



Transport Research Arena (TRA) Conference
The 4SECURail approach to formalizing standard interfaces
between signalling systems components

D. Belli^a, A. Fantechi^{a,b,*}, S. Gnesi^a, L. Masullo^c,
F. Mazzanti^a, L. Quadrini^c, D. Trentini^c, C. Vaghi^d

^a *ISTI_CNR, Via G. Moruzzi 1, Pisa, 56124, Italy*

^b *University of Florence, Via S. Marta 3, Firenze, 50139, Italy*

^c *MER MEC STE, Via Bombrini 11, Genova, 16149, Italy*

^d *FIT Consulting, Via Sardegna 38, Roma, 00157, Italy*

Abstract

In the context of the Shift2Rail open call S2R-OC-IP2-01-2019, one of the two work streams of the 4SECURail project (GA 881775) pursues the objective to corroborate how a clear, rigorous standard interface specification between signalling sub-systems can be designed by applying an approach based on semi-formal and formal methods. The objective is addressed by developing a demonstrator case study of the application of formal methods to the specification of standard interfaces, aimed at consolidating the most suitable techniques for rigorous standard interface specification, as well as at supporting a Cost-Benefit Analysis to back this strategy with sound economic arguments. This paper discusses the main results of the project.

© 2022 The Authors. Published by ELSEVIER B.V. This is an open access article under the CC BY-NC-ND license (<https://creativecommons.org/licenses/by-nc-nd/4.0>)

Peer-review under responsibility of the scientific committee of the Transport Research Arena (TRA) Conference

Keywords: Signalling systems; Formal Methods; Standard Interfaces; Cost-Benefit Analysis;

1. Introduction

In an increasingly competitive market as the railway one, the application of Formal Methods (FM) within the process of developing standard interfaces between signalling sub-systems is believed to be a winning strategy for the construction of high-quality, safe, and reliable signaling infrastructure, gaining in this way the interest by the infrastructure managers (IMs). Such a trend is fostered by economic and technical reasons. Economic reasons can be found, besides the market competition, in the reduction of both vendor lock-in effect and of costs caused by change requests due to requirements inconsistencies. Technical reasons concern the reduction of interoperability problems,

* Corresponding author. Tel.: +39-0552758639

E-mail address: alessandro.fantechi@unifi.it

and the fact that clear, rigorous specifications of standard interfaces are well suited to exploit formal methods within the development of signalling systems.

In the context of the Shift2Rail open call S2R-OC-IP2-01-2019, one of the two work streams of the 4SECUrail project (GA 881775) pursues the objective to corroborate how a clear, rigorous standard interface specification can be designed by applying an approach based on semi-formal and formal methods.

The work stream was intended at developing a *demonstrator* to study the application of formal methods to an exemplary case study from the railway domain, composed by systems that should interoperate by means of standard interfaces. The demonstrator is aimed at consolidating the most suitable techniques for rigorous standard interface specification, as well as at supporting a Cost-Benefit Analysis to back this strategy with sound economic arguments.

In this paper we show the main results of the cited workstream of the 4SECUrail project, both in terms of recommended techniques for the specification of standard interfaces (Sect. 2) and of a Cost-Benefit Analysis of the adoption of formal methods in the railway industry (Sect.3).

2. The demonstrator case study

The current trend in the direction of clear and rigorous specifications of standard interfaces is to complement the use of natural language requirements with graphical SysML/UML artifacts - see, e.g., EULYNX (2021). However, the unrestricted use of SysML/UML as a specification language for “Systems of Systems” (SoS) can be problematic because of its genericity and the lack of precise semantics. SysML/UML conceals many hidden assumptions that may have a strong impact on the expected behaviors of the modelled system. Formal models that can be rigorously analysed must be mechanically associated to the semiformal SysML/UML-based designs. The goal of our work is to show a possible approach and highlight pros and cons in the application of formal methods in this respect.

The adopted methodology is exemplified in Mazzanti and Belli (2021) with the development of a demonstrator that illustrates the application of formal methods to a selected case study, namely the RBC/RBC communication layer that supports the execution of the RBC/RBC handover protocol, described in Piattino (2020), based on the standard interfaces defined in natural language by the documents UNISIG (2007) and UNISIG (2015).

Figure 1 summarizes the overall structure of the UNISIG standards supporting the handover of a train. The goal is to demonstrate how formal methods provide an even more efficient requirements definition, reducing development problems related to residual uncertainties, and improving interoperability of different implementations.

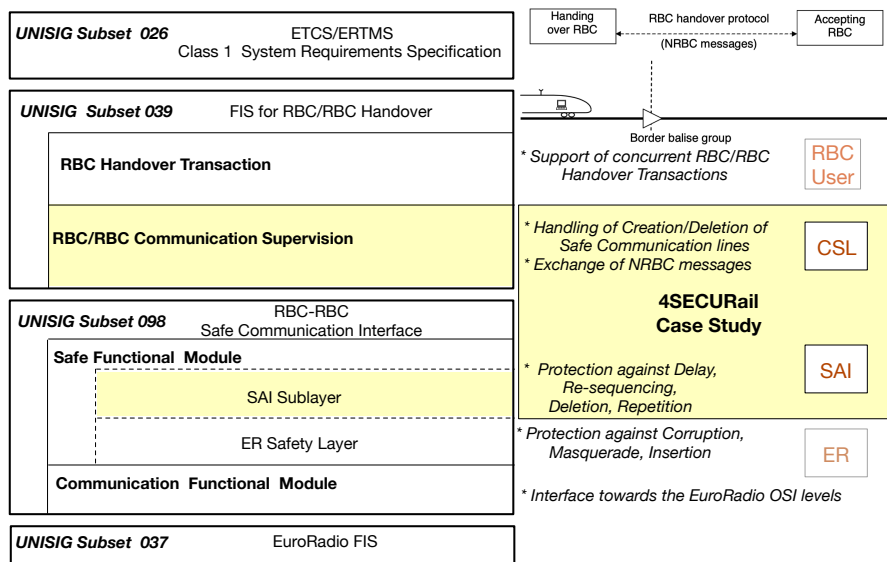


Fig. 1 - Overall structure of the 4SECUrail case study

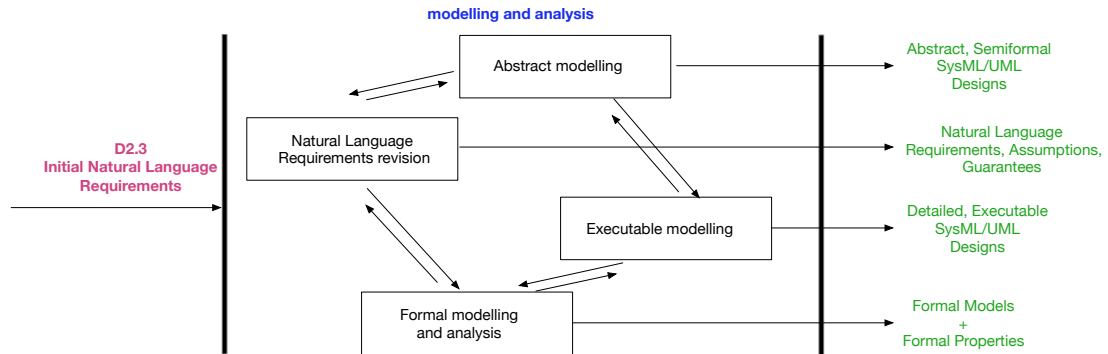


Fig. 2 - The 4SECURail demonstrator generated artefacts

The overall approach followed during the modelling and analysis process is incremental and iterative. About 53 versions of the system have been generated, each one widening the set of requirements of the case study modelled, and each one passing through the steps of semi-formal and formal modelling and analysis. During this iterative process, four kinds of artefacts have been generated and kept aligned:

1. An abstract, semi-formal UML state machine design of the components under analysis.
2. A more detailed executable version of the same UML state machines.
3. A set of formal models derived from the executable UML state machines.
4. A natural language rewriting of the requirements based on the designed and analysed models.

Figure 2 depicts the relationship between these artefacts. The activity of generating and elaborating most of the shown artefacts (currently) requires a human problem understanding and solving activity, apart from the generation of the formal models starting from the UML executable ones, that can be (and has been in part) automated.

The natural language requirements describe the system at a high abstraction level, omitting all the details related to not relevant implementation issues. On the contrary, during the executable modelling, which is the base for formal modelling and analysis, we need to specify these details as well.

Indeed, we found useful to introduce an intermediate "abstract modelling" level, in which the logical structure, the interfaces and the expected main control flow of the system is modelled in a rigorous notation, while the not relevant implementation issues are still described in an abstract way using natural language. These abstract models need to be further refined into executable models before starting the formal modelling activity.

As a first formal modelling step, the executable UML system diagrams corresponding to a given scenario are translated into the notation accepted by the UMC tool¹, chosen as the target of the initial formal encoding because it is a tool natively oriented to fast prototyping of SysML systems. At the beginning of the project, the possibility of designing the SysML system using a commercial MBSE framework – namely SPARX-EA² – has been evaluated. But implementing a translator from the SPARX-generated XMI towards UMC would have been a significant effort and it would have tied the whole analysis approach to a specific commercial tool, a fact which was not considered desirable.

Therefore, our initial SysML models have the structure of simple graphical designs; their role is just to constitute an intermediate, easy-to-understand documentation halfway between the natural language requirements and the formal models. Their translation in the UMC notation constitute a step towards a full formalization: UMC supports a textual notation of UML state-machine diagrams that directly reflects the graphical counterpart, allows fast state-space exploration, state- and event-based (on-the-fly) model checking, and detailed debugging of the system. However,

¹ <https://fmt.isti.cnr.it/umc>

² <https://sparxsystems.com/products/ea/index.html>

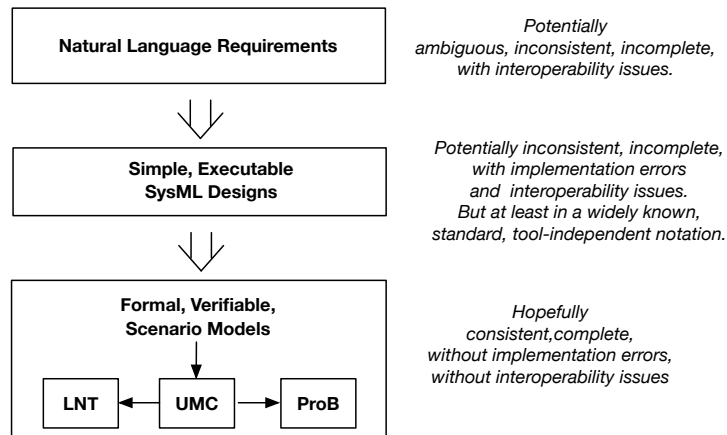


Fig. 3 From natural language to formal models

UMC is essentially a teaching/research-oriented academic tool and lacks the maturity, stability, and support level required by an industry-usable framework.

So, we have planned the exploitation of other, more industry-ready, formal frameworks and further formal models have been automatically generated in the notations accepted by the ProB³ and CADP/LNT⁴ tools (Fig 3). ProB has been selected as the second target of the formal encoding because of its recognized role - see Ferrari et al. (2020) - in the field of formal railway-related modelling. It provides user-friendly interfaces, and allows LTL/CTL model checking, state-space exploration, state-space projections, and trace descriptions in the form of sequence diagrams. CADP/LNT has been selected as the third target of the formal encoding, because of its theoretical roots on Labelled Transition Systems, that allow reasoning in terms of minimizations, bisimulations, and compositional verifications. CADP is a rich toolbox that supports a wide set of temporal logics and a powerful scripting language to support verification.

There are indeed several ways in which SysML/UML designs might be encoded into the ProB and LNT formal notations. In our case, we made the choice to generate both ProB and LNT models automatically from the UMC model. The translation implemented in our demonstrator is still a preliminary version and does not exploit at best all the features potentially offered by the target framework. Nevertheless, the availability of the automatic translation proved to be an essential aspect of the demonstrated approach. Our models and scenarios have been developed incrementally, with a long sequence of refinements and extensions. At every single step, we have been able to quickly perform the lightweight formal verification of interest with almost no effort. This would not have been possible without an automatic generation of the ProB and LNT models. We refer to Mazzanti and Belli (2021, 2022a, 2022b) for a detailed presentation of the generation process and of the generated models.

Summarizing, the demonstrator has provided explicit evidence about the advantages and difficulties associated with the introduction of formal methods in the standardization of specifications of railway systems, in particular in relation with their SoS nature. Furthermore, it has shown how the application of formal methods can provide useful feedback for improving the process of writing specifications, and how formal methods can detect and help to solve ambiguities and uncertainties introduced by natural language and semi-formal descriptions.

³ <https://prob.hhu.de/>

⁴ <https://cadp.inria.fr/>

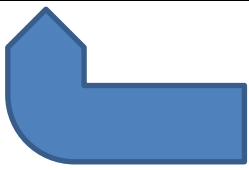
| | Cost/Benefit Item | Meas. unit | Monetary meas unit | |
|--------------------------|--|--|------------------------------------|-----------------------------|
| Investment costs (CAPEX) | RBC (or similar device) Purchase price | | €/software/year | |
| |  | Savings in SW management/assistance | Person-days | €/day |
| | | Lower development time | Person-days | €/day |
| | | Costs for SW verification and validation | Person-days | €/day |
| | Learning / personnel training costs | | Person-days | €/day |
| Operational costs (OPEX) | Time to define requirements for RBC/RBC interface supply through FM | | Person-days | €/day |
| | SW Licences for requirements development through FM | | €/software/year | |
| | Costs for RBC acceptance, verification and validation | | Person-days | €/day |
| | Higher maintenance efficiency | | Replacement costs | €/year |
| | Higher availability in case of service disruption (lower penalties from service contracts) | | # service disruptions/year (prob.) | €/day penalty |
| Benefits for users | Lower service disruptions | | # hours saved by users | €/pax*hour |
| Externalities | Lower accident risks | | Accidents/year | €/accident (external costs) |



Fig. 4 Cost/Benefit matrix

3. Cost-Benefit Analysis

A further objective of the 4SECURail project has been to perform a Cost-Benefit Analysis (CBA) of the adoption of formal methods in the railway industry – see Vaghi (2021b). A fully fledged CBA has indeed never been applied to cases

of formal methods adoption in railway sector: the literature survey in Vaghi (2021a) reports a few examples of quantitative and qualitative assessment of benefits of such adoption.

In 4SECURail the CBA is developed from the “point of view” of the Infrastructure Manager (IM). The methodology follows guidelines set in the EC Guide to Cost-Benefit Analysis reported in Essen H. et al. (2019), and is composed of (i) Financial Analysis, which includes the assessment of additional costs borne and additional savings accrued by an IM faced by the choice to use formal methods, and costs/benefits for suppliers, e.g. savings in terms of shorter time needed for SW development, that are reflected in the price paid by IMs to purchase a RBC (of which the RBC/RBC handover interface is a key component); (ii) Economic Analysis, which considers benefits for users, i.e. passengers of train services, and for the “society” at large.

Relevant categories of costs and benefits for the CBA have been identified (Fig. 4), such as additional costs for learning Formal Methods and for developing, by means of FM, tender specifications for the procurement of a railway signalling component, as well as savings in SW development, verification and validation, benefits for rail users due to higher maintenance efficiency, higher service availability and time saved for lower probability of service disruption.

A micro, bottom-up case study for CBA was set-up, to assess costs and savings borne by an IM faced by the choice to use FM in the development of specifications for the provision of RBC-RBC handover interfaces, vs. the baseline scenario, that is the development with no use of FM. The business case of “semi-formal methods development” (mirroring the parallel business model proposed in the X2RAIL-2 project reported in Aïssat, R. and Borälv, A. (2020)) assumes the adoption of a “tender model”, in which tender requirements are developed – with the use of FM (Fig.5).

The quantitative assessment of cost and benefit categories was possible by integrating the outcome of the demonstrator developed in 4SECURail, and by assumptions based on literature and on Consortium’s knowledge and experience, so overcoming the lack of fully comparable case studies, data confidentiality of SW developers, and low availability of quantitative cost data about FM adoption.

The Financial Analysis performed on the case study demonstrated that, if cost savings enjoyed by suppliers are passed on to prices, the IM faces net cash flow savings over a multi-annual time horizon (assumed 15 years): comparing additional investment and operating costs with savings, the Net Present Value (NPV) of the adoption of FM is 50.917 € and the internal rate of Return (IRR) is 17,9%. Such values demonstrate the financial feasibility of the adoption of FM from the point of view of a single IM.

The convenience for the IM to adopt FM is connected to the economies of scale generated by the replication of savings in SW re-development in reply to change requests, issued by the IM through further tender processes. Since such economies of scale are likely verifiable but not easily quantifiable, the analysis has followed up with the identification – by means of sensitivity analysis - of the optimal scale for which the additional resources deployed by the IM generate enough savings in SW development to balance the additional investment and operational effort needed. In other words, the sensitivity analysis aimed at detecting what is the business scale for which the higher effort borne by IM is balanced by savings in the development of the interface, and how much suppliers should save in the development of interfaces in reply to change request, to ensure a competitive purchase price.

As evidenced in Figure 6, according to 4SECURail assumptions, the break-even between additional costs borne by IM and savings is verified if the purchase price of SW upon change requests is -40% vs. the baseline.

The Economic Analysis assessed the benefits due to higher maintenance efficiency, higher service availability and time saved for lower probability of service disruption. It was based on the quantification of service disruptions that may happen on a rail line due to failure of RBC/RBC handover interface, and in particular those due to ambiguity of specifications. They are very rare according to 4SECURail Consortium’s knowledge (0.1% of total cases).

Assuming penalties for service disruptions as prescribed by Performance Regime set in the RFI (Italian IM) Network Statement: RFI (2021), the related amount saved by the IM is taken into account as net benefit in the CBA. Moreover, avoided service disruptions mean avoided delays for passengers, which can be monetized applying the appropriate Value of Time (VoT), defined in Essen H. et al. 2019), see Fig. 7.

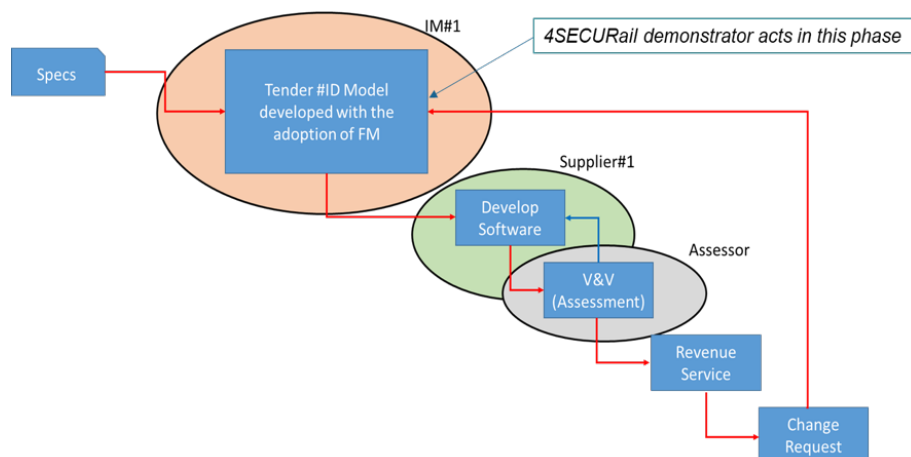


Fig. 5 Product life-cycle

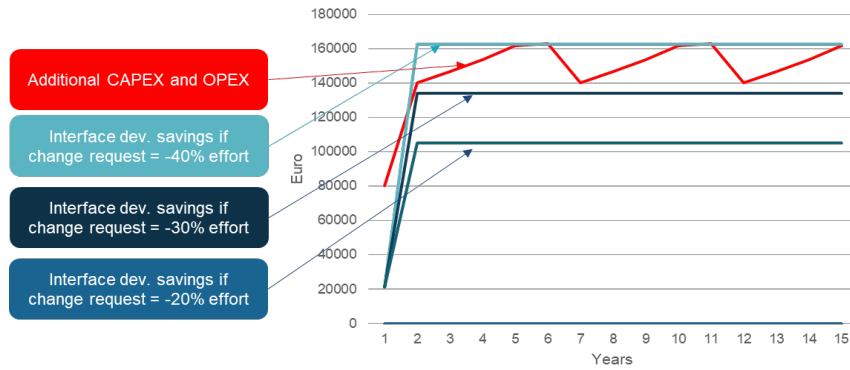


Fig. 6 Break-even computation

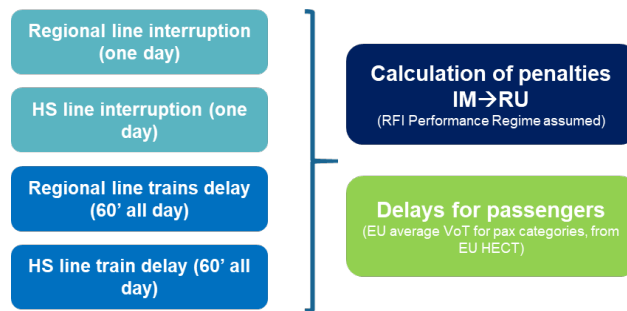


Fig. 7 Assumptions for the calculation of benefit for users

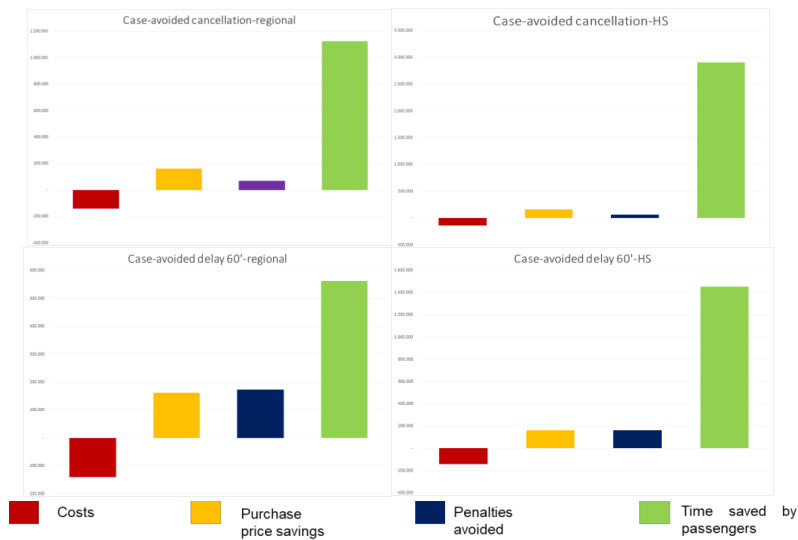


Fig. 8 – Value of benefit categories per scenario (Euro/year)

Some scenarios have been considered on two Italian lines (a high-speed line and a highly congested node) to assess benefits for users in case cancellations or delays are avoided due to higher maintenance efficiency generated by FM. The Economic analysis has demonstrated the net convenience of the FM adoption for the society as a whole (IM, users

and all other involved stakeholders), since the net positive cash flow of benefits vs. costs during the 15-year period is about 9 M€. Indicators of the Economic analysis are highly positive: NPV is 7.067 M€ and the Benefit/Cost Ratio is 5,05, i.e., the process generates (actualized) benefits 5 times higher than cost borne by the IM. Such benefits are likely higher if FM are applied on a EU-27 scale. The net benefits for users and society may justify public granting of the adoption of FM in the railway safety domain.

Not surprisingly, in line with a major part of CBAs developed for rail infrastructure projects, benefits from time saved for passengers are by far the most relevant benefit category (Figure 8). Indeed, expected benefits for users, although calculated using many (realistic) assumptions, justify the adoption of FM and the necessary investment.

4. Conclusions and future works

The goal of the 4SECURail demonstrator has been the study of a possible way in which formal methods can be exploited to improve the quality of System Requirement Specifications of signalling systems, and to use this study as an information source to base a Cost-Benefit Analysis. We have shown how the creation of an easy to understand and communicate executable model is an intermediate step that already allows to detect possible weaknesses in the natural language requirements, but that formal modelling and analysis are needed to detect and remove less trivial errors.

The Cost-Benefit Analysis carried on the developed Formal Methods demonstrator suggest that efforts and costs for formal analysis of system requirements are likely to be distributed among the various entities supporting the standard itself, and not to a single IM. Benefits are spread over the entire supply chain, including suppliers, if economies of scale are activated among IMs and suppliers in SW development. The “multi-supplier” mode enabled by FM is likely to generate time and cost savings for rail safety industry.

Acknowledgements

This work has been partially funded by the 4SECURail project. The 4SECURail project received funding from the Shift2Rail Joint Undertaking under the European Union’s Horizon 2020 research and innovation programme under grant agreement No 881775 in the context of the open call S2R-OC-IP2-01-2019, part of the “Annual Work Plan and Budget 2019”, of the programme H2020-S2RJU-2019. The content of this paper reflects only the authors’ view and the Shift2Rail Joint Undertaking is not responsible for any use that may be made of the included information.

References

- Aïssat, R., Borály, A., 2020. X2RAIL-2, Deliverable 5.3 – Business Case.
- Essen, H., Fiorello, D., El Beyrouty, K., et al., 2019. European Commission, Directorate-General for Mobility and Transport, Handbook on the external costs of transport: version 2019 – 1.1, Publications Office, <https://data.europa.eu/doi/10.2832/51388>
- EULYNX, 2021. Project site. <https://eulynx.eu/>
- Ferrari, A., Mazzanti, F., Basile, D., ter Beek, M.H., Fantechi, A., 2020. Comparing Formal Tools for System Design: a Judgment Study. 42nd ACM/IEEE International Conference on Software Engineering (ICSE’20), ACM, pp. 62–74, doi:10.1145/3377811.3380373.
- Mazzanti, F., Belli, D., 2021. 4SECURail deliverable D2.5 "Formal development demonstrator prototype, final release". July 2021. <https://www.4securail.eu/Documents.html>
- Mazzanti, F., Belli, D., 2022a. Formal Modeling and Initial Analysis of the 4SECURail Case Study. 5th Workshop on Models for Formal Analysis of Real Systems (MARS 2022). Electronic Proceedings in Theoretical Computer Science vol. 355, April 2022, doi 10.4204/EPTCS.355.
- Mazzanti, F., Belli, D., 2022b. The 4SECURail Formal Methods Demonstrator. 4th International Conference on Reliability, Safety and Security of Railway Systems - RSSRAIL 2022, Paris June 2022. Lecture Notes in Computer Science 13294
- Piattino, A., 2020. 4SECURail deliverable D2.3 "Case study requirements and specification". <https://www.4securail.eu/Documents.html>
- RFI - Rete Ferroviaria Italiana, 2021. Prospetto Informativo della Rete 2023, updated December 2021.
- UNISIG, 2007 - “RBC/RBC Safe Communication Interface” - SUBSET-098 - 21-05-2007
- UNISIG, 2015. - “FIS for the RBC/RBC Handover” - SUBSET-039 - 17-12-2015 (Issue 3.2.0)
- Vaghi, C., 2021a. 4SECURail Deliverable D2.4: "Specification of Cost-Benefit Analysis and learning curves, Intermediate release". March 2021. <https://www.4securail.eu/Documents.html>
- Vaghi, C., 2021b. 4SECURail Deliverable D2.6: "Specification of Cost-Benefit Analysis and learning curves, Final release". November 2021. To appear in <https://www.4securail.eu/Documents.html>