ISSN 1866-721X

DLR-TS 1.35

1st SmartRaCon Scientific Seminar - Proceedings

1st SmartRaCon Scientific Seminar

Proceedings

Berichte aus dem DLR-Institut
für Verkehrssystemtechnik

Band 35

Deutsches Zentrum
für Luft- und Raumfahrt

DLR

Reports of the DLR-Institute of Transportation Systems

Volume 35

Proceedings of the
1st SmartRaCon Scientific Seminar

June 25. 2019
Villeneuve d'Ascq, France

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

ISSN 1866-721X

DLR-TS 1.35

Braunschweig, June 2019

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

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

International Scientific Committee

Dr. Marion Berbineau (IFSTTAR, Villeneuve d'Ascq, France)
Michael Hutchinson (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)
Dr. Sandro Scalise (DLR, Oberpaffenhofen, Germany)

Host

The 1st SmartRaCon Scientific Seminar has been hostet by IRCICA

https://ircica.univ-lille.fr/

Table of Contents

1 Introduction by SmartRaCon 1
Marion Berbineau; IFSTTAR, France; Michael Hutchinson; NSL, United Kingdom; Jaizki Mendizabal; CEIT, Spain; Emilie Masson, IRT RAILENIUM, France; Michael Meyer zu Hörste; DLR, Germany

2 System-Level Evaluation of 3GPP LTE System in Railway Environment.. 7
Loïc Brunel, Hervé Bonneville, Akl Charaf, Mitsubishi Electric R&D Centre Europe, Rennes, France; Émilie Masson, IRT RAILENIUM, Famars, France

3 SDN-assisted Train-to-Ground Communication Architecture for Dynamic Traffic Routing and Slicing 17
David Franco; University of the Basque Country (UPV/EHU), Bilbao, Spain; Eder Ollora Zaballa; Technical University of Denmark (DTU), Lyngby, Denmark

4 Channel Characterization and Emulation 23
Nerea Fernández, Jaizki Mendizabal; CEIT, San Sebastián, Guipúzcoa, Spain

5 Satellite communication prototype based on SDR...................... 29
Benjamin Barth, Federico Clazzer, Marcel Grec; German Aerospace Center (DLR), Institute of Communications and Navigation, Oberpfaffenhofen, Germany

6 Introduction to various threats on wireless networks and their detection 35
Jonathan Villain , Grecia L. Romero, Virginie Deniau, Anthony Fleury, Christophe Gransart, Eric P. Simon, Raouf Kousri ; IRT RAILENIUM, Famars, France

7 Railways cyber security, human factors part: What happens when the automatic countermeasures fail?..................................... 41
Patrick Millot; Université de Valenciennes, LAMIH-UMR CNRS, Valenciennes & IRT RAILENIUM, Famars; Mathieu Mouchel, Christopher Paglia; rHesuS Consulting & IRT RAILENIUM, Famars, France

8 Shifting tests from on-site to the lab for automatic train operation.. 53
Oliver Röwer, Lennart Asbach, Michael Meyer zu Hörste; German Aerospace Center (DLR), Institute of Transportation Systems, Braunschweig, Germany

9 Tward application of operational parameters for testings in laboratory to reduce on-site testing: focus on human operators ... 63
Philippe Richard; IRT RAILENIUM, Famars, France; Simon Collart-Dutilleul; IFSTTAR, ESTAS, Villeneuve d'Ascq, France

10 Authors Index 71

1 Introduction by SmartRaCon

Marion Berbineau; IFSTTAR, Villeneuve d'Ascq, France
Michael Hutchinson; 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

Innovative technologies enable new approaches for train control, command and signaling systems. E.g. digitalization and automation lead to completely new concepts. The partner RAILENIUM, NSL, CEIT and DLR have founded the consortium Smart Rail Control (SmartRaCon) to develop new concepts, approachs and technologies for the train control, command and signaling systems of the future. In this contribution the developments in the areas of communication, localization and train integrity will be discussed. For the communication the next generation of mobile radio 5G is in the focus with the capability to support software defined networks and radio as well as virtualization potentials. For localization and train integrity supervision algorithms for the fusion of sensor data and digital maps are the key elements. E.g. Global Navigation Satellite Systems (GNSS) together with complementary sensors can be used to achieve a safe and reliable localization. This concept again can serve as a core of a end-of-train device for train integrity monitoring. Further elements like the traffic management or moving block as well as procedural aspects like simulation-based testing are subject of the SmartRaCon concepts and are related to the issues discussed here. The architectural concept to integrate all those elements is based on the idea to use components and software common-off-the-shelf (COTS) and to integrate them into a railway network in a modular way.

Figure 1-1: Logo of SmartRaCon

1.2 Partnership in the frame of international collaboration

The four partners CEIT, DLR, NSL and RAILENIUM; are cooperating in SmartRaCon to accelerate the introduction and implementation of innovation in the railway sector. This gives the opportunity to validate if the approaches developed over several European and non-European countries.

The Centro de Estudios e Investigaciones Técnicas (CEIT) is a multidisciplinary research centre with the unique capability to bring technology to market. During the last 16 years, CEIT has created 14 spin-offs; some of them have been acquired by international companies present in the NASDAQ (IXYS), PAR (ERASTEEL), NYSE (PRAXAIR) & IBEX (CAF). Of major relevance is the expertise of CEIT in dependable ICT solutions, e.g. working with INTEL for 17 years & for 5 years with the US DoD in 75 GHz solutions.

The German Aerospace Centre (Deutsches Zentrum für Luft-und Raumfahrt e.V – DLR) brings large experience from the domains of aviation, automotive, robotics, space and energy, especially in the field of control command & human factors. DLR has a wide ranging experience in the field of human factors. Based on a long history of human factors research in the aeronautics area, DLR continuously broadened this field of research to the automotive and rail traffic domain. Especially with the experience of research in the field of air traffic management, transdisciplinary synergies are used to analyse and improve traffic management systems in the railway sector.

Fondation de Coopération scientifique RAILENIUM is one of 8 Institutes for Innovation, Research and Technology (IRT) created by the French government in 2012 to boost economic competitiveness by filling up the gap between academia research and industry. The added value of RAILENIUM is based on a long history of research of the founding members (IFSTTAR, Univ. of Lille, Univ. of Valenciennes) in collaboration with industry in the domains rail, automotive & aeronautics. They bring large experience from wireless com., positioning, control-command, signalling, simulations, field trials etc. RAILENIUM intends to works with SME's as subcontractors. A governing board, based on representatives of the French Government ensures that the projects are independent and have no overlapping or double funding.

Nottingham Scientific Limited (NSL) is a UK based hi-tech small-to-medium sized enterprise (SME), formed in 1998 as a spin-out company from the University of Nottingham. NSL is a private limited company (staff-owned), consisting of approximately 50 staff. The annual turnover is approximately €3.5m. NSL is an applications and technology development company that focuses on developing solutions for GNSS markets. NSL specializes in solutions where there is a requirement to demonstrate the robust, reliable and assured use of GNSS and other positioning technology. This includes developing robust and reliable algorithms, software, devices and applications using GNSS technologies. The company's core business centers around the development of applications and provision of services for safety critical transport operations (aviation, maritime and rail), mission critical applications (security, justice, law enforcement) and high value economic applications (e.g. road pricing). The company is also a supplier into GNSS programs e.g. Galileo and EGNOS. NSL clients include government departments, international organizations, infrastructure operators, service providers and system integrators.

To disseminate the results of the scientific work, the SmartRaCon partners organize 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].

1.3 Research Infrastructures and Simulators

The SmartRaCon Partner are developing and operating a large number of simulators and research infrastructures which are used to validate the approaches for new systems. Among them are:

1. Railway operation simulators like the TMS simulation or the OVM tool

2. Test laboratories like the ETCS On-Board lab or the RailSiTe®
3. Test vehicles like the RailDriVE®
4. Measurement labs like the EMC test or EMC interference detection
5. GNSS equipment like DETECTOR or the GNSS equipment at the ERTMS national integration facility – ENIF
6. And many more, which can be seen at Fig. 1-2 …

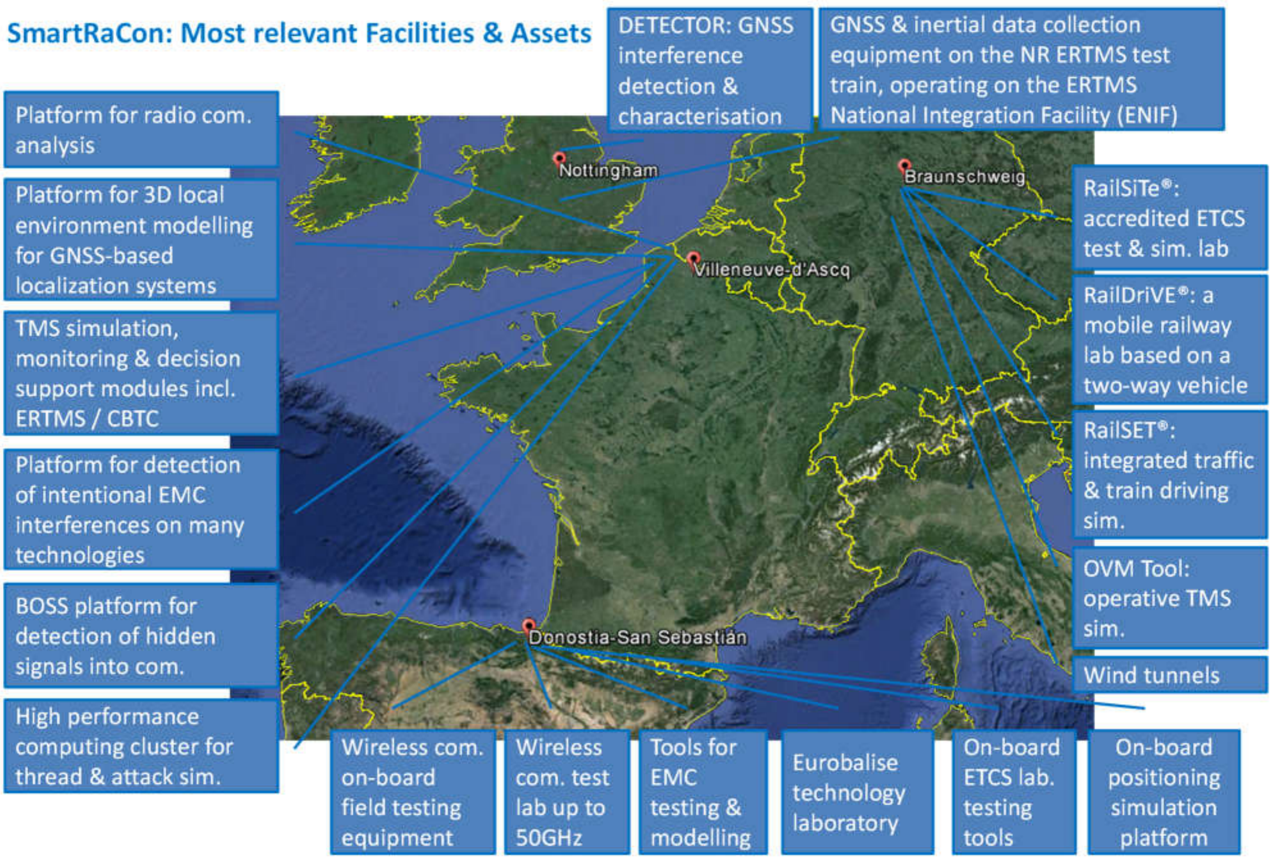


Figure 1-2: Selected Research Infrastructures and Simulators SmartRaCon

1.4 Authors

Marion Berbineau received the Engineer degree from Polytech'Lille (France) and the Ph.D. degree from the Univ. of Lille, both in electrical engineering, respectively in 1986 and 1989. She is a full time Research Director at IFSTTAR, in the Component and SYStem department. 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@ifsttar.fr

Michael Hutchinson is a Senior Navigation Engineer and has over ten years of experience in the GNSS industry. He is the business lead in the NSL Safety and Integrity Unit. Michael is also the NSL lead engineer and project manager in rail initiatives within the company including the UK RSSB FuTRO Map3 project, ESA SBS-RailS (use of SatCom and GNSS for ERTMS) and EC FP7 ETCS Advanced Testing and Smart Train Positioning System (EATS) project. He has conducted user requirements and state-of-the-art reviews regarding navigation and communications solutions in the European rail industry and has been involved in the development of GNSS assessment units for installation on operational trains in the UK and Spain. Finally Michael has developed and used data archiving, processing and analysis tools to assess the potential of alternative GNSS-based solutions for rail (professional and low-cost receivers, DGPS, EGNOS, GNSS/IMU integration architectures). He holds an MSc (Master of Science) in Satellite Positioning Technology from the University of Nottingham, UK.

michael.hutchinson@nsl.eu.com

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

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-IK4, 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 System-Level Evaluation of 3GPP LTE System in Railway Environment

Loïc Brunel, Hervé Bonneville, Akl Charaf, Mitsubishi Electric R&D Centre Europe, Rennes, France
Émilie Masson, Institut de Recherche Technologique Railenium, 59300 Famars, France

2.1 Introduction

GSM-R, the radio communication system based on GSM, has been adopted in most of the European countries on main lines. In order to fulfill railway operators' needs of new applications, like closed-circuit television, and to overcome the upcoming GSM obsolescence, the design of the next radio communication system for train-to-ground communications has started in Europe. Evolutions of 3GPP LTE (Long Term Evolution) are among candidates, together with 5G. As one aim of the X2Rail-1 project is to overcome the limitations of the existing communication system, it analyses candidate systems for the next generation and, in this context, evaluates the system throughput of the 3GPP LTE mobile cellular system.

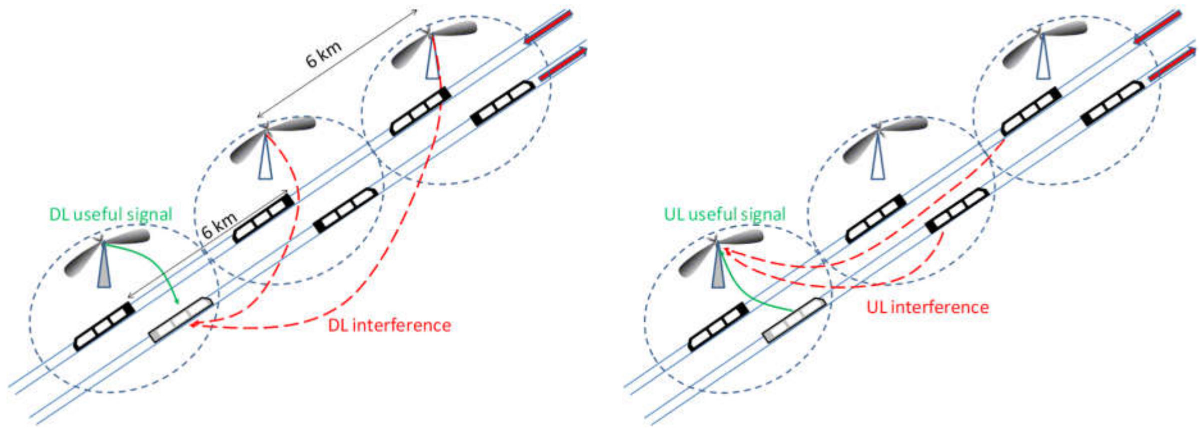
2.2 3GPP LTE mobile cellular system for railways

The LTE system is based on multi-carrier modulations, namely Orthogonal Frequency Division Multiplexing (OFDM) in downlink (DL) and DFT-spread OFDM (DFT-s-OFDM) in uplink (UL) as specified in [1]. The bandwidth currently allocated to the train radio communication system in Europe is at most 5.6 MHz, namely 4 MHz around 900 MHz (UIC band) in all European countries and a future additional adjacent 1.6-MHz bandwidth (E-UIC band). Hence, we focus here on a 5-MHz LTE system for railways operated over the UIC and E-UIC bands. In order to achieve high spectral efficiency whatever the channel conditions and variations, the LTE system offers a large panel of specified multi-antenna schemes [1]. We focus here on the transmit diversity schemes, which are more robust to high velocity. In DL, the transmit diversity scheme is, with two transmit antennas, the Alamouti Space Frequency Block Code (SFBC) applied on two adjacent sub-carriers, and, with four transmit antennas, a combination of Alamouti SFBC and Frequency Switched Transmit Diversity (FSTD) on four adjacent sub-carriers. In UL, LTE Release 8, which we focus on, only includes closed-loop transmit antenna switching which is not feasible with train mobility due to strong channel state information aging. Thus, we focus here on single-antenna transmission and rely on the base station (BS) receive antennas, to obtain spatial diversity.

2.3 Multi-cell system level evaluation

In a multi-cell system, a neighbouring BS generates interference on the DL signal received at a train, as depicted in Fig. 2-1. Likewise, trains located in neighbouring cells generate interference on the UL signal received at a BS. Trains located at the cell edge or suffering from higher shadowing are more impacted by inter-cell interference. Typical LTE deployments are frequency reuse 1 deployments, which offer better spectrum usage and higher cell-center throughput. However, they are interference limited. Thus, due to the high inter-cell interference, the cell-edge throughput drops significantly compared to cell-center throughput. The inter-cell interference level can be reduced by performing inter-cell interference mitigation. We focus here on downlink. Among inter-cell interference mitigation techniques, partial frequency reuse

[2] offers the best compromise between cell-edge throughput and cell-center throughput [3]. In partial frequency reuse, hard frequency reuse 2 is performed only on a part of the band, here a portion α of the band, and frequency reuse 1 is kept on the other part, as depicted in Fig. 2-2. Patterns A and B are used every other cell and cell-edge trains are scheduled in the part of the band using hard frequency reuse 2.



(a) (b)

Figure 2-1: Railway deployment and inter-cell interference (a: downlink; b: uplink).

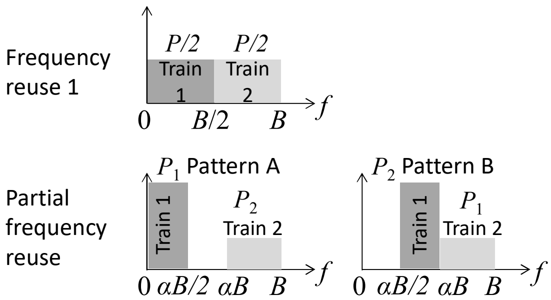


Figure 2-2: Downlink Tx power patterns for frequency reuse 1 and partial frequency reuse.

Link level simulations allow to compute the packet error rate (PER) of a transmission scheme, including detailed simulation of modulation and coding, MIMO scheme, channel estimation, small-scale fading effects and AWGN. However, they do not include any effect of large-scale fading, i.e., distance-dependent path-loss and shadowing, which impact the experienced signal-to-noise ratio (SNR) but also the inter-cell interference level. System level evaluation is needed in order to quantify the impact of inter-cell interference on cellular system throughput. Since keeping the same level of details as in link level simulations for a multi-cell system level simulation would result in too much computation effort, the evaluation is split in two steps:

- Step 1: Link level evaluation
  1. Computation of the PER_i vs. Signal-to-Interference-plus-Noise Ratio (SINR) for N different transmission schemes (characterized by a specific modulation, coding rate, MIMO scheme) providing different throughputs T_i, i=1,…,N, thanks to a link-level simulation (interference is assumed AWGN)
  2. For each scheme i and each SINR value, computation of the resulting throughput $T_{res,i}$(SINR) taking PER into account as

$$T_{res,i} = T_i \times \left(1 - PER_i\left(SINR\right)\right)$$

3. For each SINR, storage in a look-up table of the maximum resulting throughput among all schemes as a result of ideal link adaptation to large-scale channel properties:

$$T_{\max}\left(SINR\right) = \max_i\left(T_{res,i}\left(SINR\right)\right)$$

– Step 2: System level evaluation
  1. For many drops of terminals (UEs for User Equipments) and large-scale channel realizations, computation of SINR for each UE
  2. From all the drops, computation of the Cumulative Density Function (CDF) of the throughput by using the obtained SINR as input in the look-up table

System-level simulations are helpful to compute the cell average spectral efficiency or the cell-edge throughput (e.g., the 5%-ile throughput, i.e., the maximum throughput among the 5% of UEs with worst SINR). As the train radio communication system will deliver critical services, its reliability at any location on the railway is crucial. In order to evaluate this reliability, we compute the 5%-ile throughput at any position on the railway. It is much stricter than the 5%-ile throughput taken over the whole cell.

For evaluating LTE as train radio communication system, we assume a rural environment and a straight railway. Simulating track curves would result in different throughput results, due to reduced powers of useful and interfering signals, but would also correspond to very specific scenarios. Furthermore, we keep the same inter-BS distance as in a typical GSM-R deployment, i.e., 6 km. The intention is to be able to reuse GSM-R masts in order to limit the migration cost. We evaluate a worst-case train load scenario, in which the train traffic is maximized. Trains move in two opposite directions and trains moving in the same direction are 6 km apart. With a higher density of trains, which might happen in an urban environment, the distribution of interference level would not be different but the total throughput would be divided among more trains. A worst-case interference level is assumed: all active cells are fully loaded in both UL and DL, i.e., full buffer traffic occurs in the whole bandwidth.

As propagation channel, we use the Rural Macro (RMa) channel model [5] for link-level and system-level IMT-Advanced evaluations. Among ITU-R channel models, the RMa one appears as the most appropriate for a railway environment. For instance, the ITU-R urban channel model targets an urban street environment, which is not suitable to describe an urban railway environment. The RMa channel model is defined for Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS) and the probability to be in LoS for a UE located at a distance d from a BS is described as

$$p_{LoS} = exp\left(-\frac{d-10}{1000}\right) \text{ where } d \text{ is in meters}$$

Thus, the probability of LoS equals 100% for a distance of 10 m and drops to 37% for a distance of 1 km. For LoS, a fixed Rice factor of 6 dB is used. Another approach could have been to use 100% LoS and a decaying Rice factor according to distance. The RMa channel model relies on 10 or 11 clusters. Thus, it results in a channel delay spread which might be high for low distances. For distances of several km, the rural environment may be more dispersive while keeping a LoS path. Especially, some hilly terrains may result in high delay spread.

Table 2-1 details the deployment scenario in the UIC and E-UIC bands. Real channel estimation using frequency-domain Wiener filtering and time interpolation between consecutive sub-frames can be performed, even in UL. In order to enable time interpolation between consecutive sub-frames in UL, each train must be scheduled in every sub-frame in UL. This strong assumption holds for a low number of trains per cell. In case time interpolation between sub-frames is not possible, UL performance will degrade for high speed.

Carrier frequency (DL/UL)	922.5 / 877.5 MHz
Cell radius	3 km
Train density	2 trains per cell – 6-km spacing in each direction
Physical layer	3GPP LTE 5 MHz with normal cyclic prefix in [1]
Transmit BS/UE max power	46/36 dBm
Transmit UE power control	Full compensation
BS/UE antenna gain	14/0 dB
BS directional antenna pattern	Parabolic in dB scale as MBS in [4] Horizontal beamwidth : 10 degrees Vertical beamwidth : 15 degrees Vertical tilt : 20 degrees
BS/UE antenna height	21/4.5 m
Channel estimation	Frequency-domain Wiener with or without time interpolation
Link channel model, clustered delay lines	ITU-R RMa LoS, K_{Rice}=6 dB, 11 clusters ITU-R RMa NLoS, 10 clusters
Pathloss model	ITU-R RMa LoS & NLoS
Shadowing standard deviation (dB)	4 dB for a distance below 1826 m or 6 dB above in LoS, 8 dB in NLoS

Table 2-1: Downlink Tx power patterns for frequency reuse 1 and partial frequency reuse.

2.4 Performance evaluation

Evaluations are run for 1600 pairs of positions of the two trains in the cell of interest and with 400 channel realisations per pair of positions. Figure 2-3 shows the DL throughput obtained along the railway within a cell of radius 3 km with a 2x2 MIMO scheme, at 500 km/h. Due to inter-cell interference, with frequency reuse 1, the 5%-ile throughput drops from 20.4 Mbit/s at the cell center down to a few hundreds of kbit/s at the cell edge. With partial frequency reuse, we observe a strong gain in cell-edge 5%-ile throughput, which becomes 4.3 Mbit/s. However, cell-center throughput is reduced but maintained to a better average level than with hard frequency reuse 2 [3]. Figure 2-4 shows performance behaviour in UL, with 1x4 SIMO, for frequency reuse 1, at 500 km/h, with and without time interpolation between consecutive sub-frames for channel estimation. Without inter-sub-frame time interpolation, the throughput at cell center and cell edge strongly degrades.

Table 2-2 and Table 2-3 present a summary of LTE performance for frequency reuse 1 and different speeds and MIMO/SIMO schemes, in DL and UL, respectively. SISO results are also shown as reference. In DL, we can see that there is a strong gain by using 2 transmit antennas and 2 receive antennas compared to SISO. Using a 4x2 MIMO configuration in DL does not increase the throughput due to the additional pilot overhead. At 500 km/h, the 4x2 MIMO scheme also suffers from poorer channel estimation because the pilot density is reduced for the two additional antennas compared to the 2-transmit-antenna case. The results confirm that the LTE system can cope with high speeds up to 500 km/h in railway environment in DL and that UL the throughput is not significantly degraded by such high speeds if time interpolation between consecutive sub-frames is enabled for UL channel estimation. Otherwise, the UL throughput strongly degrades between 350 km/h and 500 km/h. Furthermore, in all cases for frequency reuse 1, 5%-ile throughput remains very low at cell edge. Table 2-4 presents results with partial frequency reuse allowing a better 5%-ile throughput at cell-edge.

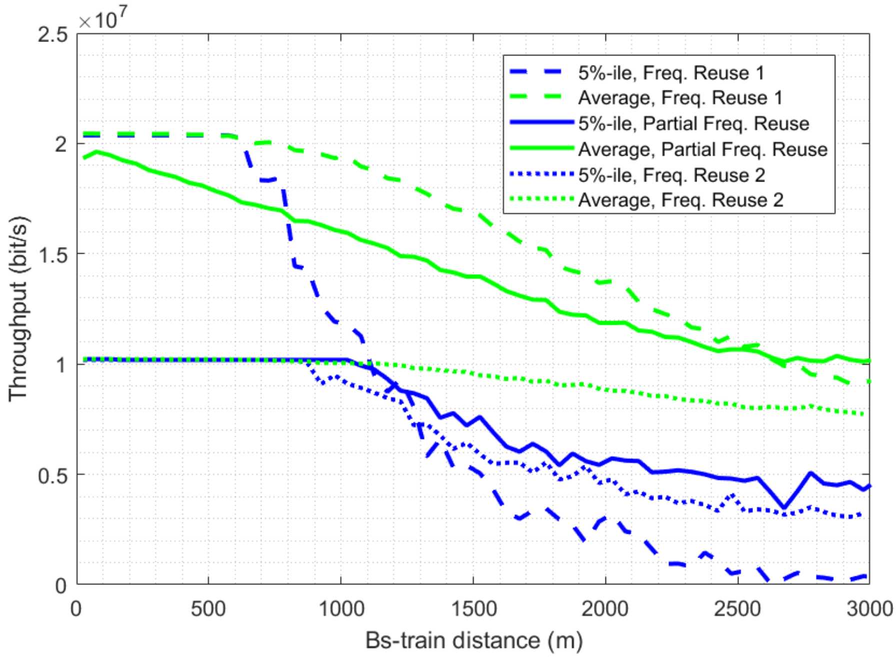


Figure 2-3: Downlink throughput with 2x2 MIMO at 500 km/h

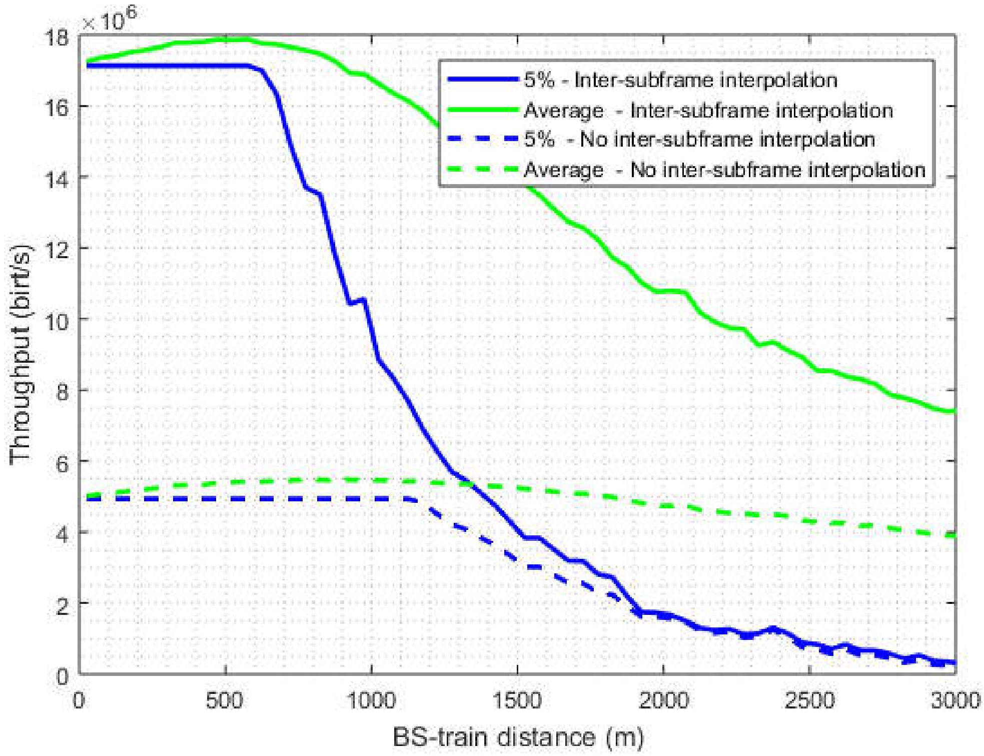


Figure 2-4: Uplink throughput with 1x4 SIMO and frequency reuse 1 at 500 km/h

Train velocity (km/h)	MIMO	Cell-center 5%-ile throughput (Mbit/s)	Cell-edge 5%-ile throughput (Mbit/s)	Whole-cell average throughput (Mbit/s)	Whole-cell 5%-ile throughput (Mbit/s)
30	1x1	17.9	0.1	12.7	1
30	2x2	20.4	0.4	16.5	2.2
30	4x2	19.2	0.4	16	2.8
350	1x1	13.9	0	7.6	0
350	2x2	20.4	0.4	16	2.7
350	4x2	19.3	0.3	15.3	2.6
500	1x1	12	0	6.9	0
500	2x2	20.4	0.3	16	2.7
500	4x2	17	0.4	14.4	2.6

Table 2-2: Summary of DL LTE throughput results with frequency reuse 1.

Train velocity (km/h)	MIMO	Cell-center 5%-ile throughput (Mbit/s)		Cell-edge 5%-ile throughput (Mbit/s)		Whole-cell average throughput (Mbit/s)		Whole-cell 5%-ile throughput (Mbit/s)	
		Interp	No Interp	Interp	No Interp	Interp	No Interp	Interp	No Interp
30	1x1	18.2	18	0.1	0	10.8	10.8	0.6	0.6
30	1x2	19.3	19.3	0.1	0.1	12.7	12.7	1.3	1.2
30	1x4	19.3	19.3	0.5	0.4	14.5	14.4	2.6	2.5
350	1x1	17.9	17.9	0	0	10.6	10.6	0.5	0.5
350	1x2	19.3	19.3	0.1	0.1	12.6	12.6	1.2	1.2
350	1x4	19.4	19.4	0.4	0.4	14.4	14.4	2.3	2.3
500	1x1	16.1	4.8	0	0	9.5	3.8	0.5	0.5
500	1x2	17.1	4.9	0.1	0.1	11.8	4.4	1.2	1
500	1x4	17.1	4.9	0.3	0.2	13.5	5	2.3	2

Table 2-3: Summary of UL LTE throughput results with frequency reuse 1

(Interp: interpolation between successive sub-frames, No Interp: No interpolation between successive sub-frames)

Train velocity (km/h)	MIMO	Cell-center 5%-ile throughput (Mbit/s)	Cell-edge 5%-ile throughput (Mbit/s)	Whole-cell average throughput (Mbit/s)	Whole-cell 5%-ile throughput (Mbit/s)
30	1x1	9.5	2.3	11.7	3.3
30	2x2	10.2	4.4	14.3	6.1
30	4x2	9.7	4.4	13.6	6.3
350	1x1	8.9	0	7.4	0
350	2x2	10.1	4.3	14.3	6.1
350	4x2	9.7	4.1	13.6	6.1
500	1x1	7	0	7	0
500	2x2	10.2	4.3	14.3	6.1
500	4x2	8.5	4.3	12.8	5.9

Table 2-4: Summary of DL LTE throughput results with partial frequency reuse.

2.5 Acknowledgements

This work was performed in the framework of the WP3 (Adaptable Communication System) of the X2Rail-1 project. The authors would like to thank the Shift2Rail Joint Undertaking for financial support.

2.6 References

[1] 3GPP TS 36.211, Evolved Universal Terrestrial Radio Access (E-UTRA); Physical Channels and Modulation. V8.9.0. 3rd Generation Partnership Project (3GPP), 2009.

[2] M. Sternad, T. Ottosson, A. Ahlén, A. Svensson, "Attaining both coverage and high spectral efficiency with adaptive OFDM downlinks," 38th IEEE Vehicular Technology Conference, Fall, Orlando, Florida, October 2003.

[3] L. Brunel, H. Bonneville, A. Charaf, E. Masson, "System-Level Evaluation of Next-Generation Radio Communication System for Train Operation Services," 7th Transport Research Arena, Vienna, Austria, April 2018.

[4] 3GPP TR 25.996, Spatial channel model for Multiple Input Multiple Output (MIMO) simulations.V12.0.0. 3rd Generation Partnership Project (3GPP), 2014.

[5] ITU-R, 2009. Guidelines for evaluation of radio interface technologies for IMT-Advanced. TR, M.2135-1, International Telecommunication Union - Radiocommunication.

2.7 Authors

Loïc Brunel received the electrical engineering degree of the Ecole Supérieure des Télécommunications (ENST), Paris, France, in 1996 and the Ph.D. degree in 1999. In 2000, he joined, as a Research Engineer, the Communications Technology Division of the Mitsubishi Electric R&D Centre Europe in Rennes, France, with research interests such as multiple-access systems, multi-carrier transmissions, channel estimation, channel coding and multiple-antenna technologies. From 2005 to 2012, he has contributed in 3GPP RAN1 Working Group on physical layer aspects of the LTE mobile cellular system. In 2012, he became Research Manager of the Wireless Communication System team and, in 2019, Head of the Communication and Information Systems division. The division covers physical layer, protocol and software design. It addresses cellular, optical and satellite communication systems and professional fields like transportation, automotive and factory automation.

l.brunel@fr.merce.mee.com

Hervé Bonneville graduated from the University of Paris XI in 1987. He worked in telecommunication area and embedded real-time systems for Sagem, Transpac and Thomson before joining Mitsubishi Electric R&D Centre Europe in 1999. He participated in the conception and design of MERCE HiperLAN/2 prototype, has been involved in European projects IST-

PULSER and ARTIS4G, and in the French project SYSTUF on radio system design for urban rail control signalling. He actively participated in the IEEE 802.11n standardization, is contributing in 3GPP LTE/LTE-Advanced architecture standardization since 2006 and in ETSI RT-NG2R since 2016. His research interests include layers 2 and 3 of communication stack, more specifically for wireless communications in the context of high QoS requirements, and extend to network architecture for radio access systems. He is now working QoS and mobility aspects for train communications and on architecture for 5G systems.

Akl CHARAF graduated from the Faculty of Engineering, Lebanese University, Beirut, in 2007. In 2012, he received his Ph.D degree in digital communications from Telecom ParisTech, Paris. He worked as R&D engineer in wireless communications for Orange Labs, Alcatel-Lucent and Naval Group. Since 2014 he is a R&D consultant for Mitsubishi Electric R&D Centre Europe where he is involved in research on Future Railway Mobile Communications Systems as well as 5G standardization within 3GPP.

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

3 SDN-assisted Train-to-Ground Communication Architecture for Dynamic Traffic Routing and Slicing

David Franco, University of the Basque Country (UPV/EHU), Bilbao, Spain
Eder Ollora Zaballa, Technical University of Denmark (DTU), Lyngby, Denmark

3.1 Introduction

The continuous evolution of telecommunication technologies has created the necessity of updating railway communication systems. These new systems must ensure the performance of traditional ones, while being flexible and adaptable in order to be ready for constant advances. In this context, Software Defined Networking (SDN) is used to dynamically configure, control and allocate network resources, becoming one of the key technological enablers for 5G networks. SDN introduces the programmability of the network and opens the door to new communication interfaces that enable flexibility and adaptability. Therefore, the concept of Adaptable Communication System (ACS) turns up to face up the challenge of decoupling high-level functions from underlying technologies and enable their independent development.

This paper provides a description for 2 different but coexisting SDN use cases for the ACS architecture. The first use case targets communication flow management (creation, provisioning and adaptation) in order to provide a better performance by means of Multipath TCP (MPTCP). The second case, leverages traffic isolation by means of traffic tagging in order to provide slicing features.

3.2 Case I: Dynamic traffic routing

This case aims to demonstrate the feature of dynamic traffic routing in the context of an ACS architecture and ensuring a compliance with the requirements of communications for signalling services [1]. For that purpose, SDN allows the dynamic creation, provisioning and adaption of communication flows at runtime. The SDN controller centralises the control of the network, enabling the on-demand programmability of the data plane. The controller runs an application that is in charge of offering path diversity and assuring resiliency by rerouting traffic in case of link or switch failure. Transport-level redundancy techniques are also applied in order to provide end-to-end redundancy.

3.2.1 Proposed architecture

This section describes the proposed architecture for the train-to-ground communication. The architecture has two main components (see Figure 3-1): the network and the ACS functions.

The network is divided into core and access subnets, which are both based on SDN equipment. The core is a dedicated network whose data plane consists of several SDN-OpenFlow switches. The access network is composed of dedicated LTE and WIFI networks. In this architecture, Access Points (APs) are SDN-based, while eNodeB (eNB) and Evolved Packet Core (EPC) entities are not. This means that the controller can take forwarding decisions over the APs in order to dynamically create routes. All the SDN switches are point-to-point connected to the controller, forming an out-of-band control plane, and they use the OpenFlow protocol to exchange control information.

The ACS functionality relies on an SDN centralised controller that takes forwarding decisions and establishes data paths between end-user entities. The controller runs a locally developed routing algorithm that is oriented to reduce the delay of the communication and provide resiliency and path diversity. The EnhAnced Mirroring Sdn diSjoint (sEAMleSS) path computing algorithm is based on DynPaC [2] and it is responsible for calculating disjoint data paths between two selected SDN switches. Although SDN does not extend to the On-board Equipment (OBE) nor the Control Centre Equipment (CCE), they are part of this ACS because they run MPTCP with redundant scheduler [3] to provide a redundant end-to-end communication.

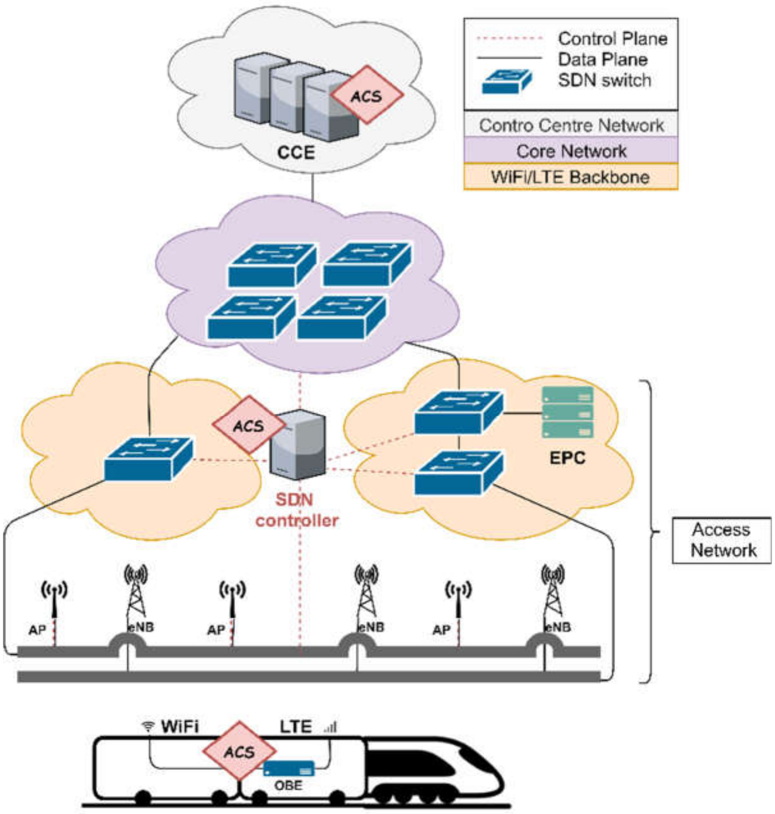


Figure 3-1: Proposed architecture for case I

3.2.2 Prototype description

This section explains how to deploy the aforementioned communication architecture using real equipment. Consequently, Figure 3-2 depicts control and data plane layouts of the designed prototype for that purpose.

In the data plane, two Virtual Network Functions (VNFs) are allocated in the cloud infrastructure or Virtual Infrastructure Manager (VIM). These VNFs are the EPC and the Control Centre Equipment (CCE). The EPC is a Linux image running Open Air Interface (OAI) LTE core software and the CCE is another Linux image configured to execute MPTCP with redundant scheduler. In this case, it is used an own OpenStack VIM, however, it is possible to deploy these functions over physical equipment. A single SDN switch is partitioned to create three instances that are the three SDN switches shown in Figure 3-2. The first one is connected to the VNFs, the second one to the APs and the third one to the eNB. The APs are OpenFlow-based so they can be managed from the controller. The eNB consists in a Linux PC that runs OAI LTE softmodem and which is connected to an USRP B210 to emulate the LTE air interface. There is also another Linux PC, running MPTCP redundant, which is provisioned with WiFi and LTE wireless interfaces.

The control plane is formed by a legacy switch that interconnects all the SDN devices to the SDN controller, creating an out-of-band control plane. The controller is also allocated in the OpenStack cloud infrastructure.

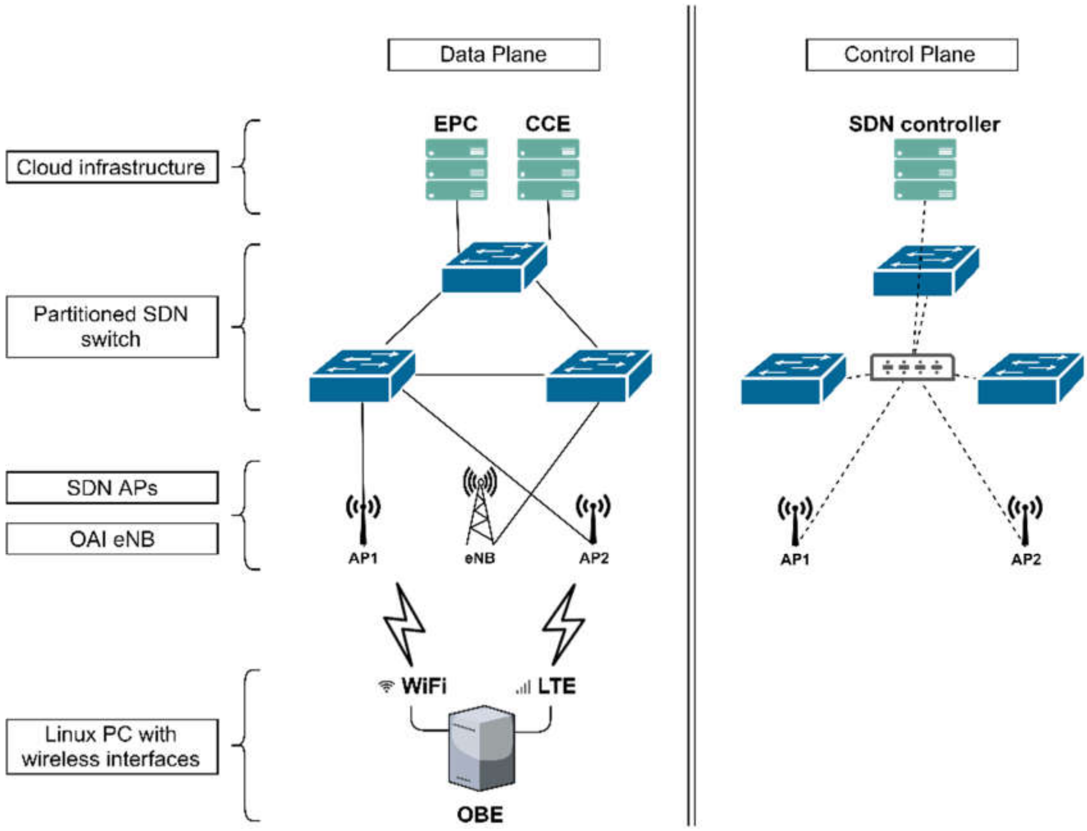


Figure 3-2: Control and data plane layouts of the prototype for case I

3.3 Case II: Traffic isolation

The case described in this section leverages traffic isolation by means of SDN slicing. This feature enables different tenants to share the same network. The traffic is forwarded and managed by SDN switches and an SDN controller respectively. The case analysed in this section tries to accommodate the different tenants and services that use the same physical network by dynamically tagging packets according to the configuration applied by the SDN controller. The SDN controller is expected to interact with other devices in the train, such as the ACS equipment, in order to dynamically tag and classify the traffic.

3.3.3 Proposed architecture

This section will describe the architecture used in the traffic isolation case. It will introduce how the SDN switches and controller are integrated with the rest of the network. Besides it argues on the rationale behind strategic SDN switches and controller placing.

As seen in Figure 3-3, SDN switches are introduced at two particular locations. One SDN switch is placed at the train and the other one is located on the premises. The motivation behind this design is that SDN switches must be able to tag/untag traffic at the edges. The centralized controller provides an API to external applications as well as applications running within the controller. The applications running in the SDN controller provide traffic forwarding as well as proper traffic tagging and ARP traffic management. The traffic tagged in one end cannot interact with any traffic differently tagged either in the same or the opposite end, thus providing isolation between the different traffic sources.

The SDN switches in Figure 3-3 are placed in between the ACS at both ends and the services running at each end. In this way, the ACS can have the traffic tagged according to the rules installed by the SDN controller. Afterwards, the ACS can command the SDN controller to change any parameter related to traffic tagging if necessary. Tagging procedure changes can take place at runtime, by exposing an API by the controller or by issuing proper commands using the SDN controller CLI (which the traffic isolation and forwarding application support). The communication between the SDN controller and switches is done using OpenFlow. OpenFlow is the most popular Data-to-Controller Plane Interface (DCPI) protocol, becoming the de facto protocol for SDN deployments.

Considering how future networks and their programmability options are evolving, programmable data planes could play a key role in future SDN deployments. Although this use case design only considers OpenFlow compatible switches, future networks and thus, the train equipment and networking devices involved, could be deployed using programmable switches, such as those that can be programmed using P4 [4]. Moreover, P4Runtime, as the DCPI protocol used with P4 switches, could effectively be used to fulfil this use case's requirements. This is because modern SDN controllers, such as the Open Network Operating System (ONOS), can support both Openflow and P4Runtime.

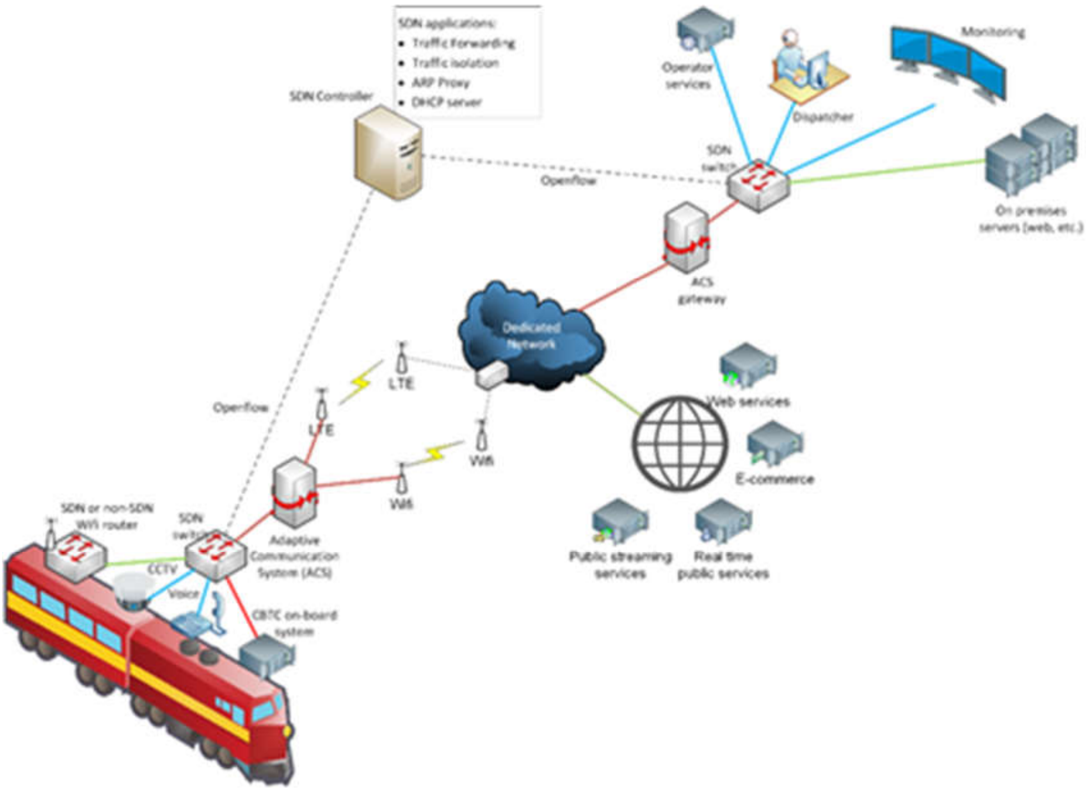


Figure 3-3: The proposed architecture for case II

3.3.4 Prototype description

This final section will explain how the different components interact and how the functionalities have been validated so far. As described before, SDN switches are placed at the edge of the network (in-train and on-premises). An example of a case and its test is described in the following lines.

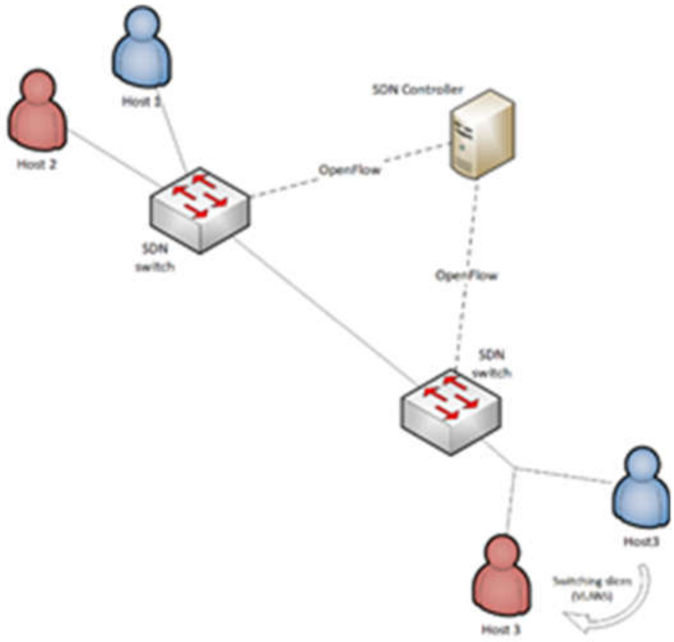


Figure 3-4: Simplified validation test case for use case II

To begin, the SDN controller assigns multiple slices (slices are defined by the VLANs in this use case) to multiple services/ports. Services such as onboard internet services, CCTV or voice can be pre-configured beforehand, but these configurations can be modified at the runtime too. In Figure 3-4, each slice is represented by the host's colour (blue and red) and each slice remains isolated from the other slices. At each edge of the network, the two SDN switches are responsible for VLAN tagging/un-tagging the traffic, creating the specific "service slices". Each slice can be assigned a different priority by setting the VLAN PCP bits or the IP DSCP field. The ACS can read those priority bits and reserve the appropriate resources or assign a specific path to the traffic. This is how the ACS interacts with the SDN controller and can program which PCP bits can be assigned as well as which VLAN IDs should be used.

Additionally, the SDN controller also offers firewall-like capabilities which enable the ACS, through an API, to block the traffic that matches a specific pattern (i.e. all passenger traffic should be limited/blocked under low capacity network conditions). On future deployments and under OpenFlow version compliance, SDN switches can rate-limit traffic for each slice if SDN switches support OpenFlow Meters [5]. This feature effectively partitions resources between slices by being able to rate limit services which might not be critical for the train service. Zodiac FX [6] switches were used to test traffic tagging, addressing and slice management, although higher capacity SDN switches will be used when the use case is integrated with other demonstrators. After carrying the tests, the slices have been proofed to be isolated, by blocking any host discoverability (ARP request/responses, for instance) between slices that must never interfere. This effectively blocks any services from accessing critical equipment/traffic sources in the train.

3.4 Conclusion

As a 5G enabler technology, SDN, along with other technologies such as NFV, both can provide great flexibility and programmability to the network. In this project, we try to implement two interesting use cases in order to increase network performance, management, and flexibility. This can be achieved by dynamically routing traffic using a custom path computing algorithm (case I) and providing slicing features to isolate traffic (case II). This effort aims to reduce equipment costs and power consumption as well as boost openness and multi-tenancy. In the near future, these use cases are expected to be deployed along with the rest of the relevant networking entities in order to validate the premises that support each case.

3.5 References

[1] International Union of Railways (UIC), "EIRENE System Requirements Specification," Mandatory Specification UIC CODE 951 v16.0.0, Dec. 2015.

[2] A. Mendiola, J. Astorga, E. Jacob, M. Higuero, A. Urtasun and V. Fuentes, "DynPaC: A Path Computation Framework for SDN," 2015 Fourth European Workshop on Software Defined Networks, Bilbao, 2015, pp. 119-120. doi: 10.1109/EWSDN.2015.77

[3] I. Lopez, M. Aguado, C. Pinedo, and E. Jacob, "SCADA systems in the railway domain: Enhancing reliability through Redundant Multipath TCP," in ITSC 2015, sep 2015.

[4] P4 Language Consortium. P4. http://p4.org/.

[5] OpenFlow specification terms, Meter. Page 10. https://www.opennetworking.org/wp-content/uploads/2013/04/openflow-spec-v1.3.1.pdf

[6] Zodiac FX. https://northboundnetworks.com/collections/zodiac-fx/products/zodiac-fx [Online]

3.6 Authors

David Franco received his MSc. degree in Telecommunication Engineering from the University of the Basque Country (UPV/EHU) in 2018. He joined the Communications Engineering Department of the UPV/EHU as a researcher in the I2T (Engineering and Research on Telematics) research lab. His research is focused on communication systems for railway signalling and Software Defined Networking (SDN). He is a current PhD student in Telecommunication Engineering at UPV/EHU.

david.franco@ehu.eus

Eder Ollora Zaballa received his MSc from the Technical University of Denmark (DTU), in 2017. He is currently a PhD student at the Network Technologies and Service Platforms group of the Photonics department, at DTU. Currently, his research covers topics like Software Defined Networks (SDN), Network Function Virtualization (NFV) and programmable data planes.

eoza@fotonik.dtu.dk

4 Channel Characterization and Emulation

Nerea Fernández, Jaizki Mendizabal; CEIT, San Sebastián, Guipúzcoa, Spain

4.1 Introduction

This work describes the Channel Characterisation Tool (CCT) and Channel Emulation Tool (CET) as one of the prototypes being developed in X2RAIL-1 WP3 Adaptable Communication System (see Figure 4-1) as part of TD2.1 Adaptable Communications Systems of IP2 Advanced Traffic Management and Control systems in the frame of Shift2Rail.

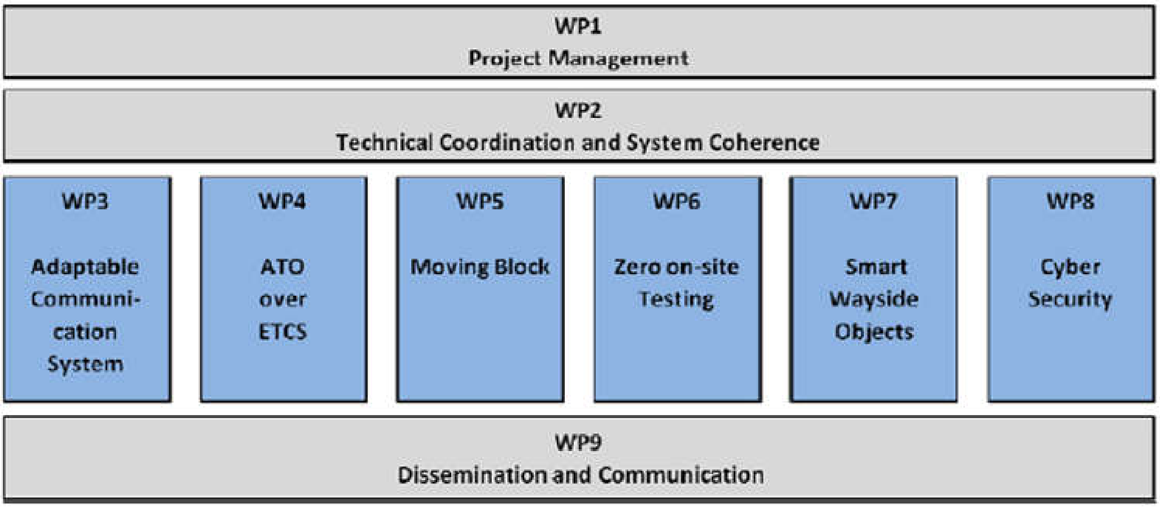


Figure 4-1: WP3 in the X2Rail-1 project (Ref: https://shift2rail.org/)

4.2 Communication impairments

Nowadays, current railway operation relies on the communication between train and trackside for a correct railway operation 0. The quality and performance of this communication depends, among others, on the communication channel. This communication channel can be affected by external impairments causing a worse performance than the ideal communication channel. Some of these external influences are the following ones:

- Environment, such as tunnels, urban areas, etc.
- Speed of train
- Electromagnetic disturbances
- Weather conditions

All these external influences result in a modification in the communication channel as Figure 4-2 shows.

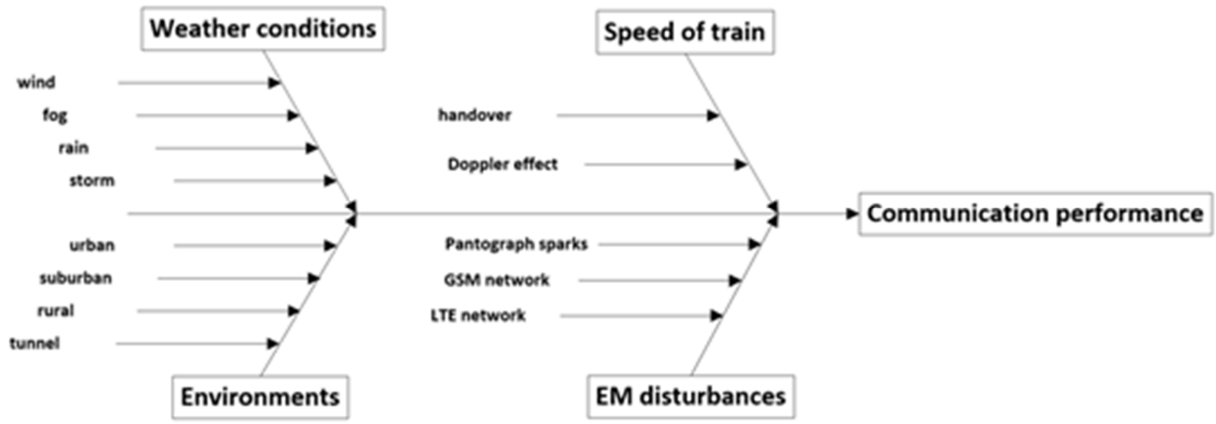


Figure 4-2: Cause and effect diagram

Depending on the railways application, the disturbances caused in the communication channel can result in:

- Normal operation of the application: if there is any disturbance but not affecting the requirements for the normal operation of the application.
- No correct operation of the application causing even a possible safety risk.

4.3 CEIT prototype

In the context of adaptable communications for railways and taking into account the communication impairments, a tool to measure and reproduce the impairments in the laboratory is needed with the aim of validating the applications relying of communications in the laboratory. For that, Ceit is working on a prototype aiming at two main objectives. To achieve them two different parts are defined: Channel Characterization Tool (CCT) and Channel Emulator Tool (CET). The first one aims to measure different parameters on site that could exist along a given track. The second one (CET) is to emulate different communication channels based on real (from real measurements), synthetic (any possible scenario) or mixed scenarios.

4.3.1 CCT (Channel Characterization Tool)

The objective of this tool is twofold. First, to measure in field the different parameters of each channel available and to see how the environment, e.g. a tunnel 0, could affect to the channel; second, to compare them with the KSR defined in the deliverable D.3.1 0 of the X2RAIL-1 WP3.

This tool permits an analysis in the communication channel in terms of measuring different parameters, it will provide a temporal and spatial characterisation of the communication channel. By this manner, the results of the different measurements and the position can be mapped.

The CCT architecture is represented in the Fig. 4-3. This tool will consist of an on-board and trackside equipment in order to measure parameters from the communication channel such as delay and bandwidth along the track.

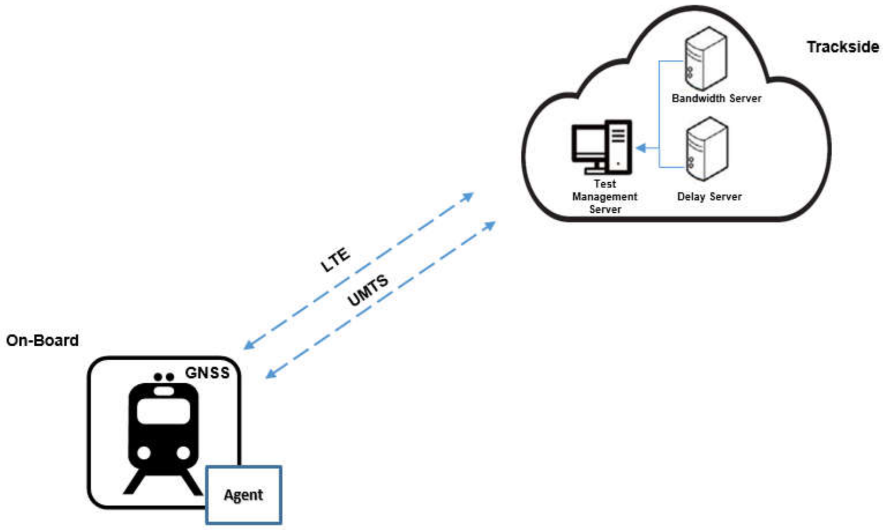


Figure 4-3: CCT

The tool needs the PLMN, e.g. LTE or UMTS, as the network for the analysis on field. Therefore, it could be aligned for any type of line, mainline, regional or urban lines; since they use some of these technologies.

The different parameters of the technologies that the CCT could measure are always at IP level analysing the transport and network layers, the radio layer is transparent for the tool. So, after these measurements on field, the communication channel is characterized in terms of different IP level parameters. Therefore it is independent of the bearer and it just required IP communication.

In the preliminary results 0 (mapped with the position of the train in each instant), the final results are, e.g., the following one:

Figure 4-4: Real Measurements

These real measurements are obtained in a regional line in the Basque Country (Spain). The Fig. 4-4 shows how the round trip time (RTT) vary among the track in two different moments. In fact, the results of different measurements done in different times can be not the same.

The visualization part of the CCT is thoroughly configurable in order to get the final results the most understandable. This visualization has different sections in order to show the different results from the communication channel and to compare between them (see Figure 4-5).

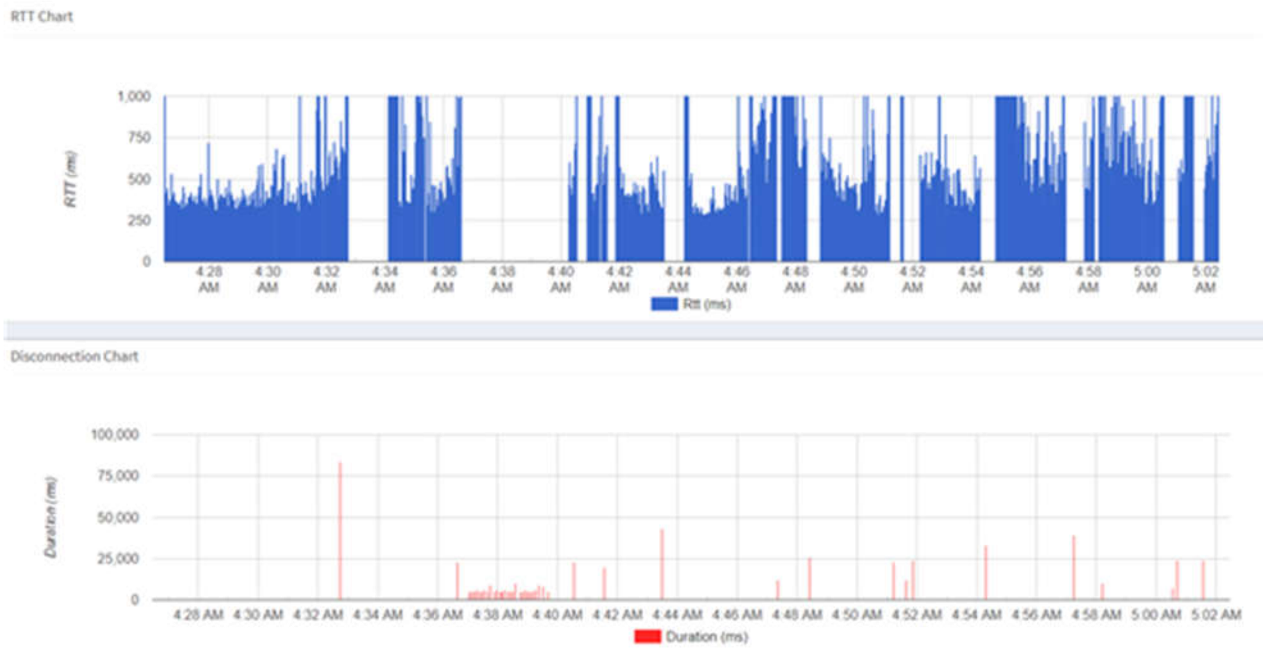


Figure 4-5: Results from the channel characterized

These results can be used as input for the configuration of the channel emulator explained below in order to test different railways applications in the same real scenarios; having, as conclusion if the desired application could be used in the given track.

4.3.2 Channel Emulator

The objective of this network emulator is to shift the most the on-site testing to the laboratory. The reason of preferring to shift the real cases to the laboratory are preferentially saving costs and the repeatability of the different scenarios. By this manner, different applications could be proved in a given scenario. In fact, this situation could be a real scenario (i.e. the channel characterized with the CCT), in a synthetic scenario (totally made up) or in a hybrid one (both of them). Therefore, configuring the channel emulator as a real scenario has as result the replay of the channel characterized from the CCT.

Therefore, the channel emulator allows configuring the different network parameters that make possible to playback a situation. The Fig. 4-6 shows the different inputs and outputs for this specific channel emulator.

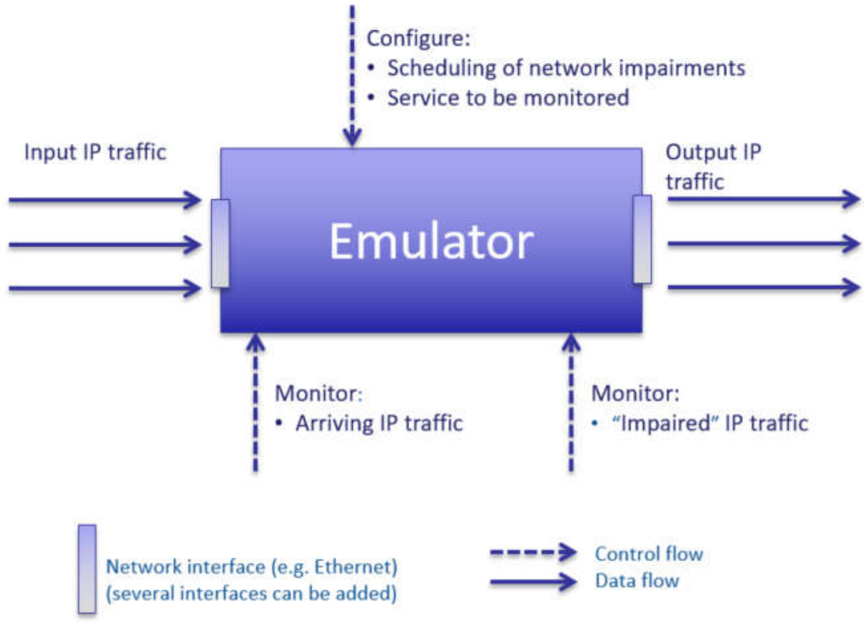


Figure 4-6: Channel Emulator

The channel emulator will have IP traffic as an input and, depending of the IP configuration parameters, will have different output IP traffic. The application that sends the input IP traffic can be whatever the tester wants such as ETCS, CBTC or voice dispatcher among other possibilities.

The purpose of the channel emulator is to see how the different technologies, depending on the network impairments configured, affect to the railways applications.

4.4 Conclusions

The railways applications are in continuous evolution with different technical requirement to accomplish. The fulfilment of these requirements depends on the communication channel, which will be used to transmit the information. However, the amount of applications is higher and higher and, another point to take into account, the communication channel is variable. This is a problem for testing channel in field due to the implicit high costs. However, there is another way to reduce costs and increase benefits: testing in laboratory.

For this alternative, channel emulator is the best option; it permits testing different applications in different moments with different communication channels configurations (inserting the network impairments). As well, to have a realistic channel, real parameters for the different communication channel have to be acquired and it is exactly the goal of CCT. By this way, the emulated communication channel can be characterized with real, synthetic or mixed data in a controlled environment.

As well, the CCT has a visual part, which allows understanding the different data collected by the fact that the communication channel can be different in different moment caused by disturbances such as environment, EM disturbances, etc.

4.5 References

[1] Nerea Fernandez, Saioa Arrizabalaga, Javier Añorga, Jon Goya, Iñigo Adín, Jaizki Mendizabal, "Survey of environment effects in railway communications", 13TH international workshop on communication technologies for vehicles, Nets4Cars – Nets4Trains – Nets4Aircraft – Nets4Spacecrafts 2018 – May 17-18, 2018 Madrid – Spain

[2] X2Rail-1 D3.1 User Requirements (Telecommunications). 2017

[3] Sijia Yang, Saioa Arrizabalaga, Iñigo Adin, Javier Añorga, Jon Goya, Zheng Liua, "Channel Characterization Tool (CCT): Distributed Network Performance Evaluation Framework for the Feasibility Study of public IP networks in Railway", Proceedings of 7th Transport Research Arena TRA 2018, April 16-19, 2018, Vienna, Austria

4.6 Authors

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-IK4 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

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-IK4, 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 Satellite communication prototype based on SDR

Benjamin Barth, Federico Clazzer, Marcel Grec; German Aerospace Center (DLR), Institute of Communications and Navigation, Oberpfaffenhofen, Germany

5.1 Introduction

A recent study on how Satellite Communication (SatCom) systems can satisfy Future Railways Communication System (FRCMS) requirements revealed that none of the current system is able to fulfil all requirements [1]. This implies that either SatCom systems can only be used for certain applications or that the requirements must be loosening. In other words, it must be decided by an application if it excludes SatCom, if the requirements are not met, which can mean a loss of service if terrestrial infrastructure is not available, or it includes SatCom which could mean limited service. A system considering SatCom and terrestrial systems must be flexible to allow the integration of different SatCom systems. In this way the train providers can select a suitable SatCom solution for their demands.

The main blocking factor according to the study is the voice application with requirements on availability and latency that cannot be fulfilled by SatCom. Focusing on signalling use cases SatCom systems can match the criteria and are a fitting solution.

The study further showed that a theoretical MEO/C-Band system would fit the best which shows that future SatCom systems will probably deal better with the requirements. This includes LEO mega-constellations but also upcoming MEO and GEO solutions, again dependent on the applications demands. Again, the possibility to include those possible future systems is beneficial.

The added value by including a SatCom system highly depends on the scenario, e.g. in urban scenario there is already coverage provided by terrestrial systems and due to shadowing SatCom might be unavailable. On the other hand SatCom fits well the high speed line and the regional line scenario due to their availability and low CAPEX, see also [1].

The SatCom prototype developed during the X2Rail-1 project will model a satellite system by the use of software defined radio (SDR). The prototype can be included as a bearer for field tests and advantages, disadvantages, potential gains or losses can be evaluated in tests without including real satellite system hardware. In principle, FRMCS shall be independent from radio access technology providers. Since most commercial SatCom systems are proprietary and do not follow a common standard, the easiest way for testing is a flexible test bed that can be adapted to different systems models. The SDR approach offers this flexibility and could even be enhanced to model future SatCom systems that are planned for the next decades.

Especially for the urban area, it is expected that the requirements on the future communications system can be addressed entirely by terrestrial technologies since they are highly available and the coverage of SatCom suffers due to shadowing caused by buildings [1]. The biggest advantage of SatCom is the coverage area which can save a lot of costs, especially in rural areas where additional terrestrial infrastructure would be needed. Hence, SatCom is considered for the regional/freight line and for the mainline/high-speed line demonstrators.

5.2 Architecture

A multi-bearer system is assumed that uses the adaptable communication system (ACS) developed in the X2Rail-1 project. The system can in principle use multiple bearers like 5G, LTE, WiFi or SatCom to connect to the backbone. The ACS routes in a transparent way traffic through the bearers satisfying QoS parameters of the dedicated applications. Focusing on the SatCom bearer Fig. 5-1 shows a SatCom setup for railways as it was proposed by [1]. The setup fits also the approach followed in X2Rail-1. SatCom systems usually consist of a ground segment, i.e. the terrestrial backbone, the space segment (satellites) and the user segment. The transceiver unit of the user segment is called terminal. The link from gateway to terminal is referred as forward link, the one from terminal to gateway as return link, both having their own characteristics and technologies used and can be investigated separately. Hence, we divided the prototype in two parts that can be used to optimally investigate the SatCom bearer within the X2Rail-1 demonstrators.

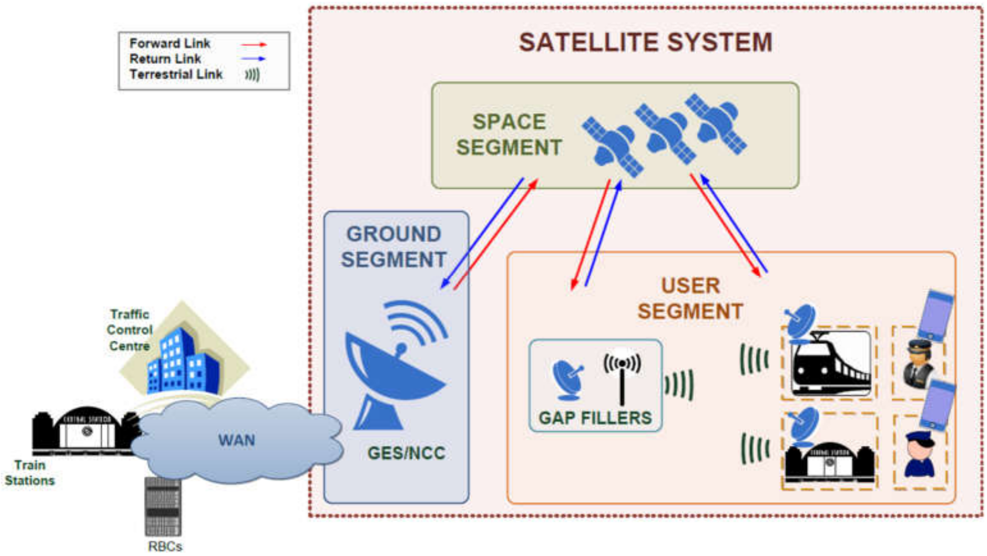


Figure 5-1: SatCom for railway [1]

5.3 Prototype

For our prototype we focus on the return link in which multiple terminals (up to tens of thousands) are connected to the system (via one or more transparent satellite(s)) and the resource allocation is not as simple as in the forward link. Differently from the forward link, each active terminal sends a request for data transmission and waits for its allocation in the available resources (time and frequency). Due to the large propagation delay – in the order of 250ms for typical satellite links – such a procedure may become particularly inefficient for small data transmissions. Efficient solutions targeting messaging systems have been lately developed, relying on advanced random access (RA) protocols. Positioning and safety related railway messages are included in the messaging systems for which advanced RA schemes are developed, making them an ideal solution for future railway communication standards.

Therefore in our prototype we consider a RA protocol where multiple uncoordinated transmitters share the available band.

Random access ALOHA-like [2] protocols have been originally proposed for the satellite domain already from the early 70's. The far distance among terminals served by a common satellite or satellite constellation prevents the use of sophisticated carrier sensing techniques.

In the recent past several advanced random access schemes have been proposed [3]. The recent enhancements have shown that RA is able to become efficient in terms of spectral efficiency and appealing in terms of target packet successful probability (probability of correctly decoding a terminal), which have been the key drawbacks in the seminal protocols ALOHA and slotted ALOHA [4]. Among the many narrowband solutions proposed in the last years, two main classes of protocols can be identified. On the one hand, slot-synchronous schemes, derived from the slotted ALOHA protocol can be found in recent literature. On the other hand, asynchronous schemes, derived from ALOHA have been proposed as well. Due to their simplified terminal architecture (no slot synchronization is required) and therefore reduced cost, asynchronous random access protocols shall be a preferred solution.

Contention Resolution ALOHA (CRA) [5], makes the use of two key ingredients to improve the spectral efficiency: the use of proactive replication of packets at the physical layer and the use of successive interference cancellation at the receiver side. User terminals benefit in terms of complexity, since no common clock to synchronize is needed anymore. The terminals transmit their replicas within a maximum delay (called virtual frame) whose duration is known also at the receiver. Time slots, synchronized to the transmitters' own internal clocks (and therefore asynchronous among different users and with receiver) can be adopted so to simplify the signalling of the replicas location within the header. At the receiver side, the receiver will need to operate with a sliding window. The receiver window duration shall exceed the virtual frame duration, while the window shift shall be small enough to guarantee that no decodable replica is lost after the moving of the window forward in time. The successive interference cancellation (SIC) procedure iterates within the receiver's decoding window, and iteratively cleans up the received signal every time a replica is correctly decoded. The successive interference cancellation in CRA is also described with the example of Fig. 5-2.

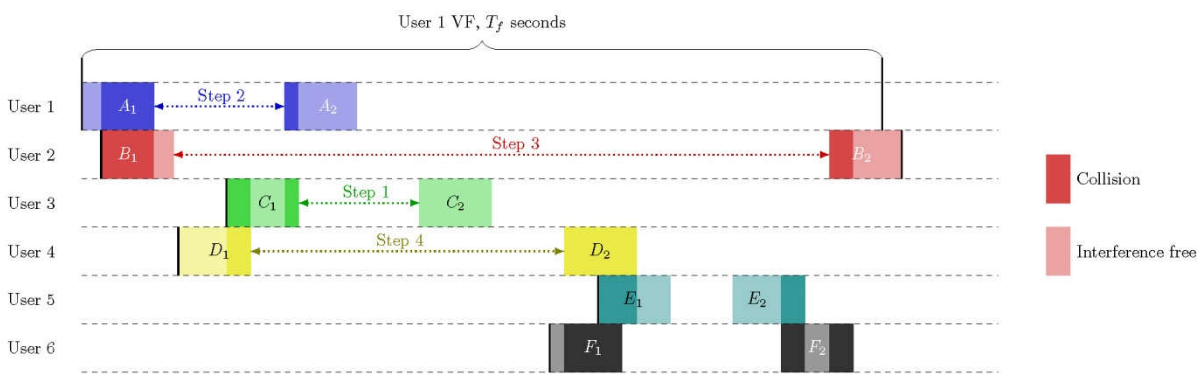


Figure 5-2: SIC Procedure of CRA

The receiver starts seeking for replicas that can be correctly decoded. The first one to be found is replica C2, which is free from interference. Interference cancellation can be applied once the location of C1 is retrieved upon successful decoding of the packet content, leading to a decrease in the interference level perceived by replicas D1 and A2. In the second step replica A2 is correctly decoded and SIC is applied on both A2 and A1. Iterating over all detected replicas yields the successful retrieval of all data packets of users 1 to 4. User 5 and 6 may be also decoded, assuming that the PHY error correcting code used to protect the replicas is strong enough. Extensive studies have investigated a reasonably good waveform and identified the configuration using 2 replicas, QPSK modulation Turbo Code rate 1/3 as very good candidate [6].

The presented scheme can be extended to be adopted also with multiple channels. The key difference is that terminals are required to be able to operate on different frequencies. A full CRA protocol implementation will be implemented in SDR, including all estimation, encoding and decoding blocks. Random Access protocols in general, feature high flexibility in terms of population size, mobility, terminals inhomogeneous requirements. The presented protocol is able to achieve high efficiency with low terminal complexity (and therefore cost) so to be very appealing for the industry as well.

In Figure 5-3 the high level architecture of the testbed is presented. At transmitter (Tx) side the aggregate traffic of the multiple transmitters is generated by a single hardware unit (PC). The full transmitter chain including, data generation, encapsulation and header generation, encoding, physical layer preambles and pilots (for detection and channel estimation) are added. The signal is then oversampled and pulse shaped. White Gaussian noise, typical channel model for satellite channels is added. The generated signal is passed to the SDR which converts the digital signal into analogue domain and transmits it. At the receiver side, the SDR is responsible for the analogue to digital conversion. After matched filtering, packet detection is performed.

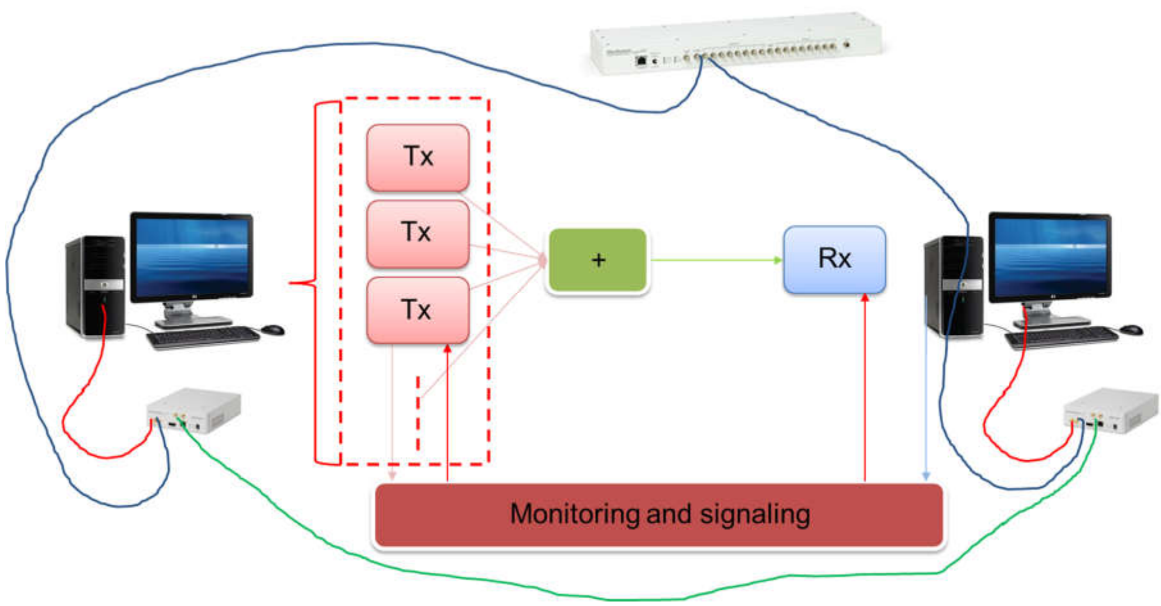


Figure 5-3: Prototype return link

For all candidate replicas identified, detailed channel estimation (including timing, frequency and phase offset estimation) is performed. The channel decoder counteracts the channel noise and finally, upon correct decoding, the data transmitted is retrieved at the receiver. Once this is achieved, successive interference cancellation on the replicas of the decoded packet takes place. Both the transmitter and receiver SDR are connected to a GPS-based external reference clock that guarantees high stability of the oscillators for timing and frequency offsets.

The setup can be interconnected with the demonstrators on Ethernet level, as can be seen in the table above. Ethernet traffic is required as input and will also be the output whereby the SatCom characteristics have been considered.

5.4 Conclusion

We presented a SDR based prototype for SatCom that can be used for evaluation and lab-test. It is based on a modern RA scheme focusing on signalling application.

5.5 References

[1] Indra, ALG, “Study on feasibility of SATCOM for railway communication Final Report”, ERA 2016 01 SC

[2] N. Abramson, “Multiple Access in Wireless Digital Networks,” Proc. IEEE, vol. 82, no. 9, pp. 1360–1370, Sep. 1994.

[3] R. De Gaudenzi, O. Del Rio Herrero, G. Gallinaro, S. Cioni, P.-D. Arapoglou, “Random access schemes for satellite networks, from VSAT to M2M: a survey”, Intl. J. of Sat. Comm. and Net., Vol. 36, No. 1, pp.66-107, Jan./Feb. 2018

[4] L. G. Roberts, “ALOHA packet system with and without slots and capture,” Proc. SIGCOMM Comput. Commun. Rev., vol. 5, pp. 28–42, Apr. 1975.

[5] F. Clazzer, C. Kissling, M. Marchese, “Enhancing Contention Resolution ALOHA Using Combining Techniques”, IEEE Trans. Comm., Vol. 66, No. 6, pp.2576-2587, Jun. 2018.

[6] R. de Gaudenzi, O. del Rio Herrero, G. Acar and E. Garrido Barrabes, “Asynchronous Contention Resolution Diversity ALOHA: Making CRDSA Truly Asynchronous”, IEEE Trans. Wireless Comm., Vol. 13, No. 11, pp.6193-6206, Nov. 2014.

5.6 Authors

Benjamin Barth graduated in Electrical Engineering at the Technical University Berlin (TUB) in 2014. He was a working student at Fraunhofer Heinrich Hertz Institute (HHI) where he wrote his Master's Thesis connected to the EU-FP7 project BATS. Since 2015 he has been with DLR's Institute for Communications and Navigation working on EU and ESA projects. He is currently serving as Technical Coordinator of the EU-H2020 funded HEIMDALL project and is participating in the X2Rail-1 and X2Rail-3 project. His research activity deals with networking and integration of satellite and terrestrial networks, resource management for satellite communications systems and system engineering for mobile and broadband satellite communications, hybrid systems and communications for public protection and disaster relief.

Benjamin.Barth@dlr.de

Federico Clazzer received the M.S. and Ph.D. degrees in Electrical Engineering from the University of Genoa, Italy, in 2012 and 2017, respectively. His main research interests include satellite communication systems, random access techniques, and signal processing algorithms. Since 2012, he has been with the Institute of Communications and Navigation, German Aerospace Center (DLR). During the past years, he has been involved in several national and international projects on advanced medium access and random access techniques. From 2014 to 2016, he was a frequent visitor at the Institute of Network Coding, The Chinese University of Hong Kong. In 2017 he visited the University of Sydney and the University of Newcastle. Dr. Clazzer serves the IEEE as a reviewer for transactions, journals, and conferences, and a technical program committee member. In 2017, he was appointed as an Exemplary Reviewer of the IEEE Transactions on Communications

Federico.Clazzer@dlr.de

Marcel Grec received his M.Sc. degree in Electrical Engineering from the Technical University of Munich (TUM) in 2016. Since 2018, he has been with the Institute of Communications and Navigation, German Aerospace Center (DLR) working on EU and ESA projects concerning software defined radio. Recently his focus shifted towards SatCom participating at the 9th Advanced Satellite Multimedia Systems Conference (ASMS) and 15th Signal Processing for Space Communications Workshop and at the TUM-COM Ultra-Reliable Low-Latency Communications and Applications for 5G Workshop. His main research interests include rateless codes, software defined radio and random access. During the past years, he has been with the same institute where in the context of his internships, B.Sc. and M.Sc., efficient implementations of ML decoding algorithms for fountain codes and their complexity analysis have been carried out.

Marcel.Grec@dlr.de

6 Introduction to various threats on wireless networks and their detection

Jonathan Villain , Grecia L. Romero, Virginie Deniau, Anthony Fleury, Christophe Gransart, Eric P. Simon, Raouf Kousri ; IRT RAILENIUM, Famars, France

6.1 Introduction

In railways, trains can be equipped with Wi-Fi networks for operational purposes or for passenger services. However, Wi-Fi communications can be victim of cyberattacks and used by malicious people to disturb services or intercept sensitive data [1]. We have then studied the impact of certain attacks and proposed a protection strategy based on the detection of the attacks.

In the X2RAIL-1 Project, two main attacks were considered: attack by jamming and protocol based attack. Firstly, the mechanisms of impairments and the impacts of both attacks were studied. Secondly, an outsourced monitoring solution i.e., perfectly independent of the communication network, was developed to detect the occurrence of attacks. This monitoring solution is based on the analysis of the electromagnetic (EM) signals received by a monitoring antenna and a receiver collecting EM spectra. It thus works mostly at a physical level (lower ones of the OSI model) and avoids being confronted with problems of privacy.

The first part of this abstract is focused on the description of the 802.11n communication standard and the jamming attacks. The characteristics of such attacks and the analysis of their impact are studied. The second part is dedicated to the attack detection, based on a classification method, which was studied.

6.2 Jamming signal impact on Wi-Fi communications

This study is focused on the analysis of the attacks impact on Wi-FI communications using the 802.11n protocol. This protocol is described in this section.

6.2.1 Wi-Fi 802.11n

The IEEE 802.11n standard employs the Multiple Input / Multiple Output (MIMO) technology, and Orthogonal Frequency Division Multiple Access (OFDMA). At the MAC layer, the access method is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). That means that all the stations (STA) sense the channel occupation (to check if another STA is transmitting) before transmitting any packet.

The 802.11n standard offers the possibility of using signal bandwidths of either 20MHz or 40MHz. The 40MHz bandwidth is used to yield a higher data throughput. Therefore, the data field construction depends on the bandwidth, the frame format, the number of spatial streams, and the Modulation and Coding Scheme (MCS) index. Each MCS index corresponds to a set of parameters defining the data encoding and modulation.

OFDM is a parallel transmission scheme, where a serial data stream is split up into a set of N substreams. Each substream is modulated on a separate subcarrier. The subcarrier spacing is denoted Δf and is equal to 312.5 kHz. High spectral efficiency is obtained by selecting orthogonal subchannel frequencies, i.e. $\Delta f = 1/Tu$, where Tu is the duration of the useful part of the OFDM symbol.

6.2.2 Jamming signal characteristics

The existence of telecommunication jammers is widely noticed despite having been banned in many countries. In the literature, there are many descriptions for jamming communication signals [2]. However, the jammers that are available on the internet at low costs are mostly of the same type. They affect the PHY layer by covering the frequency channels dedicated to the communication standard. They can cover partially or totally the frequency bands of the standard. Currently, the jamming signal does not permanently cover the whole frequency band. The jammer is basically a transmitter, whose interference signal is a chirp signal type, and its frequency band is swept in time. We call this kind of signal a frequency-sweeping interference signal. A representation is given Fig. 6-1.

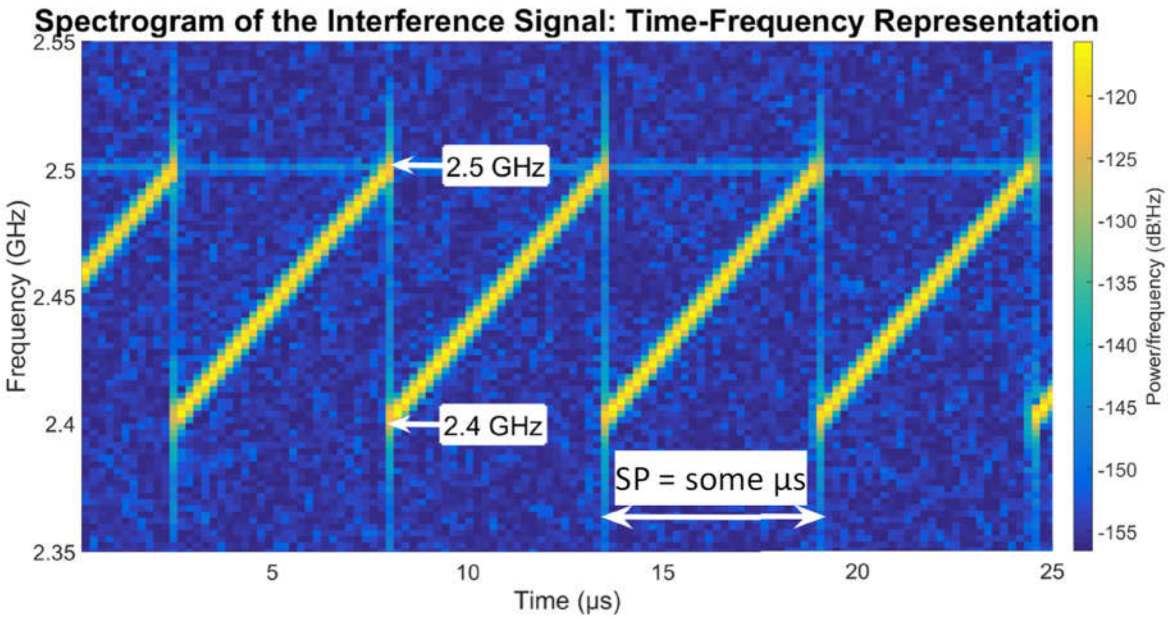


Figure 6-1: Time-frequency jamming signal representation

In comparing different commercial jammers, we noticed that the main difference in waveform of the generated jamming signal is the sweep time period (SP in Fig. 6-1) to cover the frequency bandwidth of the communication system to jam. We have then studied the impact of the jamming signals according to the value of these sweep periods [3].

6.2.3 Impact of jamming signal according to the sweep period

To analyse the impact of the sweep period, we performed tests in anechoic chamber and we controlled the bit rate of Wi-Fi communication between an access point and a client. The maximal bit rate of the Wi-Fi connection was about 100 Mbit/s. The achieved bit rate in presence of attack was measured using Iperf software. Jamming signals with different sweep periods were defined with matlab and generated with an arbitrary waveform generator. For each jamming signal, we increased step by step its power and we measured the associated bit rate. Fig. 6-2 reports the bit rate measurements for 8 different SP values of the jamming signal.

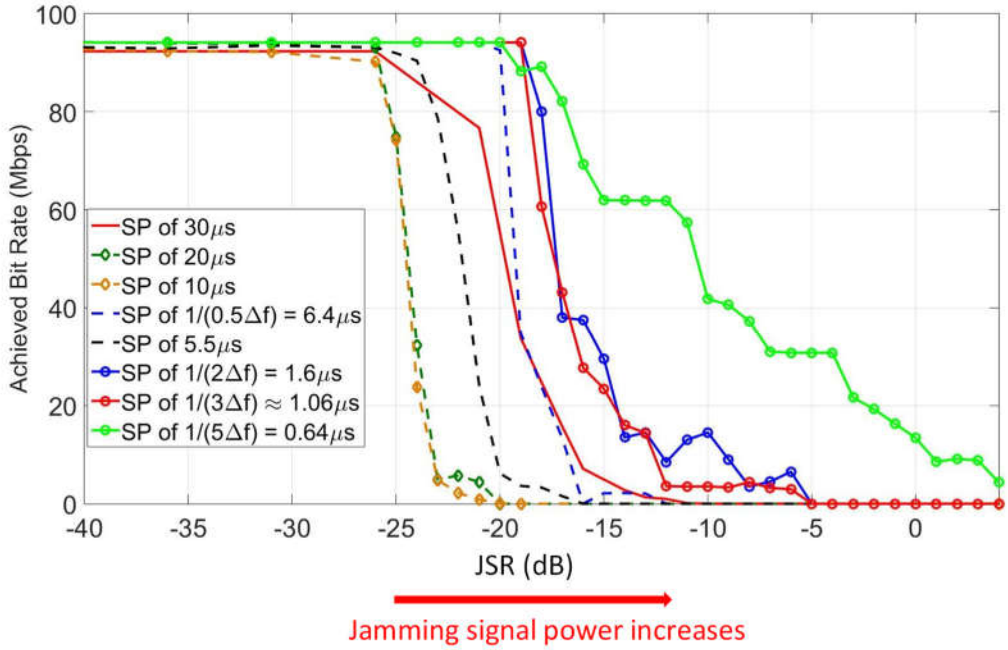


Figure 6-2: Achieved bit rate as a function of the Jamming to Signal Power (JSR) ratio

For each applied SP, the bit rate is represented as a function of the Jamming to Signal power Ratio (JSR). We observed a varying impact of the ISR on achieved bit rate: for an ISR lower than -26 dB and whatever the SP value, the system performance is not affected (i.e., the bit rate is nearly 100Mbps). However, for a JSR bigger than – 26 dB, the bit rate is affected and the loss depends on the SP of the interference signal. For example, at a JSR of -20 dB, the bit rate can be 0bps for a SP of 10 µs while the communication is never completely lost for a SP of 0.64 µs.

In these results, we observed that the most degrading jamming is obtained with a SP = 10 µs. We then applied this 10 µs sweep time in the work on the detection of attacks.

6.3 Protocol based attack

The protocol based attack that we studied is the attack by deauthentication frames [4]. This attack can be applied in order to avoid other clients to access the Wi-Fi resources and to avoid sharing the channel. This attack is also employed to disconnect a station from a licit access point and to force the station to connect to an illicit access point in order to intercept private data. In that case, that corresponds to a man-in-the middle attack.

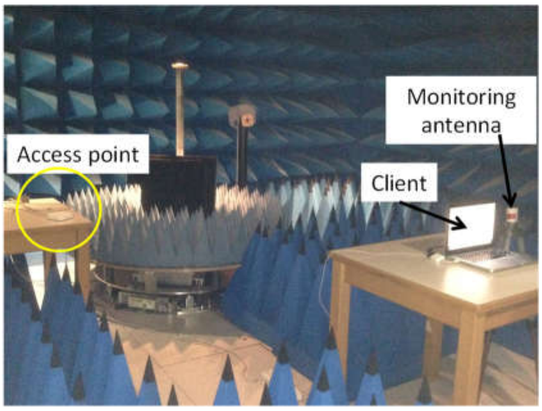
The attack by deauthentication frames uses management frames defined into the IEEE 802.11 standard. In a network infrastructure composed of several access points, when a client station (STA) is moving, the power of the Wi-Fi signal evolves. As for cellular networks (3G, 4G), a roaming principle has been specified in the standard. When a STA is connected to an Access Point (AP) and moves away from this AP, the Wi-Fi received signal power decreases. In moving the STA can detect the Wi-Fi beacon signal from another AP with an increasing power. In that case, a roaming procedure is launched. The roaming procedure consists in disconnecting the STA from the first AP and in reconnecting the STA to the second AP using IEEE 802.11 management frames deauthentication and authentication.

The attack by deauthentication sends to a STA a frame of deauthentication even if the STA is not moving. In general, the sending of deauthentication frames is repeated to keep the victim station offline.

6.4 Detection by classification

6.4.4 Experimentations

Attack experimentations were performed in anechoic chamber. During the attack, a monitoring system composed by an antenna and a spectrum analyser was employed to collect frequency spectrum along the time. The antenna is wideband biconic antenna, placed in vertical polarisation. The classification was performed on the spectra obtained.



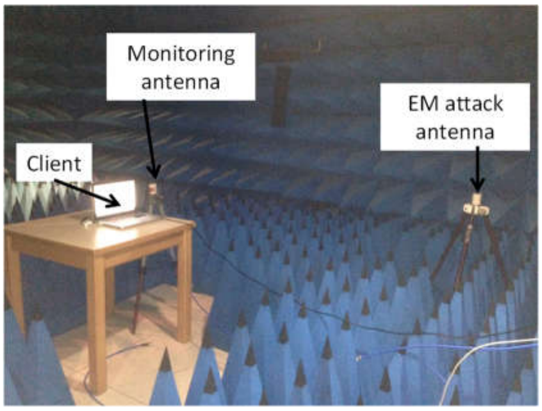


Figure 6-3: Test configuration in anechoic chamber

To assess the performances of the classification approach, we tested 6 configurations. The first configuration is without attack: spectra acquisitions are carried out with a Wi-Fi communication only. Three jamming attack configurations are tested, corresponding to three power levels of the jamming signal. The first jamming attack is performed with a low powerful jamming signal. This jamming signal has no impact on the communication quality. The bit rate is still at the maximal level. The second configuration uses a jamming signal power level which sligthly degrades the communication quality. The bit rate is reduced at about 75 Mbits/s. The third configuration uses a jamming signal power level 1 dB inferior to the required power to totally interrupt the communication. Thus, the three configurations with three different jamming signal power levels represent a jammer which would be at three different distances from the client and the AP.

Another tested configuration consists in degrading the communication quality but without any attack. To reproduce such a situation, electromagnetic absorbing materials were placed around the access point in order to degrade the signal quality. Finally, the last configuration corresponds to the deauthentication attack for which a dedicated computer has been used and introduced in the anechoic chamber. This dedicated computer sends deauthentication requests to the STA to force it to leave the Wi-Fi network.

6.4.5 Principal Component Analysis (PCA)

For each configuration, the spectra were collected along the time over a 40 MHz frequency span, centred at 2.412 GHz . The preliminary step was to check if the different situations (different attacks, absorbing materials, no attack…) can be distinguished by classification [4] [5]. A way to verify the classes can be separated is to compute a Principal Component Analysis (PCA) on all spectrum data, i.e. 99 spectra for the 6 configurations. These components correspond to the axes obtained from the eigenvectors constructed from the spectra. When we project the spectra on the two components associated to the eigenvector possessing the higher eigenvalues (see Fig. 6-4), we can check if the different configurations can be discriminated by classification.

In this figure, each point corresponds to one spectrum. The six different colors represent the spectra collected in the six different configurations: Wi-Fi communication alone in blue, Wi-Fi in the presence of absorbers in yellow, Wi-Fi with jamming signal without effect in red, Wi-Fi with jamming signal with lightly effect in green, Wi-Fi with jamming signal at the limit of the break in purple and Wi-Fi communication with a deauthentication attack in brown.

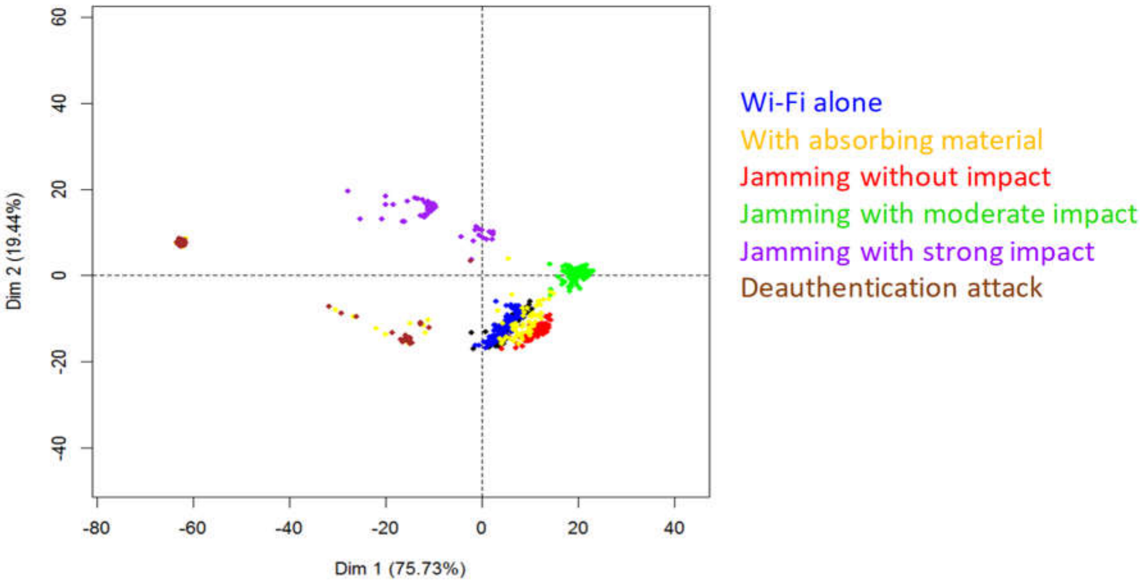


Figure 6-4: Representation of the collected spectra according to the two main components of the PCA

We notice that the attack by deauthentication is well separated from the other classes. This result is very satisfying because the nature of the deauthentication attack signal is not different from a normal communication. Nevertheless, it is significantly separated from the Wi-Fi communication alone in the representation space. We also observe a good separation of the strong and moderate jamming situations. This result is encouraging to develop a detection approach able to distinguish various kinds of attacks.

6.5 References

[1] M. Heddebaut, V. Deniau, J. Rioult, C. Gransart, "Mitigation Techniques to Reduce the Vulnerability of Railway Signaling to Radiated Intentional EMI Emitted From a Train," in IEEE Transactions on Electromagnetic Compatibility, vol.59, Issue. 3, pp. 845 – 852, 2017.

[2] M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A Communications Jamming Taxonomy," IEEE Security & Privacy, vol. 14, no. 1, pp. 47–54, jan 2016.

[3] V. Deniau, C. Gransart, G. L. Romero, E. P. Simon, and J. Farah, "IEEE 802.11n Communications in the Presence of Frequency-Sweeping Inter- ference Signals," IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 5, pp. 1625–1633, 2017.

[4] V. Ramachandran, BackTrack 5 Wireless Penetration Testing Beginner's Guide. Packt Publishing Ltd., 2011, ISBN: 978-1-849515-58

[5] V. Vapnik, "The nature of statistical learning theory. 2000," Red Bank: Springer, vol. 2.

[6] P. Halmos, Introduction to Hilbert space and the theory of spectral multiplicity. Chelsea Pub. Co., 1957

6.6 Authors

Jonathan Villain received the Ph.D. degree in applied Mathematics from the University of Bretagne-Sud, Vannes, France, in 2016 in a French Laboratory of mathematic (LMBA, Vannes) and a Pharmaceutical Laboratory (CERMN, Caen). During 2015 and 2017, he was a Teaching Assistant at the IUT of Vannes. His research field include machine learning and pattern recognition modeling in pharmaceuticals toxicity and cyber-security. He participates to WP8 Shift2Rail programs by studying classification models of electromagnetic disturbances in the railway. He is actually attached to the IMT Lille Douai as a Postdoctoral fellow.

jonathan.villain@imt-lille-douai.fr

Grecia L. Romero received her B.S degree in Electrical Engineering from University of Carabobo, Valencia, Venezuela in 2002. In 2002, she joined the Department of Electrical Engineering, University of Carabobo, as an Instructor and became an Assistant Professor in 2010. Since 2011, she has been working in the Telecommunications Engineering department at the University of Carabobo, in the area of signals and systems where she was Director of the department and became an Aggregate Professor in 2012. She received the PhD degree in 2017 at the University of Lille. She is actually attached to the Railenium test and research center as a Postdoctoral fellow. Her current work is focused on analysis of the impact of the intentional electromagnetic (EM) interferences on the performance of LTE communications.

Grecia.ROMERO@railenium.eu

Virginie Deniau, IFSTTAR, IRT RAILENIUM, virginie.deniau@ifsttar.fr
Anthony Fleury, IMT Lille Douai, IRT RAILENIUM, Famars, France
Anthony.Fleury@imt-lille-douai.fr
Christophe Gransart, IFSTTAR, IRT RAILENIUM, Famars, France

christophe.gransart@ifsttar.fr
Eric P. Simon, University of Lille, IRT RAILENIUM, Famars, France, eric.simon@univ-lille1.fr
Raouf Kousri, IRT RAILENIUM, Famars, France

7 Railways cyber security, human factors part: What happens when the automatic countermeasures fail?

Patrick Millot ; Université de Valenciennes, LAMIH-UMR CNRS, Valenciennes, France & IRT RAILENIUM, Famars, France
Mathieu Mouchel, Christopher Paglia ; rHesuS Consulting, Famars, France *& IRT RAILENIUM, Famars, France*

7.1 Introduction

The networks used in the Railway domain are usually heterogeneous, not enough protected and not fitted to the usual Cyber Security requirements in terms of sustainability, protection and attack detection. Furthermore, the quick evolution of the telecommunication means, the threats and the sustainability aspects have to be taken into account in order to protect the Railway system.

The contributions of Railenium are divided into three main steps:

1. monitoring the environment in order to detect potential threats by detecting abnormal behaviors with dedicated algorithms,
2. an automatic treatment that decides which reaction to take (e.g. an alarm or a reconfiguration).
3. The third approach is reported here. It deals with the human part in complement to the first ones and tries to answer the questions:

If the automatic detection and mitigation fail the human remains alone in the loop to try coping with the consequences of the attack. Can the human replace the automatic means to detect and mitigate the threat? If so, how can we support him/her to finally secure the system or at least avoid the worst consequences?

The research presented here aims at assessing the professional human driver and OCC supervisor abilities to detect, to understand and to react to (simulated) cyber-attacks, or to their consequences, in a realistic simulator. For that purpose, we chose and play scenarios involving humans, and analyze their behaviors and their abilities to detect and to mitigate the threats. Then, the method will look for strategies, indicators and devices useful for human counter measures. More generally, the work consists in improving human detection and recovery and enhancing their Situation Awareness.The reader interested in the theoretical aspects of the work can find the foundations in the next section. Otherwise, the cybersecurity part starts at section "General Method against Cyber Attacks ".

7.2 General Principles to Treat Unexpected Events

Our approach focuses on "**human(s) in the loop**" systems and simulations, taking advantage of human ability to cope with unexpected dangerous events on one hand, and attempting to recover from human errors and system failures on the other hand. That can be achieved through a human centered automation [1]. It is based on the concepts of **vulnerability** and **resilience** [2] and **risk management methods**.

7.2.1 Vulnerability assessment

Vulnerability "corresponds to the sensitivity of a system to threats in specific circumstances or catastrophic situations depending on:

- v1: the context influencing the system and its threats (social, political, moment in the day…) at a given time,
- v2: the potential threats able to disrupt some or all the main system functions,
- v3: the system functioning and its components especially those subject to degradation".3

In our study, especially v2 and v3 classes of parameters will be taken into account in a vulnerability analysis. We will proceed to:

- va1: the threat characterisation (the type of event particularly malevolence),
- va2: the identification of physical, informational, organizational defensive and reactive properties of the system,
- va3: the environmental and internal circumstances in space and time; for malevolent threats, the political economic and social climate are important.

Mainly va1 and va2 are taken into account here, assuming that v1 as well as va3 parameters are at a high dangerous level.

7.2.2 Resilience and Risk Management

After this vulnerability analysis phase, we try to find preventive actions for reducing the vulnerability or mitigating the consequences, and so enhancing the overall **system resilience**. Resilience is the "ability of a system to recover from a perturbation or a danger that could change the system state to unacceptable" [2].

The strategies are then based on risk management methods dealing with prevention, decision-making, action taking, crisis management and recovery, taking into account consequences of unexpected events, whether the origin, a technical failure, an unwilling human error or a deliberated attack [3]. The approach globally developed here consists in three complementary steps:

- **Prevention**, where any unexpected event could be blocked or managed before its propagation. In our case, let us imagine a cyberattack on the OCC numerical information system attempting to propagate wrong data on the vehicle location. Prevention measures could have detected and blocked the attack on the Automatic Vehicle Location System

(AVLS). Moreover prevention consists in anticipating this attack - and more generally all possible attacks we can imagine - and in enhancing the protection. In our example that can be achieved by coding and encrypting the communication channel between OCC and drivers.

- **Recovery**, when the prevention measures fail and the attack is close to result in an accident, protective measures become mandatory to avoid the occurrence of the accident. In our case, let us imagine the attack succeeds propagating wrong messages. Different countermeasures can then be available: stop all the vehicles, send an alert to the whole vehicle fleet …

- And possibly if recovery measures fail and an accident occurs **management of consequences** is required to minimize damages, at least the most severe ones. In our case, this last step can consist in starting a general rescue plan involving emergency teams, medical personal, rescue equipment…

Along these 3 steps and mainly the 2 first ones automatic solutions can be studied. But these automatic means can fail, and for that reason a safety and security policy generally places a series of several kinds of defenses of different and complementary natures: **technical, procedural, human** and **organizational** [2].

Technical, procedural as well as **organizational defenses** must have been foreseen so that the countermeasures may be played in an adequate manner. Moreover the defense based on the organization is relevant to give a collective answer and to test the pertinence of the series of defenses regarding the characteristics of the attack.

However the serial defenses can be insufficient in themselves to insure the total robustness against the attacks. For instance as shown by Reason (1990) [4] with the wellknown Swiss cheese metaphor, each defense cannot be fully efficient to block anunexpected event. Then placing several successive defenses aims at blocking the event propagation with the second or third defense in case the first one fails, like a hole in the Swiss cheese. But in some rare cases, according to Reason's metaphor, the holes of the series of defenses can be aligned, which makes the serial defenses inefficient.

The last kind of defense we mentioned above is "**human**". What we mean by "human defenses" deals with all the events that have not been foreseen, and for the treatment of which no solution still exist. Therefore, the humans involved in the control and/or in the supervision of the transport system remain the last "barrier" to block or mitigate the threat.

Can these humans be efficient in this role? Must they be aided to do so, and how? For instance in increasing their Situation Awareness? with dedicated tools? individually or in an adequate organization? We will evaluate that experimentally.

7.2.3 Resilience based on human Situation Awareness

Situation Awareness (SA) is defined by Endsley as "the decorative term given to the level of awareness that an individual has of a situation, an operator's dynamic understanding of what is going on" [5]. Endsley's model is based on three levels of SA, the human ability to **perceive the elements** (SA1), to **understand the situation** (SA2) and to **project that situation in the future** (SA3). SA is very useful for evaluating and enhancing the system resilience, either by an individual Operator [6] or by a team [7].

Supporting human SA is a central issue in several domains aiming at enhancing safety purposes and can be transposed to security. In the Nuclear Industry K. Schmitt proposes a method to assess the human operator behavior when he/she faces with incidents depending on whether a procedure does exist or not [8]. She exhibits several cases (of minor incidents) where the procedure does not exist and the operator does not produce the right answer. D. Platt and colleagues show that astronaut SA increases when assisted with a dedicated tool in critical phases of a deep space exploration mission [9]. In a simulated crisis situation of a Nuclear Power Plant L. Stephane shows that a 3D visualization improves risk assessment and management, especially in complex situation involving the sociotechnical system and the environment together [10].

In the present study, our objective is to enhance the system resilience through maintaining the tram driver SA. Then we are looking for a method allowing to understand (and to model) the driver cognitive mechanisms. Therefore we do not pretend providing exhaustive enhancements to the transport system face with cyberattacks. But we intend proposing a method for supporting the human operators involved in preventive and recovery actions to a cyberattack.

7.3 General Method Against Cyber Attacks

The principle consists 1) in placing the professional human drivers and OCC supervisors in a realistic simulator, face with scenarios of malfunctions which could result in the consequences of a simulated cyber-attack and 2) to observe these drivers in order to assess their abilities to detect the threat and to react.

7.3.4 Method in five steps

This method is deployed in 5 steps:

1) It starts elaborating a list of threats and building related scenarios (ie. an external entity takes the control of the train, or of certain devices or the control of signals). The choice of the threats is done through an analysis of the vulnerability to cyber-attacks especially of connected and wireless devices. To be chosen the threat must have a consequence on the driving task and /or on the vehicle behavior and the driver must be able to get the relevant information to detect it and to react, either using the commands or sending an alarm to the OCC supervisor.

2) The consequent behavior of the related devices is then used as a scenario to be simulated. Devices that remain robust to cyber-attacks, for instance because of their old technology are ruled out of the list.

3) Then in the 3rd step we simulate the scenarios involving real humans (usually professional drivers of a tram company) and analyzing the human behaviors through dedicated sensors like camera, eye movements, completed with dedicated indicators such as workload, Situation Awareness, [3] and questionnaires, in order to evaluate their abilities to detect the threats, and to give relevant answers. The scenario can be replayed of line in front of the tested human operator in order to allow the analyst asking relevant questions for further explanations on the operator behaviour, called auto-confrontation. In a variant, called allo-confrontation the analyst asks a second operator who has the same Know-how to give explanations and comments in place of the real driver on a track of his/her recorded activities. At least 12 real human operators must participate to the experiments, in order to allow the analysts comparing the different answers and detecting convergences as well as divergences in their behaviour.

4) The forth step consists in analysing these answers, the most relevant ones could be derived to establish new strategies, new procedures and/or new devices useful for human countermeasures. An important issue is the existence of procedure – or not - to respond to the threat, that impacts the human behavior in detecting the problem, understanding it, and finally finding the relevant answer. If the procedure does exist, the designer must enhance the driver Situation Awareness through, for instance dedicated displays (ie: from the detection algorithm and the automatic blocking module). If the procedure does not exist, the only answer will come

from the human imagination to invent (or to adapt) a relevant countermeasure (for instance a general safety procedure as a general emergency stop). In that important case, this new solution must be transposed into new procedures and inserted in the past experience feedbacks for enhancing a training program or building a dedicated assistance tool.

5) Finally, in an ideal project, these procedures and/or devices should be integrated with new scenarios to the simulator for evaluating their utility.

7.3.5 Transposition to threat detections

Following the method described above, the first choice was to identify a set of vulnerable devices the unusual behaviors of which could result of a cyber-attack, ie: 1) loss of the speedometer display (or displaying a wrong speed value) in the cabin, 2) loss of braking, 3) jamming or disappearance of the camera rear view) in order to study the driver answers.

The list of threats to be reproduced in the simulator is established according to 4 criteria: the technical plausibility of the threat (is it technically possible?); the dangerousness of the threat and because we are in an exploratory study, the technical possibility to simulate the attack with our simulator. In a more systematic approach, this last criterion can be waived in enhancing the simulator. A fourth criterion is the possibility to transpose the attack to another kind of rail system, for instance from tramway to metro or to train.

Let us remark that our discussion with the professional operators of this area does not mention any training dedicated to the management of cyberattacks, neither at the driver level nor to the OCC level.

Once the list of threats established and due to the lack of training of the operators to deal with these attacks, the next step was to evaluate malfunctions that could be relevant results of the attack, and to test if they are realistic. As already mentioned above, the advantage is to define relevant procedures to face with the malfunctions and evaluate if the humans are able to implement them in case of a cyberattack. The identification of the relevant procedures has been made through discussions with several drivers, training instructors, supervisors coming from different French transport networks (mainly North and North-West). Analyses of several regulation documents and training programs were made.

7.3.6 Simulator PSCHITT-Rail

The Simulator PSCHITT-Rail (French acronym for: Collaborative, Hybrid, Intermodal Simulation Platform in Land Transport – Rail) is developed at LAMIH, lab of the University of Valenciennes. (https://www.uphf.fr/LAMIH/en/PSCHITT-Rail)

It allows 4 functionalities:

- an editor of infrastructures: railways for tram and train, with their environment (traffic, passengers on the platform, technical equipment); 45 km of railways are stored in the data base and original tracks can be developed by the software designer,

- an editor of scenarios allowing to create time tables, itinerary management and events. Several scenarios corresponding to unexpected events can be stored in the data bases and played several times to several human drivers or supervisors. For instance, events occurring on the trains could result on braking defaults, wrong on-board signals… On the railway, error on rail switching control device, disturbance on the way signals, disturbances on rail-road crossing barriers can be simulated. Specific events can also be programmed by the software designer.

- a driving cabin with one driver equipped with the same devices as in a real tram-train or tram (see Figure 7-1). In front of the cabin, several screens display the dynamic scenes the simulated tram is inserted in.

- a supervision work place (Operational Control Center) with a human supervisor face to the same devices as in a real system: network synopsis, trains signals, rail switching …

The simulator is mobile and its movements are programmed to give the cabin some realistic dynamics regarding the simulated scenario (see Figure 7-2).

Figure 7-1 Simulator PSCHITT-Rail Driver desk

Figure 7-2 Simulator PSCHITT-Rail cabin

7.4 Case Studies and Results

We only describe here two examples: the loss of control of the rear vision system and the loss of braking system.

7.4.7 Attack on the rear vision system

The first example relates here the result of the loss of control of the rear vision systemwhich usually allows the driver to monitor through cameras the behavior of the passengers on the platform, especially when the tramway arrives in a station. At this moment he/she selects the side corresponding to the platform for opening the doors. That allows displaying on the screens the content of what take the front and rear cameras. Then the driver can monitor the passengers entering and going out the tram.

A loss of this device can result in a serious incident or accident as reported as follows by one of the operators tested in our study who was confronted in his professional life at his driving post.

He stopped his tram at a station and was going to restart after having checked the platform. But just before starting he decided to check again the rear vision, and then he detected a person who was lying on the platform and tried to catch with his hand an object under the tram. The driver said "if I started my tram at this moment, this person would get his arm cut". This anecdote shows the real interest of the rear vision for security.

The scenario starts with a normal driving during 30 minutes in a realistic and moderately loaded environment (downtown, station with several pedestrians, rail-road crossing). Then the attack appears and results in the loss of rear vision when the tram arrives at an overcrowded station with the platform on the right side of the way. The driver must then select the right side doors to be open, but due to the attack, the rear view shows an empty platform, despite a lot of passengers were visible outside on the platform and even on the pedestrian sidewalk (through the simulator screen, see Figures 7-3 and 7-4). The usual procedure the driver should apply in that case, is to call OCC; by order of the OCC supervisor, the driver must interrupt his service or return to the depot in deadhead mode (no passengers in the train); cross the stations at a low speed (less than 10km/h) ; and mention the anomaly on the roadmap.

Then we would have logically expected that the different tested drivers apply this procedure, thinking to a breakdown. But none of the 6 drivers detected the display discordance (no extension of the stop time in the station, no particular comment, to him/herself or to the OCC supervisor, no special surprise). During the debriefing after the experiment all drivers say they did not detect an abnormal display of the rear views. They were all focused on the driving post showing the doors, they wait they close and then restarted the tram to quit the station.

Figure 7-4: Direct outside view through the window

Figure 7-5: Example of rear view display (side part) incoherent with the real direct outside view

7.4.8 Attack on the braking system

The second example is related to the loss of braking, which is a main fear of the questioned drivers. Discussions with maintenance operators and the companies relate that only the emergency braking engaged through the dedicated devices on the desk is robust to an attack. That gave us a track to build the second scenario.

The tram is rolling on a straight line after a curve in a urban environment with few information to manage. The drivers enter this zone of experiment with an average speed of 30.5 km/h (σ

=2,3). The speed limit is 40 km/h. 218 meters behind the curve, the simulated environment plays a station where the tram must stop. But 183 meters ahead the station a simulated loss of the braking devices of the tram occurs. The aim was to test the driver reactions (response time, braking distance, actions on the driver's desk, verbal comments…) when facing with this malfunction.

At the beginning of braking, the driver behaviors are quite homogeneous: the average braking distance was 72.9 meters ahead the station (σ =14.7). All the drivers have detected the braking defect and engaged the rescue braking (5/6 used the master controller, 2/6 the emergency stop key, 1 driver then used both devices). The average tram response time after an Emergency Braking engagement is 20.8 seconds (σ =3.2). The average distance to stop the tram is 225.6 meters (σ =18.6). Then the trams driven by 3 drivers among crossed the station: 2 at a distance of 4 meters, 1 at a distance of 25 meters.

At the debriefing, the drivers mentioned they perceived an incoherence between their action on the master controller and their proprioceptive and/or visual perception: "I expected to perceive the deceleration, but I did not", "the scene seemed to go too quickly".

7.5 Discussion

These results are very instructive and surprising:

- Many drivers are not trained for detecting such abnormal situations, they seem to favor the direct vision instead of the devices, even these ones increase the safety;

- No training sessions are proposed to the drivers to detect as well as to manage such situations, and moreover no dedicated procedures do exist.

- Therefore, even the automatic countermeasures fail to prevent or to block the attacks, at least they could provide a signal in order to alert the human drivers or supervisor of the occurrence of the attack and place them in an increasing vigilance state for allowing them to react.

- During the more routine activities like braking management drivers seem fully able to quickly detect a malfunction and to react appropriately in order to make the situation safe and secure. But, some of them had a lack of anticipation and fail in stopping the tram early enough.

Of course these results should have been confirmed by the other cases as evoked above, but they are encouraging for developing a relevant methodology to reinforce the driver ability to detect and treat the cyberattacks, especially to define and implement relevant devices for that, that could be seen as "manual countermeasures". Moreover as this kind of study is also carried out in other domains, such as aviation, our results could also be compared with these other results [11]. Finally this methodology could be extended to several other situations for reinforcing trouble shooting procedures for the rail driving and management.

7.6 Conclusion

The human approach is developed to give a final answer to consequences of cyberattacks especially if the preventive and recovery automatic countermeasures fail. In these cases, the human driver or supervisor is alone to face with the attack and we studied experimentally the strategies he/she develops to answer the attack. A methodology has been described involving the way to choose the more realistic attacks, to simulate their consequences in dedicated scenarios played on a realistic dynamic simulator and the data to be recorded during the experiments and the expected results. Two examples show the experimental results of two types of abnormal behavior of the tram. Reactions of 6 drivers have been studied and the results showed that their capacity to detect a malfunction depends on the situation and on the function under attack. These results were briefly discussed.

This methodology to choose relevant cyberattacks to simulate the consequences of them seems adequate in order to draw a training program for the drivers and to enhance the procedures for fighting against cyberattacks.

Moreover it seems pertinent to extend the methodology to more general trouble shouting situations in order to define new operation procedures (especially in the cases they do not exist at present). Another extension could concern new tools to assist the driver fault detection capacity and maintain their Situation Awareness.

7.7 Acknowledgment

The authors would also like to thank the engineers of LAMIH-PSCHITT-Rail for their involvement.

7.8 References

[1] Millot P., (ed). Designing Human-Machine cooperation systems, ISTE-Wiley, London, June 2014, 386 pages, ISBN 978-1-84821-685-3.

[2] Chatelet, E. Vulnerability and Resilience Assessment in Infrastructures and Networks: Concepts and Methodologies. In P. Millot (ed) "Risk management in Life Critical Systems", ISTE-Wiley, London, pp 21-40, ISBN: 978-1-84821-480-4. October 2014

[3] Millot P., (ed). Risk management in Life Critical Systems, ISTE-Wiley, London, 420 pages, ISBN: 978-1-84821-480-4. October 2014

[4] Reason J., Human errors, Cambridge University Press, 1990.

[5] Endsley, M., Towards a Theory of Situation Awareness in Dynamic Systems, Human Factors, 37(1), pp 32-64, 1995.

[6] Millot P., Situation Awareness: is the glass half empty or half full? Cognition Technology & Work, Springer, London, volume 17, Issue 2, pp 169-177, May, 2015, DOI: 10.1007/s10111-015-0322-6.

[7] Millot P. and M. P. Pacaux-Lemoine, "A common work space for a mutual enrichment of human-machine cooperation and team-situation awareness," Proceedings of IFAC HMS 2013, vol. 12, no. PART 1, pp. 387–394, 2013 DOI: 10.3182/20130811-5-US-2037.00061

[8] Schmitt K., Function Allocation in Complex Socio-Technical Systems: Procedure usage in nuclear power and the Context Analysis Method for Identifying Design Solutions

(CAMIDS) Model. PhD dissertation, Florida Institute of Technology, USA, December 2013.

[9] Platt, D., Millot, P. & Boy, G.A., Design and Evaluation of an Exploration Assistant for Human Deep Space Risk Mitigation. 12th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Human-Machine Systems. Las Vegas, Nevada, USA, August, 2013.

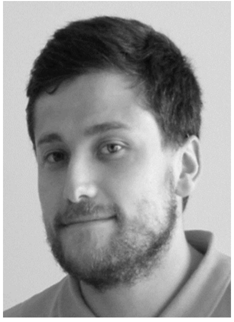
[10] Stephane, A., L., Visual Intelligence for crisis management, PhD dissertation, Florida Institute of Technology, USA, November 2013.

[11] Gontar,P., Homans,H., Rostalski, M., Behrend,J.,Dehais,F.,Bengler,K., Are pilots prepared for a cyber-attack? A human factors approach to the experimental evaluation of pilots' behavior. Journal of Air Transport Management 69 (2018) 26–37.

7.9 Authors

Patrick Millot received a PhD in Automatic Control (1979) and is “Docteur d’Etat es Sciences” (1987). He is full Professor at the University of Valenciennes (Université Polytechnique Hauts de France) since 1989. He conducts research on Automation Sciences, Artificial Intelligence, Supervisory Control, Human-Machine Systems, Human Reliability and Situation Awareness with applications to production, telecommunication and transport systems (Air Traffic Control, Car Traffic, Trains, Metro…). His scientific production covers about 200 publications, collective books, conference proceedings. He has been research supervisor of 40 PhD students and 11 HDR since 1989, reviewer of 51 PhD Thesis and 11 HDR from other universities. He was successively head of the research group “Human Machine Systems” in LAMIH (1987-2004, 25 researchers), head of LAMIH (1996-2005, 222 researchers and engineers) and vice President- in charge of Research of the University of Valenciennes (2005-2010). He was member of the scientific board / Manager of several regional research groups on Supervisory Control and Transport system safety. He was also member of the French Council of the Universities (CNU 1996-2003), member of the scientific board of the French national research group in Automation Sciences supported by CNRS (1996-2001). He was partner of several European projects and networks and IPC member of several International Conferences and Journals, member since 2000 and Vice Chairman since 2009 to 2011 of the IFAC Technical Committee 4.5 Human-Machine Systems. He was visiting Professor at Florida Institute of Technology (Melbourne FL 2011-2012).

patrick.millot@uphf.fr



Mathieu Mouchel is a Cognitive Psychologist, expert in Ergonomics, Human Factors and Organization since 2012. He took part to several projects for designing railways systems.

mathieu.mouchel@rhesus-consulting.fr

Christopher Paglia is expert in Ergonomics, Human Factors and Organization with 6 years of experience in designing human machine systems, especially Expert interface, Final User interface with application in railways systems, work stations, and a particular interest for disabled persons employment.

christopher.paglia@rhesus-consulting.fr

Christopher and Mathieu both created rHesuS Consulting Company in march 2017. They took part to several projects for guided transport system design (rolling stocks, infrastructure), aiming at integrating the final Users through an experimental human centered approach mixing risk analysis methods, Human Factors and Organization.

8 Shifting tests from on-site to the lab for automatic train operation

Oliver Röwer, Lennart Asbach, Michael Meyer zu Hörste; German Aerospace Center (DLR), Institute of Transportation Systems, Braunschweig, Germany

8.1 Introduction

"Zero on-site testing" is the title and hence the target of Shift2Rail TD 2.6. The objective is to standardise the testing scope and procedures for signalling and telecom systems in order to improve quality and interoperability, reduce significantly on-site testing as well as the time to market. Due to the complexity of railway signalling systems and the differences between sites, many tests must be carried out on-site, which takes about five to ten times the effort of similar laboratory tests. Reduction of on-site tests for railway signalling systems is therefore a reasonable approach to reducing testing costs.

Today functional testing becomes more and more important, as complex train control systems (e.g. ETCS) offer a lot of functionalities, with their specification written in natural language. The tests are necessary to reach real interoperability but also offer a chance to reduce the field tests. DLRs research aims to reduce time and costs of test runs and increase the scope of the tests to make the final European admission as easy as possible.

With its laboratory RailSiTe® DLR is researching tomorrows testing methods in the railway domain. Main focus of the research is testing for ETCS and the standardized interfaces. In the field of ETCS especially the on-board unit (OBU) and radio-block centre (RBC) communication is focused, but also interfaces for Interlocking and field elements are included to allow a comprehensive test execution and evaluation. By now the test bench is able to connect to almost every RBC in the world using internet protocols and special tools for GSM-R adaption. The goal of the research work on OBU testing is attained when the following scenario is reality: All ERTMS tracks are virtually rebuild in a test bench. All European operational scenarios have been created and formalized. Assuming this, there cannot be any requirement in the system specification, which is not tested in one of the operational scenarios. If there is any, it can be removed from the specification, because it is obviously not needed. By virtually testing every new on-board system on the entire European network in all operational situations, interoperability is proven and inherits conformity.

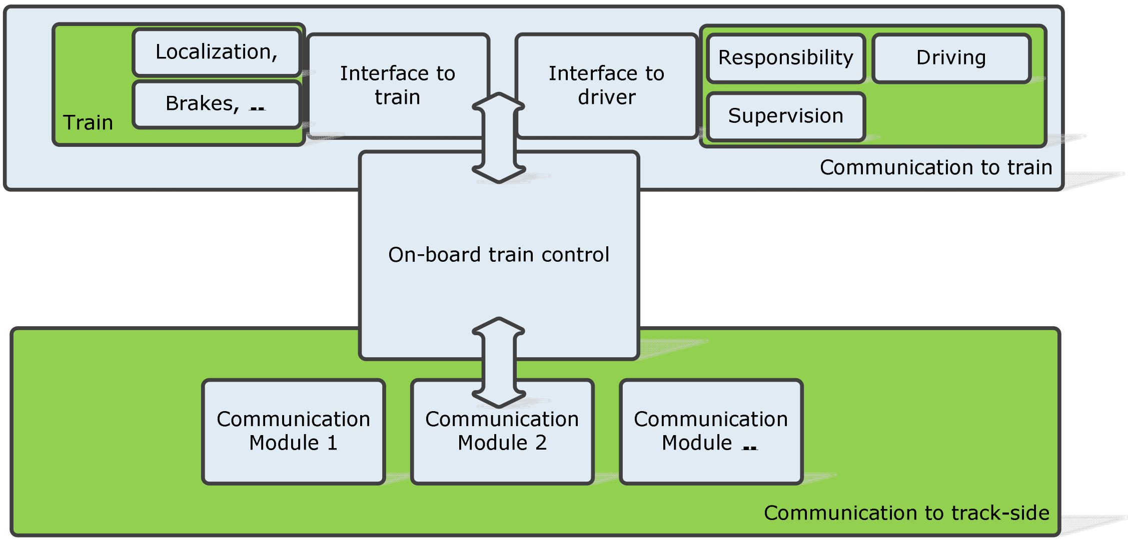


Figure 8-1: Overview of current setup of on-board train control

Fig. 8-1 shows a basic setup of today's on-board train control. The communication to the track-side is available by many technologies, in case of ETCS one of the communication modules could be the GSM-R channel. The train interface is also already connected to the train control system. Information and commands are exchanged, e.g. braking, doors, pantograph or localization information. In most cases the driver has to control the traction lever according to the information of the train control system. From a technical perspective the main task of the driver is supervision and responsibility for the train.

Due to the increasing demand for automated train operation (ATO) this gets more and more into the focus of DLR's research. Also one of the goals of Shift2Rail TD2.6 "Zero on-site testing" is to integrate new functionalities like ATO, next generation of communication systems, moving block and many more into the general test architecture for lab-testing.

Right now there are already many ATO systems, or at least driverless systems, available and in service. The real challenge will be the implementation of those systems on main-line tracks. Having a look at the current train control systems, on the functional level there is only a very small gap between driver-operated and automatic trains. The track-train communication is safe and ready for automatic train operation. Thus we can assume that the ATO for main line tracks will be an add-on module for train control systems. This includes track-side and on-board systems. This contribution shows first ideas to reuse current testing methodologies for testing ATO systems.

8.2 Testing on-board ATO modules

8.2.1 Changes in testing due to ATO

In the current implementations the on-board conformity tests are running 100% automatically. Since the driver machine interface (DMI) has to be part of the test, because of the current law, it is controlled by a robot. The train interface is controlled by the laboratory. In case of ATO functions of the system-under-test these laboratory modules (robot and train interface) can be replaced by the ATO module. At least if the ATO module is tested together with the on-board train control (in case of ETCS this is called European Vital Computer, EVC) the test could be performed in the same manner but with less effort on the laboratory side.

The interesting question is what additional descriptions in the test specification are necessary to ensure the proper testing of the ATO module. Since we assume a black-box test for the ATO module, the first inspection has to be done on the interfaces of the module. Today there are many ideas for these interfaces; one could be the reuse of the interface between the DMI and the EVC, in case of ETCS. As long as there is a radio connection available between the track-side and the on-board, all necessary information will be provided. For example a new movement authority is transmitted to the train control system and the ATO simply has to follow this information. Today it is shown with "permitted speed" and many more values on the DMI. I.e. for all information, which is available via the current DMI, the functional test specification of ETCS can be reused.

A simple approach to such an ATO module would be a listening design, i.e. the ATO module receives all information from the EVC-DMI interface but is not able to give commands back to the EVC directly (only to the traction lever). This way, both implementations would be possible: remove the DMI in fully automated trains (GoA4), or have the DMI connected additionally in case the possibility for a manual interaction by a driver or an agent is necessary (GoA2 or GoA3).

Of course, the evaluation methods have to be adapted, because now not only the train control behaviour has to checked but also the ATO behaviour (train interface unit, driver machine interface etc.). If there are any additional inputs for the ATO-module, maybe cameras to replace the driver's eyes or diagnostic systems to ensure the proper function of the train, they have to be included by adding new test cases in the test specification. Since this should be relatively easy for all "pure digital"-interfaces, like diagnostic information of the train, it will be more complex for kind of analogue information like the camera image. If, maybe due to legal restrictions, there is a certain reaction required based on the output of image recognition, this will lead to very complex tests.

The challenge is the number of possible inputs. It gets even worse, if state-of-the-art methods like machine learning are used for the image recognition. In the current authorization process the certification of a machine learning systems seems to be impossible. Current research approaches are trying to solve certification issues for machine learning algorithms by using watch-dogs, which assure that the machine cannot leave certain boundaries. But right now there is no efficient methodology found.

8.3 Solution Approach

Components and systems for railway applications, especially for safe applications, need to be tested comprehensively before taken into operation. These tests have different aims: they can be used to show that a system fulfils the relevant specification, the foreseen operational profile or safety requirements. All these tests need to be described to be performed in the field or to be formalized to be executed in a lab. Both need a formal definition and description to prove the correctness of the results.

The approach used for the conformity tests for ETCS can be extended for operational and safety lab tests, operational field tests and fits very well for testing ATO-systems, too. The principle method of the generation of the test sequences can be used for the different types of tests. The optimization criteria as well as the rules for the parameterization differ for the different kinds of tests. If the same approach for the formalisation and parameterization is used, the lab environment can be used for any type of test, with some adaptations to be made to achieve sufficient flexibility.

Test case generation and the test sequence construction profit substantially from the application of formal approaches. This field features a variety of languages, methods and tools. Present-day solutions cover only part of the needs of practice, but show potential to be much more useful if applied in a carefully designed process employing adequate formalisations.

8.4 Test Generation

8.4.2 Conformity Test Sequences

The group of eight suppliers of train control systems called UNISIG (Union of European Signalling Companies) have specified the ETCS by writing the SRS (System Requirements Specification – SRS – [2]) and produce and deliver ETCS components for different railway undertakings and infrastructure manager like Deutsche Bahn AG (German Railways) in Europe. Before these may come into operation, their conformity with the SRS and their interoperability has to be proven with lab tests as stated in the previous section.

The issue 3.1.0 of the conformity test was specified by the "Subset-076 Working Group" (CEDEX, DLR, INECO, MULTITEL, RINA). This specification includes the Hardware-in-the-loop tests of the ERTMS/ETCS on-board equipment [1], the method of their creation [3] and the method of test [4]. The specification of the reference lab architecture [5] completes the set of specifications.

The defined target of test sequences is to test each requirement of the SRS at least once. Firstly, to organise and reduce the amount of requirements of the SRS, more than 200 features have been identified. After this, the required positive and negative test cases have been created for each feature. Totally more than 1700 test cases have been generated.

Equivalent test cases for different ETCS modes or levels have been merged to reach a first optimisation and reduction of number of test cases. This means that test cases which are applicable for different mode-level combinations are described as only one test case, if the feature was not dedicated to a specific mode-level combination. Important is the testing of the feature itself. Just for clarification, each ETCS mode is an operational state of the on board equipment and the ETCS level is an overall degree of the usable functionality of ETCS.

For the execution of the tests the test cases are concatenated to 775 test sequences, which all start at the powering on of the on-board equipment and end with the no power mode. The test subsequences are concatenated due to their start- and end-conditions to reach a consistent sequence of system states. The test sequences have been optimised to reach the lowest degree of redundancy of testing. Parts of a test are only executed twice or more if they are needed to reach a state which has not been tested yet. Up to the test sequences the specification is completely generic. At this stage the variables and parameters are filled with values, though some remain to be set dynamically during execution of the sequence. So the test sequences could be understood as operational test trips.

The relation from the SRS up to the test sequence is shown in Fig. 8-2. The ETCS System Requirements Specification (SRS) can also be seen as a composition of approximately 200 features. For every feature one or more test case was created. These test cases aim to describe possible situations which may be encountered and should be tested. This way, for a correct behaviour the system-under-test has to follow at least one requirement of the ETCS SRS and every requirement of the SRS is used in at least one test case.

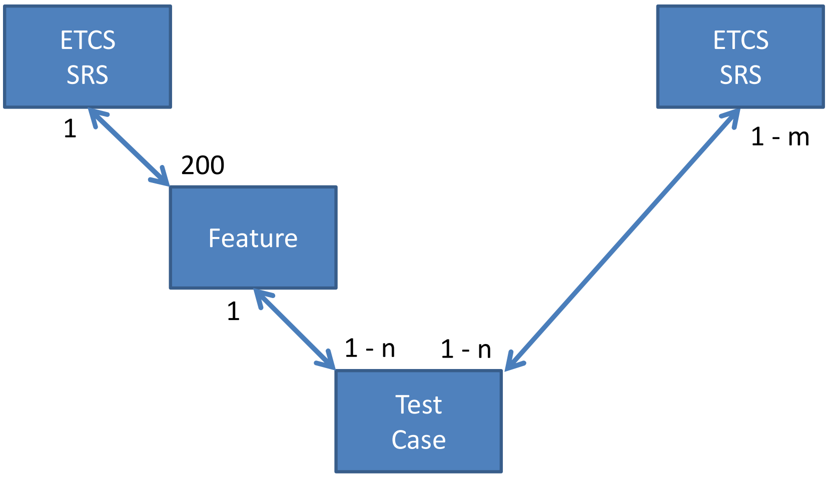


Figure 8-2: Relation between SRS and Test Sequence

Finally the fundamental structure of the test sequence should be clarified. Each test sequence simulates a test trip by stimulating the on-board equipment via the black-box-interfaces. In addition, the SRS-conformant reactions of the on-board equipment are defined in each test sequence. The reactions and the stimulating events are bound to the interface where they should be observed and evaluated or raised. Essentially the test sequences consist of the stimuli and the expected reactions of the on-board equipment. In the test sequence one stimulus or reaction is represented by a test step. Fig. 8-3 shows the structure of a test sequence.

The 775 test sequences contain up to several hundred test steps and their execution in real-time in the labs need up to several hours. A time rafting testing is not possible due to the fact that the real time behaviour of the ETCS component is tested. As mentioned above the test sequences are implemented in the reference labs. Some of the test sequences have been executed successfully, but the stated problems of duration and unstable inputs on the user interface by the human being show that automation is needed. As soon as an input is missed or incorrect the complete test sequence must be repeated.

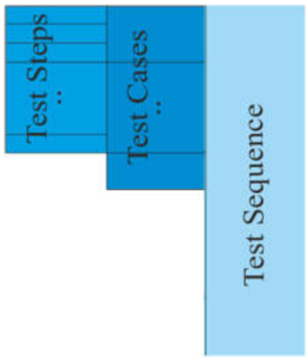


Figure 8-3: Symbolic structure of a test sequence for conformity testing

The tests defined by this method are documented in the ETCS Subset 076. These are used to proof the conformity of the constituent European Vital Computer (EVC) which is the core of the on-board unit.

8.4.3 Operational Test Sequences

The conformity test sequences which have been discussed in the previous section fulfil the purpose to show that an application is realising the specification sufficiently complete. They do not claim to be operationally reasonable. Thus, a railway undertaking tendering ERTMS/ETCS systems need to check whether these fulfil their operational requirements. These tests are a separate set of test sequences at the moment. They need to be defined by a similar methodical approach as shown above, but they have need to fulfil more requirements: the test sequences must represent the most typical or important scenarios of the operation of the railway. They need to show the fulfilment of the European requirements as well as the national add-ons.

The approach is to use the same test cases for the operational test sequences as well. Some specific test steps and test cases are added to represent operational aspects which are not represented in the technical tests. The same method for the generation of the test sequences is used, too. So the test cases consist out of technical and operational test steps. The test cases are concatenated to a realistic test sequence as shown in Fig. 8-4. This operational test sequence is formalised and filled with parameters according to the same rules as the technical test sequences.

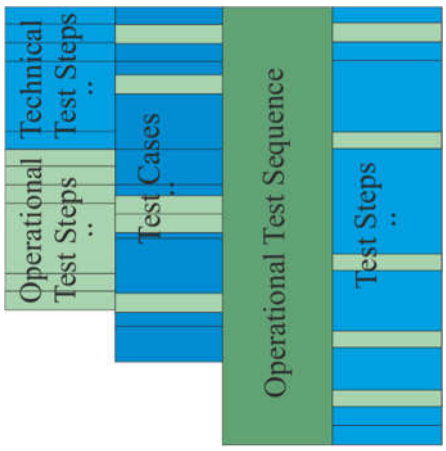


Figure 8-4: Structure of a test sequence for operational testing

The main difference is that the definition of the test sequences is not optimized to fulfil the specification requirements using the shortest possible sequences. The optimisation criteria are here to find as much relevant or important regular or disturbed operational scenarios to be tested.

The parameterization of the test sequences is done according to the operational environment. Average or standard parameters are typically used for this purpose. Extreme or rare parameters are to be avoided.

8.4.4 Perspective: ATO Test Sequences

No matter if the implementation of the ATO is done by integrating new features in the on-board train control or by adding a module replacing the driver, both approaches can be tested on functional level by the approaches described above. Due to the experience with the ETCS test specification, the conformity approach is recommended. In contradiction to the current implementation of the conformity tests a closer relationship to the real operation is useful to avoid too artificial scenarios in the lab tests. This is even more important if a field test shall be executed with the same scenarios.

Looking a little bit into the details this means that for example the correct driving behaviour (acceleration/deceleration) of the ATO module can be tested similar to the current implementation of the tests for the braking curve behaviour of the ETCS EVC. The laboratory would stimulate the driving action by sending a movement authority (or whatever signals necessary) and the virtual position of the traction lever can be evaluated by the laboratory.

This methodology can be transferred to all functional interfaces of an ATO-module or an integrated ATO system easily, as long as there is digital information available. Beside the already available methodology there is another advantage of this lab-testing approach: Assuming the number of tests will increase massively to reach a certification for an ATO module, the high efficiency of laboratory tests will reduce the effort to a productive level. During a migration phase there will be a lot of data available from the non-automatic operated trains. These data can be easily reused for testing the ATO systems. I.e. a huge number of tests can be defined by using the real data, the trust in the systems can be maximized and a comprehensive testing for ATO on functional interfaces can be assured easily.

8.5 Conclusion

The approach used for the conformity tests and operational tests for ETCS is proven in use and can therefore be extended for testing ATO functionalities and interfaces, too. As long as the interfaces are functional and digital, the methodology can be reused easily. It may, like for interface conformity, even applied to partial standardisations. The principle method of the generation of the test sequences can be used for the different types of tests. The optimization criteria as well as the rules for the parameterization differ for the different kinds of tests. If the same approach for the formalisation and parameterization is used, the lab environment can be used for any type of test, with some adaptations to be made to achieve sufficient flexibility.

8.6 References

[1] ERTMS -- Test Sequences, SUBSET-076-6-3, Version: 3.0.0, 1/06/2016

[2] ERTMS -- System Requirements Specification. SUBSET-026, Version 3.4.0, 15/06/2016

[3] ERTMS -- Test Sequence Generation: Methodology and Rules. SUBSET-076-4-1, Version 1.0.2, 1/07/2016

[4] ERTMS -- Methodology of testing. SUBSET-076-3, Version 2.3.1, 1/07/2016

[5] ERTMS -- Functional requirements for an on-board reference test facility, Version: 3.0.0, 15/06/2016

8.7 Authors

Dipl.-Inf. **Oliver Röwer** graduated in computer science in 2013 at the University of Rostock in Germany. He specialized in the field of Smart and Virtual Environments. At the German Aerospace Center (DLR) he is an expert for test automation and hardware-in-the-loop tests. He is the deputy laboratory leader of the RailSiTe®, the ISO 17025 accredited railway simulation and testing laboratory of the DLR. There he gathered expert knowledge of ERTMS/ETCS, especially regarding subset-026 and subset-076 tests, as well as interoperability tests. He is involved in the European projects X2Rail-1 WP6 and X2Rail-3 WP5.

Oliver.Roewer@dlr.de

Dipl.-Ing. **Lennart Asbach** graduated in mechatronics in 2009 at the University of Dresden in Germany. He specialized in the field of testing of control, command, communication and signalling systems. At the German Aerospace Center (DLR) he is an expert for test systems, test automation and hardware-in-the-loop tests, with an expert knowledge on ERTMS/ETCS. He is the head of laboratory of the RailSiTe®, the ISO 17025 accredited railway simulation and testing laboratory of the DLR as well as head of a research group in the DLR institute of transportation systems. He is involved in many European projects with respect to development of subset-026 and subset-076 tests, as well as interoperability tests.

Lennart.Asbach@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

9 Toward application of operational parameters for testings in laboratory to reduce on-site testing: focus on human operators

Philippe Richard; IRT RAILENIUM, Famars, France
Simon Collart-Dutilleul; IFSTTAR, ESTAS, Villeneuve d'Ascq, France

9.1 Introduction

Nowadays, several tests in railway domain must be carried out on-site. These are extremely time consuming and can become quite expensive. For this reason, some studies, such as [1] and the research project X2RAIL-1 Work Package (WP) 6: Zero on-site testing, aim to transfer on-site tests to laboratories.

Even if the title of this work package seems utopian, it is possible to reduce on-site tests. To achieve this goal, the main proposition is to operationalize tests in laboratories. Operationalization means that on-site tests, including the validation of results from laboratory tests, are done under operational conditions. In this paper, we suggest the inclusion of operational data in laboratory tests and we distinguish two families of parameters:

- Technical data;
- Human data linked to their behavior. The paper is focused on this part.

This paper presents the genesis of our reflexion as well as the related view that has been proposed in X2RAIL, linked to human data, and focuses on what would be necessary, from our point of view, to achieve the objective of operationalizing the tests.

9.2 Tests done in laboratories today

To situate the problem, we firstly approached how tests are done in laboratories. We focus our attention on EURA SUBSET-076-6-3 – test sequences to highlight that the study was carried out using the baseline 2.3.3 [2]. The test sequences point out two main factors for each step:

- The distance at which the steps are triggered;
- The definition of the step.

If we explore the test sequences, we can observe some distances that are not compatible with operational data (technical or linked to human behaviour). If we translate this distance into speed, we find some inconsistencies with the real world. For example, instantaneous actions of the human operator or extraordinary braking forces for the rolling stock.

It is necessary to note that these test sequences do not consider the railway infrastructure as there are no curves, no level crossing, and no slopes or ramps. It is also necessary to point out that these tests were not designed to consider operational data, but to verify that materials under test conform with the specifications defined in SUBSET-026 [3]. This document also presents the architecture of ERTMS/ETCS (European Railway Traffic Management System/European Traffic Control System, Fig. 9-1). In this architecture, some agents (technical or human) gravitate around the ERMTS architecture (red boxes in Fig. 9-1), like onboard and trackside parts. We call these agents interfaces.

Moreover, this document mentions that: "The InterOPerability (IOP) requirements for the ERTMS/ETCS on-board equipment are related to the functionality and the data exchange between the trackside sub-systems and the on-board sub-system **and to the functional data exchange between the onboard sub-system and: a) the driver; b) the train**."

In this example, the interfaces "Train" and "Driver", are reduced to exchanging functional data. Because of the lack of real operation like data, this kind of test cannot replace on-site tests, which actually take operational data from these interfaces into account. Therefore, we suggest that to decrease the number of on-site tests in favour of laboratory tests, it is necessary to consider operational data. We define operational data as an interval of real values representing the parameter(s) linked to an interface and which are inseparable from it. For example, the breaking forces of the train, the response time of the driver, the precision of odometry, the delay of GSM-R (Global System for Mobile communication – Railway) communication or the bandwidth of GSM-R are treated as operational data. During IOP tests, these interfaces are not considered, or they are assumed to be perfect.

Proposal to consider parameters linked to human behaviour in laboratory tests

Some requirements have been defined in this X2RAIL-1 WP6. They are presented in [4] and some of them are directly linked to the integration of operational data. To consider those, 3 human factors use cases are proposed, one automated without a human operator (driver…) and 2 semi-automated. These use cases aim to integrate some requirements linked to the subject presented below: operational data and real users. All the details are presented in [4].

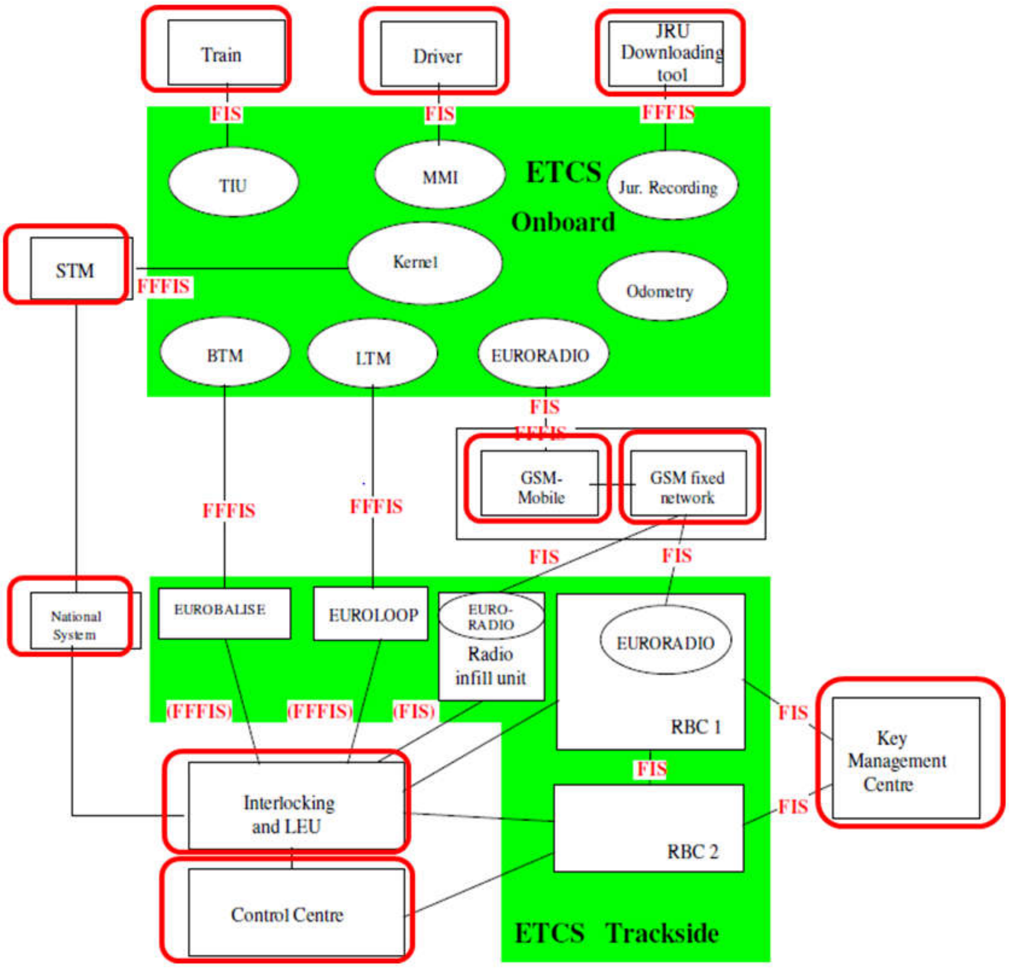


Figure 9-1: UNISIG ERTMS/ETCS reference architecture, except from SUBSET-026 [3], with our interface's identification

With the aim of minimizing the number of tests on site and from our experiment's feedbacks, we think it is better to privilege automatic test which allows to allocate the actions of the human operator to a robot. The main advantages are:

- The possibility to reduce time costs by accelerating test executions;
- The repeatability of the test;
- The lack of necessity to call on several experts.

But this test also presents some disadvantages. Indeed, it will be necessary to determine what parameters need to be addressed and how to quantify them to create the operational data for the human operator. In the following paragraphs, we will address human operator identitykit. In this context, we define an identitykit as a limited representation of a railway system agent. It will be characterized by an identifier and some associated attributes. An attribute is characterised by one or several parameters. Each parameter will contain a value range and a standard deviation. The first step is to determine the list of parameters. The literature often cites at least two parameters:

- The efficiency can be represented by the human error rates;

- The time to perform an action (time between the perception and the end of the action) that is called response time in the following parts.
- This list may be completed by consulting literature on Performance Shape Factors (PSF) [5] and using various sources:
- State of the art (for example [6,7]);
- Focus groups or individual interviews [8,9] with experts;

Simulations in laboratories to observe human behaviours and measure their parameters. This implies that the human operator does verbalization;

- Observations on field to measure parameters [9].
- These sources can also help to quantify these parameters.

Ideally, it would be interesting to be able to update these data, for example, in the event of a change of equipment, without having to carry out the whole study again. We have started to conduct studies on this subject regarding the response time to a request on a Digital Man Interface (DMI) on an On Board Unit (OBU). This work is based on the Keystroke-Level Model (KLM) methodology [10, 11, 12] and the specification of DMI [13]. An experimental campaign will have to be performed to confirm the adequacy with this theoretical calculation.

9.4 Next steps

Therefore, for the operations tested, it is necessary to project the relevant operators' parameters. This projection will be named after the human operator's identitykit. The identitykit will probably not be unique as the value of the parameters will depend on the human operator's family (novice, expert, lambda…). This family can be represented by an "id" and the parameters by attributes. Each attribute has intervals as values associated with a standard deviation. The next step is to confirm that the estimation of these parameters conform with the reality. These values can be estimated by using the methods presented in the previous section. After that, it will be necessary to confirm that the estimated values are representative of the real world (on-site). To do that, we can use specific methods, for example the test of Student for mono-criterion parameters [14]. But some parameters are influences by multiple criteria. Experimental plans methodologies [15] may respond to this problematic.

Of course, the railway system cannot be resumed only to human operators. It is a complex system. That is why, our long term objectives are to be able to determine an operational identitykit considering at the same time, the human operator identitykit, also the rolling stock identitykit and the situation identitykit (cf. Fig. 9-2).

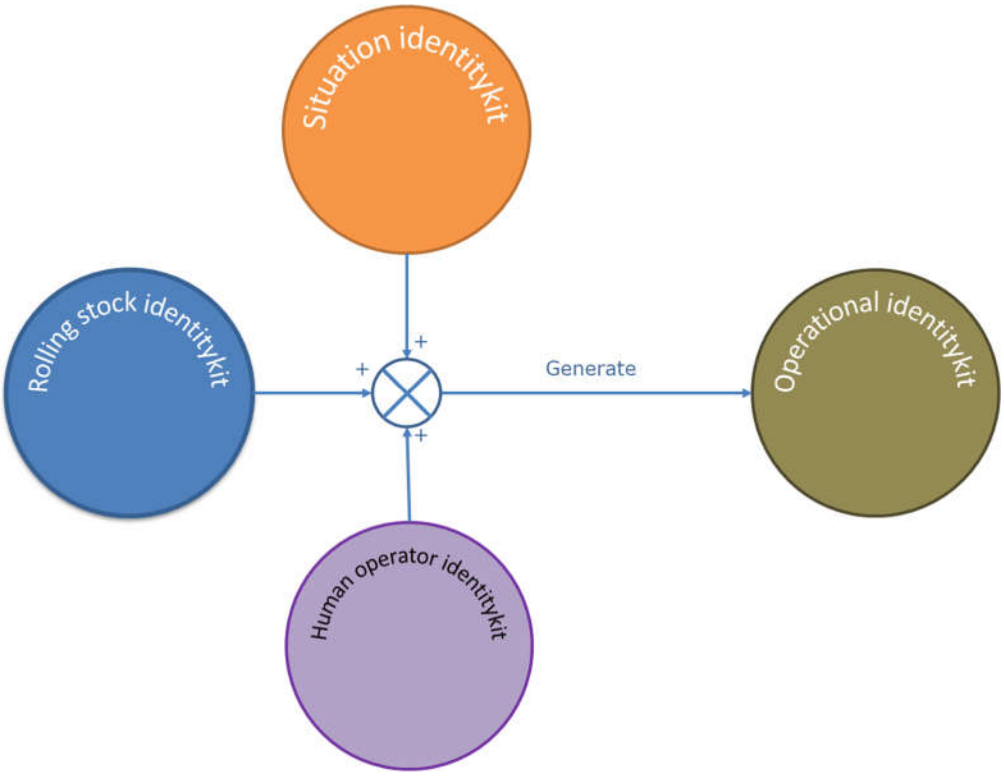


Figure 9-2: Theorical proposal of operational data generation

The rolling stock identitykit have to include all parameters that must be considered in the test according to operations that are under testing and the situation identitykit must consider the context and railway infrastructure.

In our point of view, once all the parameters are identified and quantified for each identitykit, a fusion must be done to generate the operational identitykit. The experimental plans could be used to determine the parameters of operational identitykit but it will be a time-consuming work. Indeed, the value of parameters generated for the operational identitykit will differ depending on the combination of human operator, rolling stock and situation identitykits. For example:

$$\mathrm{Operational}_{\mathrm{identitykit}} \text{ of } \left(\mathrm{id}_{\mathrm{operator}} = 1 + \mathrm{id}_{\mathrm{rollingstock}} = 1 + \mathrm{id}_{\mathrm{situation}} = 1\right) \neq \mathrm{Operational}_{\mathrm{identitykit}} \text{ of } \left(\mathrm{id}_{\mathrm{operator}} = 2 + \mathrm{id}_{\mathrm{rollingstock}} = 1 + \mathrm{id}_{\mathrm{situation}} = 3\right)$$

9.5 Conclusion

In this paper, we presented the context of ERTMS official tests in laboratories that use as input, the SUBSET-076-6-3. This SUBSET proposes IOP tests to demonstrate that the system (using real and/or simulated components) under test conforms with the functional specifications detailed in SUBSET-026. The test sequences obtained from SUBSET-076-6-3 do not consider operational data. This is a sufficient reason to complement them with on-site tests. To reduce on-site tests, it will be necessary to include operational data in laboratory tests. Two families of data must be considered, technical data and data linked to human operator behaviours.

Technical data must be extracted from documentation, measurement, etc. The human data must also be determined by measurement, study of documentations, etc. The paper proposed some future works to generate the operational data that have to be inserted as an entry for test execution.

We are also working on a methodology to update some parameters, especially response times considering HMI modifications without requiring new measurements. We also think that these parameters, characterized by an interval, must be extracted from a model of the operational railway system.

9.6 References

[1] Stefan Bode, RAIL FREIGHT1&3 NSA Working Group, Guideline For CCS Authorisation On Corridor Rail Freight, December 2016.

[2] UNISIG, SUBSET-076-6-3-001_v233, ERTMS/ETCS – Class 1, Test sequences, UNISIG, 2012.

[3] UNISIG, SUBSET-026_v300, ERTMS/ETCS – Class 1, System requirements specification, UNISIG, 2008.

[4] X2RAIL-1, Deliverable D6.3 Description of general test architecture, 2018.

[5] Rangra, S., Performance shaping factor based human reliability assessment using evaluation based systems: application to railway operations. PhD Thesis. Université Technologique de Compiègne, France, 2017

[6] OpenData from SNCF. https://data.sncf.com/explore/

[7] UNISIG, SUBSET-091_v340, ERTMS/ETCS – Class 1, Safety Requirements for the Technical Interoperability

[8] Rana Muhammad Dilshad et Muhammad Ijaz Latif Focus Group Interview as a Tool for Qualitative Research: An Analysis, Pakistan Journal of Social Sciences (PJSS) Vol. 33, No. 1 (2013), pp. 191-198.

[9] Handbook of Human Factors and Ergonomics Methods; Neville Stanton et al., CRC PRESS, 2005.

[10] The Keystrok-Level Model for User Performance Time with Interactives Systems, Stuart K et al., 1980.

[11] Using the Keystroke-Level Model to Estimate Execution Times, David Kieras, 2001

[12] Enhancing KLM (Keystroke-Level Model) to Fit Touch Screen Mobile Devices. Karim El Batran and Mark D. Dunlop. MobileHCI '14, September 23 – 26, 2014.

[13] ETCS DRIVER MACHINE INTERFACE, ERA, reference ERA_ERTMS_015560, 2014.

[14] On Student's 1908 paper "The probable error of the mean", Journal of the American Statistical Association 103 (2008), p. 1-7

[15] Garcia-Diaz, A., Phillips T. D. « Principles of experimental design and analysis » Ed. Chapman & Hall - 1995

9.7 Authors

Dr. **Philippe Richard** received the PhD degree from the University of Valenciennes and Hainaut-Cambresis (France) in 2012 in automation and computer engineering. He is currently contributing to two European projects (X2RAIL-1 WP6 and X2RAIL-1 WP8) and two national projects (TC-Rail (train remote driving) and autonomous train). In these two last projects, he coordinates 3 work packages. He also contributed to the expertise of a human factors study for the superposition of the ERTMS/ETCS level 1 and the national system. His main competences are Human Machine-System, Human Factors (estimation of human error, analyse of consequences, detection of human error risk on the line…) applied to the railway domain. He performed studies, focused on human operator, on IFSTTAR ERTMS/ETCS simulator in accordance with SUBSET-026 of EURA. He was involved in the conception of numerical simulators dedicated to research and learning in the railway domain: COR&GEST and MissRail®.

philippe.richard@railenium.eu

Dr. **Simon Collart-Dutilleul** obtained his PhD degree from the Savoie Mont Blanc University (France) in 1997. He is a senior researcher at an equivalent professor level at IFSTTAR. He is a scientific expert of Discrete Event Systems (DES) and Formal Methods (FM). He has been involved in various national and European projects. He was the coordinator of the ANR granted PERFECT project dealing with formal methods, safety and ERTMS implementation. He is the scientific leader of the ERTMS –regional project of the IRT-Railenium. He authored and co-authored more than 130 scientific papers. Dr. Simon Collart-Dutilleul is also an industrial safety expert concerning the SUBSET-076 of ERA.

simon.collart-dutilleul@ifsttar.fr

10 Authors Index

Asbach, L. 53
Barth, B. 29
Berbineau, M. 1
Bonneville, H. 7
Brunel, L. 7
Charaf, A. 7
Clazzer, F. 29
Collart-Dutilleul, S. 63
Deniau, V. 35
Fernández, N. 23
Fleury, A. 35
Franco, D. 17
Gransart, C. 35
Grec, M. 29
Hutchinson, M. 1
Kousri, R. 35
Masson, E. 1, 7
Mendizabal, J. 1, 23
Meyer zu Hörste, M. 1, 53
Millot, P. 41
Mouchel, M. 41
Ollora Zaballa, E. 17
Paglia, C. 41
Richard, P. 63
Romero, G. 35
Röwer, O. 53
Simon, E. 35
Villain, J. 35