RobustRailS

Next generation train control communication architectures: Cybersecurity and resilience aspects

PhD Marina Aguado
Associate Professor

i2t Research Group

eman ta zabal zazu

Universidad del País Vasco
Euskal Herriko Unibertsitatea
The University of the Basque Country

GOBIERNO DE ESPANA

MINISTERIO DE ECONOMIA Y COMPETITIVIDAD

SECRET PROJECT

SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS

INDEX

1. **The Railway Context**
2. Railway Services: a taxonomy
3. The Safety Concern & Train Control Fundamentals
4. Railway Research on Train Control Systems
5. Our on-going research & Demo
6. Tooling & Simulation Frameworks

The Rail Transport

- Rail transport as the key enabling factor for sustainable mobility. Rail transport underpins economic growth

- A key strategy to promote a significant cut in Green House Gas emissions

↑

- Increasing demand for environment-friendly transport modes such as the rail transport, including metro, light rail and heavy rail

- European vision for the future of rail in 2050 embraces an integrated, sustainable and safe high speed passenger, freight and urban mass transport service

- The 2011 White Paper points out that the creation of a Single European Railway Area (SERA) will be crucial to achieving a modal shift from road towards more sustainable modes of transport such as rail

↑ Safety
Efficiency
Competitiviness
Sustainability

The Railway Context

- Railways are large and complex systems , built, expanded and upgraded over the years
- New and old solutions and equipment coexist in use
- Lifetime of railways is counted in decades
- Although transport markets are becoming more and more global, the European rail sector continues to have a strong national focus, due to technical, organisational, regulatory and cultural barriers
- Unlike in the aviation and road sectors where products are placed on the market for use in many Member States, many products in the rail sector continue to be tailored to particular national or even regional transport authorities
- Strong need for a common framework of rules and regulations for rail operators in all EU countries more specifically standardization in signalling technology
- A complex set of players: ERRAC, ERA, UNISIG, ERTMS users group, UIC
- Technological diversity is a major obstacle in international train operation
- Ageing skill force (30% of the workforce expected to retire in the 10 years to come)

Telecommunications in the Railway Domain

- Railways is a large and complex system with a largely distributed set of assets
- Asset mobility … railway intrinsic nature .. Strong link with telecom services
- Frequent handovers .. mobility management challenge
- Railway industry pretty conservative from the telecom point of view due to safety considerations …Currently… not at all early adopters
- Why… life cycle time in telecom industry vs life cycle time in railway industry…:
    - Different cycle lifetime or evolution speeds: Wireless technologies, computers, smartphones have a very short life cycle time when compared to the automotive and railway industry

A Railway Telecom Architecture: particularities ..

- Why do we need a specific railway telecommunication architecture?

- Different philosophy : Traditional public communication architectures designed for financial return versus Railway communication architectures are designed to cater to the stringent performance requirements

Train control systems and other information systems for operational goals are designed to meet very stringent safety standards (RAMS, SIL levels) & legislative requirements

- Mobility management harsh conditions: While in traditional public communication architectures handover process is a rare exception, in railway communication architectures is the rule

- Railway context benefits : highly predicted mobility management, low loaded telecom networks, pre-established data application profile

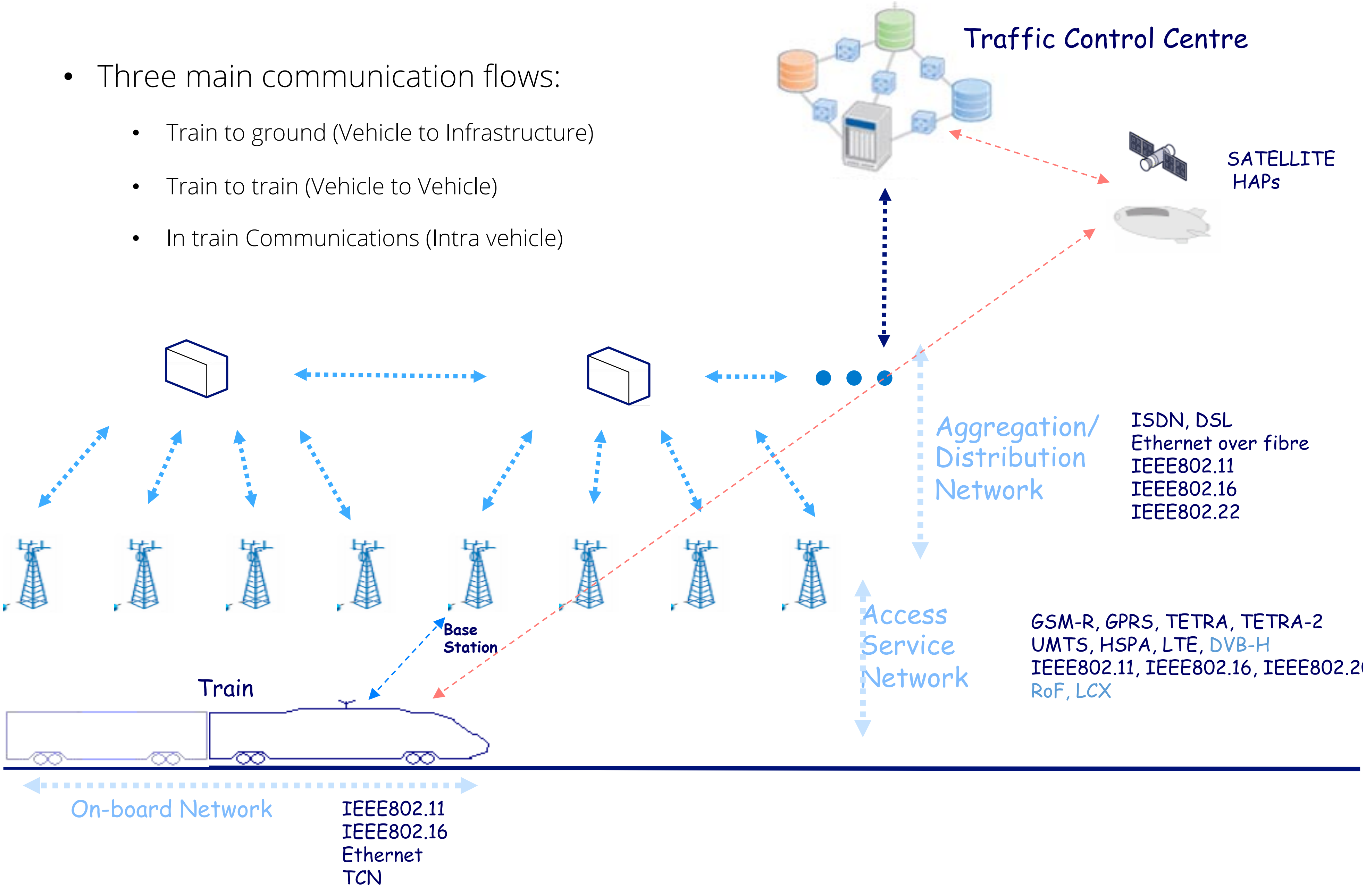
- Air Road Train Synergies (i.e mobility management .. Harsh conditions, Railway stamp, need for standarization)

INDEX

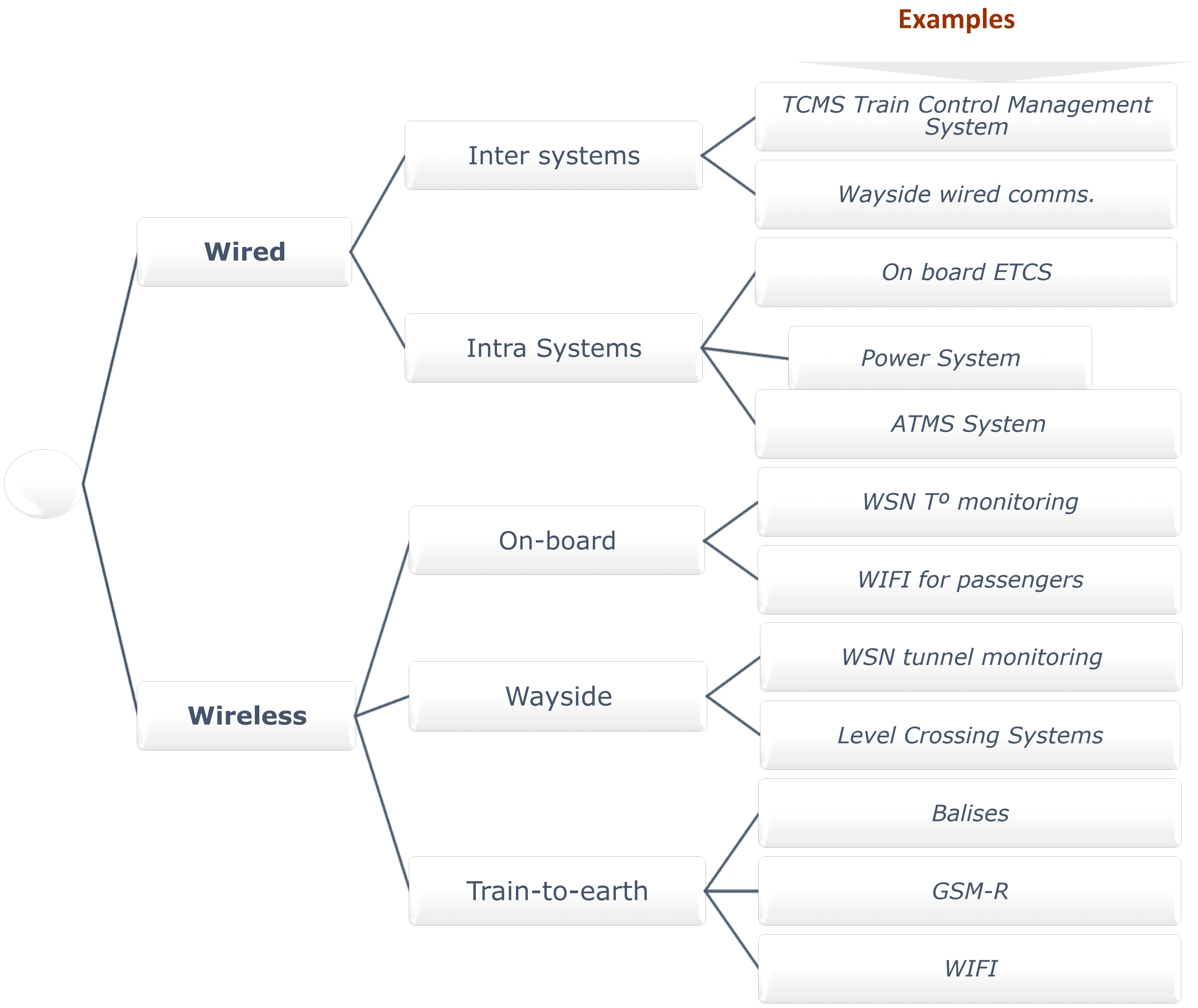
1. The Railway Context
2. **Railway Services: a taxonomy**
3. The Safety Concern & Train Control Fundamentals
4. Railway Research on Train Control Systems
5. Our on-going research & Demo
6. Tooling & Simulation Frameworks

Railway Information Flows: V2I .. V2V ..

- Three main communication flows:
  - Train to ground (Vehicle to Infrastructure)
  - Train to train (Vehicle to Vehicle)
  - In train Communications (Intra vehicle)



Examples of Wired and Wireless services in the Railway Domain



Examples

Wired

Inter systems

TCMS Train Control Management System

Wayside wired comms.

Intra Systems

On board ETCS

Power System

ATMS System

Wireless

On-board

WSN Tº monitoring

WIFI for passengers

Wayside

WSN tunnel monitoring

Level Crossing Systems

Train-to-earth

Balises

GSM-R

WIFI

IT services in the railway domain:

The Safety Concern

- Motivation: the braking distance of a rail vehicle exceeds the driver visibility distance
- Human lives involved so a train control or signalling system has to be fail safe
- A system is **fail safe** when in the event of failure, it responds in a way that will cause no harm, or at least a minimum of harm, to other devices or danger to personnel
- In the Signalling system implementation relay-based track circuits are designed in a way that most failures will result in a "track occupied"
- **Safety critical "vital"** applications are those ones which use processor-based technology to implement safety-critical functions to achieve a certain level of safety
  - Example: Use of multiple computers : 2 out of 2 or 2 out of 3 voting schema
  - Each computer runs sofware coded differently

……………… SEARCHING ROBUSTNESS & RESILIENCE…

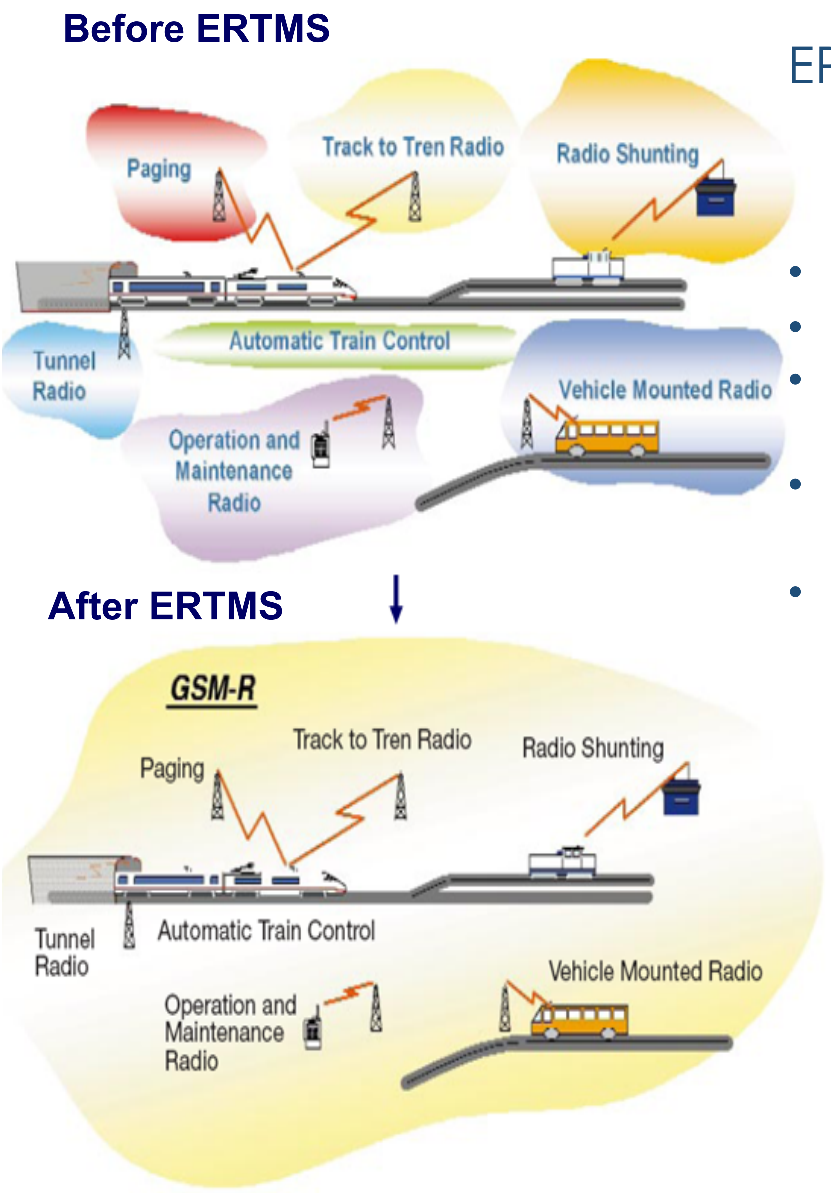
Train Control Systems

- Any technology that can be applied to improve safety and efficiency in real-time train operation

- Examples of systems that support real-time train operation

  - Hot-Box / Hot Wheel Detector
  - End of Train Detector (EOT)
  - Locomotive Distributed Power
  - Locomotive Onboard Computerized Systems
  - Signaling Systems
  - CBTC (Communications-Based Train Control) Systems

ERTMS Overview



ERTMS – Brief History

- 1996 – Interoperability framework design
- 2001 – Specification of characteristics of the system
- 2005 – Six freight corridors selected for ERTMS deployment
- Between 2005-2008 – Technical specification for interoperability
- 2009 – European Deployment Plan was established to guarantee interoperability and transition timeline

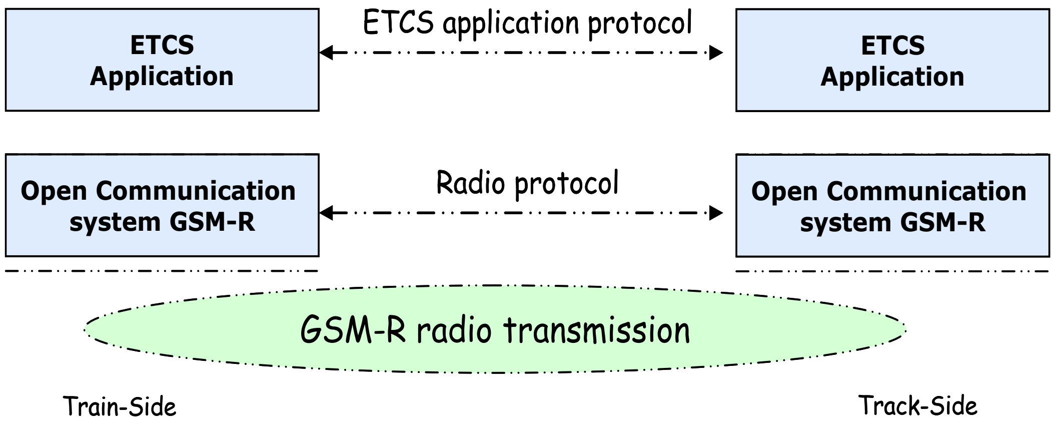
European Railways, following the MoU, will use GSM-R as the "bearer service" for their communications (including ETCS).

However, future applications demand more capacity
Some national applications (already today, e.g. shunting) need higher data rate wireless technology

ERTMS Overview

ERTMS – Design

- ERTMS consists of two primary components: GSM-R and ETCS (European Train Control System).
    - GSM-R is a radio system based on GSM mobile communications standards. GSM-R uses a specific frequency for voice and data communications between the train and the control center.
    - ETCS is the signaling and train protection system used to monitor train speed and movements. The safety functionalities for ETCS are divided into three application levels



INDEX

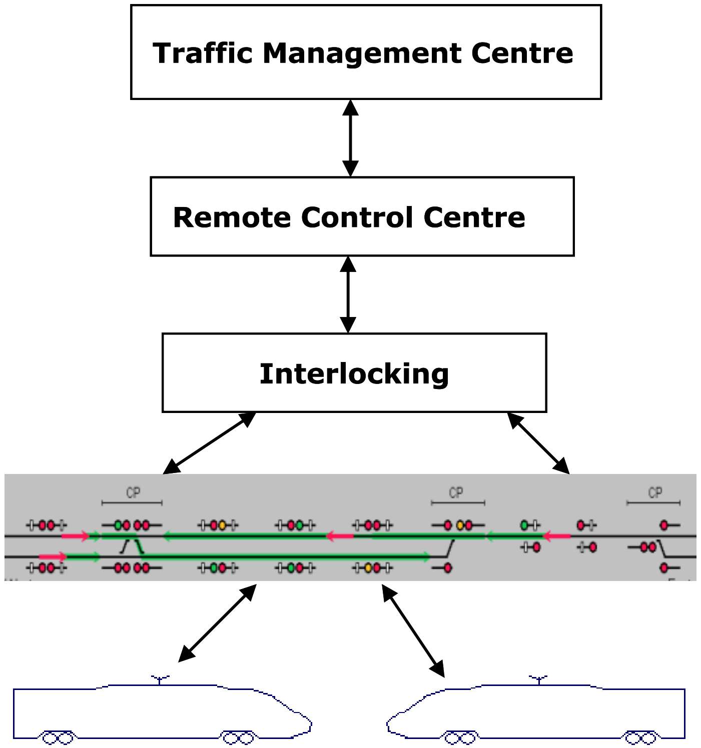
1. The Railway Context
2. Railway Services: a taxonomy
3. The Safety Concern & Train Control Fundamentals
4. **Railway Research on Train Control Systems**
5. Our on-going research & Demo
6. Tooling & Simulation Frameworks

Telecom technology ⛓ safety and efficiency

Safety
Efficiency
Competitiviness
Sustainability

⛓ Traffic Management System ⛓ Railway Communication Technologies and Architectures

Railway Communication
Wireless fixed Network
All Kind of voice and data communication



Traffic Management
- Strategic Management, Planning

Signalling System

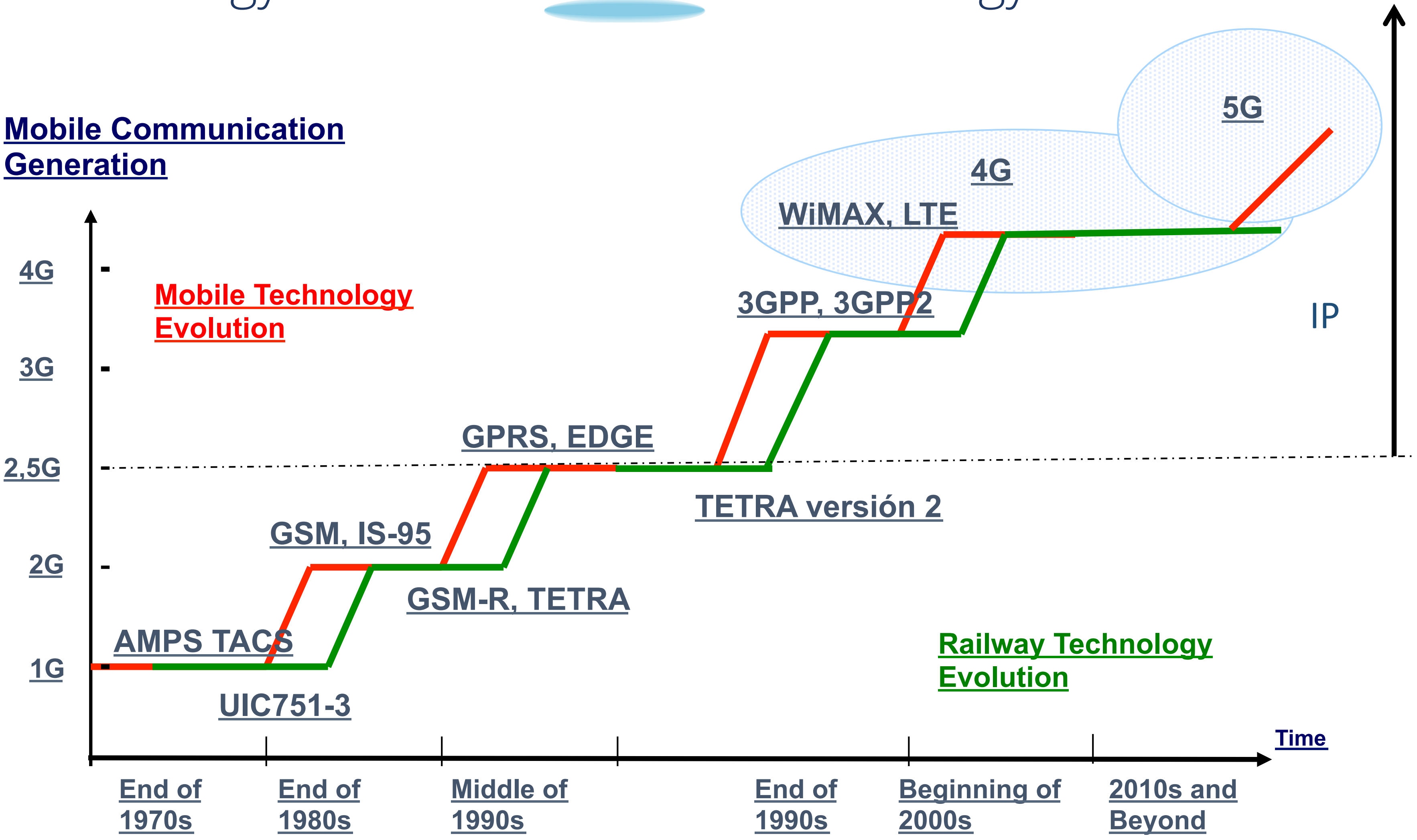
- Control of level crossings
- Control of Switch points
- Control of line side signals
- etc..

Train Control-comand

- Automatic train command with in-cabin signalling
- Train-side location based block control
- etc..

Railway Signalling Technology Evolution

Mobile Communication Technology Evolution



Research question

Wireless telecom life cycle equipment much lower than life cycle train equipment.

Currently ERTMS is linked to an obsolete 2nd Generation technology

data rate just 9.6 kbps with a low number of available traffic channels for high priority connections (congested crossing) and it is based on reserved circuits -> Inefficient spectrum allocation

Safety concern when migrating from a circuit based towards a packet switch technology (shared resources .multiple routes for msgs.> QoS & security concerns

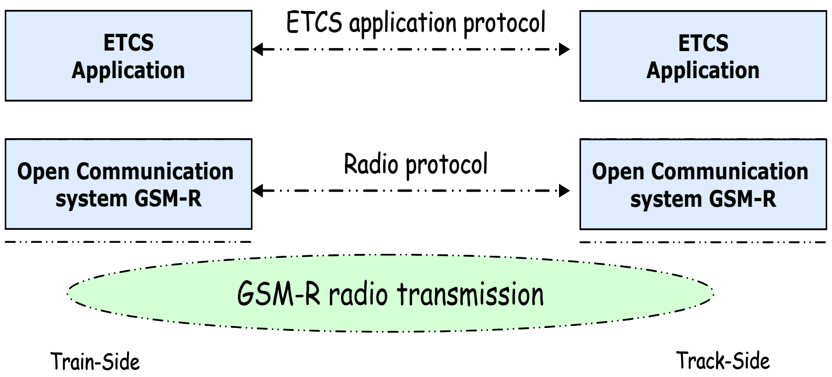
Research Goal:

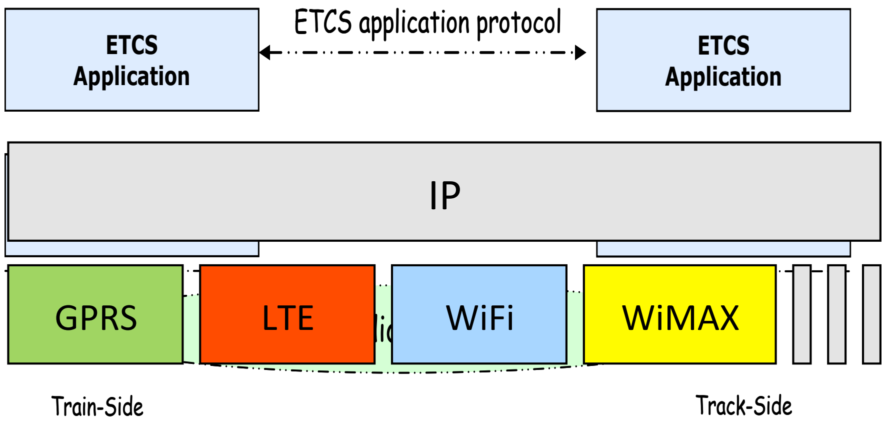
Develop a Train Control application and a safety and security layer agnostic to the underneath communication technology

Research question?

<u>Research Goal:</u>

Develop a Train Control application and a safety and security layer agnostic to the underneath communication technology





Railway Research

- Research activity in railway transport is healthy.

- Current Research Framework H2020 will run from 2014 to 2020 with an estimated total budget of EUR 77 billion. EUR 450 million has been earmarked for rail research and innovation activities. Three times more than Union funding under (FP7).

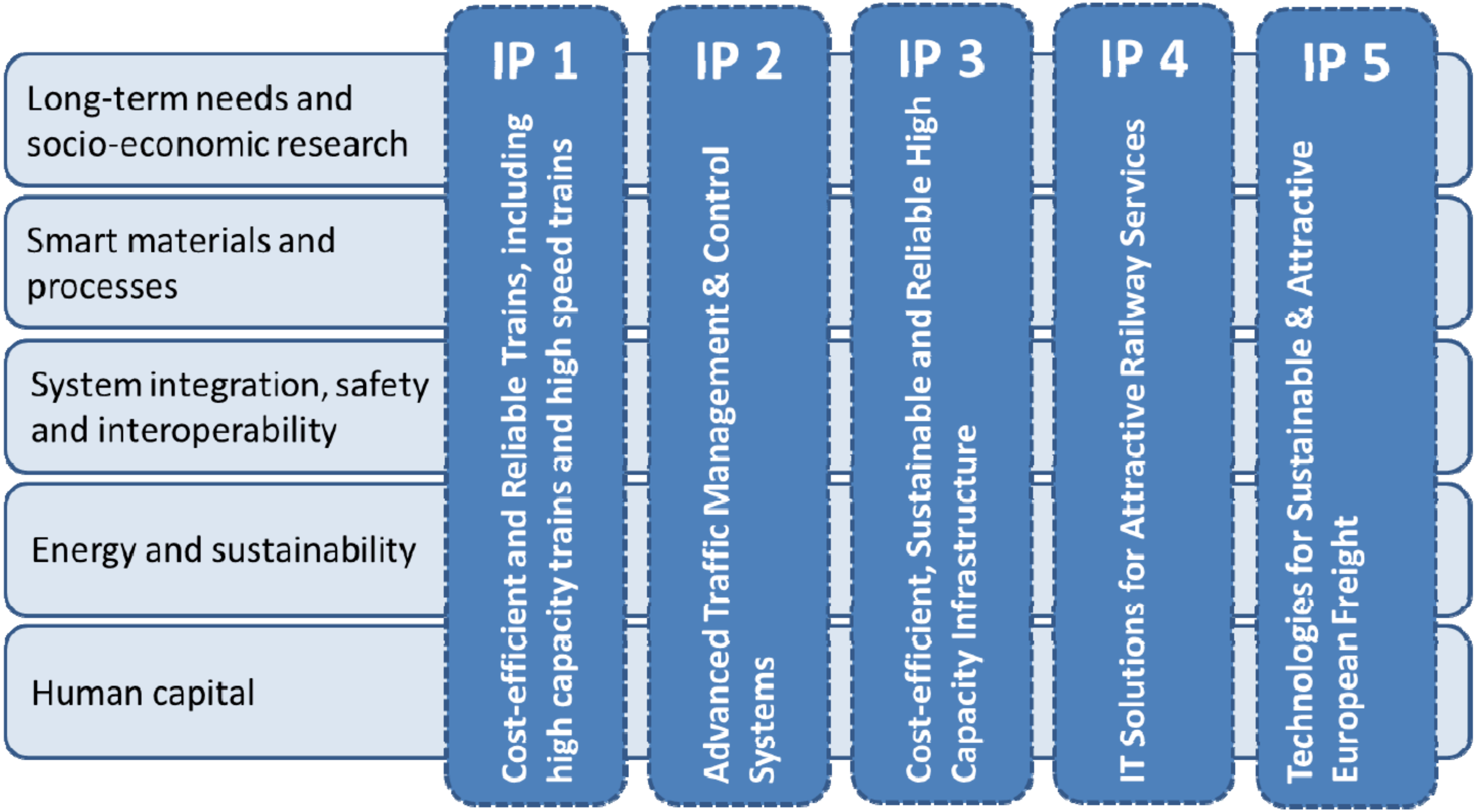
- A key objective of H2020 is to improve the efficiency of EU funding through Public-Private Partnerships (PPPs) in the form of Joint Undertakings.

- Shift2Rail Joint Undertaking (S2R JU) was established in 16 June 2014. It is a public-private partnership. 8 core group industrial members contribute with another EUR 450 million in research activities.

- S2R published a Master Plan which sets out a vision for the future European Railways . This Master Plan is a “forward looking” strategic roadmap to drive innovation in the rail sector in the long term, looking at a 2030 horizon

Railway Research

Shift2Rail Innovation Programs IP and Cross Cutting Activities



Long-term needs and socio-economic research

Smart materials and processes

System integration, safety and interoperability

Energy and sustainability

Human capital

IP 1
Cost-efficient and Reliable Trains, including high capacity trains and high speed trains

IP 2
Advanced Traffic Management & Control Systems

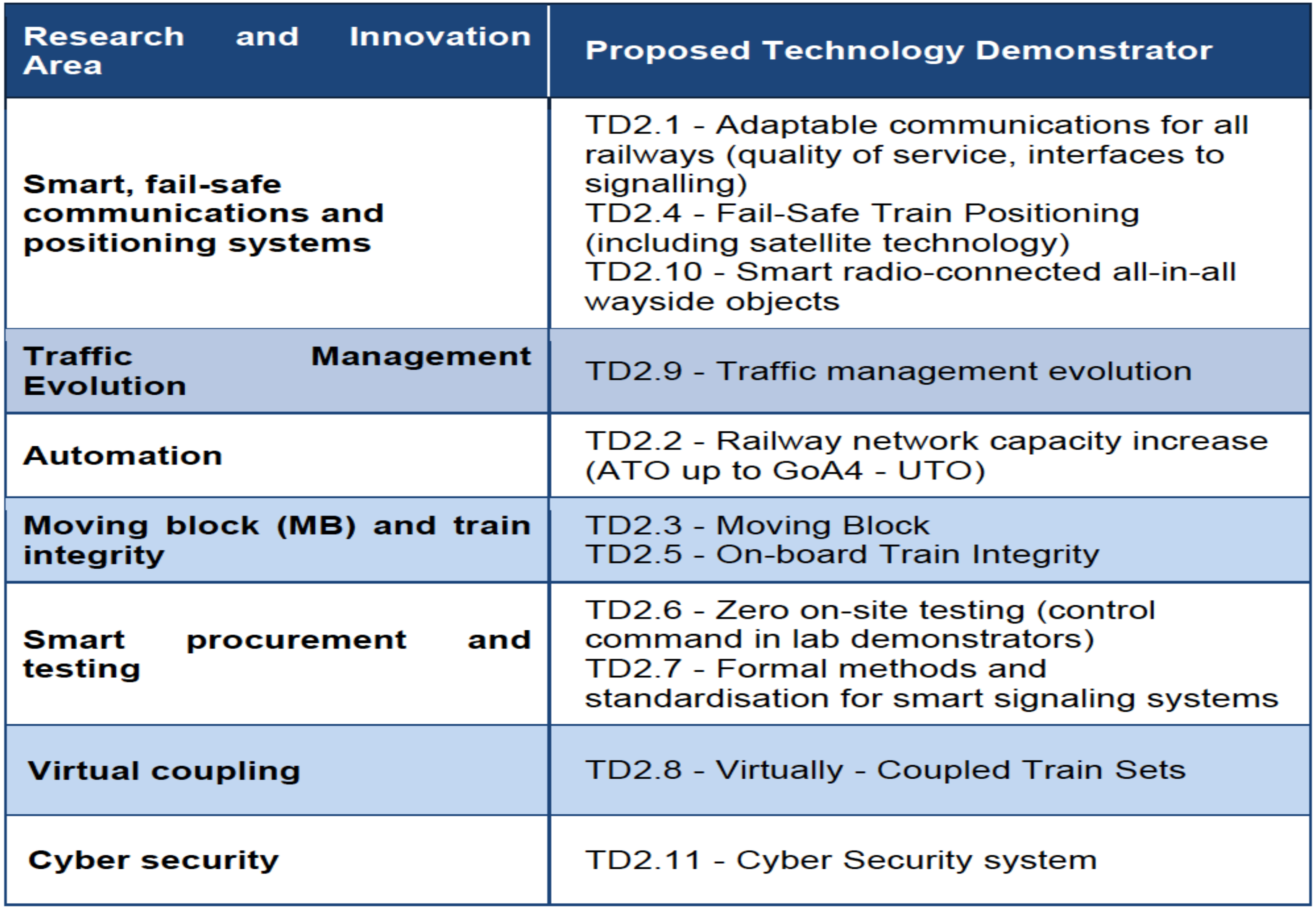
IP 3
Cost-efficient, Sustainable and Reliable High Capacity Infrastructure

IP 4
IT Solutions for Attractive Railway Services

IP 5
Technologies for Sustainable & Attractive European Freight

Railway Research

IP2 Advanced Traffic Management and Control Systems



Research and Innovation Area	Proposed Technology Demonstrator
Smart, fail-safe communications and positioning systems	TD2.1 - Adaptable communications for all railways (quality of service, interfaces to signalling) TD2.4 - Fail-Safe Train Positioning (including satellite technology) TD2.10 - Smart radio-connected all-in-all wayside objects
Traffic Management Evolution	TD2.9 - Traffic management evolution
Automation	TD2.2 - Railway network capacity increase (ATO up to GoA4 - UTO)
Moving block (MB) and train integrity	TD2.3 - Moving Block TD2.5 - On-board Train Integrity
Smart procurement and testing	TD2.6 - Zero on-site testing (control command in lab demonstrators) TD2.7 - Formal methods and standardisation for smart signaling systems
Virtual coupling	TD2.8 - Virtually - Coupled Train Sets
Cyber security	TD2.11 - Cyber Security system

Previous Related Research Projects

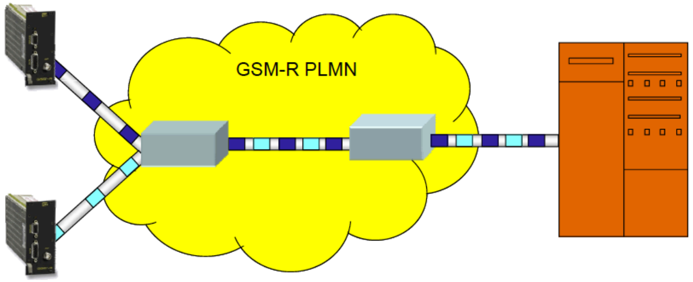
uic
INTERNATIONAL UNION
OF RAILWAYS

UIC GSM-R Projects 2010-2012

Work on introspecting Future Railways Telecommunications Systems.
looking if LTE could be the GSM-R follower,
and on Railways criteria when choosing a
new technology. Technology survey

GPRS for ETCS

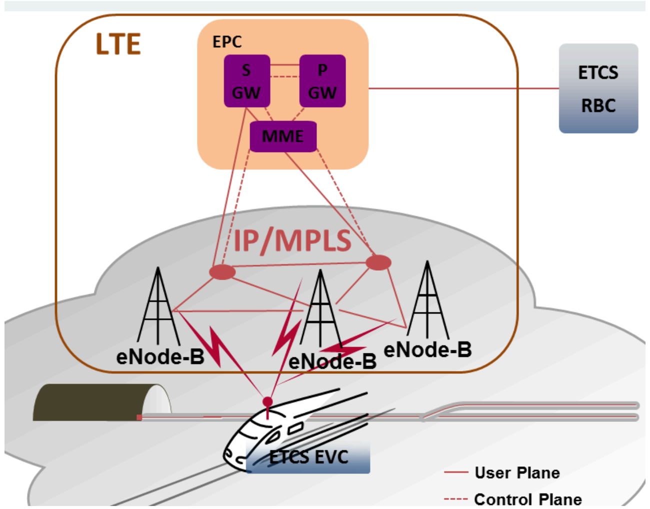
European Pilot, with partial funding from the TEN-T, with the participation
of ERTMS UG, GSM-R IG, UNISIG and UIC starts in April 2012,
and is scheduled to be finished in 2014.
Achieve a technical solution for using GPRS for ETCS.
From Circuit switched data to Packet switched data



((NGTC))
Next Generation of
Train Control systems

The main scope of NGTC is to analyse the commonality and differences of the required functionality of both ETCS and CBTC systems, and to determine the level of commonality of architecture, hardware platforms and system design that can be achieved.

Related Research Projects cont.



Tecrail

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD
SECRETARÍA DE ESTADO DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN
UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa
INNPACTO

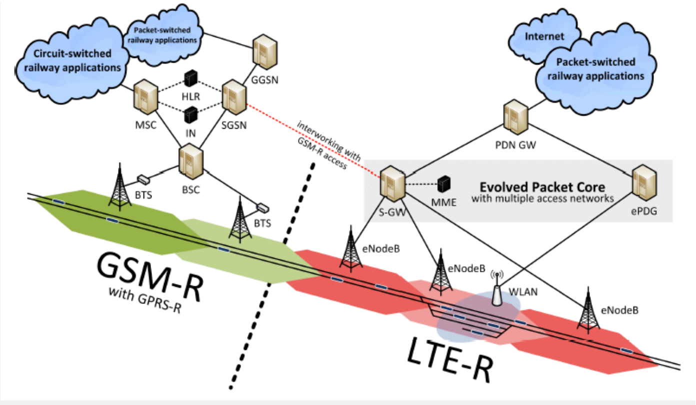
LTE communication technologies for the automated driving and control railway

Objectives: Analysis of the feasibility of adaptation of LTE and IP convergence railway environments, so they are applicable to railway signalling, automatic driving, communications and onboard train to ground communication for the purpose of contributing to the standardization and development.

SYSTUF Project SYStemes telécoms pour les Transports Urbains du Futur

IFSTTAR

TELECOM Bretagne


Circuit-switched railway applications
Packet-switched railway applications
GGSN
HLR
MSC
IN
SGSN
BSC
BTS
BTS
interworking with GSM-R access
GSM-R
with GPRS-R
Internet
Packet-switched railway applications
PDN GW
S-GW
MME
Evolved Packet Core
with multiple access networks
ePDG
eNodeB
eNodeB
WLAN
eNodeB
LTE-R

RobustRailS

DTU Fotonik
Department of Photonics Engineering

DTU

Next Generation Train Control Research Trends

- Integrating approaches ERTMS, PTC, CBTC for metro lines
- Overcome signalling system dependency on the underlying telecommunication technology by detach the application layer from the communication layer
- Migration towards IP
- Cyber Security Analysis
- Resilient Communication Architectures

INDEX

1. The Railway Context
2. Railway Services: a taxonomy
3. The Safety Concern & Train Control Fundamentals
4. Railway Research on Train Control Systems
5. **Our on-going research & Demo**
6. Tooling & Simulation Frameworks

Our ongoing Research :

European Research Projects:

FP7-SEC-2011-1 SECRET “SECurity of Railways against Electromagnetic aTtacks” (2012-2015)
Specification of resilient architecture using multipath/multihoming

Spanish Public Research Projects:

Contribution to a Safe Railway Operation: Evaluating the effect of ElectroMagnetic Distubances in Railways Control Systems (2014-2016) MINECO

On-Going Industrial Doctorate with railway sector – CAF
Zabalduz Grant currently entitled “New reliability and security protocol proposal for the ETCS applications over 4G technology” by Igor lopez Orbe

UPV/EHU has recently launched an inter-departmental Research oriented Master Program on Transportation Systems with the local railway industry support.

SECRET
PROJECT
SECURITY OF RAILWAYS AGAINST
ELECTROMAGNETIC ATTACKS

GOBIERNO
DE ESPANA

MINISTERIO
DE ECONOMIA
Y COMPETITIVIDAD

CAF

i2t Research Group

Our Research Topics :

TD 2.1 – Adaptable Communications for all railways (quality of service, interfaces to signalling).

Towards an adaptable train-to-ground communications system.

TD 2.11 - Cyber Security system

TD 2.6 - Zero on-site testing (control command in lab demonstrators)

Resilience Architectures for Train Control Signalling Systems through end-to-end Multipath approaches

Design and validation in different testbeds of a Railway Multipath TCP approach

Cyber Security analysis on future Train Control Signalling Systems over IP and packet switch technologies.

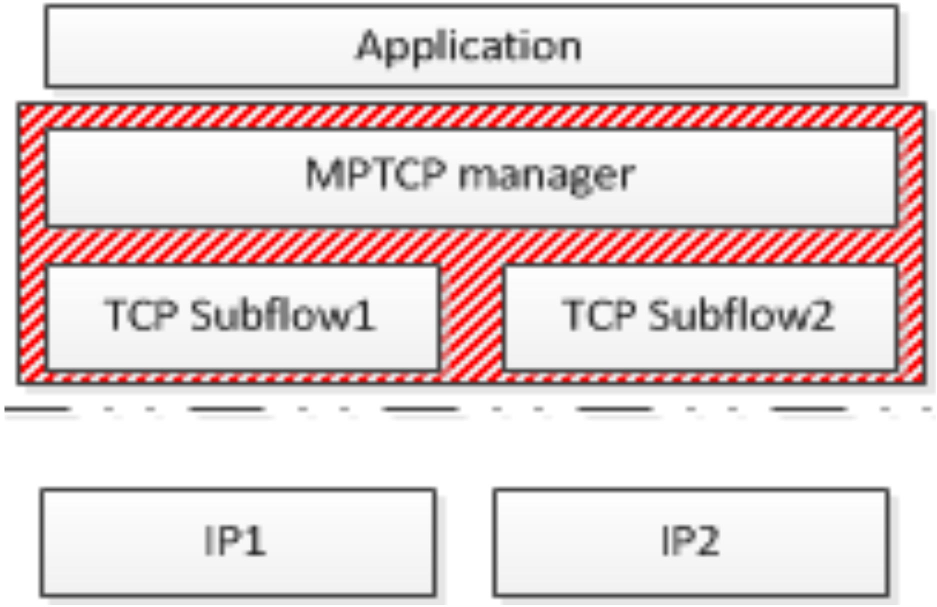
Development of new Key Management strategies for the challenging railway domain (frequent handovers, challenging mobility scenario)

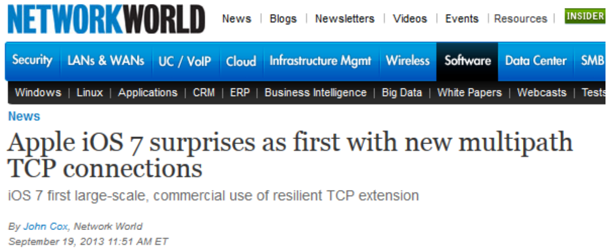
The EuroRadio replace project opens a good opportunity to apply modern security mechanisms to enhance authentication, integrity and confidentiality. On going thesis " New reliability and security protocol proposal for ETCS over 4G technologies"

Introducing Software Defined Networking technologies in the transport domain for increasing resilience and security

Our ongoing Research : End-to-End Multipath Technology

Take advantage current strategies in the IT world regarding end-to-end multipath protocols.
End-to-end multipath protocols provide higher reliability and higher effective throughput.




NETWORKWORLD
News | Blogs | Newsletters | Videos | Events | Resources | INSIDER
Security | LANs & WANs | UC / VoIP | Cloud | Infrastructure Mgmt | Wireless | Software | Data Center | SMB
Windows | Linux | Applications | CRM | ERP | Business Intelligence | Big Data | White Papers | Webcasts | Tests

News

Apple iOS 7 surprises as first with new multipath TCP connections

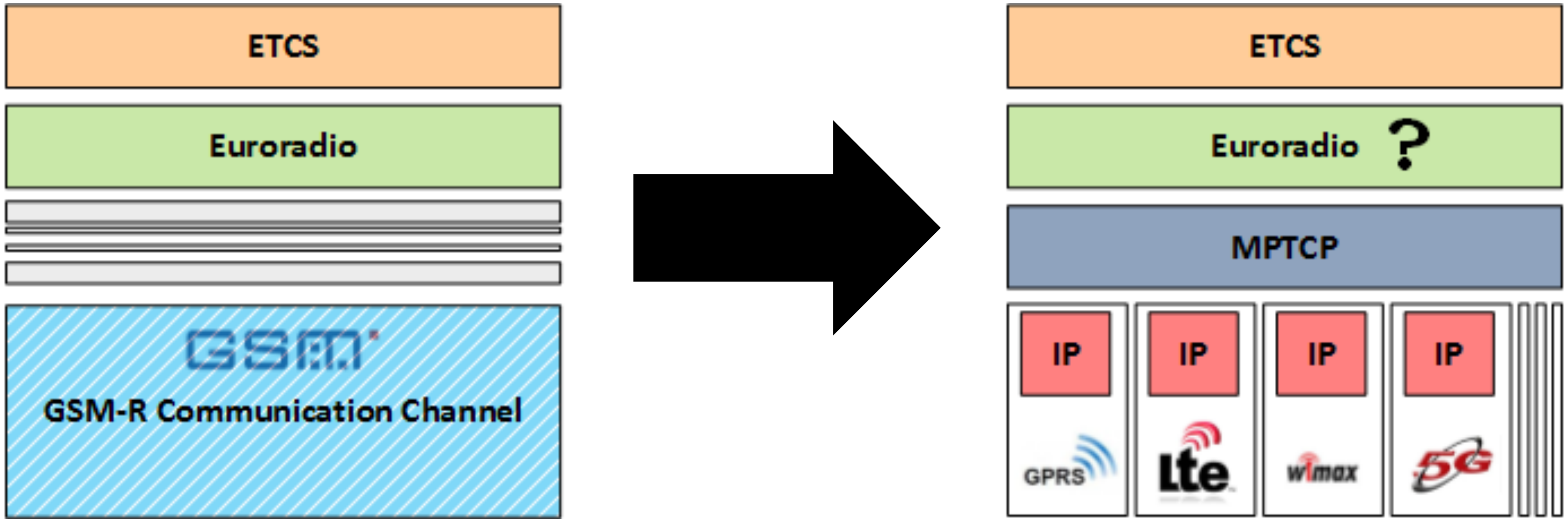
iOS 7 first large-scale, commercial use of resilient TCP extension

By John Cox, Network World
September 19, 2013 11:51 AM ET

- Lopez, I., Aguado, M., & Jacob, E. (2014). End-to-End Multipath Technology: Enhancing Availability and Reliability in Next-Generation Packet-Switched Train Signaling Systems. IEEE Vehicular Technology Magazine, 9(1).

Our on-going research

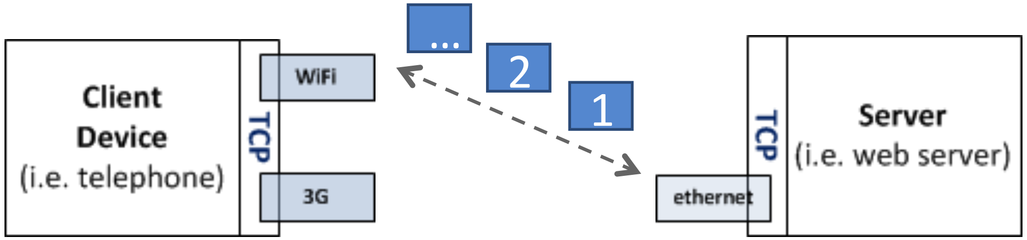
Our prototype allows coexistence of heterogeneous access networks with the same network protocol stack



It unlinks signaling application and access network permitting a continuous evolution of railway communications

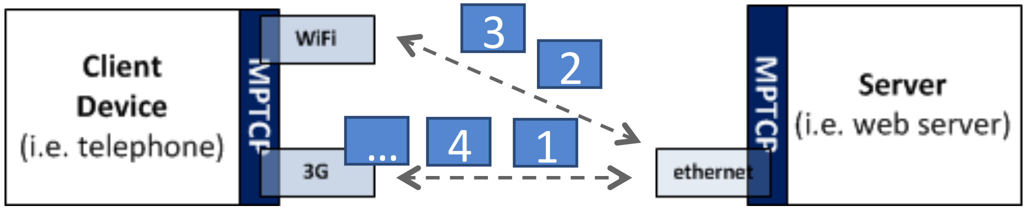
Our ongoing Research : End-to-End Multipath Technology

TCP vs MPTCP



TCP:

- Only 1 TCP connection
- If TCP connection fails or changes one IP address, re-establish a new TCP connection

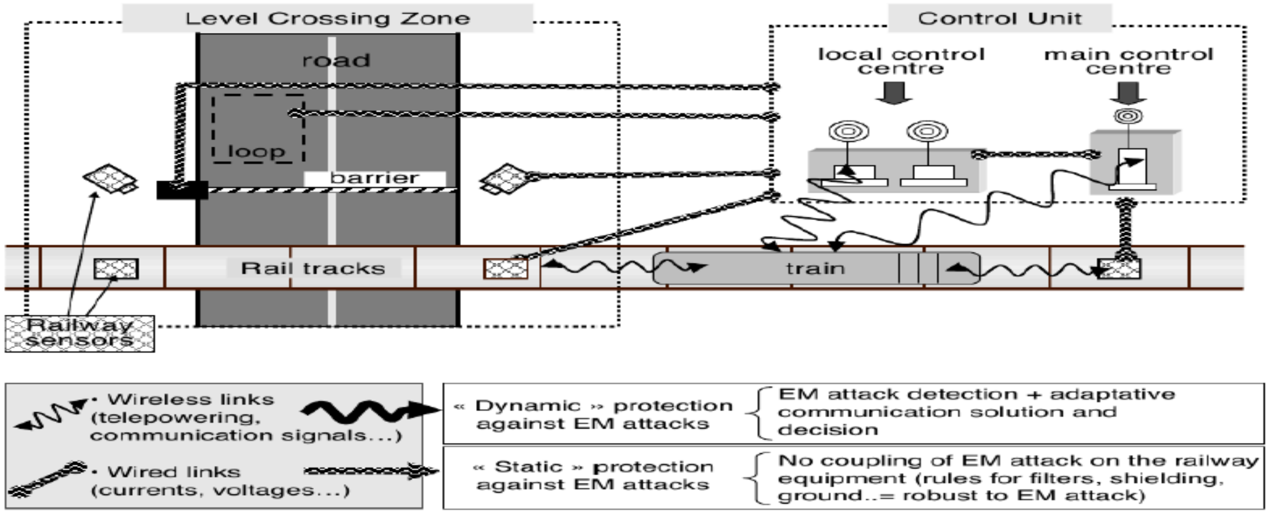


MPTCP:

- Multiple TCP connections (subflows) per MPTCP connection
- If one subflow fails or changes one IP address, MPTCP connection is not lost
- Advantages:
  - Resilience
  - Throughput
  - Vertical/Horizontal soft-handovers

Towards Resilience: Ongoing Research Projects

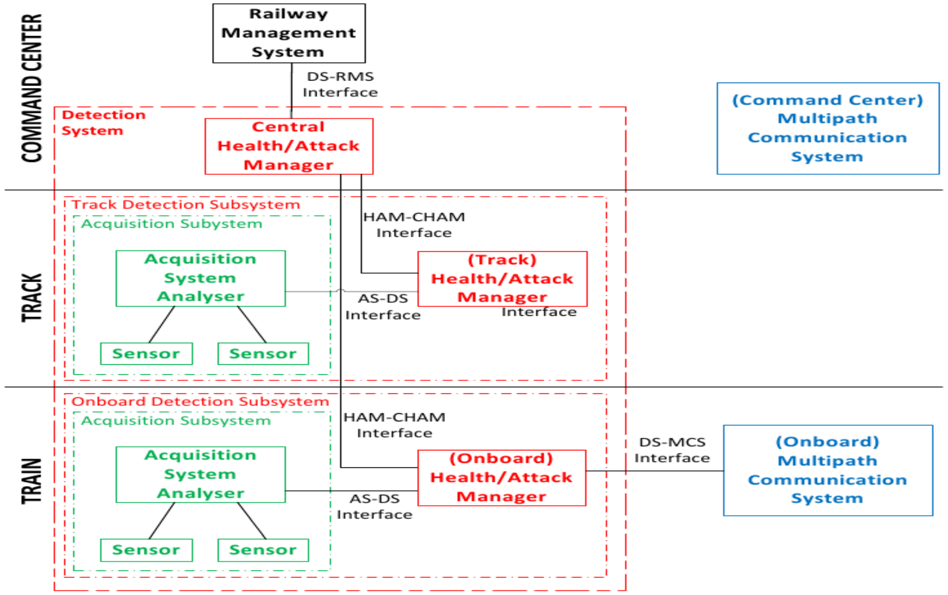
SECRET: Security of Railways against Electromagnetic Attacks (FP7-SEC-2011-1- 285136 STREP) (2012 – 2015)
www.secret-project.eu


Level Crossing Zone
road
loop
barrier
Rail tracks
Railway sensors
train
Control Unit
local control centre
main control centre
• Wireless links (telepowering, communication signals…)
• Wired links (currents, voltages…)
« Dynamic » protection against EM attacks
EM attack detection + adaptative communication solution and decision
« Static » protection against EM attacks
No coupling of EM attack on the railway equipment (rules for filters, shielding, ground..= robust to EM attack)

The project SECRET aims to assess the risks and consequences of EM attacks on the rail infrastructure, to identify preventive and recovery measures and to develop protection solutions to ensure the security of the rail network, subject to intentional electromagnetic (EM) interferences, which can disturb a large number of command-control, communication or signalling systems.

Towards Resilience: Ongoing Research Projects

WP4 - Definition of resilient communication architecture able to support current and advanced traffic management control systems.

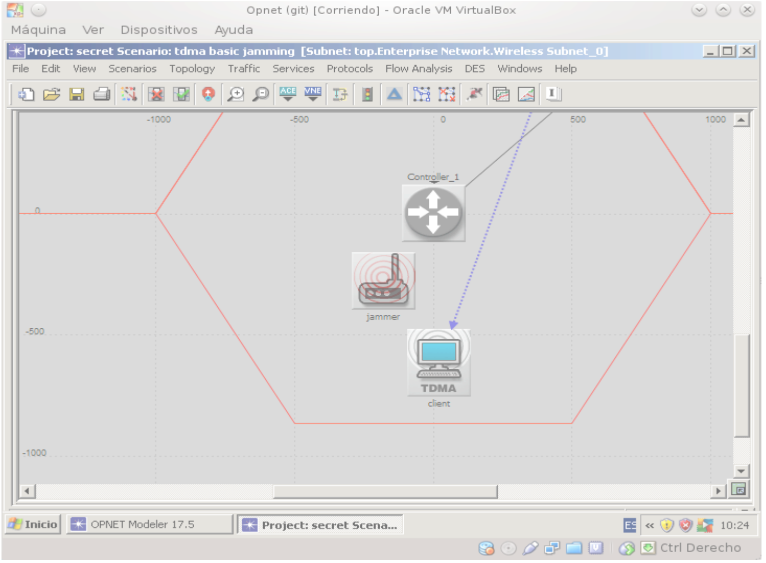

COMMAND CENTER
TRACK
TRAIN
Railway Management System
DS-RMS Interface
Detection System
Central Health/Attack Manager
(Command Center) Multipath Communication System
Track Detection Subsystem
Acquisition Subystem
Acquisition System Analyser
Sensor
Sensor
HAM-CHAM Interface
(Track) Health/Attack Manager
AS-DS Interface
Interface
Onboard Detection Subsystem
Acquisition Subsystem
Acquisition System Analyser
Sensor
Sensor
HAM-CHAM Interface
(Onboard) Health/Attack Manager
AS-DS Interface
DS-MCS Interface
(Onboard) Multipath Communication System

“Heddebaut, M., Mili, S., Sodoyer, D., Jacob, E., Aguado, M., Zamalloa, C. P., ... & Deniau, V. (2014, January). Towards a resilient railway communication network against electromagnetic attacks. In TRA-Transport Research Arena (p. 10p).

Towards Resilience: Ongoing Research Projects

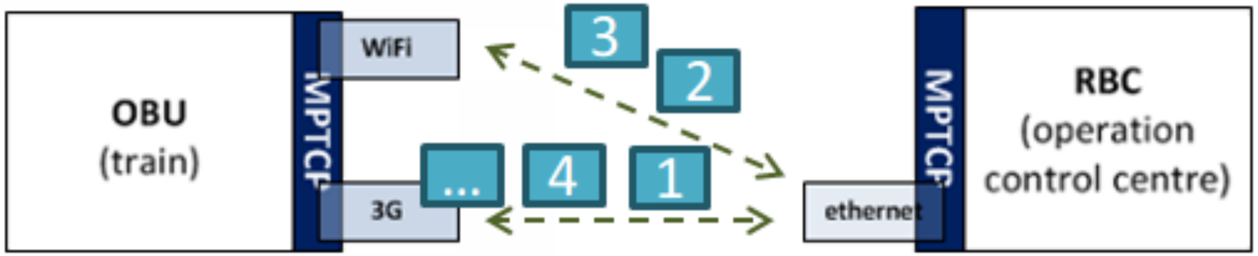
WP3: Monitoring the EM environment. EM attack signatures on communication systems [leader: EHU]

The objective is to evaluate the performance of attacked systems in terms of different operational parameters (packet loss rates, delays, signal/noise ratios…) to provide additional information to the health/attack manager (WP4).



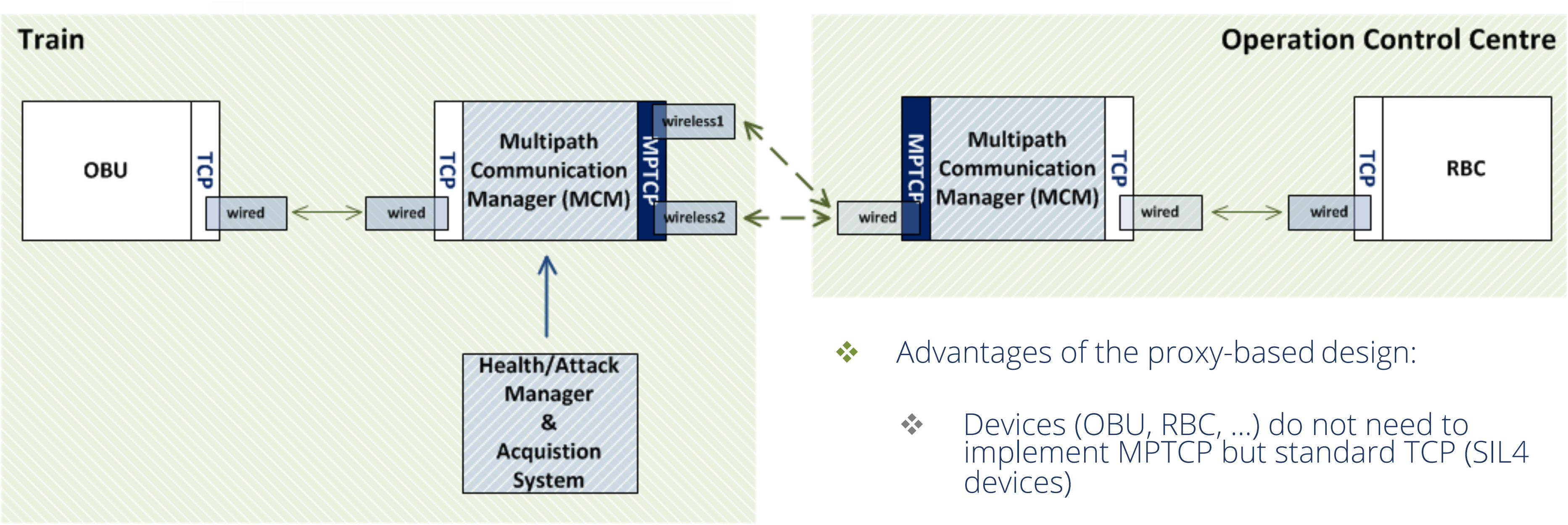
Aguado, M., Pinedo, C., Lopez, I., Ugalde, I., De Las Munecas, C., Rodriguez, L., & Jacob, E. (2014, September). Towards zero on-site testing: Advanced traffic management & control systems simulation framework including communication KPIs and response to failure events. In Wireless Vehicular Communications (WiVeC), 2014 IEEE 6th International Symposium on (pp. 1-2). IEEE

MPTCP in SECRET’s Multipath Communication System



- MPTCP in each device that requires resilient communication

MPTCP in SECRET’s Multipath Communication System


Train
OBU
TCP
wired
wired
TCP
Multipath Communication Manager (MCM)
MPTCP
wireless1
wireless2
Health/Attack Manager & Acquistion System
Operation Control Centre
wired
MPTCP
Multipath Communication Manager (MCM)
TCP
wired
wired
TCP
RBC

- MPTCP provided via TCP-MPTCP proxies (MCM)

- Advantages of the proxy-based design:
  - Devices (OBU, RBC, ...) do not need to implement MPTCP but standard TCP (SIL4 devices)
  - Possibility to provide resilient communications to multiple devices simultaneously with one MCM
  - Better integration with the rest of components of the Resilient Communication Architecture (Health/ Attack Manager and Acquisition System)

Contributions

- Lopez, I., Aguado M. (2015) . Cyber security analysis of the European Train Control System. IEEE Communications Magazine *(to be published in Oct 2015)*
- Lopez, I., Aguado, M., & Jacob, E. (2014). **End-to-End Multipath Technology: Enhancing Availability and Reliability in Next-Generation Packet-Switched Train Signaling Systems.** IEEE Vehicular Technology Magazine, 9(1).
- Aguado, M., Pinedo, C., Lopez, I., Ugalde, I., De Las Munecas, C., Rodriguez, L., & Jacob, E. (2014, September). **Towards zero on-site testing: Advanced traffic management & control systems simulation framework including communication KPIs and response to failure events.** In Wireless Vehicular Communications (WiVeC), 2014 IEEE 6th International Symposium on (pp. 1-2). IEEE.
- Lopez I., Aguado M., Pinedo C., Jacob E.,. (2015). SCADA system in the railway domain: Enhancing reliability through Redundant Multipath TCP. IEEE ITSC2015, September 2015
- Pinedo C., Aguado M.,, Lopez I. (2015)., Modelling and simulation of ERTMS for current and future mobile technologies. Submitted to International Journal of Vehicular Technology.
- Heddebaut, M., Mili, S., Sodoyer, D., Jacob, E., Aguado, M., Zamalloa, C. P., ... & Deniau, V. (2014, January). **Towards a resilient railway communication network against electromagnetic attacks.** In TRA-Transport Research Arena (p. 10p).
- Christophe Gransart, Christian Pinedo, Marina Aguado, Marc Heddebaut, Eduardo Jacob, Igor Lopez, and Marivi Higuero "**Cyber attacks in the guided transport domain** ". Caesar Conference 2014

Thank you

Questions ?

RobustRailS

Next generation train control communication architectures: Cybersecurity and resilience aspects

PhD Marina Aguado
Associate Professor

i2t Research Group

eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
The University of the Basque Country

GOBIERNO DE ESPANA
MINISTERIO DE ECONOMIA Y COMPETITIVIDAD

SECRET PROJECT
SECURITY OF RAILWAYS AGAINST ELECTROMAGNETIC ATTACKS