eli Ben-Yizhak Artur Krukowski	EOS EOS STAM CURIX TREE ERARGE LDO WINGS RINA RINA ELBIT ICOM
Internal reviewer(s)	Stephen Crabbe Antonio de Santiago Laporte (Security Assessment)	Fraunhofer MDM
External reviewer(s)	Jeroen van de Tweel	PRO (not closely involved in deliverable production)

Document control			
Version	Date	Author(s)	Change(s)
0.1	17/08/2021	Eduardo Villamor	ToC release
0.2	24/08/2022	Eduardo Villamor	Section 3 and 4 draft
0.3	08/09/2022	Eduardo Villamor	Section 3 and 4 final contributions
0.4	15/09/2022	Eduardo Villamor	Updates on section 3,4. Section 2 finalised
0.5	18/09/2022	Eduardo Villamor	Section 1, 5 and 6 finalised
0.6	03/10/2022	Eduardo Villamor	Comments implemented after internal review. Ex. summary and Glossary added
1.0	07/10/2022	Stephen Crabbe	Creation of V1.0 from V0.6. Update of this table, footer 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 wil be validated by two rail transport operators and the results will support the re-design of the final prototype.

TABLE OF CONTENT

List of tables

List of figures

Executive summary

Thorough market and business analyses provide key information to describe the Go-to-Market Roadmap of any business initiative. In this deliverable, the market landscape is researched in order to identify the structure, segments, size, trends and expected growth, providing the necessary information to define the SAFETY4RAILS position in the market. Based on this, business models for each of the core Key Exploitable Results (KERs) have been defined, not only for the invididual tools but also having a dedicated emphasis on the commercialisation of the S4RIS platform. The outcomes provide they key strategic and financial indicators to perform the next steps after the project and to progress towards achieving the commercialisation of the results.

The work performed in this deliverable fall under the scope of **T10.5: Business Plan and Exploitation, IPR**, where a strong collaboration between the corresponding subtask took place for the whole task runtime. The exploitation strategy defined in D10.9 was continuously mapped into the definition of the Business Plans in this document.

After an introductory chapter, Section 2 addresses the methodological framework followed to complete all business models. Section 3 presents the market analysis performed to characterise the market landscape and define the main opportunities for the commercialisation of the KERs. This section also provides the position of the project solutions in the market, where these solutions may support the creation of new markets, as well as a competitive benchmark analysis.

In Section 4, emerging business models for each of the core KERs were produced following a Business Model Canvas, an in-depth risk assessment and a financial analysis in optimistic and pessimistic conditions. Based on these, Section 5 reports the S4RIS platform business plan for taking the main project result to the market.

The market and business analyses produced as part of this report should be periodically updated after the project as the KERs approach the commercialisation phase.

1. Introduction

1.1 Overview

This document present the results of **T10.5.1 Market analysis and Business Plan**. The main objective of this deliverable is to define the core mechanisms and strategies to commercialise the Key Exploitable Results (KER) developed by commercial partners.

An assessment of the market landscape of railway security is required to determine size, structure, trends, drivers, economic growth and competitors in the sector. Such information provides the necessary inputs to build the commercialisation strategy, including which geographical, technological, subsector, etc… market segments are more promising than others, as well as the value added by each technology to the market. A competitive benchmark analysis has been performed, as part of the market analysis and as a fundamental step for the definition of the value proposition – What do we offer to the customers that others cannot?

Emerging business plans based on the KERs developed by commercial partners have been designed to be fully materialised within 5 years after the project end. The Business Model Canvas (BMC) was used to define each partner's business strategy. As a result, the business plans outline how to exploit these results in terms of economic return, considering the different national conditions of each partner and the most relevant risks to achieve commercialisation. For this, a strong collaboration was established with **T10.5.2 Exploitation strategy** to align both the exploitation roadmaps and the business plans. The main outcome is the S4RIS platform business plan, which builds upon the business plans of each contributory tool. End-users feedback from the Simulation Exercises developed in WP8 was embedded in the definition of the individual business plans, as well as the S4RIS platform business plan.

An Intellectual Property Right (IPR) repository was developed in close collaboration with T10.5.2. The repository tool was employed as a screening system to review the project's technical advances and define the necessary IP protection policies. The final version of the repository will be reported within **D10.9: Exploitation Strategy.**

1.2 Structure of the deliverable

This document includes the following sections:

- Section 1: Introduction. An overview of the deliverable is provided, including the main objectives behind it and the relevance for the next steps after the project.
- Section 2: Methodology for SAFETY4RAILS business plans development. This section describes the process used to develop the business plan for all KERs developed by commercial partners, as well as the S4RIS platform.
- Section 3: Market Analysis. The market landscape relevant to the project is introduced in this document, together with the positioning of the KERs developed in the primary market segments, and a competitive benchmark analysis.
- Section 4: Emerging Business Plans from commercial/business partners. In this section, the value proposition, business model canvas, risk and mitigation measures and a financial analysis is performed for each of the KERs to evaluate the viability of the business plan.
- Section 5: S4RIS business plan. As for the previous section, a full business plan is produced for the SAFETY4RAILS Information System.
- Section 6: Conclusions.
- ANNEX I. GLOSSARY AND ACRONYMS
- ANNEX II. CASHFLOW EVALUATION TEMPLATE

2. Methodology for SAFETY4RAILS business plans development

The SAFETY4RAILS business plans have been developed, refined and finalised according to a series of steps contributed to by the commercial partners. The core input considered was the IP foreground and exploitation strategies developed in the context of D10.9: Exploitation Strategy. The Key Exploitable Results (KERs) from commercial/business partners, defined in the same deliverable, were considered as the main subject of the business plans. Business plans of the KERs developed by academic/research partners were not included, since technology transfer to industry is required and the selected industrial organisation should be engaged in the definition of such business plans. The S4RIS platform business plan takes input from all the business plans elaborated in this document, as well as considers the joint exploitation roadmap described in D10.9. The following steps were carried out:

1. Characterisation of the KERs (collaboration with D10.9)

Characterisation of the KER is performed to understand the exploitation roadmap, the market where the KER is expected to be introduced, and the Go-to-Market Strategy. For what concerns this deliverable, the questionnaire presented in Table 1 was circulated among partners.

TABLE 1 KER CHARACTERISATION QUESTIONNAIRE

KER NAME	
Unique Selling Point USP - Unique Value Proposition UVP	*Describe the competitive advantages, the innovative aspects. What does your solution do better, what are the benefits considering what your user/customer wants, how does your solution solve his/her problem better than alternative solutions, what distinguishes the KER from the competition / current solutions?*
"Market" – *Target market*	*Describe the market in which your product/service will be used/can "compete", answering the following questions:* *- What is the target market?* *- Who are the customer segments?*
"Market" - Competitors	*Who are your "competitors" (note: they are the ones offering "alternative solutions")?*
Go to Market – Use model	*Explain what is your "use model", how the KER will be put in use (made available to "customers" to generate an impact). Examples of use models: manufacturing of a new product, provision of a service, direct industrial use, technology transfer, license agreement, contract research, publications, standards, etc.* *Note training is a service.*

2. Business Plan Development

For each commercial/business partner owning a KER, a draft Business Model Canvas was produced with the information from the previous step. Based on this draft, the partners completed the Canvas by answering the following questions:

- **Customer Segments.** Who are your customers? Describe your target audience in a couple of words [Described in more detail in Section 3.4.1.]
- **Channels.** How are you going to reach your customers?
- **Customer Relationships.** How often will you interact with your customers?
- **Key Partners.** What are your key partners to get a competitive advantage? [Described in more detail in Section 3.4.2]
- **Key Activities.** What are the key steps to move ahead with your customers? This is based on the exploitation roadmap reported in D10.9.
- **Value Propositions.** How will you make your customers' life happier?
- **Key Resources.** What resources do you need to make your idea work?
- **Revenue Streams.** How are you planning to earn money (e.g. revenues from sales, fees for commercial use by third-parties, consultancy, training, etc…)
- **Cost Structure.** What are you planning to spend on product development and marketing (e.g. Personnel costs for R&D, sales & marketing, customer support (including development, customization, training, consultancy, technical support) and management teams, licenses, Cloud/server hosting, etc…)?

Section 4 and 5 provides the final version of the business plans for all Key Exploitable Results, developed by business/commercial partners, and the S4RIS platform plan agreed by the consortium. The final versions presented consider the findings from the simulation exercises and the end-users evaluation.

3. Risk Assessment

Risk Assessment Maps are provided in Section 4 and 5, corresponding to each of the main SAFETY4RAILS results. The description of risks included an assessment performed by the consortium on the degree of criticality of the risk related to the achievement of the commercialisation of the result, as well as the probability of the risk happening. A potential intervention to mitigate the risk is suggested, including the estimated feasibility of such intervention. Priority maps were then produced to show the results of the risk assessment scores calculated, where the following interpretation should be considered:

1) **No action** – risk severity is low, and no action is required,
2) **Control** – risk should be monitored in case external factors modify the initial assessment performed,
3) **Action** – Appropriate mitigations should be implemented to prevent obstacles in the market uptake,
4) **Warning** – Critical risk that could hinder market uptake.

4. Cost-benefit analysis and financial viability assessment

For producing a solid business plan, a cost-benefit analysis and a viability assessment need to be performed to understand the key financial indicators supporting the profitability of the product. This process is comprised of the following steps:

1. Identification of the activities associated to the use of the product that can provide **incomes to the end-users (benefits)**. For each of the activities, the additional incomes (€/year) are estimated based on the partner knowledge of the market and a series of assumptions.

2. **Price product calculation**. Based on the benefits provided to the end-users, the business partner sets the profit percentage (the price) for each revenue stream (e.g. licensing, direct purchase, yearly maintenance).
3. **Estimate cashflow** (after project finalisation – Year 0). Based on the activities and timeline defined in the exploitation strategy at D10.9, partners estimated the yearly investments required to take the solution to the commercialisation phase. Once this phase is reached (e.g. Y1-Y2), incomes and costs of the activities are estimated based on the revenue and cost structure defined earlier in the Business Model Canvas. This was done for: 1) an optimistic sales scenario, and 2) a pessimistic sales scenario, following the assumptions performed by each partner. The objective is to define a solid financial plan preventing the failure of the commercialisation phase even in the worst circumstances

For this step, each of the business partners national conditions are considered including local prices, market, early adopters and taxes. The template used to prepare the cost-benefit analysis and the financial viability assessment is reported in Annex II. Sales figures and price of the product are kept **strictly confidential** within the consortium to avoid any risks on each partner business strategy.

3. Market Analysis

3.1 Market Structure and Size

SAFETY4RAILS developed a resilience-oriented framework based on a set of technological solutions supporting rail and metro infrastructures against cyber, physical and combined cyber-physical threats. As such, SAFETY4RAILS targets the Global Public Transportation Market, and more specifically the **Global Rail Public Transportation Market**. Figure 1 provides a concise structure of the markets and subsegments addressed by the results developed in the project.

Global Public Transportation Market

The **Global Public Transportation Market** includes road, rail and others mode of public transport (water, cable car, etc…). The market was valued at €208.3B in 2021 and is expected to expand at a compound annual growth rate (CAGR) of 5.9% from 2022 to 2028[1]. Europe holds the largest share in the market with over 38%, followed by Asia (34%) and America (26%)[2]. Road transportation leads the ranking within the market segments, accounting for the largest share with over 55%, followed by the rail transportation with nearly 35% of market share. The rail segment is anticipated to reach a lucrative CAGR of 6.3% from 2022 to 2028.

Within this market, the main drivers were identified as follows[1]:

- Vast migration of population into urban areas, leading to the expansion of urban/metro cities
- Infrastructure development and technological advancements in bus rapid transit, metro, monorail and light rail transit
- Increasing preference for passenger cars and two-wheelers is restraining market growth

Global Rail Public Transportation Market

As the most relevant subsegment, the **Global Rail Public Transportation Market** is where SAFETY4RAILS is expected to generate a long-term impact. This market includes passenger rail transportation, rail freight medium-distance passenger transport, long-distance passenger transport, short-distance passenger transport, intermodals, tank wagons, freight cars, heavy rail and light rail. The market was valued at €79.2B in 2021[2] and is expected to expand at a CAGR of 9.1% from 2022 to 2028[3]. According to SCI of the global rail market[4], China leads the railway market, followed by USA, Russia, Germany, France, India, UK, Japan, Italy and Canada.

Within this market, the main drivers were identified as follows[3]:

- Increasing preference towards public transport
- Rising number of urban population
- Growing traffic congestion
- Improved infrastructure in public transport and intelligent transport solution

Major challenges ahead that restrict market growth are the following[3]:

- Increasing need of high-capital investment to improve existing transport
- Security concerns in public transport

---

[1] https://www.grandviewresearch.com/industry-analysis/public-transportation-market-report#:~:text=Report%20Overview,economic%20growth%20across%20the%20world

[2] https://www.statista.com/outlook/mmo/shared-mobility/shared-vehicles/public-transportation/americas?currency=EUR

[3] https://www.databridgemarketresearch.com/reports/global-rail-public-transport-market

[4] https://www.railjournal.com/in_depth/sci-study-forecasts-upturn-in-global-rail-market/

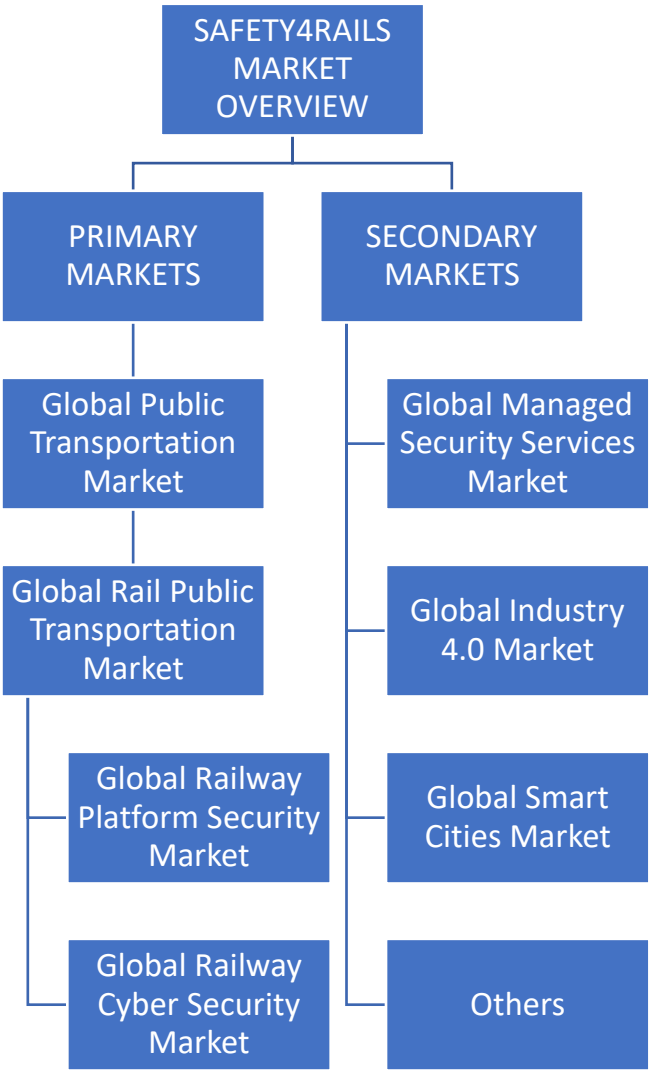

FIGURE 1: SAFETY4RAIL MARKET OVERVIEW

The Global Rail Public Transportation Market comprises the overall set of services and infrastructures existing in the railway sector, as described above. Some of the most relevant subsegments where SAFETY4RAILS is expected to generate an impact are outlined below:

- Global Railway Platform Security Market: The market is expected to grow from €1.7B in 2019 to €2.3B by 2024, at a CAGR of 5.9% in the same period[5]. The market segmentation, based on components, is divided in: 1) Solutions – Sensors, video surveillance systems, platform edge doors, alert/alarm systems, etc…; 2) Services – Professional Services and Managed Services. Asia-Pacific accounted for the largest share in the market with 36.66%, followed by Europe (30%) and North America (23.33%). The main market drivers are:
    - Increasing suicide instances
    - Growing need of minimising the risk of unauthorised access to platforms
    - Increasing demand for advanced solutions for security management

[5] https://www.marketsandmarkets.com/Market-Reports/railway-platform-security-market-116139286.html

- Global Railway Cyber Security Market: The market is expected to grow from €9.8B in 2021 to €16.7B in 2028, at a CAGR of 8% in the same period[6]. The market segmentation based on components is divided into: 1) Network, 2) Application, 3) Data protection, 4) Endpoint protection and 5) System administration. The network security segment accounts for the largest share in the market with 33.33%, followed by the application segment (20.8%) and the data protection segment, which is expected to register a significantly high CAGR of 8.8%. With regards to the geographical segmentation, Asia-Pacific accounts for the largest share of the market with 35%, followed by Europe and North America. In Europe, the market is projected to grow at a fast pace with a CAGR of 7.2% in the forecasting period. The main market drivers are:
    - The European government and other private companies invest heavily in developing and enhancing railway infrastructures and systems.
    - Trade treaties have encouraged freight transportation and transnational trade between EU Members States, leading to increased cybersecurity sector.

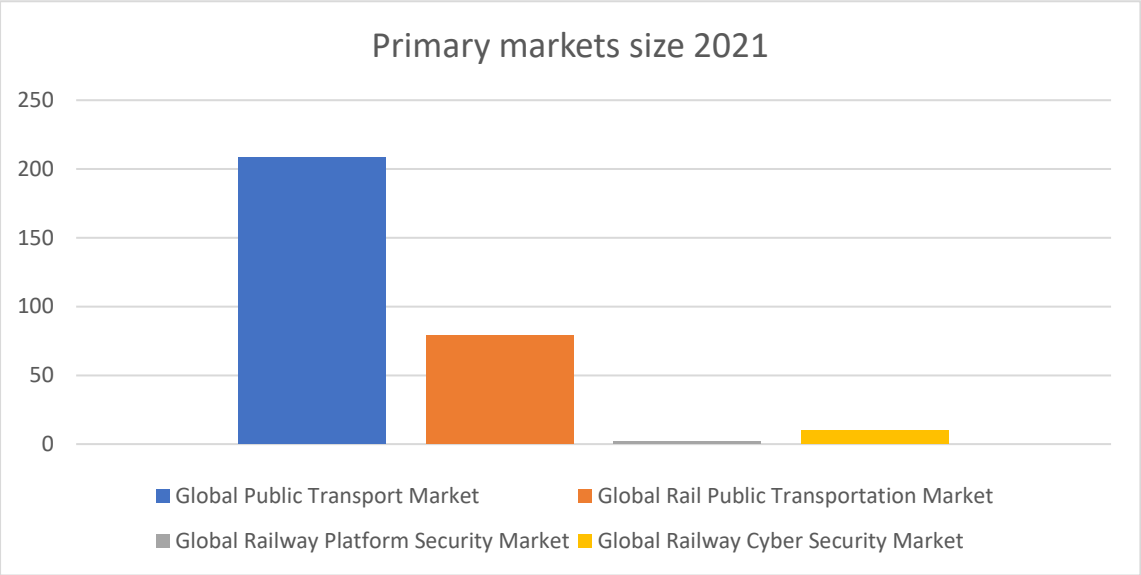

FIGURE 2: PRIMARY MARKET AND ITS SUB-SEGMENTS SIZE

While the first sub-segment focuses on physical security, the second sub-segment covers all the cybersecurity domain. Furthermore, it is to be expected that the project will contribute to the **creation of new markets** addressing the resilience and/or combination of cyber-physical elements in railway infrastructure, which is currently not tackled by the main market components.

Secondary Markets

On top of the primary markets addressed by the project, there are several other potential markets where the results could be easily exploited. In the following, the **main secondary markets** were identified by the project partners:

- Global Managed Security Services Market was valued at €22.45B in 2020, and is projected to reach €77B by 2030, growing at a CAGR of 12.8% during the forecasting period[7]. The market focuses on different applications including Managed Intrusion Prevention Systems and Intrusion Detection Systems, Distributed Denial of Services, Unified Threat Management, Secured Information and Event Management, Firewall Management and Endpoint Security. Such applications can be further segmented by Industry Verticals, including Banking, Financial Services and Insurance, Healthcare, Manufacturing, Retail, and IT&Telecom. Market growth is primarily driven by the following factors:

[6] https://www.fortunebusinessinsights.com/railway-cyber-security-services-market-103556
[7] https://www.alliedmarketresearch.com/managed-security-services-market

- Increase in cybercrime activities
- Cost-Effectiveness of Managed Security Services Providers

- Global Smart Cities Market was valued at €457B in 2021 and is projected to reach €873.7B in 2026, following a CAGR of 13.8% in the forecasting period[8]. The market definition focuses on Smart Transportation, Smart Buildings, Smart Utilities, and Smart Citizen Services. The main drivers are detailed below:
  - Concerns over the proliferation of environmental wastes
  - Increasing concerns over global warming and ozone depletion
  - Implementation of intelligent infrastructure automation, smart grids, and controlling systems
- Global Industry 4.0 Market was valued at €114.5B in 2021 and is projected to reach €377.3B by 2029, following a CAGR of 16.3% in the forecasting period[9]. The market includes the following vertical: Manufacturing, Energy&Utilities, Automotive, Oil and Gas, Aerospace and Defence, Electronics and Consumer Good. The main drivers are detailed below:
  - Increased adoption of industrial robots and surge in Industrial Automation Demand Drive

Partners have also expressed the potential contributions to other markets, but those with the highest consensus were included above. Other addressable markets may include: Telecommunications, Ports, Airports and other critical infrastructures.

3.2 SAFETY4RAILS positioning in the market

Within the market structure linked to the Global Rail Public Transportation Market, SAFETY4RAILS contributes with several Key Exploitable Results (KERs), as described in D10.9. The consortium analysed the fit of each KER in the scope of each of the markets analysed in Section 3.1 and produced the map in Figure 3.

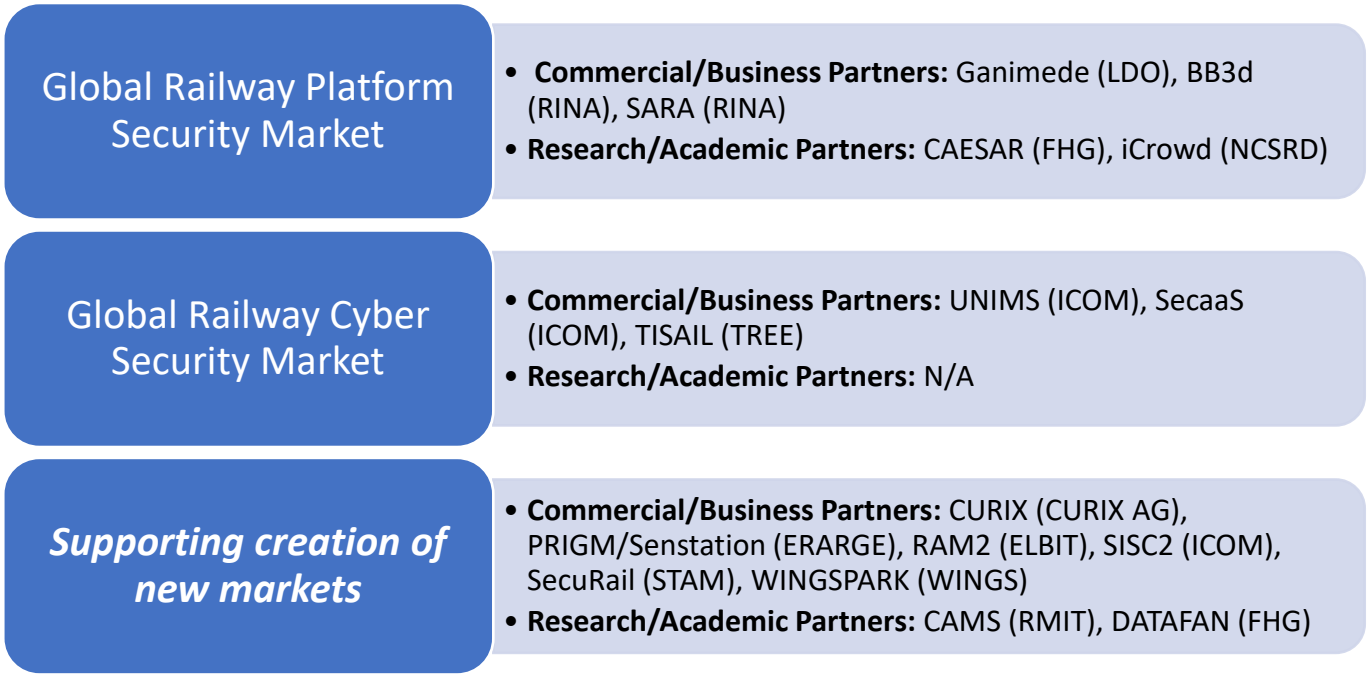

FIGURE 3: SAFETY4RAILS POSITIONING IN THE MARKET

[8] https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html#:~:text=What%20is%20the%20projected%20market,13.8%25%20during%20the%20forecast%20period
[9] https://www.fortunebusinessinsights.com/industry-4-0-market-102375

In this process, it was identified several results that do not fit in neither of the existing market, to the best of our knowledge. Such results tackle both cyber and physical threats/events, as well as their combination, therefore supporting the creation of new markets associated to this concept. Of course, the SAFETY4RAILS Information System (S4RIS), where all tool providers contributed, would also contribute in this sense.

3.3 Competitive benchmark analysis

This chapter aims to provide a comprehensive benchmarking analysis of the main competitors relevant to SAFETY4RAILS KERs, defined in D10.9, and highlight the differences and innovative features of the SAFETY4RAILS solutions. Competitors were identified based on tool providers expertise.

In general, the analysis performed below highlights that most of the tools are innovative or even pioneers in the field. All tools have been developed according to the requirements formalised as part of WP1 with input from WP2 in the earlier phases of the project, expanding their capabilities and automating existing ones to support cyber-physical resilience.

3.3.1 SecuRail – STAM SRL

Potential market competitors to this KER were investigated in detail, where the most relevant are described below:

- **RATING (Engineering S.p.A.).** RATING is a risk assessment tool developed by Engineering S.p.A. during a European funded project which has the aim to support organizations to evidence-based risk profiles. This software aims to identify and classify the most common cyber-attacks, threat agents and their motivations to attack.
- **Rail Risk Toolkit[10] (Rail Safety and Standards Board).** The Rail Risk Toolkit is a collection of tools which have been developed to support the rail industry in Great Britain. Among various tools which comprise this collection there are: the Safety Risk Model, the Risk Assessment Support Service, the Risk Profile Tool, and the Taking Safe Decision Analysis Tool.
- **RAMs App[11] (BeAccreditedGroup).** RAMs App is cloud-based software that allows the user to carry out various task ranging from risk assessment COSHH assessments and staff training. Concerning its application on the railway sector it has been applied to activities ranging from repair to installation.

They are proposing alternative risk management digital solutions and some of them are focused on railway domain. Unlike STAM, they are large companies with several resources and used to launch products on the market. However, SecuRail is capable of carrying out analysis tailored on peculiarities of the network, like the geographic position and real-time data, and infrastructure that traditional tools based on questionnaires and inventory cannot offer.

3.3.2 CURIX – CURIX AG

Potential market competitors to this KER were investigated in detail, where the most relevant are described below:

[10] Rail Risk Toolkit https://www.rssb.co.uk/safety-and-health/improving-safety-health-and-wellbeing/rail-risk-toolkit

[11] RAMs App https://www.rams-app.co.uk/rail-works-risk-assessment-software

- Tanium - is a platform that delivers complete, accurate and real-time endpoint data regardless of scale and complexity. It converges IT management and security operations under a single platform, providing the capabilities of identifying low-level system risks / vulnerabilities as well as providing real-time visibility over every IT infrastructure endpoint.
- Bigpanda – is an AIOps platform that aggregates, normalises, and enriches events collected from other tools and turns it into actionable insights with the use of AI. It also provides threat-hunting analysis capabilities such as visualizing the incident progression and Level-0 automation to allow workflow automations for faster responses.
- Dynatrace – is an all-in-one platform that delivers observability capabilities (metrics, logs, traces), application security, Cloud Automation and AIOps capabilities. It also provides a full topological model with contextual data and entity relationships.

Compared to traditional tools on the market CuriX® has a lot of strengths and advantages against the competitors: Detect the unknown Unknowns, Process Metrics, Logfiles and Traces (not only logfiles), Failure Prediction, Intelligence Alerting (Integration Target Systems), Agnostic (Multiple Data Sources), Enrichment Metadata (Linking Business Model and IT System Architecture), Zero Configuration Effort, Fully Automated Data Correlation and Causalities, Noise Filtering / Reduction, Root Cause Analysis, Determination Fault Locations, Heal Advice / Self-Healing (automated fault correction)[12].

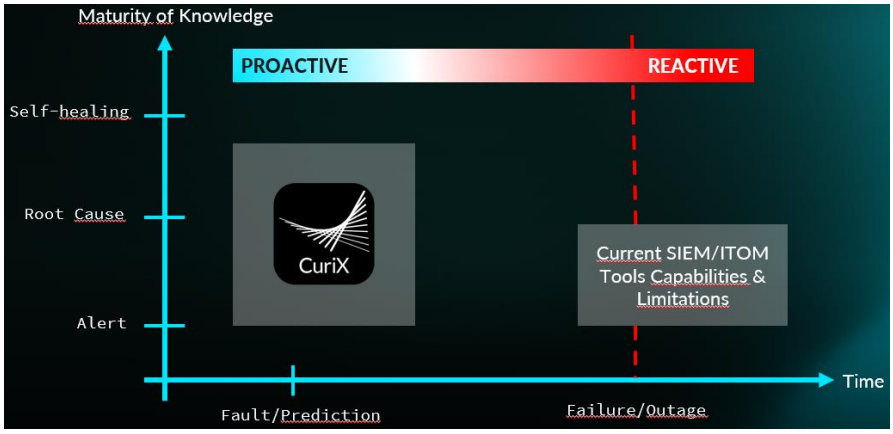

FIGURE 4: CURIX MARKET POSITIONING

3.3.3 TISAIL – TREELOGIC

Potential market competitors to this KER were investigated in detail, where the most relevant are described below:

- OTX Endpoint Security (Alien Vault). It enables private companies, independent security researchers, and government agencies to openly collaborate and share the latest information about emerging threats, attack methods, and malicious actors, promoting greater security across the entire community.
- Threat Intelligence Platform (INTSIGHTS). Continuously synchronize network and security solutions with the most up-to-date IOCs for faster incident response and threat workflows. Proactively research malware, TTPs, phishing scams, and other threat actors. Understand potential impact so to identify the gaps that carry the most risk.

[12] https://www.curix.ai/

- Other competitors: Karpersky and Decyfir. Besides there are threat intelligence platforms for cryptocurrency and blockchain, such as Chain analysis, CipherTrace,...but they do not cover the TISAIL functionality.

The existing related services are services on Threat Intelligence in general, not customised for the railways sector. TISAIL is focused on the railway operators and goes deeper understanding their problems and possible vulnerabilities in their systems.

3.3.4 PRIGM&Senstation – ERARGE

Potential market competitors to **PRIGM** were investigated in detail, where the most relevant are: Utimaco GmbH, Thales e-Security, Futurex, Gemalto, IBM, Hewlett Packard Enterprise, Yubico, and Ultra Electronic.

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". It is expected that PRIGM can become a "Cash Cow" throughout or early after SAFETY4RAILS because the underlying techniques are patented worldwide and promoted in top scientific conferences and journals so far. For the list of the patents visit http://ergtech.ch/research.html.

Potential market competitors to **Senstation** were investigated in detail, where the most relevant are: Equinix (Smart key, BIG-IP), Yubico (YUBIHSM 2), nCipher (nShield), Gemalto and recently Thales (SafeNet), Atos (Horus), Utimaco (CryptoServer, SecuritySErver, TimeStampServer), SPYRUS (Rosetta Spycos), IBM (Cloud Hardware Security Module 7.0). These companies collaborate with big organisations like Bosch, Siemens, and GE to integrate their HSM with their secure gateways. There is a trend to use secure gateways for the automotive industry where reliable CAN-Bus communication is settled.

ERARGE's Secure Gateway, when considered with PRIGM, presents a general purpose and high-throughput secure communication for IoT, cloud and edge interfaces. It is compatible with all wired and wireless interfaces and can be used as a fast smart meter as well. This makes Senstation and PRIGM an integrated cyber-physical security platform, which is currently something not offered by the competitors mentioned above.

3.3.5 Ganimede – Leonardo

Potential market competitors to **Ganimede** were investigated in detail, where the most relevant are:

- BriefCam – Video content analytics platform making video searchable, actionable and quantifiable. Review hours of video in minutes; respond to critical situational changes in the environment; and quantitatively analyze video to derive actionable insights for data-driven safety, security and operational decision making.
- innoVi (Agent Vi) – Provides a set of video analytics capabilities for enhanced security, safety and business operations, such as real-time detection of events of interest, rapid search and analysis of recorded video, and extraction of statistical data. Available as a cloud-based SaaS or as an on-premise software.

The most important advantages of Ganimede solution are:

- **capability:** multiple analysis can be performed on the same stream simultaneously (complex algorithms can also be applied)

- **scalability:** increase the analysis capability only adding new algorithms and business logic in the central platform without any intervention on site
- **flexibility:** the same algorithms for CCTV of different brands and streaming from different sources (video recorder, broadcasting, …)
- **easiness:** central configuration and maintenance, one system to know (different brands for cameras, different configuration modes, …)
- **reliability:** servers in data center allow high levels of availability, reliability and scalability
- **investment saving:** exploitation of existing cameras safeguarding investments in security systems

3.3.6 WINGSPARK – WINGS

Competitors offer solutions that leverage on the IoT and AI. Their strength relies on the fact that most commercially available solutions focus and are tailored for a specific domain, but they cannot be applied in the same manner in another domain. On the other hand, WINGSPARK+ provides an abstraction layer in order to accommodate assets coming from different infrastructures similarly.

3.3.7 BB3d – RINA

The competitors include all institutions that are capable to use software to perform blast analysis and assessment. These institutions include the software houses which develop and offer blast design related services, specialised companies (e.g. consulting firms) and professionals.

The strengths of those using advanced solutions and software such as hydrocodes include the production of detailed results for a very large type of blast scenarios accounting for the effect of complex physical phenomena (i.e. containment and multi-reflections of different blast wave fronts). The main disadvantages include the high costs related to software licenses, machines, skilled users required to set up the case, run simulations and assess results. Moreover, the activities envisaging the use of these computational means are characterised by a longer time and much higher costs.

3.3.8 SARA – RINA

To the best of the knowledge of the partners responsible for this innovation, there is no available similar solution in the market yet. This is a pioneering solution that can solve a very specific problem, having the advantage of considering all the three main aspects of the loss, such as direct, indirect, and people losses.

3.3.9 RAM2 – ELBIT

Common solutions in the OT market are usually IDS products, which are focused on monitoring of the network traffic and deep packet inspection. These solutions are mainly reactive and limited by visibility. RAM2 is an orchestration platform that has some overlapping with IDS solution (although not covering all DPI capabilities), but integrate with multiple data sources (including IDS solutions) to provide maximum visibility into the operational network, focus on the operational team as stakeholders rather than cyber security experts alone, assess risk and add operational context for better decision making.

3.3.10 UNIMS & SISC2 & SecaaS – ICOM

Potential market competitors to **UNIMS** were investigated in detail, where the most relevant are described below:

- Cloud and Network Management (CISCO). It offers a single, unified solution provides wired and wireless lifecycle management, and application visibility and control. It also offers policy monitoring and troubleshooting with the Cisco Identity Services Engine and location-based tracking of mobility devices with the Cisco Mobility Services Engine. It allows to manage the network, devices, applications, and users – all from one place. However, it is explicitly managing CISCO products, hence not directly applicable to 3rd-party network products, unlike UniMS that can integrate network management of any commercial networking component.
- OpManager (ManageEngine), is an easy-to-use, and affordable network monitoring solution. It monitors network devices such as routers, switches, firewalls, load balancers, wireless LAN controllers, servers, VMs, printers, storage devices, and everything that has an IP and is connected to the network. It continuously monitors the network and provides an in-depth visibility and control over it. In case of a fault, it can easily drill down to the root cause and eliminate it before operations are affected. With over 2000 built-in network performance monitors, monitor health and critical metrics such as packet loss, latency, speed, errors and discards, and analyse performance bottlenecks.

UniMS redefined Network Management, unlike its competitors, addressing the main challenges faced by carriers and operators, such as plethora of technologies, convergence of networks and the ever-increasing demand for complex services - and seek for an all-in-one solution to replace existing management silos efficiently and cost-effectively. Third-party network elements can be managed through element mediation drivers that can be developed as a service. The uni|MS™ unifies the management of access and transport networks, improving user experience, lowering OpEx and improving efficiency.

Potential market competitors to **SecaaS** were investigated in detail, where the most relevant are described below:

- Cloud Access Security Broker (Oracle). This product was the first on the market to automate the entire security lifecycle, from preventative measures to detection and remediation. The CASB solution covers cloud security, user behaviour analytics, and shadow IT discovery. The Oracle Security and Identity Cloud also offers a web application firewall, identity and access management, identity cloud services, and key management.
- Identity and access management (Okta). Okta focuses on the identity and access management (IAM) aspect of cloud security. Part of their mission is to “grant people access to applications on any device at any time, while still enforcing strong security protections. Okta’s single sign-on solution uses Security Assertion Markup Language 2.0, Secure Web Authentication, or OpenID Connect to validate log-in credentials and let users securely access any application with a single username and password. Okta provides strong central administrative features, so IT managers can set custom policies and report on usage, as needed. They also offer one of the broadest integration networks in the industry, so you can add SSO capabilities to about every application imaginable — whether cloud or desktop.
- NTT | Application Security (Synopsys) provides complete web application security at a high scale and level of accuracy, helping businesses to find and remediate weaknesses before the bad guys can exploit them. NTT Application Security embeds security throughout the software development lifecycle (SDLC), while reducing threats and costs to enable faster deployment of new business capabilities. Our solutions work across departments to provide faster turnaround times, near-zero false positives, and precise remediation plans.

The emphasis of SecaaS is given on high-standard security methods, which guarantee that any customer will safely adapt to the new era and realize his/her plans for an efficient transition to Cloud. SecaaS provides 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.

Potential market competitors to **SISC2** were investigated in detail, where the most relevant are described below:

- Wide Area Surveillance Platform (Thales) *"provides the key to ensuring that intrusion threats to base perimeters are detected and communicated as early as possible in order that appropriate responses can be initiated. It features 360° coverage, 24 hours a day and in all weather conditions, self-contained system that can be deployed for over 30 days without re-supply, mast-mounted optronic sensor head (TI camera, TV camera, Laser Range Finder and Laser Pointer) cued by a detection sensor for automatic threat alerting, detection sensors (radar, acoustic or visual), automatic information on position and bearing, rugged control suite capable of being remote from the system, control suite includes displays for imagery and Geographical Information System (GIS)"*, as described in their website[13].
- Smart Perimeter (Johnson Controls). Offer everything from access controls to intruder prevention, from video surveillance to cybersecurity. From alarms to video surveillance to access management, everything in the security ecosystem is as reliable as the equipment they use. Johnson Controls' products enhance the safety from visitor management systems, remote surveillance, and complete alarm control to monitor and control facilities.

Intracom Telecom 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 3rd party applications to produce meaningful intelligence[14]. As compared to other competitive solutions, it avoids false positives caused by detection of threats from multiple overlapping security cameras and other sensors, allowing to reliably categorise, track and assess risk for vast number of threats simultaneously, with soft handover among dispersed sparse security sensors.

3.4 Stakeholders' analysis

In this section, the deliverable reports an analysis of the main stakeholders involved in the SAFETY4RAILS results commercialisation. The analysis was performed on the basis of the commercialisation strategy elaborated by each business partners, and formalised later in the Business Model Canvas at Section 4.

3.4.1 Customer segments

The primary customers are **Railway Infrastructure Managers**, as the train operating company and part of the Global Public Rail Infrastructure Market. To understand the size of these customers per country in Europe, the number of rail passenger transports in 2020 was considered[15]. In this sense, France leads the ranking with 88.3B passengers (calculated as passengers times kilometres travelled), followed by Germany with 77B, Ukraine (53.1B), UK (51.8B) and Italy (47B)[16]. If metro transport is specifically considered, Germany stands as the country with the largest number of cities with metro coverage (21), followed by Spain (9), Italy (8) and France (7)[17]. In terms of rail freight transport, Germany leads the ranking as well with 108 billion tonne-kilometres in 2020, followed by Poland (50), France (30), Sweden (22), Austria (20) and Italy (19)[18].

The needs of these customers were collected in WP2 and formalised across the various deliverables reported in the same work package in the form of requirements. To address their needs properly, the main roles and

[13] https://www.thalesgroup.com/en/worldwide/defence/wasp-wide-area-surveillance-platform
[14] https://intracom-telecom.com/en/products/ict_services_solutions/sis/cip.htm
[15] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20210329-1
[16] https://www.worldatlas.com/articles/highest-railway-passenger-traffic-in-the-world.html
[17] https://mapa-metro.com/en/Europe/
[18] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Railway_freight_transport_statistics

performers should be considered: The Security Operations Centre, Station Manager, Operational Control Centre and Asset Management Department.

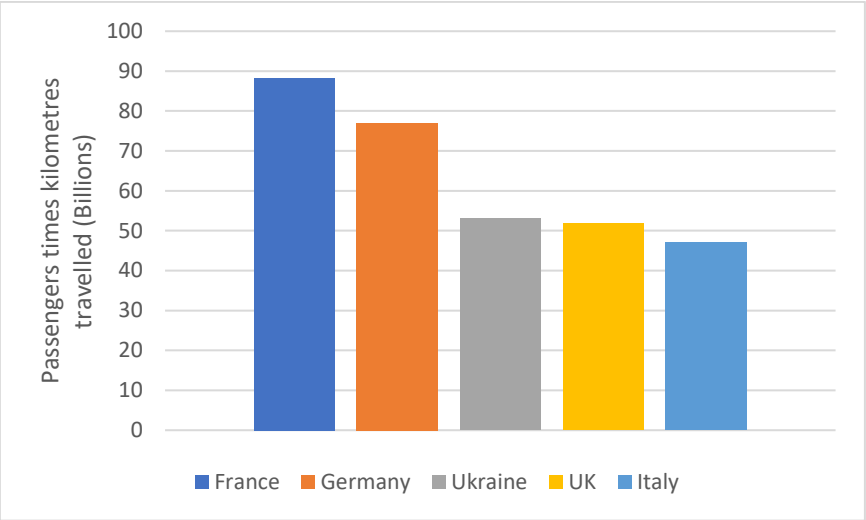

FIGURE 5: NUMBER OF RAIL PASSENGER IN EUROPE

Even though Railway Infrastructure Managers are the primary customers of the S4RIS, and the individual components, there are potential adaptations and extensions that can be made to make the results marketable to other customers, such as **other transport operators** (e.g. buses companies, ports, airports, etc…) **and other critical infrastructure operators** (energy, banking, health, telecommunications, etc…).

As a matter of fact, more than 55% of all public transport journeys in the EU are made by urban and sub-urban buses[19]. Germany accounts for the largest share of bus travellers, with more than 5.5M in 2019, followed by Poland (4.1M), Hungary (1.6M) and Romania (1.5M)[20].

3.4.2 Key partners

The identified key partners as part of the commercialisation strategy of the SAFETY4RAILS Key Exploitable Results are the following:

1) **System Integrators** with established commercial agreements with railway and metro infrastructures, who are willing to include one or more tool components into the overall railway system. Relevant system integrators include major players such as MTR Corporation, Atos SE, FREQUENTIS. A licensing agreement is expected to be established with such entities to expand the customer base.
   Business partners with related expertise in the sector, including cybersecurity, physical security and railway operations, who are willing to contribute with their related knowledge and participate in a joint venture.
2) **Regulatory experts** supporting GDPR compliance, IP protection, better understanding the regulatory landscape as well as the certification and compliance schemes required.
3) **Cloud hosting service provider** will support deployment of the SAFETY4RAILS results, enabling cloud-based storage and computation.

[19] https://www.acea.auto/fact/fact-sheet-buses/
[20] https://www.nationmaster.com/nmx/ranking/passengers-travelling-by-buses-and-coaches-in-transport

These stakeholders, mainly 1) and 2), are interested in increasing their margins and reach new market segments within the Global Rail Public Transportation Market.

As discussed, the results produced by the project will open new opportunities in the context of cyber-physical resilience and are expected to contribute further to the economic growth of the market. On the other hand, the funding received by the EC and the validation steps already performed in SAFETY4RAILS project are expected to support the technical and commercial credibility of the solutions and boost the interest from these key partners. For these reasons, a swift engagement of the relevant stakeholders towards market uptake is to be targeted.

4. Emerging Business Plans from commercial/business partners

A business plan comprises a documented strategy for a business to achieve a set of goals based on actionable plans. In this section, the KERs defined in D10.9 are analysed from a commercial and financial point of view. More specifically, the task focused on the KERs developed by commercial/business partners since these are the partners whose objective is to make profit. The business plan related to the S4RIS platform, which includes KERs from research/academic partners, is reported in Section 5.

4.1 STAM SRL - SecuRail

4.1.1 Value proposition

SecuRail 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.

Furthermore, SecuRail aims also at implementing dynamic risk analysis to support infrastructure managers according to real-time alerts delivered by sensors.

4.1.2 Business model canvas

<table>
<tr>
<td rowspan="2">Key Partners
- Business partner – cybersecurity company, for Joint Venture
- Legal entities -> how functionalities could contribute to certification and compliance
- System integrator -> to include SecuRail into the overall system of the railway</td>
<td>Key Activities
- Improvements on robustness and reliability of results
- Perform demos/workshops
- Define a final go-to-market strategy</td>
<td rowspan="2">Value Propositions
SecuRail 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.</td>
<td>Customer Relationships
Customisation, updates in software, technical support, training.
Already under discussions with major players in Italy (railway and metro)</td>
<td rowspan="2">Customer Segments
Large railway infrastructure managers. Security Department
Large metro infrastructure managers. Security Department
Customer Needs
- Automated, easy and faster risk analysis processes
- Quantitative indicators for risk
- Automatic generation of reports (risk register)</td>
</tr>
<tr>
<td>Key Resources
- IPR expertise
- Legal consultancy
- Access to various data sources from railways
-Cloud or service hosting infrastructure
- Marketing and commercial expertise</td>
<td>Channels
- Direct sales exploiting STAM network
- Sell together with a business partner, including other components such as asset management (Joint Venture)
- Technical support, customisation, maintenance, training</td>
</tr>
<tr>
<td colspan="3">Cost Structure
- Personnel cost for further R&D
- Personnel costs for sales&marketing
- Cloud hosting
- Management teams
- Personnel costs for development and deployment
- Royalties from embedding SecuRail with business partner large platform</td>
<td colspan="2">Revenue Streams
- 1) Direct sales: Upfront fee + subscription fee (maintenance+improvements)
- 2) Sales through joint Venture: Upfront fee + subscription fee (maintenance+improvements)
- Technical support, training
- Delivery of consultancy about risk assessment (without purchasing the tool)</td>
</tr>
</table>

FIGURE 6: SECURAIL BUSINESS MODEL CANVAS

4.1.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partners break out and create competitive products	*7*	*2*	**14**	Have strong legal support to define the agreement for collaboration	*8*	**Control.**
2	Disagreement on joint business model	*6*	*3*	**18**	Regular meetings to define and agree on the terms of the joint business model for each partners	*7*	**Control.**
Technological Risk Factors							
3	Significant dependency on other technologies.	*6*	*9*	**54**	Develop stand-alone software modules based on proprietary technologies	*7*	**Action!**
4	Result aiming at replacing existing status-quo	*8*	*8*	**64**	Highlight benefits for end-users and provide support for the whole risk analysis process	*8*	**Action!**
Market Risk Factors							
5	Nobody buys the product. Too expensive.	*9*	*6*	**54**	Think about alternative business models	*5*	**Between Action & Warning**
6	Nobody buys the product. Rejected by end-users.	*9*	*7*	**63**	Spot the light on end-users' needs	*5*	**Between Action & Warning**
IPR/Legal Risk Factors							
7	Lack of definition of compliance and certification schemes	*8*	*9*	**72**	Request specific consultancies to obtain needed certification(s)	*8*	**Action!**
8	IPR issues between partners	*7*	*3*	**21**	Make IPR agreements	*8*	**Control.**
Financial/Management Risk Factors							
9	No adequate resources (human and/or financial) secured to make the next step toward exploitation	*6*	*6*	**36**	Revise resources involved within the company	*6*	**Control.**

10	Immature business plan	*7*	*5*	**35**	Revise business plan	*6*	**Control.**
Environmental/Regulation/Safety risks							
11	Product/service does not comply with the standards.	*8*	*8*	**64**	Revise current standards and implement needed ones	*7*	**Action!**
12	Influence of laws and regulations.	*7*	*7*	**49**	Make current assessment of laws	*5*	**Between Control & No Action**

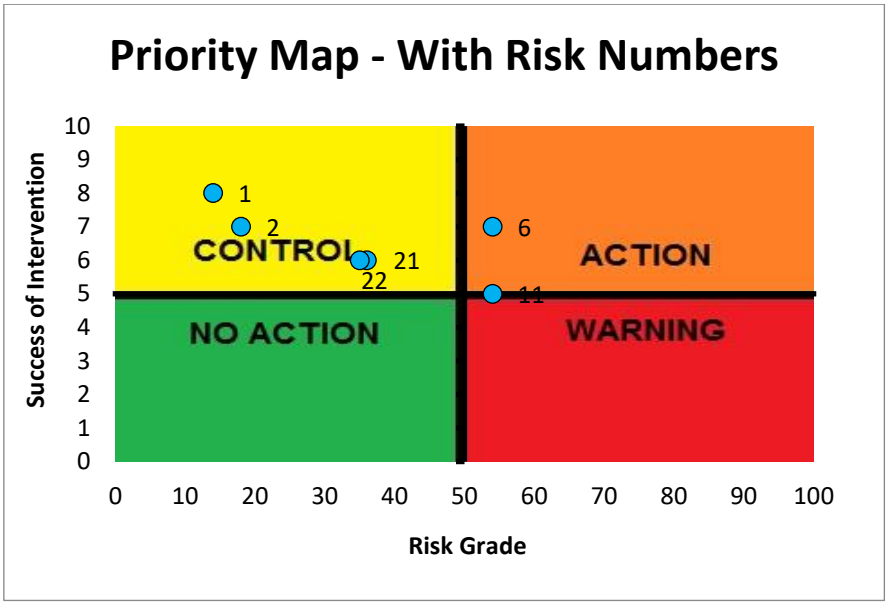

FIGURE 7: SECURAIL RISK MAP

4.1.4 Financial analysis

A financial analysis was performed in a 5-years timeline based on STAM individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users thanks to the impact reduction of catastrophic events was estimated at €40,000/year. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	96,000.00	96,000.00	184,000.00	252,000.00
Costs	-	47,500.00	45,500.00	30,500.00	30,500.00	30,500.00
EBITDA calculation	-	- 47,500.00	50,500.00	65,500.00	153,500.00	221,500.00
Investments	10,000.00	10,000.00				
Net cash-flow	- 10,000.00	- 57,500.00	39,610.00	51,310.00	119,950.00	172,990.00
IRR (Internal Rate of Return)	79.45%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	60,000.00	74,000.00	88,000.00	156,000.00
Costs	-	57,500.00	57,500.00	37,500.00	37,500.00	37,500.00
EBITDA calculation	-	- 57,500.00	2,500.00	36,500.00	50,500.00	118,500.00
Investments	20,000.00	20,000.00	-			
Net cash-flow	- 20,000.00	- 77,500.00	2,390.00	28,910.00	39,830.00	92,870.00
IRR (Internal Rate of Return)	15.88%					

Amortization period of the investment was estimated at 10 years. Corporate tax at 22%.

4.1.5 Summary of investment case

STAM performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require only to be monitored and those identified as “requiring action” have defined already mitigation actions to be implemented in the roadmap to commercialisation.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €156k in year 5 is expected, with an IRR of 15%, a NPV of €38k, and a ROI of 53% (considering the further investment required to finalise the tool). Break-even is achieved in Y2 for both the optimistic and pessimistic scenario.

4.2 CURIX AG - CURIX

4.2.1 Value proposition

CuriX® is a NextGeneration Tool for system resilience: With CuriX® we holistically protect IT systems from threats inside or outside the system – like a human immune system. The main value proposition stands for:

- Holistic Analytics (consolidates and correlates all available numeric data)
- Predictive Alerting (unlike existing tools, CuriX® predicts resilience issues, this enables preventive and right on time counter measures)
- Fully automated cycle (from anomaly detection to heal advice).
- Plug and play deployment.

4.2.2 Business model canvas

Key Partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
- System integrator - Reseller distributors - Touch point with other related vendors for co-marketing - Influencers – consulting companies	- Raise awareness with customers (marketing, webinars, etc.) - Get closer to system integrators (then closer to the customers) - Implement feedback loops with customers	- Holistic resilience for digital business (automating tasks that are time-consuming today, predictive analytics (being ahead of the threats), integrating any kind of metrics and inputs))	- Proof of value – first step - Subscription service - Training and customer success management	1. Insurance and banking companies 2. Large hospitals 3. Pharma and medtech 4. Cloud service providers 5. Railways and metro owners 6. Energy distribution or production

	Key Resources - Finalise product development - Sales and marketing		**Channels** - Direct sales - System integrators (distributors) - Cloud provider (distributor)	
Cost Structure - Personnel costs for R&D - Personnel costs for sales & marketing - Personnel costs for channel development - Management team - Software licenses - Cloud hosting - Margin out of revenues from indirect sales			**Revenue Streams** 1. Direct sales – Prove of value fee + subscription fee (if sold). 2. Consulting – Training and adapting the infrastructure/architecture 3. Indirect sales (system integrator/cloud provider) - % based on resellers sales	

FIGURE 8: CURIX BUSINESS MODEL CANVAS

4.2.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Risk of losing research track if there is no follow up research project	*3*	*5*	**15**	Define follow up project jointly with partners	*5*	**Between Control & No Action**
Technological Risk Factors							
2	Better or alternative concepts in the AI market	*5*	*3*	**15**	Focus on CuriX USPs which are unique	*5*	**Between Control & No Action**
3	Risk of launching a next generation technology as a start up	*3*	*7*	**21**	Cooperate with strong SI-partners	*2*	**No Action'**
4	Risk of concept limitation (only metrics)	*7*	*7*	**49**	Enhance concept for other input sources	*4*	**No Action'**
Market Risk Factors							
5	Reluctance of customers to buy the solution unproven	*3*	*7*	**21**	Offer Pre-Sales Consulting and PoVs	*2*	**No Action'**
IPR/Legal Risk Factors							
6	Being copied as only method set is IPR, but not the methods themselves	*5*	*3*	**15**	Offer visualization as additional USP, secure core stack against copying	*3*	**No Action'**
Financial/Management Risk Factors							
7	Inadequate funding for the final go to market / scale up	*8*	*5*	**40**	Present Business Case to potential Investors	*5*	**Between Control & No Action**

8	Capacity for deployment / support of customers and partners	*7*	*5*	**35**	Strong commercial and technical enablement programmes for partners	*2*	**No Action'**
Environmental/Regulation/Safety risks							
9	No sustainability arguments at the moment (e.g. less power or data consumption)	*1*	*5*	**15**	Find provable marketing arguments	*2*	**No Action'**

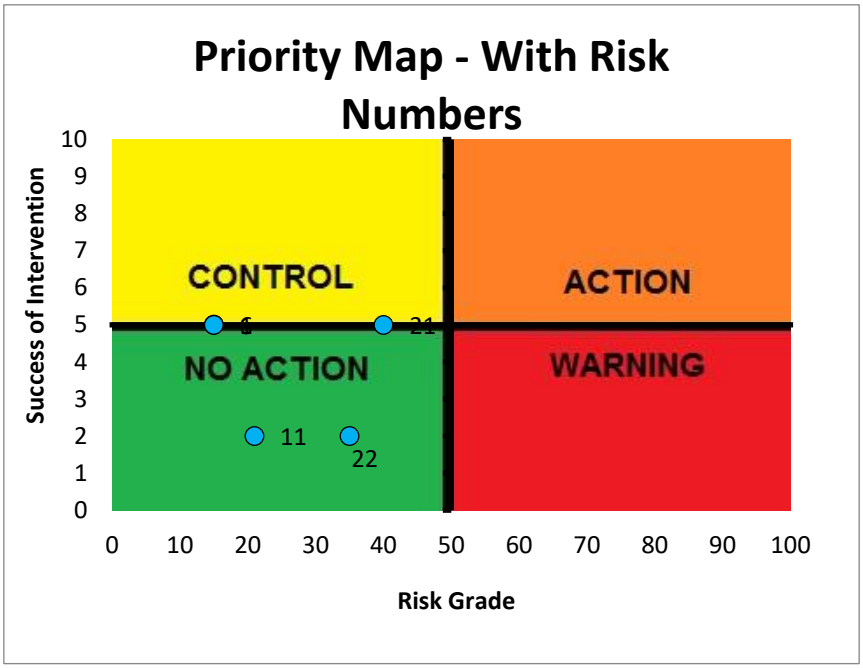

FIGURE 9: CURIX RISK MAP

4.2.4 Financial analysis

CURIX evaluated internally the sensitiveness of the data requested to complete the business plan of the results obtained as part of the R&D activities developed in SAFETY4RAILS. The internal assessment concluded that this information cannot be shared nor released, in any form, without putting at risk the business strategy of CURIX.

4.2.5 Summary of investment case

CURIX performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require no action and those identified as “requiring control” will be closely monitored. For these, relevant mitigation actions have been defined and will be enforced as necessary.

4.3 TREE TECHNOLOGY SA - TISAIL

4.3.1 Value proposition

TISAIL is a Threat Intelligence Service for Railway sector. It provides a platform for gathering, analysing and sharing relevant Open Source Threat Intelligence, allowing operators to identify their vulnerabilities. TISAIL will

be important for prevention and detection of attacks to the railway's infrastructure. The main advantage of TISAIL compared with other existing solutions is that it was designed specifically for the railway sector. 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 in twitter. Other available tools for Open Source Threat Intelligence are more concentrated in a company infrastructure (FW, servers...) not physical devices such as cameras, ...

4.3.2 Business model canvas

<table>
<tr>
<td rowspan="2">Key Partners
Organisations with knowledge in security in the railway sector. Could be railway operators (e.g.,Metro de Madrid, Rete Ferroviaria Italiana,etc), or organisations with railway cybersecurity products that have the knowledge about the railway ecosystem and may take advantage of TISAIL threats. (Cervello).</td>
<td>Key Activities
Integration with end-user premises and a better understanding of security requirements of the specific stakeholders.</td>
<td rowspan="2">Value Propositions
Our value proposition would be a tailored product for railway operators, according to their infrastructure/sensors.</td>
<td>Customer Relationships
Online/phone communication channels and on-site support when needed.</td>
<td rowspan="2">Customer Segments
The customer segment is the 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.</td>
</tr>
<tr>
<td>Key Resources
-Human capital in engineers for R&D (specific knowledge in railway security)
-Technology infrastructure</td>
<td>Channels
Direct sales based on license (upfront + service fee)</td>
</tr>
<tr>
<td colspan="3">Cost Structure
Personnel costs for R&D, sales and marketing</td>
<td colspan="2">Revenue Streams
Upfront fee
Monthly subscription fee</td>
</tr>
</table>

FIGURE 10: TISAIL BUSINESS MODEL CANVAS

4.3.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low-10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partners break out and create competitive products	*6*	*3*	**18**	Have strong legal support to define the agreement for collaboration	*7*	**Control.**
2	Risk of losing research track if there is no follow-up research project	*3*	*6*	**18**	Define follow up project jointly with partners	*8*	**Control.**
Technological Risk Factors							
3	Significant dependency on other technologies.	*7*	*2*	**14**	Develop stand-alone software modules	*7*	**Control.**

					based on proprietary technologies		
4	Result aiming at replacing existing status-quo	*3*	*2*	**6**	Highlight benefits for end-users and provide support for the whole risk analysis process	*8*	**Control.**
Market Risk Factors							
5	Nobody buys the product. Too expensive.	*9*	*3*	**27**	Review alternative business models options	*5*	**Between Control & No Action**
6	Reluctance of customers to buy a disruptive solution	*4*	*7*	**28**	Offer Pre Slaes Consulting and PoVs	*2*	**No Action'**
IPR/Legal Risk Factors							
7	Lack of definition of compliance and certification schemes	*3*	*7*	**21**	Request specific consultancies to obtain needed certification(s)	*5*	**Between Control & No Action**
8	IPR issues between partners	*7*	*3*	**21**	Make IPR agreements	*8*	**Control.**
Financial/Management Risk Factors							
9	Capacity for deployment / support of customers and partners	*7*	*4*	**28**	Strong commercial and technical enablement programmes for partners	*2*	**No Action'**
10	Inmature business plan	*7*	*5*	**35**	Revise business plan	*7*	**Control.**
Environmental/Regulation/Safety risks							
11	Influence of laws and regulations.	*6*	*3*	**18**	Make current assessment of laws	*6*	**Control.**

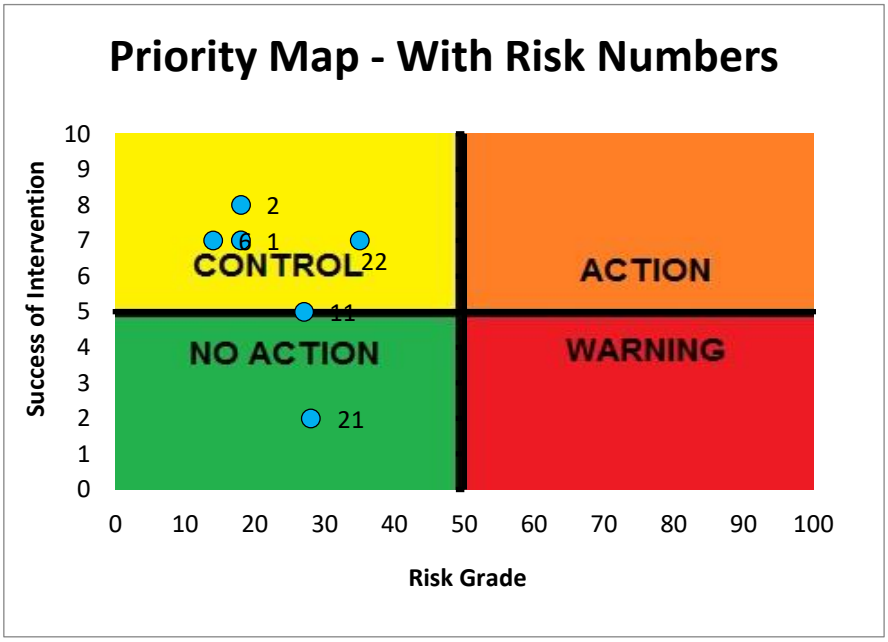

FIGURE 11: TISAIL RISK MAP

4.3.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on TREE individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users thanks to the tailored threat intelligence was estimated at €260,000/year. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	444,000.00	892,000.00	1,342,000.00	3,469,000.00	5,821,000.00
Costs	-	21,275.00	21,275.00	22,425.00	21,850.00	21,850.00
EBITDA calculation	-	422,725.00	870,725.00	1,319,575.00	3,447,150.00	5,799,150.00
Investments	25,000.00					
Net cash-flow	- 25,000.00	317,668.75	653,668.75	990,306.25	2,585,987.50	4,349,987.50
IRR (Internal Rate of Return)	1370.43%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	195,000.00	195,000.00	390,000.00	390,000.00	585,000.00
Costs	-	16,275.00	16,775.00	16,925.00	15,850.00	15,850.00
EBITDA calculation	-	178,725.00	178,225.00	373,075.00	374,150.00	569,150.00
Investments	25,000.00					
Net cash-flow	-	134,043.75	133,668.75	279,806.25	280,612.50	426,862.50
IRR (Internal Rate of Return)	552.37%					

Amortization period of the investment was estimated at 10 years. Corporate tax at 25%.

4.3.5 Summary of investment case

TREE performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require only to be monitored, being the most relevant the "Immature business plan". TREE will perform further iterations of the business plan after the project building on the information reported in this deliverable.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €585k in year 5 is expected. Given the low investment required and the high revenues expected, break-even is achieved in Y1 for both the optimistic and pessimistic scenario.

4.4 ERGUNLER INSAAT PETROL URUNLERI OTOMOTIV TEKSTIL MADENCILIK SU URUNLER SANAYI VE TICARET LIMITED STI.- PRIGM&SENSTATION

4.4.1 Value proposition

PRIGM

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.

PRIGM, as a high-throughput Hardware Security Module, 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 sufficient supply amount of true random numbers whenever they are needed to generate private keys. This approach makes PRIGM compliant with high throughput IoT applications and suitable for both node and person authentication, fast cryptographic functions and cryptographic verification and validation.

SENSTATION

Competitive advantage is that the method offers a 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.

4.4.2 Business model canvas

ERARGE business strategy is based on the commercialise of both **PRIGM and SENSTATION** jointly as a part of a combined product offering. The business model canvas and the financial analysis were defined taking this into consideration.

Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
System integrators and solution partners to integrate PRIGM/SENSTATION in any target cyber-physical system. Business partners and investors who would need ready solutions to promote and market tools for cyber-physical systems	Software and hardware-based developments and integration of PRIGM/SENSTATION to present reliability and robustness of the targeted solution Perform demonstrations in simulation exercises Define and improve a proactive Dissemination, Communication and Exploitation.	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.	Regular discussions and joint studies are ongoing with solution partners (biweekly) Visits and bilateral business meetings (monthly or bimonthly depending on the customer) Discussions are ongoing with major players, especially the solution providers, integrators and OEMs, in Turkey and Poland	The customer segment is the railway, metro or transportation service companies

	Key Resources Strong relations with railway stakeholders to identify their up-to-date requirements Patents and IPR expertise Productisation and commercialisation expertise		**Channels** Direct visits led or organised by ERARGE commercialisation team Through joint project partnerships Consultancy and technical assistance & service Through dissemination events (fairs, brokerage events, etc.)	
Cost Structure Personnel costs for further R&D and integration Personnel costs and overheads for sales & marketing Personnel costs and overheads for deployment, training and maintenance Equipment and consumables for further production, refinement and productisation Common Criteria and FIPS evaluation costs Patent and utility model cost			**Revenue Streams** Direct Sales including a 2-year warranty Integration with other solutions and fee for integration, deployment, tests, verification and validation Technical support and training Consultancy for further use, risk assessment and refinements	

FIGURE 12: PRIGM&SENSTATION BUSINESS MODEL CANVAS

4.4.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Industrialisation at risk: no system integrators for the exploitable result	*8*	*4*	**32**	SAFETY4RAILS consortium already includes some large-scale system integrators who could take this role to enter the market	*5*	**Between Control & No Action**
2	Investors are not interested in the solution	*8*	*3*	**24**	Review alternative business models options	*6*	**Control.**
Technological Risk Factors							
3	Integration in third parties' solution is problematic	*7*	*4*	**28**	PRIGM/Senstation is a highly interoperable platform solution that can be easily adapted to other third-party services	*8*	**Control.**
4	Users find challenging the use of the solution	*6*	*3*	**18**	Training sessions will be performed to give support to the users and facilitate adoption	*7*	**Control.**

Market Risk Factors							
5	Nobody buys the product. Too expensive costs	*8*	*2*	**16**	Review cost structure and licensing strategy	*4*	**No Action'**
6	Unsuitable marketing force	*7*	*6*	**42**	Increase advertising and hire an account manager to approach customers and suitable key stakeholders enabling commercialisation	*6*	**Control.**
IPR/Legal Risk Factors							
7	Legal problems - fail to establish a licensing agreement with system integrators	*8*	*5*	**40**	Liaise with IPR experts and review the framework of the agreement to find alternative economic or legal provisions to address the issues identified	*7*	**Control.**
8	Legal problems - IPR violation	*7*	*3*	**21**	Liaise with IPR experts and establish appropriate legal/commercial agreements	*8*	**Control.**
Financial/Management Risk Factors							
9	Capacity for deployment / support of customers and partners	*7*	*2*	**14**	Strong commercial and technical enablement programmes for partners	*2*	**No Action'**
10	Marketing and distribution fails due to a weak strategy	*7*	*3*	**21**	Strategy will be revised and expert consultancy will be required if needed	*7*	**Control.**
Environmental/Regulation/Safety risks							
11	Fail to comply with existing standards and procedures in place for railway infrastructures	*8*	*2*	**16**	SAFETY4RAILS analysed the standardisation landscape and integrated all relevant standards as part of its requirements	*5*	**Between Control & No Action**

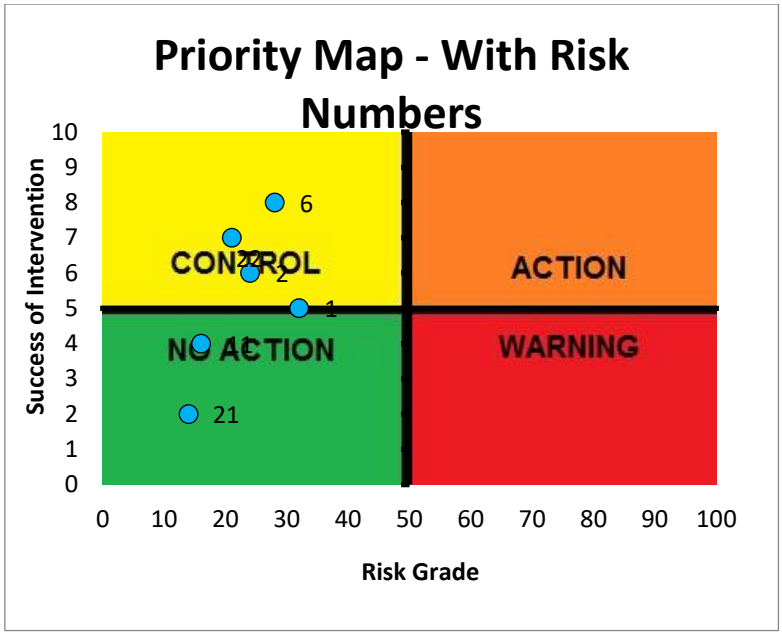

FIGURE 13: PRIGM/SENSTATION RISK MAP

4.4.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on ERARGE individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users for security and privacy resilience, as well as node and person authentication, were estimated at €90,000/year. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	241,000.00	474,000.00	932,000.00	1,398,000.00
Costs	-	45,000.00	41,000.00	36,000.00	31,000.00	31,000.00
EBITDA calculation	-	- 45,000.00	200,000.00	438,000.00	901,000.00	1,367,000.00
Investments	5,000.00	10,000.00				
Net cash-flow	- 5,000.00	- 55,000.00	156,110.00	341,750.00	702,890.00	1,066,370.00
IRR (Internal Rate of Return)	301.421%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	110,000.00	230,500.00	346,000.00	466,500.00
Costs	-	57,000.00	55,000.00	50,000.00	45,000.00	45,000.00
EBITDA calculation	-	- 57,000.00	55,000.00	180,500.00	301,000.00	421,500.00
Investments	35,000.00	32,000.00	-			
Net cash-flow	- 35,000.00	- 89,000.00	45,730.00	148,640.00	247,450.00	346,260.00
IRR (Internal Rate of Return)	77.871%					

Amortization period of the investment was estimated at 10 years. Corporate tax at 22%.

4.4.5 Summary of investment case

ERARGE performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Several risks require no action and those identified as “requiring control” will be closely monitored. For these, relevant mitigation actions have been defined and will be enforced as necessary.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €466k in year 5 is expected, with an IRR of 78%, a NPV of €453k, and a ROI of 300% (considering the further investment required to finalise the tool). Break-even is achieved in Y2 for both the optimistic and pessimistic scenario.

4.5 LEONARDO - SOCIETA PER AZIONI - Ganimede

4.5.1 Value proposition

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

- provide a single platform for video but also audio analysis
- have a single solution both for data centers and edge computing
- support live video processing for real time alerts and offline recorded video analysis for investigation
- be scalable in resources and algorithms and easily configurable
- exploit existing systems and equipment safeguarding customer investment

4.5.2 Business model canvas

<table>
<tr>
<td rowspan="2">Key Partners
• University
• Regulator (GDPR)</td>
<td>Key Activities
• Sales and marketing
• Technology R&D
• Content licensing
• Data analytics</td>
<td rowspan="2">Value Propositions
• Provide a single platform for video but also audio analysis
• Have a single solution both for data centers and edge computing
• Support live video processing for real time alerts and offline recorded video analysis for investigation
• Be scalable and flexible in resources and algorithms and easily configurable
• Exploit existing systems and equipment safeguarding customer investment</td>
<td>Customer Relationships
Adaptation to user needs, updates in software, deployment, technical support, training.</td>
<td rowspan="2">Customer Segments
<u>Direct:</u>
• First Responders
• Smart Cities
• Transportation
• Security
• Safety
• Production
<u>3rd parties:</u>
• Video Management System
• PSIM (Physical Security management system)</td>
</tr>
<tr>
<td>Key Resources
• Brand
• SW Engineering
• R&D Laboratories</td>
<td>Channels
• Sales
• Institutional</td>
</tr>
<tr>
<td colspan="3">Cost Structure
• SW Development
• Research and Development
• Infrastructure
• Marketing</td>
<td colspan="2">Revenue Streams
• Sales Licensing
• Sales as a Services</td>
</tr>
</table>

• Sales • General	

FIGURE 14: GANIMEDE BUSINESS MODEL CANVAS

4.5.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partner quits executing the exploitation plan	*9*	*2*	**18**	The partner is committed and is already seeking additional opportunities to follow-up with the product development	*5*	**Between Control & No Action**
2	Partner carries out low quality exploitation activity	*6*	*2*	**12**	The partner already counts with a large commercial background. Regular meetings with users will be performed to improve performance and exchange experiences	*4*	**No Action'**
Technological Risk Factors							
3	Clients do not like the solution, and thus there is low interest	*7*	*2*	**14**	The partner has already received interest from potential clients. Adapt the functionalities and user experience according to the end-users' and customers 'needs.	*4*	**No Action'**
4	Integration in third parties' software is problematic	*7*	*3*	**21**	The partner counts with a standalone solution	*8*	**Control.**
Market Risk Factors							
5	Nobody buys the product. Too expensive costs	*7*	*4*	**28**	Review cost structure and licensing strategy	*6*	**Control.**
6	Unsuitable marketing force	*7*	*1*	**7**	Increase advertising and hire an account manager to approach customers and suitable key stakeholders	*4*	**No Action'**

					enabling commercialisation		
IPR/Legal Risk Factors							
7	Legal problems - IPR violation	*7*	*3*	**21**	Liaise with IPR experts and establish appropriate legal/commercial agreements	*5*	**Between Control & No Action**
Financial/Management Risk Factors							
8	Marketing and distribution fails due to a weak strategy	*8*	*4*	**32**	Strategy will be revised periodically	*6*	**Control.**
Environmental/Regulation/Safety risks							
9	Fail to comply with existing standards and procedures in place for railway infrastructures	*8*	*3*	**24**	SAFETY4RAILS analysed the standardisation landscape and integrated all relevant standards as part of its requirements	*5*	**Between Control & No Action**

FIGURE 15: GANIMEDE RISK MAP

4.5.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on Ganimede individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users thanks to the more efficient management of critical events (time reduction) was estimated at €80,000/year. In this sense, Ganimede system can reduce the stress of the control room staff allowing a more effective management of critical events by freeing precious resources from repetitive work and that normally reduce the attention threshold. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	160,000.00	360,000.00	760,000.00	1,040,000.00	1,160,000.00
Costs	-	50,000.00	75,000.00	70,000.00	77,500.00	72,500.00
EBITDA calculation	-	110,000.00	285,000.00	690,000.00	962,500.00	1,087,500.00
Investments	175,000.00					
Net cash-flow	- 175,000.00	93,500.00	230,000.00	545,900.00	758,450.00	855,950.00
IRR (Internal Rate of Return)	127.13%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	80,000.00	180,000.00	380,000.00	520,000.00	580,000.00
Costs	-	50,000.00	70,000.00	65,000.00	70,000.00	70,000.00
EBITDA calculation	-	30,000.00	110,000.00	315,000.00	450,000.00	510,000.00
Investments	175,000.00					
Net cash-flow	- 175,000.00	30,000.00	93,500.00	253,400.00	358,700.00	405,500.00
IRR (Internal Rate of Return)	69.41%					

Amortization period of the investment was estimated at 5 years. Corporate tax at 22%.

4.5.5 Summary of investment case

LDO performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require no action and those identified as “requiring control” will be closely monitored. For these, relevant mitigation actions have been defined and will be enforced as necessary.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €580k in year 5 is expected, with an IRR of 69%, a NPV of €792k, and a ROI of 248% (considering the further investment required to finalise the tool). Break-even is achieved in Y1 for both the optimistic and pessimistic scenario.

4.6 WINGS ICT SOLUTIONS INFORMATION & COMMUNICATION TECHNOLOGIES IKE – WINGSPARK

4.6.1 Value proposition

Existing solutions target a specific domain, either parking, rail or road infrastructures, whereas WINGSPARK targets at serving different infrastructures in the same manner. This will be achieved through an abstraction layer in order to accommodate different customer needs/requirements. The proposed solution aims at the efficient monitoring and management of the transport infrastructure in real time, but also the possibility of maximizing its use, through the exploitation of the data coming from the different sensors deployed in the infrastructure. The management software and the utilization of the data collected from the individual systems that make up the proposed solution, make it possible to offer value-added services for facility managers and for the benefit of the end users maximising the possibilities offered by the Internet of Things and Artificial Intelligence.

4.6.2 Business model canvas

<table>
<tr>
<td rowspan="2">Key Partners
- Business partner – security / cybersecurity company, for Joint Venture
- Telecom operator already providing services to the customer (Optional, could help faster access to the market)</td>
<td>Key Activities
- Define a final go-to-market strategy
- Marketing activities</td>
<td rowspan="2">Value Propositions
The proposed solution aims at the efficient monitoring and management of the transport infrastructure in real time.
Delivery of insights to better understand past and current issues to predict and optimize the current and future actions, enabling faster, more efficient and reliable decision making.</td>
<td>Customer Relationships
Adaptation to user needs, updates in software, deployment, technical support, training.
Already under discussions with major players in Greece (airport, railway, municipalities)</td>
<td rowspan="2">Customer Segments
- Public and private sector companies managing the infrastructure (Railway, Metro, Airport, Municipalities)
- Service providers
- Network providers</td>
</tr>
<tr>
<td>Key Resources
- Access to various data sources from railways
- Marketing and commercial expertise</td>
<td>Channels
- Direct sales exploiting WINGS network
- Sell together with a business partner, including other components such as asset management (Joint Venture)
- Technical support, customisation, maintenance, training</td>
</tr>
<tr>
<td colspan="3">Cost Structure
- Personnel cost for further R&D
- Personnel costs for sales & marketing
- Personnel costs for development and deployment
- Customer support (including development, customization, training, consultancy, technical support)</td>
<td colspan="2">Revenue Streams
- 1) Direct sales: Upfront fee + subscription fee (maintenance + improvements)
- 2) Sales through joint Venture: Upfront fee + subscription fee (maintenance +improvements)
- Technical support, training</td>
</tr>
</table>

FIGURE 16: WINGSPARK BUSINESS MODEL CANVAS

4.6.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partners break out and create competitive products	*6*	*3*	**18**	Have strong legal support to define the agreement for collaboration	*6*	**Control.**
2	Partner carry out low quality exploitation activity	*8*	*4*	**32**	The team plans to organise regular meetings to check the status of the work and plan contingency actions in case needed	*7*	**Control.**
Technological Risk Factors							

3	The system is not scalable and fails to provide reliable results with a large network of IoT sensors	*8*	*7*	**56**	Test solution in pre-operational environment before actual commercial deployment and adjust if needed	*9*	**Action!**
4	Integration in third parties' software is problematic	*7*	*4*	**28**	WINGSPARK a highly interoperable solution that can be easily adapted to other third-party services	*7*	**Control.**
Market Risk Factors							
5	Reluctance of customers to buy a disruptive solution	*4*	*7*	**28**	Offer pre-sales consulting and training	*5*	**Between Control & No Action**
6	Unsuitable marketing force	*8*	*4*	**32**	Increase advertising and hire an account manager to approach customers and suitable key stakeholders enabling commercialisation	*4*	**No Action'**
IPR/Legal Risk Factors							
7	Lack of definition of compliance and certification schemes	*4*	*7*	**28**	Request specific consultancies to obtain needed certifications(s)	*5*	**Between Control & No Action**
8	IPR issues between partners	*7*	*3*	**21**	Make IPR agreements	*8*	**Control.**
Financial/Management Risk Factors							
9	Marketing and distribution fails due to a lack of resources	*8*	*4*	**32**	Adapt strategy to low cost activities. Dedicate staff more specifically	*6*	**Control.**
10	Marketing and distribution fails due to a weak strategy	*7*	*5*	**35**	Strategy will be revised periodically	*6*	**Control.**
Environmental/Regulation/Safety risks							
11	Fail to comply with existing standards and procedures in place for railway infrastructures	*8*	*2*	**16**	SAFETY4RAILS analysed the standardisation landscape and integrated all relevant standards as part of its requirements	*5*	**Between Control & No Action**

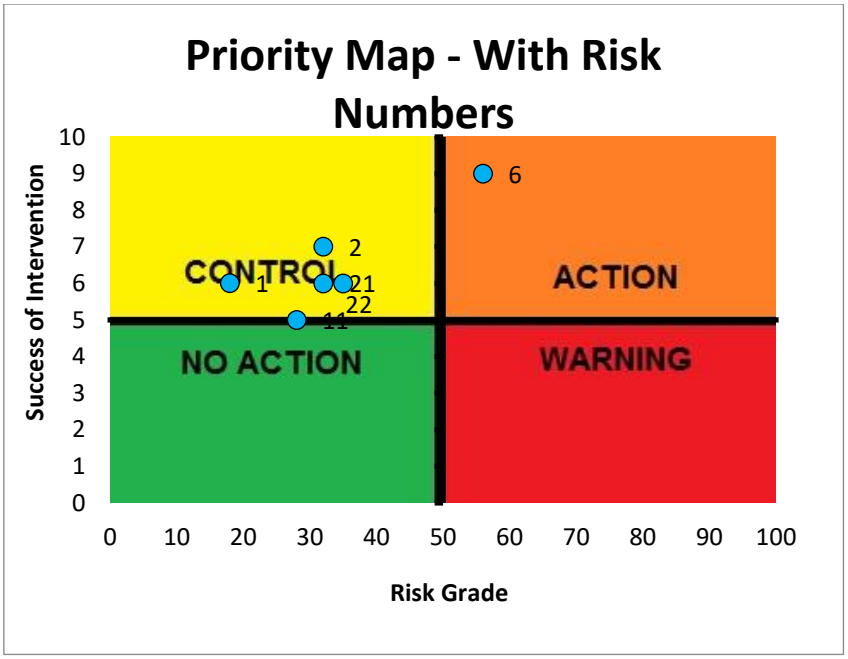

FIGURE 17: WINGSPARK RISK MAP

4.6.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on WINGS individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users thanks to the better monitoring of the infrastructure and the early detection preventing incidents and casualties was estimated at €100,000/year. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	386,000.00	772,000.00	1,544,000.00	1,930,000.00	2,702,000.00	3,088,000.00
Costs	432,000.00	432,000.00	504,000.00	504,000.00	576,000.00	576,000.00
EBITDA calculation	- 46,000.00	340,000.00	1,040,000.00	1,426,000.00	2,126,000.00	2,512,000.00
Investments						
Net cash-flow	- 46,000.00	241,400.00	738,400.00	1,012,460.00	1,509,460.00	1,783,520.00
IRR (Internal Rate of Return)	676.20%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	193,000.00	386,000.00	579,000.00	772,000.00	772,000.00	965,000.00
Costs	432,000.00	432,000.00	504,000.00	504,000.00	504,000.00	576,000.00
EBITDA calculation	- 239,000.00	- 46,000.00	75,000.00	268,000.00	268,000.00	389,000.00
Investments						
Net cash-flow	- 239,000.00	- 46,000.00	53,250.00	190,280.00	190,280.00	276,190.00
IRR (Internal Rate of Return)	27.94%					

Amortization period of the investment was estimated at 10 years. Corporate tax at 29%.

4.6.5 Summary of investment case

WINGS performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require only to be monitored and those identified as “requiring action” have defined already mitigation actions to be implemented in the roadmap to commercialisation.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €965k in year 5 is expected, with an IRR of 28%, a NPV of €447k, and a ROI of 38% (considering the further investment required to finalise the tool). Break-even is achieved in Y2 for the pessimistic scenario and in Y1 for the optimistic scenario.

4.7 RINA CONSULTING SPA - BB3d

4.7.1 Value proposition

The BB3d tool 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.

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.

4.7.2 Business model canvas

Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
- Business partner – physical security company, for Joint Venture and company for Cloud services - Legal entities -> how	Technically: performance and visualization improvement. Addition of some features related to blast wave propagation phenomena and structural damage for modern structures. Full validation: validation of the gainable results. Commercially: put the tool in the cloud through a web application.	BB3d main value proposition is based on facility of use, coupled with fast and stable computing.	- Proof of value – first step - Subscription service - Training and customer success management - Customisation, updates in software, technical support, training.	- Blast experts and designers - Civil infrastructures managers - Organizations working in the fight against

functionalities could contribute to certification and compliance - System integrator -> to include BB3d into the overall system of the railway	**Key Resources** - IT experts development - Sales and marketing - Legal consultancy - Cloud or service hosting infrastructure		**Channels** - Consulting services - Direct industrial use: according to this approach the BB3d is released to the client once a contract for its use has been put in place (e.g. temporary lease, perpetual purchase). This solution can include maintenance activities, on-premises or remote training and support. - SaaS (Software as a Service): One of these is according to by making available its use through the web.	terrorism (Police, Army) - Manufacturing plants which handle explosive materials
Cost Structure - Personnel cost for further R&D - Personnel costs for sales and marketing - Cloud hosting - Management teams - Personnel costs for development and deployment			**Revenue Streams** - Direct sales – paid up or lease. - SaaS paradigm (pay per use or lease) - Consulting – Training and customization	

FIGURE 18: BB3D BUSINESS MODEL CANVAS

4.7.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low-10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partner quits executing the exploitation plan	*9*	*2*	**18**	The partner is committed and is already seeking additional opportunities to follow-up with the product development	*5*	**Between Control & No Action**
2	Industrialisation risk: no system integrators for the exploitable result	*8*	*3*	**24**	SAFETY4RAILS consortium already includes some large-scale system integrators who could take this role to enter the market	*5*	**Between Control & No Action**
Technological Risk Factors							
3	Confidentiality of blast data of past bomb attack may hinder the full validation of the tool	*7*	*8*	**56**	Work together bomb blast experts with strict confidentiality agreements	*5*	**Between Action & Warning**
4	Integration in third parties' software is problematic	*7*	*4*	**28**	Invest in improving interoperability and data	*7*	**Control.**

					exchanges protocols		
Market Risk Factors							
5	Nobody buys the product. Too expensive costs	*8*	*5*	**40**	Review cost structure and licensing strategy	*5*	**Between Control & No Action**
6	Unsuitable marketing force	*7*	*2*	**14**	Increase advertising and hire an account manager to approach customers and suitable key stakeholders enabling commercialisation	*4*	**No Action'**
IPR/Legal Risk Factors							
7	Legal problems - IPR violation	*7*	*3*	**21**	Liaise with IPR experts and establish appropriate legal/commercial agreements	*5*	**Between Control & No Action**
Financial/Management Risk Factors							
8	Marketing and distribution fails due to a weak strategy	*7*	*3*	**21**	Strategy will be revised periodically	*6*	**Control.**
Environmental/Regulation/Safety risks							
9	Fail to comply with existing standards and procedures in place for railway infrastructures	*8*	*2*	**16**	SAFETY4RAILS analysed the standardisation landscape and integrated all relevant standards as part of its requirements	*5*	**Between Control & No Action**

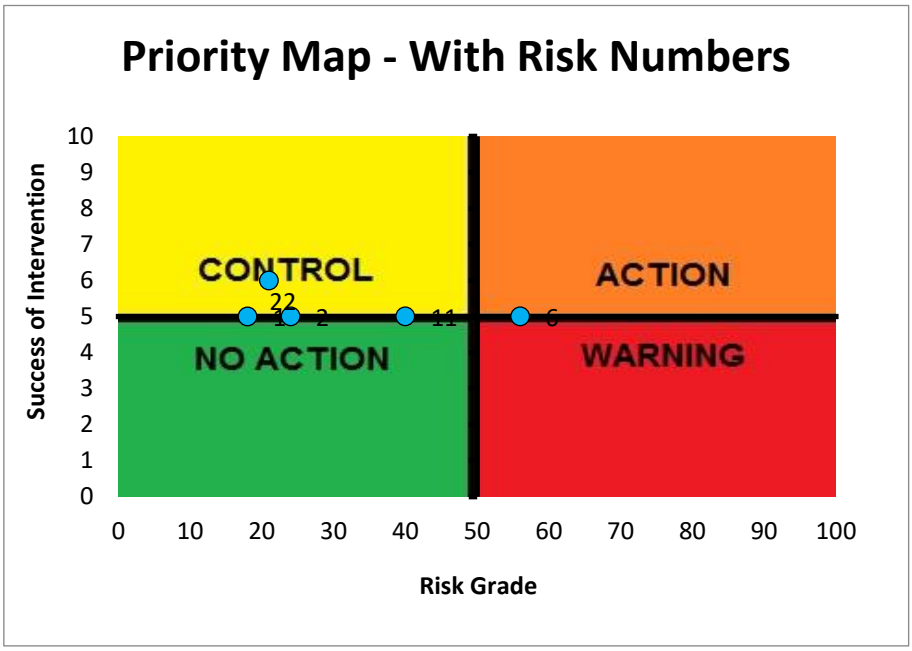

FIGURE 19: RINA (BB3D) RISK MAP

4.7.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on RINA individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users were estimated at €150,000/year. Such estimation is based on the bomb blast analyses capabilities provided, therefore neutralising the need of external consultancy services, and the easier identification of countermeasures. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	18,000.00	54,000.00	90,000.00	126,000.00	180,000.00
Costs	-	10,500.00	17,850.00	23,625.00	31,500.00	39,900.00
EBITDA calculation	-	7,500.00	36,150.00	66,375.00	94,500.00	140,100.00
Investments	20,000.00					
Net cash-flow	- 20,000.00	6,730.00	29,077.00	52,652.50	74,590.00	110,158.00
IRR (Internal Rate of Return)	117.32%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	18,000.00	18,000.00	36,000.00	54,000.00
Costs	-	10,500.00	17,325.00	17,850.00	21,000.00	25,200.00
EBITDA calculation	-	- 10,500.00	675.00	150.00	15,000.00	28,800.00
Investments	20,000.00					
Net cash-flow	- 20,000.00	- 10,500.00	675.00	150.00	12,580.00	23,344.00
IRR (Internal Rate of Return)	4.49%					

Amortization period of the investment was estimated at 5 years. Corporate tax at 22%.

4.7.5 Summary of investment case

RINA performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require only to be monitored, being the most relevant the cost of the product. For this, relevant mitigation actions are already defined and will be enforced to reduce the risk. There is one risk element which is critical, namely the confidentiality of blast data from past bomb explosions. RINA has already defined some potential mitigations (see the table) and will work on this after the project to neutralise this barrier.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €54k in year 5 is expected, with an IRR of 4%, a NPV of €14k, and a ROI of 13% (considering the further investment required to finalise the tool). Break-even is achieved in Y2 for the pessimistic scenario and in Y1 for the optimistic scenario.

4.8 RINA CONSULTING SPA - SARA

4.8.1 Value proposition

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.

Compared to ERARGE or ICOM business models, RINA does not foresee a joint exploitation of the BB3d and SARA tools, as described in D10.9. The rationale is that both tools address different types of end-users, with different needs, within the railway domain.

4.8.2 Business model canvas

<table>
<tr>
<td rowspan="2">Key Partners
Critical Infrastructure Experts who can share data required to take the tool to the commercialisation phase</td>
<td>Key Activities
Improvements and adaptations following further end-user feedback

Need for further development (SW architecture) before commercialization plus RINA technical analysis</td>
<td rowspan="2">Value Propositions
The strong point of the tool is the possibility of simulating different mitigation actions available, such as redundancy or strengthening of physical elements. 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.</td>
<td>Customer Relationships
- Proof of value – first step
- Subscription service
- Training and customer success management
- Customisation, updates in software, technical support, training.</td>
<td rowspan="2">Customer Segments
Railway infrastructure

Managers, locally, regionally or national scale
railway infrastructure managers, but also transport IMs more generally</td>
</tr>
<tr>
<td>Key Resources
- Sensitive data of the assets
- Sales and marketing
- Legal consultancy
- Cloud or service hosting infrastructure</td>
<td>Channels
Direct sales based on license (upfront + service fee)

Yearly maintenance and consultancy services</td>
</tr>
<tr>
<td colspan="3">Cost Structure
- Personnel cost for further R&D
- Personnel costs for sales and marketing
- Cloud hosting
- Management teams
- Personnel costs for maintenance and customer support</td>
<td colspan="2">Revenue Streams
- Direct sales – upfront + yearly fee
- Maintenance and consultancy services fee</td>
</tr>
</table>

FIGURE 20: SARA BUSINESS MODEL CANVAS

4.8.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion

Partnership Risk Factors							
1	Partner quits executing the exploitation plan	*9*	*2*	**18**	The partner is committed and is already seeking additional opportunities to follow-up with the product development	*5*	**Between Control & No Action**
2	Industrialisation risk: no system integrators for the exploitable result	*7*	*3*	**21**	SAFETY4RAILS consortium already includes some large-scale system integrators who could take this role to enter the market	*5*	**Between Control & No Action**
Technological Risk Factors							
3	Confidentiality of assets data required for SARA may hinder the full validation of the tool	*8*	*7*	**56**	Work together critical infrastructure experts with strict confidentiality agreements	*6*	**Action!**
4	Integration in third parties' software is problematic	*8*	*6*	**48**	Invest in improving interoperability and data exchanges protocols	*6*	**Control.**
Market Risk Factors							
5	Nobody buys the product. Too expensive costs	*8*	*6*	**48**	Review cost structure and licensing strategy	*5*	**Between Control & No Action**
6	Unsuitable marketing force	*7*	*2*	**14**	Increase advertising and hire an account manager to approach customers and suitable key stakeholders enabling commercialisation	*4*	**No Action'**
IPR/Legal Risk Factors							
7	Legal problems - IPR violation	*7*	*3*	**21**	Liaise with IPR experts and establish appropriate legal/commercial agreements	*5*	**Between Control & No Action**
Financial/Management Risk Factors							
8	Marketing and distribution fails due to a weak strategy	*7*	*5*	**35**	Strategy will be revised periodically	*6*	**Control.**
Environmental/Regulation/Safety risks							
9	Fail to comply with existing standards and procedures in place for railway infrastructures	*8*	*5*	**40**	SAFETY4RAILS analysed the standardisation landscape and integrated all relevant standards as part of its requirements	*6*	**Control.**

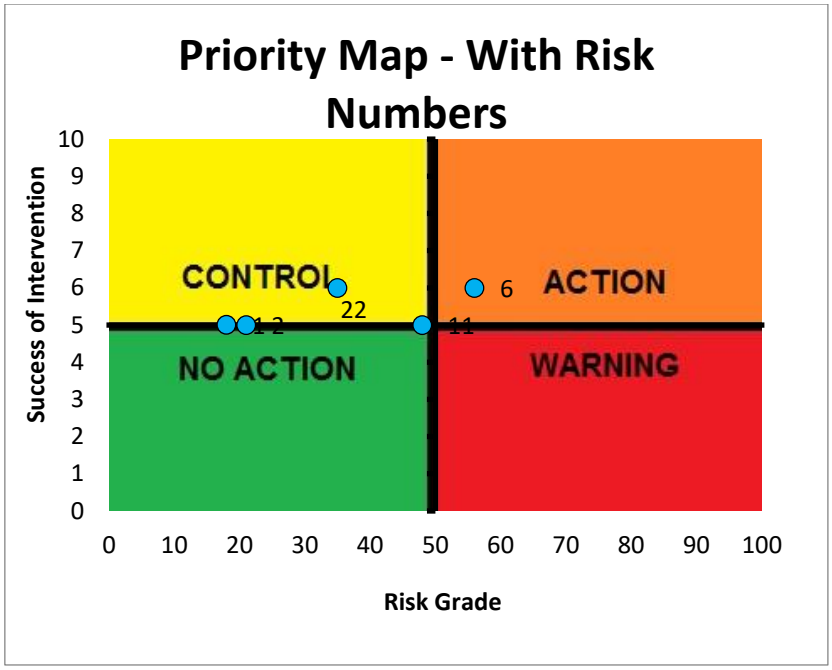

FIGURE 21: RINA (SARA) RISK MAP

4.8.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on RINA individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users thanks to the impact reduction of catastrophic events was estimated at €80,000/year. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections, therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	60,000.00	120,000.00	120,000.00	180,000.00
Costs	-	-	35,000.00	48,500.00	62,000.00	75,500.00
EBITDA calculation	-	-	25,000.00	71,500.00	58,000.00	104,500.00
Investments	70,000.00	70,000.00				
Net cash-flow	- 70,000.00	- 70,000.00	25,000.00	61,930.00	51,400.00	87,670.00
IRR (Internal Rate of Return)	15.46%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	60,000.00	60,000.00	120,000.00	120,000.00
Costs	-	-	23,000.00	36,500.00	38,000.00	39,500.00
EBITDA calculation	-	-	37,000.00	23,500.00	82,000.00	80,500.00
Investments	70,000.00	70,000.00				
Net cash-flow	- 70,000.00	- 70,000.00	31,250.00	21,125.00	65,000.00	63,875.00
IRR (Internal Rate of Return)	8%					

Amortization period of the investment was estimated at 5 years. Corporate tax at 22%.

4.8.5 Summary of investment case

RINA performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Most of the risks require only to be monitored and those identified as “requiring action” have defined already mitigation actions to be implemented in the roadmap to commercialisation.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €120k in year 5 is expected, with an IRR of 8%, a NPV of €62k, and a ROI of 74% (considering the further investment required to finalise the tool). Break-even is achieved in Y2 for both the optimistic and pessimistic scenario.

4.9 ELBIT SYSTEMS C4I AND CYBER LTD – RAM2

ELBIT evaluated internally the sensitiveness of the data requested to complete the business plan of the results obtained as part of the R&D activities developed in SAFETY4RAILS. The internal assessment concluded that this information cannot be shared nor released, in any form, without putting at risk the business strategy of ELBIT.

4.10 INTRACOM SA TELECOM SOLUTIONS - UNIMS&SISC2&Secaas

4.10.1 Value proposition

ICOM business strategy is to commercialise **UNIMS, SISC2 and SecaaS** jointly as a part of a combined product offering. This section provides the value proposition of each product with respect to their relevant competing solutions:

UNIMS

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 & Field Engineers and tackles complexity, from a single screen.

An exciting collection of capabilities in the form of Network Lifecycle Automation Applications, 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[21,22].

SISC2

[21] https://www.intracom-telecom.com/en/products/wireless_network_systems/netw_manag_systems/ConnectedSite.htm
[22] https://www.intracom-telecom.com/en/products/wireless_network_systems/netw_manag_systems/NetworkLifecycleMgmt.htm

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[23].

Key Characteristics

- Highly-intuitive human machine interfaces
- Superior situational awareness with dynamic 2D/3D maps and sensor data
- Authentication & authorization with Role Based Access Control
- Multilingual user interface
- Fully customized screen layouts with support for multi-monitor workstations
- Modular design and use of open protocols allows system to scale horizontally
- High Availability ensures 24/7 operation and avoids single point of failure

- Seamless integration with a variety of third-party systems.

SECAAS

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. 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[24].

- Reduction of capital and operating expenses
- Compliance to regulatory requirements
- Fully customizable solutions to suit individual customer needs
- Guaranteed performance and monitoring
- Improved manageability and service provisioning
- managed and unmanaged offerings
- Improved network performance and bandwidth usage
- Fully customizable security policies and rules
- VPN connectivity (site-to-site and client-to-site)
- End-user management
- Custom web application protection rules
- Support of encrypted site traffic
- Administrators' training sessions
- Administration, operations and monitoring for the customer

4.10.2 Business model canvas

ICOM's business model canvas encompasses the combination of UNIMS, SISC2 and SECAAS commercialisation strategies:

Key Partners	**Key Activities**	**Value Propositions**	**Customer Relationships**	**Customer Segments**
Cybersecurity experts Telco operators	Adaptations and adjustments required to respond to the specific user	Improved network lifecycle management introducing operational agility, unprecedent efficiency and optimised network building and maintenance.	- Onsite deployment and customisation	Customer segments are: - Telecom service providers

[23] http://www.intracom-telecom.com/downloads/pdf/products/sis/sisc2.pdf
[24] https://www.intracom-telecom.com/en/products/ict_services_solutions/cloud/SecaaS.htm

	needs of railways infrastructures **Key Resources** Staff – R&D/developers Staff – marketing/sales Technology infrastructure	Maximise threat detection efficiency and timely situational awareness Reduction of capital and operating expenses, and compliance to regulatory requirements	- Onsite & remote technical support - Remote fault monitoring - Other means (to be agreed) **Channels** - Existing customers for WiBAS (another ICOM tool) - License-based service fee - Hardware costs upfront - Hardware deployment fee included	- Mobile & network operators - Transport infra/service operators - Energy infra/service operators
Cost Structure R&D costs Marketing and sales Customer support (incl. technical maintenance)			**Revenue Streams** Sales include: - Cost of hardware (if required) paid upfront - Maintenance service agreement (yearly/monthly)	

FIGURE 22: ICOM BUSINESS MODEL CANVAS

4.10.3 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low- 10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partner quits executing the exploitation plan	*9*	*2*	**18**	The partner is committed and is already seeking additional opportunities to follow-up with the product development	*6*	**Control.**
2	Partners carries out low quality exploitation activity	*6*	*2*	**12**	The partners already count with a large commercial background. Regular meetings with users will be performed to improve performance and exchange experiences	*5*	**Between Control & No Action**
3	Partner change priorities for exploitation	*8*	*3*	**24**	Finding alternative partner with similar enabling technology and/or employing	*7*	**Control.**

					proprietary alternatives		
Technological Risk Factors							
4	Clients do not like the solution, and thus there is low interest	*7*	*2*	**14**	The partner has already received interest from potential clients. Adapt the functionalities and user experience according to the end-users' and customers' needs	*5*	**Between Control & No Action**
5	Integration of the three products (UNIMS, SISC2 and SecaaS) is problematic	*8*	*3*	**24**	Invest in improving interoperability and data exchanges protocols	*6*	**Control.**
6	Partner's solutions become outdated/discontinued	*8*	*2*	**16**	Finding alternative partner with similar enabling technology and/or employing proprietary alternatives	*7*	**Control.**
Market Risk Factors							
7	Nobody buys the product. Too expensive costs	*7*	*3*	**21**	Review cost structure and licensing strategy	*6*	**Control.**
8	Reluctance of customers to buy a disruptive solution	*4*	*4*	**16**	Offer pre-sales consulting and demonstrations	*4*	**Control.**
9	Customers' need for major shift in internal procedures	*7*	*6*	**42**	Provision of complementary add-ons in favour of complete system replacement to reduce risk of drastic changes to operational practices	*7*	**Control.**
IPR/Legal Risk Factors							
10	Legal problems - IPR violation	*8*	*4*	**32**	Liaise with IPR experts and establish appropriate legal/commercial agreements	*6*	**Control.**
11	IPR issues between partners	*7*	*3*	**21**	Make IPR agreements	*8*	**Control.**
12	Patent related restrictions	*8*	*1*	**8**	Solutions avoid conflicts with patents by securing them with own IPR	*8*	**Control.**
Financial/Management Risk Factors							
13	Capacity for deployment/support of customers and partners	*7*	*2*	**14**	Strong commercial and technical expertise onboard	*6*	**Control.**
14	Marketing and distribution fails due to a weak strategy	*8*	*2*	**16**	Strategy will be revised periodically	*7*	**Control.**

Environmental/Regulation/Safety risks							
15	Fail to comply with existing standards and procedures in place for railway infrastructures	*8*	*2*	**16**	SAFETY4RAILS analysed the standardisation landscape and integrated all relevant standards as part of its requirements	*5*	**Between Control & No Action**
16	Legal compliance of ICOM products with relevant legislations	*7*	*1*	**7**	All ICOM products are compliant with relevant norms, standards and regulations	*8*	**Control.**

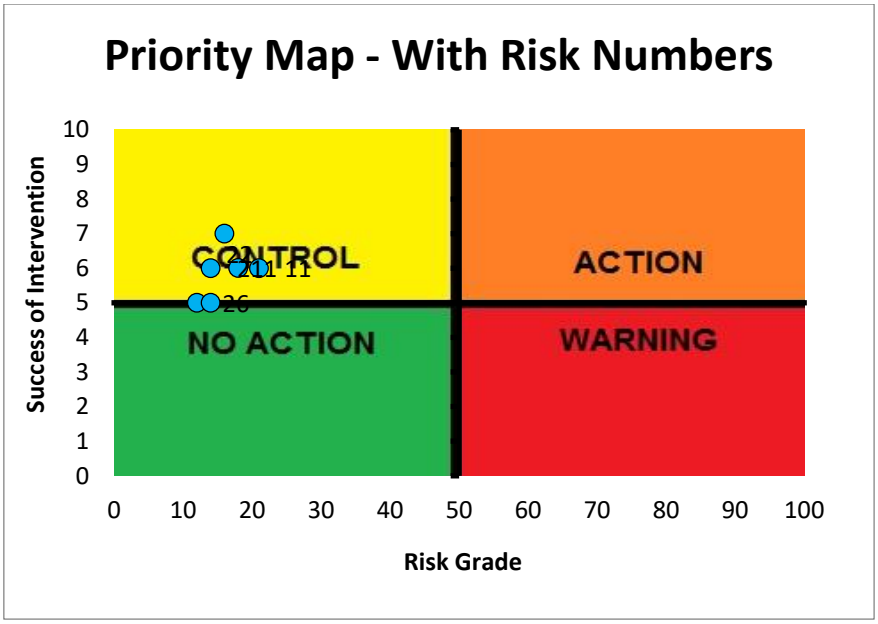

FIGURE 23: ICOM (UNIMS, SISC2, SECAAS) RISK MAP

4.10.4 Financial analysis

A financial analysis was performed in a 5-years' timeline based on ICOM individual business strategy. The pricing strategy for each of the revenue streams was based on a cost-benefit analysis, where the savings offered to the end-users due to the better monitoring of the infrastructure and early detection of potential issues, were estimated at €100,000/year. Sales projections are based on ICOM's historical data from the past 2 years for the same tools in other markets. An optimistic and a pessimistic scenario were considered based on the best and worst sales projections (no increase in sales), therefore assessing the solidity of the business plan:

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	105,749,900.00	108,130,000.00	110,510,100.00	112,890,200.00	115,270,300.00	117,650,400.00
Costs	47,860,000.00	48,915,000.00	49,970,000.00	51,025,000.00	52,080,000.00	53,135,000.00
EBITDA calculation	57,889,900.00	59,215,000.00	60,540,100.00	61,865,200.00	63,190,300.00	64,515,400.00
Investments	15,024,000.00	17,250,000.00	19,476,000.00	21,702,000.00	23,928,000.00	26,154,000.00
Net cash-flow	29,468,425.00	28,311,250.00	27,154,075.00	25,996,900.00	24,839,725.00	23,682,550.00
IRR (Internal Rate of Return)	-					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	105,749,900.00	105,749,900.00	105,749,900.00	105,749,900.00	105,749,900.00	105,749,900.00
Costs	47,860,000.00	47,860,000.00	47,860,000.00	47,860,000.00	47,860,000.00	47,860,000.00
EBITDA calculation	57,889,900.00	57,889,900.00	57,889,900.00	57,889,900.00	57,889,900.00	57,889,900.00
Investments	15,024,000.00					
Net cash-flow	29,468,425.00	44,492,425.00	44,492,425.00	44,492,425.00	44,492,425.00	44,492,425.00
IRR (Internal Rate of Return)	-					

Amortization period of the investment was estimated at 10 years. Corporate tax at 25%.

4.10.5 Summary of investment case

ICOM performed a through risk assessment to identify the most relevant risks that would have an influence on the business strategy. Several risks require no action and those identified as “requiring control” will be closely monitored. For these, relevant mitigation actions have been defined and will be enforced as necessary.

For evaluating profitability, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed. Even in the pessimistic scenario, a yearly turnover of nearly €105M in year 5 is expected, a NPV of €168M, and a ROI of 108% (considering the further investment required to finalise the tools for the railway market). Break-even was already achieved before the forecasting period.

5. S4RIS business plan

5.1 Introduction

The SAFETY4RAILS Information System business plan comprises the inputs from all partners individual business plans, as presented in this deliverable, as well as considers the joint exploitation roadmap described in D10.9.

In D10.9, it is highlighted that a European Union (EU) Pre-commercial Procurement (PCP) project could be a good opportunity to reduce the financial risk in implementing the joint exploitation roadmap and to secure customers' interest. In a PCP, the early adopters of the system would be those EU buyers (customers) engaged in the PCP, who would in return have royalty shares over the revenues obtained from its commercialisation. The royalty shares obtained by these EU buyers is proposed in this section based on financial indicators but should be revised as the exploitation strategy is implemented and progresses.

As described in D10.9, technical partners planned already to join efforts for the exploitation of the platform. For this, the core applied research and academic partners (namely FRAUNHOFER, NCSRD & RMIT) will establish the necessary agreements with commercial partners (in the consortium or beyond it) and/or system integrators (in the consortium or beyond it) to transfer the technology to the industry.

5.2 Value proposition

SAFETY4RAILS Information System value proposition comprises the key value added by each of the individual tools integrated in the system, as well as the value added by their synergies. This includes the value propositions from the products described in Section 4, but also that of the solutions developed by academic/research partners. All of them were listed and combined into 7 simplified groups, following an assessment of the core value-added by the whole system:

- **Holistic resilience analytics,** consolidating and correlating all relevant indicators and legacy systems (CCTV, microphones, presence sensors, etc…) to produce real-time alerts. Integration of the data ecosystem of the railway infrastructure enables Big Data Analysis, predictive analytics (being ahead of the threat) and event correlation to detect hidden patterns.
- **Digital, easy and fast dynamic and static risk management**. Risk assessment is transformed from a complex, costly and non-reactive process into a user-friendly, reactive and automatised service. Furthermore, integration of the data ecosystem from the railway infrastructure unlocks real-time decision-support about ongoing risks.
- **Multi-level multi-threat infrastructure simulations.** Railway infrastructure resilience can be assessed for the implementation of optimal countermeasures at multiple levels, from the station to the whole network, and at multiple threat scenarios, allowing the discovery of unknown vulnerabilities.
- **Cost-effective, less time consuming and proactive asset management.** Data-driven decision support for life-cycle management of the infrastructure, including proactive interventions and detection of weak components in the system giving indication of priority of intervention and therefore delivering a good maintenance plan. Optimal budgetary strategies are proposed to optimise investment cost and minimise recovery time.
- **Seamless authentication, true randomness and uniqueness of crypto-keys**. S4RIS contributory tools PRIGM/Senstation provide the capability to secure any critical data where it is generated and stored, as well as assures the security of data on transit.
- **Unlocked Common Operational Picture and Cyber-physical Situational Awareness.** Cyber and physical layers of the infrastructure are combined and analysed together through one single system (S4RIS), allowing preparedness against complex heterogenous threats, rapid detection and understand of how IT and OT domains are affected, and improved (and therefore less costly) response.

- **Intelligence-driven targeted decision-support.** Countermeasures/mitigation measures are proposed to the security operator, powered by the intelligence produced by the system. Less time of reaction and better countermeasures are implemented as a result.

The value propositions described above present a significant competitive advantage with respect to other solutions in the market. These features are tightly linked to benefits offered to the primary customer (Railway Infrastructure Managers), which involve the following:

1. **Operating expenses reduction and resource optimisation**
2. **Risk minimisation**
3. **Systemic resilience, with guaranteed and enhanced performance** against inside and outside threats

5.3 Business model canvas

<table>
<tr>
<td rowspan="2">Key Partners
As defined in Section 3.4.2:
• System Integrators
• Reseller distributors
• Business partners with related expertise in the sector
• Regulatory experts
• Cloud hosting service provider</td>
<td>Key Activities
As described in D10.9, Section 3.5.</td>
<td rowspan="2">Value Propositions
• Holistic resilience analytics, consolidating and correlating all relevant indicators
• Digital, easy and fast dynamic and static risk management
• Multi-level multi-threat infrastructure simulations
• Cost-effective, less time consuming and proactive asset management
• Seamless authentication, true randomness and uniqueness of crypto-keys
• Unlocked Common Operational Picture and Cyber-physical</td>
<td>Customer Relationships
• Commercial demonstration and hands-on training sessions
• Customer support including consultancy activities, customisation, integration with legacy systems, software updates and maintenance</td>
<td rowspan="2">Customer Segments
<u>Primary customer:</u>
Railway Infrastructure Managers

<u>Secondary customers:</u>
Other transport infrastructure managers (e.g. bus companies, ports, airports, etc…)
Other critical infrastructures (energy, banking, health, telecom,…)</td>
</tr>
<tr>
<td>Key Resources
• Cloud or local server hosting infrastructure
• Access to sensors and devices used in the infrastructure
• Marketing and commercial expertise
• IPR expertise</td>
<td>Channels
• Engagement with EU buyers through pre-commercial procurement
• Direct procurement (sales) to Railway Infrastructure Managers
• Procurement (sales) cooperation with system integrators</td>
</tr>
</table>

		• Situational Awareness • Intelligence-driven targeted decision-support		
Cost Structure • Deployment, integration, maintenance costs, including technical team, equipment and certifications • Sales&Marketing, customer support, management teams • Software licenses • Cloud/server hosting costs for the S4RIS platform • PCP end-user participants royalty fee			**Revenue Streams** • Upfront fee from direct sales (procurement) of the S4RIS • Subscription fee (yearly) for maintenance, consultancy and training for S4RIS buyers • Royalty fee from system integrators	

5.4 Risks and mitigation measures

	Description of Risks	Degree of criticality (1 low-10 high)	Probability of risk (1 low - 10 high)	Risk Grade	Potential intervention	Estimated Feasibility/Success of Intervention (1 low- 10 high)	Conclusion
Partnership Risk Factors							
1	Partners do not follow the exploitation schedule due to lack of business competencies or technology transfer from academia	*7*	*4*	**28**	Regularly review opportunities for the joint exploitation and perform meetings to evaluate when needed	*7*	**Control.**
2	Partners carries out low quality exploitation activity	*7*	*3*	**21**	Regular meetings to improve performance and update partners on new developments, exchange on experiences, etc	*6*	**Control.**
3	Partners quit executing the exploitation plan (technical or end-users)	*9*	*2*	**18**	Partners are committed and already seeking additional opportunities to follow-up with the S4RIS development	*5*	**Between Control & No Action**
Technological Risk Factors							
4	User interface and experience do not cover all end-user usability needs	*8*	*7*	**56**	Redesign/customise UI and UX to conform the end-user usability needs and run usability tests	*8*	**Action!**
5	Integration in third parties' software is problematic	*8*	*5*	**40**	Invest in improving interoperability and data exchanges protocols	*7*	**Control.**

6	The system is not scalable and fails to provide some of its capabilities when deployed with a large number of assets	*10*	*5*	**50**	Extend data storage and processing capabilities and evaluate more complex scenarios	*8*	**Between Control & Action**
7	Lack of validation reliability of results for individual and/or combined tools	*8*	*7*	**56**	Perform further testing campaigns to ensure results platform-wise are reliable	*7*	**Action!**
Market Risk Factors							
8	Nobody buys the product. Too expensive costs	*8*	*4*	**32**	Review cost structure and licensing strategy	*4*	**No Action'**
9	Unsuitable marketing force	*8*	*4*	**32**	Increase advertising and hire an account manager to approach customers and suitable key stakeholders enabling commercialisation	*7*	**Control.**
10	Fail to find system integrators enabling transferability of the solutions developed by research partners	*9*	*6*	**54**	SAFETY4RAILS consortium already includes large system integrators who can take this role to enter the market	*8*	**Action!**
IPR/Legal Risk Factors							
11	Legal problems - IPR violation	*6*	*3*	**18**	Liaise with IPR experts and establish appropriate legal/commercial agreements	*7*	**Control.**
12	Legal problems - fail to establish a licensing agreement with system integrators	*8*	*5*	**40**	Liaise with IPR experts and review the framework of the agreement to find alternative economic or legal provisions to address the issues identified	*7*	**Control.**
Financial/Management Risk Factors							
13	Marketing and distribution fail due to a weak strategy	*7*	*4*	**28**	SAFETY4RAILS consortium counts with a strong commercial expertise that can support/revise/optimise the market uptake of the solution	*6*	**Control.**
14	Lack of endorsement from top management	*9*	*3*	**27**	The management teams in the consortium have always supported the project initiative. The investment needed to exploit the research results after the end of the project will be sought through public funding sources such as PCP	*8*	**Control.**
Environmental/Regulation/Safety risks							
15	Fail to comply with existing standards and	*8*	*3*	**24**	SAFETY4RAILS analysed the standardisation	*6*	**Control.**

	procedures in place for railway infrastructures				landscape and integrated all relevant standards as part of its requirements		
16	Fail to comply with applicable legislation at specific countries	*8*	*5*	**40**	Liaise with legal experts in local applicable legislation. SAFETY4RAILS consortium includes partners with wide expertise in the analysis of legal and ethical aspects related to the tools developed that could support the further identification of requirements	*8*	**Control.**

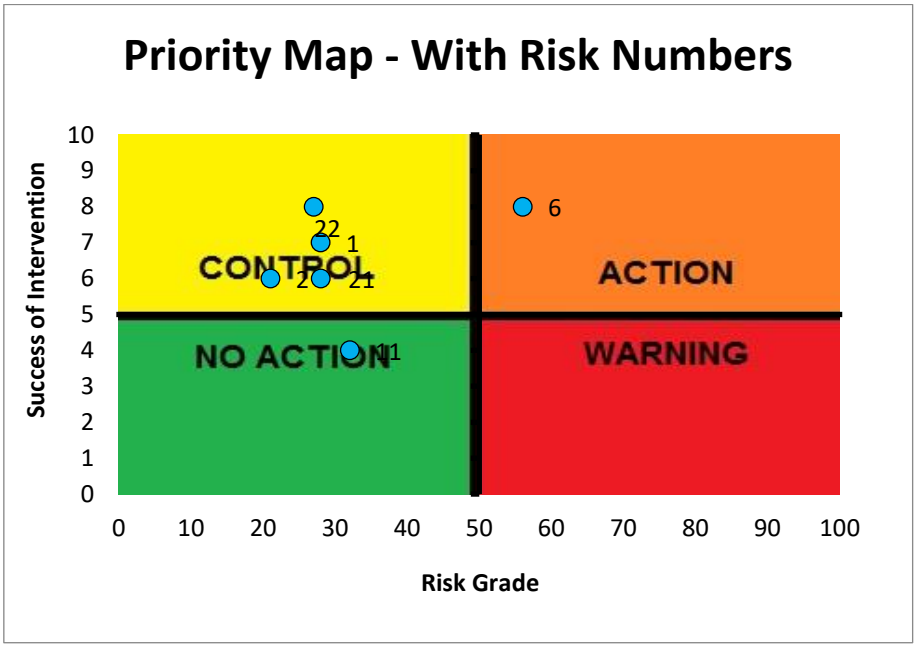

FIGURE 24: S4RIS RISK MAP

5.5 Financial analysis

In this section, a summary is provided regarding the business analysis that has been carried out to elaborate the business plan of the S4RIS. The summary depicts the incomes from the exploitation of the project up to five years after SAFETY4RAILS project closure, the IRR, and the expected ROI. The calculation considers the commercialisation of the platform as a whole, being the sales independent from those from the individual tools sales, as defined in Section 4. The following general assumptions were included in the calculation:

- Pre-Commercial Procurement (Y1&Y2) budget is estimated at €1.4M. This is based on the joint exploitation roadmap reported in D10.9, the investment required to take each of the KERs to the market, described in Section 4 of the present deliverable, and the exploitation plans of the KERs developed by academic partners as reported in D10.9. While PCP can be funded up to 100% under the Horizon Europe programme, a conservative 90% was considered.
- Direct sales (procurement) to Railway Infrastructure Managers are based on an upfront + yearly subscription fee model, as depicted in the business model canvas. The selected price considers expected additional incomes offered to the end-users, which is estimated to be €1.37M/yearly. This

calculation was based on the individual cost-benefit analyses performed on Section 4, as well as the exploitation plans of the KERs developed by academic partners, as reported in D10.9.

- Number of sales consider a total of 6 EU buyers engaged during the PCP project (referring to MDM, PRO, RFI, FGC, EGO & TCDD), who are the most likely to become early adopters, and increasing steadily in the forecasting period.
- Additional revenues will come from licensing contracts arranged with large-scale system integrators who will leverage their network to reach a wider customer base, starting at Y4, where the average income expected is €100k.
- Cost structure includes personnel costs (management, maintenance and customer support, SW updates, marketing and commercial), software licenses, royalties share per IM who participated in the PCP and General Expenses. Royalty share is estimated at 3.75%, based on the industrialisation costs involved in the PCP and the number of EU buyers.
- Considering that the Global Railway Platform Security Market and the Global Railway Cyber Security Market were valued at €2B and €9.8B in 2021, respectively, S4RIS will reach a fairly conservative amount of the overall market in the first years

OPTIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	-	780,900.00	1,565,900.00	2,720,800.00
Costs	-	-	-	590,702.50	962,687.09	1,531,734.26
Financing (PCP-funded)		-	945,000	319,500	-	-
EBITDA calculation	-	-	945,000.00	509,697.50	603,212.91	1,189,065.74
Investments	-	1,050,000.00	355,000.00			
Net cash-flow	-	- 1,050,000.00	443,920.00	459,384.05	532,326.07	989,291.28
IRR (Internal Rate of Return)	37.36%					

PESIMISTIC CASHFLOW SCENARIO

	Y0	Y1	Y2	Y3	Y4	Y5
Incomes	-	-	-	520,600.00	1,250,800.00	1,830,300.00
Costs	-	-	-	502,135.00	884,443.06	1,295,996.26
Financing (PCP-funded)		-	945,000	319,500	-	-
EBITDA calculation	-	-	945,000.00	337,965.00	366,356.94	534,303.74
Investments	-	1,050,000.00	355,000.00			
Net cash-flow	-	- 1,050,000.00	443,920.00	325,432.70	347,578.41	478,576.92
IRR (Internal Rate of Return)	18.89%					

Amortization period of the investment was estimated at 5 years. Corporate tax at 22%.

5.6 Summary of investment case

The consortium performed a thorough risk assessment to identify the most relevant risks that would have an influence on the business strategy of the S4RIS platform. Most of the risks require only to be monitored and those identified as “requiring action” have defined already mitigation actions to be implemented in the roadmap to commercialisation. These are the following:

- *User interface (UI) and experience (UX) do not cover all end-user usability needs.* Further work will be devoted to redesign/customise both aspects. Various iterations will be performed to ensure both technical and usability aspects are fully targeted to the end-user operation. This is expected to be covered during the PCP phase.
- *Fail to find system integrators enabling transferability of the solutions developed by research partners*. System integrators participating in the consortium will be approached with dedicated meetings with Legal/Technology Transfer Offices in order to define the necessary agreements. Alternative system integrators have been already identified in Section 3.4.
- *Lack of validation reliability of results for individual and/or combined tools.* Perform further testing campaigns to ensure results platform-wise are reliable. This is expected to be covered during the PCP phase.

As for the previous financial analyses, NPV (Net Present Value), and ROI (Return on Investment) were calculated based on the financial outcomes described above. An estimated discount rate of 10% (composed of an Average Cost of the capital without risk of 2% more than the risk price estimated at 8%) was used to calculate the NPV. The results show the financial viability of the commercialisation strategy developed.

Even in the pessimistic scenario, a yearly turnover of nearly €1.83M in year 5 is expected, with an IRR of 19%, a NPV of €191k, and a ROI of 19% (considering the further investment required for the PCP and the related funding). Break-even is achieved in Y3 for both the optimistic and pessimistic scenario.

In the case of the optimistic scenario, a yearly turnover of €2.7M in year 5 is expected, with an IRR of 37.36%, a NPV of €735k, and a ROI of 41% (considering the further investment required for the PCP and the related funding).

.

6. Conclusions

The present deliverable has researched the market landscape relevant to SAFETY4RAILS and identified the relevant market segments where the core KERs would have an economic impact. Within the Rail Public Transportation Market, the primary target market, the project will largely contribute to the Railway Platform Security Market and the Railway Cyber Security Market. The fusion of both cyber and physical layers is expected to support the creation of new market segments and the overall growth of the target market. Secondary market segments where the KERs could contribute in the future, following technical adaptations, were also identified.

Emerging business models have been also produced for each of the core KERs developed by the commercial partners. Overall, while some mitigation measures are proposed for very specific risks, the assessment of the business feasibility is positive from both the strategic and financial perspective. Nevertheless, the information presented in this document will be continuously updated as the technology reaches its full maturity, and the market landscape researched is updated with new information.

In the case of the S4RIS platform business model, the consortium performed an assessment of the added value of each tool and the synergies between tools to produce the final value proposition as key input for the Business Model Canvas. An in-depth risk assessment was performed to discover the most relevant barriers, where the necessary mitigation actions will be enforced. Based on this and the financial viability assessment, it was concluded that a EU-funded PCP would largely de-risk the commercialisation roadmap and would work as a key enabler of the platform exploitation as a whole.

The document also depicts incomes coming from the exploitation of the project up to five years after closure, as well as the IRR, NPV and ROI. SAFETY4RAILS will start transferring solutions to the market within a coherent process starting immediately after the end of the project, targeting profits in less than 5 years after the end of the project.

ANNEXES

ANNEX I. GLOSSARY AND ACRONYMS

TABLE 2 GLOSSARY AND ACRONYMS

Term	Definition/description
AI	Artificial Intelligence
ASCII	American Standard Code for Information Interchange
BMC	Business Model Canvas
CAGR	Compound Annual Growth Rate
CCTV	Closed Circuit Television
D	Deliverable
DPI	Deep Packet Inspection
EBITDA	Earnings Before Interest, Taxes, Depreciation and Amortization
EC	European Commission
EGO	Elektrik-Gaz-Otobüs
EU	European Union
FGC	Ferrocarrils de la Generalitat de Catalunya
GDPR	General Data Protection Regulations
GIS	Geographical Information System
IAM	Identity and Access Management
IDS	Intrusion Detection Systems
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Right

IRR	Internal Rate of Return
IT	Information Technology
KER	Key Exploitable Result
LAN	Local Area Network
MDM	Metro de Madrid
NPV	Net Present Value
Ops	Operations
OT	Operational Technology
PCP	Pre-Commercial Procurement
PRO	ProRail BV
R&D	Research and Development
RFI	Rete Ferroviaria Italiana
ROI	Return on Investment
S4RIS	SAFETY4RAILS Information System
SDLC	Software Development Life-Cycle
SSO	Single sign-on
T	Task
TTP	Tactics, techniques and procedures
UI	User Interface
UX	User Experience
VPN	Virtual Private Network
WP	Work Package

ANNEX II. Cashflow Evaluation Template

1.	Estimated price of sale
1.1	Identify which activities associated to the use of your product can provide incomes to the end-users (benefit)

Activity	*Description*	*Estimated additional incomes [€/year]*	*Comments*
	Total		

Assumptions (please specify):

1.2 Price product calculation

Licensing option	
Reasonable profit percentage from end user additional incomes	
Direct purchase (10 years)	
Reasonable profit percentage from end user additional incomes **(relative to 10 years of use)**	
Yearly maintenance and Consultancy services	
Estimated price of reports associated to you product	

	0	1	2	3	4	5
Incomes						
Direct purchase - Complete platform (#)						
Direct purchase - Complete platform (€)						
Yearly licenses (#)						
Yearly licenses (€)						
Yearly maintenance and Consultancy services (#)						
Yearly maintenance and Consultancy services (€)						
Costs						
Personal cost - Direct Labour						
Maintenance and customer support						
SW updates						
Software licenses						
Marketing and Commercial activity						
Other costs						
General expenses						
EBITDA calculation						
Amortization (years)						
Earning Before Interest and Taxes (EBIT)						

Taxes (Country specific)						
NOPAT. Net operating Profit After Tax						
NOPAT (%)						
Investments						
Subcontracting						
Direct labour						
Visualization platform						
Materials						
Others						
Net cash-flow						
Project cash flow (incomes minus costs)						
Working capital (>0 investment; <0 excess)						
Working capital variation						
IRR (Internal Rate of Return)						

SAFETY4RAILS

Partners:

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

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