Digital Technology and Railway Security

ADVANTAGES AND OPPORTUNITIES

Francisco Cardoso dos Reis

Washington, 5 May 2016
"We cannot build and protect our future with yesterday solutions"
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES

AGENDA

• Portuguese Railways Today
• Our digital Rail Performance
• The Future
  • Society and Costumers Expectations
  • Trends and Challenges
  • What Opportunities to Overcome
• Cyber Challenge - Threats and Response
  • Threats
  • Portuguese Cyber Responsibilities
  • National Approach
  • European Approach
  • Common Approach
• Some Conclusions
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Portuguese Railways Today

THE RAILWAY SECTOR IN PORTUGAL

THE REGULATOR
A STATE RULED INSTITUTION

RAIL AND ROAD INFRASTRUCTURE MANAGER

RAILWAY UNDERTAKINGS

CUSTOMERS & MARKET

[*] Passengers

[*] Freight

Francisco Cardoso dos Reis
Washington 5 May 2016
DIGITAL TECHNOLOGY AND RAILWAY SECURITY ADVANTAGES AND OPPORTUNITIES
Portuguese Railways Today

THE RAILWAY SECTOR IN PORTUGAL

IP detains all the essential functions foreseen in the legal European framework for the railway infrastructure managers.

RAILWAY NETWORK STATEMENT
Published in Portuguese since 2003 and English since 2004, and available on IP website.
ABOUT IP

INFRAESTRUTURAS DE PORTUGAL results from a merger between the Portuguese companies National Railway Network - REFER and EP - Estradas de Portugal. REFER and EP became a new company, changing its name to Infraestruturas de Portugal, SA.

The merger was celebrated on June, 1st 2015, following the Decree-Law No. 91/2015 of May, 29th.
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Portuguese Railways Today

ABOUT IP

OUR NUMBERS

- TRAINS: 35,000,000
- ELECTRIFIED RAIL: 1,633.7 km
- RAILWAY: 2,562 km
- STATIONS: 500
- GOODS - BY RAILWAY: 10,000,000 Tons/year
- BRIDGES AND TUNNELS: 7,392
- SUB-CONCESSIONED NETWORK: 1,589 km
- NETWORK UNDER DIRECT JURISDICTION: 13,664 km
- VEHICLES: 22,200,000,000 km/year
- GOODS - BY ROAD: 200,000,000 Tons/year
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

General Systems and Digital Services Delivered
• Signaling systems and automatic train protection
• Tele-surveillance in stations and buildings
• Free Wi-Fi hotspots
• Centralized trains command (we control/dispatch 70% of our network from a single center)
• Real time timetable graphic output
• Real time passengers information
• Tele-command and tele-control of energy supply (power traction)
• All the data transmission needed for our daily activity
There is an urgent need to harmonize the integration of operational functionality and operations on both the road and rail areas. Thus, we began in 2001 the migration of railway operational communications to the IP transmission (Internet Protocol) in order to create an infrastructure "future proof", allowing the emergence of a more efficient, flexible and "off the shelf" infrastructure.

The Portuguese railway network was recognized by UIC in 2009 as the most developed in Europe in this field, which highlights the "mission critical" communications operating systems as the IP transmission technology strong signage. In this context, we continue to evolve the networks "legacy" for this technology.
Infrastructure Level

We are adopting standardized communications systems in the European space within the environment of the CCS - Command Control and Signaling - including the ERTMS system, which telecommunications component deals with the implementation of the network operating mobile GSM-R.

Integration and Interfaces

With regards to the integration of systems we are increasing the capacity of integration between digital transport systems through the adoption of standardized protocols and interface applications, exemplified by the DATEX II on the highway and the TAF-TSI rules and TAP-TSI (telematics applications freight/passenger) on the railroad.
We are seeking to increase the coverage level by sensors in the road and rail network. This is a growing trend to achieve simplicity with today's technology. This allows us to connect with remote devices, installed on open track, and optimize maintenance processes through the collection and processing of real-time information data on infrastructure behavior. The monitoring allows moving from a model of analysis and prediction of infrastructure renewal to a model based on the infrastructure performance conditions, with effective gains in operating costs and future renewals assessment.
Customers and Assets Security

To ensure security it is necessary to increase the level of control and awareness of peoples’ mobility in public spaces and on mass transportation systems as well as the protection of critical infrastructures with impact on service availability and reliability. That's why the implementation of surveillance systems, detection and access control are increasing. Thus providing security authorities better information to be used by the police forces in correlation with other events, allowing superior conditions to protect the society as a whole.
Digital Accessibility

Communication with the transport network user is shifting from personal contact to the "self-service" digital use. The paradigm of Internet and social networks has brought new ways to access services pushing transport service providers to adapt to this new contact channel with their customers. Therefore, we are providing Wi-Fi networks on stations and online services.
As a result of adopting open source technologies, ensuring a successful digital processing (IP - Internet Protocol) it was necessary to develop a new approach regarding the cyber security management (authentication and validation).

We monitor all traffic at strategic network locations (border with external networks, command and control centers, data center, power plants, etc.) to detect cyber attacks, malware, botnets and other security incidents in real time.
Infrastructure Level

To ensure a higher level of cybersecurity awareness we participate in national working groups (eg. Ciberperseu, CERT.pt) as well as international ones (eg. European research projects, ECOSSIAN, ...)

We are working with Portuguese Security Experts to create an internal (IP company and rail sector) awareness policy and training strategy due to be implemented in the next months (information and readiness of all the staff).

Special attention will be dedicated to the operational staff.
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

MAINTENANCE ENGINEERING
• Reliability-Centered Maintenance
• Remote Online Condition Monitoring
• Condition Based Maintenance
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

ENERGY EFFICIENCY MANAGEMENT
• Telemetering + Fleet monitoring
• Driver Advisory System
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

POWER ELECTRONICS
• Upgrade from GTO to IGBT
• Repairing Services
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

Ongoing and deployed projects - Portugal

- RCM ONLINE
- ENERGY EFFICIENCY
- REMOTE CONDITION MONITORING
- REMOTE CONDITION MONITORING
- ENERGY EFFICIENCY
- ENERGY EFFICIENCY
- REMOTE CONDITION

Francisco Cardoso dos Reis
Washington 5 May 2016
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

Ongoing and deployed projects

Norway - VE 923, 12
ON-LINE CORRIDOR MONITORING

Norway - VE 927
ON-LINE CORRIDOR MONITORING

Norway - MAR 2/2/3
ON-LINE CORRIDOR MONITORING

Norway - SNR 71/1
ON-LINE CORRIDOR MONITORING

Norway - SNR 72/2
ON-LINE CORRIDOR MONITORING

Norway - SNR 73/3
ON-LINE CORRIDOR MONITORING

Francisco Cardoso dos Reis
Washington 5 May 2016
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

Ongoing and deployed projects
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
Our Digital Rail Performance

Rolling Stock Level

Ongoing and deployed projects

REMOTE CONDITION MONITORING
ENERGY EFFICIENCY + REMOTE CONDITION MONITORING
REMOTE CONDITION MONITORING
DIGITAL TECHNOLOGY AND RAILWAY SECURITY ADVANTAGES AND OPPORTUNITIES
The Future

Society and Customer Expectations

Better and innovative transport services

• Friendly choice and use of transport modes
  • Efficient network
  • Clear and comprehensive information
  • Simple and integrated offer
• Digital Comfort
  • At stations
  • On trains
  • At interfaces
• Innovative solutions
  • Digital
  • Interactive
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
The Future

Society and Customer Expectations

Better and innovative transport services

- Digital Integration
  - Multimodality/Co-modality
  - Ticketing
- No barriers (stations, interfaces....)
  - Efficient but friendly control systems
  - Balanced approach on security and on commercial needs
- Reduced costs and tariffs (more automation and monitoring)
  - to customers
  - to society
DIGITAL TECHNOLOGY AND RAILWAY SECURITY ADVANTAGES AND OPPORTUNITIES
The Future

Society and Customer Expectations

Better and innovative transport services

- Increased Security (Digital)
  - Services
  - Systems
  - Equipment
- All on/all connected availability
  - Free Wi-Fi
  - Integrated digital offer
- Less disruptions
DIGITAL TECHNOLOGY AND RAILWAY SECURITY ADVANTAGES AND OPPORTUNITIES
The Future

Trends and Challenges

Society General Trends

• Bigger and Smarter Cities
• Teleworking
• Daily activities based on low energy consumption
• Use of clean energy
• Decrease of car use and of total number of trips
• More people walking and using bicycles
• Increase of collective transport
• Decrease of human intervention on transport operation
• Increase of digital services and its use
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
The Future

Trends and Challenges
General Challenges on Transport

Tele-maintenance
Tele-command
Tele-surveillance
Digital Information
Automation
Smart Cities
Smart Mobility
Ticketing
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
The Future

Trends and Challenges

General Challenges based on IP

Internet of Businesses
Internet of Mobility
Internet of Health
Internet of Leisure
Internet of Defense

Internet of Things
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
The Future

What Opportunities to Overcome

Connected and Automated Driving
Technological developments in the field of communications V2I (Vehicle to Infrastructure) and V2V (Vehicle to Vehicle).

Sensors and embedded devices increase, turn the road and rail vehicles in a collaborative and integrated entity of the infrastructure.

Both the rail and road infrastructure level’s must keep pace with technology, allowing the digital automation.

Francisco Cardoso dos Reis
Washington 5 May 2016
What Opportunities to Overcome

Internet-Of-Things / Big Data

Infrastructure management, transport operation and digital sensors collects an increased amount of data. That knowledge leads to the adequacy of models of operation and maintenance of infrastructure. There is a significant trend on the evolution of connected devices like autonomous sensors and related equipment.

In the management of transport infrastructure, the use of these devices allows mass scanning at lower costs and participation in collaborative environments to exchange information, particularly with use of consolidated standards.
What Opportunities to Overcome

Smart Cities

Cities are progressing in the digital approach. Cities need to have a comprehensive, integrated and efficient systems of transport management and access to the infrastructure. Integration of Intelligent Transportation Systems with the Smart Cities concept will enable in general the performance of all transport networks.
What Opportunities to Overcome

Safe and Secure Services

Efficient monitoring and efficient cybersecurity policies will be necessary to the management of the digital infrastructure. Thus we will focus on the continuous implementation of automated monitoring security processes in real time.

It is a part of IP’s strategy to have a cybersecurity laboratory to perform "mission critical" application testing (eg SCADA Systems and other applications to support the railway operation), testing of new equipment and their vulnerabilities in situations of attempted security breach.

We also intend to implement a 24/7 operating position for the Security Operation Center dedicated function to promote the monitoring of critical infrastructure and to address cybersecurity incidents.
Cyberspace is a space of threats, opportunities and power, in a virtual world, where National security and our way of life is in risk.
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
CYBER CHALLENGE THREATS AND RESPONSE

Threats

Are we safer or cyberspace makes us more vulnerable to external attacks?

• North Korea tried to hack South's railway system (World, 8 MAR 2016)
• Schoolboy hacks into city's tram system (Telegraph, 11 Jan 2008)
• Al-Qaeda allegedly Hacks Indian Railways (Indianexpress.com, 2 MAR 2016)
• Hackers Breached Railway Network, Disrupted Service (wired.com, 24 MAR 2012)

“Everyone” can do cyberattacks, not only hackers.

That’s why we create a complex infrastructure to stop the threat...Cybercenters and cyber institutes.
Portuguese’s cyber Responsibilities

- Ministry of Justice: cybercrimes
- Ministry of Internal Affairs: cyberterrorism
- Intelligence Services: cyber intelligence
- Portuguese Armed Forces: protection against external military aggression (Includes Cyberspace)
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
CYBER CHALLENGE THREATS AND RESPONSE

National Approach

National Cyber Security Strategy

"... promote a free use, safe and efficient cyberspace by all citizens, businesses and public and private entities."

RCM nº 36/2015 (Approves the National Cyber Security Strategy)
National Strategy

The National Strategy to Secure Cyberspace, published by Resolution of the Council of Ministers nº36/2015 of 12 June, is based on the commitment to reinforce the security of networks and information. This was to ensure the protection and defense of critical infrastructure and vital information services, and promote a free use, safe and efficient cyberspace by all citizens, businesses and public and private entities.

Axis for National Cybersecurity Action Plan:

Axis 1 - Security Structure of Cyberspace
Axis 2 - Combating Cybercrime
Axis 3 - Cyberspace Protection and Infrastructure
Axis 4 - Education, Awareness and Prevention
Axis 5 - Research and Development
Axis 6 - Cooperation
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
CYBER CHALLENGE THREATS AND RESPONSE

The Defense of the National Cyberspace
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
CYBER CHALLENGE THREATS AND RESPONSE

BENEFITS FROM NATIONAL CYBERSECURITY POLLING AND SHARING PROGRAMS

• Leverage the expertise and experience of existing private/public sector critical infrastructure protection organizations to improve the resilience of each other’s and the nation

• Maximize the share of information between the government and private sector critical infrastructures, as well as share information among sectors

• Maximize protection against modern attacks and malware
European Approach

To address cybersecurity in a comprehensive manner; activities should span across three key pillars— NIS, law enforcement, and defense—which also operate within different legal frameworks:

Network and Information security

EU

NATIONAL

European Approach


The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems (definition of criminal offences, relevant sanctions, and improving cooperation between competent authorities, agencies and bodies).
European Approach

ENISA (European Network and Information Security Agency)

- ENISA was formed in 2004. The original mandate was renewed and extended in 2013.

The Agency is a Centre of Expertise that supports the Commission and the EU Member States in the area of information security.

**General role of ENISA**

**Assistance to Member States and the Commission by providing its expertise and advice and by facilitating exchange of best practices.**

- Assistance to Member States in developing national NIS strategies.
- Participation within the EU NIS Cooperation Group.
- Provide secretariat support for the CSIRT network.
- Support the Commission in developing security and notification requirements for ESP and DSP.
- Assistance to Member States in developing national CSIRTs.

Elaborate advices and guidelines regarding standardization in NIS security, together with Member States.
European Approach

NIS Directive (Network and Information Security)
Scope: to achieve a high common level of security of NIS within the Union (first EU regulatory act at this level).
Key Provisions:
- Obligations for all Member States to adopt a National NIS strategy and designate National Authorities.
- Obliges Member States to designate national competent authorities and CSIRTS (Computer Security Incident Response Teams).
- Creates first EU cooperation group on NIS, from all Member States.
- Creates an EU national CSIRTS network.
- Establishes security and notification requirements for operators of Essential Services (ESP) and Digital Service Providers (DSP).
Common Approach

Portugal, having responsibilities at European level, needs to ensure compliance with European standards, particularly regarding the European Security Plan for Critical Infrastructures. National critical infrastructures should be a focus of attention in what management of public risks is concerned, since these represent a set of services that are essential to the functioning of the country and to the forces that ensure national defense.
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES
CYBER CHALLENGE THREATS AND RESPONSE

Short/Medium term challenges on CYbersecurity

Decision and policy makers

- Promote public/private collaboration on IPT cyber security at national level and EU-wide
- Promote and ease the development of a common EU approach to IPT security
- Develop a comprehensive strategy and framework for cyber security in IPT
- Integrate and converge security efforts made in other sectors of activity
- Foster the development of harmonized cyber security standards for IPT
**Short/Medium term challenges**

**Infrastructure Managers and Operators**
- Integrate cyber security in their corporate governance
- Develop and implement an integrated corporate strategy addressing holistically cyber security and safety risks
- Implement risk management for cyber security in multi-stakeholder environments including external contractors and dependencies
- Clearly and routinely specify their cyber security requirements
- Annually review organizational cyber security processes, practices and infrastructures

**Manufacturers of IPT systems and solutions**
- Create products/solutions that match the cyber security requirements of IPT end-users
- Collaborate in the development of IPT-specific standards and apply them to IPT solutions
- Develop a trusted information sharing platforms on risks and vulnerabilities
- Provide security guidance for your systems, products and solutions
We are living challenging times that stimulate our innovative capacities.

We must find and follow the opportunities to:

- Increase efficiency and the use of public transport
- Adapt the structure of our offer and our commercial approach to new customers’ expectations and requirements
- Contribute to more sustainable cities and a better quality of life
- Have more driveless and electric vehicles
- Increase sensing solutions on transport
- Promote solutions on demand

We shall increase the use of Digital and Automation in Railways.
Despite threats, we must not fear the future but:

- Be aware and cautious (Improve awareness through cross-training and joint formation)
- Be resilient and competent
- Predict and avoid disruptions
WE SHALL NOT FEAR THE FUTURE BUT BE AWARE, RESILIENT AND PREDICTIVE
DIGITAL TECHNOLOGY AND RAILWAY SECURITY
ADVANTAGES AND OPPORTUNITIES

THANK YOU FOR YOUR ATTENTION