# SAFETY4RAILS Final Conference

## Main lessons learnt and Recommendations for the future
## From Technical point of view

**Uli Siebold, CURIX, technical coordinator**

SAFETY4RAILS

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

# Agenda

- Project related:
  - Make the project resilient!
  - Data, Data, Data
- Artefact and Product -Related:
  - Overall Resilience Cycle
  - Identification
  - Protection
  - Detection
  - Response
  - Recovery

Extract out of the final brochure

# Project related lessons learned
# Or:
# Is a project dealing with resilience resilient?
(TM personal perspective)

Main project challenges impacting technical aspects

- We planned without Covid
- We had last minute changes
- We had an ultra-tight schedule anyway

- We were relying on potentially sensitive data of end-users during the project

# What we learned (project related)

- We planned without Covid
  - Fast adaption to online meetings
  - Psychologically challenging

  ➔ Be patient, stick to succesfull workflows (e.g. plan the meetings, have agendas), prepare to repeat things (statements, requests, descriptions) more often

- We had last minute changes
  - Professional coordinator! Thanks a lot to Stephen – to handle this
  - Flexible team, transparent communication about possibilities, open minded partners

  ➔ Choose your consortium well! Modify winning teams only marginal

# What we learned (project related)

- We had an ultra-tight schedule anyway
  - We could not work on all our optionals or nice-to-haves
  - We agreed on minimal valuable outcomes that we can accept

  ➔ Have an excellent coordinator (thanks again Stephen) that has all constraints in mind and keeps a close communication channel with EU officer;
  declare nice-to-haves in the beginning (and/or declare must-haves)

- We were relying on sensitive data of end-users during the project
  - Sensitive data usage difficult to handle in projects like this; data-owners have long processes
  - We asked early, we generated data and have let end-users confirm, we used open data

  ➔ Try to assure data availability already in proposal phase. Increase trust in data usage; maybe even new concepts for data persistency need to be consider: e.g. self-destructing data

# Project content – lessons learned

- Overall Resilience Cycle
- Identification
- Protection
- Detection
- Response
- Recovery

# Overall Resilience Cycle

- Data modeling
  - Usage of proprietary model representations
  - ➔ Consider well established model representations fit for purpose or generic
- Data gathering and availability
  - Individual data stores per tool – for demos
  - Bus allows sharing of data within our platform
  - Shared space: repository of data as basis for data generation
- Data security
  - Project-wise: consider anonymisation, self-destructing data
  - Toolwise: conceptwise considered, not rated as innovation relevant
- Guidance through our tool
  - We achieved to implement a collaborative platform
  - ➔ Open point: guidance through the process by the platform itself

# Identification - Phase

- Asset management
  - Made fit for purpose (railway domain)
  - ➔ IT specifics, extreme events to be added
- Risk assessment
  - Methodology: Scenario-based vs. Threat-Vulnerability-Attack
  - Simulation requires adequate information
  - ➔ Legislative aspects to be added; adress more effective information gathering
- Risk management strategy
  - Mitigation measures taken into account (simulation and quantitative analysis)
  - ➔ Enhancement possibilities in simulation model identified;
  - ➔ UX enhancements for quantitative analysis identified

# Protection - Phase

- Monitoring method
  - Open-Source intelligence in use
  - ➔ Cooperation between stakeholders and threat intelligence providers should be intensified

- Cascading effects analysis
  - Core algorithm improvement potentials identified
  - ➔ Consider historical data

# Detection - Phase

- Anomalies and events detection
  - Demonstrated CCTV capabilities in the light of anomaly and event detection
  - ➔ Extend experiments in operational environments
  - ➔ Configuration simplifications identified
  - ➔ Cyber-Threat: automatization is seen as a high potential for actionable intelligence

- Real time monitoring
  - Anomaly detection demonstrated for real data as well as for simulated data
  - ➔ Motivated, that monitoring of additional sensor data could lead to increased awareness

# Response - Phase

- Crisis management
  - Desicion Support implemented in S4RIS
  - ➔ Feedback showed that explainable results of analytic tools would be rated as helpful

- Crisis communication
  - Lack of academic research identified
  - Crisis communication guidance is applicaple to cyber-attacks
  - ➔ Perform academic studies
  - ➔ elaborate on uniqueness of crisis communcation for cyber-attacks
  - ➔ improve awareness of ethical-security risks existing in crisis communication

# Recovery - Phase

- Recovery planning
  - Integration of predictive maintenance tool in S4RIS

  ➔ Potential identified to consume cyber-physical events to improve accuracy of budget charts and predictive investing models

  ➔ Feature optimizations identified, e.g. audit management functionality

# Conclusions / Summary

- Key take aways for next project
  - Resilient project
  - Take care about data early!
- Individual improvement possibilites for roadmaps
  - Per tool provider
  - Per research partner
- Concrete features identified that need to be implemented for productive version: e.g. authentication, encryption

# Thank you for your attention!


Uli Siebold

CuriX

uli.siebold@curix.ai


## SAFETY4RAILS Consortium:

# SAFETY4RAILS Final Conference

## Main lessons learnt and Recommendations for the future From End-Users point of view

Marie-Hélène Bonneau, UIC, end-user coordinator

SAFETY4RAILS

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

# Agenda

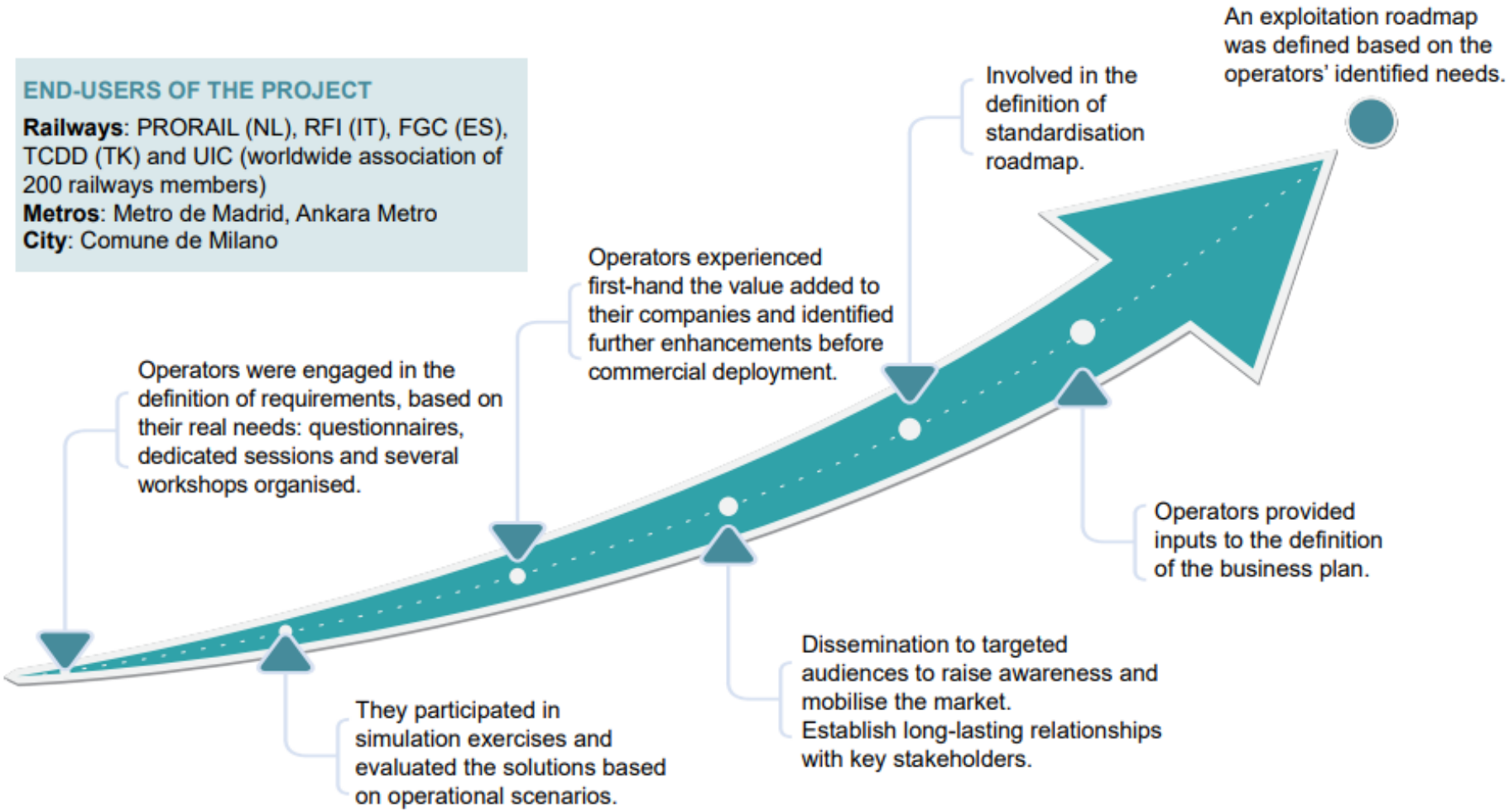
- Uptake of the results by the operators
- Simulation exercises
- Evaluation of the S4RIS platfom
- Related deliverable

Extract out of the final brochure

# Uptake of the results by the operators

**END-USERS OF THE PROJECT**

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



# Simulation exercises

- **From January 2022 until July 2022, four simulation exercises were performed:**
  - **Madrid (Metro de Madrid):** Combined cyber-physical attack at the metro station close to the stadium during a large sporting event.
  - **Ankara (EGO and TCDD):** Series of cyber and physical attacks targeting sensitives devices and sensors.
  - **Roma (RFI):** Physical attack – Potential terrorist attack via IED carried via baggage and terrorist using firearms inside a railway station.
  - **Milan (CDM):** Natural Disaster - Flooding in the city during a major event.

- Each simulation exercise was evaluated by the end-users through questionnaires, debriefings and focus groups. The evaluation focused on two main aspects:
  - The organisation of the exercise (as carried out).
  - The performance of the S4RIS against pre-defined objectives related to:
    - **Usability**.
    - **Specific requirements** laid out by the end-users.
    - **Scenario-based requirements/objectives**

# Evaluation of the S4RIS platform by the end-users (1/3)

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

## Main added value of the tools higlighted during the evaluation:

- **The combination of the capacities** of the tools with the dashboard **grouping all the alerts** coming from the different tools addressing both cyber and physical threat provides a very good situational awareness to the end-users.
- **The simulation capacities** bring a lot of added value for managing cyber and physical risks and helping decision makers on the measures to be put in place to make rail and metro systems more resilientThe knowledge on
- **The detection tools** which demonstrated early detection of anomalies or vulnerabilities were appreciated by most of the responders for anticipating situation and preventing or mitigating the consequences of cyber and physical attacks.

# Evaluation of the S4RIS platform by the end-users (2/3)

## Some possible improvements highlighted by the end-users:

- Simulation capacities would benefit from more accurate data as well as more variables.
- The integration of the S4RS tools with the company information systems would need to be assessed.
- The integration of tools in the S4RIS platform should be further developed.
- Inclusion of user manuals and change management schemes, adapted to each end-user, for the adequate implementation of the S4RIS platform in different environments and OT systems.

# Evaluation of the S4RIS platform by the end-users (3/3)

## Main challenges

- **Provision of operational data**
  - Sensitivity of data
  - Data regulation
- **Organisation of the simulation exercises**
  - Even more realistic conditions (e.g. test site) and further extended tests
- **Evaluation of the solutions**
  - Duration of the project too short (2 years) for such a broad scope and many tools
  - The tools are very innovative, most of them are based on artificial intelligence which is at a very early stage within rail companies.
  - Many different areas of expertise were needed to answer the questions, so that experts from one domain were not able to answer questions pertaining to another and vice versa.

# Main related public deliverables

| No | Work Package and Deliverable name | Lead participant |
|---|---|---|
| **WP2** | Requirements, specification and architecture of SAFETY4RAILS framework | CEIS |
| **D2.2** | Report on past failure analysis and lessons learnt | CS |
| **WP8** | Simulation Exercises and Evaluations in Operational Environments | UIC |
| **D8.1** | Evaluation Methodology | UIC |
| **D8.3** | Final version of development of a blueprint exercise handbook | LDO |
| **D8.5** | Final version of evaluation report | LAU |
| **D8.6** | Lessons learnt from SAFETY4RAILS for future research projects | EGO/UIC |

# Thank you for your attention!


Marie-Hélène Bonneau

UIC

bonneau@uic.org


## SAFETY4RAILS Consortium:

# SAFETY4RAILS Final Conference

## Contribution to compliance with EU directives and recommendations

EOS

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

# Table of contents

# EU Critical Infrastructure Protection Framework

*Council Directive 2008/114/EC & (proposed) Directive on the resilience of critical entities*

- Rail and metro infrastructures are 'European critical infrastructures' (ECI) or 'critical entities'
- **Obligations will be extended:**
  - to conduct risk assessments and take resilience enhancing measures against all relevant man-made and natural non-cyber risks;
  - to notify disruptive incidents without undue delay to the relevant national authorities.
- Resilience enhancing measures include:
  - disaster risk reduction and climate adaption measures;
  - fencing, barriers and perimeter monitoring tools;
  - implementation of risk and crisis management procedures and protocols and alert routines;
  - business continuity measures and the identification of alternative supply chains;
  - employee security management and training.

# EU Cybersecurity Framework

*Directive (EU) 2016/1148 & (proposed) Directive on measures for a high common level of cybersecurity across the Union.*

- Rail and metro operators are 'operators of essential services'
- **Obligations:**
  - take cybersecurity risk management measures based on an 'all-hazards approach' to protect both the network and information systems and their physical environment from incidents.
  - prevent and minimise any incidents and their impact on the network;
  - notify competent authorities of such cyber-incidents.
- **Baseline measures:**
  - risk analysis and information system security policies;
  - business continuity, such as backup management and disaster recovery, and crisis management;
  - supply chain security;
  - vulnerability handling and disclosure;
  - testing and auditing to assess the effectiveness of cybersecurity risk management measures;
  - use of cryptography and encryption;
  - basic cybersecurity training.

# SAFETY4RAILS Contribution

*SAFETY4RAILS Information System (S4RIS) platform*

- Risk assessment tools:
  - E.g., railway-component-specific risk assessment tools (SecuRail); decision-support systems (RAM2); threat intelligence (TISAIL)
- Early detection of threats:
  - E.g., object detection (GANIMEDE); anomaly detection (CURIX, WINGSPARK); crowd monitoring (iCrowd)
- Simulation and prediction tools:
  - E.g., prediction (BB3d, CAESAR, DATAFAN, SARA)
- Planning and business continuity measures:
  - E.g., asset management (CAMS)
- Crisis communication framework
- Ethics & Data Protection

# SAFETY4RAILS Policy Recommendations

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

# Thank you for your attention!


Angeliki Tsanta, Juliette Vieillevigne

European Organisation for Security (EOS)

angeliki.tsanta@eos-eu.com

juliette.vieillevigne@eos-eu.com


## SAFETY4RAILS Consortium:

# SAFETY4RAILS project

## Go-to-market Roadmap, next steps after SAFETY4RAILS

ETRA&EOS

# Exploitation Strategy

## Individual Exploitations Plans & S4RIS Exploitation Strategy

# Project Results

- >30 exploitable results (tools, guidelines, methodologies)
- All partners are committed to taking the necessary actions to exploit their IP and ensure that the impact of SAFETY4RAILS will continue after the end of the project.

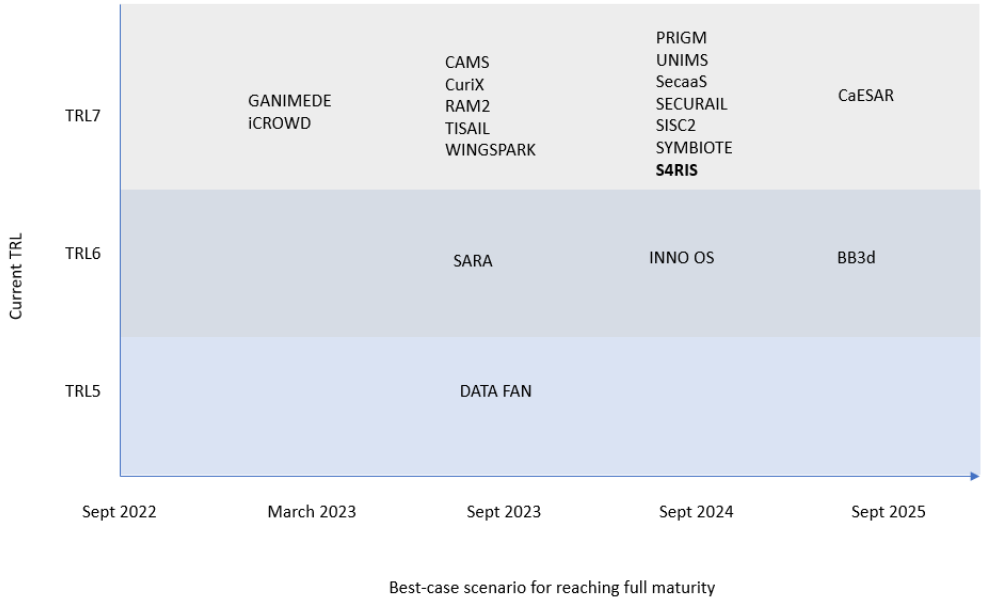
TABLE 2 OVERVIEW OF PROJECT FOREGROUND

| No | Owner | Type of Exploitable Foreground | Description of Exploitable Foreground | Background needed to use Foreground | Exploitable product(s) | Is this a KER (Key Exploitable Result)? | Sectors of application | Status and schedule for exploitation | Planned IP protection strategy | Other Beneficiaries involved |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | RINA-C | Tool | BomBlast3d computes the loading due to the blast wave impact over structures such as buildings and supplies the main physical quantities of interest both over the wall surface of three-dimensional models (e.g.), virtually reproducing potential attractive targets for terrorists, and in air. | BomBlast3D (know-how) | BB3d | YES | Infrastructure, Railways, blast-design, retrofitting, Security | TRL5 to TRL6 at the end of the project.<br><br>3 years until full maturity. | Know-how | None |
| 2 | AC | Tool | Block-chain based system for the exchange of sensitive information between CI. The system would be based on a REST-based interface to provide the possibility to manage heterogeneous data, coming from multiple sources, and for the implementation of easy-to-use APIs. | Expert know-how of design, development, implementation and validation of data sharing infrastructures based on blockchain technologies | Blockchain solution | NO | Critical infrastructure, railways, Security | TRL1 to TRL5 at the of the project.<br><br>At least 3 additional years until full maturity. | Know-how | None |
| 3 | Fraunhofer | Tool | Cascading effect simulation to assess and increase resilience. Simulation tool for computing cascading effects within critical infrastructure and especially across | CaESAR (know-how) | CaESAR | YES | Critical Infrastructure, Resilience analysis and management | TRL5 to TRL7 at the end of the project. | Know-how | None |
| 22 | UIC | Methodology | applied to the equipment of the station in order to reduce the effects of a terrorist attack. | | | | | | | |
| 23 | UNEW | Web-based Integrated tool platform | | | | | | | | |
| 24 | RINA-C | Tool | | | | | | | | |

# Partners' individual exploitation strategies

Guidelines & Methodologies are ready for direct exploitation.
Within 3 years, all tools will reach full maturity.

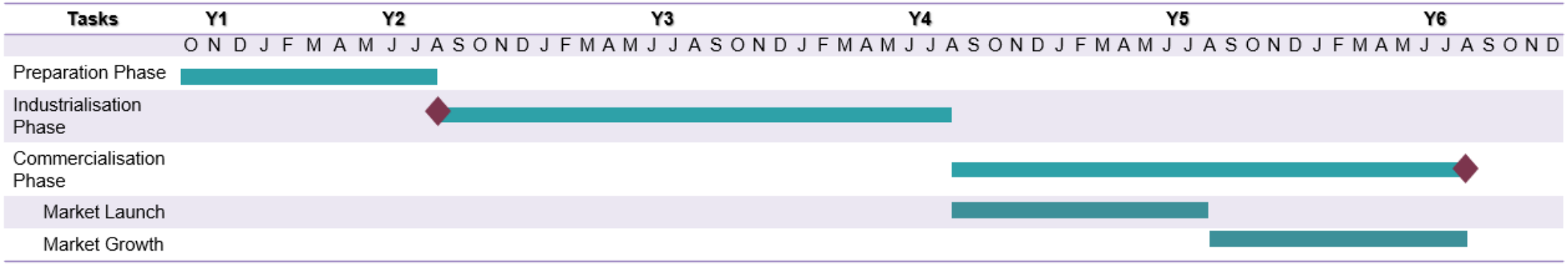
- Industrial partners:
  - will continue the development of their results using own resources and R&D funding
  - mechanisms already in place for market uptake.
- Academic/Applied Research partners:
  - knowledge transfer through scientific publications, seminars and teaching activities.
  - technology transfer to system integrators/spin-offs
- SAFETY4RAILS end-user representatives (rail and metro operators):
  - disseminating SAFETY4RAILS results
  - cooperating with providers to allow them to reach their markets.




Best-case scenario for reaching full maturity

# S4RIS exploitation strategy

5-year plan for market entry.




- Exploitation Plan (tentative planning):
  - Phase 1 – Preparation: At least one-year-long after the end of the project
  - Phase 2 – Industrialisation: Years 2 & 3
  - Phase 3 – Commercialisation: Years 4 & 5
- Actors involved: SAFETY4RAILS technical partners as well as end-user partners
  - A list of interested partners is being kept by the consortium to kick-start this process.

# Proposed exploitation plan*

*The plan and timeline proposed are tentative and should be further explored and adapted to the available funding opportunities

## Y1: PREPARATION PHASE

- EU buyers would prepare and launch the Pre-Commercial Procurement
- Technical partners would perform market promotion actions to engage early adopters

## Y2: INDUSTRIALISATION PHASE – 1ST YEAR OF THE PCP PROJECT

- Customisation&adaptation of the UI/UX to specific end-user usability needs
- Scale the SAFETY4RAILS solution to the management of large volume of data
- Developed additional modules/features required by the end-users (if any)

## Y3: INDUSTRIALISATION PHASE - 2ND YEAR OF THE PCP PROJECT

- Develop and test pre-operational system
- Full integration and deployment with legacy systems at the end-user premises
- Perform the certification of the S4RIS according to the required standards

## Y4: COMMERCIALISATION PHASE – MARKET LAUNCH WITH EARLY ADOPTERS

- Selected business partners will establish a salesforce, marketing and customer support team
- Specific procurement mechanisms will be launched from the end-user side to adopt the solution
- Further training activities will be performed with the end-user to facilitate adoption

## Y5: COMMERCIALISATION PHASE – MARKET GROWTH AND EXPANSION THROUGH THE EU

- Launch commercial activities with Railway Infrastructure customers in other countries with high market value
- Close licensing contracts with large-scale system integrators

# Market Analysis and Business Plans

## Market landscape & Emerging Business Models

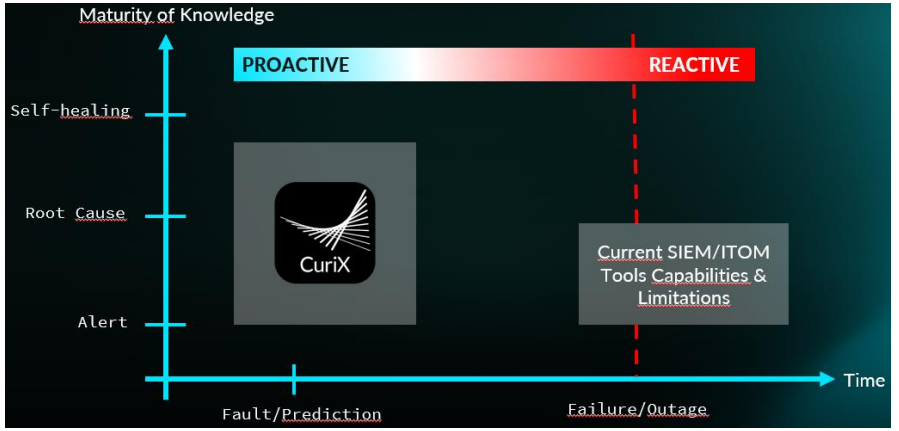
# SAFETY4RAILS positioning in the market

| | |
|---|---|
| Global Railway Platform Security Market | • **Commercial/Business Partners:** Ganimede (LDO), BB3d (RINA), SARA (RINA)<br>•**Research/Academic Partners:** CAESAR (FHG), iCrowd (NCSRD) |
| Global Railway Cyber Security Market | •**Commercial/Business Partners:** UNIMS (ICOM), SecaaS (ICOM), TISAIL (TREE)<br>•**Research/Academic Partners:** N/A |
| ***Supporting creation of new markets*** | •**Commercial/Business Partners:** CURIX (CURIX AG), PRIGM/Senstation (ERARGE), RAM2 (ELBIT), SISC2 (ICOM), SecuRail (STAM), WINGSPARK (WINGS)<br>•**Research/Academic Partners:** CAMS (RMIT), DATAFAN (FHG) |

## Competitive benchmark analysis

In general, the analysis performed highlights that most of the tools are innovative or even pioneers in the field. Some of the most relevant benefits (not limited) with respect to competing solutions:

- Risk assessment considering **real-time data** and **geographic positioning**
- **Self healing**
- Threat intelligence **tailored to railways infrastructure**
- Integrated **cyber-physical** security platform



# Emerging Business Plans from commercial/business partners

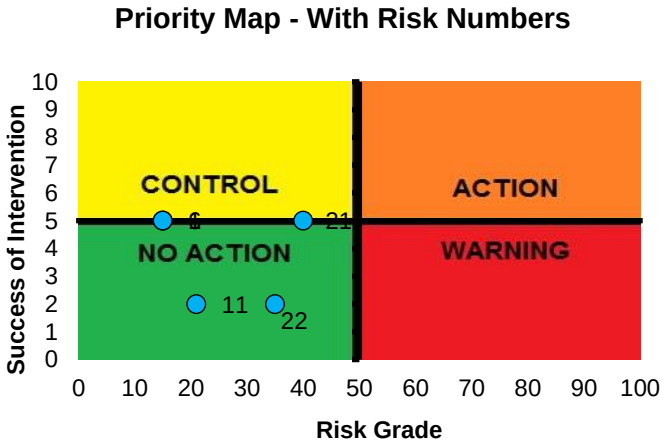
## Value proposition

Describe the competitive advantages of each KER, benefits based on what the user/customer wants.

## Business model canvas

Customer Segments, Channels, Customer Relationships, Key Partners, Key Activities, Value Propositions, Key Resources, Revenue Streams, Cost Structure.

## Risks and mitigation measures




While some mitigation measures are proposed to very specific risks, the assessment of **the business feasibility is positive from both the strategic and financial perspective**. Nevertheless, business models will be continuously updated as the technology reaches its full maturity, and the market landscape is researched.

## Financial analysis

- Activities that can provide incomes to the end-user (benefit)
- Price product calculation
- Estimate cashflow (optimistic vs. pessimistic scenarios)

# S4RIS business plan

<table>
<tr>
<td>Key Partners<br><br>As defined in Section 3.4.2:<br><br>• System Integrators<br>• Reseller distributors<br>• Business partners with related expertise in the sector<br>• Regulatory experts<br>• Cloud hosting service provider</td>
<td>Key Activities<br><br>As described in D10.9, Section 3.5.<br><br>Key Resources<br><br>• Cloud or local server hosting infrastructure<br>• Access to sensors and devices used in the infrastructure<br>• Marketing and commercial expertise<br>• IPR expertise</td>
<td>Value Propositions<br><br>• Holistic resilience analytics, consolidating and correlating all relevant indicators<br>• Digital, easy and fast dynamic and static risk management<br>• Multi-level multi-threat infrastructure simulation kernel<br>• Cost-effective, less time consuming and proactive asset management<br>• Seamless authentication, true randomness and uniqueness of crypto-keys<br>• Unlocked Common Operational Picture and Cyber-physical Situational Awareness<br>• Intelligence-driven targeted decision-support</td>
<td>Customer Relationships<br><br>• Commercial demonstration and hands-on training sessions<br>• Customer support including consultancy activities, customisation, integration with legacy systems, software updates and maintenance<br><br>Channels<br><br>• Engagement with EU buyers through pre-commercial procurement<br>• Direct procurement (sales) to Railway Infrastructure Managers<br>• Procurement (sales) cooperation with system integrators</td>
<td>Customer Segments<br><br><u>Primary customer:</u><br><br>Railway Infrastructure Managers<br><br><u>Secondary customers:</u><br><br>Other transport infrastructure managers (e.g. bus companies, ports, airports, etc…)<br><br>Other critical infrastructures (energy, banking, health, telecom,…)</td>
</tr>
<tr>
<td colspan="3">Cost Structure<br><br>• Deployment, integration, maintenance costs, including technical team, equipment and certifications<br>• Sales&Marketing, customer support, management teams<br>• Software licenses<br>• Cloud/server hosting costs for the S4RIS platform<br>• PCP end-user participants royalty fee</td>
<td colspan="2">Revenue Streams<br><br>• Upfront fee from direct sales (procurement) of the S4RIS<br>• Subscription fee (yearly) for maintenance, consultancy and training for S4RIS buyers<br>• Royalty fee from system integrators</td>
</tr>
</table>

# S4RIS business plan

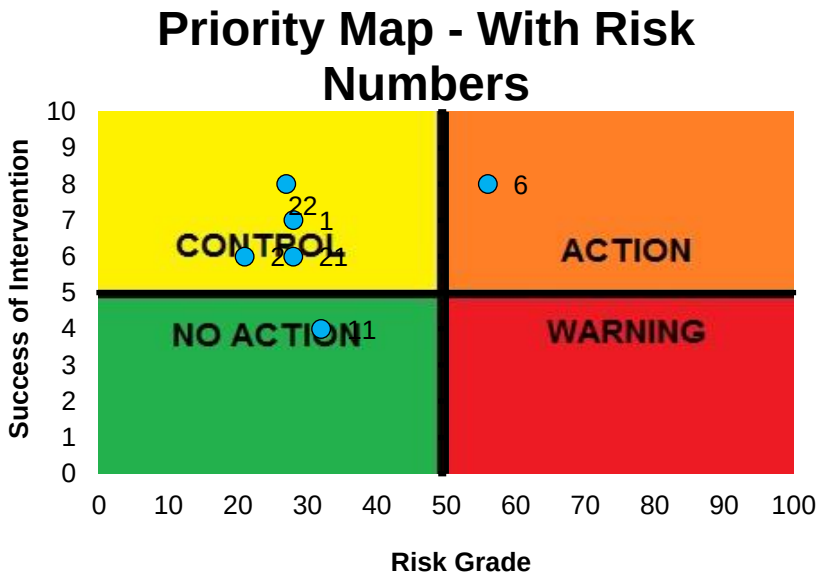
## Risks and mitigation measures

In-depth risk assessment to discover risks potentially hindering commercialisation. Most relevant:

- 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.

## Financial analysis

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.



# Thank you for your attention!


Eduardo Villamor Medina

ETRA

evillamor.etraid@grupoetra.com


## SAFETY4RAILS Consortium: