ISSN 1866-721X

DLR-TS 1.37

2nd SmartRaCon Scientific Seminar - Proceedings

2nd SmartRaCon Scientific Seminar

Proceedings

Berichte aus dem DLR-Institut
für Verkehrssystemtechnik

Band 37

DLR Deutsches Zentrum
für Luft- und Raumfahrt

Reports of the DLR-Institute of Transportation Systems

Volume 37

Proceedings of the
2nd SmartRaCon Scientific Seminar

November 24. 2020
San Sebastian, Guipúzcoa, Spain

Publisher:
Deutsches Zentrum für Luft- und Raumfahrt e.V.
Institut für Verkehrssystemtechnik
Lilienthalplatz 7, 38108 Braunschweig

ISSN 1866-721X

DLR-TS 1.37

Braunschweig, November 2020

Institute Director:
Prof. Dr.-Ing. Katharina Seifert

Preface

Dear reader,

you are holding the newest volume of the series „Reports of the DLR-Institute of Transportation Systems" in your hands. In this series we publish fascinating scientific research results from our Institute of Transportation Systems at the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt e.V. - DLR) and its collaborating partners.

With this series we communicate results of our scientific work in the fields of automotive, railway systems and traffic management. We hope to enable a broad access to scientific work and results for the national and international scientific community and practitioners in the field of transportation. Beyond that, researchers in the early phase of their academic career of our staff and external doctoral candidates are offered the opportunity to publish their dissertation. In addition, the publication includes outstanding scientific contributions and project reports as well as proceedings of conferences in our house with different contributors from science, economy and politics.

The current volume contains the proceedings of the second SmartRaCon Scientific Seminar, which has been held on November 24th, 2020 virtually from San Sebastian, Spain. This SmartRaCon Scientific Seminar aimed to bring together researchers from different railway research areas with focus on fail-safe train positioning (including satellite technology), on-board train integrity, formal methods and standardization for smart signaling systems interfaces, and traffic management evolution. The seminar was a vivid and fruitful forum for the presentation and discussion of new and on-going research.

We wish you an interesting and inspiring reading!

Prof. Dr.-Ing. Katharina Seifert

All contributions have been double refereed as abstract and full paper by the International Scientific Committee

International Scientific Committee

Michael Hutchinson (GMV NSL, Nottingham, United Kingdom)
Dr. Marion Berbineau (Univ. Gustave Eiffel, Villeneuve d'Ascq, France)
Dr. Mohammed Ghazel (Univ. Gustave Eiffel, Villeneuve d'Ascq, France)
Dr. Emilie Masson (RAILENIUM, Lille, France)
Insaf Sassi (RAILENIUM, Lille, France)
Dr. Michael Meyer zu Hörste (DLR, Braunschweig, Germany)
Dr. Daniel Schwencke (DLR, Braunschweig, Germany)
Dr. Florian Brinkmann (DLR, Braunschweig, Germany)
Stefanie Schöne (DLR, Braunschweig, Germany)
Dr. Jaizki Mendizabal (CEIT, San Sebastian, Spain)
Dr. Jon Goya (CEIT, San Sebastian, Spain)
Dr. Iñigo Adin (CEIT, San Sebastian, Spain)
Dr. Gorka de Miguel (CEIT, San Sebastian, Spain)
Paul Zabalegui (CEIT, San Sebastian, Spain)

Host

The 2nd SmartRaCon Scientific Seminar has been hosted by CEIT

ceit MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

http://www.ceit.es/

SmartRaCon Steering Committee

Dr. Marion Berbineau (Université Gustave Eiffel, Villeneuve d'Ascq, France)
Michael Hutchinson (GMV NSL, Nottingham, United Kingdom)
Dr. Jaizki Mendizabal (CEIT, San Sebastian, Spain)
Dr. Emilie Masson (RAILENIUM, Lille, France)
Dr. Michael Meyer zu Hörste (DLR, Braunschweig, Germany)

Organising Committee

Dr. Jaizki Mendizabal (CEIT, San Sebastian, Spain)
Dr. Jon Goya (CEIT, San Sebastian, Spain)
Dr. Gorka de Miguel (CEIT, San Sebastian, Spain)
Iñaki Lopetegui (CEIT, San Sebastian, Spain)
Dr. Michael Meyer zu Hörste (DLR, Braunschweig, Germany)
Dr. Marion Berbineau (Univ. Gustave Eiffel, Villeneuve d'Ascq, France)
Michael Hutchinson (GMV NSL, Nottingham, United Kingdom)
Dr. Emilie Masson (RAILENIUM, Lille, France)

Table of Contents

1 Introduction by SmartRaCon

Marion Berbineau; Université Gustave Eiffel, Villeneuve d'Ascq, France
Michael Hutchinson; GMV NSL, Nottingham, United Kingdom
Emilie Masson; IRT RAILENIUM, Famars, France
Jaizki Mendizabal; CEIT, San Sebastián, Guipúzcoa, Spain
Michael Meyer zu Hörste; German Aerospace Center (DLR), Institute of Transportation Systems, Braunschweig, Germany

1.1 Smart Rail Control Systems - SmartRaCon

Digitalization and Automation will prepare the ground for a completely new generation of train control and railway management systems. SmartRaCon aims to design and develop a technology -independent system for an adaptable train-to-ground communication system resilient to radio technology evolution considering threats such as interferences or cyber-attacks. Some of the concepts to be explored are:

- Communication concepts
  - the anticipation of the 5G standardization;
  - Software Defined Networks (SDN) and Network Function Virtualization (NFV);
  - radio system KPI evaluation;
  - hardware development using Software Defined Radio (SDR) platforms,
  - IP-based communication gateway with bandwidth aggregation, dynamic spectrum allocation and mobility support;
  - traffic pattern recognition tool to ensure minimum conditions;
- Localization and train integrity concepts
  - innovative use of satellite localization technologies.
  - sensor data fusion
  - digital maps

The overall concept is based on the idea to reuse COTS and to integrate them into a railway network in a modular way, which allows on the one hand a flexible scaling of the rail control system in a cost-efficient way and on the other hand a building block approach for certification and modulewise change of technology.

1.2 The methodology

Smart Railway Control (SmartRaCon) will be the core to enable high capacity and cost efficient rail systems for the next century. The proposed approach of SmartRaCon is to control smartly intelligent, autonomous trains on a scalable and more flexible infrastructure. Main challenges for the rail system are the enhancement of capacity, the reduction of investment and operations cost. The reductions of energy consumption as well as the reduction of cost for test and certification are two aspects for the cost reduction. These are the conceptual objectives of SmartRaCon [1] and are coherent with the Master Plan topics of Shift2Rail [2]. The SmartRaCon

idea for a credible, coherent and long-term approach to achieve the Master Plan Objectives is to meet those challenges by:

- intelligent trains, which communicate safely & securely, localize & supervise integrity autonomously and operate as virtual coupled train-sets
- infrastructure which is flexible, easy & fast to configure, less fixed (e.g. wired) & scalable, communicating safely & securely with trains and operating them in moving block
- traffic management system operating both with optimization algorithms
- supported by cost-efficient process for design, test and certification which uses highly automated test labs to avoid on-site tests based on formal test specifications

For the capacity increase, an integrated moving block (MB) system has to be implemented. Hence technologies work together: train positions need to be reported safely & securely in real-time to the trackside train control and traffic management system (TMS). Positioning and communication are ensured by combining different technologies. To implement the MB logic on-board train integrity (TI) supervision is required, applying similar technologies. An evolution of the TMS is needed to adopt the MB logic besides increasing the efficiency of dispatching. Virtual coupled train-sets can help to improve capacity by reducing the number of train routes required. The approach is fully in line with the standardized European Rail Traffic Management System (ERTMS) and the European Train Control System (ETCS) and enhances interoperability. New functionalities & technological solutions require being formally specified and tested. Hence testing needs to be automated & moved from on-site to lab. This achieves the objectives of reliability, improved standardization, lower costs & simplified processes. This prioritization is justified since traffic management, positioning and communication are enabling technologies that need to be tested and certified. The complementary work in areas as e.g. moving block and decentralized interlocking technologies extends the concept to reach a significant and sustainable effect on capacity & cost.

Figure 1-1: SmartRaCon Logo

1.3 Technological research areas

The overall concept is based on technology-independent adaptable train-to-ground communications resilient to radio technology evolution, ensuring safety levels of GNSS based on-board positioning and train integrity supervision. Some of the most relevant areas of technological research are shown in Fig. 2 and the conceptual groups “communication”, “localization” and “train integrity” are discussed below.

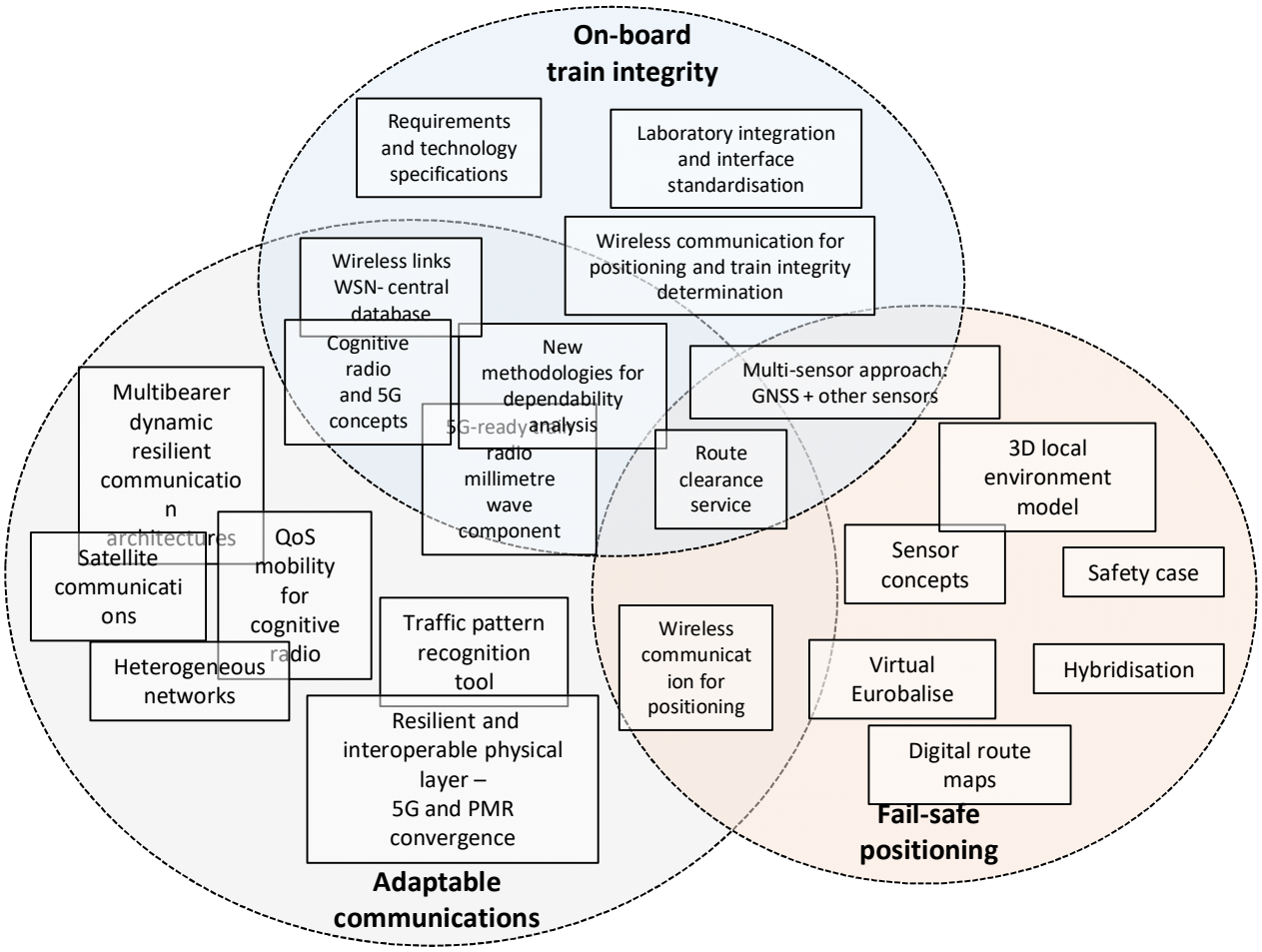


Figure 1-2: Core Areas of Research in SmartRaCon

1.3.1 Conceptual group "Communication"

The contribution from communication is based on the idea to reuse COTS and to integrate them into a railway network. For that, SmartRaCon will design and develop a technology-independent system for an adaptable train-to-ground communications system resilient to radio technology evolution considering threats such as interferences or cyber-attacks. Some of the concepts to be explored are a) the anticipation of the 5G standardization; b) Software Defined Networks (SDN) and Network Function Virtualization (NFV); c) radio system KPI evaluation; d) hardware development using Software Defined Radio (SDR) platforms, e) IP-based communication gateway with bandwidth aggregation, dynamic spectrum allocation and mobility support; f) traffic pattern recognition tool to ensure minimum conditions; g) innovative use of satellite communications technologies.

The impact for future communication infrastructure relying on standardized technologies and COTS products is high for the European railway, telecom and space industry as well. The use of satellite communications is especially relevant for railway lines, where the availability of a reliable communication infrastructure is critical. By using cognitive radio systems maximum use of surrounding infrastructures will be achieved. Through the use of cognitive radio, 5G, satellite and adaptable, resilient architecture CAPEX will be reduced and moreover IP communication technology supporting a fast radio technology evolution will reduce OPEX.

Current radio technology, i.e. GSM-R, will become obsolete by 2030 and therefore 4G is being analyzed. 5G is already planned to be commercialized by 2020, which will limit the life-cycle of a 4G-only solution. The main advance relies in the ability to successfully integrate a number of heterogeneous technologies and communication protocols into one network in order to take advantage of various deployments (3G, 4G, 5G, Satellites) provided by external network operators (Network as a service) and/or dedicated infrastructures (Network as an asset). Thus, CAPEX and OPEX of communication systems can be minimized. Smooth migration will be enabled by designing middleware platforms for transparent switching radio components.

Impacts on the infrastructure, line capacity and definition of certification processes will be made thanks to the future communications and on-board positioning.

1.3.2 Conceptual Group “Localization”

The overall concept for localization is based on the need to ensure that the safety levels provided by existing signaling systems are not compromised when a train-borne positioning system is employed. SmartRaCon will set up and undertake test campaigns, analyze the data from such campaigns, improve specifications, provide inputs to the development of a safety case, as well as making other more specific contributions building on the positioning technology expertise within the consortium such as simulation based KPI evaluation, multi-constellation, sensor integration, etc.

In terms of impacts of localization future business will be generated. A core of safety expertise concerning the use of train-borne positioning technology for railway applications will be established. A Route Clearance service will be used to safely introduce the technology to specific new lines and applications. SmartRaCon will bring an important support to the involved supply chain by developing and certifying dedicated hardware, algorithms and the infrastructure required to deliver the services. The impact will be the contribution to the optimization of global railway operation by providing very efficiently all the needed information to facilitate decision-making process at different stakeholders levels (engineering, exploitation, maintenance, customer services, etc.). Such systems will achieve decentralized control of remote track-side objects without cable connections.

Testing processes and the route to acceptance of GNSS and associated technology will be enhanced such that standardized methods are set in terms of the equipment used, measurements made, analysis tools and results delivery (Route Clearance service, simulation tools for railway KPIs evaluation, Digital Route Maps (DRM)). A consolidated set of specifications and a methodology for testing COTS equipment capabilities will be defined. The need for lab simulations will be identified and a 3D Local Environment Model will be developed. Performance optimization will be proposed through hybridization of GNSS with inertial sensors, odometry, dead reckoning, DRM and Wireless Communications Technologies. Further specific proposed tasks are related to the Safety assessment.

1.3.3 Conceptual Group “Train Integrity”

The key issue for the overall concept of on-board train integrity determination is that this function becomes mandatory for the implementation of more efficient signalling systems based

on concepts like moving block. Systems based on these concepts will deliver very significant advantages in terms of capacity (shorter headways will be allowed), capital and maintenance cost (expensive track infrastructure for block detection will be obsolete), resiliency, and others such as compatibility among lines, etc.

1.3.4 Further conceptual Groups

The three above mentioned conceptual groups are related to many others in the context of future systems. Some examples are given below and visualization is given in Fig. 3:

- Moving block operation requires safe localization and train integrity as well as reliable as well as adaptable communication.
- Automatic train operation requires a high performance adaptable communication as well as safe and precise localization.
- Future traffic management systems, which can optimize capacity, punctuality or energy-consumption require real-time precise localization.
- Virtual coupled train sets are based on very precise and highly safe absolute and relative localization as well as adaptable train-to-train and train-to-trackside communication.
- Smart radio-connected wayside elements require a highly safe and secure communication
- Freight telematics needs an adaptable communication and localization.

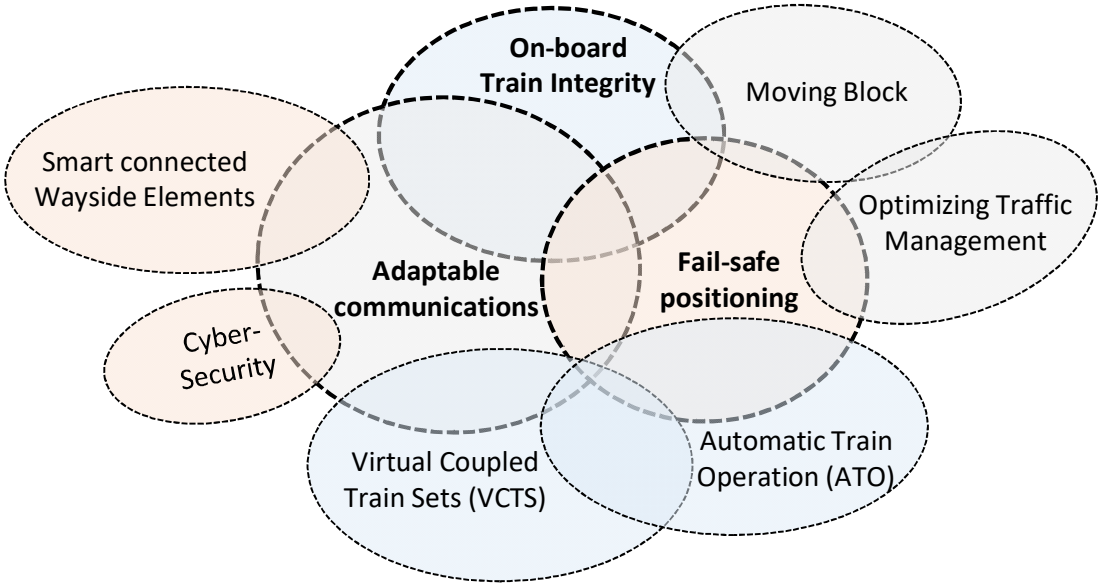


Figure 1-3: Core and further Areas of Research in SmartRaCon

1.4 Conclusions

The SmartRaCon Partner are performing research work on innovative technologies for Digitalization and Automation to prepare the ground for new generations of train control and railway management systems. The core elements are technologies for adaptable communication, safe positioning and train integrity supervision. In parallel to the technological

research, SmartRaCon Partner are developing and operating simulators and research infrastructures for the validation of the technologies.

To disseminate the results of the scientific work, SmartRaCon organizes the yearly Scientific Seminars to present and discuss their results on a high scientific level. The first SmartRaCon Scientific Seminar took place on the 25th of June 2019 in Villeneuve d'Ascq in France [3]. The second seminar is now this one on the 24th of November 2020 in San Sebastian, Spain. Due to the situation in Europe, it is done in a complete digital format. The next one is expected to take place in Braunchweig, Germany in 2022.

1.5 References

[1] SmartRaCon: Technical Concept. May 2015.
[2] Shift2Rail Master Plan. Shift2Rail Joint undertaking 1st issue 2015. www.shift2rail.org.
[3] SmartRaCon: Proceedings of the 1st SmartRaCon Scientific Seminar. 25. June 2019, Lille. Reports from the DLR-Institute of Transportation Systems Volume 35, ISSN 1866-721X

1.6 Authors

Dr. **Marion Berbineau** received the Engineer degree from Polytech'Lille (France) and the Ph.D. degree from the University of Lille, both in electrical engineering, respectively in 1986 and 1989. She is a full time Research Director at Université Gustave Eiffel in the Component and SYStem department and in charge of coordination of Railway R&I activities of the University. She is associated researcher at LEOST laboratory. She is expert in the fields of radio wave propagation in transport environments (particularly in railway tunnels and high speed lines), electromagnetic modeling, channel characterization and modeling, MIMO, wireless systems for telecommunications, cognitive radio for railways and GNSS localization-based system for ITS particularly for the rail and public transport domains. She is responsible for Railway research coordination for the Institute. She is active as an expert for the GSM-R and future systems like LTE-A or 5G NR and beyond 5G. She is involved in several National and European research projects. She is author and co-author of several publications and patents. She is expert at the French national council for the railway system. She is on the reserve list of the Scientific Council of Shift2Rail.

marion.berbineau@univ-eiffel.fr

Michael Hutchinson has over 14 years of experience in the GNSS industry. Michael has developed solutions for and provided consultancy on a wide range of GNSS applications involving robust and reliable positioning and navigation. This includes aviation approach operations, liability critical automotive programmes, future train control systems and Unmanned Aerial Vehicles (UAVs). Michael also provides consultancy on GNSS system level topics. Michael currently

works as Business Manager and Principal Navigation Engineer at GMV NSL, coordinating business development activities and leading the company's work in the railway domain.

michael.hutchinson@gmvnsl.com

Dr. **Émilie Masson** is a Project coordinator at Railenium, France. She received the Engineer degree from the Institut Supérieur de l'Électronique et du Numérique, Lille, in 2005 and the PhD degree in electronics from the University of Poitiers, in 2010. She is in charge of the telecommunication activities at Railenium and her professional research activity lies in the field of modelling and simulation of the propagation of radio waves, radio measurement campaigns and channel sounding, wireless transmission systems and Cognitive Radio.

emilie.masson@railenium.eu

Dr. **Jaizki Mendizabal** received his M.Sc. and Ph.D. degrees in Electrical Engineering from TECNUN (University of Navarra, San Sebastián, Spain) in 2000 and 2006 respectively. He joined Fraunhofer Institut (Nuremberg, Germany) and SANYO Electric Ltd, Japan as RF-IC designer. Nowadays, he is at CEIT, in San Sebastián (Spain) where his research interests include communications and electronic systems. He is lecturing "Communications Electronics" and "Communications via Radio" at TECNUN (University of Navarra).

jmendizabal@ceit.es

Dr.-Ing. **Michael Meyer zu Hörste** holds a PHD in mechanical engineering from the technical University of Braunschweig. He has joined DLR Institute of Transportation Systems in 2001 bringing already 6 years of railway research experience with him. He is expert in railway operations, command, control and signalling systems, especially ERTMS/ETCS as well as train localisation. Currently he is working the business development of the DLR Institute of Transportation Systems He was a major contributor in building the DLRs ETCS test laboratory RailSiTe®. He is chairman of the ERTMS Reference Labs Association since 2012. He is fellow of the Institution of Railway Signalling Engineers (FIRSE) since 2012. He is member of the Shift2Rail governing board and coordinator in the DLR for Shift2Rail.

Michael.MeyerzuHoerste@dlr.de

2 GNSS Radio Frequency Interference in the Railway Environment

Michael Hutchinson, David Payne, Terri Richardson
GMV NSL, Nottingham, NG7 2TU, United Kingdom

2.1 Introduction

The power levels of GNSS signals are very weak and so they are vulnerable to interference. This is a phenomenon where other unwanted signals disrupt the GNSS signals potentially leading to reduced accuracy or even an inability of the user receiver to compute a PVT solution. Signals overlapping GNSS frequencies are likely to come from sources closer than the satellites and then, can easily overpower GNSS signals and render them unusable. In order to protect GNSS signals, regulations forbid the intentional broadcast of any non-GNSS signals near GPS L1 and Galileo E1 while lesser restrictions apply to GPS L2, GPS L5 and Galileo E5A frequencies. Despite those regulations, RFI affecting GNSS at L1/E1 is occasionally observed. As explained in [1] the GPS signal level lies approximately 15dB under the background noise floor. Spread spectrum processing raises this by about 60dB therefore if an interfering signal at the GNSS receiver location has power 45dB above the noise floor then the GNSS receiver will be completely jammed.

Characterisation of an RF interference (RFI) source is important in determining the impact that it will have on GNSS receivers and the likely source. It also makes it possible to identify multiple detections of the same RFI source. Full characterisation requires Intermediate Frequency (IF) data samples to work with. Using post correlation methods, e.g. SNR analysis, supports a coarser understanding of interference events. GNSS RFI sources may be unintentional or intentional.

2.2 Unintentional Interference

An unintentional interference source is likely to be at a constant frequency or single tone, over time. Unintentional man-made RF interference can be caused by a number of sources, including television signals and mobile communication devices.

[1] provides the following useful summary of the different types of source of unintentional interference:

- Pulsed interference from radar signals in frequency bands near to those used for GNSS, that are inadequately filtered;
- Accidental transmission in the wrong frequency band;
- Out-of-band interference caused by nearby transmitters;
- Harmonics and intermodulation products of various ground and airborne transmitters.

Television broadcasts have the potential to interfere with GNSS through the harmonics of the primary frequency in the event of a system malfunction or changes to the broadcast that

increase the power of the 2nd or 3rd harmonics. Similarly, there is the potential for TV antennas with internal pre-amplifiers to cause interference if the unit malfunctions. In Turin, Italy it has been documented that out-of-band interference from TV broadcasts has interfered with GNSS frequencies.

Unintentional sources of RFI that are specific to the railway environment are not yet well understood. One type of unintentional interference source that has been noted is where the magnetic characteristics associated with a train travelling along tracks with AC catenary disrupt the field patterns of a receiving antenna. It was observed in the UK that a train powered from 25kVAC overhead catenary could disrupt the reception pattern of an antenna operating in the 300kHz frequency band (used for UK DGPS service). Electric supply systems to the train e.g. DC-DC converters may represent a further cause of RFI.

2.3 Intentional Interference

In recent years, man-made intentional interference events have emerged as a credible threat. Many events have been experienced, detected and reported. A widely reported case of RF interference caused significant disruption to a GNSS landing system at Newark Airport. After lengthy and costly investigation by multiple US government agencies, the source was found to be a low-cost (≈$30) jammer in a truck on the nearby highway. This device was being used by the truck driver to prevent his employer tracking his location, a so-called Privacy Protection Device (PPD). Dedicated data collection campaigns triggered by this case detected a large number of separate interference events per day.

In another case, numerous jammers were being used by a logistics company in Sydney to jam a GNSS-based tracking and dispatch system. However, the use of such jammers has impacted the availability of the GBAS (Ground based Augmentation System) at Sydney Airport.

Intentional jammers tend to vary their frequency, sweeping back and forth across the GPS L1 central frequency creating a so-called "chirp" signal. This is because it is relatively straightforward for a receiver to mitigate the effects of single tone interference by "nulling" it out - adjusting the antenna gain so that measurements at a specific frequency have little impact on the overall solution. This creates the principle of a notch filter. Conventional notch filters are not so effective against a swept signal (frequency varying rapidly over time). To date, no explanations have been found which would account for an unintentional interference source emitting a chirp signal at L1, so all chirp signals may be identified as having a high probability of being generated by deliberate jammers. Some interference signals which are not chirp may also be deliberate jammers, but as there is no evidence for this, to date all non-chirp signals are assumed to come from unintentional interference sources.

2.4 NSL Detector

The NSL GSS200D DETECTOR system detects, characterizes and classifies RFI sources which disrupt GNSS services. Two different versions exist:

- GSS200D GPS GLONASS GALILEO L1

- GSS200D GPS GALILEO L1/E1 + L5/E5a

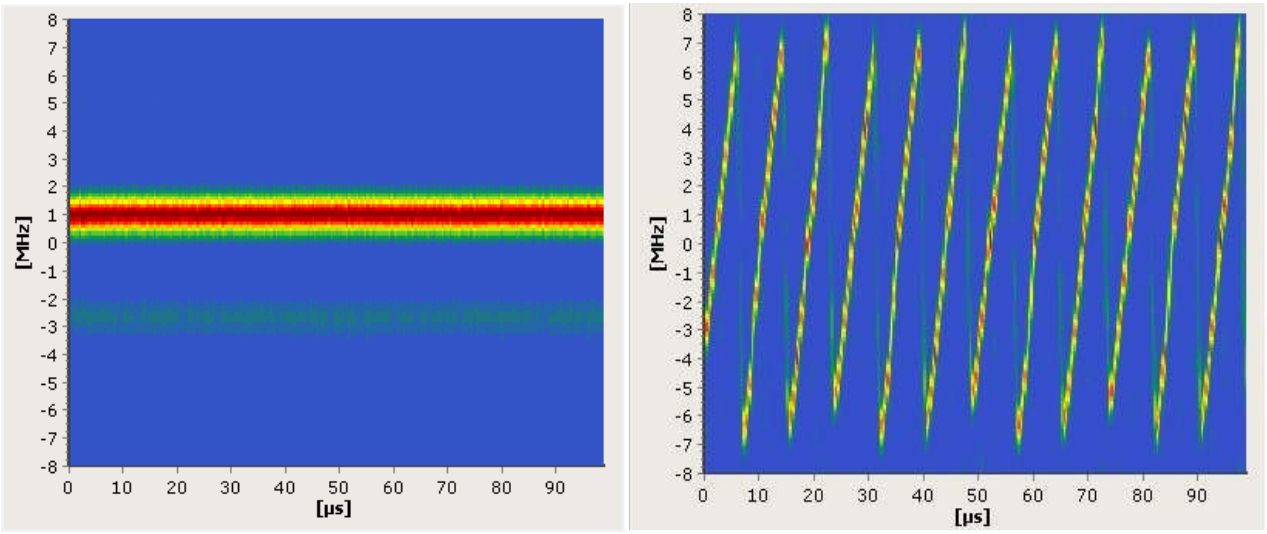


Figure 2-1: Single Tone (left) and chirp signal (right)

The Probes operate autonomously, continuously monitoring the RF spectrum around the GPS L1/Galileo E1 spectrum band (1575.42MHz±10MHz) and GPS L5/Galileo E5a spectrum band (1176.45MHz±10MHz). If RFI is detected the Probes will store a sample of raw RF data, perform some preliminary analysis, decide the following actions, and then communicate this automatically to a central DETECTOR Server & Database. Further automated processing at the Server determines the type of interference, and the results are then sorted and stored in the Database. It makes it possible to determine the likely impact of an interference event; to differentiate unintentional interference from jamming; to distinguish different jammers; to identify multiple detections of the same jammer; to identify trends in the interference threat; and to support the development of effective countermeasures.

2.5 Detector deployment in the railway environment

Within the X2RAIL-2 project, the GSS200D (GPS GALILEO L1/E1 + L5/E5a versión) was deployed onboard trains operating on railway lines in the Czech Republic (Brno – Tisnov line), Germany (Thales LUCY test runs), and Italy (Cagliari – San Gavino line) in order to investigate the RFI environment in the railways.

2.5.1 Brno – Tisnov Line, Czech Republic

This train travelled from Brno to Tisnov in Czech Republic between 12:33 and 14:36 on the 29/06/2018. Over the monitoring period 54 interference events were detected, all of which were classed as low priority, indicating a low-powered and short-duration interference signal. 30 of these events were false alarms, caused by physical obstructions between the receiver and the sky. These generally consisted of tunnels and bridges and led to disruptions of a few seconds. This shows a need to refine the DETECTOR server-side processing for the railway dynamic use case (DETECTOR has been used almost exclusively for monitoring at static locations to date).

There are however a few events which were not apparently caused by bridges and tunnels. An example on the L1 frequency is given below in Figure 2-2. When looking at a map of the region where the event was detected there are no physical obstructions around (Figure 2-3). There is however an electrical device next to the tracks which could be the source of the RFI. Alternatively, a second train with some electrical equipment could have passed by at this time. The impact on positioning algorithms is likely to be negligible due to the low power of the signal, which is typical of wide band signals.

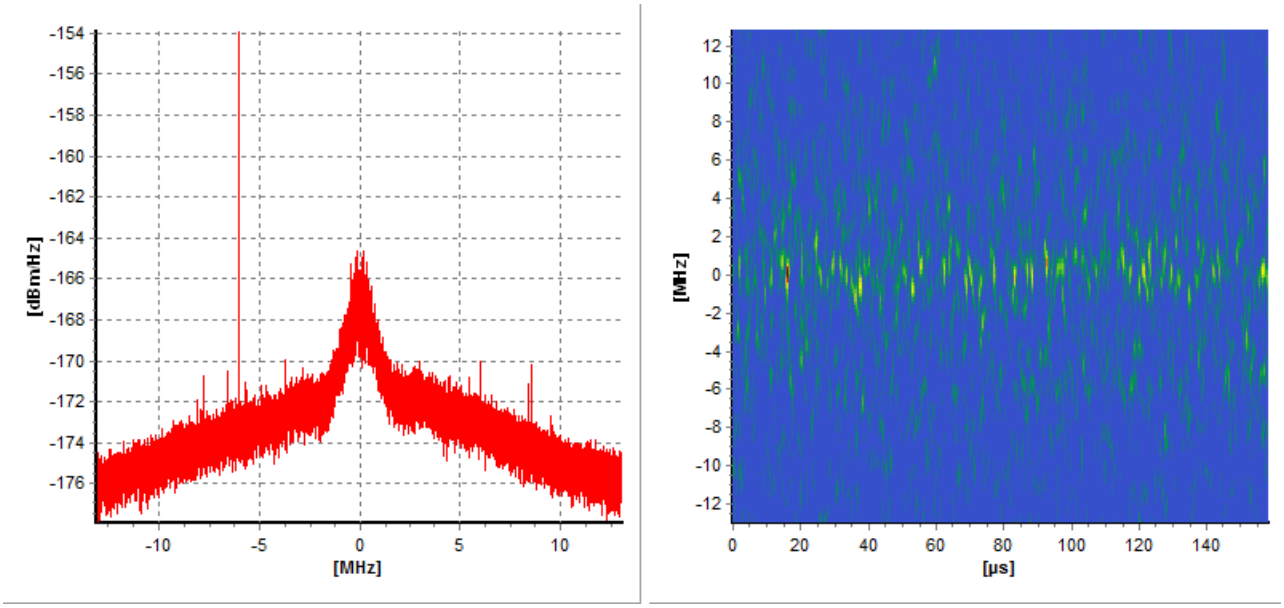


Figure 2-2: Spectrum and spectrogram of an interference event on 29/06/2018 at 13:55:46

Figure 2-3: Map of the area surrounding the interference event with the possible source encircled.

2.5.2 TTS Test Train, Germany

The DETECTOR probe installed on the TTS test train in Germany was active from 23/08/2018 – 24/10/2018. Over the course of the monitoring period 674 events were detected. 76% of those signals were white noise and a further 19% were narrow band type signals. The latter of the two are typically produced unintentionally by nearby electrical equipment. With the exception

of one high priority event, all the signals were very low priority and low power. Figure 2-4 shows a very narrow band signal around that of the GNSS operating frequency. The interesting feature is the weak narrow chirp type signal at a lower frequency. The presence of this secondary signal does not seem to have had an impact on positioning. The chirp type signal occurred 14 times between 08:56 and 09:09 and was never seen again. This was found when the probe was in the rail yard near Zur Centralwerkstätte in Weiden in der Oberpfalz.

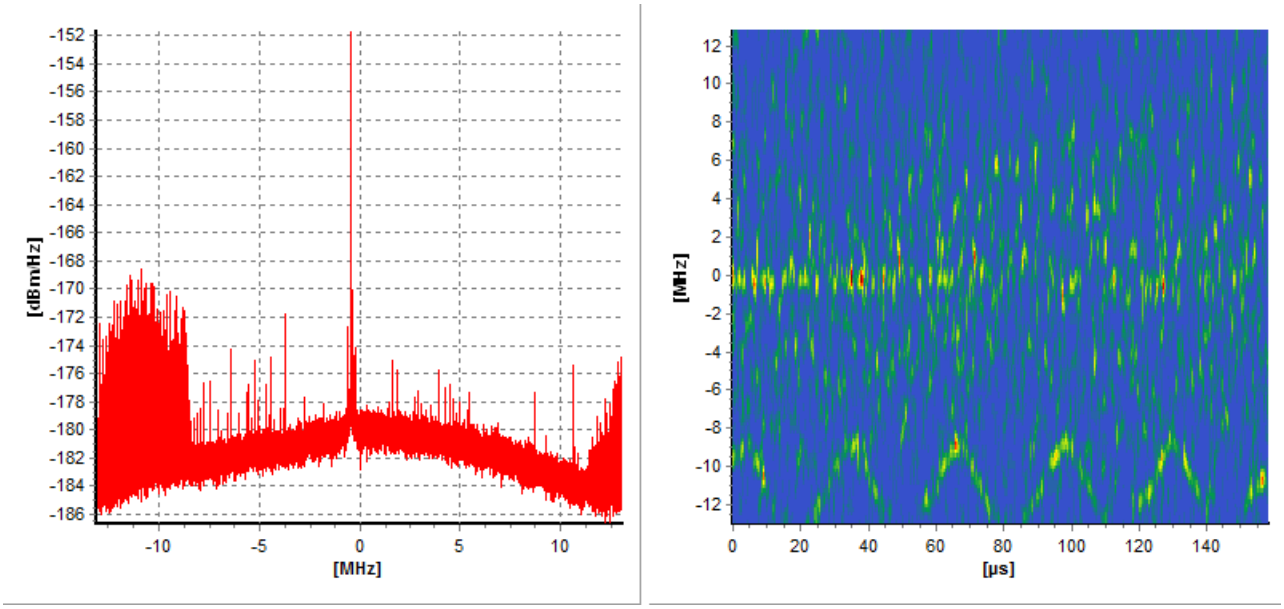


Figure 2-4: Spectrum and spectrogram for an interference event on 23/08/2018 at 09:01

2.5.3 Cagliari – San Gavino Line, Italy

The third GSS200D DETECOR probe was installed on a train traveling along the San Gavino Line from Cagliari. The probe was operational from around 8 am to 12pm on 15/11/2018 & 16/11/2018. Overall, the primary source of interference was found to be white noise and wide band signals, with a low power and duration. Throughout the two days there were several events with a noticeable peak in power at a specific frequency. Most commonly this is around 2.5MHz below the central frequency of the L1 band. There are some smaller peaks at a greater frequency however they are less noticeable in certain events. These events had little effect on the position calculations.

2.6 Conclusions

The following conclusions can be made as a result of the RFI analysis:

- The RFI events detected had little to no impact on GNSS positioning;
- Longer monitoring periods would be required in order to enable a thorough analysis of the RFI environment on different vehicle classes and in different geographical locations. For example, the chirp event detected, typical of a jamming device, may be better understood through the installation of a DETECTOR probe in the rail yard near Zur Centralwerkstätte in Weiden in der Oberpfalz;

- There is a need to refine the DETECTOR server-side processing for the case of a dynamic probe (installed on a vehicle). In particular, this is needed in order to avoid false alarms due to loss of GNSS signals in locations such as tunnels.

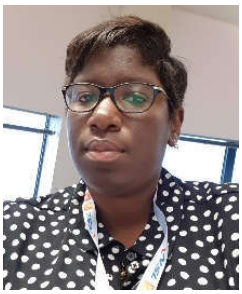
2.7 References

[1] European Commission Joint Research Centre, 'Radio Frequency Interference Impact Assessment on Global Navigation Satellite Systems', EUR 24242 EN, January 2010

2.8 Authors

Michael Hutchinson has over 14 years of experience in the GNSS industry. Michael has developed solutions for and provided consultancy on a wide range of GNSS applications involving robust and reliable positioning and navigation. This includes aviation approach operations, liability critical automotive programmes, future train control systems and Unmanned Aerial Vehicles (UAVs). Michael also provides consultancy on GNSS system level topics. Michael currently works as Business Manager and Principal Navigation Engineer at GMV NSL, coordinating business development activities and leading the company's work in the railway domain.

michael.hutchinson@gmvnsl.com



Terri Richardson is a Senior Navigation Engineer at GMV NSL, having joined the company in 2018. In this time, Terri has worked on projects involving the use of GNSS in the railway domain and GNSS system-level performance monitoring. Terri previously managed a knowledge transfer partnership research project between the University of Nottingham and Veripos Limited based on multi-constellation GNSS positioning. She holds a PhD in Civil Engineering and Geodetic Science from the Ohio State University, USA.

Terri.Richardson@gmnvnsl.com

David Payne joined GMV NSL in 2018 on the company's graduate scheme and is now a junior navigation engineer. David obtained an MSci in Physics with Astronomy from the University of Nottingham in 2018. Since joining NSL David has worked on the GNSS radio frequency interference detection in the H2020 STRIKE3 project and has helped to build the company's in-house robot named Wombat, used for dynamic testing of navigation equipment.

david.payne@gmnvnsl.com

3 Integrity assessment-oriented performance analysis of a fault-tolerant weighted tightly coupling GNSS/IMU integration

Nourdine Aït Tmazirte, IRT RAILENIUM, Famars, France
Juliette Marais, Université Gustave Eiffel, Villeneuve d'Ascq, France
Maan El Badaoui El Najjar, Université Lille Nord-Europe, Villeneuve d'Ascq, France

3.1 Introduction

Global Navigation Satellite Systems (GNSS) represent an opportunity to shift the railway ecosystem, to the point that they are considered as a game changer. Current positioning systems are based on physical balises scattered along the tracks. They, intrinsically, present various disadvantages such as the multitude of competing non-interoperable solutions, or their high costs of maintenance. The prospect of sharply lowering these CAPEX / OPEX costs motivates stakeholders to explore possible solutions. Among the reasons for considering the use of GNSS, the following (not exhaustive) are the main ones:

- global coverage of different constellations (Galileo, GPS, GLONASS, Beidou …),
- unlimited capacity (number of users),
- ability to determine a position all over the world without apriori knowledge or calibration,
- improvement infrastructures, available for free, such as EGNOS.

The envisaged applications are various, ranging from non-safety critical, such as passenger information services or asset management, to safety relevant ones such as Automatic Train Protection or Train Integrity/Train Length Monitoring.

GNSS alone, used as standalone positioning systems, satisfy most of the requirements for the firsts cited applications. Recent experimentations suggest that, they could also meet expectations for safety-relevant ones in open areas, including some equipped regional lines. However, the need of high available, accurate and safe onboard positioning systems, in any circumstance, motivates the community to investigate state-of-the-art solutions. In this context, multi-constellation multi-frequency SBAS-aided GNSS receivers have proven their ability to enhance the provided solutions.

Thus, to ensure continuity of a fail-safe positioning solution, the use of complementary heterogeneous sensors with a smart hybridization becomes essential. Inertial measurement units (IMU) are particularly interesting candidates. The fusion of GNSS and IMU raw data leverages the benefits of each of these sensors. It permits to find a good compromise between a non-precise but accurate along time GNSS alone solution, and a very precise IMU solution,

but only in a short-time window. It also ensures, for a determined period, to provide an IMU alone based positioning solution when GNSS is no more available, like in tunnels.

Safety-critical systems not only require the localization unit to meet accuracy or continuity, but more importantly, it requires the unknown positioning error to be correctly bounded in order to avoid to hazardously mislead the train control system and to satisfy the allocated Tolerable Hazardous Rate (THR). The concept of integrity was first developed for aviation applications and is currently investigated for rail applications. Indeed, Receiver Autonomous Integrity Monitoring (RAIM) algorithms defined for aviation applications are not applicable, as such, due to the difference in safety requirements and operational environment between aviation and land applications. New dedicated algorithms are developed for railway applications [1,2]. Terrestrial applications can face particularly harsh environments (urban canyon, forests ...) where a dilemma appears between the reduced number of visible satellites and the possibility of confronting multiple simultaneous errors (NLOS, multipath interferences ...). Based on that observation, implementing a strategy uniquely based on a Fault Detection and Exclusion (FDE) layer can lead to a decrease of the localization function availability. Oppositely, relying exclusively on a strategy of weighting observations cannot guarantee the coverage of all errors, particularly those having a large impact on positioning error. Only a harmonious employment of these two strategies can fulfill both the availability and safety requirements.

With a real dataset collected along a railway line, we aim to highlight the impact of weighting as a first step to globally improve accuracy. We then show that the FDE strategy, based on a solution separation (SolSep) approach, correctly removes outliers. Finally, a discussion on the need to express the concepts of protection level and position errors no longer simply on the horizontal component (HPL/HPE) but on the along track (ATPL/ATPE) and cross track (CTPL/CTPE) components is conducted.

3.2 GNSS/IMU tightly coupling scheme

A tightly coupled algorithm uses a stochastic filter to estimate the current bias of the IMU positioning solution by integrating the error between the GNSS observations, namely pseudoranges and pseudoranges rates ($\rho_{gnss}\dot{\rho}_{gnss}$), and the corresponding deduced information ($\rho_{ins}\dot{\rho}_{ins}$) from the position, velocity and attitude coming from the mechanization equations of IMU raw data. A block diagram of the implemented tightly coupled architecture is reported in Figure 3-1.

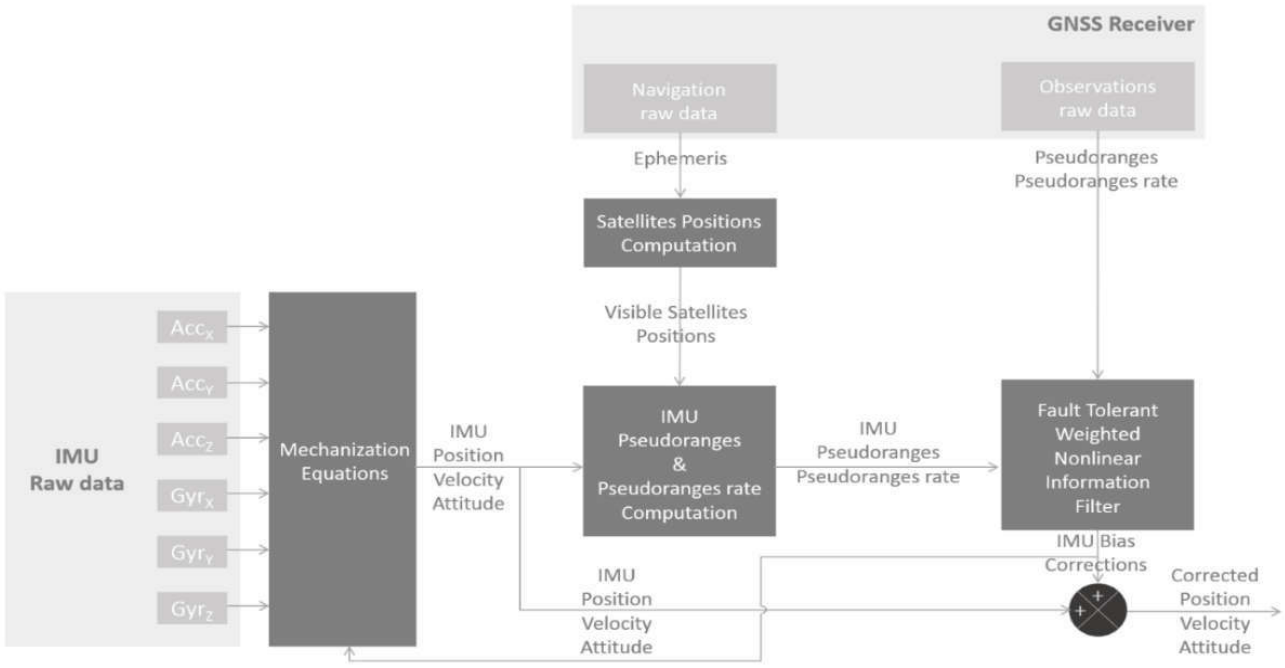


Figure 3-1: Block diagram of the tightly coupled architecture.

To achieve an efficient fail-safe positioning function using the fusion between GNSS and IMU raw measurements, a Nonlinear Informational Filter (NIF), which is a different representation of usually used Extended Kalman Filter (EKF) is implemented. This form is chosen mainly because it makes a SolSep approach, easy to implement and more efficient in term of computation burden[3].

3.2.1 Nonlinear Information Filtering

The NIF consists of two steps:

1. The prediction step which is usually based on a mathematical model roughly describing the train evolution.

2. The correction step where the GNSS and IMU measurements are used to update the estimation.

The seventeen variables error state used in the tightly coupling integration to correct the IMU bias is as follow:

$$\delta X = \left[\delta x\ \delta y\ \delta z\ \delta V_x\ \delta V_y\ \delta V_z\ \delta A_x\ \delta A_y\ \delta A_z\ \delta \omega_x\ \delta \omega_y\ \delta \omega_z\ \delta f_x\ \delta f_y\ \delta f_z\ \delta t\ \delta t'\right]$$

Where $\delta x\ \delta y\ \delta z$ are the errors related to position, $\delta V_x\ \delta V_y\ \delta V_z$, the errors related to velocity and $\delta A_x\ \delta A_y\ \delta A_z$ the errors related to attitude. $\delta \omega_x\ \delta \omega_y\ \delta \omega_z\ \delta f_x\ \delta f_y\ \delta f_z$ are the errors associated with the IMU gyroscopes and accelerometers. While δt and $\delta t'$ are the clock bias and drift errors that affect the GNSS receiver.

The evolution model of the error state is:

$$\delta X_{k|k-1} = \Phi_{k-1} \delta X_{k-1|k-1} + w_{k-1}$$

with w_k the model noise considered to be a Gaussian white noise of zero mean value with Q_k as covariance matrix.

And Φ_k is the model transition matrix defined in [4,5] as:

$$\Phi_k = \begin{bmatrix} I_{3*3} & T_k.I_{3*3} & 0_{3*3} & 0_{3*3} & 0_{3*3} & 0 & 0 \\ N^e & I_{3*3} - 2T_k\Omega_{ie}^e & -T_k.F_k & 0_{3*3} & T_k C_{b,k3*3}^e & 0 & 0 \\ 0_{3*3} & 0_{3*3} & I_{3*3} - T_k\Omega_{ie}^e & T_k C_{b,k}^e & 0_{3*3} & 0 & 0 \\ 0_{3*3} & 0_{3*3} & 0_{3*3} & I_{3*3} + T_k D_g & 0_{3*3} & 0 & 0 \\ 0_{3*3} & 0_{3*3} & 0_{3*3} & 0_{3*3} & I_{3*3} + T_k D_a & 0 & 0 \\ 0_{1*3} & 0_{3*3} & 0_{3*3} & 0_{1*3} & 0_{1*3} & 0 & 1 \\ 0_{1*3} & 0_{3*3} & 0_{3*3} & 0_{1*3} & 0_{1*3} & 0 & 0 \end{bmatrix}$$

with:

- $C_{b,k}^e$ the Direct Cosine Matrix (DCM) computed from body-frame to earth frame
- D_a and D_g are the time-constant diagonal matrices that define a first-state Gauss-Markov model for the accelerometers and the gyroscopes
- F_k the skew-symmetric matrix of the accelerometers measured at time-k
- N^e the tensor of gravity gradients
- $T_k$is the time interval between two consecutive executions of prediction step
- Ω_{ie}^e the Earth rotation rate

In the information form, instead of dealing with state co-variance matrix P and state vector δX, the filter estimates an information matrix Y and an information state vector δy.

$$Y_k = P_k^{-1}\delta y_k$$

The predicted information matrix is computed by inversing standard EKF predicted state covariance:

$$Y_{k|k-1} = \left[\Phi_k P_{k-1|k-1}\Phi_k^T + Q_k\right]^{-1}$$

Predicted state vector is then computed:

$$\delta y_{k|k-1} = P_{k|k-1}^{-1}\delta X_{k|k-1}$$

$$\delta y_{k|k-1} = Y_{k|k-1}\delta X_{k|k-1}$$

When a new set of measurements (pseudo-ranges and pseudoranges rate) is available, Z_k, the measurements vector is constructed as follow:

$$Z_k = \begin{bmatrix} \rho_{gnss} - \rho_{ins} \\ \dot{\rho}_{gnss} - \dot{\rho}_{ins} \end{bmatrix} = \left[\delta\rho_{sat1,k} \ldots \delta\rho_{satn,k}, \delta\dot{\rho}_{sat1,k} \ldots \delta\dot{\rho}_{satn,k}\right]$$

The equation which describes the observations measurements in the NIF is:

$$Z_k = H_k X_{k|k-1} + v_k$$

with v_k the observation noise also considered to be a Gaussian white noise of zero mean value and with R_k as covariance matrix.

The observation matrix H_k is time varying and depends on the number of satellites in visibility at each epoch:

$$H_k = \begin{bmatrix} H_{n,3}^{gnss}(k) & 0_{n*6} & 0_{n*6} & 1_{n*1} & 0_{n*1} \\ 0_{n*3} & H_{n,3}^{gnss}(k) & 0_{n*9} & 0_{n*1} & 1_{n*1} \end{bmatrix}$$

where $H_{n,3}^{gnss}$ is the Jacobian matrix of the non-linear relationship $h^{gnss}(k)$ between the user's state (position, velocity and clock) and the n pseudoranges ρ^{sat_1} … ρ^{sat_n}:

$$H_{n,3}^{gnss}(k) = \left[\frac{\delta h^{gnss}(k)}{\partial X}\right]_{X=X_{k|k-1}} = \begin{bmatrix} (x^{sat_1} - x)/R_{sat_1} & (y^{sat_1} - y)/R_{sat_1} & (z^{sat_1} - z)/R_{sat_1} \\ \vdots & \vdots & \vdots \\ (x^{sat_n} - x)/R_{sat_n} & (y^{sat_n} - y)/R_{sat_n} & (z^{sat_n} - z)/R_{sat_n} \end{bmatrix}$$

$$R_{sat_j} = \sqrt{(x^{sat_j} - x)^2 + (y^{sat_j} - y)^2 + (z^{sat_j} - z)^2}$$

$(x^{sat_j}, y^{sat_j}, z^{sat_j})$ denotes the position of the j^{th} satellite and (x, y, z) the linearization point $X_{k|k-1}$, here the IMU estimated position.

Finally, the corrected information matrix and vector are respectively computed as follow:

$$Y_{k|k} = Y_{k|k-1} + \sum_{sat=1}^{n} I_{sat}(k)$$

$$\delta y_{k|k} = \delta y_{k|k-1} + \sum_{sat=1}^{n} i_{sat}(k)$$

where $I_{sat}(k)$ and $i_{sat}(k)$ are the individual information contribution of each satellite to the correction step:

$$I_{sat}(k) = H_i^{gnss}(k)^T R_i^{-1}(k) H_i^{gnss}(k)$$

$$i_{sat}(k) = H_i^{gnss}(k)^T R_i^{-1}(k) Z_i(k)$$

3.2.2 GNSS observations weighting model

In contrast with a naïve strategy of providing an equal variance value to all measurements, the principle of weighting observations is to construct the observation noise covariance matrix R_k [6] such that the estimator takes advantage of apriori-considered as optimally received measurements and reduce the impact of potentially affected ones (by local propagation phenomena). This is even more true in harsh environments, where the user has often a limited visibility of the sky and where signals may be subject to local feared event such as multipath or NLOS. The work presented in [7] shows the benefit of a Weighted EKF along an urban road path.

Weighting models from the literature are dependent on elevation [8] and/or C/N_0 [9]. If satellite elevation dependent observations weighting has been successfully used in high precision applications, C/N_0 also provide valuable knowledge on signal that should be integrated. A comparison of elevation and C/N_0 based models is given in [10] where it is shown that low elevation satellites are more accurately weighted with C/N_0 based weightings. For this reason, we have chosen to apply a balanced combination between elevation (ELEV-model) and C/N_0 weighting model ($sigma - \Delta$):

$$\sigma^2_{pr_{satj}} = \left(\frac{1}{2} + \alpha(El_{sat_j})\right)\frac{1}{sin^2\left(El_{sat_j}\right)} + \left(\frac{1}{2} - \alpha(El_{sat_j})\right)\left(a + b.10^{\frac{-C/N_{0satj}}{10}}\right)$$

where a, b are antenna, receiver and frequency depending parameters and $\alpha(El_{sat_j})$ the balance parameter in function of satellite elevation and following a sigmoid shape curve as drawn in Figure 3-2:

$$\alpha\left(El_{sat_j}\right) = \gamma_{scale}\left(\frac{1}{1 + exp^{\lambda\left(El_{slope} - El_{sat_j}\right)}} - \frac{1}{2}\right)$$

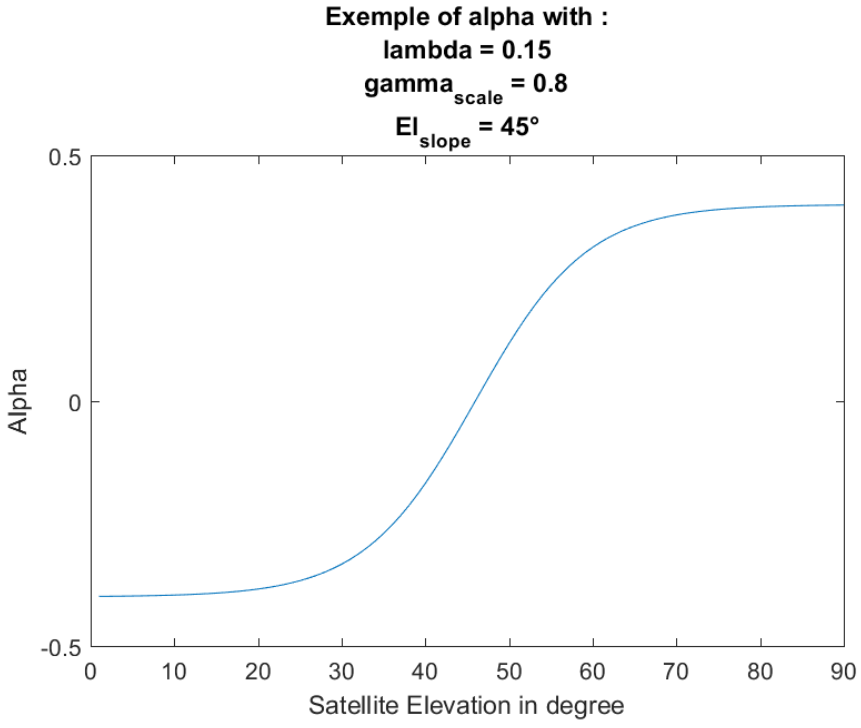


Figure 3-2: α: balance parameter between CN/0 sigma-Δ and ELEV models

3.2.3 Fault Detection and Exclusion layer

Integrity relates to the ability of a system to timely issue warnings to users when the information provided by the system is considered unreliable. An integrity monitoring scheme is usually composed of two steps. First one consists in a Fault Detection and Exclusion (FDE) module. Second one concerns the computation of a protection level.

Two main different strategies for detecting faults in GNSS observations exist. A great part of the FDE algorithms implemented in GNSS for RAIM, are based on detection at pseudorange level. They present the advantage of being particularly efficient in terms of execution time, but do not guarantee that an overestimation (or under-) of the pseudorange has a real impact on the estimated position. Conversely, in case of very bad satellites geometry (Dilution Of Precision DOP), a small pseudorange error may not be detected with a pseudorange level FDE algorithm but could badly affect the position estimation.

In this study, a SolSep strategy is implemented. The NIF correction being a simple sum between the predicted state and the sum of each individual observation information contribution (which is not the case in the EKF form), it is straightforward to design a SolSep approach removing only faults affecting the estimated position. Another main strength of using the informational form is the multiple choice of divergences from information theory usable as consistency test, notably the widely used Kullback-Leibler divergence [3]. Figure 3-3 gives on overview of the implemented approach.

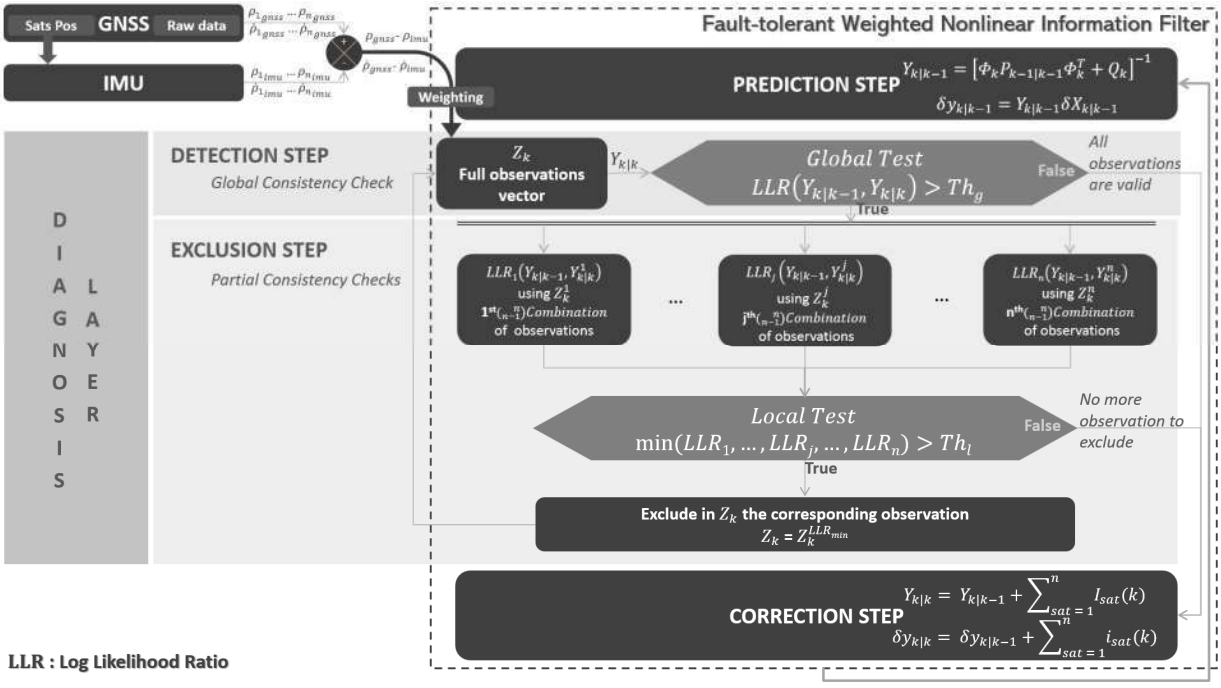


Figure 3-3: Solution Separation approach based on a Weighted Nonlinear Information Filter

3.3 Integrity monitoring

Integrity could be defined as a measure of trust that can be placed in the correctness of the information supplied by the localization function. In [12], the EKF Innovation-based Classic Test and the EKF Innovation-based Danish (IBDAN) methods are proposed in a GNSS alone configuration. This paper will analyze the performance of the IBCT method in a GNSS/IMU integration scheme.

3.3.4 Cross Track & Along Track definition

In classical uses, derived from aeronautics requirements, the protection level is expressed as 3D volume where HPL (Horizontal Protection Level) and VPL (Vertical Protection Level) respectively bounds residual errors in the horizontal and vertical planes. In railway application, only the HPL is applicable. Furthermore, the train runs on 1D tracks. The GRAIL-2 project introduces the "along-track" PL (ATPL), considering the projection of HPL on the train track [13]. The other dimension is the "cross-track" protection level (CTPL).

Some proposals for computing the position consider the track as a [14][15]. Thus, the corresponding ATPL could make use of the track description information in its computation [16].

Figure 3-4: Illustration of ATPL and CTPL concepts

CTPL will be an important element for track discrimination that remains today a strong issue for the use of GNSS in rail.

ATPL is of main importance for train safety. Indeed, in modern signaling systems, the Movement Authority (MA) gives the train the permission to run to a specific location within the constraints of the infrastructure. This information is based on the on-board estimated train position and speed as well as the train position confidence interval [15].

3.4 Conclusion

Meeting the requirements of availability, precision, and safety can be considered as a challenging target. In order to achieve, this study investigates the implementation of a multi-sensor fusion technique. The IMU, in the literature, is presented as ideally complementary to

GNSS. Different integrations, occurring more or less early in the navigation chain are possible, namely the loosely coupling, the tightly coupling and the deeply coupling integrations. A tight integration has been developed for its ability to continue to benefit from GNSS measurements even with a satellites' visibility below four. Added to this, a GNSS measurements weighting procedure and a fault detection and exclusion module permit to increase precision and thus ensure integrity. Finally, the specificities of rail require a redefinition of RAIM algorithms, the concepts of along track and cross track protection level are discussed.

3.5 References

[1] J. Liu, B. Cai, D. Lu and J. Wang, "Integrity of GNSS-based Train Positioning: From GNSS to sensor integration," 2017 European Navigation Conference (ENC), Lausanne, 2017, pp. 48-56.

[2] Brocard P., Julien O., Mabilleau M. Autonomous Integrity Monitoring Proposal for Critical Rail Applications. GNSS+ 2015, 28th ION International Technical Meeting of The Satellite-Division-of-the-Institute-of-Navigation, Institute of Navigation, Sep 2015, Tampa, United States. pp. 706-734.

[3] Al Hage J. and El Najjar M. E. B., "Improved Outdoor Localization Based on Weighted Kullback-Leibler Divergence for Measurements Diagnosis," IEEE Intell. Transp. Syst. Mag., 2018.

[4] Petovello, M. Real-time Integration of a Tactical-Grade IMU and GPS for High-Accuracy Positioning and Navigation. Ph.D. Thesis, University of Calgary, Calgary, AL, Canada, April 2003.

[5] Falco G, Pini M, Marucco G. Loose and Tight GNSS/INS Integrations: Comparison of Performance Assessed in Real Urban Scenarios. Sensors (Basel). 2017;17(2):255.

[6] Zhu, N. "GNSS Propagation Channel Modeling in Constrained Environments: Contribution to the Improvement of the Geolocation Service Quality", Doctoral dissertation of the University of Lille, October 2018.

[7] Zhu, N., Betaille, D., Marais, J., & Berbineau, M. (2018, September). Extended Kalman Filter (EKF) Innovation-Based Integrity Monitoring Scheme with C/N 0 Weighting. In 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI). pp. 1-6

[8] Wang, J., Stewart, M. P., & Tsakiri, M. (1998). Stochastic modeling for static GPS baseline data processing. Journal of Surveying Engineering, 124(4), 171-181.

[9] Kuusniemi, H., Wieser, A., Lachapelle, G., & Takala, J. (2007). User-level reliability monitoring in urban personal satellite-navigation. IEEE Transactions on Aerospace and Electronic Systems, 43(4), 1305-1318.

[10] Luo X., Mayer M. and Heck B., 2012, Analysing Time Series of GNSS Residuals by Means of ARIMA Processes. International Association of Geodesy ymposia, Vol. 137, pp 129-134.

[11] M. Joerger and B. Pervan, "Fault detection and exclusion using solution separation and chi-squared ARAIM," in IEEE Transactions on Aerospace and Electronic Systems, vol. 52, no. 2, pp. 726-742, April 2016.

[12] Zhu, Ni, "GNSS Propagation Channel Modeling in Constrained Environments: Contribution to the Improvement of the Geolocation Service Quality," Université Lille, 2018.

[13] Marradi, L., Galimberti, A., Foglia, L., Zin, A., Pecchioni, C., Doronzo, M., ... & Lekchiri, M. (2012, December). GNSS for enhanced odometry: The GRAIL-2 results. In 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing (pp. 1-7).
[14] O. Heirich, P. Robertson, and T. Strang, "RailSLAM - localization of rail vehicles and mapping of geometric railway tracks," in Proc. IEEE Int. Conf. on Robotics and Automation (ICRA), 2013, pp. 5212–5219.
[15] Winter, H., Willert, V., & Adamy, J. (2018, November). Increasing Accuracy in Train Localization Exploiting Track-Geometry Constraints. In 2018 21st International Conference on Intelligent Transportation Systems (ITSC) (pp. 1572-1579).
[16] Presti, L. L., & Sabina, S. (Eds.). (2018). GNSS for Rail Transportation: Challenges and Opportunities. Springer.

3.6 Authors

Nourdine Aït Tmazirte works at French Institute of Technology Railenium since 2018. He got his engineering and M.Sc. degree in automation engineering from Ecole Centrale de Lille, France, both in 2010. His research interests include multi-sensor fault tolerant fusion for localization and integrity assessment.

AIT.TMAZIRTE@railenium.eu

Dr. **Juliette Marais** received the engineering degree from Institut Supérieur de l'Electronique et du Numérique. She received the Ph.D. degree in electronics and the "Habilitation à diriger des recherches" from the University of Lille, France, in 2002 and 2017 respectively. She is a research fellow with Université Gustave Eiffel (former IFSTTAR). She is involved on two main research projects: integrity monitoring for land transport applications and GNSS propagation characterization in railway environments, with some contributions in EU or national projects. Her research interests principally include propagation phenomena, positioning and pseudorange error modeling, filtering technics, and simulation.

juliette.marais@Univ-Eiffel.fr

Pr. **Maan El Badaoui El Najjar** received his Engineer Diploma and his Master of Science degrees in control system from the INP Grenoble - France respectively in 1999 and 2000. He received the Ph.D. degree in Perception and Control Systems from the University of Technology of Compiegne in 2003. In November 2011, he obtained the Habilitation à Diriger des Recherches from the University of Lille. He joined the University of Lille in 2005 as a permanent asso ciate Professor. Since 2014, he is Full Professor at the same University. He is also with the CRIStAL Laboratory UMR 9189, a joint research unit between CNRS, University of Lille and Ecole Centrale de Lille. He is also the head of the DiCOT Team "Diagnostic, Control and Observation for fault Tolerant Systems" of the CRIStAL Laboratory.

maan.el-badaoui-el-najjar@univ-lille.fr

4 Radiolocalization technologies for on-board positioning

Jon Goya, Gorka de Miguel, Nerea Fernández, Iker Moya, Jaizki Mendizabal; CEIT, San Sebastián, Guipúzcoa, Spain

4.1 Introduction

The study of the radiolocalization technologies has been covered in the X2R2-WP3. The aim of this WP is to develop the concept of fail-safe train positioning. As a contribution to that, an analysis of the radio localization is carried out. The analysis of this technology has been done based on the Shift2Rail TD2.1, where technologies for the communication between coaches and to the ground where studied. As radio localization is currently considered as a complementary positioning technique, the focus is to solve critical issues that GNSS based position systems are facing, such as tunnels and station where the GNSS signals are partially or fully blocked. Based on the preliminary analysis and the location requirements for train operations (in terms of accuracy and availability), such as for the cold start-of mission (track selective capabilities), UWB seems to be the best alternative. Thus, in this paper UWB technology is described and test is carried out under a complex scenario in order to determine a more realistic performance of the technology.

4.2 Analysis of technology maturity and readiness for safety-critical applications

In this section, the UWB technology is analysed from the technology perspective in order to extend the knowledge regarding the capabilities and possibilities that offers. Particularly, the maturity level of the technology, possible side effects and scalability of the proposed solution in order to be able to solve particular situations in which UWB could be beneficial. This general perspective is necessary to understand the technology; however, a more particular analysis of the impact of UWB in the railway domain is covered in section with title "Processing of measured data and expected performance".

4.2.1 Suitability and maturity of radio localization technologies

In this section, UWB maturity is presented regarding several important aspects:

- Performance regarding the position accuracy
- Scalability of the system
- Positioning strategies
- Potential security hazards and mitigations of the technology

Concerning this, UWB seems to be a unique technology capable of achieving accuracy requirements to be track selective. This is the reason why further analysis is carried out to

understand the maturity of the technology and its capabilities. The description of the technology regarding the physical layer has been already covered in the c, this why in this article only the key aspects are going to be presented to provide to the reader enough information to understand UWB technology and its status.

For an overall overview, Table 4-1 [3] covers a summary of the different technologies. Table 4-1 compares aspects such as the range, accuracy, availability, maintenance, etc. are included. As it can be seen none of the technologies can fulfil all the characteristics. As each of them has different strengths, it is important to decide based on the requirements will fit better. In general, the increase of the range leads to a decrease in the accuracy. The number of elements needed to set-up in the infrastructure also is linked to the range and maintainability of the solutions. Based on this, the best alternatives are Wi-Fi, Bluetooth and UWB, being UWB the one with the highest accuracy among them and thus the most interesting from the railway point of view.

Table 4-1: Comparison of Wireless Positioning Technologies [3]

Characteristics	**IR**	**Passive RFID**	**Active RFID**	**Wi-Fi**	**Bluetooth**	**UWB**
Range	- -	- -	-	++	+	++
Accuracy	++	+++	++	+	++	+++
TTFF, TTF	+++	+++	+++	++	++	++
Availability of location	-	- -	- -	+++	++	+++
Communication capacity	- -	N/A	N/A	++	+	+
Infrastructure cost efficiency	- -	- -	-	++	+	+
Tag/receiver cost efficiency	+	+++	++	+	+	-
Deployment cost efficiency	- -	-	+	++	+	+
Maturity	+++	+++	+++	++	++	- -
Maintenance	+	+	+	++	+	+
Electrical consumption	-	+++	++	-	+	-
Excellent (+++), Very Good (++), Good (+), Poor (-), Very Poor (- -), Not Applicable (N/A)						

Once the overall picture is presented, the next steps in this document is to go through the detailed description of other aspects in order to analyse the UWB radio localization feasibility for the railway domain. In the preliminary field-test COTS UWB solutions have been used. However, as technology evolves, new modules are being developed. These modules are used to provide a Two-Way-Ranging (TWR) used for Real-Time Location Systems (RTLS).

4.2.2 UWB performance

The system performance can be divided into several aspects such as the performance related to positioning or UWB physical parameters which are already fixed.

Regarding the positioning performance, there are several aspects that are worthy of particular focus, such as accuracy (<10 cm) under Line-of-Sight conditions and the UWB range as it will determine the number of nodes needed in order to scale the system to cover larger areas.

The system is based on a TDMA channel access TN [1]. This means that the number of tags that can be used is determined by the location update frequency requested. The higher the number of nodes that the system is aiming to position at the same time, the lower the position update frequency that the system is going to have (see Figure 4-1). Considering the UWB measurement as a Real-Time Location System (RTLS) for a certain area the following table 4-2 shows the obtained performance for this solution.

Table 4-2: UWB Performance [5]

Parameter	Description	Notes
RTLS System Performance		
X-Y location accuracy	<10 cm (typical)	Line-of-Sight (LOS)
UWB Range (node to node LOS)	~60 m	
System capacity / cluster	150 Hz	750 tags @ 0.2 Hz 150 tags @ 1 Hz 15 tags @ 10 Hz etc.
Max. Location Rate / Tag	10 Hz	
Min. Location Rate / Tag	0.0167 Hz	Every 1 minute
Max # Anchors (theoretical)	Area Dependent	See section 7
Max. # Tags / cluster (theoretical)	9000	@ min. rate of 0.0167 Hz (every 1 minute)

Figure 4-1: UWB Performance [5]

Once the system performance based on the datasheet is shown, the scalability of the system should be considered in order to determine the feasibility of the system for the railway environments.

4.2.3 UWB positioning topologies

The simplest manner to cover areas is by following structured topologies. There exist two main topologies, but any other can be generated if it fulfils the previously mentioned deployment rules.

The first example is the star topology that could be used for circular areas. The blue dots depict the external anchors, the brown anchors are considered as routing anchors and the green dot

is the one that will work as a gateway connected to a managing system. The yellow dots are the tags example of tag location that can be located by using this architecture.

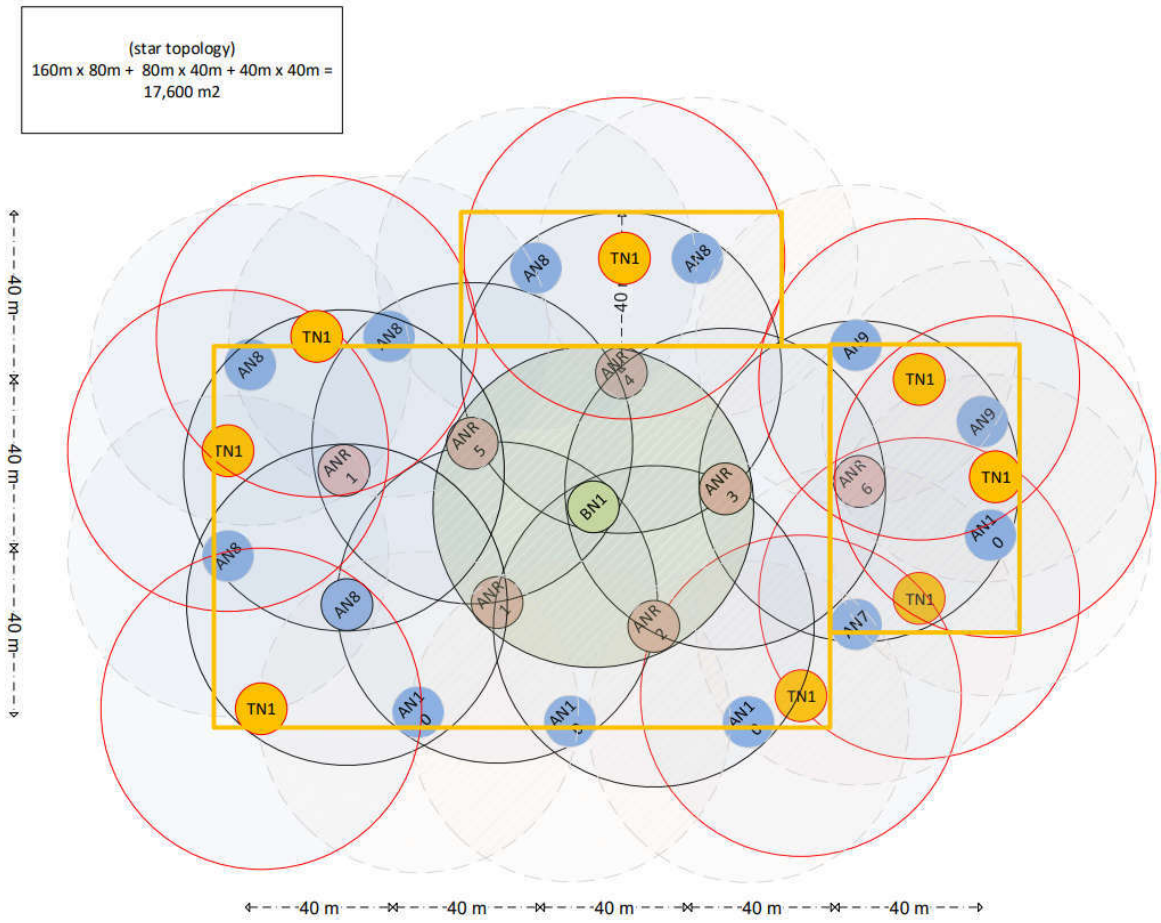


Figure 4-2: Star topology example [5]

In the same way, there is the possibility to create a line topology that would be more appropriate for the railway domain.

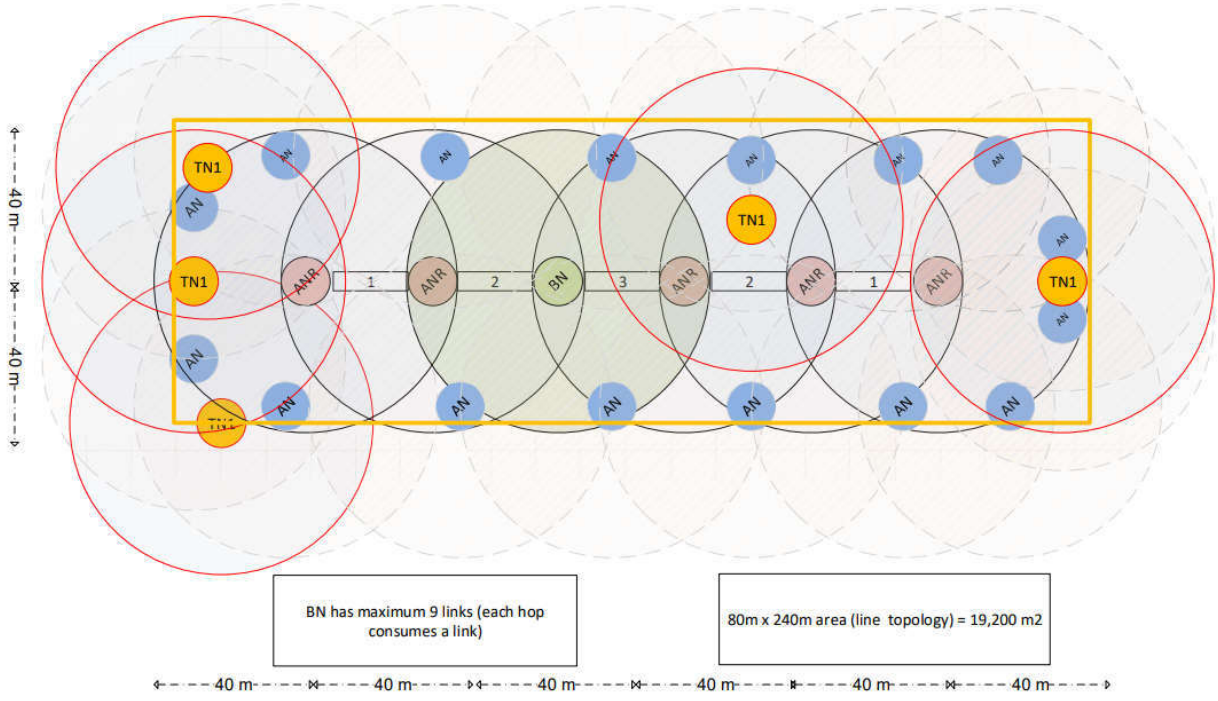


Figure 4-3: Line topology example [5]

4.2.4 UWB potential hazards

The aim of this section is to analyse the physical phenomena that can affect the UWB signals. These effects could incur in the degradation of the received signal and impact the performance of the final positioning system.

Possible physical phenomena that can affect the UWB Radio Localization in the railway domain [6] are:

- Multipath signal
- Non-line Of Sight (NLOS) signal
- Signal obscuration
- Electromagnetic interferences and radio equipment
- Access Control and Security
- Dilution of precision (DOP)
- Number of objects to locate

The transmitted signal has vulnerabilities similar to other wireless signals and techniques that are applicable to other mature wireless technologies can be applied to the UWB if necessary.

4.2.5 UWB potential mitigation

The aim of this section is to identify mitigations of potential hazards, as described in the previous section.

- Multipath signal, Non-line of Sight (NLOS) signal and Signal obscuration: Mitigation consists in evaluating the position of the UWB stations present in the area and possibly repositioning and/or increasing them to improve the received signal in all points of the line.
- Electromagnetic interferences: in addition to complying with the regulations in each country, mitigation consists of identifying possible sources that can reduce system performance. The sources of the disturbance may be other active objects that transmit, such as pantographs, train motors, or other devices placed in the vicinity of the transmitter. Relocating the antenna so as to maximize the distance from the source and if possible, deploying protection screens for unintended emissions.
- Access Control and Security: mitigation consists of introducing cryptographic data protection techniques with cryptographic keys that must be known to Tx and Rx.
- Number of objects to locate: the mitigation consists of performing an in-depth study of the maximum number of trains to be located in each area of coverage by performing a slight overestimation so as to also cover any degradation and reconfiguration of the UWB network according to the obtained results.

4.3 Processing of measured data and expected performance

In this section, the results obtained during the testing activity are described. In this case, the scenario has been selected due to the similarities with a train station, where there exist metallic structures and the overall shape of the area is rectangular.

4.3.6 Scenario description and measurement procedure

Figure 4-4: Field-test environment scenario

Figure 4-4 shows the environment in which the UWB performance test was carried out. This scenario is selected to measure the UWB signal reception under a high multipath environment due to the numerous metallic objects, and walls in which the signal could be reflected.

Figure 4-5 depicts the top view of the scenario. The scenario deploys the anchors higher than the tag to be located. In this case, only ranging measurements were performed in order to determine the accuracy of the ranging estimates of the system. Four anchors were deployed in order to have better visibility of the area and to detect different situations (see the blue dots in Figure 4-5). Additionally, eight different measurement points were selected (see the green dots in Figure 4-5).

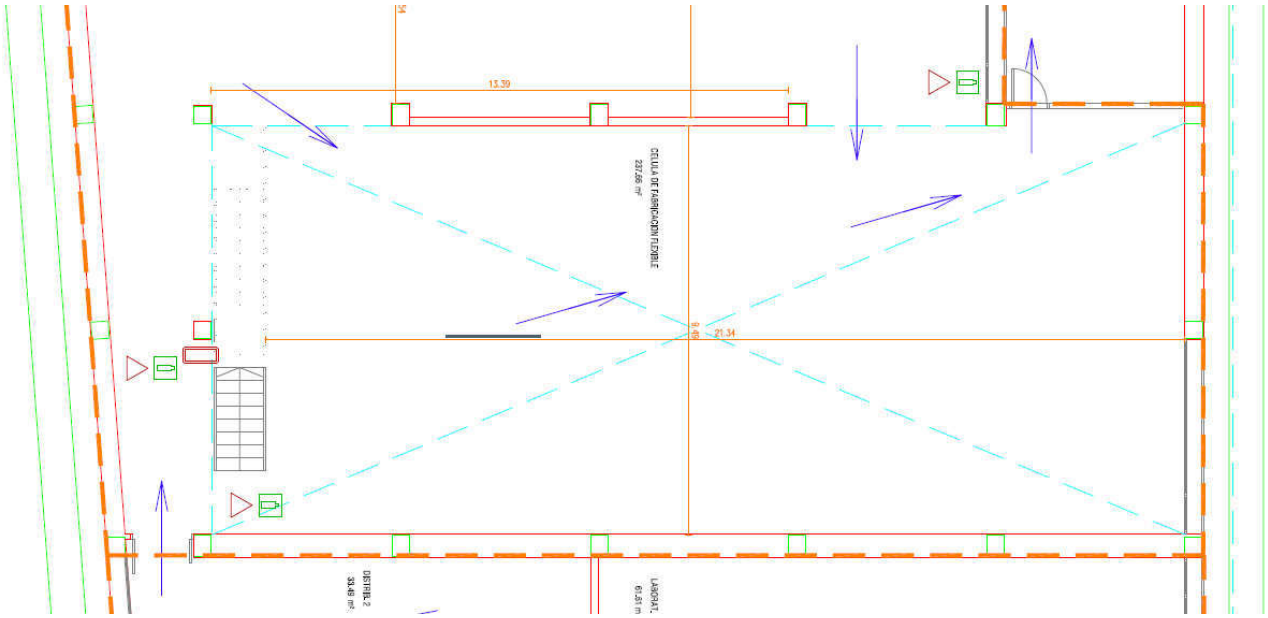


Figure 4-5: Schematic of the laboratory

For each of the measurement points, five minutes of measurements were recorded.

The location of the tags are selected to follow a straight line emulating the train location. Additionally, another set of measurements are carried out in a parallel line emulating another train in another platform. In this case, the performance analysis only measures the effect in the TX and RX signals.

Apart from determining the location of the measurement point, one of the most important points to take into account during the measurements is the reference location estimation. The accuracy of this measurement has a relevant impact on the final performance results. In order, to estimate these locations accurately, laser-based measurements have been carried out to determine the relative location of the tags inside the test area (see Figure 4-5).

4.4 Results

In this section, the ranging results obtained from the different measurements are presented. Table 4-3 shows the results obtained under LOS conditions, this means that at least the main anchor had a LOS vision with the tag. The obtained results show that the ranging error of the anchors is always under 50 cm (P4). In P4, the tag was out of the recommended area of coverage of the anchors and the performance compared to the rest of measurements is clearly worse. This means that a proper infrastructure deployment could provide ranging measurements with lower errors because of the visibility of all the anchors to the tag.

Table 4-3: Results for LOS field-test

Experiment no.	Real rang (cm)	Estimated range (cm)	Mean (cm)	Std (cm)	RMSE (cm)	P(95%)	P(99%)	P(Error<5cm)	P(Error<15cm)	P(Error<30cm)	Max Error (cm)
P1	468	468.19	1.6	1.06	1.92	3.5	4.5	99.51%	100.00%	100.00%	5.4
P2	853	871.74	18.74	1.98	18.84	22.4	22.9	0.00%	1.80%	100.00%	24.3
P3	1357	1366.41	9.41	2.08	9.63	12.9	14.29	1.13%	100.00%	100.00%	14.8
P4	1927	1967.55	40.55	2.32	40.61	44.79	46.18	0.00%	0.00%	0.00%	47.6
P5	1880	1880	1.84	1.31	2.26	4.09	5.3	98.18%	100.00%	100.00%	7.2
P6	1481	1492.8	11.8	2.05	11.98	14.88	15.9	0.00%	95.72%	100.00%	17.3
P7	1055	1072.78	17.78	1.71	17.86	20.5	21.38	0.00%	7.18%	100.00%	22.4
P8	909	943.49	34.49	1.67	34.53	37.19	38.1	0.00%	0.00%	1.15%	40

4.5 Conclusions

The capabilities of the radio localization technology, more precisely of UWB, to support fail safe train positioningin areas where the GNSS localization is not feasible. The readiness and maturity of the technology has been described in order to check and validate all the capabilities that this technology would need to fulfil railway requirements. Additionally, a preliminary analysis of the impact of the UWB technology for the Start of Mission scenarios is presented. As it can be seen, the introduction of these kinds of technologies could enhance the safety of the systems by starting at Level 2 after sending a valid position report. Finally, the performance of the technology is assessed during controlled field-test analysis validating the capabilities of the technology to fulfil the demanding accuracy requirements in order to discriminate between contiguous tracks. All this makes, radio localization technology promising for safety critical applications. Next steps will be to focus the development of the systems in order to adapt the technology and increase the systems reliability by introducing some of the presented countermeasures and critical chain redundancies. Additionally, the end user requirements should be used to determine which of the channel access modes should be selected based on the boundary conditions.

4.6 References

[1] X2RAIL-2, "Technical Note on Task 3.2 - Subtask 3 X2Rail-2 WP3 Analysis of the State-of-Art in radio localisation technologies." .

[2] X2RAIL-2, "Technical Note Task 3.2 Subtask 5.1 - High Level Functional Architecture suitable for the introduction of the Virtual Balise Concept." .

[3] H. Lin, L. Ye, and Y. Wang, "UWB, Multi-sensors and wifi-mesh based precision positioning for urban rail traffic," 2010 Ubiquitous Position. Indoor Navig. Locat. Based Serv. UPINLBS 2010, vol. 56500, 2010.

[4] Decawave Ltd., "DW1000 User Manual," pp. 1–21, 2013.

[5] Decawave Ltd., "DWM1001 System Overview and Performance | DecaWave," p. 42, 2017.

[6] A. Goldsmith, Wireless Communications. 2005.

4.7 Authors

Jon Goya received the M.Sc. degree in telecommunications engineering in 2011 and the Ph.D. degree from the Universidad de Navarra in 2016. He is currently a Lecturer with the TECNUN, Universidad de Navarra, and also a researcher with the CEIT. His professional research activity lies in the simulation of on-board positioning system and performance analysis for railway. He has participated in FP7 projects coordinated by CEIT and is now actively participating in actively in Shift2Rail.

jgoya@ceit.es

Gorka de Miguel received the M.Sc. degree in telecommunications engineering from TECNUN (School of Engineering of San Sebastián), University of Navarra, Donostia-San Sebastián, Spain, in 2015. In 2015, he joined the CEIT Research Centre, Donostia-San Sebastián, Spain, where he is currently a Research Assistant and a Ph.D. Student within the Transport and Sustainable Mobility Group. He is also an Assistant Lecturer in Electronic Fabrication Systems with TECNUN. His research interests include the field of positioning and software development. He is now actively participating in H2020 European funded projects in Railway signaling and positioning topics.

gdemiguel@ceit.es

Nerea Fernández received the M.Sc. degree in Telecommunications Engineering from Faculty of Engineering in Bilbao (University of the Basque Country) in 2016. She joined the CEIT Research Centre in San Sebastián in 2017, and she is currently a PhD student within the Transport and Sustainable Mobility group. Her research activity lies in the field of railway signaling specially in zero on-site testing and adaptable communication systems.

nfernandez@ceit.es

Iker Moya received his M.Sc. degree in computer science and intelligent systems in 2019 and his computer architecture degree in 2017 from the Faculty of computer science of San Sebastian (University of the Basque Country). He joined the CEIT Research Centre in San Sebastian in 2017, and he currently is an engineer within the Transport and Sustainable Mobility group. He performs different activities related to embedded systems and programming in the field of railway signalling and he has expertise in machine learning algorithms.

imoya@ceit.es

Dr. **Jaizki Mendizabal** received his M.Sc. and Ph.D. degrees in Electrical Engineering from TECNUN (University of Navarra, San Sebastián, Spain) in 2000 and 2006 respectively. He joined Fraunhofer Institut, Germany) and SANYO Electric Ltd, Japan as RF-IC designer. Nowadays, he is at CEIT, in San Sebastián (Spain) where his research interests include communications and electronic systems. He is lecturing "Communications Electronics" and "Communications via Radio" at TECNUN (University of Navarra).

jmendizabal@ceit.es

5 Performance evaluation issues for on-board positioning systems

Jon Goya, Jaizki Mendizabal, Gorka de Miguel, Paul Zabalegui, Iñigo Adin ; CEIT, San Sebastián, Guipúzcoa, Spain

5.1 Introduction

Currently, most of the projects that are aiming to move towards the most relevant solution for the railway sector are dealing directly with the positioning. These projects can face the positioning problem in many different ways, even propose more than one solution, but there exist always open points related with how this position performance is going to measured. Firstly there is the objective of the positioning system and the produced information, secondly regarding the requirements definition and quantification, and lastly the performance evaluation. This paper aims to target these points in order to reinforce the need of defining a common procedure to be followed by all the railway community.

5.2 Open Points

The main distinction of the use of the position relies on the final purpose of the obtained information. In this case the focus is settled only in those cases where the unreliable position information could cause severe hazards on the operation or even worse, an accident involving human fatalities. Railway sector already ranks this kind of risk defining a safety integrity level, which links the frequency in which the system/information is used, the probability of having misleading information and the consequences. Then the discussion should be moved towards which is the SIL that the on-board positioning systems should have and if it is feasible to reach a SIL4 solution.

This decision already defines procedures related with the implementation of the final system, from all the points of view, electrical compatibility, software design and even a full system life-cycle specification. Based on the SIL defined the processes face more tight and tedious procedures in order to ensure that the SIL is meet.

Even if the selection of a SIL level is complex the trend/needs of the railway sector are leading to have at least a level greater or equal to two. Now once a SIL level is defined, the next point is to move to the definition of the requirements. It should be something easy to tackle but, railway operators, infrastructure managers and developers amongst others have different KPI making difficult to translate and evaluate which is the impact of having a translation for example, between the accuracy and the capacity enhancement that produces. However, at the end the end-user requirements must be translated to measurable KPI related with the position, such as: availability, accuracy, integrity with additional statistical figures.

Once the outcome of the on-board positioning system is obtained and now which are the KPI that have to be measured, the next obstacle to face is the comparison. Mainly, from two points of view: firstly, finding a reliable and faithful reference to compare the results with and secondly, how to compare those results.

For the first issue, one of the most used solution is to use a high-end positioning system which usually uses the same input data as the one that is under test. In this situation, it is difficult to ensure the independence of the data. How can I ensure that I am not having the same issues in both systems shadowing the reality? In other cases, to avoid this issue often maps are used, those can be provided by the end-user or obtained from different public sources. In this case, maps have to be digitalized and convert into a proper format/coordinates to facilitate the comparison labour. Hopefully, in some cases the map provider has worked on this and it is easier to manage the data, but another issue will arise. Data is static, this means only a position is provided, there is no timestamp to be used and thus comparisons are done by taking the closest point to the estimated position. What if the position estimation has a position drift? This way of comparing the data will mask the error obtaining misleading results. The importance of having a fair method for the performance comparison is important (e.g., the use of independent information sources, such as RFID beacons or other technologies as used in STARS project [3].)

And last but not least, can these results be extrapolated to other environments? The answer is complex as the environment is also complex and particular to each of the lines, orography, weather conditions, etc.

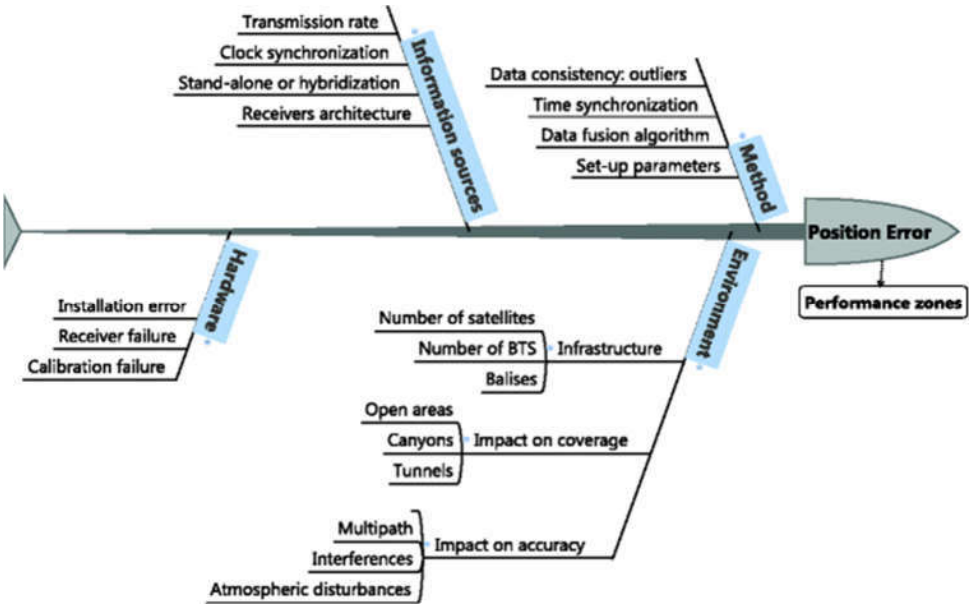


Figure 5-1: Figure 5-1

Then the most important point is, how can we deal with all these open points? The next section proposes one approach that could diminish the impact and provide a common alternative to start facing some of the presented problems while measuring the performance of the on-board positioning systems.

5.3 Proposal/Standards

The proposed methodology aims to work in the side where the requirements are defined and evaluated. Using the same KPI, those which are relevant from the operational point of view. This shared stage is introduced seamlessly on the current system life-cycle, allowing different alternatives, mainly because the focus apart from trying to solve the previously mentioned open

issues is to tune up the model in order to have reliable conditions to simulate the a priori performance and use this information as preliminary analysis and expected system outcome.

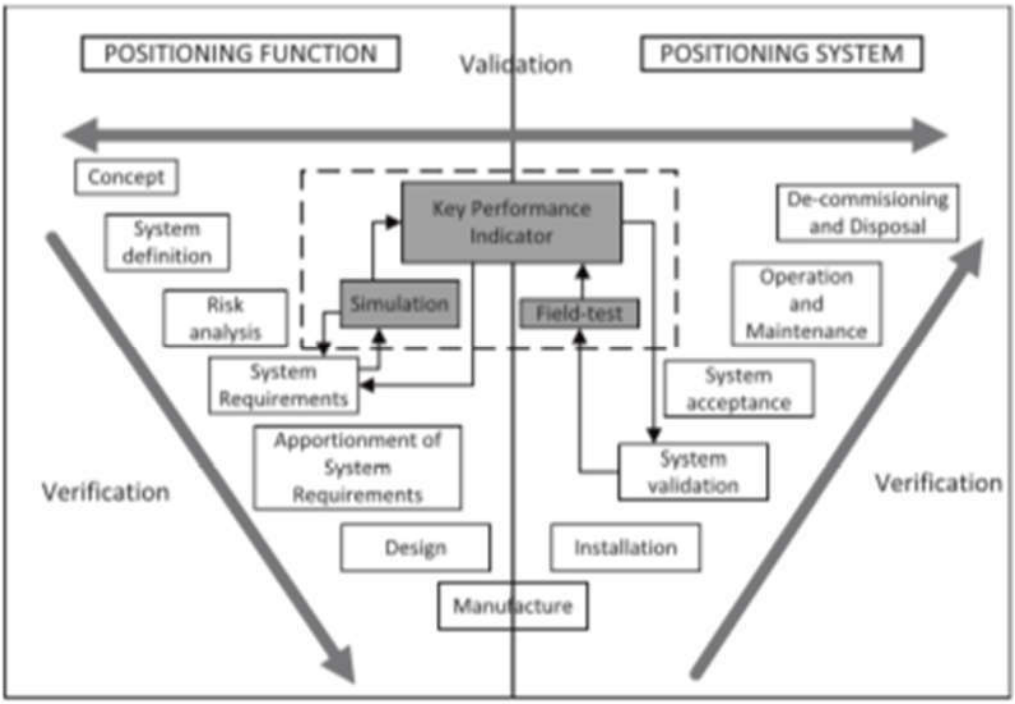


Figure 5-2: Figure 5-2

As mentioned, the use of a simulation stage is important as this will also allow an easy comparison, at least from the positioning performance point of view. Each of the blocks works independently and improving each part is beneficial for the final system performance measurement. The more realistic the models are the easier it is to rely on them in order to carry out additional tests to certify the correct behaviour of the system and latterly certify the system itself.

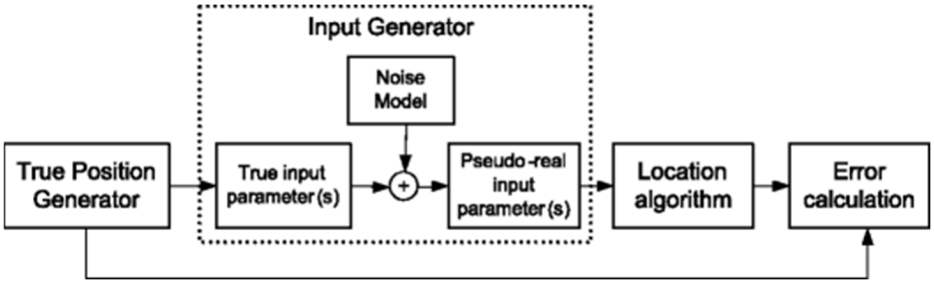


Figure 5-3: Figure 5.3

In the first block the use of the map and railway dynamics model will aim to provide a realistic and independent reference. In the second block, inputs signals are injected depending on the level of realism needed. This could be done by injecting recorded signals, generated signals, or even generated already processed data. Next block is part of the system under test, that depending on the level of abstraction and development phase will interact in a different manner. However, the outcome will be presented in a manner that will allow an easy and fair comparison. Reaching a consensus of the procedure and the models, the system under test can

easy be substituted and what is more, detect where the system fails to perform according to the defined requirements, allowing the reduction of time and cost effort and speeding up the process to move towards a more safe and automated transportation systems.

5.4 Conclusions

The analysis of the performance is an issue that the railway industry and the developers are facing. The need of having a reliable manner to quantify the performance of the on-board positioning systems is a priority. If there is no consensus on this point it will be impossible to move forward and use Global Navigation Satellite Systems (GNSS) in order to get closer to the full autonomous train. The certification process has to cover all the possible issues that the on-board system could see in order to determine the safe behavior of it. The field-tests for this purpose will make the system certification a really expensive process and thus an extensive test list could not be carried out using this method. The 'why' is clear, but the 'how' must be answered. The proposed method mixes both worlds with the aim of reducing the certification cost by simulating most of the processes but also having a real field-test where the operational performance is checked.

5.5 References

[1] Goya et. al. Methodology and Key Performance Indicators (KPIs) for Railway On-Board Positioning Systems. IEEE Transactions on Intelligent Transportation Systems

[2] Goya et al. Advanced Train Location Simulator (ATLAS) for developing, testing and validating on-board railway location systems. European Transport Research Review. 2015

[3] STARS project - Satellite technology for advanced railway signaling. http://www.stars-rail.eu/wp-content/uploads/2017/05/STARS-project-Satellite-technology-for-advanced-railway-signalling.pdf

5.6 Authors

Jon Goya received the M.Sc. degree in telecommunications engineering in 2011 and the Ph.D. degree from the Universidad de Navarra in 2016. He is currently a Lecturer with the TECNUN, Universidad de Navarra, and also a researcher with the CEIT. His professional research activity lies in the simulation of on-board positioning system and performance analysis for railway. He has participated in FP7 projects coordinated by CEIT and is now actively participating in actively in Shift2Rail.

jgoya@ceit.es

Dr. **Jaizki Mendizabal** received his M.Sc. and Ph.D. degrees in Electrical Engineering from TECNUN (University of Navarra, San Sebastián, Spain) in 2000 and 2006 respectively. He joined Fraunhofer Institut, Germany) and SANYO Electric Ltd, Japan as RF-IC designer. Nowadays, he is at CEIT, in San Sebastián (Spain) where his research interests include communications and electronic systems. He is lecturing

"Communications Electronics" and "Communications via Radio" at TECNUN (University of Navarra).

jmendizabal@ceit.es

Gorka de Miguel received the M.Sc. degree in telecommunications engineering from TECNUN (School of Engineering of San Sebastián), University of Navarra, Donostia-San Sebastián, Spain, in 2015. In 2015, he joined the CEIT Research Centre, Donostia-San Sebastián, Spain, where he is currently a Research Assistant and a Ph.D. Student within the Transport and Sustainable Mobility Group. He is also an Assistant Lecturer in Electronic Fabrication Systems with TECNUN. His research interests include the field of positioning and software development. He is now actively participating in H2020 European funded projects in Railway signaling and positioning topics.

gdemiguel@ceit.es

Paul Zabalegui received the M.Sc. degree in Telecommunications Engineering from TECNUN (School of Engineering of San Sebastián), Spain, in 2019. He joined the CEIT Research Centre in San Sebastián in 2019, and he is currently a Researcher Assistant and Ph.D. student within the Transport and Sustainable Mobility group. His research activity lies in the field of positioning and software development. He is now actively participating in H2020 European funded projects in Railway signaling and positioning topics.

pzabalegui@ceit.es

Dr. **Iñigo Adin** received his M.Sc. Degree in Electronics Engineering in 2003 and his Ph.D. in 2007 from the University of Navarra. His research interests include safety-critical designs, with special interest in positioning, communications, electromagnetic compatibility and transport interoperability. He is author, or co-author, of four patents, 2 technical book, an invited chapter and 40 articles in journals and international conferences. He was the coordinator of the FP7 European Project TREND and now coordinates the H2020 AIOSAT for GSA. Moreover he has participated in 4 projects from the Shift2Rail initiative.

iadin@ceit.es

6 Extended method for safety target apportionment for the certification of satellite-based railway localization system

Insaf Sassi, Nourdine Ait Tmazirte, IRT Railenium, Famars, France
Julie Beugin, Université Gustave Eiffel, COSYS, ESTAS, Villeneuve d'Ascq, France
Mohamed Sallak, UTC, Heudiasyc, UMR CNRS 7253, Compiègne, France

6.1 Introduction

Due to the transportation growing demand, rail industry stakeholders have proposed and today adopted the ERTMS standard (European Rail Traffic Management System). The specifications of this system are public thanks to available documents called Subsets, and the European Commission has regulated technical specifications (TSI CCS) that allow interoperability of its Control-Command and Signaling part, the ETCS (European Train Control System), on the European railway network. The expected objective is to facilitate the competition between manufacturers and the management, by several operators, of trains that cross Europe borders. The interoperability constituents that are related to the train localization function examined in this abstract are currently specified by the joint use of odometry equipment and beacons (balises). This choice takes into account the advantage of the odometry, which is to determine a train position continuously over time by providing a traveled distance from a reference point. However, the distance delivered by the odometry includes an error that drifts over time because of its operating principle based on the rotation of the train wheels. The joint use of balises, separated by a few kilometers on the tracks, allows this error to be punctually reset. The balises then serve as new reference points for odometry. As the track is divided into sections, the trackside part of the signaling subsystem in its most advanced development level existing today (the level 2), manages train routes in a safe way by giving authorizations or not to trains to enter into sections thanks to radio messages. For this, this subsystem periodically receives track occupation information and sends back to each train an updated target point to be not crossed.

It becomes quite clear that satellite-positioning systems that deliver an absolute continuous position can, a priori without any other installation than GNSS equipment (Global Navigation Satellite Systems) embedded in trains, constitute an attractive alternative solution because it is less expensive and more precise. There are several integration options: 1) purely and solely replacing odometry equipment and balises with an on-board solution using GNSS; 2) keeping existing odometry equipment and completely removing track balises by realizing the resetting operation with absolute position coming from a GNSS equipment; 3) replacing the existing odometry equipment with an odometry whose quality is improved by the use of GNSS, fewer balises to reset the drift are then necessary. All these options are conceivable and various research projects have addressed them [1]. However, to go beyond prototype solutions and obtain an Authorization for Placing Into Service (APIS) the new signaling subsystem benefiting from the GNSS advantages, it becomes obvious to guide developments according to the European logic already adopted with ERTMS. Any solution that would completely change the way of controlling trains would have much more difficulty to be established in Europe. In this context, work package WP 3 of the X2Rail-2 project addresses option 2) which emanates from

past works showing the interest, in terms of interoperability, of using the concept of virtual balise rather than using an enhanced odometry as proposed in option 3). Nevertheless, developments related to option 1) are not excluded in terms of innovation.

The definition of a Virtual Balise Transmission System (VBTS) integrating the ETCS in an interoperable way, is conducted in WP3 and its operation principles are briefly recalled in this paper. The introduction of new functionalities in this system, in particular those using GNSS, generates new risks and leads to a use that jeopardizes the safety of rail traffic. A new safety analysis is needed and is based on the analysis of these new risks. It will lead to the definition of safety measures to counter the risks to an acceptable level. However, some safety measures are defined within the ETCS and will remain with the use of VBTS to maintain compatibility with what exists. Those that overcome the possible failures of the balises and their transmitted data will be mentioned in this paper. They are specified by safety functions, development and operation constraints (qualitative safety requirements), as well as by high-level quantitative safety targets allocated to safety functions in terms of THR (Tolerable Hazard Rate) [2][3].

Adapting the ETCS safety analysis framework to the VBTS, the NGTC and ERSAT-GGC research projects have been able to underpin some elements to facilitate the certification of VBTS (or in the future, to the interoperability constituent(s) that could characterize it). In particular, the work carried out has shown how to define safety targets with the same apportionment logic of the ETCS core hazard target of 2.10-9 / h to causes of VBTS failures. Thus, a parallel could be made by manufacturers between the safety insurance process they have put in place to verify compliance with ETCS subsystems safety requirements (process prior to obtaining certificates of conformity) and the one to be developed for the new subsystem.

Errors on GNSS signals lead to an erroneous virtual balise detection and consequently to VBTS failure. Failure detection mechanisms have been proposed to mitigate the risks related to signal errors. However, strong model hypotheses on distributions associated to system measurements and environmental effects make these processes suffer from safety flaws. Add to that, the performances of these mechanisms are evaluated without considering the variability of all operational conditions. Thus, a methodology of allocation of imprecise safety targets based on Fault Tree Analysis (FTA) is proposed.

In the present paper, we started with defining the VBTS and its functional architecture integrated within ETCS. Section 3 is devoted to describing the challenges behind using GNSS in railway safety critical applications. A safety analysis based on previous projects is summarized in section 4 and a methodology of imprecise safety targets allocation is proposed in section 5. A conclusion and perspectives are given in section 6.

6.2 Virtual Balise Transmission System

A virtual balise (VB) is an absolute position information registered in a digital database. In order for this database to be used by the on-board ETCS subsystem, the principle of interoperability adopted at this level is as follows: each position information is encapsulated in a telegram which is itself encoded digitally. These digital data of the database can then be exchanged with the on-board ETCS kernel as if the latter received the information from a physical balise. Thus, the impact of introducing satellite positioning in ERTMS is minimized and interoperability can be

guaranteed. To define a VBTS architecture that enhances the ETCS reference architecture with GNSS in view of its conformity assessment performed by notified bodies, especially regarding compliance to safety requirements that are going to be defined, X2Rail-2 has almost formalized and specified interfaces and functional aspects for the VBTS. Figure 6-1 shows a hypothetical architecture adapted from [4] and attempting to synthetize substantial works performed in WP3.

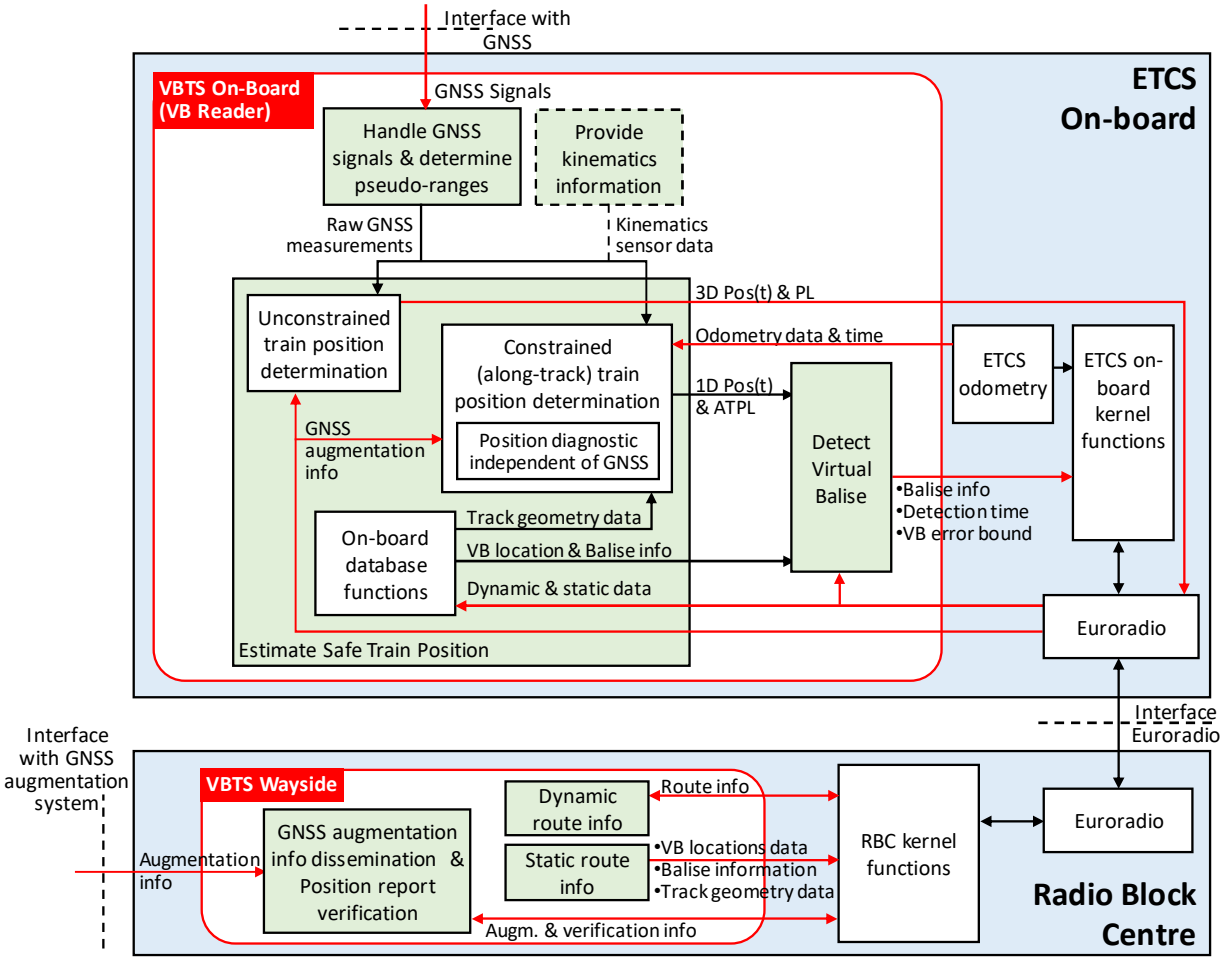


Figure 6-1: Hypothetical VBTS functional architecture (adapted from [4])

The VB detection function is included into the VB Reader, which is an on-board functional block within the ETCS. The VBR is in interface with GNSS signals and with trackside verification mechanisms for reducing risk of wrong VB detection through GNSS augmentation and verification information transiting by the Euro-radio link. The VB detection is based on the Estimate Safe Train Position (ESTP) function using GNSS and odometry data, these ones being potentially coupled with kinematics sensor data (when the GNSS signals are blocked). The ESTP provides two types of output: 1) 3D position and 1D position because of the use of track geometry data (map-matching), 2) estimated safety margins in meters for the 3D case used when the train starts a mission (Protection Level, PL) and for 1D case (Along the Track Level Protection, ATPL).

6.3 Challenges of using GNSS in railway safety critical applications

GNSS is already widely used in railways, mainly in non-safety relevant applications like passenger information or asset management. For these types of applications neither precision nor reliability constitute an imperative. When dealing with safety critical applications such as Train Control and Signaling or Protection and Emergency Management Systems, the difficulty of ensuring that the position error is correctly bounded makes difficult the emergence of system based on GNSS as main sensor. For a while, the aviation sector was considered as a reference for its capability to integrate GNSS in a fail-safe positioning system. For ensuring safety, the concept of Receiver Autonomous Integrity Monitoring (RAIM) was developed to guarantee a bounded position error. The main idea is to compute protection levels (Horizontal & Vertical HPL & VPL) that always confine the unknown true errors (Horizontal & Vertical Position Errors HPE & VPE) and to provide a position estimation only when the protection levels are lower than the predefined alarm limits (AL). In case a PL is greater than its corresponding AL, RAIM should be able to warn the system and make the localization function unavailable within a predefined time limit called Time To Alarm (TTA) as shown in Figure 6-2, known as Stanford diagram. The situation considered as safety critical consists in having a true position error PE greater than AL and not bounded by PL (PL<AL<PE).

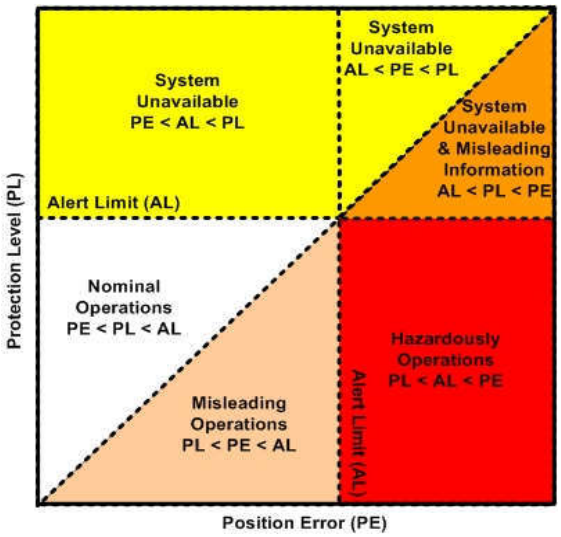


Figure 6-2: Stanford Diagram

Recent European projects NGTC, STARS and ERSAT GGC have emphasized the impossibility of using those algorithms, as such, for contextual reasons. Indeed, unlike in aviation that makes a strong assumption of single satellite fault at a time, in land applications including railway, signals used to position, can face particularly harsh environments (urban canyon, forests, etc.), resulting in one or multiple local faults leading to:

- Multipath: received reflected replica(s) signal(s) in addition to the direct signal
- NLOS (Non-Line of Sight): received reflected replica(s) without receiving direct signal
- Interferences (intentional or non-intentional): producing additional unbounded measurement noise.

All these phenomena could conduct to either the unavailability of positioning function, or worst, to the feared event "unbounded erroneous position" as illustrates Figure 6-3.

In addition, the concepts of HPE/HPL and VPE/VPL can be refined to better fit rail requirements. The vertical component is no more necessary, and the horizontal component should be decomposed into two: Along Track & Cross Track Protection Levels (ATPL/CTPL) and Position Errors (ATPE/CTPE). CTPL will be an important indicator for track discrimination where ATPL will be of main importance for safety. To reduce the frequency of integrity risk occurrence (ATPE>ATAL>ATPL, ATAL: Along Track Alarm Limit), called hazard, two strategies may be considered at measurements (i.e. pseudo-ranges) integration filter level:

- GNSS measurements weighting model;
- Fault detection and exclusion.

However, the lack of railway data representative of the different environments that a train can cross does not allow to validate these improvements. For these reasons, a paradigm shift is required in order to achieve the goal of safety requirement verification related to the certification of a GNSS-based localization function.

We propose to relax the constraint around the GNSS by considering it not as a sensor with a unique operating point, but rather as a sensor functioning around an operating range covering the whole possibilities. Concretely, this range will be represented by an interval both in the top-down analysis for the allocation phase (THR apportionment) and in the bottom-up analysis for validation phase. Both analyses will use the common Fault Tree method that provides an ideal framework for deductive analyses with notations to represent causal relationships between a system feared event and its associated failure events. The following section introduces this approach and focuses on the interval propagation.

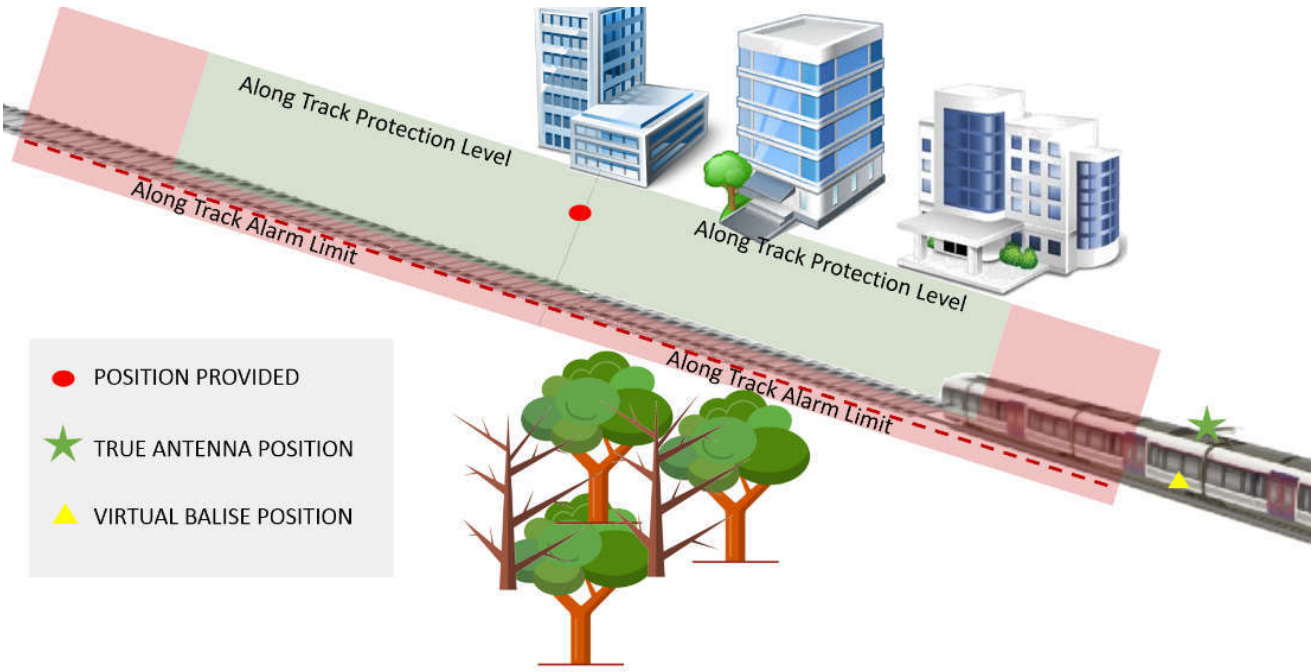


Figure 6-3: Illustration of Integrity Risk

6.4 Safety targets allocated to the VBTS function failures using Fault Tree

The localization of the virtual balise is used to reset to the odometry errors that impact the train position. Following the same approach adopted in the safety analysis of ETCS, the allocation of safety targets to the VBTS using GNSS in ERTMS consists in apportioning the ETCS Core Hazard THR to the grouping of constituents described in Subset-088 part 3 and to the VBTS functions. The THR of the ETCS Core Hazard is apportioned between the trusted and untrusted parts of the ETCS on-board and trackside functions. The THR allocated to the VBTS failure is related to the untrusted part and is 0.66□10-9 per hour [4]. The main hazards, that have been identified as causes of virtual balise transmission subsystem failure, are analogous to the information hazards of balise transmission subsystem defined in Subset-088. Thus, the hazards applicable to virtual balise in certain operational scenario are defined as follows:

- TRANS-VBALISE-1 (corruption hazard): Incorrect Virtual Balise message that is received by the on-board kernel functions as consistent
- TRANS-VBALISE-2 (deletion hazard): VB not detected by the on-board functions
- TRANS-VBALISE-3 (insertion hazard): Inserted VB message received by the on-board kernel functions as consistent

One of the causes, that leads to the occurrence of TRANS-VBALISE-3 hazard, is the erroneous localization of virtual balise because of an unbounded along track error. This error is due to local effects on GNSS signals; Multipath, NLOS, Pseudo-Range-NOISE which contribute to the occurrence of the feared event: unbounded erroneous position.

At this level, we propose to consider THR no longer as crisp values but as intervals (see Figure 6-4) to consider the variability of the operational conditions and the uncertainty of the models used for failure detection and exclusion and the environment effect. This uncertainty is depicted through interval of THRs as epistemic uncertainty to avoid having strong requirements for the developed (or in development) safety mechanisms.

Section 6-5 gives an overview of the allocation method of imprecise safety targets.

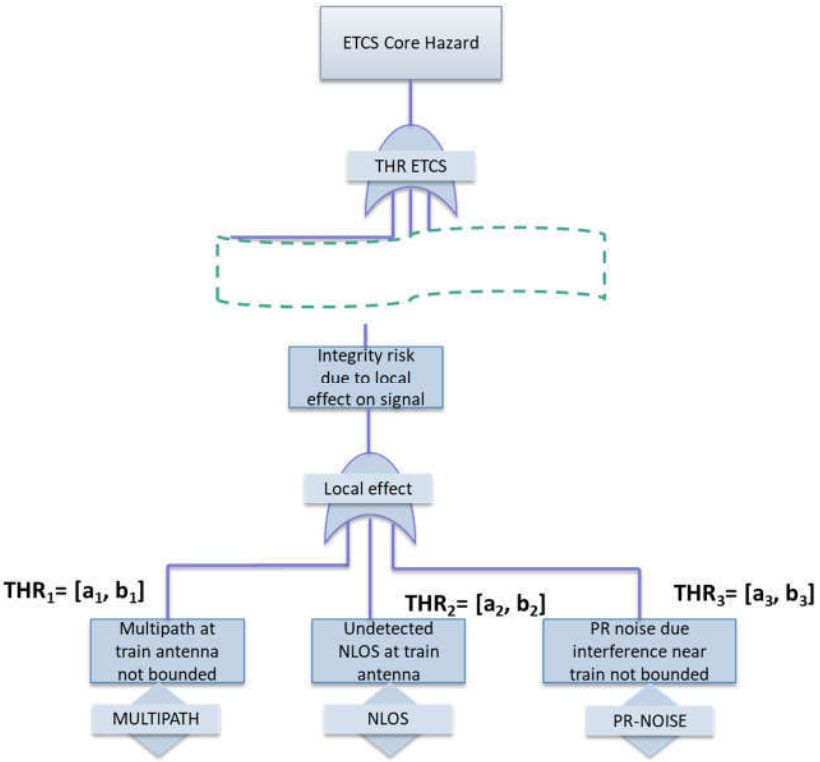


Figure 6-4: Fault tree part for GNSS safety targets apportionment

6.5 Allocation method of imprecise safety targets

The THR allocation process can be described, in general, as the process of assigning THR to basic events of the fault tree within a top event to attain the specified safety target. The allocation process is performed from the top event of the fault tree, at different intermediate gates, until reaching basic events.

On the other hand, the safety targets will be considered as intervals instead of crisp value. Indeed, in this work, the considered uncertainties related to the occurrence of events, will be divided into two types: aleatory uncertainty and epistemic uncertainty. Aleatory uncertainty is due to the natural variability of random phenomena (failure of a component, reparation of component, etc.). Aleatory uncertainty is usually represented by probability distributions (exponential law, uniform law, normal law, etc.) or frequentist and precise probabilities. Epistemic uncertainty (imprecision) expresses the lack of knowledge about the true values of the frequentist probabilities or parameters (e.g. failure rate, repair rate, etc.) of probability models. It reflects the subjective feature of the analyst. The distinction is important because epistemic uncertainties can be reduced by acquiring knowledge on the studied system, whereas aleatory uncertainties cannot. Furthermore, many recent works have proven that uncertainties in risk assessments are mainly epistemic [5].

The fault tree analysis permits the allocation of the safety targets in terms of THR. The top-down uncertainty propagation is performed by determining an optimal interval enclosure for intermediate and basic events using optimisation and arithmetic intervals. Thus, the obtained failure rates for basic events are defined in interval enclosures.

More specifically, using interval arithmetic, the intervals of THR are obtained depending on the type of the gate. We recall that interval arithmetic is an arithmetic over intervals. It has been proposed by Ramon E. Moore [6] in the late sixties in order to model uncertainty, and to tackle rounding errors of numerical computations. For practical applications, interval arithmetic operations can be simplified as shown in Figure 6-5.

$$
\begin{aligned}
&(a,b)+(c,d)=(a+c,b+d)\\
&(a,b)-(c,d)=(a-d,b-c)\\
&(a,b)\times(c,d)=\left(\min(a\times c,a\times d,b\times c,b\times d),\max(a\times c,a\times d,b\times c,b\times d)\right)\\
&(a,b)\div(c,d)=\left(\min(a\div c,a\div d,b\div c,b\div d),\max(a\div c,a\div d,b\div c,b\div d)\right)
\end{aligned}
$$

Figure 6-5: Interval arithmetic operations

However, whilst interval arithmetic can be applied in our work to ensure bounds on the THR of basic events, the limitations of interval arithmetic can lead to bounds that are not always tight and hence not particularly useful. As a result, some algorithms are specifically designed with interval arithmetic in mind to find high quality bounds on the obtained solution; the Krawczyk algorithm will be used in this case.

For an "OR" gate, determining THR intervals consists in solving a linear system of equations. The equivalent THR of an OR gate is calculated as:

$$THR_{eq} = \sum_{j=1}^{n} THR_j$$

Where the THRj corresponds to every basic event of the OR gate.

The objective of the use of interval arithmetic propagation is to compute the intervals of THRj while the interval of THReq is determined from the top-down analysis.

For the allocation of imprecise THR in case of AND gate, the propagation problem consists of solving a system of non-linear equations, such that the equivalent THR is defined as follows.

$$THR_{max} = \prod_{j=1}^{n} THR_j . SDT_j \,.\, \sum_{j=1}^{n} \frac{1}{SDT_j}$$

Where the SDTj is defined as the safe down time which estimated as the time for failure detection and negation.

After obtaining the THRs intervals of basic events in the allocation process of the top-down analysis, it is possible to perform an interval propagation in a bottom-up analysis. This process allows checking the obtained intervals from the allocation process. It also enables to verify if the safety target initially defined for the top event of the fault tree is contained within the propagated interval. This process is considered as uncertainty analysis and can be obtained using interval analysis.

6.6 Conclusion

Previous projects have been working on preparing the certification process of the train positioning system using GNSS as primary sensor in compliance with the ETCS safety requirements. The challenges that have been encountered are related to the determination of the safety requirements which are judged by experts to be difficult to achieve in all the operational contexts. Add to that, lack of data makes it hard to represent all the possible scenarios to rigorously validate the safety targets. We highlighted the necessity of considering the GNSS as a sensor with a versatile operating range highly linked to environment changes. We translated this operating range into an interval of THR that has to be propagated in the Fault Tree (FT) to define less constraining safety requirements in harsh environments. The present methodology will be proposed in WP3 of X2RAIL-2 to integrate this part of the GNSS safety analysis.

6.7 References

[1] Marais J., Beugin J., Berbineau M. (2017). A survey of GNSS-based Research and Developments for the European railway signaling. IEEE-Transactions on Intelligent Transportation Systems, vol. 18 (10): pp 2602-2618.

[2] UNISIG Subset 091 (2016). Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, Union of Signalling Industry, issue 3.6.0, 2016-05-12.

[3] UNISIG Subset 088 (2016). ETCS Application Levels 1 & 2 - Safety Analysis - Part 3 - THR Apportionment, Union of Signalling Industry, issue 3.6.0, 2016-06-20.

[4] Wullems, C., F. Sperandio, M. Basso, S. Sturaro, and S. Sabina. (2018). A Preliminary Apportionment of Safety Targets for Virtual Balise Detection Using GNSS in Future Evolutions of ERTMS. Intelligent Transportation Systems Telecommunications conference (ITST), 15-17 Oct., Lisboa, Portugal.

[5] Aven, T., Baraldi, P., Flage, R., & Zio, E. (2013). Uncertainty in risk assessment: the representation and treatment of uncertainties by probabilistic and non-probabilistic methods. John Wiley & Sons.

[6] Moore, R. E. (1966). Interval Analysis. Englewood Cliff, New Jersey, USA: Prentice-Hall. ISBN 0- 13-476853-1.

[7] Min, K., Qi, L., & Zuhe, S. (1999). On the componentwise Krawczyk-Moore iteration. Reliable computing, 5(4), 359-370.

6.8 Authors

Insaf Sassi has received the engineering degree from the National School of Computer Sciences (ENSI), Tunisia, in 2014; the master's degree in control systems from Ecole Centrale Lille, France, in 2014; and the PhD degree in control systems from University of Grenoble Alpes in 2017. She joined Railenium as post-doctoral fellow in 2018 to work on RAMS analysis. Her research deals with dependability and safety analysis. She is working on safety analysis of onboard train

integrity and GNSS-based positioning system in train control applications.

insaf.sassi@railenium.eu

Nourdine Aït Tmazirte works at French Institute of Technology Railenium since 2018. He got his engineering and M.Sc. degree in automation engineering from Ecole Centrale de Lille, France, both in 2010. His research interests include multi-sensor fault tolerant fusion for localization and integrity assessment.

AIT.TMAZIRTE@railenium.eu

Julie Beugin received the engineering degree from National School of Engineering for Computer Science, Automation, Mechanics and Electronics (ENSIAME), in 2002; the master's degree in automation engineering from University of Valenciennes, France, in 2002; and the Ph.D. degree in automation engineering in 2006. Since 2007, she has been with IFSTTAR, the French institute of science and technology for transport, development and networks, as a researcher. Her research interest deals with dependability and safety evaluation of complex guided transportation systems. Part of her activities addresses RAMS demonstration issues of GNSS-based solutions embedded in train control applications. She participated to the GaLoROI, STARS, ERSAT-GGC European projects. She has secondment agreements with Railenium to participate to projects in her research fields and with Certifer to realize ISA missions.

julie.beugin@univ-eiffel.fr

Mohamed Sallak received the Ph.D. degree from the National Polytechnic Institute of Lorraine, Nancy, France, in 2007. He is currently an Associate Professor / HDR with the Department of Information Processing Engineering, Compiegne University of Technology, Compiegne, France. His current research interests concern dependability assessment of complex systems (transportation systems) under uncertainties.

7 Onboard Train Integrity: Safety Analysis

Insaf Sassi, IRT Railenium, Famars, France
El-Miloudi El-Koursi, Université Lille Nord-Europe, Université Gustave Eiffel, COSYS, ESTAS, Villeneuve d'Ascq, France
Joffrey Clarhaut, Dominique Renaux, Université Polytechnique Hauts-de-France (UPHF), Valenciennes, France

7.1 Introduction

Work package 4 of the X2Rail-2 project aims to design an Onboard Train Integrity (OTI) monitoring system that must be compliant to a set of safety requirements. The OTI main goal is to autonomously and safely verify the completeness of the train in operation. It must respect safety requirements defined according to the European Railways standard CENELEC EN50126 [3] [4] and the Common Safety Method [1]. It must implement requirements that permit the achievement of the Safety Integrity Level (SIL) 4.

The Removal of trackside train detection systems shifts more responsibility for the safe operation of the railway from the infrastructure managers to the railway undertakings. Onboard equipment must then replace the trackside systems and guarantee that the train remain safely operational and complete throughout the journey. For this purpose, a framework of safety analysis has been developed in order to satisfy the recommendations of standard EN50126. One activity of this framework consists in formally verifying the functional specifications. Formal methods allow for exhaustively checking the system behavior. As a consequence, the obtained outputs can be trusted provided that the models, used for verification, reflect the system behavior in a trustworthy way. Another activity consists in performing one of the high recommended measure for SIL 4 systems which is capturing safety requirements and maintain their traceability. Safety requirements shall be traced to architecture elements that are responsible for the implementation of the measures preventing safety critical failures. Add to that, causal analysis is used to define the safety integrity level, i.e. safety requirements, of the safety related functions. This analysis is performed using Fault Tree Analysis (FTA) to apportion the SIL requirements based on the quantified safety targets in terms of Tolerable Hazard rate (THR). This technique is highly recommended by the standard EN50126. As a support for this activity, the formal models help to investigate the system behavior and discover hazardous situations.

This paper provides an overview of the aforementioned framework by focusing on the traceability activities and SIL apportionment process which is given with precising the context of the analysis. For confidentiality reasons, the results of FTA are not detailed in the present paper.

7.2 Onboard Train integrity

The onboard train integrity (OTI) system monitors the status of the train tail in order to verify that last wagon advances regularly with the head of the train. It evaluates the train integrity as

confirmed, lost or unknown and sends it to the European Traffic Control System (ETCS) onboard according to CR940 [2]. For the evaluation of the integrity, the OTI system is composed of the following modules as depicted in Figure 7-1:

- OTI Slave (OTI-S): It is the tail OTI device. It determines the status of the train tail and communicates it to the OTI Master.
- OTI Master (OTI-M): It is the head OTI device. It acquires the information of train integrity status from the OTI-S and sends it to the ETCS onboard.
- OTI Intermediate (OTI-I): It is the OTI-S non tail which is an intermediate device installed along the vehicle. An OTI slave at train tail changes its position while adding other wagons after coupling procedure. In this case, it does not contribute in the train integrity status evaluation. After the intentional splitting procedure, an intermediate slave identifies its position as slave in tail and contributes to the train integrity evaluation.
- On-board Communication Network (OCN): It is the communication channel for information exchanging between OTI monitoring system devices. It can be wired or wireless and is bidirectional between the OTI modules.

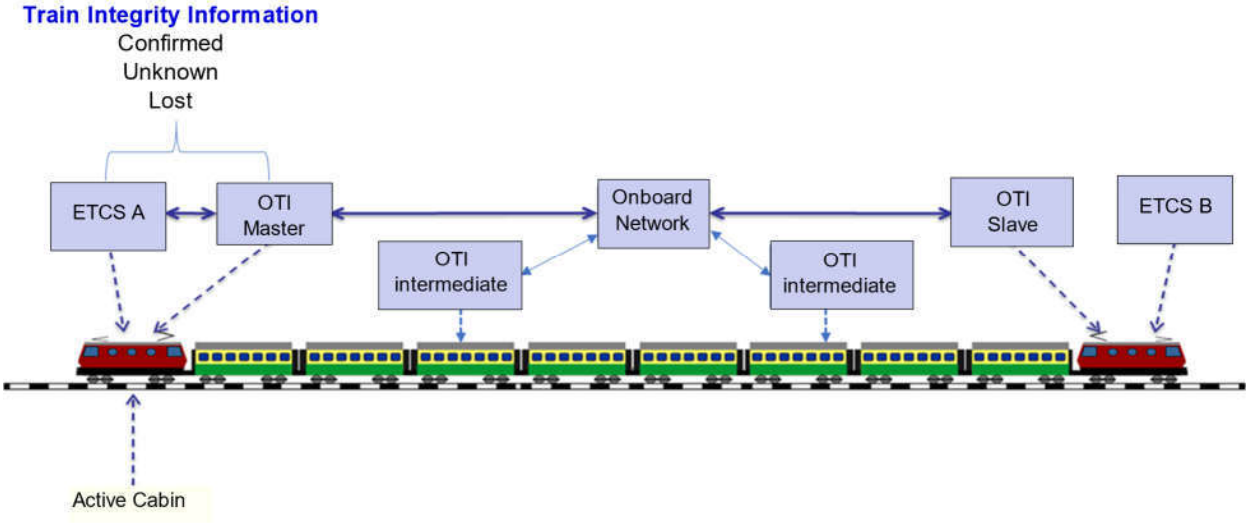


Figure 7-1: Onboard Train Integrity System [7]

The way the integrity is evaluated depends on the technology used for the communication between the OTI modules. Product class 1 refers to train with wired communication network where the integrity criteria is evaluated based on the communication liveliness between the OTI-S in tail and the OTI-M. Product class 2 refers to trains with wireless communication technology. In this case, the integrity is determined based on comparing kinematic data of train tail and front cabin (e.g. position, speed, acceleration).

The OTI modules must perform basic functionalities in order to evaluate the integrity. The OTI slave and master functional modules shall safely carry out the mastership, inauguration and monitoring phases. A preliminary hazard analysis (PHA) is carried out on the system of Figure 7-1. It provides the safety related functions whose failures lead to safety issue, such that FM1-6 correspond to master safety related functions, FS1-5 are associated to the slave functions:

- FM1: Input acquisition to determine the OTI module role (MASTER)
- FM2: Pairing procedure Master-Slave
- FM3: Reception of Vitality Message in case of wired communication
- FM4: Reception of kinematic data
- FM5: Check of train tail movement in case of wireless communication
- FM6: Send of Train Integrity information to ERTMS/ETCS On-board
- FS1: Input acquisition to determine the OTI module role (SLAVE)
- FS2: OTI module localization to define slave position in the train (TAIL/NON TAIL)
- FS3: Pairing procedure Master-Slave
- FS4: Send of Vitality Message in case of wired communication
- FS5: Acquisition and send of kinematic information in case wireless communication

7.3 Preliminary Safety Analysis

7.3.1 Safety requirements traceability

Performing safety requirements traceability enables to achieve the following objectives:

- Identifying the hazards that do not have mitigating requirements
- Capturing safety requirements and design traceability
- Identifying the mitigations without passed test cases
- Providing evidence that all safety requirements are implemented and verified
- Determining the impact of changing a requirement

The Traceability Information Model (TIM), detailed in [5], is useful for information management in a safety critical project. It is recommended to create a TIM early in a project to ensure consistency throughout the system life-cycle and to specify traceability links manually for critical requirements, i.e. safety related requirements. The model of Figure 7-2 gives an overview of the generated data, resulted from the product life-cycle and the performed safety analysis, and the links that represent the relationship between them. The data are represented by a rectangle in Figure 7-2. An identifier ID and a description are the main two properties of every artifact. The traces between the artifacts are visualized as lines.

The functional safety requirements are classified as:

- Safety relevant functional requirements that describe what the system shall do
- Safety integrity requirements that assign SIL according to the safety targets from the Tolerable Hazard Rate (THR)

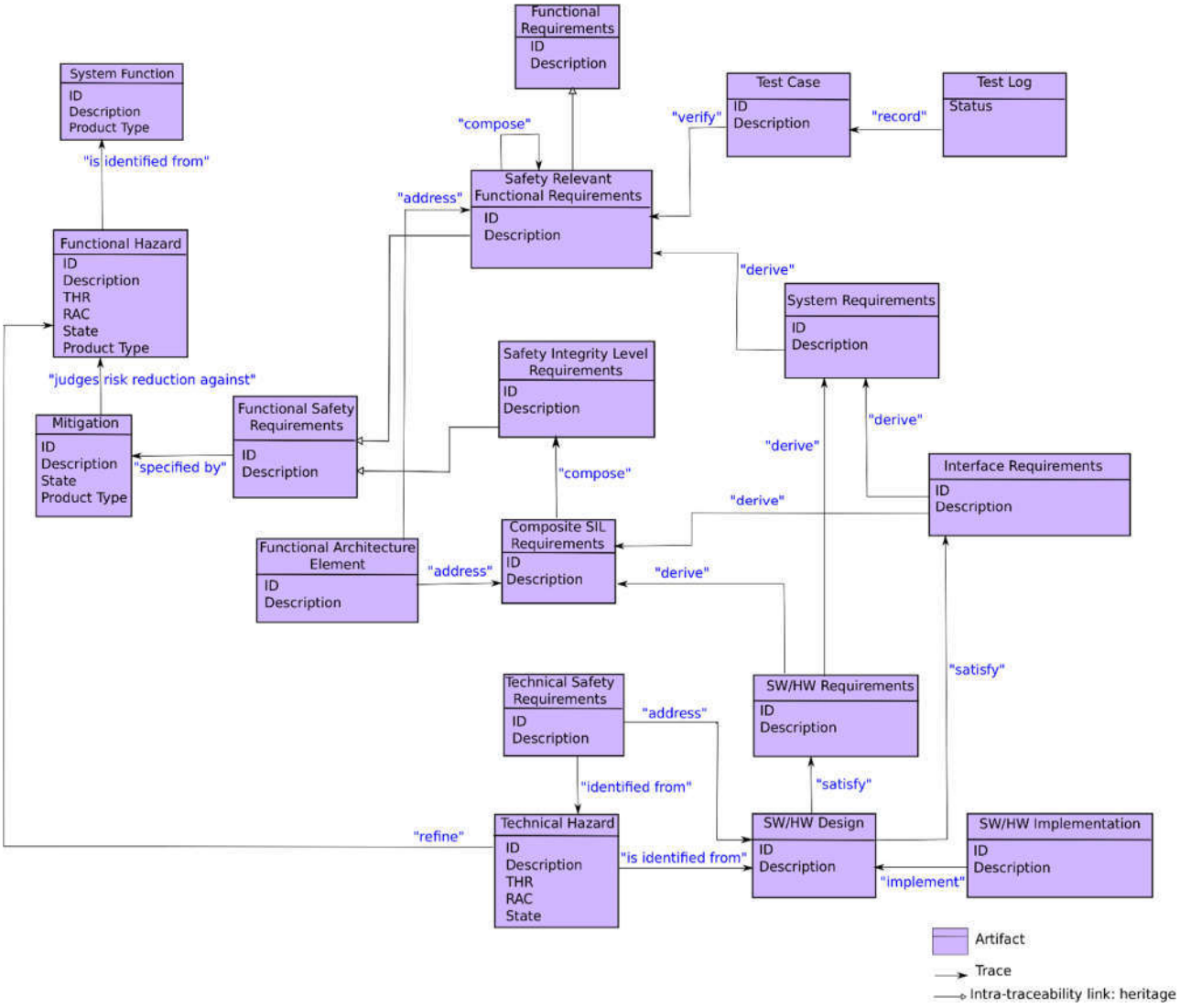


Figure 7-2: Traceability Information Model [5]

The SIL requirements are considered as functional safety requirements that associate qualitative measures to a range of tolerable functional failure rate (TFFR). A causal analysis is performed at this level using Fault Tree Analysis (FTA) to apportion the SIL requirements based on the quantified targets in terms of THR as recommended by the standard EN50126 and detailed in [6]. It consists in assigning TFFR and SIL for functions by analysing the functional architecture and allocating them to subsystems. The process of determining the SILs is given in the sequel.

This Model has been implemented using Excel during the project in order to identify the gaps between the hazards, their mitigations and the safety requirements that are defined and implemented at the technical level. The TIM covers the data that should be taken into consideration and maintains the traceability links in order to show the achievement of the implementation of safety requirements. It is noted that thanks to this model, improvements have been proposed in order to cover the gaps from life cycle level to another.

7.3.2 Assumptions for Fault Tree Analysis

The safety analysis is based on the functional hazard analysis presented in the deliverable D4.1 [7] and the formal model described in D4.6 [8]. The SIL apportionment process is developed to

determine the SIL requirements (see Figure 7-3). The apportionment process, shown in Figure 7-3 can be performed by different tools, e.g. Fault tree (FT), that allow a logic combination. The fault tree analysis (FTA) is used to represent the combination of function and their associated sub-functions whose failures lead to hazardous situation. It also expresses how failures, operation errors and external factors lead to the occurrence of the hazard of the top event. Three FTs are proposed to analyze the different product classes (1A, 1B and 2A-2B). The assignment of THR (Tolerable hazard rates) and TFFR (Tolerable Functional Failure Rate) of the top-down analysis will be consolidated with a demonstration step and safety assessment of OTI prototypes that will be provided in the next phase in X2RAIL-4 project.

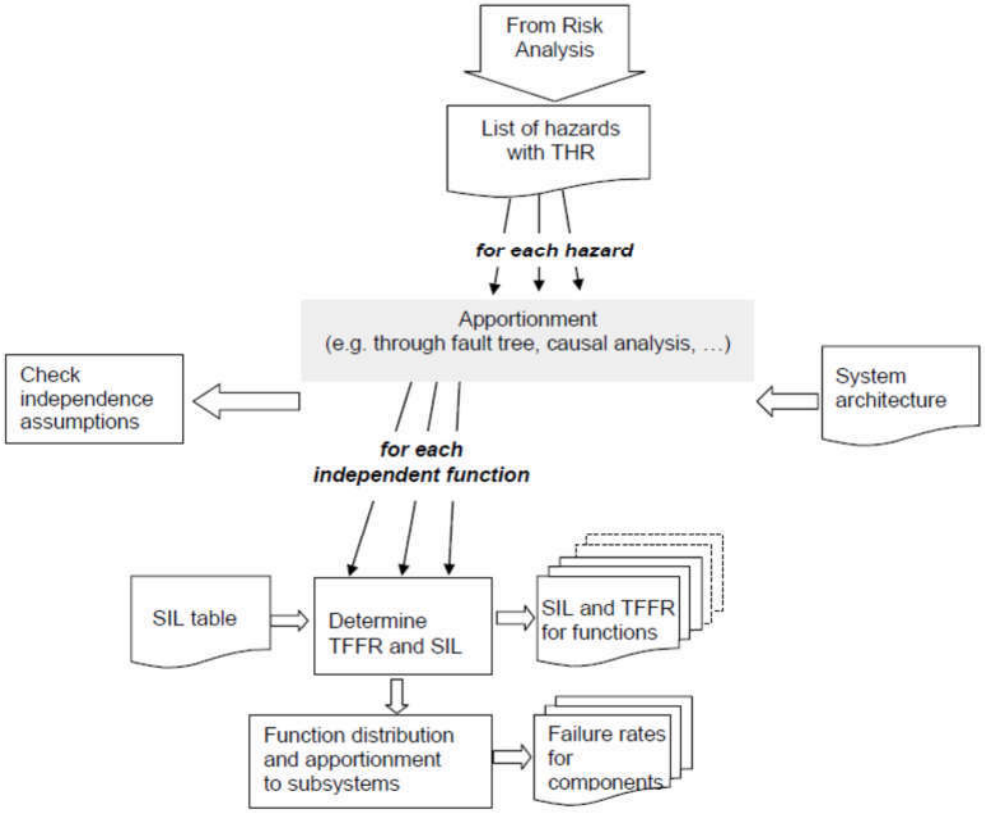


Figure 7-3: Apportionment of safety requirements [4]

The top-event that must be taken into consideration is associated to the defined hazard OTI_HZ_AB1: ETCS receives inappropriate Train Integrity confirmation: confirmed instead of unknown or lost (see Table 7-1). In fact, incorrect train integrity confirmation means that the ETCS on-board receives a corrupted, inserted, reapeated, resequenced or earlier confirmed train integrity instead of lost or unkown. An earlier received confirmation does not represent the actual state of the train integrity. A set of hazards (see Table 7-1) has been identified from the OTI functions in every phase of the train integrity evaluation (Mastership, identification, pairing, monitoring). The obtained FT of every product class models the combination of these hazards and their causes that contribute to the occurrence of the top event. Table 7-1 presents the hazards applicable to product class 1A and 1B. Mitigations have been investigated and identified in order to reduce the risk related to the aforementioned hazards. A mitigation list is introduced in deliverable D4.1.

For product classes 1A and 1B, the train integrity is evaluated based on the liveliness message exchanged between the OTI-M and the OTI-S in tail. The main difference between products 1A and 1B is that there is no ETCS at train tail as depicted in Figure 7-4. Thus, hazard OTI_HZ_B1 (see Table 7-1) is identified for product class 1B as the OTI-S can involuntarily become a Master and insert messages of integrity in the information flow between the OTI-M and the ETCS onboard.

Table 7-1: List of hazards

Hazard ID	Description	Safety related function	Product Class
OTI_HZ_AB1	The ERTMS/ETCS On-board equipment receives inappropriate Train Integrity Confirmation (incorrect or earlier information)	FM6	Products 1A-1B
OTI_HZ_AB2	OTI Slave is not installed on the last car/wagon but it localizes itself on the last wagon/car or the OTI Master receives an incorrect identification message from OTI Slave ("TAIL" instead of "Non TAIL")	FS2, FI1	Products 1A-1B
OTI_HZ_AB3	OTI Master pairs with NON TAIL OTI Slave module.	FM2	Products 1A-1B
OTI_HZ_AB4	The OTI Master receives an inappropriate change of cabin status (from "active" to "not active") and becomes Slave.	FM1	Products 1A-1B
OTI_HZ_AB5	OTI Slave sends incorrect liveliness messages	FS4	Products 1A-1B
OTI_HZ_AB6	The OTI Master receives inappropriate Train Integrity information (incorrect information, earlier or later, masquerade, etc.).	FM3	Products 1A-1B
OTI_HZ_B1	The OTI Slave erroneously receives the information of "Cab status = Cab active" and becomes Master	FS1	Product 1B

In this safety analysis, external events are also considered because the safety of the OTI depends on a set of inputs which are defined as following:

- Incorrect installation of OTI modules namely the slaves: The installation process must be considered as a part of the design. It must then be managed in compliant with SIL 4 measures.

- Incorrect "Cabin Status" information (active or non active, leading or non leading) from Rolling Stock to manage the role assignment (i.e. master/slave): Cab status, as input to the train integrity monitoring system, shall be compliant to its assigned SIL.

- Incorrect OTI-S tail/non tail signal from tail sensor to allow OTI Slave evaluating its positions (i.e. at train tail or in intermediate cabins/wagons of the train): The Tail/non

tail, as input to the train integrity monitoring system, shall be compliant to its assigned SIL.

These external events do not belong to OTI System. However, they are factors that must be taken into consideration in the safety analysis with measures to reduce their impact.

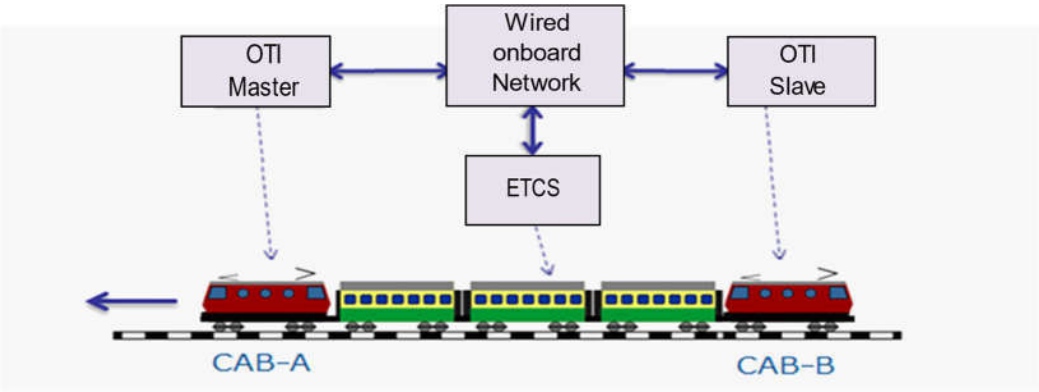


Figure 7-4: OTI Product class 1B architecture [7]

7.3.3 SIL apportionment and allocation process

This section represents a generic methodology for SIL allocation described in [6]. This methodology is developed based on standard EN50126 and Common Safety Method (CSM) [1]. The methodology, presented in the sequel, requires data from PHA to identify the functions that must be considered in the safety analysis. The data needed to run the methodology are the following:

- The list of hazardous situations for the system under consideration
- The list of the safety related functions whose failures lead to the occurrence of hazards

The functional failures combinations and scenarios leading to each hazard

Figure 7-5 represents an overview of the SIL allocation process. A Tolerable Hazard Rate (THR) is defined as a quantitative objective to be apportioned and reported in the top event of the Fault Tree. The THR values are defined after analysing the hazardous situations, and according to regulation as the CSM-DT. Allocating SIL to the safety related functions implies that these functions must be implemented according to this SIL requirements. After determining the SIL that is allocated to a function, the software or hardware implementation must fulfil this requirement. A supplier shall provide the attaignement of the obtained THR/TFFR by specifying the mission profile. The mission profile, as defined in the standard EN 50126, must be taken into consideration in order to determine the operational parameters and the contextual requirements such as system lifetime, maintenance strategy, safe down time of a failed OTI, frequency of transmitted message, etc. The mission profile enables the assessment the exposure of passenger/user to a defined hazard while considering parameters such as time, loading speed, distance, stops, tunnels. To define a mission profile, the operational parameters and the reference infrastructure must be taken into consideration. The reference infrastructure parameters describe the charecteristics of the railway network, e.g, length of the line, number

of tunnels, number of trains on the line, etc. The operational parameters can be maximum expected loss of train integrity, mean down time of the train integrity system.

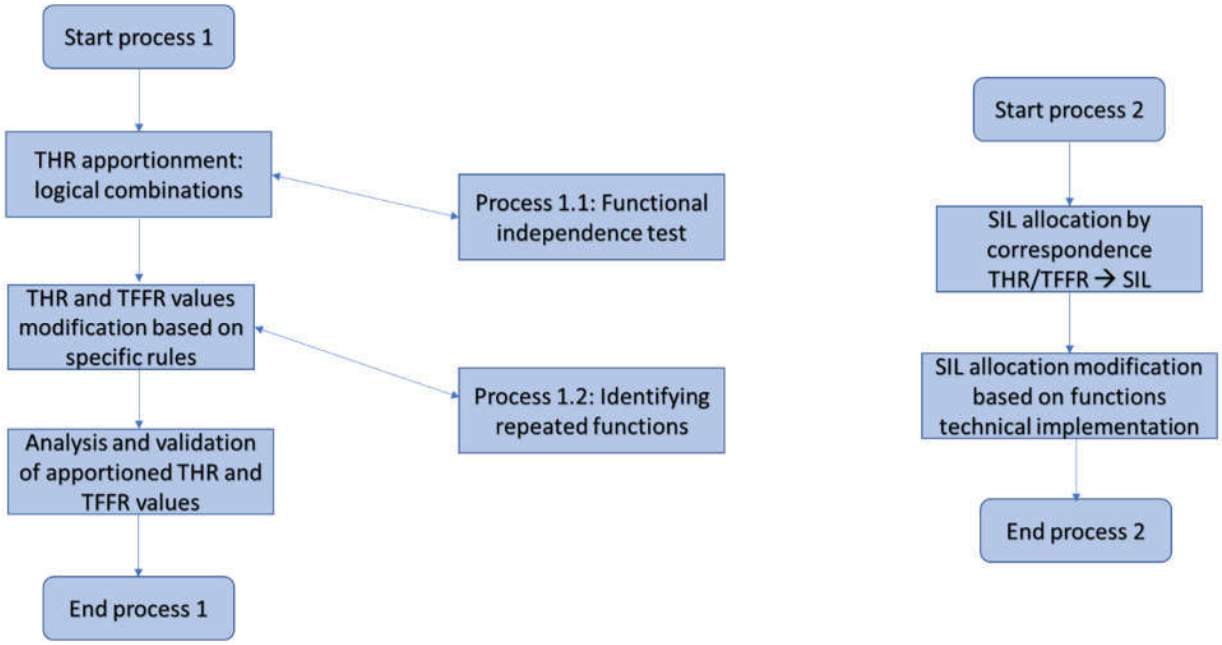


Figure 7-5: SIL allocation process

7.4 Conclusion

This work presents a framework of safety analysis that includes a list of highly recommended techniques and measures in standard EN50126. It represents the methodology that have been applied for the onboard train integrity system that need to comply with the highest SIL like the trackside train detection system. This methodology consists of many activities such as traceability of safety requirements, SIL apportionment and allocation and it prepares the process of authorization and certification. Results of FTA are confidential and described in D4.6[8]

7.5 References

[1] Common safety method for risk evaluation and assessment and repealing regulation (ec) 352/2009, document regulation (eu) 402/2013, 30th commission implementing regulation (April 2013)

[2] CR940 – Modifications related to Train Integrity functionalities, 14.06.2017.

[3] EN50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process

[4] EN50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 2: Systems Approach to Safety

[5] Insaf Sassi, El-Miloudi El-Koursi (2019), On-Board Train Integrity: safety requirements analysis, In 29th European Safety and Reliability Conference (Esrel 2019), September 2019.

[6] Ouedraogo, K. A., J. Beugin, E.-M. El-Koursi, J. Clarhaut, D. Renaux, and F. Lisiecki (2018). Toward an application guide for safety integrity level allocation in railway systems. Risk Analysis

[7] X2R2 D4.1 Train Integrity Concept and Functional Requirements Specifications.

[8] X2R2 D4.6 Results of preliminary feasibility studies and preliminary laboratory tests for candidate technologies selection and for adaptation of existing solutions

7.6 Authors

Insaf Sassi has received the engineering degree from the National School of Computer Sciences (ENSI), Tunisia, in 2014; the master's degree in control systems from Ecole Centrale Lille, France, in 2014; and the Ph.D. degree in control systems from University of Grenoble Alpes in 2017. She joined Railenium as post-doctoral fellow in 2018 to work on RAMS analysis. Her research deals with dependability and safety analysis. She is working on safety analysis of onboard train integrity and GNSS-based positioning system in train control applications.

insaf.sassi@railenium.eu.es

El-Miloudi El-Koursi is a Research Director at IFSTTAR. He has 30 years experiences in performing assessment and certification of safety related rail and associated systems. He obtained in 1985 his Ph.D in Automatic control and industrial computer sciences at University of Lille. In recent years, he has been involved in various European projects. He was the leader of European FP5, SAMNET "Safety Management and interoperability thematic network" thematic network. He is the vice chairman of EURNEX.

el-miloudi.el-koursi@univ-eiffel.fr

Joffrey Clarhaut received his PhD in automation and computer science from the University of Lille (France) in March 2009. He is currently an assistant professor at the Polytechnic University of Valenciennes. His research interests include the dependability evaluation of complex systems, particularly during the design phase with an additional concentration for transportation systems.

Joeffrey.clarauht@uphf.fr

Dominique Renaux got a PhD degree in automation and computer science from the University of Lille in France in 1989. She is now a researcher at the University Polytechnique Hauts-de-France of Valenciennes. Her research project is about dependability parameters assessment of complex systems and SIL Safety Integrated Level evaluation. She works in partnership with IFSTTAR (French Institute of Science and Technology of Transport, Planning and Networks) and RAILENIUM, which objectives are to improve the railway system and the future train's performance. The aim of this ongoing research is to develop methodology in order to ensure onboard train integrity.

Dominique.renaux@uphf.fr

8 OTI functionality simulation based validation

Gorka de Miguel, Jon Goya, Paul Zabalegui, Iñigo Adin, Jaizki Mendizabal; CEIT, San Sebastián, Guipúzcoa, Spain

8.1 Introduction

The Train Integrity is an on-board function responsible for verifying the completeness of the train permanently, while the train is in operation. As part of the Innovation Programme 2 of Shift2Rail, Train Integrity (TD 2.5) deals with an innovative on-board train integrity solution, capable of autonomous train-tail localisation, wireless communication between the tail and the front cab, safe detection (SIL4) of train interruption and autonomous power supply functionality without the deployment of any fixed trackside equipment.

The status of the train's integrity is monitored by e.g. tail and train length detection: if the last vehicle is regularly advancing in a coherent way in relation to the movement of the remaining train and the train length remains unchanged, then there is no Train Integrity loss. Train integrity loss means that a certain coach (or multiple of them) has been unhooked from the rest of the train, that is, that the distances between them abruptly increases in time. In cases where there is a Train Integrity Loss, the On-board Train Integrity (OTI) system should detect the anomaly, indicating the possibility that the train is no longer complete, namely that one or more vehicles have been separated from the train. A non-detected Train Integrity Loss constitutes a serious danger for the next train, being a possible unexpected obstacle on the line, and therefore should be promptly reported to the control, command and signalling system, e.g. via ETCS on-board unit.

The OTI functionality is essential to implement more efficient signalling systems based on concepts like Moving Block or Train Position delivered by on-board equipment that allow simplifying fixed wayside infrastructure (e.g. track circuits, axle counters) and guarantee advantages in terms of increased capacity and reduced capital and maintenance costs, especially for freight and low density mixed-traffic lines. To achieve all the above results independently from trackside infrastructure, the train integrity shall fulfill a SIL 4 Safety Integrity requirement obtained as an overall result at system level.

The study of the OTI devices has been covered in the X2R2-WP4, including all S2R application domains: Intercity-High Speed, Regional, Urban-Suburban, Freight. The solutions will depend strongly on installed electrical and communications infrastructure on-board the train, and composition criteria for the train itself. The hardest scenario is found in traditional freight trains with individual wagons not equipped with neither any electrical nor communications infrastructure. In this case, energy harvesting and storage technologies will be considered and wireless communication solution from tail to front of the train will be explored.

Moreover, WP4 analyses the feasibility of fulfilling requirements from IP5, especially from TD5.3, thus providing useful information for train composition phase and reducing time and costs and facilitating intermodal services. In practice, this additional investigation could help to find dual use technologies that can be applied to every coupling and decoupling operation, and

not only when the train interruption is accidental. Demonstration of WP4 results achievement will be obtained with laboratory tests on prototypes and mock-ups, aimed at verifying and demonstrating right technical choices and to allow the performance analysis. As a relevant part of the laboratory tests, specific models and simulation tools will be adopted thus verifying in advance the performances and the suitability of some specific solutions as well as predicting and analyzing specific behaviors that could be observed in a more complex way at system level. One of these complex behaviors could be the case of the interactions foreseen with TD2.3, with the need of simulating some specific Moving Block scenarios, and more in general the integration with ATO GoA4 functions to support coupling and decoupling phases and also the integration with the ETCS/ERTMS system.

As part of the development and validation process of the OTI functionality a simulator is shown in this work.

8.2 OTI functionality simulator definition

A simulator to virtually test the OTI device functionality is proposed as one of the phases for the validation of the system. This simulator is based on CEIT's train locations simulator RANSS (Railway Advanced Navigation Satellite System) [1][2] , that allows to configure a train and a track, configure different sensors, simulate different algorithms and analyze the results (see next Figure 8-1).

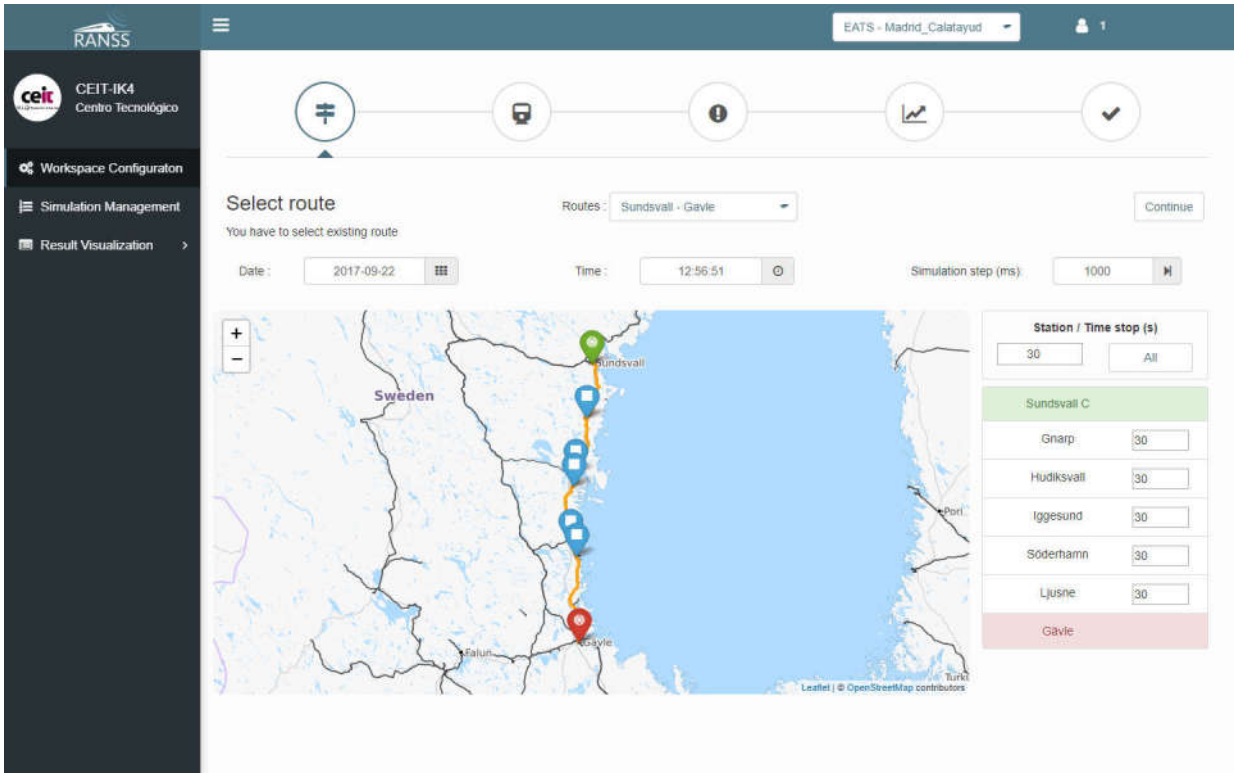


Figure 8-1: RANSS simulator

The RANSS simulator is extended with a train integrity module to test the train integrity functionality. The simulation-based validation approach of the train integrity module consists of four different sequential steps (see next Figure 8-2).

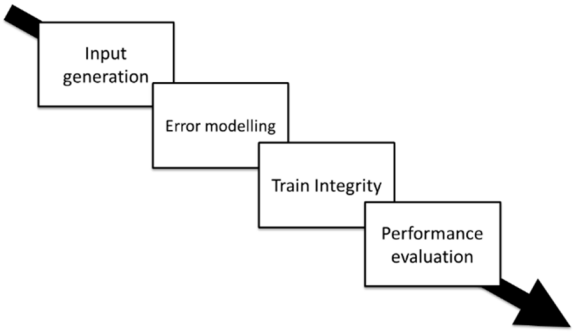


Figure 8-2: Simulation based validation approach

- Input generation: Generation of head/rear position info linked to a determined technology on a given track, that is, the position through the time and the speed. On one hand, there will be the reference data, the one that is supposed to be the real one, and on the other hand there will be all the data calculated with different technologies such as GNSS or IMU, employed as information source by the OTI device.

  In order to test the performance of the developed simulator, there have been designed multiple scenarios according to three different parameters, namely, the track, the introduction of TI loss on the reference data or not, and the third parameter is the used power supply: battery or harvested.

  Two different tracks have been chosen as reference scenarios:

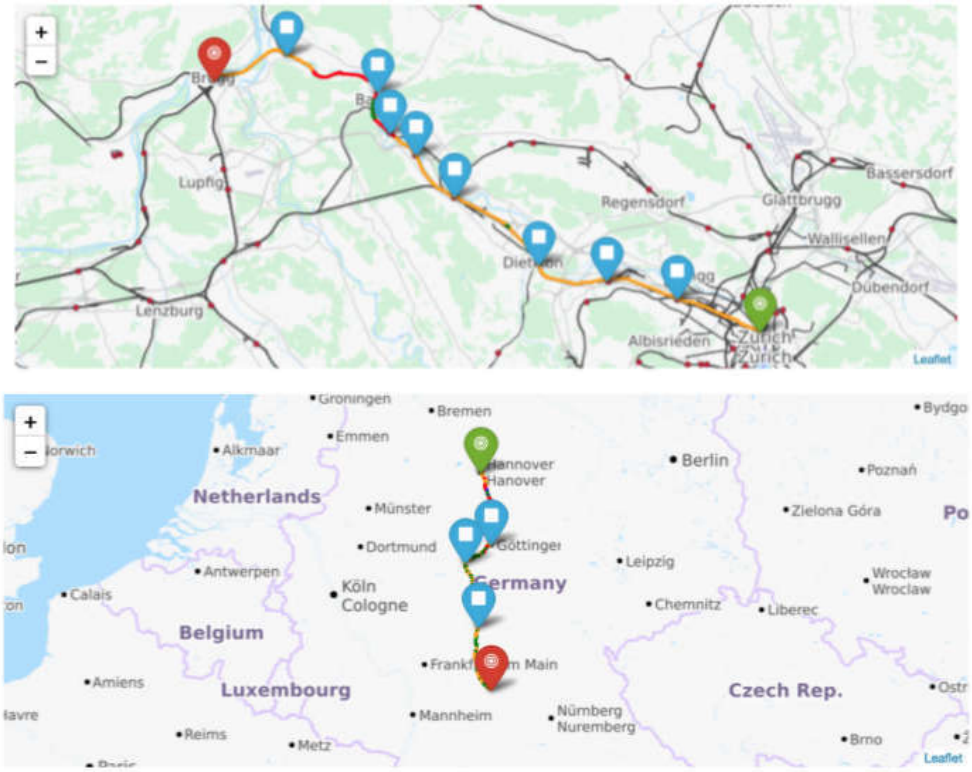


Figure 8-3: Zurich-Brugg track and Hannover-Wurzburg track

- Error modelling: as each of the technologies have different weaknesses and errors, an error modeling has to be done. These errors will determine the precision of the selected technology. The technologies considered are:

- GNSS: it is the more straightforward solution. A Global Navigation Satellite System as GPS or Galileo will give the possibility to know the position of each coach of a determined train and even to compare it with other coach's position so that it is ensured that train integrity is preserved. It fits both the technical and the energy harvesting constraints. The main drawback of the system may be the fact of being a satellite dependant choice, as occasionally tracks go through tunnels or similar.

- Wired communication: the simpler method. Just a wired solution for knowing if the integrity is fulfilled or not by connecting the rear and head coaches.

- Wireless communication: a subdivision is done into terrestrial wireless technologies, mobile cellular networks (LTE) and satellite technologies [3]. Inside the first group there are also several options: the 802.11 family, technologies such as ZigBee and 6LoWPAN (802.15.4) and solutions based on WiMAX (802.16).

- IMU: an IMU or Inertial Measurement Unit as the accelerometer providing accelerometer data of each coach could also be used to solve the train integrity problem. The speed measured by it will provide the tool to measure TI: speeds of all the different coaches will be compared and gaps will show up. It is also worth to mention that its low noise features fit perfectly for train vibration detection.

- Train Composition Sensors: this solution will be basically some proximity sensors in each wagon so that it could know if there are more coaches before and after itself. All this information will be sent to the head coach and there will be determined the integrity of the train.

In the case of GNSS for example the error has to be given by the environment where the train is, being the tunnel the worst case. The wires usually tend to worn and so the probability of being broken should be also part of the error modelling. Different error models can be taken into account in the simulator depending on the technology used in each moment. For GNSS, White Gaussian Noise is introduced in the obtained position estimation. For the other technologies, the errors are introduced in the raw measurements (accelerations, gyroscopes, ranges…). In this case, the introduced errors are a combination of a model of the errors specified in the datasheets of the sensors (bias, drift, instability…) and White Gaussian Noise.

- Train integrity function: once error modeling is done, next step to be done is train integrity determination. All the data collected in previous step has to be used and tested with a threshold for each method. This threshold will be the responsible of determining if there is a train integrity at each instant by testing if the data at each instant of each method surpasses it. This third step must be also done with the reference data so that two train integrity detections will be computed. This will be the tool to know if there has been a train integrity error or no, i.e. there has to be four possibilities for each method: a correct TI error detection, an undetected TI error, a correct detection of no TI errors and an incorrect detection when there is no TI error due to the weaknesses of the technology used. These possibilities can be also stated as the following: true positive, true negative, false positive and false negative. With all these parameters the train integrity error detection capability of a determined technology will be completely pictured.

- Performance evaluation: performance evaluation of all the technologies between them in different tracks and conditions. This will be done through the final result of the

simulator module implemented on RANSS. Through this module there will be the possibility to select different technologies and compare their TI error detection percentage and all their results through a track.

8.3 OTI functionality simulator development

In order to develop the Train Integrity module of RANSS simulator, the architecture defined beforehand has to be taken into account: reference, input generation, TI determination function and the comparison. The simulator takes into account all the selected technologies as different TI determination strategies, that is, for each of the scenarios it will be enough to run the simulator just once for getting results for all technologies. That is why the different detection methods are not considered separately, the idea is: all strategies on each scenario. Although there are exhaustively detailed below, a brief abridgment of each of these steps follows. The first of them is basically the election of a reference data. This will provide the simulator with a robust tool to test the performance of the different TI determination strategies on the fourth step. The second step, input generation, is basically the election of the different strategies to determine the possible loss of the TI and their corresponding modeling as mathematical entities. The third one corresponds to the determination of the thresholds for each strategy, in other words, the parameter or group of parameters that will determine TI loss in each strategy. Finally, the comparison between the obtained state of TI by the input and the real one by the reference are compared for each strategy or method. All the information that results from the simulator before the fourth step is sent and collected to a database so that all the information needed in the last step is located in one unique place.

- Step 1: Reference

As the main objective of the simulator is to test and consider different strategies to approach a unique problem (train integrity determination) sounds reasonable the need of a reference, something to compare it with. This reference must be something that clarifies if there has been a TI loss or not in a determined position and time of a particular track (which in turn depends on the selected scenario). In order to get that, first, exact data according to location at each instant of the train is obtained. This data is considered as the real journey of the train and its coaches, the real positions at real times. Then real train integrity is determined by means of simulation. So a reasonable criteria to determine TI loss could be to calculate the Euclidean distance between two consecutive coaches, subtract the length of the first coach and then compare it with a sharp threshold. The reason of the subtraction is that the sensors measuring position of coaches are located on the head of each coach. So what the simulator is doing is a subtraction between the distance of two positions and the theoretical value of this distance, that is, it should be 0 or almost 0. The threshold, calculated depending on the errors introduced by the model, determines if the calculated excess of distance at a determined instant and location is too high and so it represents a TI loss. In affirmative case it will be registered as a real train integrity loss event. It is worth to mention that the sensors obtain the location data in body frame coordinates, so the obtained data is then converted to ECEF coordinates in which the distance between wagons is calculated. Data can also be provided in other coordinates to the user. All the previously explained distance differences is done both in a consecutive coach by coach way and in a head-tail way. The latest means the comparison between the head and the tail of the train, taking into account like this the

whole train (and consequently subtracting the length of it), while the earliest just the comparison between consecutive coaches. These two ways and their purpose are better defined later. Just for clarification, this reference step is done for the comparison with all the different strategies. However, in the case of IMU the reference is obtained using the exact speed at each instant instead of the location in terms to do a fair comparison as IMU strategy is based on the acceleration at each instant captured by the IMU sensor.

- Step 2: Input Generation

After the computation of the reference data is done, next step is to define and model the input, the real input of the OTI device. These inputs consist of the different TI detection methods selected and each of them is modelled mathematically. A mathematical model of each of the TI models is generated complying the TI requirements for each of them. All the possible factors taking part in a TI loss detection must be taken into account, that is why in some of the methods are considered more than one parameter or "situations". Next all of them are specified.

oGNSS: based on GNSS sensors, the idea here is to collect data about location at each instant of the train in the same way that the reference. The difference with the GroundTtruth provided by the reference is basically that in this case it is not accurate, it may fail, and it will not be 100% modelling the reality. It is imperfect data. In essence, it is what we get if we implement it on real life. In order to model this TI loss strategy mathematically it is taken into account only one parameter, the detection of the separation between two coaches by using the calculated distances between them.

oWired communication: A different type of input is the one based on a wire. A simple wire connecting the whole train. In this case some other possibilities such as human error or physical deterioration are taken into account apart from the obvious break of the wire due to physical stress of the wire. So as a mathematical input the simulator considers three different parameters: a bad connection in the junctions between the wired and the coaches of the train, the possible erosion through the time of the wired and the physical disconnection or break of the wire due to remoteness between coaches.

oWireless: Wireless input type means input data generated using wireless systems. Here is where the separation between consecutive coach by coach and head-tail techniques makes completely sense. As wireless options are so vast it has been decided to use one shortrange wireless technology (for coach by coach) and a wide-range one (for head-tail). More concretely, considering the wireless technologies listed, they have been selected 6LoWPAN as short-range and 802.11p for wide-range.

In both cases, the simulator considers three events in order to model the input mathematically. The first one is the possible interference that could happen through the journey of the train. The second event is the possibility of the router to fail due to multiple reasons. Finally, the third one is the case where two routers are too far away from each other and so the range of the respective technology is exceeded.

oIMU: IMU input is the last type of input generated by the simulator. It is based on the information about acceleration of the train collected by the IMU sensor. In other words, it works in a such way of the GNSS input but using acceleration differences. As in the case of the GNSS input the simulator considers only one event: the separation of the coaches based on acceleration differences.

- Step 3: Train Integrity Determination Function

Being the input defined and correctly modeled by the simulator the next task is to use all that information to determine if there has been a TI loss in each case. Each of the events of the different strategies have a threshold that determines if a TI loss can be determined by that event. However, all of them have something in common: they all need power to be running. That is why a lack of power will mean a TI indetermination or unknown state regardless the method in use. So, in this step the simulator makes two sub-steps: checking the availability of the needed power and the determination of TI according to the thresholds of each event.

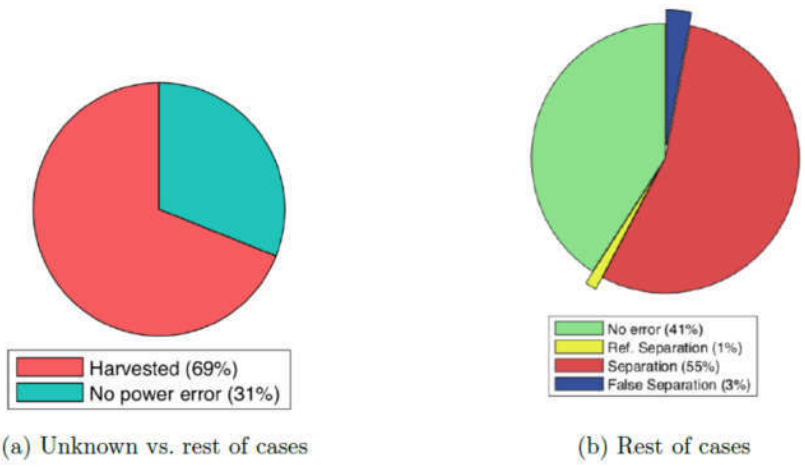
oPower availability: The simulator considers two power feeding possibilities for the OTI. Both of them are equally valid with their strengths and weaknesses: battery and harvested.

oTI determination thresholds of the strategies: As mentioned before, each event has a different threshold for consecutive coach by coach measurement and head-tail measurement. These thresholds are the ones determining if a determined event with the consequent provocation of TI loss has happened. First, some default thresholds have been defined. It is remarkable the fact that all the chosen values for these thresholds are just approximations of real life considered in a completely subjective way.

- Step 4: Comparison

The last step the simulator does for each scenario is to obtain three types of graphs. These graphs characterize completely an exhaustive comparison between the results obtained by the OTI device (results of step 3) and what really has happened in reality (results of step 1). Thereby, the simulator provides a full picture of the OTI device and its performance with all the different technologies and strategies in the selected scenario. Regarding the number of graphs, the simulator does the graphics triplet for each method or TI determination strategy. Furthermore, it computes each graph for both coach by coach and head-tail technology, so that there will be as much coach by coach graphs as consecutive coach comparisons.

- TI loss detection graph: pie chart where each slice represents one of five possibilities: Unknown, not detected, false detection, correct detection and non-existent.



(a) Unknown vs. rest of cases (b) Rest of cases

Figure 8-4: Example of TI loss detection graph

- Location based graph: The main objective of this graph is to translate the results of the other two graphs to the map of the track

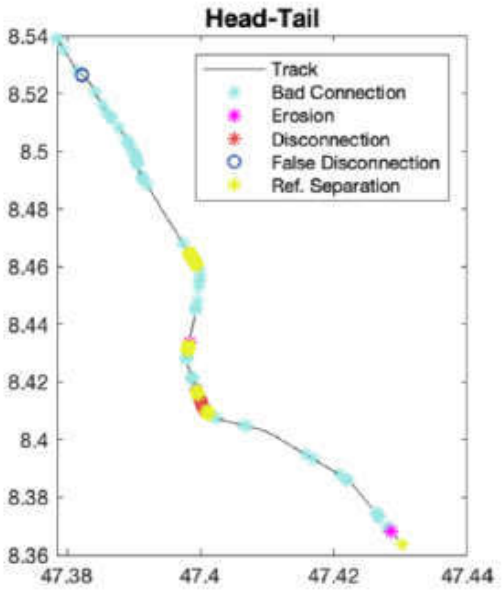


Figure 8-5: Example of location based graph

- Reaction time graph: it shows the delay suffered by the OTI device when it detects a TI loss. That is, the amount of time that passes since the TI loss happens in reality (reference detection) and the OTI detects it. It is done for each Not-detected to Correct-detection transition as it is always a minimum delay whichever the TI determination strategy is.

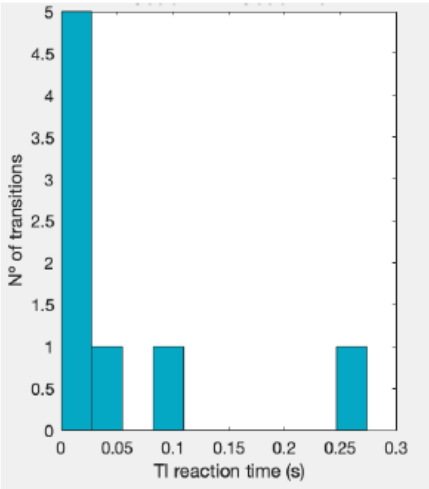


Figure 8-6: Example of reaction time graph

8.4 Conclusions

On-board Train integrity functionality will be one of the enables for the future railways allowing to remove track-side equipment and the deployment of the moving block concept. Different solutions might be deployed depending on the railway domain. However, all the solutions will need to go through a development and validation phase. In this context a simulator for the OTI functionality is proposed based on CEIT's RANSS simulator. By means of the 4 steps of the OTI functionality simulator it is possible to assess the performance of the proposed OTI functionality

solution. The 4 steps are Input generation, Error modelling, Train integrity function and Performance analysis. The simulator covers the scenario generation, different technologies that can be combined included its errors, the modelling of the OTI functionality itself and an strategy for the performance analysis.

8.5 References

[1] Goya et. al. Methodology and Key Performance Indicators (KPIs) for Railway On-Board Positioning Systems. IEEE Transactions on Intelligent Transportation Systems

[2] Goya et al. Advanced Train Location Simulator (ATLAS) for developing, testing and validating on-board railway location systems. European Transport Research Review. 2015

[3] X2R2 D4.2 Functional architecture & Interfaces specifications & Candidate technologies

8.6 Authors

Gorka de Miguel received the M.Sc. degree in telecommunications engineering from TECNUN (School of Engineering of San Sebastián), University of Navarra, Donostia-San Sebastián, Spain, in 2015. In 2015, he joined the CEIT Research Centre, Donostia-San Sebastián, Spain, where he is currently a Research Assistant and a Ph.D. Student within the Transport and Sustainable Mobility Group. He is also an Assistant Lecturer in Electronic Fabrication Systems with TECNUN. His research interests include the field of positioning and software development. He is now actively participating in H2020 European funded projects in Railway signaling and positioning topics.

gdemiguel@ceit.es

Jon Goya received the M.Sc. degree in telecommunications engineering in 2011 and the Ph.D. degree from the Universidad de Navarra in 2016. He is currently a Lecturer with the TECNUN, Universidad de Navarra, and also a researcher with the CEIT. His professional research activity lies in the simulation of on-board positioning system and performance analysis for railway. He has participated in FP7 projects coordinated by CEIT and is now actively participating in actively in Shift2Rail.

jgoya@ceit.es

Paul Zabalegui received the M.Sc. degree in Telecommunications Engineering from TECNUN (School of Engineering of San Sebastián), Spain, in 2019. He joined the CEIT Research Centre in San Sebastián in 2019, and he is currently a Researcher Assistant and Ph.D. student within the Transport and Sustainable Mobility group. His research activity lies in the field of positioning and software development. He is now actively

participating in H2020 European funded projects in Railway signaling and positioning topics.

pzabalegui@ceit.es

Dr. **Iñigo Adin** received his M.Sc. Degree in Electronics Engineering in 2003 and his Ph.D. in 2007 from the University of Navarra. His research interests include safety-critical designs, with special interest in positioning, communications, electromagnetic compatibility and transport interoperability. He is author, or co-author, of four patents, 2 technical book, an invited chapter and 40 articles in journals and international conferences. He was the coordinator of the FP7 European Project TREND and now coordinates the H2020 AIOSAT for GSA. Moreover he has participated in 4 projects from the Shift2Rail initiative.

iadin@ceit.es

Dr. **Jaizki Mendizabal** received his M.Sc. and Ph.D. degrees in Electrical Engineering from TECNUN (University of Navarra, San Sebastián, Spain) in 2000 and 2006 respectively. He joined Fraunhofer Institut, Germany) and SANYO Electric Ltd, Japan as RF-IC designer. Nowadays, he is at CEIT, in San Sebastián (Spain) where his research interests include communications and electronic systems. He is lecturing "Communications Electronics" and "Communications via Radio" at TECNUN (University of Navarra).

jmendizabal@ceit.es

9 CBA – Assessment methodology for shifting railway technology from the infrastructure onto the train

Alessa Eckert ; German Aerospace Center (DLR), Institute of Transportation Systems, Berlin, Germany

9.1 Introduction

At the moment, research on railway technology in the field control command and signalling is exploring options that shift functionalities from the infrastructure onto the trains. [1] One example is the assurance of the integrity of the train, which is currently implemented through axle counters or track circuits. The Cost-Benefit Analysis (CBA) that is being done in the Shift2Rail project X2Rail-2 Work Package (WP) 4 is not performed at a stage of selecting and comparing different technologies against each other but to disclose the cost and benefits of shifting the train integrity function from the infrastructure onto the train. One part of this cost benefit analysis is an analysis of changes in the life cycle costs of the technology.

9.2 Life Cycle Cost Methodology

The purpose of this abstract is to present a methodology for ensuring an accurate cost comparison of fixed infrastructure components that can be directly attributed to a specific location, with costs related to a moving asset such as locomotives and wagons.

9.2.1 Life cycle cost calculation

Area of investigation

When analysing indicators of a system such as costs, the first step is to find a decision on the area of investigation. Generic scenarios have to the advantage that they simplify complexity, reducing regional specifics of a certain corridor. This has the advantage that results can be extrapolated on a high level but will lack detail and an exact representation of the system.

To capture the effects of a single functionality of the railway system however, detail is often important as average values do not show all aspects.

Within X2Rail-2 WP4 it has therefore been decided to perform the CBA on different real life scenarios, thus capturing different railway corridors in various countries with their respective regional specifications. These scenarios were carefully chosen in order to be typical and representative for a certain part of the railway network.

Functionality analysis

In another step it has to be analysed which functionalities are covered by the old technology on the trackside and how they are covered by the new on-board unit. In the X2Rail-2 WP4 case, axle counters do not only monitor train integrity but also provide information on the safe train positioning. This does not mean that the cost for the two functionalities of monitoring train

integrity cannot be compared to each other but all assumptions and prerequisites have to be stated in order to ensure an objective interpretation of the result.

Net present value approach

For all assets of infrastructure elements and on-board unit, the lifespan, capital expenditure (CapEx) as well as operational expenditure (OpEx) have been collected and discounted over a period decided on depending on the project as can be seen in Figure 9-1. For railway projects a common time period is 30 years. This is especially important when comparing projects with different lifespan where some are very long as the value of money changes over time [2].

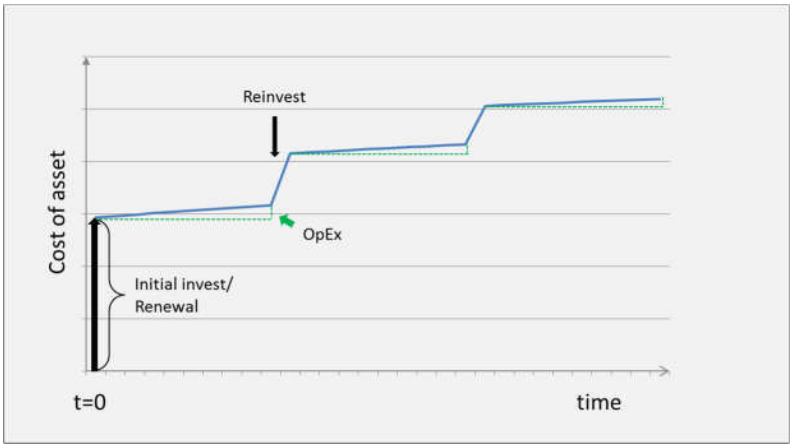


Figure 9-1: LCC infrastructure asset

The CapEx include all initial investments as well as reinvests of asset components with a shorter lifespan that have to be replaced within the common time period. In the OpEx all cost that arise continuously, in this case maintenance cost and operational cost are included. Due to the compound interest effect, inflation and opportunity cost, the value of money changes over time. Especially for assets with long life cycles it is therefore important to discount all cost that occur over the life span of the asset to the same time. This is done with the net present value (NPV) approach. Usually all costs are calculated to the present time (t=0) [3]:

$$NPV = \sum_{t=0}^{T} \frac{B_t - C_t}{(1+i)^t}$$

Where B_t = benefits in year t, C_t = costs in year t, T = lifespan of the project and i = discount rate in year t

9.2.2 Life Cycle Cost for fixed assets

For the infrastructure elements the cost can then be calculated by multiplying the number of assets within the area of investigation and the cost for each asset. As infrastructure assets have a fixed location the allocation to an area can be done. When infrastructure elements become obsolete, the benefit equals the costs per asset multiplied by the number of infrastructure elements. When a specific amount of the infrastructure assets need to remain to ensure backward compatibility it is more challenging to determine the exact number of infrastructure elements that become obsolete and therefore contribute to the benefit in the form of cost

savings. This is however not part of the analysis done in the X2Rail-2 project and therefore not further investigated here.

9.2.3 Life Cycle Cost for moving assets

The cost calculation for the trains however is more complicated as they do not run exclusively in the scenarios chosen but are used within a wider network.

Therefore an approach has been developed to estimate the number of trains that correspond to a defined corridor under the assumption that not only this corridor but the whole network will in fact be fitted with the new technology.

9.2.3.1 Approach for passenger trains

The approach contains three main steps which differ slightly between passenger and freight trains. For passenger trains these are:

1. Determine all train services that run through the scenario
2. Estimate the fleet size which is relevant for each train service determined in step one
3. Calculate the share of cost corresponding to the scenario

Once the scenario is set, all trains that run through the chosen scenario corridor have to be determined as they will have to be fitted with the new on-board technology if the functionality is no longer provided by the infrastructure. The length of each service line as well as the duration if one trip from the first stop to the last stop of the line can then be obtained from the railway undertaking providing each service (compare exemplary Table 9-1).

Table 9-1: Train Service Analysis

Train type	Service	Length (KM_T) in KM	Time per trip $(h_{T)}$ in hours
Regional_Train_1	First_stop-Last_stop	50	1
Regional_Train_2	First_stop-Last_stop	100	2
Regional_Train_3	First_stop-Last_stop	80	2
High_Speed_Train_1	First_stop-Last_stop	300	2.5
…			

In a second step the fleet size necessary to run the total service has then been calculated taking into account the trains per hour per direction, the time per return trip including a turn-around time of $\frac{1}{6}th$ of the trip time (ratio of driving and rest time in Germany), a disposition reserve as well as a maintenance reserve [4]:

$$N_F = h_R \times N_P \times (1 + \frac{R_T}{100})$$

Where N_F = Number of trains per fleet for the service line, h_R = time per return trip including turn- around time, N_P = Number of trains per direction per hour, R_T = Total train reserve

With

$$h_R = 2h_T \times \left(1 + \frac{1}{6}\right) \text{ and } R_T = R_{Maintenance} + R_{Disposition}$$

Where h_R = time per return trip h_T = time per trip, R_T = Total train reserve, $R_{Maintenance}$ = maintenance reserve, $R_{Disposition}$ = disposition reserve

9.2.3.2 Approach for freight trains

While for passenger trains these data are available as public data from the train operators, cities and regions. For the freight trains however, these numbers are not available therefore the approach differs slightly from that for passenger trains.

For freight trains the approach is as follows:

1. Determine the average number of freight trains per hour that run through the scenario
2. Estimate the number of locomotives and wagons necessary to operate the programme determined in step one
3. Calculate the share of cost corresponding to the scenario.

For high density corridors, open source data for average freight train numbers exist. Especially in the context of noise mitigation measures or infrastructure action plans these data are collected and published as open source data.

To determine the fleet size for the freight trains, two calculations have to be done as the time per trip for the locomotive is shorter compared to that of the wagons. This is due to the fact, that the wagons need an additional amount of time for loading and unloading procedures in the terminals.

The number of locomotives can be determines by multiplying the average number of freight trains per hour with the duration per trip and a maintenance reserve. In order to get a value for the trip duration, the length of the trip as well as the average speed for wagons and locomotive has to be obtained. As freight train data are not publicly available, average values are used. The average kilometre per trip for the calculation is available from most railway undertakings for domestic transport; cross-border trips however can be longer.

Average values for the yearly kilometres of freight wagon and locomotives can be obtained from railway undertakings as well. These yearly kilometres can then be divided by 365 days and 24 hours to get an average speed value. With these assumptions the fleet size of locomotive and wagons can then be calculated as follows:

$$N_{FL} = 2 \times h_{TL} \times N_P \times (1 + \frac{R_{Maintenance}}{100})$$

Where N_{FL} = Number of locomotives per fleet for the service line, h_{TL} = time per trip in h for the locomotive, N_P = Number of trains per direction per hour, RMaintenance = Maintenance reserve

With

$$h_{TL} = \frac{KM_T \times 365 \times 24}{KM_{LY}}$$

Where h_{TL} = time per trip in h for the locomotive, KM_T = average kilometre per trip, KM_{LY} = average yearly kilometre of a locomotive

And the number of wagons respectively with the following equation:

$$N_{FW} = 2 \times h_{TW} \times N_P \times (1 + \frac{R_{Maintenance}}{100})$$

Where N_{FW} = Number of wagons per fleet for the service line, h_{TW} = time per trip in h for the wagons, N_P = Number of trains per direction per hour, $R_{Maintenance}$ = Maintenance reserve

With

$$h_{TW} = \frac{KM_T \times 365 \times 24}{KM_{WY}}$$

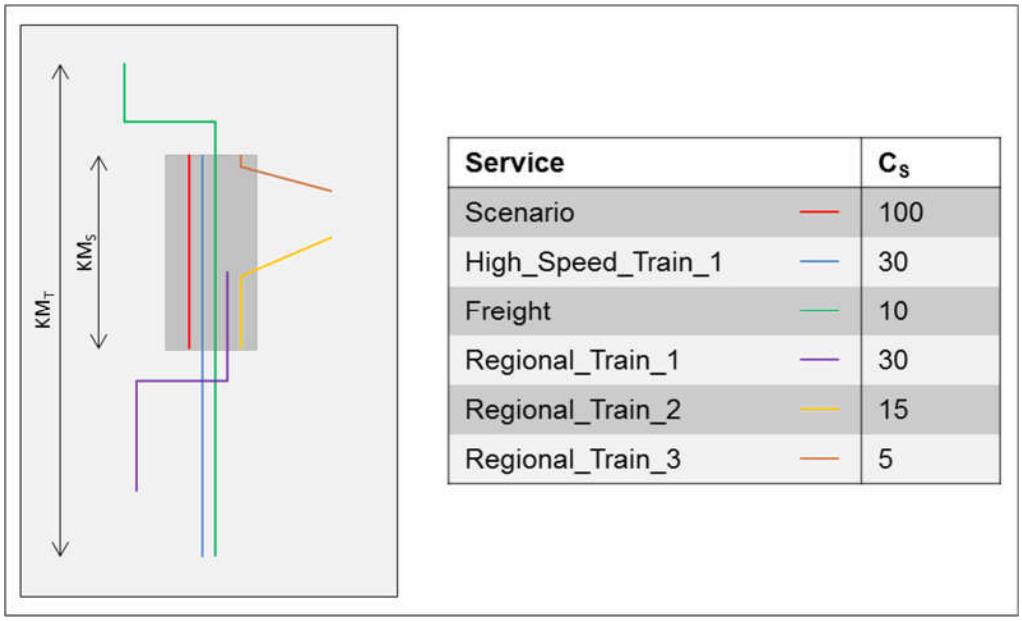
Where h_{TW} = time per trip in h for the wagons, KM_T = average kilometre per trip, KM_{WY} = average yearly kilometre of a wagon

9.2.3.3 Share of cost for passenger and freight trains

Under the assumption, that not only the investigated scenario will be retrofitted but the whole network, in the last step the ratio of the scenario km and the total kilometre of each service can be used to determine the share of cost of retrofitting the trains which can be compared to that of retrofitting the infrastructure as has been visualised exemplary in Figure 9-2.

$$C_S = \frac{KM_S}{KM_T} \times 100$$

Where C_S = Share of cost relevant for the scenario, KM_S = Service kilometre within the scenario, KM_T = Total service kilometre



Service	C_S
Scenario	100
High_Speed_Train_1	30
Freight	10
Regional_Train_1	30
Regional_Train_2	15
Regional_Train_3	5

Figure 9-2: Share of Cost - movable assets

The number of passenger trains as well as freight trains determined with the described approach can now be multiplied with the cost for retrofitting each type of train as well as the cost share (C_S).

9.3 Conclusion

The approach described above has been developed within X2Rail-2 WP4 as part of the Cost-Benefit Analysis to asses effects of shifting the train integrity functionality from the infrastructure onto the train. The approach is based on approximation when detailed numbers of passenger and freight trains are not available. It is therefore not an exact representation of the real situation. It can however be adapted to the comparison of other functionalities as well. In all cases a detailed description of all assumption taken when determining the input values is mandatory for the reader to be able to interpret the results correctly.

The Methodology is only part of the CBA to determine the change in life cycle cost of the infrastructure elements and compare these to the shift of the functionality onto the train. Additional benefits that are not primarily cost related are not captured in this approach but are performed as part of the CBA in the X2Rail-2 project as well.

9.4 References

[1] "X2R2 D4.1 Train Integrity Concept and Functional Requirements Specifications, 2019.".
[2] European Comission, "Guide to Cost-Benefit analysis of investment Projects," Luxembourg, 2015.
[3] J. Nellthorp, "The principles behind transport appraisal," in the Routledge Handbook of Transport Economics, 2017, pp. 176-208.
[4] J. Anderson, "Calculation of performance and fleet size in transit systems," Journal of Advanced Transportation, Volume 16, Issue 3, 1982.

9.5 Author

Alessa Eckert is scientific staff at the Institute of Transportation Systems since 2018 after graduating at the Institute of Transport Studies (ITS) at the University of Leeds. She works in the X2Rail-2 project on the Cost-Benefit Analysis of the Onboard Train Integrity technology.

Alessa.Eckert@dlr.de

10 Formalising the Specifications of Onboard Train Integrity System for Verification Purposes

Insaf Sassi, IRT Railenium, Famars, France
Mohamed Ghazel, El-Miloudi El-Koursi, Université Lille Nord-Europe, IFSTTAR, COSYS, ESTAS, Villeneuve d'Ascq, France

10.1 Introduction

This work describes formal validation of the functional specifications of the onboard train integrity (OTI) module being developed within X2RAIL-2 WP4 activities as part of TD 2.5 of IP2 ("Advanced Traffic Management and Control Systems"). The functional specifications of the OTI function are established in deliverable D4.1 [1]. Such specifications are presented as a list of requirements expressed in natural language and semi-formal models (high level UML State Machines (SM) and a set of Sequence Diagrams (SD)). Although these UML diagrams provide valuable graphical description of the OTI system behaviour and allow for tackling some issues related to natural language-based specifications, their lack of formal semantics opens the way to some ambiguity in terms of interpretation. In the absence of such formal semantics, it is not possible to implement formal verification techniques that are highly recommended to express and verify the specifications, and more generally for the engineering of safety critical systems [4]. In this context, our contribution, presented in this paper, is related to the development of formal specifications of the OTI system as part of X2RAIL-2 WP4 activities to ensure completeness and correctness of specifications that have been reviewed in deliverables D4.1 [1] and D4.2 [2]. Based on the established formal models, automatic verification techniques can be brought into play to check different types of properties automatically. Namely, the properties that can be verified are deadlock freeness, liveness and safety properties, etc. In particular, model checking has been used as an automatic formal verification technique that allows for formally checking such properties, expressed as temporal logic assertions, on the system behaviour. Besides checking of a list of generic functional and safety properties, model-checking was used to investigate two complex scenarios: train splitting and train joining. It is worth noting that deliverables D4.1 and D4.2 have served as a reference for the formal verification activities.

In the remainder of this paper, we firstly give a general description of the OTI system and its high-level functional behaviour, in section 2. A formal model is then proposed in section 3, to express the functional specifications of the OTI system. We then give some illustrations on how model-checking can be used to check some safety properties based on the established model. Finally, section 4 provides some discussion on the developed contribution as well as some concluding remarks.

Onboard Train Integrity

Railway signalling systems are in continuous progress to cope with the evolution of the railway industry and needs. European standards, onboard and trackside systems have been evolving in order to find a solution that safely increases the capacity of the European rail network in a cost-effective way. In order to reduce the cost, removing trackside equipment (track circuit, axle

counters) shall be possible by setting up the control-command equipment onboard the train. It must ensure, like the trackside train detection system, that the train is moving safely and that the train is complete during its journey, i.e., no wagon is lost. In fact, a lost vehicle is considered as a non-detectable obstacle on track which represents a danger to the safe journey of the other trains. This implies that continuous supervision is needed in order to communicate the train integrity status, via radio messages, to the Radio Block Centre. Using onboard control-command systems, mainly for the train integrity functionality, transfers more responsibility for the safety of train operations from infrastructure managers to railway undertakings. To respond to the new challenges, the WP4 work on the on-board train integrity aims to design an on-board system that independently and safely monitors the integrity of the train. A definition of the OTI system and the procedure of integrity evaluation are detailed in the sequel.

10.1.1 System definition

The role of the train integrity monitoring system is to supervise the integrity status of the train tail by checking the coherence of the last wagon movement relatively to the movement of the train head wagon. Namely, the tail wagon must be advancing consistently with the head of the train. The integrity information is then transferred to the European Train Control System (ETCS) onboard unit, which takes the role of the automatic train protection system, as shown in Figure 10-1. At ETCS level, the integrity information has three possible values: confirmed, lost or unknown according to CR940 [3], and is regularly provided to the Radio Block Centre. In fact, the OTI system consists of the following modules:

- **OTI Slave (OTI-S)**: It represents the OTI device that is located at the train tail. OTI-S evaluates the integrity status of the tail and communicates it to the OTI Master.
- **OTI Master (OTI-M)**: Generally, it is the OTI device that is located at the train head. It acquires the information regarding the tail status from the OTI-S in tail. OTI-M then evaluates the status of the train integrity accordingly and sends it to the ETCS onboard.
- **OTI (Slave) Intermediate (OTI-I)**: it represents the OTI device that is located at the intermediate train vehicles.
- **Onboard Communication Network (OCN)**: It is the communication channel (wired or wireless) used for information exchanging between the OTI monitoring system devices.

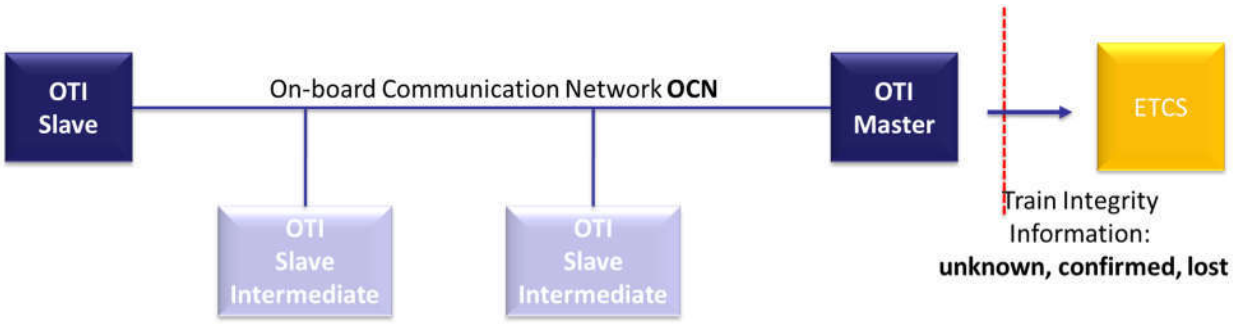


Figure 10-1: Onboard Train Integrity System

10.1.2 Train integrity evaluation procedure

It is worth noting here that several classes of products can be distinguished. The type of the communication channel is a key feature to define the integrity criteria and identify the product type among the two product classes. The first product class refers to trains with a wired communication network onboard, where the integrity criteria is evaluated based on the communication liveliness between an OTI Slave module located at the train tail and the OTI Master module. The second product class encompasses the trains with wireless communication channel, where integrity is determined based on comparing kinematic data of the train tail and the front cabin (e.g. position, speed, acceleration).

The train integrity monitoring system is used to safely detect the train dislocation, and for supervising two functional scenarios: train joining and splitting. Moreover, the OTI modules have to perform basic functionalities before starting any of the scenarios. In particular, the OTI slave and master functional modules shall safely carry out the mastership, inauguration and monitoring phases as depicted in Figure 10-2. The mastership phase consists in identifying the OTI modules' roles: master, slave. The inauguration phase aims at identifying the OTI modules connected to the OCN where the OTI-M shall send identification request messages to all OTI slave modules. The OTI-M shall activate a pairing procedure with the OTI slave module located at train tail. Finally, the monitoring phase consists in performing train integrity monitoring where the OTI-M shall receive train tail status from OTI-S frequently.

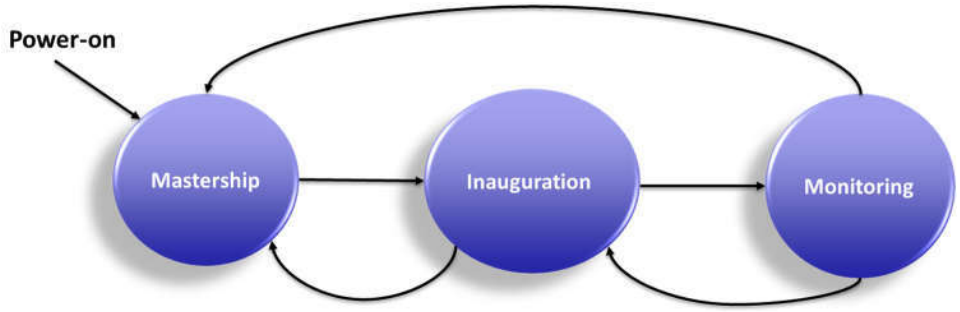


Figure 10-2: High level Finite State Machine of OTI behaviour

10.2 Formal Verification

In our work, the system model using extended timed automata [6] is established from the behaviour description. Based on such a formal model, the model checker engine can exhaustively investigate all system states to check if some given property is satisfied or not. A property specification represents what the system must and must not do. In case an encountered execution violates the scrutinized property, the model checker provides a counterexample that indicates the path traced from the initial state to some target state, in such a way as to violate the property. A simulator is also available to replay the violating scenario to isolate the error and adapt the model and/or the property.

Developed models

An OTI module can behave as a master or a slave depending on its position in the train and the operational context. Therefore, the OTI model is developed in a generic way to be able to play

the role of a master or a slave. This model combines the master sub-model and the slave sub-model, as depicted in Figure 10-3, while making it possible for an OTI model to switch between master and slave behaviours depending on the role of the OTI module.

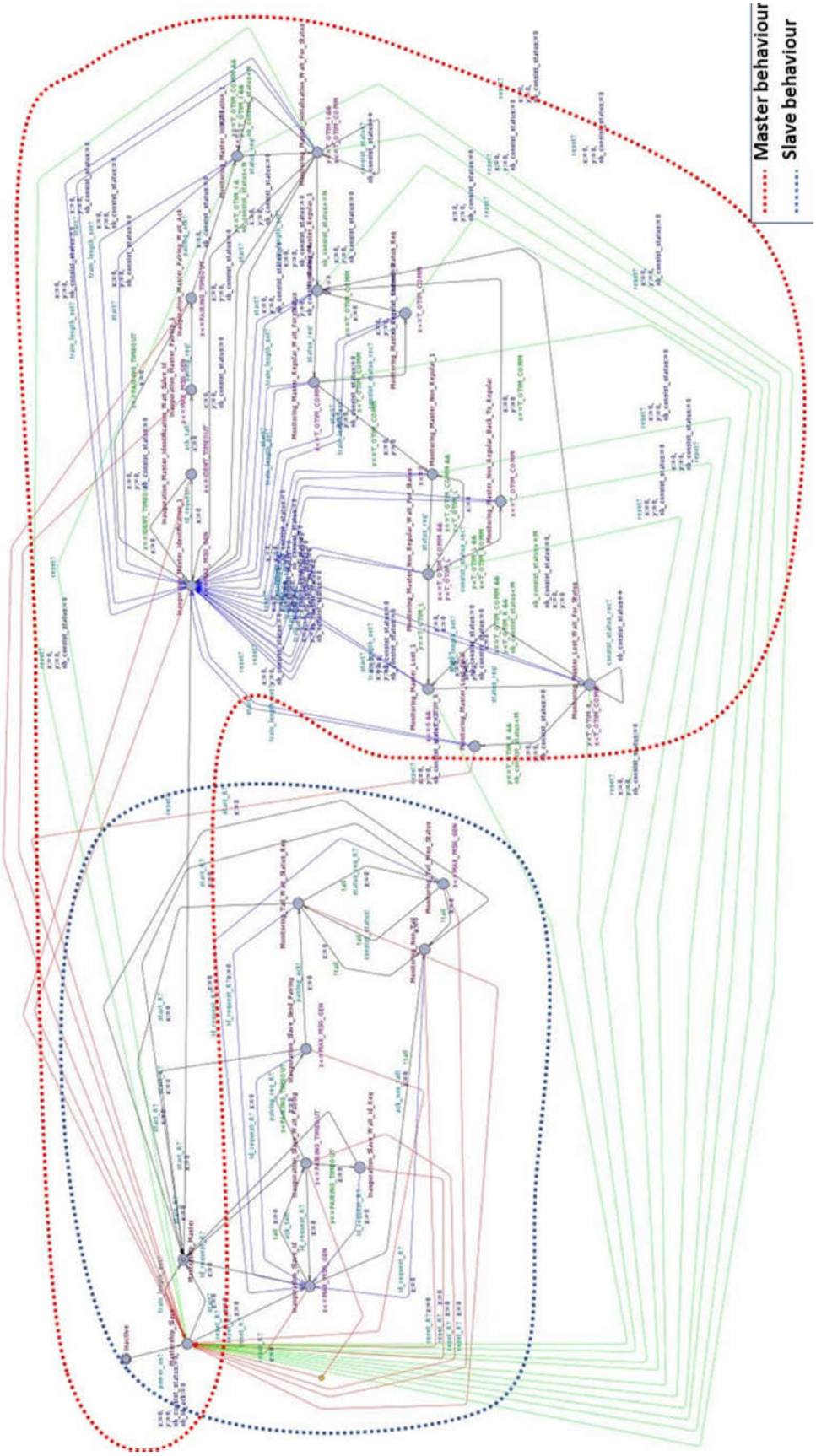


Figure 10-3: OTI generic model

The OTI model pattern of Figure 10-3 is then instantiated for the verification of OTI system specifications while fixing the values of its parameters, presented below, *in_active_cabin, tail, et1, ht2, t12* according to the actual operational context:

- *bool in_active_cabin*: to indicate the head locomotive/leading vehicle.
- *bool tail*: to localise the slave in tail position.
- *bool et1*: to indicate the last wagon in train 1 that will change its role according to the operational context (joining, splitting).
- *bool ht2*: to indicate the head locomotive of train 2 that will change its role according to the operational context (joining, splitting).
- *bool t12*: to define the belonging of wagon, if *t12=true* the OTI module belongs to train2, *false* otherwise.

It is worth noticing that some additional models are established to represent the OCN behaviour, the operational context (e.g., joining and splitting scenarios), the events issued from the environment (e.g., the power-on signal, external commands (start, reset, train_length_set)), OTI updates of the integrity, and integrity status at the ETCS level.

A variable integrity is devoted to indicating the updates of train integrity state. Initially set to 1, its value is defined as follows:

- **1** if the OTI-M evaluates the integrity as *unknown*
- **2** if the OTI-M defines the integrity as *confirmed*
- **3** if the OTI-M indicates the integrity as *lost*

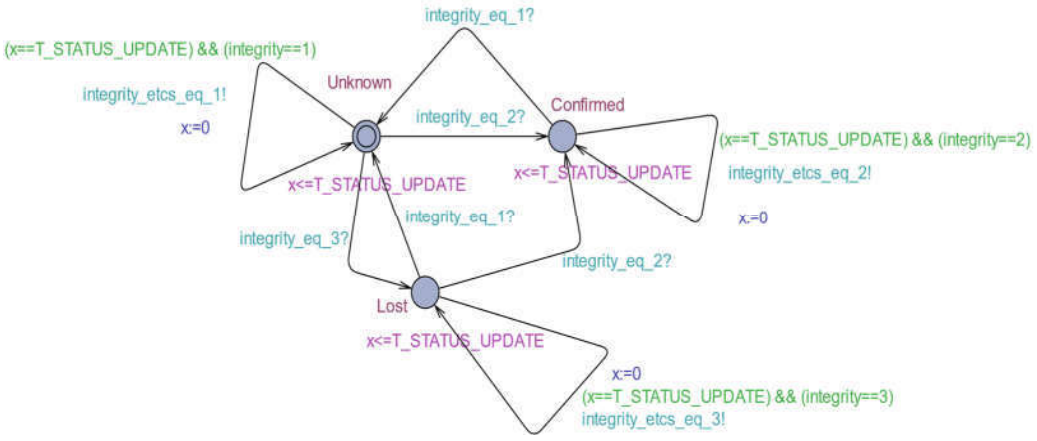


Figure 10-4: Integrity status at OTI level

The integrity value is set according to the actual state in the OTI-M sub-model of Figure 10-3. Integrity status is initially defined as unknown in the OTI-M model and also in automaton integrity status at OTI level of Figure 10-4. The automaton integrity status at OTI level is updated according the evolution of the OTI-M sub-model among the states of the monitoring phase and reset to unknown after every reset or re-start command. The integrity information must be sent

periodically from the OTI to the ETCS. So, the automaton of Figure 10-4 sends a signal to the integrity ETCS automaton of Figure 10-5 every T_STATUS_UPDATE defined as the period of communication between the ETCS and the OTI to update the integrity information.

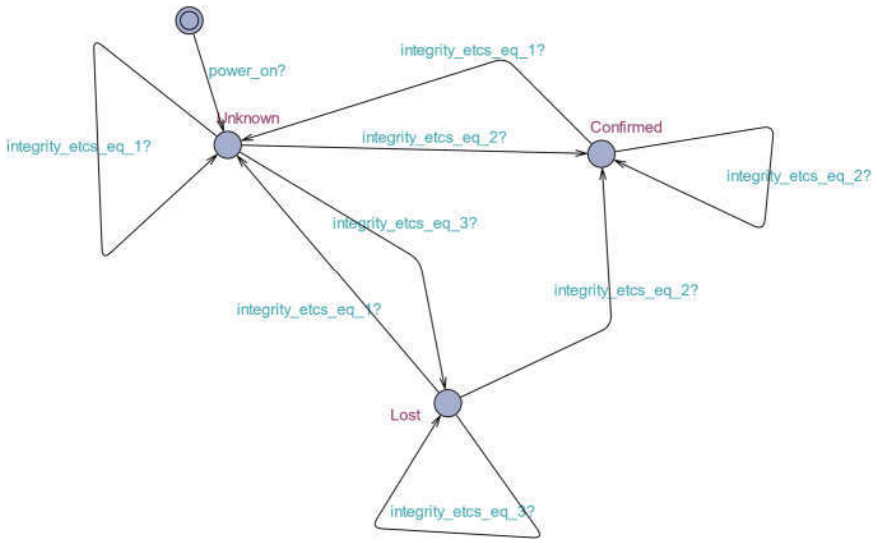


Figure 10-5: Integrity status at ETCS level

10.2.3 Formal verification of system specifications

For verification purposes, the OTI generic model, OCN models and the environment behaviour automata are instantiated, synchronized and the obtained product is used as the specifications model on which model checking can be performed to investigate a set of properties, by means of the UPPAAL tool [5]. To this aim, the properties to be analysed on the specifications need to be expressed formally as temporal logic assertions. The properties to be checked in UPPAAL are formulated using the Timed Computation Tree Logic (TCTL) specification language. A TCTL formula can be either a state formula (e.g., deadlock) or a path one (e.g., liveness). The TCTL formalism is based on a subset of the Computation Tree Logic (CTL) that is enriched with clocks constraints to express real-time properties on the system behaviour. For the sake of illustration, in the sequel we give an example of properties that were checked using model-checking. The presented property is a safety one, as defined below:

Safety Property: A safety property specifies a situation that the system must avoid, i.e., "something bad never happens". A safety property can be expressed as something good is invariantly true where something good stands for the contrary of the bad thing that must not occur. Regarding train integrity monitoring, a typical scenario that must be avoided is when ETCS onboard receives a confirmed train integrity information, while the OTI system is evaluating the train integrity as lost. This event represents a false negative that generates a safety issue. This property is expressed by the following formula:

AG !((OTI.Monitoring_Master_Lost_Wait_For_Status || OTI.Monitoring_Master_Lost_Final) && etcs_integrity_status.Confirmed)

The above formula can be read as follows: The system shall never reach (AG !) a state where the onboard train integrity is evaluated as lost and the ETCS level integrity information is confirmed.

By means of the UPPAAL model-checking engine, we found out the stated requirement is well fulfilled.

One of the targeted scenarios to investigate is train splitting. It consists of separating two trains that are initially coupled. Before splitting, the train is containing 4 OTI modules obtained by the instantiation of the OTI pattern of Figure 10-3 with predefined parameters: OTI-M, OTI-S non tail (1), OTI-S non tail (2), OTI-S tail. After splitting the trains, we must check that OTI-S non tail (1) becomes OTI-S in tail of train 1, OTI-S non tail (2) becomes master of train 2 and OTI-S tail becomes the tail of train 2.

Concerning the joining scenario, it consists of coupling two trains that are initially separated. Before joining, every train is composed of two OTI modules; a master and a slave in tail. Thus, 4 OTI modules are instantiated: master of train 1 OTI-M (1), slave in tail of train 1 OTI-S tail (1), master of train 2 OTI-M (2), slave in tail of train 2 OTI-S tail (2). After joining the two trains, we must check that the OTI-S tail (1) and OTI-M (2) switch to OTI-S non tail, so the obtained train contains only one slave identified in tail.

10.3 Conclusion

The present work deals with the formalization of the OTI specifications. Using formal models is recommended to elucidate and fix specification errors that cause of a major portion of bugs while engineering complex systems. Developing such formal models enables to fix some main specification issues, such as inaccuracy and inconsistency. Elucidating and correcting these problems as early as from the specification phase, offers great advantages for the engineering process, in terms of costs and delays. Thanks to the developed formal models and to the formal verification of various properties on the established models, several modifications and improvements have been included in the OTI specifications to set a sound basis for the subsequent development phases of the OTI system.

10.4 References

[1] X2R2 D4.1 Train Integrity Concept and Functional Requirements Specifications, 2019.
[2] X2R2 D4.2 Functional architecture & Interfaces specifications & Candidate technologies selection, 2019
[3] CR940 – Modifications related to Train Integrity functionalities, 14.06.2017.
[4] Mohamed Ghazel, Formalizing a Subset of ERTMS/ETCS Specifications for Verification Purposes, Transportation Research Part C - Emerging Technologies, Elsevier, vol. 42, pp. 60-75, 2014.
[5] Gerd Behrmann, Alexandre David, and Kim G. Larsen, A Tutorial on Uppaal 4.0, Update of November 28, 2006.
[6] Rajeev Alur and David L. Dill, A Theory of Timed Automata, Theoretical Computer Science No. 126, pp. 183-235, 1994.

10.5 Authors

Insaf Sassi has received the engineering degree from the National School of Computer Sciences (ENSI), Tunisia, in 2014; the master's degree in control systems from Ecole Centrale Lille, France, in 2014; and the Ph.D. degree in control systems from University of Grenoble Alpes in 2017. She joined Railenium as post-doctoral fellow in 2018 to work on RAMS analysis. Her research deals with dependability and safety analysis. She is working on safety analysis of onboard train integrity and GNSS-based positioning system in train control applications.

insaf.sassi@railenium.eu.es

Mohamed Ghazel is research director with the COSYS/ESTAS team at IFSTTAR. He received the Master's and Ph.D. degrees in automatic control and industrial computer sciences from École Centrale de Lille in 2002 and 2005, respectively; and the Habilitation à Diriger des Recherches from University Lille Nord de France in 2014. He specialises in safety and interoperability analysis of transportation systems using discrete models. He is member of the IFAC TC 7.4 on Transportation Systems, has been involved in several national and European research projects and acts as expert for the European Commission in the framework of innovation programs.

mohamed.ghazel@ifsttar.fr

El-Miloudi El-Koursi is a Research Director at IFSTTAR. He has 30 years experiences in performing assessment and certification of safety related rail and associated systems. He obtained in 1985 his Ph.D in Automatic control and industrial computer sciences at University of Lille. In recent years, he has been involved in various European projects. He was the leader of European FP5, SAMNET "Safety Management and interoperability thematic network" thematic network. He is the vice chairman of EURNEX.

el-miloudi.el-koursi@ifsttar.fr

11 Test Case Generation for a Level Crossing Controller

Daniel Schwencke, German Aerospace Center (DLR), Institute of Transportation Systems, Braunschweig, Germany

11.1 Introduction

Formal methods (FM) can be used for the precise specification, property-ensuring development and exhaustive property verification of systems. Thus they are especially suited for highly safety or mission critical applications. Railway signaling systems clearly belong to these applications, and there are indeed several industrial projects where FM have been successfully applied; especially to core interlocking and communication-based train control (CBTC) systems. But despite their potential, FM are not very wide-spread in the sector. Several studies [1, 2, 3] regarding their diffusion have been conducted. The main determinants for adoption that emerge from those studies are

- the maturity of available tools,
- the learnability of the tools (learning curve),
- the perceived benefits-of-use and perceived ease-of-use by engineers and professionals, and
- the compatibility with already existing tools or toolchains.

Also, the choice of a method and tool among the many different FM available can require high expertise. According to some of the studies, the cost of the potential tools to be used appears to not be an essential determinant.

Work Package 5 of the X2Rail-2 project seeks to foster the use of FM in railway signaling by providing an introduction and overview of formal methods [4] and demonstrating their use and benefit. For the latter, four different formal and one classical development methods are applied by different project partners to a level crossing (LX) controller specified by the Swedish railway infrastructure manager Trafikverket. This includes

- the refinement-based B method,
- model-based design with SCADE,
- configuration-based development with Prover iLock, and
- contract-based programming in SPARK

for formal development as well as the ladder logic-based Westrace system for the classical development. For all of these developments, the safety properties from the LX specification are planned to be formally verified afterwards using the High Level Language (HLL). Since that means proving them exhaustively, they are of less interest for testing.

However, there are further non-safety functional requirements in the specification which remain for testing. The extended abstract at hand reports on an automatic test case generation (TCG) approach of a test suite testing these requirements. In fact, this approach is based on

formal methods as well, since the test case generator applies symbolic execution and theorem solving techniques: given a behavioral model of the system under test (SUT), the former method finds feasible paths through the model, while the latter completes the test case by determining suitable test data. This way, the test design task is partly automated, ensures a structural coverage of the model and the modeling process usually leads to a high test suite quality. The different LX controller implementations are tested as black box systems, each one with the same generated test cases. In order to simplify the integration of the different implementations with the test environment, a common test interface has been drawn up.

11.2 Overview of the Approach

11.2.1 Tooling

For the work presented here, the "Automatic Test Generation" (ATG) Add-On [5] of the UML/SysML tool Rational Rhapsody of IBM is used for the TCG. This, in turn, is based on the "TestConductor" Add-On [5]. Altogether Rhapsody and the two add-ons form a tightly integrated environment, which covers the whole model-based testing process starting from model creation (Rational Rhapsody), covering TCG (ATG Add-On) and stretching to test execution (TestConductor Add-On). All of this is proprietary, commercial software. Rhapsody version 8.4 is used, running on a Windows 10 PC.

Reasons for the choice of Rhapsody ATG included its high flexibility (e.g. broad support of SysML elements and code constructs) and the integrated tool chain from model creation to test execution. Different tools for system model based TCG like Conformiq Designer or RT-Tester MBT exist, having different strengths like more options to influence the TCG algorithm or supposedly better performance. Also, different FM and semi-FM tools like ProB or Simulink come with TCG capabilities, but usually bound to a special modelling language (as opposed to the wide-spread multi-purpose UML/SysML languages).

11.2.2 Process

In Figure 11-1 the steps the steps of the test generation (left-hand side) and test execution (right-hand side) are shown. The tools used for the single steps are given in the white boxes attached to each step. While many steps are largely automated, the main manual effort lies in the "TCG Model Creation", and – in our case, due to testing of several external SUT – also in the "Implementation Integration". The most important steps are described in the next section below.

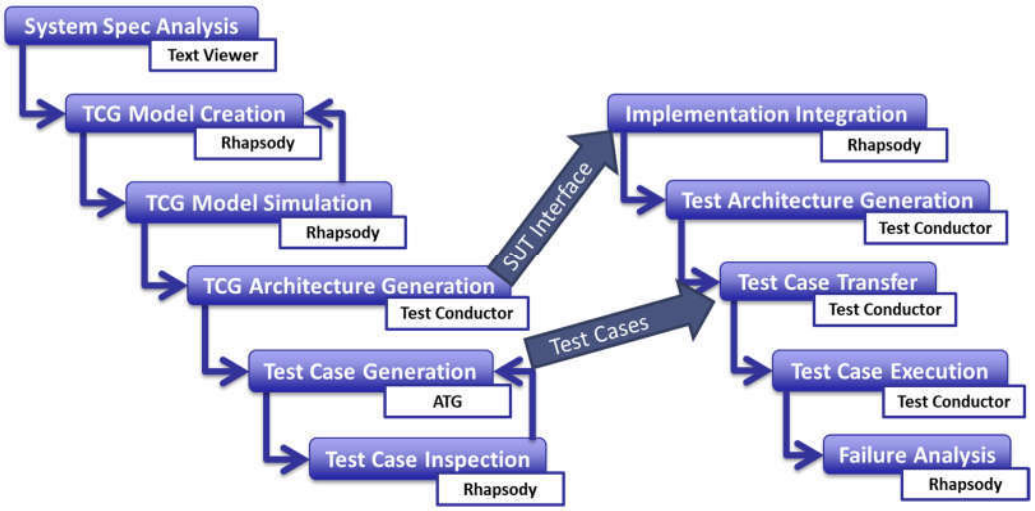


Figure 11-1: Test generation and execution process with Rhapsody and Add-Ons

11.3 Application to the LX Controller

11.3.3 Application Example: The Alex Level Crossing

As an application example for the formal methods mentioned in the introduction and for the TCG an LX controller was chosen by the work package participants. The specification by Trafikverket of the system called "Alex" is relatively recent and the system is supposed to replace several types of existing LX in Sweden in the future. For the work packages' purposes, the scope was limited to the variant controlled by an interlocking (no autonomous LX / no private road barriers), which reduced the 375 requirements to 133 requirements in scope. The functions in scope include the interfaces to interlocking, a local control box and speed sensors as well as the control of road-facing lights, barriers, sound, obstacle detection and track-facing signals. Many of these features are configurable in the number and variant of the controlled objects as well as in some delays. An average LX configuration amounts to a system complexity of about 40 Boolean inputs and 50 Boolean outputs.

11.3.4 TCG Model Creation

At first sight, the creation of the executable SysML system model for the TCG is similar to model-based system development. External interface, the system environment, its structure and its behavior (mainly as SysML statecharts) need to be modeled, as well as requirements that should be traceable and configurations that should be supported. However, a test model should abstract from the real system behavior, e. g. by means of aggregation or omission (in order to reduce the number and length of the generated test cases). On the other hand it is also legitimate to explicitly model behavioral variants that are implicit in an implementation (in order to force generation of corresponding test cases). The statechart modeling the behavior for control of the track-side LX components (signal and distant signal) is shown in Figure 11-2.

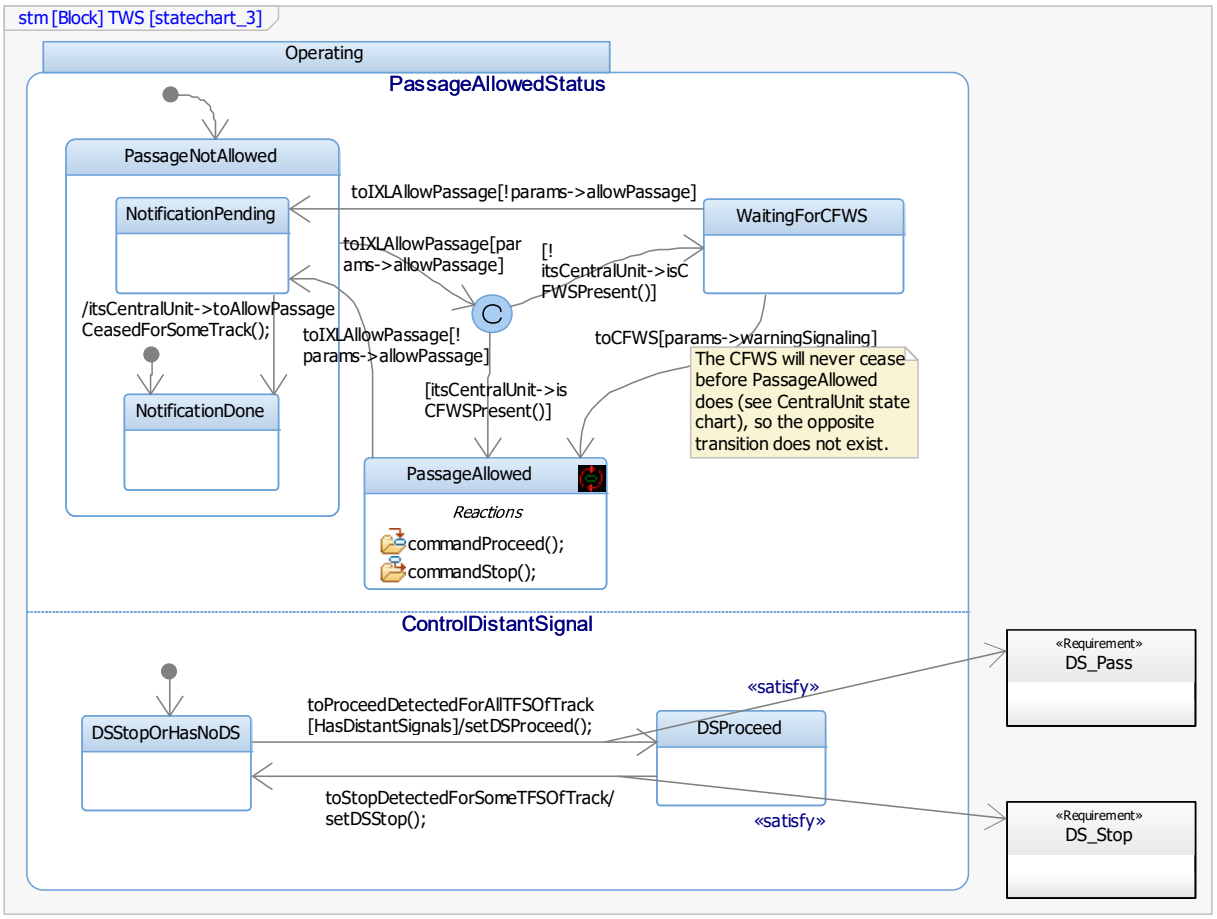


Figure 11-2: Behavior of trackside LX components control as SysML statechart. Requirements on distant signal control are linked to transitions according to the LX specification (which seems to require that distant signal control depends on detected rather than commanded main signal aspect).

11.3.5 Test Case Generation

In the "TCG Architecture Generation" step, which is a prerequisite for the TCG step, the SUT part of the model is fixed. Based on this, one defines the sub-interfaces of the SUT that should be used for stimulation (input interface) and recorded (input and output interface) by the generator. Also, one can choose whether Rhapsody ATG will try to reach structural coverage of the model (states, transitions, and operations), coverage of the generated C++ code (modified condition/decision coverage), or both. The current coverage of the different elements is displayed by ATG during generation, see Figure 3. The resulting test cases can be displayed as sequence diagrams in Rhapsody. They can be edited and completed by further generated or manually designed test cases. An example of a resulting test case is shown in Figure 11-4.

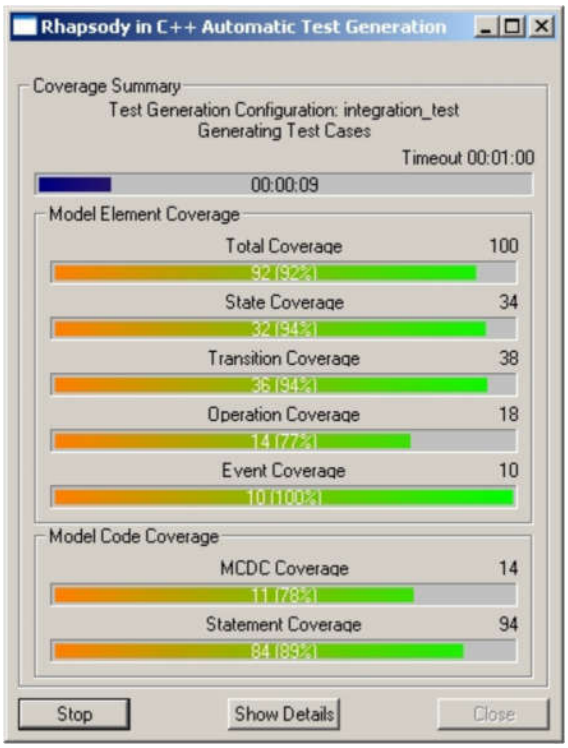


Figure 11-3: Status window shown by ATG during TCG (taken from [3], p. 52)

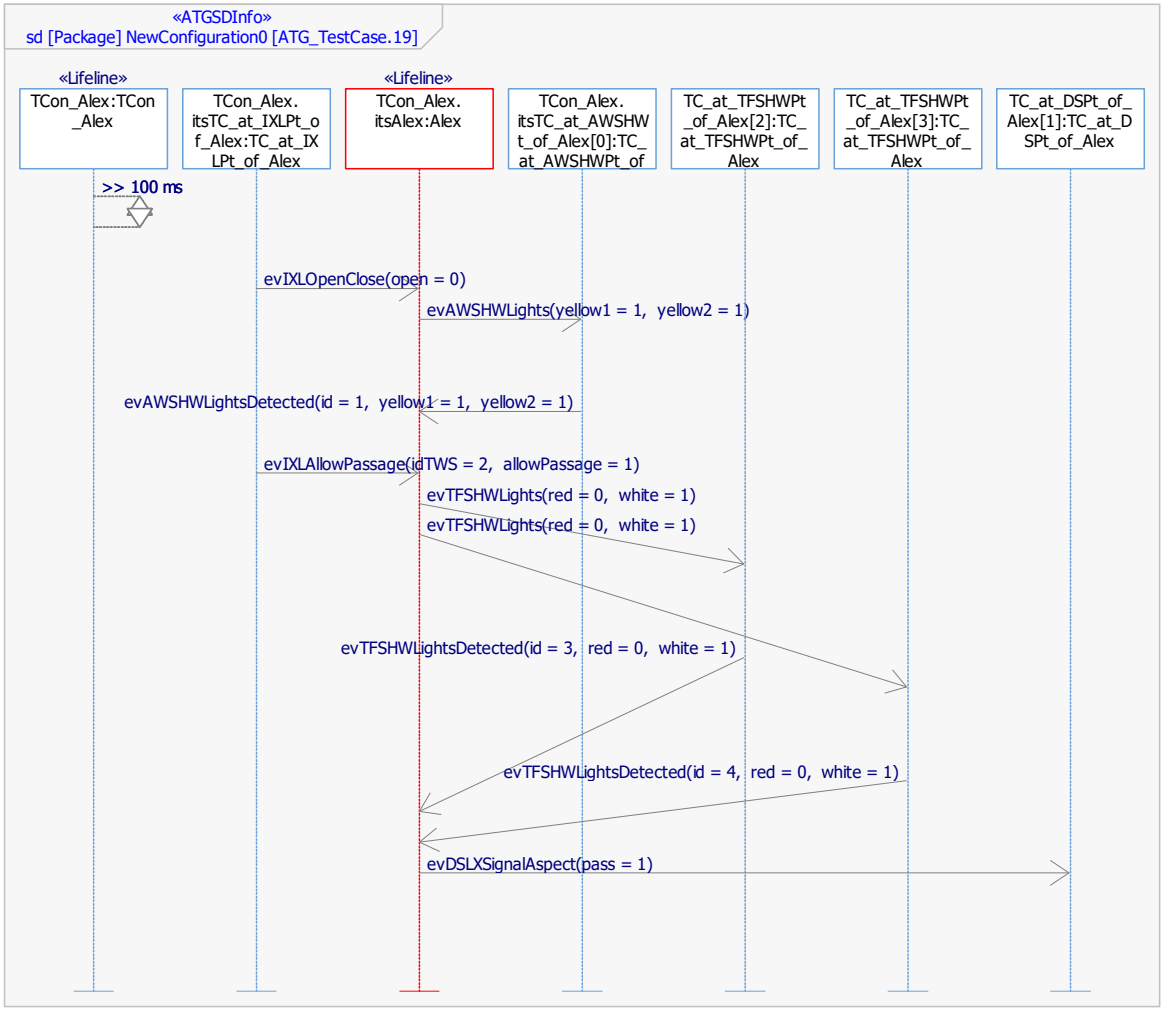


Figure 11-4: Test case generated by ATG as SysML sequence diagram

11.3.6 Implementation Integration

Rhapsody TestConductor provides convenient means to execute the test cases generated by ATG on a Rhapsody model. In our case, we use TestConductor to execute the generated test cases on the different external software implementations. To this end, a test interface suitable for all implementations under test has been defined in discussion with the developers involved. Several issues needed to be solved:

1. The general mismatch between the relay-based LX interface and the message-based test environment was resolved by means of an implementation wrapper common for all implementations.
2. Some implementers work with real-time execution frameworks, while others prefer to work with an execution-independent fixed cycle time. This was resolved by transmission of the "implementation time" to the test environment each cycle, by adapting the test environment to use that "external clock", and by keeping the TCG model independent of the Windows system clock.
3. Different programming languages are used by the test environment (C++) and the implementations (generated C code, Ada code, Westrace simulator executable). This was resolved by compiling the implementations into libraries linked by the test environment, or by using another (C++) wrapper in the Westrace case that was compiled together with the test environment.
4. While controlling single cycles of LX implementations from the test environment would be possible for the formal developments, this is not possible for the Westrace simulator. Thus, shared memories for the input and output data for the implementations were set up together with mutual exclusive access from the test environment and the implementation side.
5. The test interface needs to be able to cope with different system configurations that affect the interface (the number of Boolean in- and outputs to transmit). Here, the interface was laid out to cover an agreed fixed maximum number of configured objects such as signals or barriers.

Altogether those issues and the underlying technical details required quite some discussions, clear conceptual work and more effort than expected initially. Nevertheless, it also saves from some effort since the test execution framework of TestConductor can directly be used (simple automated test execution) and only one test interface needs to be defined, maintained and considered during test execution / failure analysis. The test interface did not require any additional behavior of the implementations apart from reading inputs and writing outputs each cycle, including a few test control in-/outputs consumed/generated on the control cycle level.

11.4 Discussion of the Approach

Currently, first test cases have been generated and executed on an implementation, confirming that our approach is feasible. Yet, no comprehensive test results are available. However, having run through the complete process depicted in Figure 11-1, we can already report on several topics that seem crucial to us:

System abstraction (TCG model creation step). Since the model for TCG is a system model and is moreover required to be executable, this may push the modeler towards modeling an implementation. This can easily lead to spending time on modeling behavior not needed for testing or to unacceptably long test generation time. It can also lead to particular interpretations of the specification, which may result in unjustified failing tests. It seems advisable to start with clear test goals and system scope, check requirements thoroughly and either make them precise or indicate intentionally left room for interpretation, simplify the external system interfaces as much as possible, and then fix a set of environment assumptions. After that, abstractions of the system behavior can be made and modeled, which sometimes is non-trivial due to interdependencies. Here it is helpful to think in terms of system functions rather than in architectural structures. One rather simple behavioral abstraction made in the LX example was to consider only "normal" behavior as a first step; failure scenarios may be added later.

Managing model configurations and variants (TCG model creation). We decided to create a "150% model" (i.e. there is one model which contains the behavior for all the configurations and variants), which can be arbitrarily configured and where the environment model can be varied through variant points. This leads to less redundancy and better maintainability than individual models, but also leads to a more cluttered model and usually to less than 100% structural coverage by the tests generated for a particular configuration.

Model validation (TCG model simulation). It is important that the TCG model is validated. Rhapsody offers interactive simulation of a model, which is a nice visual tool to check particular model behavior. Also, the modeling process itself often guides the modeler to think about possible issues, and several later steps (Rhapsody's model consistency check, compilation of the generated code, test case inspection) may uncover problems in the model. However, a more direct validation of the model against the requirements has not been performed in our case; at least attaching the tested requirements to model elements made the modeler think about the realization of those requirements in the model.

Scalability (test case generation). It is well-known that many formal methods have high algorithmic complexity. This also applies to TCG with ATG: the time needed to generate a test suite that fully covers the model quickly rises with growing model size. One important factor is the complexity of the model's input interface. Here the relay-based LX interface has proven advantageous, since it consists of a series of wires that can be modeled by simple Boolean values. So far, the generation time has not exceeded a couple of minutes, so that it is estimated to stay within reasonable range also for the future completed model. Note that in ATG the interface can be further restricted by choosing messages and parameter values in a flexible manner for each TCG run, and by modeling environment restrictions in the test components connected to the input interface. A second factor is the complexity of the behavioral model itself; in particular deep nesting may increase generation time. The TCG output complexity (number and size of test cases) seems unproblematic (so far around 20 test cases with an average of less than 10 steps). Test cases that are prefix of another one are automatically removed. Other redundancies may occur, but seem rather insignificant.

Managing implementation variants, versions and configurations (implementation integration to failure analysis). In the given project context, the five different implementations were prepared in four different configurations, amounting to 20 systems under test. In order

to be able to adapt test cases individually if necessary, and not to mix test results, it was decided to create 20 separate test architectures for them (which is an automated process in Rhapsody). The test suite for the corresponding configuration needs to be copied into the architecture. Each architecture comes with a code generation component where the library containing the implementation/configuration combination of interest can be selected. Also variants of modeled variation points can be chosen here, a possible mechanism to choose the right variant of the (configuration dependent) implementation wrapper. If, in addition, one considers that several versions of the 20 SUT may be released over time, and different test suites may be generated for them, it becomes apparent that thorough planning of the project structure in Rhapsody is of utmost importance for efficient test execution. Regarding the different test suites for different configurations and resulting from different environment models, a similar planning is necessary for the test generation.

11.5 Conclusion

The work on TCG from an LX controller model within the X2Rail-2 WP5 indicates that such an approach can be successfully applied to mid-sized signaling systems. Rhapsody and its testing add-ons provide an integrated, flexible and largely automated framework to create a system model, generate tests from it and execute them. The model-based process followed seems to supports a good quality of the central model, although in our case no extensive validation against the system requirements was performed.

The effort and costs to set up and apply such a process for the first time may be high; training and tool support will be necessary. Also finding the right abstraction level for a system model can be challenging, and it still might be necessary to add some test cases by hand. However, there are convincing benefits:

- Creating a system model often uncovers problems in the system requirements specification early which can save from costly iterations in development, and human error during test design is reduced.

- Since the generated test cases cover the elements of the model they are generated from (which are typically more fine-grained than requirements), they have the potential to detect more errors than those manually designed (covering the mere requirements).

- To have the main portion of functional test cases ready in a model will pay off whenever changes need to be made to the test suite – no matter if during initial development, maintenance or while creating new product version. The central place to implement those changes is the model – and an automatic regeneration of the test cases will consistently apply the change to the suite.

- A cross-platform and implementation-approach-independent test suite with a standard interface allows for reuse (possibly including its further development in future projects).

In the remainder of the project, our claim that the TCG scales well for the LX application needs to be confirmed as soon as the model is completed. It will be interesting to see how many errors will be detected during the execution of the generated test cases on the different

implementations, and how model-based testing and formal verification complement each other. Further research will be necessary to try out the limits of the ATG test case generator to compare with manually created test suites and to generate further kinds of tests, e.g. for failure scenarios.

The work on TCG from an LX controller model within the X2Rail-2 WP5 indicates that such an approach can be successfully applied to mid-sized signaling systems. Rhapsody and its testing add-ons provide an integrated, flexible and largely automated framework to create a system model, generate tests from it and execute them. The model-based process followed seems to supports a good quality of the central model, although in our case no extensive validation against the system requirements was performed.

The effort and costs to set up and apply such a process for the first time may be high; training and tool support will be necessary. Also finding the right abstraction level for a system model can be challenging, and it still might be necessary to add some test cases by hand. However, there are convincing benefits:

- Creating a system model often uncovers problems in the system requirements specification early which can save from costly iterations in development, and human error during test design is reduced.
- Since the generated test cases cover the elements of the model they are generated from (which are typically more fine-grained than requirements), they have the potential to detect more errors than those manually designed (covering the mere requirements).
- To have the main portion of functional test cases ready in a model will pay off whenever changes need to be made to the test suite - no matter if during initial development, maintenance or while creating new product version. The central place to implement those changes is the model - and an automatic regeneration of the test cases will consistently apply the change to the suite.
- A cross-platform and implementation-approach-independent test suite with a standard interface allows for reuse (possibly including its further development in future projects).

In the remainder of the project our claim that the TCG scales well for the LX application needs to be confirmed as soon as the model is completed. It will be interesting to see how many errors will be detected during the execution of the generated test cases on the different implementations, and how model-based testing and formal verification complement each other. Further research will be necessary to try out the limits of the ATG test case generator, to compare with manually created test suites and to generate further kinds of tests, e.g. for failure scenarios.

11.6 References

[1] S. Bacherini, A. Fantechi, M. Tempestini, and N. Zingoni, "A Story About Formal Methods Adoption by a Railway Signaling Manufacturer," in Lecture Notes in Computer Science, vol. 4085, 2006, pp. 179–189. https://doi.org/10.1007/11813040_13

[2] D. Basile et al., "On the Industrial Uptake of Formal Methods in the Railway Domain," in Lecture Notes in Computer Science, vol. 11023, 2018, pp. 20–29. https://doi.org/10.1007/978-3-319-98938-9_2
[3] M. H. ter Beek et al., "Adopting Formal Methods in an Industrial Setting: The Railways Case," in Lecture Notes in Computer Science, vol. 11800, 2019, pp. 762–772. https://doi.org/10.1007/978-3-030-30942-8_46
[4] Formal Methods (Taxonomy and Survey), Proposed Methods and Applications. Public Deliverable 5.1 of X2Rail-2, revision 1.5 from 16/05/2018, available at https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-2
[5] TestConductor and ATG Web documentation on the IBM website, https://www.ibm.com/support/knowledgecenter/en/SSB2MU_8.4.0/com.btc.tcatg.user.doc/topics/com.btc.tcatg.user.doc.html, accessed on 13/11/2019 3:50 pm.
[6] IBM® Rational® Rhapsody® Automatic Test Generation Add On User Guide, Release 3.6.2

11.7 Author

Daniel Schwencke graduated in Computer Science and received his PhD from the Technical University of Braunschweig. In 2011 he joined the DLR Institute of Transportation Systems as researcher, working in the field of railway safety, including system development and authorization processes as well as human reliability. Since 2015 he is part of the verification and validation department, conducting research on model based testing of signaling systems and test automation. He is involved in the European X2Rail-2 project.

daniel.schwencke@dlr.de

12 Decomposition-based integer programming for coordinated train rerouting and rescheduling

Peng Guo; IRT RAILENIUM, Famars, France
Paola Pellegrini, Joaquin Rodriguez; IRT RAILENIUM, Famars, France & IFSTTAR, COSYS, LEOST, Villeneuve d'Ascq, France
Raffaele Pesenti;Dept. of Management, Università Ca' Foscari Venezia, Venice, Italy

12.1 Introduction

We deals with a collaborative train rerouting and rescheduling problem faced by traffic controllers at regional railway control centers. Typically, the railway network is divided into non-overlapping control areas. And each control center coordinates several control areas. This problem arises when a perturbation (i.e., an unexpected, degraded operation) occurs and the timetable cannot be operated as planned. This implies that either timing or routes of trains have to be modified in order to optimize the given objective, e.g. minimizing the total delay.

For each control center, the real-time traffic management is hierarchically organized into two decision levels. At the lower level, the dispatchers only manage local schedules and routes of train movement in their own control areas for minimizing the deviation from the timetable. However, the local schedules often may not be optimal for a global view and maybe even incompatible for the train schedules of other areas. At the higher level, a network coordinator is responsible for ensuring the compatibility of dispatchers' rescheduling decisions over two or more areas and controls the rescheduling decisions taken by dispatchers. In general, the coordinator is mainly interested in controlling the trains traversing multiple control areas and in taking decisions at the border sections between areas, while real-time traffic management in the control areas is left to the corresponding dispatchers. In this case, the coordinator may impose constraints to the local solutions provided by the dispatchers.

This problem is known in the literature as real-time Railway Traffic Management Problem (rtRTMP) [3]. Several approaches have been proposed to deal with it [2]. Differently, only few papers focus on the coordination of traffic management across control areas. In particular, [1] proposes to use branch and bound to solve both the single dispatcher and the coordination problem at once, using bi-level optimization theory. Here, we aim to propose a general coordination framework in which the single dispatcher problem can be solved through virtually any approach among those proposed in the literature. Only the addition of some constraints or the slight modification of the objective function is considered possible to achieve coordination. This generality has the advantage of allowing the use of the most suitable approach for each control area, for example considering a microscopic or mesoscopic representation of the infrastructure depending on the layouts.

12.2 Problem description

13 The railway network is subdivided into m non-overlapping control areas which are traversed by a set of trains according to a given timetable. In each area a dispatcher manages schedule and routes of train movements. The borders between control areas represent the

coordinator space. When movements traverse two or more control areas, the coordinator has direct decision making power, or expresses preferences, on:

1. times at which trains leave or enter control areas;
2. locations crossed to move from one area to the next one;
3. precedence between trains entering or leaving areas.

Through these constraints and preferences, the coordinator aims to make dispatchers' decisions coherent. It can also compensate some time incoherences by controlling trains speed on the lines that join two adjacent but separated areas. It is assumed that the dispatchers, when they reroute and reschedule trains, collaborate with each other through the coordinator to reach a new schedule. In particular, they are required to find at least a feasible schedule for all trains, if it exists. They share the common objective of making trains meet their planned schedule as much as possible. Each dispatcher applies this general objective to the movements of trains that occur within its area. The coordinator applies this general objective to trains crossing different areas. In particular, it aims at making these trains to meet their schedules along their complete routes, not only in some particular area. Then, lexicographically, it may apply a fairness criterion which requires that no area is excessively penalized: the coordinator should distribute the burden of managing delays so that it does not fall on just a few dispatchers.

13.1 Logic-based Benders Decomposition

Logic-based Benders decomposition (LBBD) is a substantial generalization of classical Benders decomposition that, in principle, allows the sub-problems (including master problem and slave problem) to be any optimization problem rather than specifically a linear or nonlinear programming problem. LBBD provides a natural means to combine different kinds of problem formulations and solvers. The LBBD algorithm iterates between the master problem (MP) and the slave problem (SP) until their solutions converge. Since the MP is a relaxation of the original problem, its optimal solution at each iteration is a lower bound for the original model with the minimization objective function, whereas the solution value of the SP is the best upper bound for the MP's solution. The optimality of the original problem is obtained if the two bound converge. At each iteration, if not optimal, the information of SP solution is passed to the MP by optimality and feasibility cuts.

We propose to use Logic-based Benders Decomposition (LBBD) [4] to solve the problem of coordinating dispatchers' decisions. LBBD is a substantial generalization of classical Benders decomposition that, in principle, allows the slave problems to be any optimization problem rather than specifically a linear or nonlinear programming problem. LBBD provides a natural means to combine different kinds of problem formulations and solvers. In the proposed LBBD framework, we set the coordination problem as master problem and the dispatching problems as slave problems, as shown in Figure 12-1.

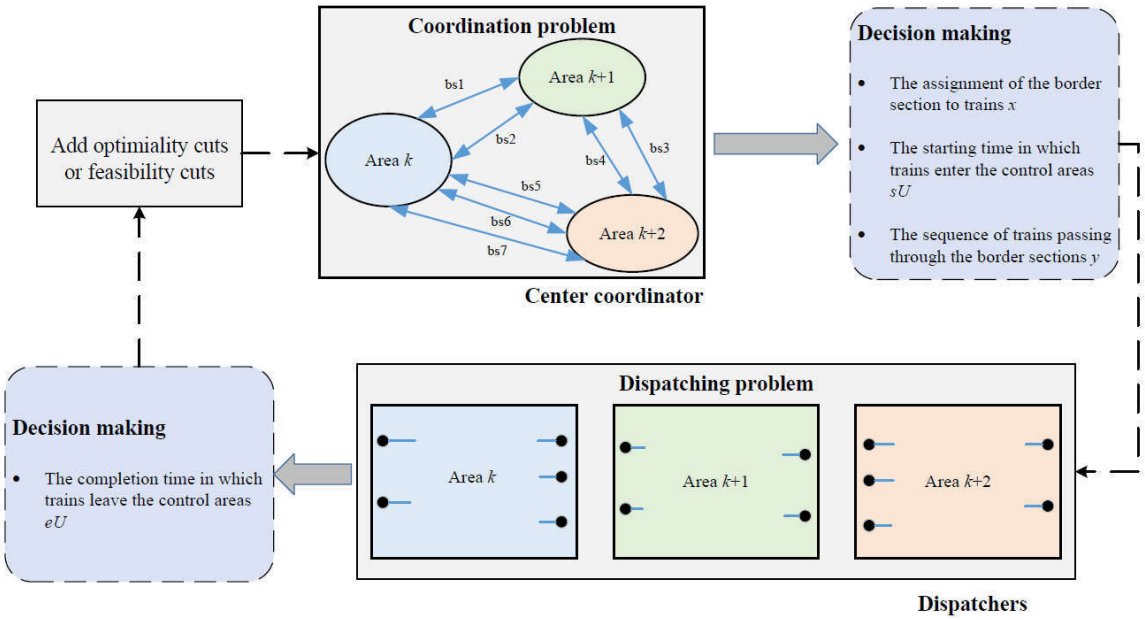


Figure 12-1: The proposed logic-based Benders Decomposition

As in classical Benders decomposition, the output of the master problem is the input of the slave problems. Based on this input, the slave problems are solved. If all slave problems can be solved, that means the master problem generates a feasible schedule for all trains. If the objective value of the master problem is greater than or equal to the maximum objective value of the slave problems, the algorithm stops with the global optimality. If there is an infeasibility observed in some slave problem, we also need to add some constraints to the master to change its output. Otherwise, optimality constraints will be added to drive the master problem towards better and better solutions. Then, the process continues iteratively until a stopping criterion related to computational time or number of iterations is reached.

In our application, the coordinator problem is solved and train timings, border section crossings and passing sequences are passed to dispatchers. The latter solve the rtRTMP considering these inputs as (hard or soft) constraints and return the value of the objective function or the infeasibility of the instance. Consequently, cuts are added to the coordination problem, which is then is solved again to obtain a better solution.

Based on the preliminary test, the proposed approach seems promising for medium and large-size instances.

13.2 Reference:

[1] Francesco Corman, Andrea D'Ariano, Dario Pacciarelli, and Marco Pranzo. Optimal interarea coordination of train rescheduling decisions. Transportation Research Part E : Logistics and Transportation Review, 48(1) :71 – 88, 2012.

[2] Wei Fang, Shengxiang Yang, and Xin Yao. A survey on problem models and solution approaches to rescheduling in railway networks. IEEE Transactions on Intelligent Transportation Systems, 16(6) :2997–3016, 2015.

[3] Paola Pellegrini, Grégory Marlière, Raffaele Pesenti, and Joaquin Rodriguez. Recife-milp: An effective milp-based heuristic for the real-time railway traffic management problem. IEEE Transactions on Intelligent Transportation Systems, 16(5) :2609–2619, 2015.

[4] J.N. Hooker and G. Ottosson. Logic-based benders decomposition. Mathematical Programming, 96(1) :33–60, 2003.

13.3 Authors

Peng Guo obtained his BS degree in Industrial Engineering and PhD degree in Mechanical Engineering from Southwest Jiaotong University in 2009 and 2014, respectively. He is currently a lecturer with School of Mechanical Engineering, Southwest Jiaotong University. He is actually attached to the Railenium test and research center as a Postdoctoral fellow. His research interests include engineering optimization, production scheduling, service operation management and railway traffic management.

Peng.Guo@railenium.eu

Paola Pellegrini received the Ph.D. degree in mathematics for economics from Ca' Foscari University, Venice, Italy, in 2007. She is currently a Research Director at the Université Gustave Eiffel (ex IFSTTAR), Lille Campus, France. She has been a Visiting Researcher at the University of Arizona (USA) and a Postdoctoral Researcher at the University of Trieste and Ca' Foscari University (Italy) and at the research institute IRIDIA (Belgium). She has participated in research projects in the field of mathematical optimization, air traffic management, and railway transportation. She has published the results of her research studies in several scientific journal articles, book chapters, and conference papers.

paola.pellegrini@univ-eiffel.fr

Joaquin Rodriguez received the Ph.D. degree in computer science at the University of Compiègne, Compiègne, France, in 1985. He is a Research Director at the Université Gustave Eiffel (ex IFSTTAR),Lille Campus, France. He is responsible for the traffic management team. He has 20 years of experience in coordinating industrial and academic research projects dealing with railway traffic management, capacity analysis, diagnosis, and safety. He has developed several decision support tools in transportation applications: real-time train circulation

management in railway nodes, simulation of guideway transit systems, and model-based diagnosis of electronic devices.

joaquin.rodriguez@univ-eiffel.fr

Raffaele Pesenti received the Ph.D. degree in systems sciences at the University of Genova, Genova, Italy. He is a Full Professor of operations research at the Department of Management, Ca' Foscari University, Venice, Italy. His major area of research is management of complex systems with application in transportation and logistics. The interests in this field are devoted to the study of the strategic and analytical elements of the systems design and to the development of models and methods that may find application in the day-by-day operations. His works appear on some of the highest impact journals in the field.

pesenti@unive.it

14 Moving Block Risk Evaluation

Stefanie Schöne, Michael Meyer zu Hörste; German Aerospace Center (DLR), Institute of Transportation Systems, Braunschweig, Germany
Mario Alonso-Ramos; Siemens Mobility Limited, Chippenham, United Kingdom

14.1 Introduction

This contribution provides an overview of the past and current works of the safety works in the X2Rail Projects Moving Block Work Packages, focusing on the identification and evaluation of risks inherent to systems following the ETCS Level 3 specifications.

14.2 Structure and contents of the X2Rail Moving Block Works

One goal of Shift2Rail is to provide demonstrators that implement European Train Control System (ETCS) Level 3 Moving Block systems. These systems shall conform to the existing ETCS specifications. However as the specifications apply to all levels of ETCS, some of these requirements have to be stated more precisely for Level 3 to reach the level of detail needed to develop individual, interoperable ETCS systems. To aim for the different needs of the market, several prototypes are to be developed up until X2Rail-5 for different railway operation systems (High speed, urban, freight and overlay systems) as well as the four railway types:

- Full Moving Block with and without Trackside Train Detection (TTD) and
- Fixed Virtual Blocks with and without TTD

To be operated in the European railway market, a new system has to be certified by the European Railway Agency. One crucial part of this certification is the proof of safety. Therefore, a process of risk management has been implemented on European level that follows the risk oriented approach of safety evaluation, using so-called Common Safety Methods (CSM). To make sure to begin the risk management as early in the system development process as possible, it is flanking the other works of the Moving Block Work Package along the whole project runtime.

The first results of the Moving Block works, and the basis for the further works in X2Rail-3 including the risk evaluation presented in this contribution, were the following Deliverables of X2Rail-1:

- D5.1 Moving Block System Specification
- D5.2 Moving Block Operational and Engineering Rules
- D5.3 Moving Block Preliminary Safety Analysis
- D5.4 Moving Block Application Analysis

14.3 Risk evaluation

14.3.1 Approach and Methodology

Starting with a Preliminary Hazard Analysis (PHA) in X2Rail-1 [1], the works in the Moving Block Work Packages in X2Rail-3 follow the standardized risk-oriented approach of safety evaluation, using the Common Safety Methods, as mandated by the European Legislation [2].

After defining and confining the examined system, in a PHA systematically possible hazards are identified (for the methodical approach see [1]). In the next step these hazards are then assessed in respect of their expected frequency and severity estimated according to tables that are shown in the Figures 13-1 and 13-2.

Frequency level	Description
Frequent	Likely to occur frequently. The event will be frequently experienced.
Probable	Will occur several times. The event can be expected to occur often.
Occasional	Likely to occur several times. The event can be expected to occur several times.
Rare	Likely to occur sometime in the system life cycle. The event can reasonably be expected to occur.
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.

Figure 14-1: Categories of hazard frequency levels

Severity category	Consequences to persons or environment	Consequences on service/property
Catastrophic	• Affecting a large number of people and resulting in multiple fatalities, and/or • extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	• Affecting a very small number of people and resulting in at least one fatality, and/or • large damage to the environment	Loss of a major system
Marginal	• No possibility of fatality, severe or minor injuries only, and/or • minor damage to the environment	Severe system(s) damage
Insignificant	• Possible minor injury	Minor system damage

Figure 14-2: Severity categories

The resulting risk is estimated and evaluated according to a risk matrix that is also part of the CSM and shown in Figure 13-3.

Frequency of occurrence of an accident (caused by a hazard)	Risk Acceptance Categories			
Frequent	Undesirable	Intolerable	Intolerable	Intolerable
Probable	Tolerable	Undesirable	Intolerable	Intolerable
Occasional	Tolerable	Undesirable	Undesirable	Intolerable
Rare	Negligible	Tolerable	Undesirable	Undesirable
Improbable	Negligible	Negligible	Tolerable	Undesirable
Highly improbable	Negligible	Negligible	Negligible	Tolerable
	Insignificant	Marginal	Critical	Catastrophic
	Severity of an accident (caused by a hazard)			

Figure 14-3: Risk matrix used for risk evaluation

If a risk is found to be undesirable or even intolerable, risk mitigation measures for future Moving Block implementations have to be proposed to lower the risk to an acceptable level. That can be additional system requirements or the implementation of operational procedures.

14.3.2 Assumptions and constraints

The works in the Moving Block safety evaluation task in the X2Rail projects is carried out to assess ETCS Level 3 risks. Therefore, risks that occur in other ETCS Levels are not considered, only such inherent to solely Moving Block systems.

The Moving Block system, as it is defined in the X2Rail projects, comprises the ETCS Level 3 Trackside, including interlocking and Radio Block Center, and the ETCS On-board system. A detailed system description containing boundaries of the evaluated system as well as interfaces to other ETCS system components, as for example the Train Integrity Management System (TIMS), the driver and Traffic Management, is conducted in [1]. The assumed functions and characteristics of the Moving Block systems are in line with the system definitions and requirements carried out in the works of the X2Rail Moving Block Work Packages

Further assumptions of the functionality of ETCS Level 3 systems that were made within the scope of the risk evaluation are

- No signals – unless required at boundaries
- No TTD – unless required e.g. at boundaries, points, or because System Type with TTD has been selected
- Level 3 Trackside uses Train Position Reports as primary source of information on train location, used to determine Track Status
- Level 3 Trackside controls points, locks routes, and issues Movement Authorities up to next obstruction
- All trains fitted, including with TIMS, unless 100% TTD.

14.3.3 Previous and actual results

An overview of ETCS Level 3 Moving Block hazards that were identified in the PHA carried out in X2Rail-1 is shown in Table 13-1. They are described in detail in [1].

Table 14-1: Identified Moving Block Hazards and their causes for, from PHA [1]

Identified Hazards	Possible Causes
1. Track status erroneously cleared	1.1 Dispatcher interaction in L3 Trackside initialization 1.2 Using invalid/outdated information for L3 Trackside initialization 1.3 Deactivating shunting area 1.4 Driver confirms train integrity 1.5 Recovery of a failed train
2. Error in train location	2.1 Confidence interval reduced at End of Mission 2.2 Lack of linking information
3. Error in train length	3.1 Reported train length shorter than actual 3.2 Reported train length longer than actual
4. Cold Movement Detection erroneously validates position	4.1 Wrong side failure in CMD
5. Undetected movements	5.1 Rollback after standstill 5.2 Movement in NP (“no Power”) mode 5.3 At entrance to Level 3 area 5.4 After End of Mission 5.5 Loss of train integrity 5.6 Propelling train 5.7 Shunting train
6. TTD erroneously indicates track clear	6.1 Wrong side failure of TTD
7. Points moved under train	7.1 Points moved after communication failure

Currently in X2Rail-3 Workshops with European railway experts are conducted to carry out the CSM risk evaluation process explained above. At this moment definitive conclusions are still to be assembled, but for example following first tendencies could be observed:

For most hazards the assumed severity category is catastrophic, including pure freight lines, as accidents could result in extreme damage to the environment (compare Figure 13-2).

The different railway operation systems (high speed, freight, etc.) have no impact on the assumed severity category, but can have an impact on the assumed frequency level, influencing the resulting risk assessment in this way.

For systems with TTD many hazards can be evaluated the same way as in ETCS Level 2 systems, therefore excluded from further X2Rail evaluations.

14.4 Outlook

The next step in the risk evaluation process carried out in X2Rail-3 is to look at the resulting categories in the risk matrix and for every hazard and either

- define additional system requirements and operational measures for Moving Block systems to lower the risks to an acceptable level or
- show that the risks are not higher than in ETCS systems today and can therefore be deemed acceptable following the CSM "comparison to similar Reference Systems" approach.

14.5 References

[1] X2Rail-1 Deliverable 5.3: Moving Block Preliminary Safety Analysis; X2Rail-1 Deliverables will be available in the near future under https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-1

[2] Commission Implementing Regulation (EU) No 402/2013 of 30 April 2013 on the common safety method for risk evaluation and assessment and repealing Regulation (EC) No 352/2009

14.6 Authors

Dipl.-Ing. **Stefanie Schöne** finished her studies of transport engineering at the Technical University of Dresden, Germany with a diploma in 2012. Since then she has been working at the Institute of Transportation Systems of the German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt, DLR), mainly in the fields of railway operations and railway signalling systems.

Stefanie.Schoene@dlr.de

Dr.-Ing. **Michael Meyer zu Hörste** holds a PHD in mechanical engineering from the technical University of Braunschweig. He has joined DLR Institute of Transportation Systems in 2001 bringing already 6 years of railway research experience with him. He is expert in railway operations, command, control and signalling systems, especially ERTMS/ETCS as well as train localisation. Currently he is working the business development of the DLR Institute of Transportation Systems He was a major contributor in building the DLRs ETCS test laboratory RailSiTe®. He is chairman of the ERTMS Reference Labs Association since 2012. He is fellow of the Institution of Railway Signalling Engineers (FIRSE) since 2012. He is member of the Shift2Rail governing board and coordinator in the DLR for Shift2Rail.

Michael.MeyerzuHoerste@dlr.de

Mario Alonso Ramos is the Head of Safety Assurance of Mainlines, Siemens UK. He has 15 years of experience on safety assurance for railways in ETCS/ERTMS projects, both for trackside and onboard equipment.

Mario.alonso-ramos@siemens.com

15 Authors Index