Deliverable D 4.3

Exploitation Plan

Project acronym:	4SECURail
Starting date:	01/12/2019
Duration (in months):	24
Call (part) identifier:	H2020-S2R-OC-IP2-2019-01
Grant agreement no:	881775
Due date of deliverable:	Month 24
Actual submission date:	29-11-2021
Responsible/Author:	Ardanuy / Albert Ferrer-Bonsoms
Dissemination level:	PU
Status:	Issued

Reviewed: yes

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 881775.

Document history		
Revision	*Date*	*Description*
1	29/11/2021	First issue

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Albert Ferrer-Bonsoms and Lambert Grange	ARD	Structure definition and coordination. General contributions in all sections.
Javier Gutierrez	TREE	Review of all sections.

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

The content of this deliverable does not reflect the official opinion of the Shift2Rail Joint Undertaking (S2R JU). Responsibility for the information and views expressed in the deliverable lies entirely with the author(s).

Table of Contents

1 EXECUTIVE SUMMARY

The present document constitutes the Deliverable D4.3 “Exploitation Plan” in the framework of the WP4. This document provides the purpose of describing the 4SECURail plan for business and exploitation of results. It focuses on the project’s exploitation objectives and methodology.

Being the project split in two workstreams (WS), the first WS1 dedicated to Formal Methods and the second one to CSIRT (Computer Security Incident Response Team), even the Exploitation Plan reflects this structure.

The principal objective for exploitation in the 4SECURail project is to implement an exploitation strategy to facilitate the successful exploitation and adoption of results and benefits within the Railway Sector, research communities and policy advisers. Exploitation activities in the 4SECURail project aim to ensure the longevity of the project’s results through either policy uptake, further research and commercial applications.

The exploitation strategy is largely based on what was described in the proposal and Grant Agreement, but with some refinements arising from the project evolution.

A list of the project results for both workstreams is provided. The Intellectual Property Right Management has been applied according to the Consortium Agreement: anyway, the consortium decided not to protect with patents any project results.

2 ABBREVIATIONS AND ACRONYMS

Abbreviation / Acronym	Description
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CMU	Carnegie Mellon University
CSIRT	Computer Security Incident Response Team
DG	Directorate General
ENISA	European Union Agency for Cybersecurity
ER-ISAC	European Rail - Information Sharing and Analysis Center
ERTMS	European Rail Traffic Management System
EU	European Union
IPR	Intellectual Property Rights
ISAC	Information Sharing and Analysis Centre
JU	Joint Undertaking
MAAP	Multi-Annual Action Plan
NIS	Network and Information Security
S2R	Shift2Rail
SysML	Systems Modeling Language
TD	Technical Demonstrator
UML	Unified Modeling Language
WP	Work Package
WS	Work Stream
XMI	XML Metadata Interchange

3 BACKGROUND

The present document constitutes the Deliverable D4.3 “Exploitation plan” in the framework of Task 4.3 (*Sustainability and Impact Maximization*) of the WP4 (*Outreach and networking*) of 4SECURail project - IP2 S2R-OC-IP2-01-2019 of the Shift2Rail initiative.

It is important to share the know-how acquired by the partners of the 4SECURail consortium with as many railway stakeholders as possible. 4SECURail partners will focus on the presentation of the results through working papers and conferences. Therefore, every single partner will share the results with its clients and present the project during fairs (for example InnoTrans, Expo Ferroviaria, etc…). These efforts will also lead to marketing strategies for later commercial exploitation of new products.

4 OBJECTIVE/AIM

Article 28 of the Grant Agreement stipulates the obligation to exploit the project results:

Each beneficiary must — up to four years after the period set out in Article 3 — take measures aiming to ensure 'exploitation' of its results (either directly or indirectly, in particular through transfer or licensing; see Article 30) by:

a) using them in further research activities (outside the action);
b) developing, creating or marketing a product or process;
c) creating and providing a service, or
d) *using them in standardisation activities.*

The Exploitation Plan has been designed in order to multiply the impact of 4SECURail results and prepare the transition towards industrial and commercial uptake in order to fully achieve the expected impact. The Exploitation Plan will describe the activities to be undertaken (how and by whom) in order to ensure the exploitation beyond the project itself.

The exploitation strategy reflects and is built-up as a result of sound analysis of the market trends, potential users, and financial sustainability.

All partners of 4SECURail are interested in the results exploitation in different manners. Research partners are more oriented to transfer knowledge and technology to interested stakeholders while the industries are focused on industrialisation and future commercialisation of the research products.

The Exploitation Plan is aimed at the following audiences and respectively at the fulfilment of the following objectives:

- European Commission: to communicate the consortium's strategy;
- Consortium partners: to inform about participants' rights and obligations, as well as notify to other participants partners' intentions in order to enable them to exercise their objection right in case their legitimate interest could be impaired.

The document is structured as follows:

- Section 5 describes the results to be exploited and how the Intellectual Property is managed;
- Section 5.1 provides an analysis of the market, describing opportunities, barriers and counter-measures;
- Section 7 focuses on the exploitation strategy, both the joint actions among partners, and their individual partners' exploitation plans.

5 RESULTS TO BE EXPLOITED AND IPR MANAGEMENT

The exploitation of 4SECURail results and the related IPR management are strictly ruled by the 4SECURail Consortium Agreement in addition to the provisions of the 4SECURail Grant Agreement n.881775 (Sect. 3 Rights and Obligations related to results).

The process followed to identify the 4SECURail Foreground knowledge and the relevant IPR ownership complies with the 4SECURail Consortium Agreement, which includes all provisions relating to the management of IPR Foreground knowledge including ownership, protection and publication of knowledge, access rights to knowledge and pre-existing background included as well as questions of confidentiality, liability and dispute settlement.

5.1 WS1 – FORMAL METHODS

The Shift2Rail Joint Undertaking (S2R JU) has identified the use of formal methods as one of the key concepts to enable reducing the time it takes to develop and deliver railway signalling systems, and to reduce high costs for procurement, development and maintenance. Formal methods, together with standard interfaces, have been recognised as needed to ensure correct behaviour, interoperability and safety, reducing long-term life cycle costs at the same time.

The main objective of the 4SECURail Work stream 1 DEMONSTRATOR DEVELOPMENT FOR THE USE OF FORMAL METHODS IN RAILWAY ENVIRONMENT has been to provide a demonstrator of state-of-the-art formal methods and tools to evaluate the learning curve and to perform a cost/benefit analysis of the adoption of formal methods in railway industry.

The following overall objectives have been targeted:

1. The development of the demonstrator consisting of the process to be followed to provide a formal validated model of a smart signalling system, and of a list of the most suitable tools to support such process.
2. The identification of a railway signalling subsystem, described by means of standard interfaces, to be used as test case to exercise the formal methods demonstrator.
3. The specification and evaluation of the cost/benefit ratio and learning curves for adopting the demonstrator in the railway environment.

It is not a goal of the project to push forward the state of the art of formal methods and tools, but just to collect, through a controlled experiment (the demonstrator) in applying state-of-the-art tools and methodologies, meaningful information and data on one of the possible paths that could be followed to associate the definition of standards and system requirements definitions with a formal basis.

The results of the Work Stream 1 are well summarised in the produced Project Deliverables of the various tasks of Work Package 2, and consist in:

- D2.1-D2.2-D2.5: An exemplification of how state-of-art formal methods might be exploited for the construction of high-quality railway signalling standards and, more in general, of rigorous system requirements specifications. In particular, some of the most relevant information provided in D2.5 illustrates with a specific example:

+ How the SysML/UML notation might be exploited as intermediate notation between natural language and formal models, to facilitate communications between the system requirements specifiers, system requirements users and the formal modelling and analysis activity.

+ How the structure of the natural language requirements structure might be improved by taking into account the existence of an underlying executable semiformal/formal model.

+ How formal analysis can be applied with almost no effort by exploiting (even if in limited way) formal methods in a simple push-button like way to detect problems in the generic system design and its executable implementation.

+ How advanced formal verification techniques can provide important feedback on the actual behaviour of the system under specification, helping to increase the confidence level on the absence of problems that might affect the system interoperability with the other systems of the infrastructure.

+ How the adoption of a safe, clear, strict, subset of SysML/UML might pave the way to mechanical, formally verifiable, translation of the UML system design into multiple formal models.

- D2.3: The description of a reasonably simple, but meaningful, signalling case study that fits well the purpose of testing the suitability of the role of formal methods for the improvement of the quality of system requirements specifications and standard interface definitions.

- D2.4-D2.6: A quantification of how much such exploitation of formal methods might affect the costs, and generate savings, of developing high quality specifications, and how many benefits for the rail industry, for rail users and for the society might arise from the choice.

Performing a formal analysis of a standard interface is a very different, and more difficult task than performing a verification of a specific product specification. The differences are in the process adopted, the tools used and the results expected.

In the case of the standard interfaces, we are likely to have a more generic specification with many parameters and options, and its description is likely to be at a higher level, not forcing any unneeded implementation detail. This is quite different from the case of a specific product specification, where parameters and option can be somewhat constrained, and where it can be acceptable that certain implementation choices are made.

So, while in the case of a specific product we might have the goal of validating the specification e.g. with respect to its safety and interoperability requirements, in the case of a generic, abstract standard interface our goals cannot go further than a partial formal analysis of these properties, built on the construction of various specific scenarios, possibly abstracting some aspects not needed for the verification of the intended properties, and possibly making specific implementation choices. This does not mean at all that the formal analysis is not useful, but just that the undergoing process and result should not be confused with the one of verifying a specific system specification. The project results (and in particular D2.5) allow to better put in light these aspects.

All the results of the Workstream 1 are public and available in open access. There is no foreground knowledge that needs to be protected by a patent.

5.2 WS2 – CSIRT

The Shift2Rail Multi-Annual Action Plan (MAAP) TD2.11 - Cybersecurity requires, under the Output 3 of the Technical Objectives, to Develop a network of Railway Cybersecurity Experts (CSIRT):

"This network of experts will analyse the feasibility of the deployment of a railway dedicated CSIRT (Computer Security Incident Response Team)/ISAC (Information Sharing and Analysis Centre). In case of positive answer, this network would be the basis of the CSIRT/ISAC and will propose a prototype of the ontology and of the workflow network model to support this CSIRT/ISAC."

Along with the development of S2R TDs aiming at digitalization of railway sector and the introduction of wireless and "open" communications, the need to protect railway assets against cyber-attacks is becoming imperative. The common approach on a cyber security method shall be adopted by all impacted railways stakeholders to reduce costs and time-to-market of proposed solutions. 4SECURail will help to meet these challenges of rail transportation system.

The 4SECURail work stream 2 SUPPORT TO IMPLEMENTATION OF CSIRT TO THE RAILWAY SECTOR will address TD2.11, establishing a CSIRT collaborative environment.

The CSIRT is a multi-layered model (Organisational, Operational, Technical Platform) developed in collaboration with the relevant stakeholders (Railway Chief Information Security Officers – CISOs, along with Railway IT overall management and concerns). The main aim of WS2 is to deliver a pilot CSIRT model for Railway, co-designed and owned by those stakeholders, along with a working pilot platform (Collaborative Environment) also co-designed with those stakeholders to ensure ownership and future uptake.

The work stream 2 specific objectives have been:

1. To define stakeholder requirements for a European Rail CSIRT collaborative activity, and to co-design with them a first draft CSIRT model for open consultation.
2. To test and validate the draft CSIRT model, and to obtain sufficient feedback and co-design input to release the final CSIRT model to support organisational collaboration, as well as collaborative platform design.
3. To identify relevant platforms to support CSIRT collaboration and, based on requirements and CSIRT model, specify and adapt to meet CSIRT needs.
4. To test and updated the CSIRT collaborative environment so as to ensure meeting user needs.

4SECURail partners agreed not to apply for a patent to protect this foreground but rather to use the knowledge acquired as a competitive advantage and offer commercial consultancies to potential clients. Additionally, 4SECURail partners are committed to exploiting the foreground in future Research and Innovation activities.

Moreover, 4SECURail partners have identified the following pieces of foreground knowledge that, even though not suitable for protection with a patent, could be further exploited in the research sector:

- The creation of a CSIRT/ISAC model as a collaborative platform at European level extends beyond purely response to threat intelligence and information sharing.

- The network of cyber security experts dedicated to the rail sector is created under the umbrella of the ER-ISAC.
- Data flows and workflows for a CSIRT/ISAC model are focused on intelligence building and information sharing for threats (incidents and/or vulnerabilities).
- The validation of the CSIRT/ISAC collaborative model should be built based on a bottom-up approach, on top of the existing processes and tools, and as a hub centre for threat intelligence expertise.
- The management, integration and deployment of MISP-related tools, as the Open-Source platform which seems to stand one step further than other solutions and is the base for the CSIRT/ISAC collaborative platform.
- Insights of use cases in the railway sector.
- Good practices in the field of threat intelligence applied to the railway sector.

6 MARKET ANALYSIS

6.1 WS 1 – Formal Methods

6.1.1 Market description

The project demonstration of how state-of-the-art formal methods might be exploited for the construction of high-quality railway signalling standards, and the analysis on the implied costs and benefits in pursuing this approach, would be of main interest to infrastructure managers and standardisation bodies in order to make informed choices on the process to be followed to create higher quality standards and system requirements specifications.

The need of high-quality standard interfaces is in fact widely recognised by Shift2Rail as a necessary step to reduce to costs of designing, creating and safely operating complex railway infrastructures, and several activities (EULYNX, ERTMS) have been set up precisely with this purpose. The exploitation of formal methods during this phase of standardisation and system requirements definition is being recognised as a potentially essential component to raise the quality of the produced specifications, and several other ongoing initiatives (X2RAIl2, X2RAIL5, FORMASIG) are also contributing to sheding more light on how this might be handled.

Also from the manufacturer side, the raising of awareness about the current trend of backing standard interfaces with formal methods might be a stimulus for being prepared to the evolutions in the market that this transition might generate.

Currently, the market of commercial formal methods tools and frameworks is mainly targeted to the phase of final product development (with the aim of reducing validation costs, see e.g., SCADE, Systerel S3, AtelierB, Simulink, Prover/ILock/Ovado) rather than to the initial phase of requirements definition. The raising of the awareness of the importance of the use of formal methods also in this initial phase might hopefully lead to an improvement of the current commercial offer also from this alternative point of view.

On the contrary, most of the advanced tools and techniques fitting well 4SECURail WS1 goal are being developed inside the academia and research centres, and often lack the level of reliability, the integration within the industrial processes, the level of support and training needed by industry. The situation is made more complex also by the absence of any "best" formal approach or technique and by the resulting great fragmentation of the proposed solutions.

6.1.2 Barriers and counter-measures

SysML/UML is being considered as a de facto standard as a semi-formal notation for complementing natural language requirements specification, and might represent a good starting point for the application of formal methods. Unfortunately, in spite of the recent attempts to clarify its definition (fUML, PSSM, Alf), the use of this notation raises severe problems of non-uniformity of semantics that might be associated with an SysML/UML design. The counter-measure adopted in the project has been to make use of a severely constrained subset of the notation that can be associated with a precise semantics and can be easily translated into other formal notations suitable for formal analysis. We believe that this is probably the most sensible counter-measure that should be further investigated and exploited.

SysML/UML design are currently supported by several commercial MBSE frameworks, but none of them is also able to support formal analysis of the design. Moreover, the translation from the supported custom XMI design representation to other formats is not facilitated and supported (some kind of lock-in effect is occurring here as well). These problems have been overcome within the project by not using any commercial MBSE framework and basing the approach on a simple textual form of representation for UML designs.

The absence of any "best" formal method or technique, and the existence of a variegated set of solutions, each one with its own advantages and weak points, has resulted in a wide fragmentation of the state of art, and corresponding difficulty in adopting a specific solution. The counter-measure adopted within the project, and which we feel confident to recommend, is that one of using multiple formal frameworks achieving some kind of "formal methods and tools diversity". This approach would allow to exploit all the different benefits offered by the various platforms, and to increase the overall level of reliability of the analysis.

It is recognised that one of difficulties in the adoption of formal methods is the high level of expertise needed for their use. This is true, but only in part. We have shown that once a formal method is set in place many useful kinds of formal analysis (e.g., deadlock checking, invariants verifications, reachability aspects) can be performed in a "push button" way without the need of any advanced knowledge of formal techniques. It is however true that in order to efficiently exploit all the power offered by the formal tools and techniques, a far deeper knowledge is needed. This aspect highlights the importance of investments for improving and supporting education and industry/academia collaborations.

The information gathered within the project is based on one of the possible paths that could be followed, given project deadlines and effort. The results obtained by the project can surely be generalised, but longer deadlines and a greater effort would have allowed more complete analysis and solution proposal. From this point of view, the results of the project might be of interest also to funding organisations (as Shift2Rail) to make informed decisions on the support of the industrial leverage of research results.

6.2 WS 2 – CSIRT

6.2.1 Market description

Cybercrime targeting Industrial Control Systems creates significant risk for Intelligent Public Transport such as the many forms of conjoint IT-managed railway operations in Europe. The very high level of integration of European transport systems requires cyber-security coordination between railway operators, and possibly other stakeholders such as railway manufacturers and system integrators. S2R identify the need to develop and support a network of cyber security experts to face that challenge, and the need to develop an organisational model and supporting tools.

Previous work in S2R has provided initial consideration of the necessary expert network.

The CSIRT concept starts in the USA as CERT (Computer Emergency Response Team) at Carnegie Mellon University (CMU) Software Engineering Institute. While the term CERT became used globally, it has been adapted to CSIRT since it is not all about “emergency”, but is historically linked to malware, since whenever a new technology arrives, misuse and intrusion quickly follow.

A CSIRT can be conceived as an organisation or distributed team that provides, to a well-defined community of interest, services and support for both preventing and responding to computer security incidents.

The state of art of CSIRTs in Europe is well documented by Member State collaborations with ENISA which has supported CSIRT developments of various kinds.

The ENISA study of CSIRT maturity, along with other sources, indicates a number of common features to be addressed in defining a European Railway CSIRT Model:

• Constituency to be supported (needs of Rail Stakeholders)
• Clarity of purpose / Mission statement
• Authority – Conjoint Trust Agreement
• Organisational structure and functions (for mission)
• Policy and Procedures (guidance on actions/functions)
• Human resources - expertise and tasks (actions/functions)
• Supporting tools and platforms
• Operational process (people and tools fulfilling policy)

For each of these, several critical aspects are identified, and need to be assessed for a specific purpose, such as an EU Rail CSIRT, requiring e.g., consideration of strategies for gaining trust and acceptance between organisations. However, while ENISA provides guidance on a number of aspects, these are highly geared towards Government CSIRTs, being the primary focus of the NIS Directive, and so there is an opportunity to capitalise on what has been done there, but also an important need to ensure an approach and model that fits the real needs of European Railways.

The layers of the above outline, when defined in a CSIRT model, will define an agreed operational approach, and the necessary functions to be implemented and supported by the platform.

Europe has the highest presence of national, governmental and sectoral CSIRTs, but transport is not yet well represented. The ENISA analysis and mapping of EU CSIRTs shows that of the 380+ operational CSIRTs, none are dedicated to transport.

However, needs related to a transport CSIRT for European Railways are understood by railway stakeholders on the formation of a European railway ISAC started at the 2017, which resulted, after support by DG-CNECT and ENISA, in formation of the European Rail ISAC. While this does not cover all aspects of a CSIRT, it has engaged a number of CISOs who have together determined a basic trust model, along with an initial vision of information sharing. This provides a good springboard from which to launch rapid discussion and agreement of the larger and more complex CSIRT concept, so as to quickly engage and work with European Railway CISOs and their Cyber Security stakeholders.

In regard to CSIRT platforms, an interesting overview of the existing Threat Intelligence Platforms and solutions can be found in following table:

Name	Type	Year	Owner	Project site/s
Collaborative Research Into Threats (CRITs)	Open Source	2014	MITRE	https://crits.github.io/ https://github.com/crits
Collective Intelligence	Open Source	2012	CSIRT Gadgets Foundation	http://csirtgadgets.org/ https://github.com/csirtgadgets
GOSINT	Open Source	2017	Cisco	https://github.com/ciscocsirt/GOSINT https://gosint.readthedocs.io/en/latest/
MANTIS Cyber Threat Intelligence	Open Source	2013	Siemens	https://django-mantis.readthedocs.io/en/latest/ https://github.com/siemens/django-mantis

Name	Type	Year	Owner	Project site/s
Management Framework				
Malware Information Sharing Platform (MISP)	Open Source / Community	2012	Circl	http://www.misp-project.org/ https://github.com/MISP https://www.misp-project.org/communities/
MineMeld	Open Source	2016	Palo Alto	https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld https://github.com/PaloAltoNetworks/minemeld
Yeti	Open Source	2017	Yeti	https://yeti-platform.github.io/ https://github.com/yeti-platform
ThreatStream	Commercial	2013	Anomali	https://www.anomali.com/platform
EclecticIQ	Commercial	2014	EclecticIQ	https://www.eclecticiq.com/platform
LookingGlass	Commercial	2015	LookingGlass	https://www.lookingglasscyber.com/products/manage-intelligence/
Soltra Edge	Commercial	2014	NC4	https://www.soltra.com/en/
Threat Central	Commercial	2015	Micro Focus	https://software.microfocus.com/en-us/software/cyber-threat-analysis
Threat Connect	Commercial	2013	Threat Connect	https://www.threatconnect.com/
ThreatQ Platform	Commercial	2015	ThreatQuotient	https://www.threatq.com/threatq/
TruSTAR	Commercial	2014	TruSTAR Technologies	https://trustar.co/
Open Threat Exchange (OTX)	Commercial	2012	AlienVault	https://www.alienvault.com/open-threat-exchange
ThreatExchange	Commercial	2015	Facebook	https://developers.facebook.com/products/threat-exchange
X-Force Exchange	Commercial	2015	IBM	https://exchange.xforce.ibmcloud.com/

6.2.2 Barriers and counter-measures

The following table analyses the possible barriers and propose the possible counter-measures that could affect the achievement of the 4SECURail-CSIRT objectives:

Type of barrier	Description and counter-measures
Political	4SECURail-CSIRT objectives are fully in line with political targets of EU in the field of railway transport. We are particularly supportive of ENISA/NIS objectives, and the objectives of the European Cooperation Group of CSIRTs, by providing a model and platform to validate how Railways can accelerate their support of European Cyber Safety and Security. Barriers are therefore minimised.
Economical	4SECURail-CSIRT objectives are supporting the strategic position of EU rail industry, according to a strategy that is shared and supported by the major stakeholders, both suppliers and operators. The CSIRT will ensure best protection from criminal and anti-European forces aiming to reduce operational and economic capacity, and so resistance on economic lines is reduced. No barriers are foreseen.

Social	4SECURail-CSIRT objectives will contribute to the improvement of the performance of railway, without negative effects on any social partner. Indeed, social partners dependent on a secure and performing railway will see less disruption through cyber incidents. No barriers are foreseen.
Technical	No critical issues or barriers are expected.
Legislative	4SECURail-CSIRT should analyse and take into account the current legal framework on data sharing (e.g. data shared in the collaborative platform), and address and overcome potential obstacles. Concerning NIS Directive, the Cyber Security Act, and the Cyber Security Agency, we have already held two workshops on these issues to confirm that the CSIRT work will accelerate Railway conformance with the developing legal framework. Barriers are addressed.
Industrial	Confidentiality of certain data can be a potential barrier to its exchange: e.g., data qualified as commercially confidential, or reluctance to share cybersecurity incident related data by end-users due to the potential damage in terms of reputation and credibility. To be considered a trusted platform, 4SECURail-CSIRT must guarantee voluntary and anonymous sharing of threat intelligence information to allow stakeholders to freely share information. CSIRT must anonymously relay information from trusted members. Choice of anonymity must be context-dependent and linked to trust.

7 EXPLOITATION STRATEGY

The 4SECURail exploitation strategy aims to keep the contacts with other relevant projects and studies established during the project duration, to increase awareness of the Consortium's work and research results. A further objective of the strategy is to facilitate collaboration among different groups of stakeholders to enhance uptake of the project's results and integration of different and diverse end-user knowledge. The Consortium will place particular emphasis on facilitating this collaboration. These actions will leverage a multi-channel, cross-country and multi-actor logic – to guarantee the maximum diffusion of the results achieved by the project.

Given the structure of 4SECURail, the dedicated media channels will be supported by a panoply of already-established channels managed by actors being part of the Advisory Board and by European sectoral public/private bodies (including the ones that are part of the S2R JU) having an interest in the promotion on the one hand, of the use of Formal Methods, on the other hand, of the realization of a Computer Security Incidence Response Team both for the railway environment. In particular, the Advisory Board members will be the first recipients of the 4SECURail results: data they shared with us was useful to achieve more detailed results. Advisory Board partners are well known and prestigious organizations, which have a strong willingness to contribute or benefit from 4SECURail results. The consortium will require their contribution to exploitation: they could present the outcomes of the project to their own business clients/partners and local or national stakeholders during commercial meetings and/or showcases organized by their own organization.

After the end of the project each partner will follow their individual Exploitation plan as described in the following section 7.2.

7.1 Joint exploitation

The process used in the Demonstrator to associate the definition of system requirements specifications with a formal analysis is potentially a relevant result from the point of view of software engineering methodology. More detailed feedback on its actual usability in an industrial setting is however needed to better evaluate its possible real fallback in terms of real industrial practice. From this point of view further collaborations with the railway-related partners might allow to better assess the relevance of the approach and its further dissemination.

In the WS-2 CSIRT, the three partners involved (UIC, Hit Rail and TREE) are committed to jointly exploiting further the results of 4SECURail project by:

- Presenting the model and the platform at the next UIC Digital conference to be held online the 3rd December 2021.
- Introducing the paper titled **0497 – A European Railway Computer Security Incident Response Team (ER-CSIRT) model and prototype for the European railway sector** at the World Congress on Railway Research 2022 to be held at the International Convention Centre Birmingham (UK) from 6 to 10 June 2022.
- Creating a Working Group at the ER-ISAC to:
    - present in detail the model and the platform of the WS2 – CSIRT to the ER-ISAC community,

- discuss the possible modifications to the model and platform to be adapted to the current development of the ER-ISAC ecosystem and
- define the road map for the possible implementation of the agreed model and platform.

Moreover, the above-mentioned partners will continue their efforts in exploiting further the methodologies developed in 4SECURail by seeking new EU-funded projects opportunities, possibly also looking at call topics other than the ones published under the Shift2Rail Joint Undertaking (and its successor Europe's rail) Open Calls.

7.2 Individual partners' exploitation plans

All 4SECURail Partners – either profit or non-profit organizations – are committed to make project results sustainable over time and purveyor of impacts for the European railway ecosystem. To this end, 4SECURail Partners are willing to embrace the exploitation strategy previously depicted. Nevertheless, besides the overarching 4SECURail exploitation strategy, the project will support the circulation of findings as well as the provision of added-value services provided independently by individual partners on top of 4SECURail knowledge base.

Partners' individual intentions are detailed below, demonstrating their strong engagement to exploit the project results to support their own business or activities.

7.2.1 Formal Methods

7.2.1.1 Ardanuy

ARDANUY is involved in the project of 4SECURail as lead beneficiary of the Project Management and Coordination. Ardanuy Ingeniería, S.A. is an engineering consulting firm with remarkable experience in project and consortia management both for conventional and R&D projects and is specialized among other in studies, works and technical guidance for railways. On the other side, ARDANUY has a high degree of specialisation in rolling stock, infrastructure projects, superstructure and installations (track, signalling systems, telecommunications, conventional and rigid catenary, system integration and many others).

ARDANUY will promote the usage of Formal Methods in railway environment together with the implementation of the Computer Security Incident Response Team (CSIRT) in the offers about cybersecurity for railways stakeholders.

On the other side, ARDANUY will deploy internal communication tools and an external exploitation infrastructure to present all 4SECURail related deliverables, workshops and activities that can be relevant to the public (without business secrets). As members of the group, ARDANUY will disseminate the results obtained through 4SECURail among its representatives, industry associations and the stakeholders of the European Rail Supply Industry, the published results will be available through: ARDANUY website, ARDANUY LinkedIn account and press articles.

7.2.1.2 CNR

Within CNR, the specific entity participating to the 4ECURail project is the "Formal Methods and Tools" Laboratory of the ISTI Institute. It is a long-term goal of the Laboratory to study formal methods,

experiment their usability with case studies, and advance the state of art with the experimentation of new methods and approaches. The tools UMC used for the system design and analysis with the project is one of the tools developed by the Laboratory in the recent years.

The exploitation of the project results by CNR therefore falls in the case a) of those expected:

> *Each beneficiary must — up to four years after the period set out in Article 3 — take measures aiming to ensure 'exploitation' of its results (either directly or indirectly, in particular through transfer or licensing; see Article 30) by:*
>
> *a) using them in further research activities (outside the action);*

In particular:

The selected case study will be used for further experimentations, comparisons, evaluations and improvement of formal verification techniques.

The modelling and formal analysis experience gained with the use of the UMC framework will be used for improving the framework itself, adding features that resulted to be useful and necessary, and improving its overall usability.

The SysML/UML modelling experience gained during the project will be exploited with the study of a larger and less constrained subset of UML features that still allow a clear and easy mechanical translation into formal notations.

The experience gained with the development of the demonstrator and the observation of the costs and benefits introduced by the use of formal methods in the requirements specification phase will be disseminated in appropriate scientific publications.

7.2.1.3 FIT Consulting

One of FIT Consulting's core activity is to develop financial and economic appraisals of infrastructures and transport/logistics services, also through the deployment of Cost-benefit Analysis methodological elements.

FIT will consolidate the internal knowledge and wide expertise in impact assessment and evaluation of transport business cases. FIT will exploit the increased expertise in leading impact assessment of solutions developed in EU-funded project to the current portfolio of clients with the aim to enlarge it by at least 5 references/year, increasing the company's turnover by 5%.

In particular, the Cost-Benefit analysis performed in 4SECURail appears to be an unexploited domain since – to the Consortium's knowledge – no fully-fledged CBA on the use of Formal Methods in railway industry as ever being developed. This assumption enhances the relevance of 4SECURail reference in FIT's portfolio, and allows adapting CBA techniques commonly used in the appraisals of infrastructure and transport services to a peculiar kind of investment such as the deployment of a structure (both software and staff) prepared for the deployment of FM.

CBA results will be disseminated in selected rail and transport research events (e.g. TRA2022) and among stakeholder platforms which FIT belongs to (e.g. ALICE).

7.2.2 CSIRT

7.2.2.1 HIT Rail

Hit Rail B.V. is a Dutch private limited liability company registered in Utrecht, The Netherlands, owned by 12 European railway companies, and providing secure interconnection of railway information systems and interoperability services for pan-European railway passenger, freight and infrastructure service management used by over 50 companies from 22 countries.

Hit Rail activities are and will be highly relevant to 4SECURail project. Hit Rail maintains a strong community of RU/IM key actors, including Railway Chief Information Security Officers (CISOs) with whom it has developed conferences and workshops on Railway Security, as well as assisting in the creation of the EU Rail ISAC (Information Sharing and Analysis Centre) concerning cyber security.

Dissemination and communications are crucial to maximise the impact of 4SECURail project: the circulation of results of 4SECURail are the main way to develop a strong exploitation plan. In this regard, Hit Rail is fully committed to circulating the results far beyond the border of the consortium, achieving the goal of a European dimension of the impact in the railway sector. For this purpose, it will be fundamental to reach all the relevant stakeholders.

For Hit Rail the exploitation of the results will have a long timeframe, as it will start after the conclusion of the project. Exploitation strategy is twofold:

- On one hand, it will address all relevant stakeholders within Shift2Rail mainly the ones active in IP2;
- On the other hand, it will involve major stakeholders related to the railway community which are not directly engaged in Shift2Rail, such as ENISA; DG MOVE and DG CONNECT, ER-ISAC, UIC, etc.

The main purpose of Hit Rail exploitation strategy related to the 4SECURail project is to ensure that these important actors are aware of the developments that 4SECURail brings to the Shift2Rail activities.

Hit Rail exploitation plan of the project will address the full range of potential users and uses. This includes Associations/Public Bodies (initially: ER-ISAC and UIC), Railway Undertakings, National Agencies, Railway Operators and Infrastructure Managers, actors in the railway supply industry, Regional/National and European Institutions. Hit Rail is aware about the importance to engage with the right stakeholders and at the right time.

4SECURail project was the starting point for the creation of the key stakeholders' community, for assuring the involvement of the key players in the EU Rail cyber security field in guiding the proposed model and collaboration platform, which will be offered for use by the Rail sector. This aim to ensure that the outcome of 4SECURail CSIRT feed forward towards a best common approach for collaborative rail cyber security by the CSIRT collaboration model and platform being collaboratively designed with the key stakeholders, as a resource for uptake.

7.2.2.2 TREE Technology

TREE Technology is an R&D-intensive SME established in Spain and specialised in IT solutions. Our expertise in the fields of Cybersecurity, Artificial Intelligence and Big Data is the cornerstone of a long track record of participation in European projects – with 17 ongoing H2020 projects and more than 30 successfully completed FP7/H2020, Eureka projects. These collaborative and multidisciplinary environments are understood as the root to boost innovation within the company and to both improve already existing products/services and reach new clients and sectors. Therefore, knowledge gained in this framework is considered to be an intangible but valuable asset.

Participation in the 4SECURail project has extended our contact network, especially in the railway sector, where our presence was very limited. This resulted in being invited to join the Safety4Rails proposal, which was awarded under the call H2020-SU-INFRA01-2018-2019-2020 "Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe". The Safety4Rails project (Grant Agreement no. 883532) was launched on 1st October 2020, and TREE Technology focuses on the definition and detection of cyberthreats to be fed to a central MISP platform. This means that we are improving our algorithms and enhancing our tools developed under the umbrella of 4SECURail project to address new use cases that will be trialled in 2022.

Threat detection and threat analysis are also at the core of the TRUST aWARE project (H2020-SU-DS03-2019-2020 "Digital security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises", Grant Agreement no. 101021377) coordinated by TREE Technology. One of the objectives is to also use a MISP platform to manage threats related to privacy, adware and malware in apps and websites. Although the architecture is similar to the one in 4SECURail, the use cases, sector and target audiences (SMEs, micro enterprises and citizens) are completely different, proving that 4SECURail outputs can be adapted and extended to other contexts.

TREE Technology will continue strengthening research on cybersecurity and looking for new opportunities within and outside the railway sector. This includes not only R&D projects but also assessing new potential services that could be offered to our clients.

7.2.2.3 UIC

UIC is a non-profit and neutral association. UIC exploitation potential should therefore be understood as the potential use of the project outcomes by UIC members and, more generally, by the railway community. One fundamental aim of UIC, since its foundation in 1922, is the spreading of industry standards and codes of practice, to which the project is expected to provide fresh inputs.

Within the organisation: 4SECURAIL knowledge has been integrated to the overall activities of the UIC security platform and the UIC Rail system department. The project findings, results and recommendations will be presented in the relevant meetings of those bodies.

Outside the organisation: UIC regularly has informed its members including Railway Undertakings and Infrastructure managers about the 4SECURAIL project, in particular the members of ER-ISAC through its public newsletters and its working structure.

UIC will promote the results of the project in related international events (organised by UIC or where UIC is participating). All the UIC dissemination capabilities will be used, namely the electronic newsletter (UIC

e-News) that globally reaches about 5000 email addresses, the UIC dedicated website, the social media accounts and the UIC network of experts.

8 CONCLUSIONS

This Exploitation Plan provides insight as how the results of the project 4SECURail are to be used, by which partner, under what context and at what moment throughout the duration of the project and from then on. The scope of the exploitation covers not only technological aspects but has considerable part of its scope on aspects of possible future commercialization.

This deliverable describes the project key exploitation objectives, results and methodology and describes the current exploitation landscape surrounding 4SECURail.

It introduces the Market Analysis focused on the sector and on the technologies field analysis exercise, describing also barriers and counter-measures to the exploitation of the project results.

Finally, the document presents next steps started with involving all partners in the joint effort of developing the final exploitation strategy to ensure successful exploitation of the project results and followed by the individual partners' exploitation plans.

9 REFERENCES

Shift2Rail - MAAP – Multi-Annual Action Plan - 14-11-2019