LABORATÓRIO NACIONAL
DE ENGENHARIA CIVIL

USE-IT – USERS, SAFETY, SECURITY AND ENERGY IN TRANSPORT INFRASTRUCTURE

Security of people and security of goods

REPORT 365/**2022 – DED/NUT**

LABORATÓRIO NACIONAL
DE ENGENHARIA CIVIL

USE-IT – USERS, SAFETY, SECURITY AND ENERGY IN TRANSPORT INFRASTRUCTURE

Security of people and security of goods

Lisbon • December 2022

R&D BUILDINGS

REPORT 365/**2022 – DED/NUT**

Title

USE-IT – USERS, SAFETY, SECURITY AND ENERGY IN TRANSPORT INFRASTRUCTURE
Security of people and security of goods

Authors

BUILDINGS DEPARTMENT

Margarida Rebelo
Assistant Researcher, Urban and Territorial Studies Unit

Paulo Machado
Assistant Researcher, Acoustics, Lighting, Buildings Components and Facilities Unit

Collaboration

BUILDINGS DEPARTMENT

Álvaro Pereira
Senior Technician, Urban and Territorial Studies Unit

AV DO BRASIL 101 • 1700-066 LISBOA
e-mail: lnec@lnec.pt
www.lnec.pt

Report 365/2022

File no. 0603/1101/19430, 0804/1101/1943003

USE-iT – Users, safety, security and energy in transport infrastructure

Security of people and security of goods

Abstract

This report presents the work done by LNEC exclusively under the WP3 – Safety and security of people and goods within the Horizon 2020 project *Users, Safety, Security and Energy in Transport Infrastructure* (USE-iT). The topic of human security, which includes the safety of people and property, has assumed a growing relevance in the concerns of European institutions, a fact not unrelated to the enormous exposure to multiple risks and the identification of evident societal vulnerabilities.

The work developed under WP3 comprised five steps, namely, 1) a survey to seek preliminary inputs to the identified concepts and areas in transport safety and security, 2) a workshop to gather the stakeholders' inputs regarding the preliminary investigation across modes and domains-technologies identified, 3) interviews with experts and stakeholders to seek more in-depth input, 4) a workshop to obtain the input from stakeholders' regarding common research challenges and to build a research roadmap and, 5) a conference to present the final roadmap of research topics and key recommendations.

Within WP3, several technologies, methodologies, and approaches with the capacity to improve transport safety and security in all modes were identified and categorised in areas and concepts. Stakeholders' multiple rounds of consultation on these technologies and approaches addressing the cross-modal challenges related to security are cybersecurity, security in transit environments, crime prevention through environmental design and the remote detection of explosives and other materials.

Keywords: Security of people / Security of goods / Transport / Users

USE-iT – Utilizadores, segurança e energia nas infra-estruturas de transporte

Segurança de pessoas e de segurança de bens

Resumo

Este relatório apresenta o trabalho realizado pelo LNEC exclusivamente no âmbito do WP3 – Segurança e segurança de pessoas e bens do projeto Horizonte 2020 *Utilizadores, Segurança, Segurança e Energia nas Infraestruturas de Transportes* (USE-iT).

O tópico da segurança humana, que compreende a segurança de pessoas e bens, tem assumido uma relevância crescente nas preocupações das instituições europeias, facto a que não é alheia a enorme exposição a múltiplos riscos e a identificação de evidentes vulnerabilidades societais.

O trabalho desenvolvido compreendeu cinco etapas, nomeadamente, 1) inquérito a interlocutores privilegiados sobre a pertinência dos conceitos e das áreas identificadas, 2) workshop para recolha do contributo dos interlocutores privilegiados sobre a investigação preliminar das tecnologias e abordagens mais relevante na segurança de pessoas e bens em todos os modos de transporte, 3) entrevistas a peritos e interlocutores privilegiados para procurar aprofundar a informação previamente recolhida, 4) workshop com interlocutores privilegiados para identificar os desafios comuns à investigação nesta área e para recolher informação relevante de base à elaboração de um *roadmap* da investigação em segurança em transportes e, 5) conferência final para apresentar o roteiro de investigação e as recomendações-chave no domínio da segurança de pessoas e bens nos vários modos de transporte.

No âmbito do WP3, diversas tecnologias, metodologias e abordagens com a capacidade de melhorar a segurança nos transportes foram identificadas e categorizadas em áreas e conceitos em todos os modos. As múltiplas rondas de consulta aos interlocutores privilegiados permitiram identificar as tecnologias e abordagens mais prementes para abordar os desafios intermodais relacionados com a segurança, nomeadamente, a cibersegurança, a segurança em trânsito, a prevenção da criminalidade através do desenho das infraestruturas e a deteção remota de explosivos e outros materiais.

Palavras-chave: Segurança de pessoas / Segurança de bens / Transportes / Utilizadores

Table of contents

List of figures

List of tables

List of acronyms and abbreviations

ACS	Access Control System
AVSEC	Aviation Security
CARONTE	Creating an Agenda for Research ON Transportation sEcurity
CBRN	Chemical, biological, radiological and nuclear
CCTV	Closed-circuit television
DfT	Department for Transport
ECAC	European Civil Aviation Conference
EU	European Union
FAA	Federal Aviation Administration
FEHRL	Forum of European Highway Research Laboratories
HLEG	High Level Expert Group
ICAO	International Civil Aviation Organization
ICT	Information and Communication Technologies
IT	Information Technologies
LEA	Law Enforcement Authorities
PROTECTRAIL	The Railway-Industry Partnership for Integrated Security of Rail Transport
SECRET	SECurity of Railways against Electromagnetic aTtacks
SECURESTATION	Station and terminal design for safety, security, and resilience to terrorist attacks
SIDOS	Security In the Design Of Stations
SOS	Standardized Onion-Skin
TASS	Total Airport Security System
TMC	Traffic Management Centres
TWCS	Train to Wayside Communication System
USE-iT	Users, Safety, Security and Energy in Transport Infrastructure
VAS	Vital Area Security

1 | Introduction

This report presents the work done by LNEC under the WP3 – Safety and security of people and goods within the Users, Safety, Security and Energy in Transport Infrastructure (USE-iT) H2020 project. This project had a significant scope, and LNEC's contribution was reflected in other WPs. However, due to the work developed in this Work Package, and even the shared coordination of some of its Tasks, it was considered valuable to systematize it independently from the other tasks carried out within USE-iT.

The specific activities of WP3 in the component of security were developed in five steps:

1) Survey implementation to seek preliminary inputs to the identified concepts and areas in transport safety and security (November 2015);
2) Stakeholders' input regarding the preliminary investigation across modes and domains-technologies identified (Workshop #1; January 2016);
3) In-person and phone interviews with experts and stakeholders in their national languages to seek more in-depth input (June-August 2016);
4) Stakeholders' input regarding common research challenges and roadmap construction (Workshop #2; September 2016);
5) USE-iT final conference to present the final roadmap of research topics and key recommendations (April 2017).

The project Users, Safety, Security and Energy in Transport Infrastructure (USE-iT) was a Horizon 2020 Coordination and Support Action (CSA) with a duration of two years (2015-2017), coordinated by the Forum of European Highway Research Laboratories (FEHRL). The project addressed MG. 8.2-2014 next generation transport infrastructure: resource efficiency, smarter and safer from the Horizon 2020 Work Programme 2014-2015 in the field of smart, green, and integrated transport.

USE-iT builds on the FORx4 method in which the four transport modes (*i.e.*, road, rail, water, and air) were merged with four shared domains (*i.e.*, infrastructure, technology, governance, and customer) to create a holistic transport system for the future (*vd*. Table 1.1).

Table 1.1 – Description of USE-iT domains

Domains	Description
Infrastructure	The transport network formed from Europe's routes and interchanges, including the required changes in construction and maintenance and the specifications used.
Technology	The information, communications, sensor, and power systems will support the future transport network.
Governance	The management, operations, investment, and appraisal of the network.
Customer	The understanding of customers' motivation for travelling and choice of mode to implement policy interventions to support political objectives.

The primary purpose of USE-iT was to examine common challenges across these domains and modes, identifying potential areas for transferring good practices and possible collaborative research. Moreover, the objective of USE-iT was to better understand the challenges experienced across transport modes, bring representatives of transport modes together to share skills and experience and develop a set of common research objectives.

The specific objectives were to:

- Understand the state-of-the-art in three technical areas: user information, safety and security, energy, and carbon across all four modes (*i.e.*, air, road, rail, and water);
- Determine opportunities for the transfer of knowledge and working practices across modes;
- Develop common future research objectives covering at least two modes;
- Bring together infrastructure owners, operators, and other stakeholders from across the transport modes to facilitate knowledge transfer and develop a network for future co-operation;
- Develop a roadmap describing the research challenges and implementation steps to achieve greater cooperation and co-modal operations in the areas covered by the project.

The project was developed in three phases according to the Description of Work, all contributing to the conception of a roadmap describing the main research challenges and implementation steps to achieve greater cooperation and co-modal operations (Figure 1.1).

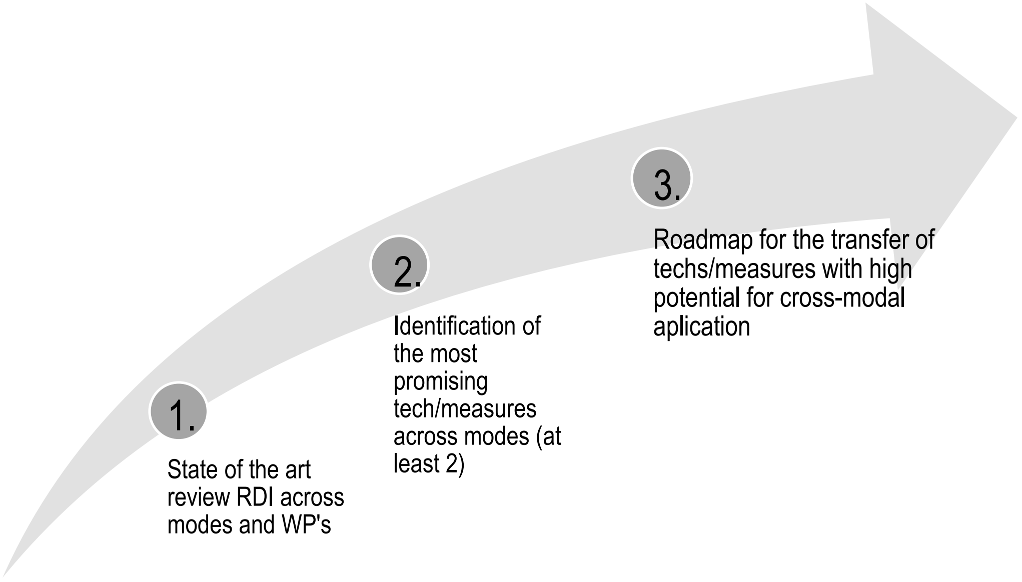

1.
State of the art review RDI across modes and WP's
2.
Identification of the most promising tech/measures across modes (at least 2)
3.
Roadmap for the transfer of techs/measures with high potential for cross-modal aplication

Figure 1.1 – Implementation phases of the USE-iT project

The first step consisted of undertaking a state-of-the-art in the specific topics across the four transport modes in each Work Package. Based on the findings of this review, the most appropriate technologies/measures/methods that can apply on a cross-modal basis or for at least two transport modes were identified and analysed according to an iterative stakeholders/expert consultation process (phase 2). The final phase consisted of developing a roadmap for future research and implementing the technologies/measures across each mode (*vd*. Figure 1.1).

2 | Measures on the security of people and of goods

This chapter presents an overview of the selected technologies and measures regarding the security of people and of goods, organised into four topics: measures to prevent criminal activity, measures to reduce opportunities for criminal activity, transportation safekeeping and surveillance. An illustrative case study was selected for each topic, providing more detailed information, namely a brief description of the technology/approach, the applicability to the transport modes, the potential applicability to other modes, the opportunities and benefits that could be derived from its development and implementation and the potential barriers to its development or implementation. The comprehensive list of the initial information is presented in Annex I.

By the security of a person, we should understand, under the constitutional principles of freedom and liberty, the absence of physical constraint to access, use and leave public transport, without any limitations real or subjective), safely and in a self-determined way. For passenger security, screening methods need to consider ensuring high-security levels with the minimum hassle (Ceccato & Newton, 2015; Crime Concern, 2004; MTRS3, 2012; Newton, 2014).

Security of goods (*e.g.,* assets) refers to the transport conditions that preserve the quality, integrity and legitimate ownership of the goods transported from malicious acts against these principles. These conditions also include track clearance, clearance of infrastructures before and after use, freight clearance control, tracking and monitoring of rolling stock carrying goods, protection of staff and information systems, stations, buildings, and infrastructure protection (MTRS3, 2012; Protectrail, 2014).

2.1 Measures to prevent criminal activity

The measures to prevent criminal activity concept refers to all measures belonging to the primary prevention stage. Primary prevention aims to prevent any unlawful and dangerous acts before they occur, wherever, whenever, and whatever. These measures should be mainly considered when planning and designing facilities or conceiving new technological devices oriented to crime prevention. Thus, probably these measures will be timelier expected in the infrastructure and technology domains and the preliminary stages of the governance domain (Crowley, 2013; Welsh & Farrington, 2010). Table 2.1 presents the approaches and technologies previously identified, with cross-modal applicability.

Table 2.1 – Measures to prevent criminal activity

Technology / measure / approach	Domains	Transport mode in which it exists	Transport mode in which it could be applied
European Security Research and Innovation Agenda	Governance	Air, Rail, Road, Water	Air, Rail, Road, Water
Security in transit environments	Technology & Infrastructure	Rail, Road, Water	Air
Security in the design of stations (SIDOS)	Infrastructure	Road	Air, Rail

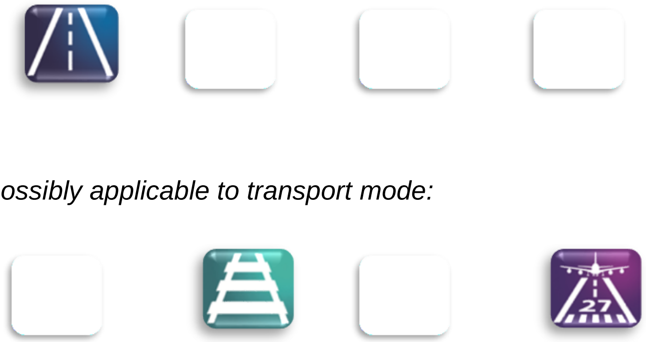
Case study – SIDOS (Security in the design of stations)

There is considerable scope in the design and planning of station infrastructure to include proven and adequate security measures that will prevent, mitigate, or deter attacks from terrorists. The following measures can be implemented:

- Mitigating effects of a blast – Implementation of appropriate physical and procedural security measures, which should be ‘designed in’ at all stages of station development;
- Operational Requirement Process – This includes containing building services and power supplies, locating public car parks as far away from station buildings as practically possible and creating a distinct separation from other ‘crowded places’;
- Station approaches – Increase stand-off using landscaping and road design features such as traffic calming chicane measures, but also consider emergency vehicle access;
- Station building structure – A quantifiable degree of blast resistance should be used; any glazing should be Polyvinyl Butyral laminate;
- Internal facilities – Reduction of flat-topped structures and waste management facilities located away from entrances and main concourses.

The identification of a technology already applied in a mode of transport and its transferability to another mode of transport is a key point of USE-iT and can be shown schematically (Figure 2.1). This Figure is concerned with an existing technology in the road mode that can have applications in rail and air modes.

Technology applicable to transport mode:



Technology/measure possibly applicable to transport mode:

Figure 2.1 – Technological transferring between modes of transport (1)

Note: The symbology of the modes of transport was consensualised between the partners of the Project and, in a way, is its brand image.

Opportunities and benefits from development and implementation:

In the design process of a station, it is essential to take a comprehensive approach considering all aspects, including passenger access, health and safety and creating a place functionally usable.

Barriers to development or implementation:

- Procedures could already be in place;
- Legal barriers in terms of specific requirements (especially in air mode).

2.2 Measures to reduce opportunities for criminal activity

Measures to reduce opportunities for criminal activity can be understood as belonging to both secondary and tertiary stages of prevention. Secondary prevention aims to reduce the impact of unlawful and dangerous acts that have already occurred. Tertiary prevention stage measures refer to those that seek to soften the impact of an ongoing structural handicap beyond the transport stakeholders' reasonable control. All these measures (*i.e.*, secondary or tertiary prevention) are appropriate to improve the security conditions of transport facilities, usually after assessing old procedures (Crowley, 2013; Welsh & Farrington, 2010). Table 2.2 presents the technologies and approaches identified so far for preventing opportunities for criminal activity, with cross-modal applicability.

Table 2.2 – Measures to prevent opportunities for criminal activity

Technology / measure / approach	Domains	Transport mode in which it exists	Transport mode in which it could be applied
Anti-terrorism aviation security policy	Governance	Air	Rail, Road, Water
Aviation security practices	Governance, Customer	Air	Rail, Road, Water
Cybersecurity	Infrastructure, Technology	Air, Rail, Water	Road

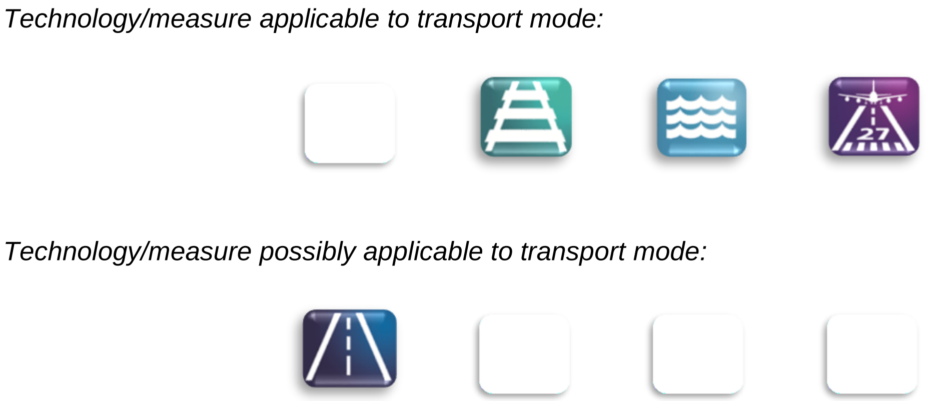
Case study – Cybersecurity

Cyber hacking attacks can affect all the technology related to electronic data transfer, such as electronic devices, software, hardware, and communications backbone is vulnerable and subject to cyber safety threats.

Cybersecurity affects surface electronic devices in entities such as road Traffic Management Centres (TMC), train signalling systems, airports, aeroplanes, tramways, passenger and cargo vessels. Potential cyber vulnerabilities in transport infrastructure and vehicles need to be mitigated by security protocols and plans ahead of time. The main goals of cybersecurity are systems safety, system security, system reliability and system resilience.

Create a cybersecurity eco-system through:

- Identifying systems, connections & interdependencies;
- Assessing vulnerabilities and risks;
- Identifying and using best practices and standards;
- Including cybersecurity in design specs and acquisitions;
- Collaborating with IT, physical security & other groups;
- Developing policies and procedures for cybersecurity;
- Motivating employees with training, exercises & "hot triggers";
- Making sure that systems and operations are resilient (*e.g.,* layers, detection, incident response);
- Developing organization-wide strategic plan linked to funding.



Technology/measure applicable to transport mode:

Technology/measure possibly applicable to transport mode:

Figure 2.2 – Technological transferring between modes of transport (2)

Opportunities and benefits from development and implementation:

As vehicles become increasingly automated, systems can be affected by:

- Control domain (Vehicle Controls, Vehicle Diagnostics, Traffic Signal Priority, Video Surveillance Duress Alarms, Vehicle Immobilizers);
- Operations domain (Automated Dispatching Vehicle Location, Route/Schedule Status Passenger Counters, Stop Annunciation Electronic Payments);
- Infotainment Domain (Customer use of Wi-Fi and WiMAX Real-time Travel Info & Trip Planning).

The implementation of cybersecurity could not only protect development in infrastructure and in-vehicle technologies but also help increase acceptance of new innovative technologies (*e.g.,* autonomous vehicles).

Barriers to development or implementation:

- Difficult to standardise.

2.3 Transportation safekeeping

Transportation safekeeping integrates all measures, namely codes, standards, technical recommendations, and others, to keep users, staff, and transportation infrastructures safe and protected (including buildings, vehicles, and equipment) from unacceptable risks and vulnerabilities. This concept regards technical procedures primarily generated within the transport system and as a result of technical expertise. In this sense, it has a less interdisciplinary reach and resembles a formal rule system and its related procedures (European Commission, 2012). Table 2.3 presents the technologies/measures/approaches previously identified within the transportation safekeeping topic.

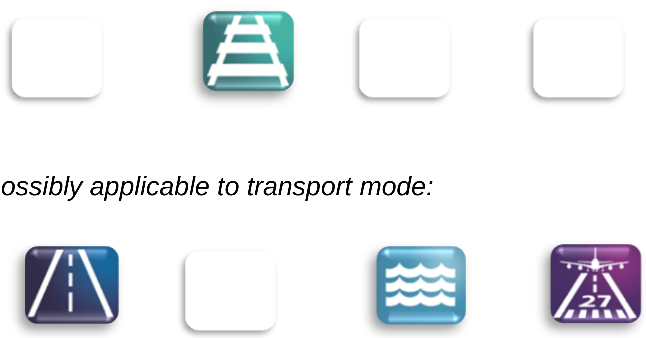
Table 2.3 – Technologies and measures for transportation safekeeping

Technology/measure/approach	Domains	Transport mode in which it exists	Transport mode in which it could be applied
Monitoring and intervention for the transportation of dangerous goods (MITRA)	Technology	Rail	Air, Road, Water
Reduction of suicides and trespasses on railway property (RESTRAIL)	Infrastructure & Governance	Rail	Air, Road, Water
Technology and measures for security of railways against electromagnetic attacks (SECRET)	Technology	Rail	Air, Road, Water
Specific technologies and measures for Secured Urban Transportation (SECUR-ED)	Technology	Rail	Road
Technology and measures for blast resistant and fire safe metro vehicles (SECUREMETRO)	Technology & Governance	Rail	Air, Road, Water
Station and terminal design for safety, security, and resilience to terrorist attack (SECURESTATION)	Technology & Infrastructure	Rail	Air, Road, Water

Case study – Station and terminal design for safety, security, and resilience to terrorist attacks (SECURESTATION)

A compendium of technologies, means, materials and engineering techniques for safety, security, and operational uses in passenger terminals, which can be implemented as a basis for developing the Constructive Design Handbook, has been proposed:

- Closed-circuit television (CCTV) and Video analytics tools to improve security in public transport (Intrusion, tracking, crowd assessment and face recognition). It can help investigate incidents;
- Access Control System (ACS) for help points, announcement facilities, signage, vehicle management, intrusion and materials detection, alarm systems;
- Smoke, flame and fire detection and protection systems (devices and control panels);
- The use of matured tools: blast attack simulations, Fire Dynamic Simulator, Fire & smoke, and evacuation modelling.



Technology/measure applicable to transport mode:

Technology/measure possibly applicable to transport mode:

Figure 2.3 – Technological transferring between modes of transport (3)

Opportunities and benefits from development and implementation:

Some relevant techniques/technologies could be implemented for the other transport stations/terminals as help points, alarms and announcement facilities, signage, access management controls, vehicle management, threat detection systems (*e.g.*, screening, materials detection), intrusion detection systems, tracking applications, access controls and barriers, indoor and outdoor systems, perimeter protection, fencing, walls, gates, and vehicles design.

Barriers to development or implementation:

Suitability and adaptability for implementing project results need more investigation, especially regarding road/water transports passenger stations/terminals security against terrorist bomb blasts and chemical, biological, radiological, and nuclear attacks. Technologies need to be investigated from ethic, legal and social points of view for the road/water transport.

2.4 Surveillance

Surveillance regards all measures aiming at monitoring water, air, and land transportation facilities, including people, goods, and infrastructure, and increasing transportation security. Surveillance could be included in the overall scope of the concept regarding the measures to reduce opportunities. However, because of the technological specificity, it is considered an independent concept and should not be reduced to CCTV. According to the literature, a surveillance task can be divided into three phases: event detection, event representation, and event recognition. The detection phase manages multisource spatial and temporal data fusion for efficiently and reliably extracting motion trajectories from video. The representation phase summarizes raw trajectory data to construct hierarchical, invariant, and content-rich representations of the motion events. Finally, the recognition phase deals with event recognition and classification (Welsh, Farrington & O'Dell, 2010; Wu *et al.*, 2003). Table 2.4 presents the technologies and measures for surveillance that were previously selected for in-depth analysis.

Table 2.4 – Technologies and measures for surveillance

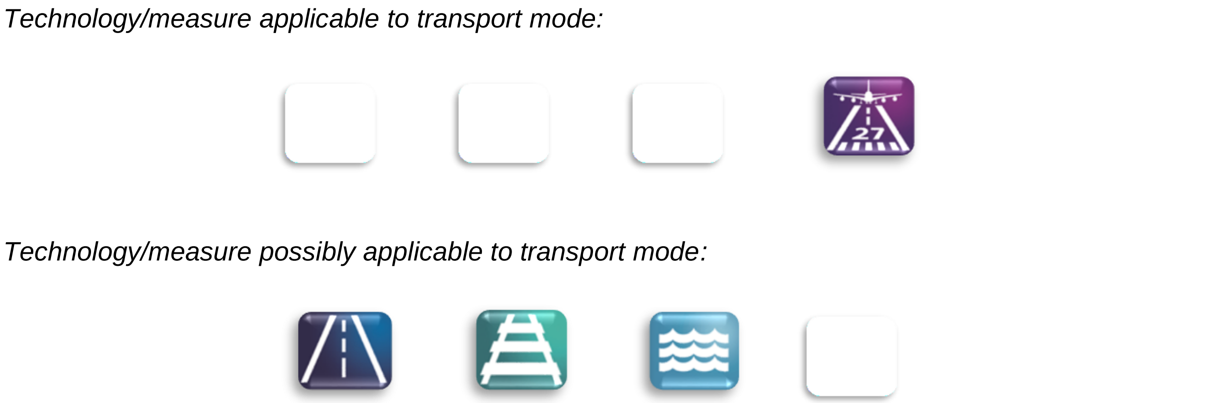
Technology / measure / approach	Domains	Transport mode in which it exists	Transport mode in which it could be applied
Technology and measures for Integrated Security of Rail Transport (PROTECTRAIL)	Technology	Rail	Air, Road, Water
Total Airport Security System (TASS)	Technology	Air	Rail, Road, Water

Case study – Total Airport Security System (TASS)

Total Airport Security System (TASS) is a multi-segment, multi-level intelligence and surveillance system aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on integrating distinct types of selected real-time sensors & amp; sub-systems for data collection in various modes, including fixed and mobile, all suitable for operation under environmental conditions.

TASS divides airport security into six security control segments: environmental, cargo, people, aeroplanes, vehicle-fleet & amp, and facilities. Each of them is monitored by various joined technologies, creating a multisource labyrinth fusion logic enabling situational and security awareness of the airport anytime and anywhere.

These joined control segments will be accessed through the TASS WEB-based portal by running a suite of applications that centralise the airport security control to all airport authorities.



Technology/measure applicable to transport mode:

Technology/measure possibly applicable to transport mode:

Figure 2.4 – Technological transferring between modes of transport (4)

Opportunities and benefits from development and implementation:

TASS is a promising technology combining different audio and video scenario recognition. A pre-modelling social interaction scenario within transport vehicles and pre-defined disruptive events (individual or group misconduct events and pre-recognition of criminals), combined with real-time recording, could be helpful to improve the protection of vehicles and passengers from anti-social behaviour.

Barriers to development or implementation:

The main barriers are:

- Technological: mainly due to modelling as the pre-classification framework, which must be adapted to different transport scenarios and operating conditions;
- Environmental: due to lighting conditions, both natural and artificial inside transport vehicles;
- Economic: due to the high technology used and time spent;
- Social: due to unknown conditions regarding the public acceptance of the technology (the existence of the system inside the vehicles can bring constraints).

3 | Stakeholders Workshop #1 – Security

3.1 Methods and materials

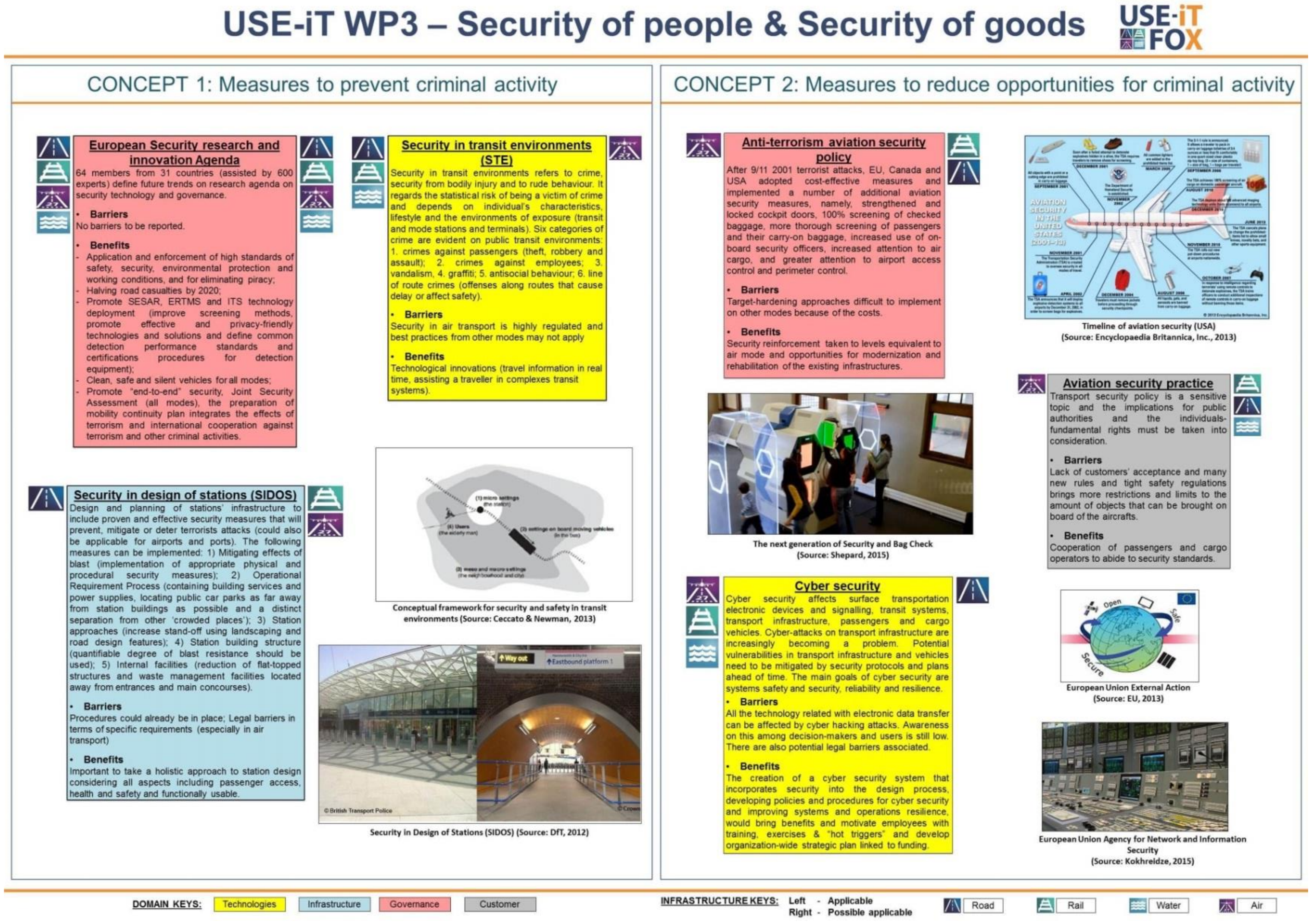
This chapter presents the results obtained through the one-day Workshop #1 with the project's stakeholders. The workshop was conducted on the 21st of January 2016, in Brussels (Belgium), using the "world round café" collaborative technique. Before the discussion, security team leaders presented the selected concepts, technologies, methodologies, and approaches in all four main security areas: measures to reduce criminal activity, opportunities for criminal activity, transportation safekeeping and surveillance. Posters presented the information in a single, simple, and efficient format. Each work package facilitated the discussion by producing posters displaying the most relevant methodologies/approaches/technologies.

USE-iT WP3 produced four posters – two for safety and two for security (Figures 3.1 and 3.2). Each poster covered two concepts and described, in the form of small boxes, the identified technologies/methods/approaches, as well as their main barriers and opportunities for cross-modally application. Each box was colour coded and indicated the domain to which it pertained, and the attached icons indicated the original transport mode and to what modes it could be applied. The posters were presented and described in detail by the facilitator.

After the analysis of the posters' content by the stakeholders, the discussion was initiated. Three questions oriented the discussion, namely:

1) Do you agree with the concepts and technologies on safety and security we have put forward?
2) What are the main barriers and opportunities for implementing the technologies/approaches from one mode to another?
3) What other technologies/methods could be included in this assessment?

Approximately 20 external stakeholders covering all transport modes attended the workshop, including industry, Research & Development community, and government agency representatives. After the presentation of USE-iT and FOX projects and the workshop's objectives, stakeholders were divided into groups of 4-6 persons each and rotated around each of the five "cafe tables". Each group spent approximately 30 minutes at each table before moving on to the next. Each "cafe" had a facilitator and a rapporteur to direct and record the discussions' most relevant points.



USE-iT WP3 – Security of people & Security of goods

CONCEPT 1: Measures to prevent criminal activity

European Security research and innovation Agenda

64 members from 31 countries (assisted by 600 experts) define future trends on research agenda on security technology and governance.

- **Barriers**

No barriers to be reported.

- **Benefits**

- Application and enforcement of high standards of safety, security, environmental protection and working conditions, and for eliminating piracy;
- Halving road casualties by 2020;
- Promote SESAR, ERTMS and ITS technology deployment (improve screening methods, promote effective and privacy-friendly technologies and solutions and define common detection performance standards and certifications procedures for detection equipment);
- Clean, safe and silent vehicles for all modes;
- Promote "end-to-end" security, Joint Security Assessment (all modes), the preparation of mobility continuity plan integrates the effects of terrorism and international cooperation against terrorism and other criminal activities.

Security in transit environments (STE)

Security in transit environments refers to crime, security from bodily injury and to rude behaviour. It regards the statistical risk of being a victim of crime and depends on individual's characteristics, lifestyle and the environments of exposure (transit and mode stations and terminals). Six categories of crime are evident on public transit environments: 1. crimes against passengers (theft, robbery and assault); 2. crimes against employees; 3. vandalism, 4. graffiti; 5. antisocial behaviour; 6. line of route crimes (offenses along routes that cause delay or affect safety).

- **Barriers**

Security in air transport is highly regulated and best practices from other modes may not apply

- **Benefits**

Technological innovations (travel information in real time, assisting a traveller in complexes transit systems).

Security in design of stations (SIDOS)

Design and planning of stations' infrastructure to include proven and effective security measures that will prevent, mitigate or deter terrorists attacks (could also be applicable for airports and ports). The following measures can be implemented: 1) Mitigating effects of blast (implementation of appropriate physical and procedural security measures); 2) Operational Requirement Process (containing building services and power supplies, locating public car parks as far away from station buildings as possible and a distinct separation from other 'crowded places'); 3) Station approaches (increase stand-off using landscaping and road design features); 4) Station building structure (quantifiable degree of blast resistance should be used); 5) Internal facilities (reduction of flat-topped structures and waste management facilities located away from entrances and main concourses).

- **Barriers**

Procedures could already be in place; Legal barriers in terms of specific requirements (especially in air transport)

- **Benefits**

Important to take a holistic approach to station design considering all aspects including passenger access, health and safety and functionally usable.

(1) micro settings
(the station)
(4) Users
(the elderly man)
(2) settings on board moving vehicles
(in the bus)
(3) meso and macro settings
(the neighbourhood and city)

Conceptual framework for security and safety in transit environments (Source: Ceccato & Newman, 2013)

Security in Design of Stations (SIDOS) (Source: DfT, 2012)

CONCEPT 2: Measures to reduce opportunities for criminal activity

Anti-terrorism aviation security policy

After 9/11 2001 terrorist attacks, EU, Canada and USA adopted cost-effective measures and implemented a number of additional aviation security measures, namely, strengthened and locked cockpit doors, 100% screening of checked baggage, more thorough screening of passengers and their carry-on baggage, increased use of on-board security officers, increased attention to air cargo, and greater attention to airport access control and perimeter control.

- **Barriers**

Target-hardening approaches difficult to implement on other modes because of the costs.

- **Benefits**

Security reinforcement taken to levels equivalent to air mode and opportunities for modernization and rehabilitation of the existing infrastructures.

AVIATION SECURITY IN THE UNITED STATES (2001–13)
© 2013 Encyclopaedia Britannica, Inc.

Timeline of aviation security (USA)
(Source: Encyclopaedia Britannica, Inc., 2013)

Aviation security practice

Transport security policy is a sensitive topic and the implications for public authorities and the individuals-fundamental rights must be taken into consideration.

- **Barriers**

Lack of customers' acceptance and many new rules and tight safety regulations brings more restrictions and limits to the amount of objects that can be brought on board of the aircrafts.

- **Benefits**

Cooperation of passengers and cargo operators to abide to security standards.

The next generation of Security and Bag Check
(Source: Shepard, 2015)

Cyber security

Cyber security affects surface transportation electronic devices and signalling, transit systems, transport infrastructure, passengers and cargo vehicles. Cyber-attacks on transport infrastructure are increasingly becoming a problem. Potential vulnerabilities in transport infrastructure and vehicles need to be mitigated by security protocols and plans ahead of time. The main goals of cyber security are systems safety and security, reliability and resilience.

- **Barriers**

All the technology related with electronic data transfer can be affected by cyber hacking attacks. Awareness on this among decision-makers and users is still low. There are also potential legal barriers associated.

- **Benefits**

The creation of a cyber security system that incorporates security into the design process, developing policies and procedures for cyber security and improving systems and operations resilience, would bring benefits and motivate employees with training, exercises & "hot triggers" and develop organization-wide strategic plan linked to funding.

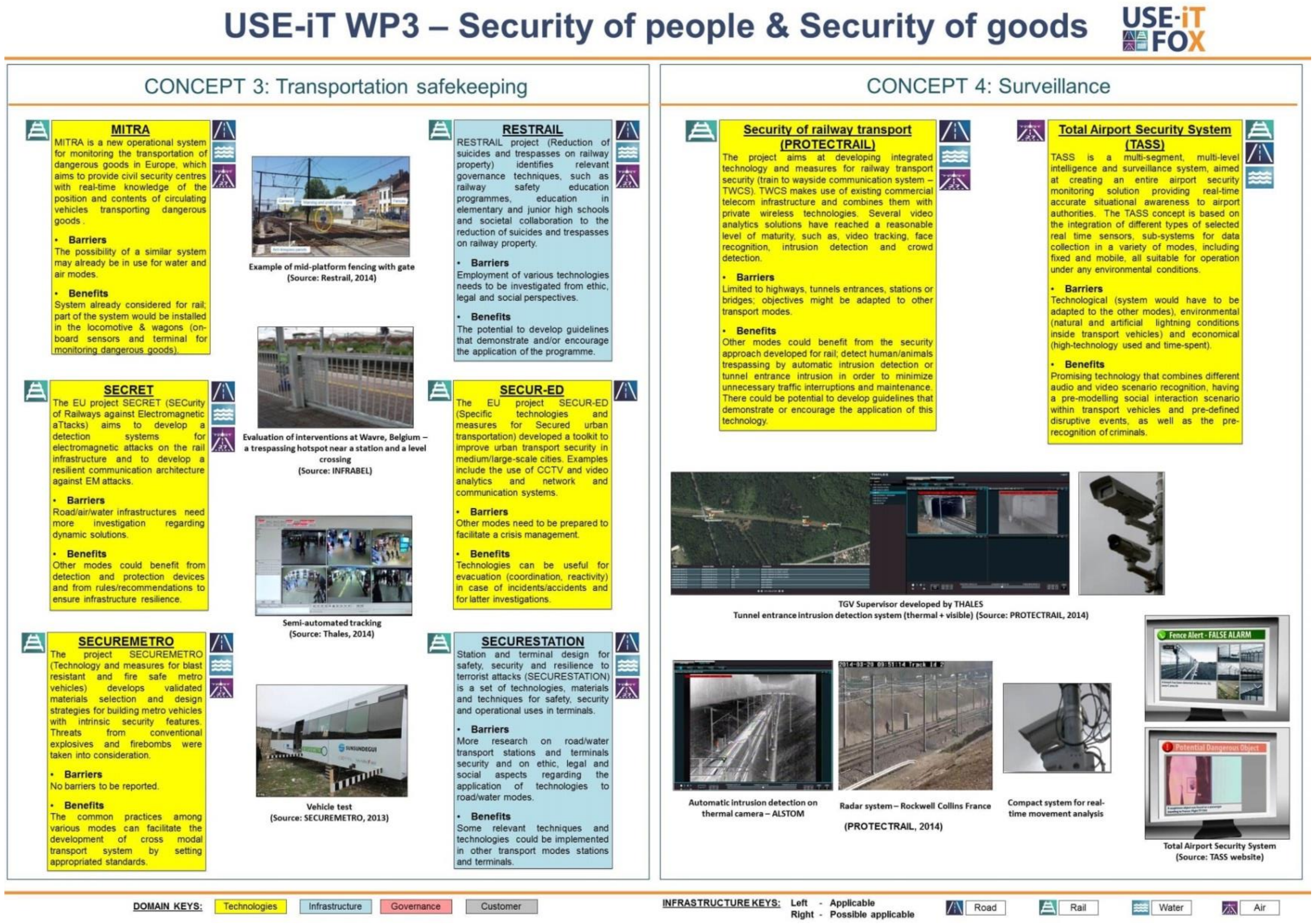
European Union External Action
(Source: EU, 2013)

European Union Agency for Network and Information Security
(Source: Kokhreidze, 2015)

DOMAIN KEYS: Technologies Infrastructure Governance Customer

INFRASTRUCTURE KEYS: Left - Applicable
Right - Possible applicable
Road Rail Water Air

Figure 3.1 – USE-iT WP3 Security Posters – 1st and 2nd Security concepts (Workshop #1)



USE-iT WP3 – Security of people & Security of goods

CONCEPT 3: Transportation safekeeping

MITRA

MITRA is a new operational system for monitoring the transportation of dangerous goods in Europe, which aims to provide civil security centres with real-time knowledge of the position and contents of circulating vehicles transporting dangerous goods .

- **Barriers**

The possibility of a similar system may already be in use for water and air modes.

- **Benefits**

System already considered for rail; part of the system would be installed in the locomotive & wagons (on-board sensors and terminal for monitoring dangerous goods).

Example of mid-platform fencing with gate
(Source: Restrail, 2014)

RESTRAIL

RESTRAIL project (Reduction of suicides and trespasses on railway property) identifies relevant governance techniques, such as railway safety education programmes, education in elementary and junior high schools and societal collaboration to the reduction of suicides and trespasses on railway property.

- **Barriers**

Employment of various technologies needs to be investigated from ethic, legal and social perspectives.

- **Benefits**

The potential to develop guidelines that demonstrate and/or encourage the application of the programme.

SECRET

The EU project SECRET (SECurity of Railways against Electromagnetic aTtacks) aims to develop a detection systems for electromagnetic attacks on the rail infrastructure and to develop a resilient communication architecture against EM attacks.

- **Barriers**

Road/air/water infrastructures need more investigation regarding dynamic solutions.

- **Benefits**

Other modes could benefit from detection and protection devices and from rules/recommendations to ensure infrastructure resilience.

Evaluation of interventions at Wavre, Belgium – a trespassing hotspot near a station and a level crossing
(Source: INFRABEL)

SECUR-ED

The EU project SECUR-ED (Specific technologies and measures for Secured urban transportation) developed a toolkit to improve urban transport security in medium/large-scale cities. Examples include the use of CCTV and video analytics and network and communication systems.

- **Barriers**

Other modes need to be prepared to facilitate a crisis management.

- **Benefits**

Technologies can be useful for evacuation (coordination, reactivity) in case of incidents/accidents and for latter investigations.

Semi-automated tracking
(Source: Thales, 2014)

SECUREMETRO

The project SECUREMETRO (Technology and measures for blast resistant and fire safe metro vehicles) develops validated materials selection and design strategies for building metro vehicles with intrinsic security features. Threats from conventional explosives and firebombs were taken into consideration.

- **Barriers**

No barriers to be reported.

- **Benefits**

The common practices among various modes can facilitate the development of cross modal transport system by setting appropriated standards.

Vehicle test
(Source: SECUREMETRO, 2013)

SECURESTATION

Station and terminal design for safety, security and resilience to terrorist attacks (SECURESTATION) is a set of technologies, materials and techniques for safety, security and operational uses in terminals.

- **Barriers**

More research on road/water transport stations and terminals security and on ethic, legal and social aspects regarding the application of technologies to road/water modes.

- **Benefits**

Some relevant techniques and technologies could be implemented in other transport modes stations and terminals.

CONCEPT 4: Surveillance

Security of railway transport (PROTECTRAIL)

The project aims at developing integrated technology and measures for railway transport security (train to wayside communication system – TWCS). TWCS makes use of existing commercial telecom infrastructure and combines them with private wireless technologies. Several video analytics solutions have reached a reasonable level of maturity, such as, video tracking, face recognition, intrusion detection and crowd detection.

- **Barriers**

Limited to highways, tunnels entrances, stations or bridges; objectives might be adapted to other transport modes.

- **Benefits**

Other modes could benefit from the security approach developed for rail; detect human/animals trespassing by automatic intrusion detection or tunnel entrance intrusion in order to minimize unnecessary traffic interruptions and maintenance. There could be potential to develop guidelines that demonstrate or encourage the application of this technology.

Total Airport Security System (TASS)

TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on the integration of different types of selected real time sensors, sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions.

- **Barriers**

Technological (system would have to be adapted to the other modes), environmental (natural and artificial lightning conditions inside transport vehicles) and economical (high-technology used and time-spent).

- **Benefits**

Promising technology that combines different audio and video scenario recognition, having a pre-modelling social interaction scenario within transport vehicles and pre-defined disruptive events, as well as the pre-recognition of criminals.

TGV Supervisor developed by THALES
Tunnel entrance intrusion detection system (thermal + visible) (Source: PROTECTRAIL, 2014)

Automatic intrusion detection on thermal camera – ALSTOM

Radar system – Rockwell Collins France

(PROTECTRAIL, 2014)

Compact system for real-time movement analysis

Total Airport Security System
(Source: TASS website)

DOMAIN KEYS: Technologies | Infrastructure | Governance | Customer

INFRASTRUCTURE KEYS: Left - Applicable
Right - Possible applicable
Road | Rail | Water | Air

Figure 3.2 – USE-iT WP3 Security Posters – 3rd and 4th Security concepts (Workshop #1)

3.2 Results of the Workshop #1

Analysis of the technologies/measures

Concepts 1 & 2 – Measures to prevent and reduce criminal activity

- Security by design was identified as an essential measure with the potential to be transferable to other modes (*e.g.,* design of airports);
- Anti-terrorism security practices (not policies) derived from aviation can be included in water transportation (*e.g.,* locked cockpit doors); these technologies can increase the feeling of security environments among users;
- Openness to data sharing should be embraced, especially sharing of data between various security agencies/security forces across transport modes;
- Cameras used on roads for traffic management could be helpful for security purposes; cameras in rest areas (*e.g.,* gas stations) are currently being used for security motives;
- Cybersecurity pointed to be relevant to the future of automation;
- More automation and innovative technologies must be developed to improve automatic security checks.

Concept 3 – Transportation Safekeeping

- The project SECRET (SECurity of Railways against Electromagnetic aTtacks) was identified as particularly applicable to the road mode;
- Remote explosive detection was identified with the potential to be applied to maritime mode;
- Potential technology: tracking of bags/valuable goods through GPS; general concerns regarding the social acceptance of this technology/measure.

Concept 4 – Surveillance

- Technologies/measures deriving from PROTECTRAIL (The Railway-Industry Partnership for Integrated Security of Rail Transport) project should be implemented to the entire length of the railway line and not limited to highways, tunnels entrances, stations, and bridges;
- Emergency evacuation concept should be included in Concept 4 – Surveillance.

Main barriers to technologies transferability

- Ethical, legal (data privacy, data purposes, and data management), and social/societal challenges (disruptive practices, privacy issues, and intrusive measures) were identified within the transferability to other modes (mainly on surveillance and aviation security technologies/ measures and practices);
- Costs identified as one of the significant barriers to technologies/measures transferability
- Cost-benefit analysis and social perception are critical factors towards the success of the implementation of technologies/measures in other modes;
- User acceptance must be taken into consideration for upcoming/transferable technologies;
- A balance should be achieved between increased security and user acceptance;

- More human resources should be allocated to air security procedures to decrease social annoyance.

Most promising security technologies and measures

Concepts 1 & 2 – Measures to prevent and reduce criminal activity

- The transferability of airport security technologies and practices (video recognition technologies, automatic luggage check) to other modes;
- Security by Design technologies and measures.

Concept 3 – Transportation Safekeeping

- Resilient communication architecture against EM attacks transferable to other modes (vd. SECRET project).

Concept 4 – Surveillance

- Mature video analytics solutions (*e.g.,* video tracking, face recognition, intrusion detection and crowd detection) transferable to other modes (*vd.* PROTECTRAIL project).

New technologies proposed by the stakeholders

- To include SecMan (Security Risk Management Processes for Road Infrastructures) project in the concept “Measures to prevent criminal activity”;
- To include CARONTE (Creating an Agenda for Research ON Transportation sEcurity) project in the concept “Measures to prevent criminal activity”.

Changes in previous concepts’ structure

- Merge Concept 1 (Measures to prevent criminal activity) and Concept 2 (Measures to reduce opportunities for criminal activity) into a new concept – “Measures to prevent and reduce criminal activity); include only the following areas: 1) Security in transit environments; 2) Design by security; 3) Cybersecurity; 4) Aviation security technologies and practices in the new concept;
- Merge “Anti-terrorism aviation security policy” and “Aviation security practice” templates.
- Relocate SECURESTATION project to Concept 1.

In-depth analysis of the identified technologies

- More detailed analysis of SECRET project (SECurity of Railways against Electromagnetic aTtacks).

Inclusion of new technologies

- Include SecMan project in the concept “measures to prevent criminal activity”;
- Include CARONTE project in concept “measures to prevent criminal activity”;
- Security by design concept to be investigated regarding other modes, namely airports;
- Include emergency evacuation concept in transportation safekeeping/surveillance concept;
- Investigate/include remote explosive detection in transportation safekeeping.

3.3 Scoring security technologies and measures

Following workshop #1, a selected list of technologies/methodologies and approaches were chosen as having the cross-modal potential to increase safety and security in all transport modes. This list of overall topics was then subjected to further rounds of feedback through discussions, face-to-face meetings, and telephone interviews to yield a short list of multi-modal research opportunities.

3.3.1 Initial prioritisation and scoring

Based on the results of workshop #1 and the feedback received from the security experts, the initial list of 14 topics was downsized to a list of 10 topics that were considered to have the most cross-modal potential. This list is presented above:

1) Measures to prevent and reduce criminal activity
    a. Cybersecurity;
    b. Aviation security technologies and practices;
    c. Security in transit environments;
    d. Security in design.
2) Transportation safekeeping
    a. Security of railways against electromagnetic attacks;
    b. Remote detection of explosives;
    c. Operational system for monitoring the transportation of dangerous goods;
    d. Technology and measures for blast resistant and fire safe metro vehicles (underground metro systems).
3) Surveillance
    a. Security of railway transport;
    b. Total airport security system.

A system for scoring the technologies under different criteria was developed and commonly used across USE-iT work packages to further consolidate the topics with the most potential in a consistent and transparent manner. The criteria used were the following:

A. Potential to increase safety and security

Criterion A is a high-level assessment of the potential of a technology/approach to increase safety or security. This addresses the main objective of the work package and therefore has been given a ×2 weight. This is a qualitative assessment by the assessor based on their view of the ability of a technology or approach to enhance safety or security, assuming it has been implemented successfully.

B. Transferability and potential for widespread use

Criterion B is an assessment of the potential for transferability of a technology/approach across modes and for its widespread use across different transport systems. In addition to transferability across modes, the criterion considered other factors, such as geographic location or other limits (*e.g.,* technologies to increase safety or security can only be installed in specific vehicles, or some methodologies can only be employed on certain types of transport users).

C. Efficiency

Criterion C is a high-level, qualitative assessment of the potential efficiency of a technology/approach in terms of the resources invested compared to the number of saved lives or reduced accidents/critical events. This should involve whole-life cycle approach; for example, the initial effort to implement a technology/methodology/approach may be high, but the potential long-term benefits may be even more important.

D. Ease of implementation

Criterion D assesses the ease of implementation for a technology/methodology/approach regarding barriers and enablers. Examples of potential barriers include conflicting legislation and user acceptance, and enablers could be supportive legislation or targets and existing funds or organisations to support implementation. The overall balance should be used if there are both barriers and enablers.

E. Co-benefits or dis-benefits

Criterion E assesses the additional benefits or dis-benefits over the long-term associated with a technology/approach/methodology. This assessment includes environmental factors such as noise, air quality or biodiversity and social factors such as safety, security, and impact on local communities. The overall balance should be used if there are both benefits and dis-benefits.

The guidelines for scoring each criterion are presented in Table 3.1.

Table 3.1 – USE-iT scoring guidelines

Scoring Criteria	1	2	3	4	5
A. Potential to increase safety/security	Negligible impact foreseen	Low potential	Medium potential	High potential	Very high potential
B. Transferability and potential for widespread use	Not transferable or very niche	Low transferability	Medium transferability	High transferability	Very high transferability and potential for widespread use
C. Efficiency	High effort/investment for little benefit	Low efficiency	Medium efficiency	High efficiency	Very high efficiency – very large benefit for little effort/investment
Scoring Criteria	**-2**	**-1**	**0**	**1**	**2**
D. Ease of implementation	Significant barriers to implementation	Barriers identified that could impact implementation	Neutral – No barriers or enablers/ Balance between barriers and enablers	Enablers identified that could improve ease of implementation	Significant enablers to implementation
E. Co-benefits or dis-benefits	Significant dis-benefits identified	Some dis-benefits identified	Neutral – No co-benefits or dis-benefits/positive and negative impacts balance	Some co-benefits identified	Significant co-benefits identified

Table 3.2 presents the initial scoring regarding security technologies and measures.

Table 3.2 – Security technologies and measures initial scoring

Technology/measure/approach		Domains	Transport mode in which it exists	Transport mode in which it could be applied	Potential [1 - 5]	Transferability [1 - 5]	Efficiency [1 - 5]	Ease to implement [-2 - 2]	Co-benefits [-2 - 2]	Emerging	Under development	Mature	SCORE	RATE (weighted)
Measures to prevent criminal activity	European Security Research and Innovation Agenda	Governance	Air Rail Road Water	---	3	3	3	1	1	0	0	1	14	9,8
	Security in transit environments	Technology Infrastructure	Rail, Road, Water	Air	5	4	3	1	2	0	0	1	20	14,0
	Security in design of stations (SIDOS)	Infrastructure	Road	Air Rail	5	4	3	1	2	0	0	1	20	14,0
Measures to reduce criminal activity	Anti-terrorism aviation security policy	Governance	Air	Rail Road Water	5	4	5	-1	2	0	1	0	20	16,0
	Aviation security practices	Governance Customer	Air	Rail Road Water	5	4	5	-1	2	0	1	0	20	16,0
	Cybersecurity	Infrastructure Technology	Air, Rail, Water	Road	5	4	4	1	2	0	1	0	21	16,8
Transportation safekeeping	Monitoring and intervention for the transportation of dangerous goods (MITRA)	Technology	Rail	Air Road Water	4	4	3	-1	1	0	1	0	15	12,0
	Reduction of Suicides and Trespasses on Railway property (RESTRAIL)	Infrastructure Governance	Rail	Air Road Water	5	2	2	-1	1	0	1	0	14	11,2
	Technology and measures for security of railways against electromagnetic attacks (SECRET)	Technology	Rail	Air Road Water	5	4	3	1	2	0	1	0	20	16,0
	Specific technologies and measures for Secured Urban Transportation (SECUR-ED)	Technology	Rail	Road	5	4	3	-1	1	0	1	0	17	13,6
	Technology and measures for blast resistant and fire safe metro vehicles (SECUREMETRO)	Technology Governance	Rail	Air Road Water	3	4	3	0	1	0	1	0	14	11,2
	Station and terminal design for safety, security and resilience to terrorist attack (SECURESTATION)	Technology Infrastructure	Rail	Air Road Water	5	5	3	1	2	0	0	1	21	14,7
Surveillance	Technology and measures for Integrated Security of Rail Transport (PROTECTRAIL)	Technology	Rail	Air Road Water	5	4	5	-1	2	0	1	0	20	16,0
	Total Airport Security System (TASS)	Technology	Air	Rail Road Water	5	4	5	-1	2	0	1	0	20	16,0

3.3.2 Final list of security technologies and measures

Table 3.3 presents the final scoring and listing on the USE-iT security technologies and measures.

Table 3.3 – Security technologies and measures final scoring

Technology/measure/ approach		Domains	Transport mode in which it exists	Transport mode in which it could be applied	Potential [1 - 5]	Transferability [1 - 5]	Efficiency [1 - 5]	Ease of implement [-2, - 2]	Co-benefits [-2 - 2]	Emerging	Under development	Mature	SCORE	RATE (weighted)
Measures to prevent and reduce criminal activity	Cyber security	Infrastructure Technology	Air Rail Water	Road	5	4	4	1	2	0	1	0	21	16,8
	Aviation security technologies and practices	Governance	Air	Rail Road Water	5	4	5	-1	2	0	1	0	20	16,0
	Security in transit environments	Technology Infrastructure	Rail Road Water	Air	5	4	3	1	2	0	0	1	20	14,0
	Security in design	Infrastructure	Road	Air Rail	5	4	3	1	2	0	0	1	20	14,0
Transportation safekeeping	Security of railways against electromagnetic attacks	Technology	Rail	Air Road Water	5	4	3	1	2	0	1	0	20	16,0
	Remote detection of explosives	Technology	Road	Water	5	4	4	1	1	0	1	0	20	16,0
	Operational system for monitoring the transportation of dangerous goods	Technology	Rail	Air Road Water	4	4	3	-1	1	0	1	0	15	12,0
	Technology & measures for blast resistant and fire safe metro vehicles	Technology Governance	Rail	Air Road Water	3	4	3	0	1	0	1	0	14	11,2
Surveillance	Security of railway transport	Technology	Rail	Air Road Water	5	4	5	-1	2	0	1	0	20	16,0
	Total Airport Security System	Technology	Air	Rail Road Water	5	4	5	-1	2	0	1	0	20	16,0

The final technologies and measures regarding the topic “measures to prevent and reduce criminal activity” were cybersecurity, aviation security technologies and practices, security in transit environments and security in designing infrastructures. Security of railways against electromagnetic attacks, remote detection of explosives, operational system for monitoring the transportation of dangerous goods and technology and measures for blast resistant and fire safe metro vehicles (underground ferrovial systems) received the higher rate scores in transportation safekeeping concept and security of railway transport, and Total Airport Security System obtained the higher rate scores in surveillance concept.

In order to stabilise the technologies and measures, a new round of consultations with key stakeholders took place after the scoring process. The results of the undertaken actions are presented in the next chapter.

4 | Interviews with experts on security

4.1 Structure of the interview to security experts

The next step in WP3 was to further consult key stakeholders to streamline the topics with the most cross-modal potential to increase safety and security measures technologies and approaches. Each consortium partner working in WP3 identified a list of relevant stakeholders, from different countries, transport modes and types of organisations with expertise in safety and security. After this list was stabilised, each stakeholder was contacted, and bi-lateral interviews were scheduled. The list of questions is presented below:

1) What new/innovative techniques/methodologies to increase security have been newly introduced in the organization in the last five years?
2) Do you think that these techniques/methodologies have the potential to be transferred to other transport modes?
3) If there are no innovative techniques to be reported, please let us know if any standards or procedures have been changed using the same techniques and technologies in the last five years.
4) Presentation of our list of topics and concepts, along with explanations; Ask for approval, additional comments, scoring/rating; What are the Top 3?
5) Are the topics relevant in their modes?
6) Are there any specific needs regarding research (knowledge gaps)? (Please specify how those knowledge gaps could be overcome).
7) Do you have past experience with cross-modal activities in your organization? Please specify.
8) What do you think are the common challenges to increase security across modes?
9) Have you been involved in any cross-modal activities in this area (security)? If yes, please elaborate or specify.
10) What opportunities do you think there are for cross-modal research in enhancing transport security?
11) Would your organization be interested in practical involvement in transferring best practices across modes? If yes, please elaborate.

4.2 Results of the interviews with security experts

The interviews were either by phone, email or face-to-face and included the range of questions presented above, including a prioritisation of the security topics, implementation issues, research gaps and cross-modal opportunities. For the security aspects of the WP3, twelve face-to-face interviews were conducted. Additionally, the input from the other seven stakeholders was considered and collected in a technical meeting (*i.e.*, HLEG “Airports of the future“– 25th June 2016). Figure 4.1 show a more detailed description of the involved stakeholders.

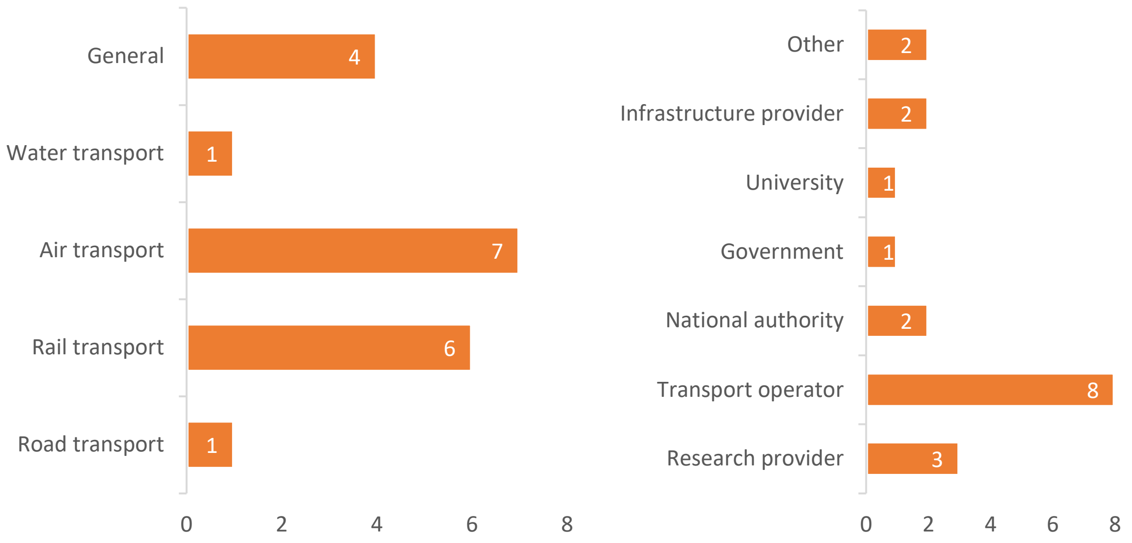


Figure 4.1 – Security-related stakeholders per transport mode and expertise/background

The interview topics on security included three main areas: general aspects of security, the USE-iT security concepts and topics and multi-modal involvement. The USE-iT concepts were specified in sub-topics, and a flyer (*vd.* Annex II) with more detailed information was presented to the interviewees before the interview began. A full version of the interviews is presented in Annex III.

Innovative techniques/methodologies to increase security adopted in the last five years

Most of the stakeholders from all modes stated the introduction of new/innovative techniques/ methodologies, such as:

- Electronic security has been the most sensitive area deriving from the use of critical infrastructure (bridge);
- Electronic surveillance systems and human surveillance;
- Combat fraud and vehicles vandalism by using system alarms associated with CCTV systems;
- Introduction of operating rules, including the work of the security forces before train circulation;
- Spring system implemented into a given terminal (technology explicitly developed for considering the existing space in the terminal); the installation of this system was made to ensure the damping in the event of a collision to ensure the safety of employees and passengers inside the vehicle;
- Close contacts with civil protection agents for action optimisation, emergency planning into operation and some safety procedures were updated;
- Creation of the department of security road-rail;
- Procedural changes in the administrative conduct of the criminal situation/criminal reporting;
- Identity double-checks (security and customs forces and onboarding) and the ones deriving from ICAO's annexe 17;
- Differentiated updates and training according to the access levels to the airport infrastructure;

- Special firewalls and software solutions against cyber-attacks;
- Video monitoring systems at railway stations and terminals;
- Regular training with security forces;
- Risk assessment based on 3D modelling of the area to be protected, using drone and photogrammetry;
- Near real-time standoff detection of explosives: wide area of surveillance capability at distances of about 30 m; remote, stand-alone system; non-contact;
- Short-wave infrared hyperspectral imaging by liquid crystal tuneable filter;
- LAG-screening technology included new SW and new processes;
- ETD-screening technology for different cross-checks for Pax and Handbag;
- Use of new generation of body scanners for Pax screening;
- New equipment (*e.g.,* evaluation of security scanners, multiplexed x-rays, ACBS);
- Implementation of a “security culture”;
- Innovation programme to develop airports partnerships (*e.g.,* “Vision Sûsete”);
- Crisis management based on quantitative indicators assessing systems resilience (*e.g.,* the ability to cope with disruptions/failures/faults, etc.) and the identification of systems' weaknesses and vulnerabilities;
- Research on cybersecurity to improve systems and operations resilience.

Potential of technologies/measures to be transferred to other modes

Most stakeholders recognise the potential of the selected technologies/measures to be transferred to other modes, somehow trying to contradict the idea and practice of seeking solutions exclusively anchored in a mode of transport, ignoring the interest and possibility of transferring certain solutions between modes of transport. Their comments included:

- Transferability of CCTV and thermal cameras (infrared) to water mode;
- Electronic security (cyber) to water and road modes;
- The spring system can be interesting in other modes since it is designed to absorb the energy of the vehicle's crash at the end of the line in a short journey; the existing models needed a larger space to absorb the necessary energy;
- Aviation security technologies are challenging to implement in other modes (high costs, research needs, service time constraints) but have the potential for maritime (long-distance cruises) and high-speed railway transport;
- Methodologies can be used for developing a 3D model of an airport, harbour, central bus depot, and railway station;
- Out of the aviation industry are demands in the transportation and logistics industry;
- More communication and consultation services between all transport modes for cross-modal implementation, as aviation security technologies and practices are very particular.

Standards or procedures have been changed using the same techniques and technologies since the last five years

Stakeholder responses included:

- Technology has evolved substantially in the last five years and has become more effective and valuable, but not necessarily friendlier or cheaper. The systems and security procedures were maintained to operate; much like the existing form, and “attention/vigilance” regarding security was strengthened;
- The situation could be described as follows: the rules did not dictate practices, and these were not justified because the degree of threat was null or negligible;
- Existing changes were in the procedures regarding the speed set on the line and the optimisation contacts/joint work with civil protection agents;
- Alarm systems with defined tasks for the staff;
- Training lessons with specialised content;
- Communication rules with security authorities and ambulance services;
- New equipment for processes and procedures in security are certified by different international regulations (ECAC, ICAO, FAA) and national regulations.

Scoring/rating, top 3 and additional comments on the security list of topics and concepts

All stakeholders agreed with the USE-iT WP3 Security presented topics. After compiling the results, the prioritisation of the topics is as follows:

- Cybersecurity (10 choices);
- Security by design (7 choices);
- Security of railway transportation (6 choices);
- Security in transit environments (3 choices);
- Total airport security system (3 choices);
- Remote detection of explosives (3 choices);
- Aviation security technologies and practices (2 choices);
- Operational system for monitoring the transportation of dangerous goods (1 choice).

The additional comments to this question included the following aspects:

- Security issues should be treated in a complementary and subsidiary way, attending the emerging threats;
- Resilience should be achieved with the use and implementation of various systems and crossing of different technologies and approaches;
- Threats are no longer linear since it requires reflecting on what are the threats and risks and what value of the property to protect, and think what is accurate;
- The more systems are functioning, the better, and the question is how to analyse large amounts of information; hence, the most important is to have an interface that aggregates all the

technologies and systems and displays the information in a more tailored way (*e.g.,* “alert“ displays);

- Securing a transport system (whatever the mode considered) must be understood globally, from access ports and traffic corridors to existing public furniture, and includes visibility from LEAs; the dialogue between LEAs and transport operators is critical;
- Security training is crucial and should be valued;
- The information/knowledge sharing management on the evolution of the security demands versus the evolution of security solutions regarding the various transport modes are relevant;
- The difficulty that organisations/companies have been having in addressing security results from the vulnerability/difficulty of managing the “unknown” or the “insufficiently known”; the current global context will bring short-term challenges in this field, and organisations/companies will have greater difficulty to overcome if this issue is not mitigated;
- The main challenge in the remote detection of explosives is the need to be done without disturbing the passengers;
- Radioactive material detection will be an emergent issue, and the airports will have to install it;
- Currently, radioactive material is being transported a lot, and the airport cargo staff is exposed to this material since there is no real-time detection;
- Passenger experience and acceptance are significant (*e.g.,* the concept of Smart Security Solutions);
- Need for the calculation of the probability of an event: the concept of Integrated Security based on the Onion Skin Principle is an important issue since one cannot provide 100% security at each ring; there is a need to be mindful regarding the objectives and purposes and what is crucial to protect; the main challenge is the calculation of the probability of an event; this could be more cost-effective for civil aviation;
- There is a challenge regarding the lack of communication between different agencies in a given and specific infrastructure; this implies a consequent challenge regarding responsibility procedures (*e.g.,* who does what in various critical situations).

Relevance of the presented security topics

Most stakeholders responded affirmatively to this question, although some topics were considered more relevant than others (CCTV- surveillance systems, cybersecurity, and security by design). Stakeholders made the following noteworthy comments:

- Lack of control of the objects carried by passengers; lost and found objects are a problem (given the frequency and the amount), and there are no rapid methods of analysis;
- Existing systems are too open and challenging to implement security measures;
- Safe areas in passenger traffic are a significant concern since these areas are not designed to consider threats, and there is no joint management between the various modes;
- Introduction of standard procedures towards more effective prevention and more effective control of occurrences.

Gaps in knowledge and how to overcome them

Stakeholders made the following comments and research gaps:

- Systems that can be scaled/customised to produce early warnings;
- Cybersecurity culture implementation is not achieved at the various decision-making levels;
- Nanotechnologies applied to security are underused;
- User willingness to pay (considering the transferability of air security technologies and procedures to rail mode);
- Data protection issues;
- New forms of crime (terrorism) and the information management process/knowledge on this topic;
- There are some shortcomings, such as the lack of communication between the various agents; a greater sharing of experience and know-how, allowing a more efficient joint action;
- Legislation should also follow the existing needs in security, which often does not permit an effective action;
- Necessary to contradict the idea that rail mode is safe for the practice of criminal acts; the presence of security forces (even though the constraints affect the service, *e.g.,* delay on trains) can increase objective security and the security perceptions among users;
- Inefficiency in communicating crime occurrences in transport modes;
- Lack of systematic procedures and rules for registry and data treatment since many security procedures are still “handmade”;
- Body and baggage scanning technologies.

Past experience with cross-modal activities

Eleven stakeholders indicated that they have previous experience with cross-modal activities and specified various activities, namely:

- Management of security in the implementation of various events, such as local festivals, marathons, and other operations where there is joint coordination of resources and procedures between the various transport modes, civil protection agents and municipal services;
- Partnerships at the level of emergency management, with standard emergency plans elaboration and simulation actions across various transport modes;
- Regular meetings and know-how transfer with road administration;
- Designing integrated bomb-explosion detection systems for critical infrastructures;
- Workshops on security in public transportation
- Potential collaboration with other modes for the use of explosive detection dogs (*e.g.,* railway);
- Video surveillance data treatment and systems resilience assessment on road and railway modes;
- Research activities in different transport modes.

Common challenges to increase security across modes

The respondents indicated the following common challenges to increase security across modes:

- Increase system resilience across different transport modes by using sets of available tools (technological and procedural);
- Increase effective technological monitoring;
- Specific training of the security forces to raise security in public transport;
- Extracurricular training on security regulations and procedures across different modes;
- Anti-terrorism preventive action;
- Collaborative work to define a standard security policy involving the public security forces and public and private operators;
- Introduction of CCTV in transport vehicles (mainly road and rail modes);
- Data disclosure;
- Shared information with other modes about the entry of problematic passengers in a given mode in order to improve response readiness;
- Recording crime data occurrences in different modes (statistics production and analysis);
- Background check of the candidates to staff in all modes;
- Adequate training;
- Delineation of security sensitive areas + CCTV introduction + control of accesses;
- Expanded list of prohibited articles (air mode);
- Regular checking of security equipment;
- Lack of interoperability between security system components used by different modes operators;
- Inadequate increase of security system against cyber-attacks;
- Technology development to allow early threat detection;
- Collaborative work between different stakeholders and authorities to share information and data, consultation for decision-making of best practices among stakeholders;
- Effective communication between companies, security forces and other administrations about threats;
- Balancing the security requirements with the privacy demands of passengers;
- Sufficient financial support for the implementation of security measures;
- Lack of awareness regarding radioactive material in rail cargo: the challenge is to develop a decision tool to calculate the probability assessment of a threat in rail stations/infrastructures;
- Increased use of virtual reality in training by creating a virtual reality of the target area that needs to be assessed: this measure would be cost-effective, as it would save monetary resources from performing real-live assessments of various infrastructures and could be applied to air, maritime and rail modes.

Stakeholder involvement in cross-modal activities regarding security

The following examples were provided:

- Security management in the implementation of specific events such as local festivals, marathons, and similar events;
- Collaborative work and joint coordination of resources and procedures between different modes, civil protection agents/agencies and municipal services;
- Partnerships and cooperation on emergency management, with standard emergency plans elaboration and simulation actions with different transport modes;
- Regular meetings and know-how transfer;
- Design of integrated bomb-explosion detection systems for critical infrastructures;
- Workshops on security in public transportation;
- Possibility of collaboration between modes for the use of explosive detection dogs (*e.g.,* rail);
- Video surveillance data treatment and systems resilience assessment on road and rail modes;
- Research activities in different transport modes.

Opportunities for cross-modal research in enhancing transport security

- There are exciting projects funded by the European Union (EU) in this area that were never implemented; it would be a good idea to start by listing those projects and try to understand what could be done with those that have potential in this area;
- Greater integration between the security forces and critical infrastructures operators;
- Aviation anti-terrorism procedures and technologies should be implemented in high-speed rail;
- Conventional solutions are harder to implement in urban and suburban rail transport because of the discomfort to the user, and the opportunity is to identify less intrusive measures of policing and surveillance;
- Digital footprint approaches are an essential way to trace criminal activity;
- Cooperation between public and private entities in combating urban criminal activity;
- The hubs of greater interoperability (with different modes) because they are more challenging to manage due to the high influx of users and the consequent impact on the operation;
- Implementation of security culture at the societal level using younger generations as modelling agents (*e.g.,* like what has been done regarding waste recycling);
- Improvement of the AVSEC for all modes, that is, appropriate regulation, adequate training of human resources and technology improvement;
- Better and secure communication between partners/players;
- Common training sessions for all modes;
- Combining the Standardized Onion-Skin (SOS) Principle, *e.g.,* multiple security layers with increasing security level towards the target area to be protected with the Vital Area Security (VAS) Concept;
- Opportunity of sharing best practices among stakeholders;

- Direct communication between all mode's companies (*e.g.*, technical engineers, decision-making entities), especially in crisis management;
- Opportunities for data and best practices exchange.

Organisation interest in practical involvement for transferring best practices across modes

Most stakeholders indicated that they would be interested in transferring best practices across modes, with the condition that the specific activity would have to be related to specific topics linked to their area of interest. Given examples include participation in expert groups, exchange of information through cooperation/partnerships between various stakeholders and society in general, participation in cross-modal projects regarding specific themes (*e.g.*, cybersecurity, surveillance systems, training methods), using existing technologies to create security systems for cross-modal transport components and developing work on security improvement (for road and railway systems).

The High-Level Experts Group (HLEG) highlighted the following:

- Cybersecurity was considered an exciting topic; on one side, the concept is evolving from an “equipment” oriented approach to a “system” oriented approach, including networking of various pieces of equipment, which opens new vulnerabilities to cyber-attacks.
- Aviation security technologies and practices: we are already totally convinced by this concept. It is crucial to consider practices and technologies since human factors, for instance, are very important. New technologies are an improvement only if operators and passengers use them correctly.
- Security in transit environments: this is more related to security in the public areas of the terminals, which are not really in the jurisdiction of the civil aviation authority in France. Matters of security in these areas are dealt with by the border police (PAF). Positions might change considering recent events.
- Security in design: it is a real challenge since it is difficult to forecast the evolution of technologies. For example, new technologies in carry-on luggage inspection led to longer lines which might not be accommodated in all facilities designed some years ago for other technologies.
- Remote detection of explosives: interesting; however, applicability for civil aviation requires reliable detection of small amounts of explosives in a short time.
- Operational system for monitoring the transportation of dangerous goods: this subject is increasingly attractive, especially after the recent incidents with lithium batteries.
- Technology and measures for blast-resistant and fire-safe metro vehicles: exciting research for blast-resistant aircraft or luggage containers is worth investigating.
- Security of railway transport: good intentions on paper.
- Total Airport Security System: same remark.

The summary of the stakeholder interviews in the security topic highlighted the following aspects:

- Common agreement with the final list of topics and respective ranking;

- Cybersecurity is a topic that was distinguished from all others and was much more assumed to be a societal challenge rather than a technological one, although the recognition of associated diffuse risks;
- A lack of security culture, transversal to all modes, was assumed;
- A solid cooperation between managers, engineers, technicians, operators, and law enforcement authorities, associated to better training, seems to be the key to a better understanding of the threats and more effective prevention of criminal activity;
- Remote detection of explosives was elected as one of the more central technologies in transportation safekeeping topic.

The most important topics in security are:

1) Cybersecurity (tools, policies, safeguards, guidelines to protect the cyber environment);
2) Security of railway transport (surveillance, Train to wayside communication system – TWCS);
3) Security by design (procedures in infrastructure conception & use);
4) Security in transit environments (stations, immediate vicinity & ‘en-route’ travel).

5 | Stakeholders Workshop # 2 – Security

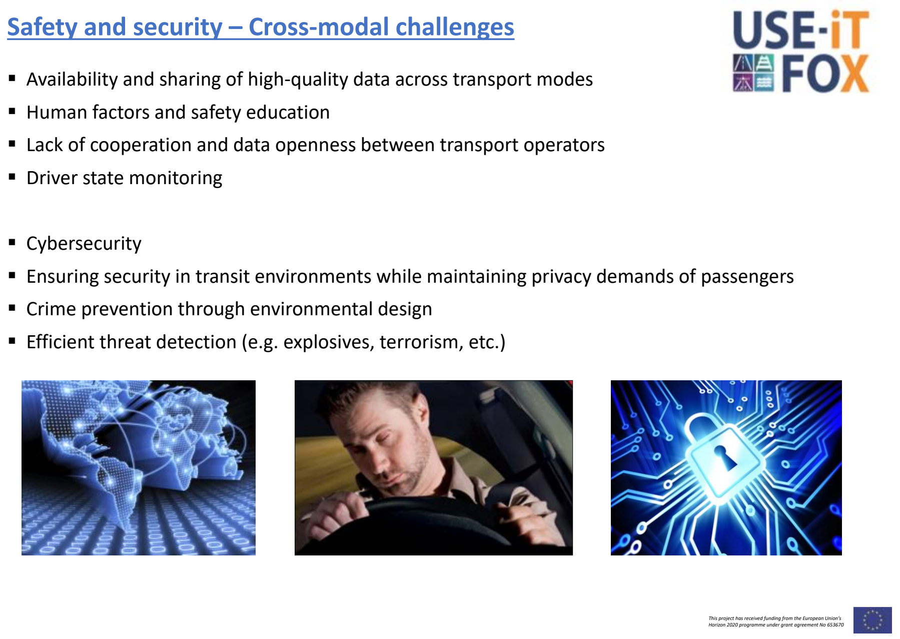
5.1 Methods and materials

This section presents the results obtained in Workshop #2 with stakeholders during a one-day session. The second USE-iT stakeholder workshop was held on 15th September 2016, included in USE-iT and FOX projects' three-day event (14 – 16 September 2016) at Diamond Centre in Brussels. Fifty international stakeholders participated across a range of national road authorities and industries. The objective of this workshop was to receive input/feedback from experts to identify the research areas which have the most potential in the development of the cross-modal application, or in other words, identifying the most promising opportunities, knowledge, and practices of all modes. This also includes identifying challenges and other possible research areas, proposed allocation of funding for each research area or challenge, and discussion of which research areas should be prioritised.

Ninety-minute parallel sessions comprise a short introduction about the WP and the poster by the moderator (5 min), followed by the experts' input and feedback about the challenges and research topics (30 min). After, a funding allocation exercise was conducted in which each stakeholder received ten dots and needed to determine which research areas should be prioritised. After this exercise, brainstorming about how to put research into practice (“From the implementation to the main goal”) was conducted with small groups of 2-3 people (30 min). The workshop ended with a wrap-up of the session (10 min).

The workshop preparation involved producing several materials, namely, posters (*vd.* Figures 5.1 and 5.2), handouts (*vd.* Annex IV) and identifying the discussion topics to be addressed during the planned brainstorming exercise. The main questions for discussion were:

1) What needs to happen for these technologies/approaches to be implemented?
2) What are the gaps in knowledge?
3) How can different transport modes work together?
4) What are the common research topics for more than two transport modes?



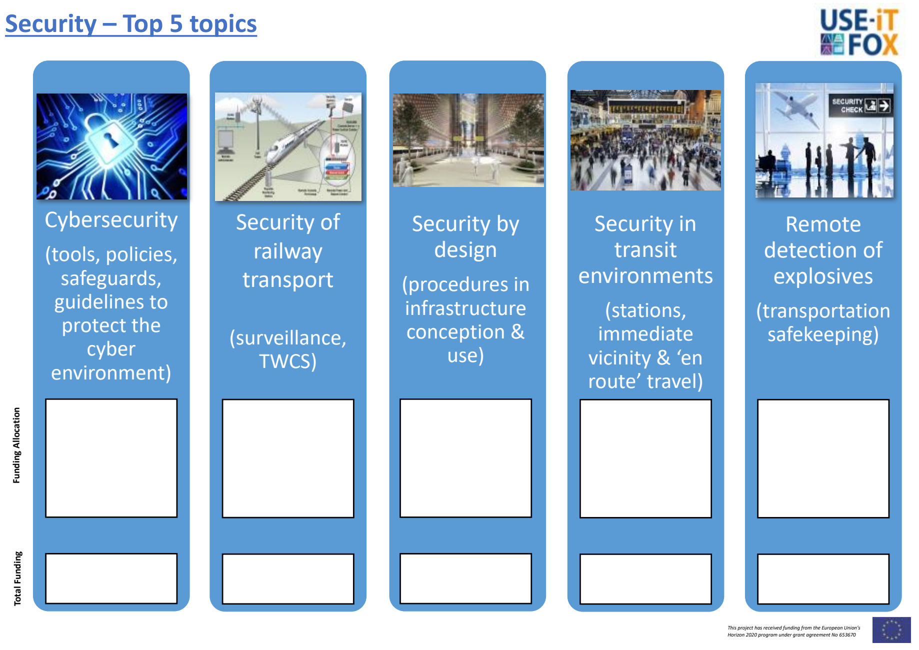
Safety and security – Cross-modal challenges

- Availability and sharing of high-quality data across transport modes
- Human factors and safety education
- Lack of cooperation and data openness between transport operators
- Driver state monitoring

- Cybersecurity
- Ensuring security in transit environments while maintaining privacy demands of passengers
- Crime prevention through environmental design
- Efficient threat detection (e.g. explosives, terrorism, etc.)

This project has received funding from the European Union's Horizon 2020 programme under grant agreement No 653670

Figure 5.1 – USE-iT WP3 2nd Stakeholders Workshop Poster with cross-modal challenges



Security – Top 5 topics

	Cybersecurity (tools, policies, safeguards, guidelines to protect the cyber environment)	Security of railway transport (surveillance, TWCS)	Security by design (procedures in infrastructure conception & use)	Security in transit environments (stations, immediate vicinity & 'en route' travel)	Remote detection of explosives (transportation safekeeping)
Funding Allocation					
Total Funding					

This project has received funding from the European Union's Horizon 2020 program under grant agreement No 653670

Figure 5.2 – USE-iT WP3 2nd Stakeholders Workshop Poster – Security

5.2 Results of the Workshop #2

All the participants (10 in total; 3 were external stakeholders) were security experts, and the discussions were lively (although strong and contradictory arguments ensued, results were still guaranteed). For some concepts, the meaning and actual scope were discussed in detail. Several implications of using some of the concepts selected (from the list of five) should be discussed and incorporated into the final list.

The final rating results, obtained through the funding allocation task were (with a similar result to the second, third and fourth positions):

1) Security by design (8 votes);
2) Security in transit environments (7 votes);
3) Remote control of explosives (7 votes);
4) Cybersecurity (7 votes).

The more critical aspects of putting research into practice procedure are:

- Cybersecurity is a fundamental cross-modal issue in its nature;
- Security by design is in the early stages of a complex process to provide security, which belongs to the construction of infrastructure; real-world testing is needed;
- There was not a consensus about the scope of remote detection of explosives (transportation safekeeping); some would call it remote detection of threats (automated image-processing is already done, even high-resolution videos are used); include social aspects, physical characteristics, and education;
- Insurance policies, risk analyses, liability and ownership are critical points to the implementation;
- Reinforcement of collaborations (regulatory); lack of communication cooperation.

As an example, a question was asked about what needs to happen for "cybersecurity" to be implemented". It was noted that this is dependent on areas such as:

- Allocation of responsibilities (legal aspects, ownership);
- Insurance policies;
- Liability degree;
- Reinforcement of collaboration/cooperation among stakeholders;
- Overcome the lack of communication among stakeholders.

It was also acknowledged that the research's desired outcome and the organisations involved should include society (in general), law enforcement agencies, regulators, and technology providers. This information was then intended for discussion towards research into further phases of the project (*e.g.,* implementation of this information and development of the roadmaps).

6 | Common security research challenges and opportunities

The three phases of stakeholder consultations yielded a final list of common challenges and research opportunities with the highest cross-modal potential for enhancing security. Similarly, to the safety topics, they are predominantly from the technology and infrastructure domains; however, the governance and user issues are even more relevant for the transport security challenges.

The security topics are described in terms of benefits, challenges, and steps to implementation, with an estimative timescale being provided.

6.1 Challenge #1 – Crime prevention through environmental design

Security by design refers to the structure or its form and the planning of transport infrastructures and includes proven and adequate security measures to prevent, mitigate or deter threats.

These measures include the implementation of appropriate physical secure stations/terminals against bomb blast, chemical, biological, radiological, and nuclear (CBRN) attacks involving particle dispersion and fire events; security procedures (screening, materials detection, intrusion detection systems, and tracking applications) should be considered at all stages of transport infrastructures development.

The containment of building services and power supplies, locating public car parks as far away as possible from station buildings, and creating a distinct separation from other “crowded places” are secure by design measures.

Benefits for cross-modal implementation

- High relevance for cross-modality since it applies to all transport modes;
- Should be applied at an early stage of infrastructure design and development and not be considered as an extra concern that could be later addressed
- Should be applied to obviate high costs of facilities adaptation/renovation;
- Design is the initial step of a complex process of providing security, which starts with a concept and finishes with the production of an infrastructure;
- Transport system enhancement must be understood globally, from access ports, and traffic corridors to existing public furniture and the visibility to law enforcement authorities.

Challenges for cross-modal implementation

- Difficulties to forecast the evolution of security technologies (*e.g.,* new technologies on carry-on luggage inspection led to longer lines which might not be accommodated in older facilities);
- Existing transport infrastructures are not prepared for the installation of new technologies and need to be adapted (*e.g.,* new x-ray machines that, due to their weight, cannot be incorporated in most airports);
- Safe areas in passenger traffic are not designed to consider security;

- Complex joint management between the various transport modes; the dialogue between law enforcement authorities, emergency management services and transport operators is critical.

Steps to implementation

- Development of guidelines/strategies;
- Building information modelling and design simulation tools;
- Risk assessment to identify the most important physical and non-physical vulnerabilities;
- Research production regarding best practices and needs for security by design methods for building infrastructure;
- Security by design should be extended to include ICT security by design (*e.g.,* the design of ICT systems where security is embedded) (Burbiel, Grigoleit, & Kochsiek, 2016; Burbiel, Grigoleit & Ghazel, 2016).

Implementation timescale

- Short-term (2-5 years) and mid-term (5-10 years).

6.2 Challenge #2 – Cybersecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

Cybersecurity affects surface transportation, electronic devices and signalling, transit systems, transport infrastructure, passengers and cargo vehicles. The potential vulnerabilities in transport infrastructure and vehicles need to be mitigated by security protocols and plans ahead of time. It is necessary to understand critical systems, interdependencies and the importance of cyber-physical control systems, traffic control and operations management systems, safety management systems, and traveller and operator services (112, e-commerce, e-payment).

Creating a cybersecurity system that incorporates security into the design process, developing policies and procedures for cybersecurity and improving systems and operations' resilience would bring benefits and motivate users with training, exercises & "hot triggers".

Benefits for cross-modal implementation

- Cybersecurity is a highly cross-modal topic in its nature;
- Improve prevention, detection, and fast reaction in the event of cyber-attacks or cyber disruption, promoting cyber resilience (Burbiel, Grigoleit, & Kochsiek, 2016; Burbiel, Grigoleit & Ghazel, 2016);
- Implies knowledge transfer frameworks;
- Implies regulation of standards;
- Adoption of minimum standards of cyber technologies.

Challenges for cross-modal implementation

- Difficulties with cyber threat detection (*i.e.*, regarding nature, severity, type of attack);
- Capability of ICT systems being resilient to cyber-attacks;
- Ability to operate transportation systems in the case of IT failure (Burbiel, Grigoleit, & Kochsiek, 2016; Burbiel, Grigoleit & Ghazel, 2016);
- Evolving from an “equipment” oriented approach to a “system” oriented approach, including networking of various pieces of equipment, which opens new vulnerabilities to cyber-attacks;
- Increase social awareness regarding cyber threats as a societal challenge and not an IT one;
- Develop appropriate safety measures and seamless cybersecurity applications to transport sensitive data on a local and international scale: BIM data, TMC control of traffic signals, operation of multimodal transport platforms, etc.

Steps to implementation

- Development of security plans, operation centres and anticipatory cybersecurity governance models;
- Development of national and international cyber defence;
- Build-up of competencies for doing cybersecurity;
- Allocation of responsibilities (legal aspects);
- Reinforcement of collaboration between stakeholders to establish best tackling procedures (*e.g.,* procedures for exchanging threat information) and regulatory aspects;
- Early detection and rapid response for targeted cyber-attacks;
- More research on cybersecurity (i.e., identify potential threats; protection solutions; assess systems resilience; publish and share mature research results);
- Provide control and supervision mechanisms for a continuous cyber risk assessment;
- Promote cyber intelligence communities towards a solid level of cyber resilience (Kerkdijk & Meijerink, 2015);
- Harmonize ICT systems between transport modes.

Implementation timescale

- Urgent (1-2 years).

6.3 Challenge #3 – Ensuring security in transit environments while maintaining privacy demands of passengers

Security in transit environments refers to the security of bus stops, stations, interchanges, the immediate vicinity of transport stops and stations and the ‘en-route’ travel (different onboard modes). Criminal acts in transit contexts result from the environment of the transport node itself (*e.g.,* design of platforms, CCTV, dark corners, poor lighting, hiding places) and the social interaction within those environments (*e.g.,* poor guardianship, crowdedness).

A multi- and interdisciplinary approach is required to tackle transit security and demands a more integrated, holistic, and cross-disciplinary approach. In addition, the identification and assessment of transport infrastructure vulnerabilities regarding man-made threats can contribute to the strengthening of the resilience of the European Transport Network against various man-made hazards. This could be done by providing infrastructure owners and operators with an easy-to-manage, practice-oriented tool for the assessment of the infrastructure.

Benefits for cross-modal implementation

- Approach is focused on the layout of the transit environment (infrastructure) and the users of the entire transport system;
- Responsibilities for minimizing transit risk can also be examined within this framework by assigning responsibility to those who police, manage, regulate, design, and maintain the transit settings;
- Extended security forces intervention and operation;
- Common level of security for all modes of transport;
- Security in transit settings tries to identify and mitigate security threats.

Challenges for cross-modal implementation

- Complexity of the system complicates transit environment analysis (*e.g.,* passenger density, offender proximity and familiarity with a setting/area; guardianship; design and management; user proximity, familiarity, and feelings of security; relative position within the network; type of security concern; time of day, day of week and season);
- Transit settings can potentially limit the potential positive influence of capable guardianship due to issues such as unfamiliarity or poor design;
- The dynamic and transient nature of the transportation system and the rapidly changing nature of its use makes it complex to understand;
- Interventions directed only at transit nodes have less chance of succeeding in reducing security concerns at transit stations than those which consider the nodes nearby other environments;
- Wide range of organizations with responsibilities for the security of the system (*e.g.,* at large multimodal interchanges) adds multi-ownership and management issues (*e.g.,* who does what in various critical situations);
- Risk assessment through behaviour pattern recognition/profiling;
- Ensuring security in transit environments while maintaining the privacy demands of passengers and avoiding disturbances;
- Make sure that all modes have the same information basis.

Steps to implementation

- Analysis of the movement of passengers at the stations to identify the best possible routes for guardians (Ceccato & Newton, 2015);
- Determine ridership patterns and exposure to potential targets; this changes as a function of the system growth (Ceccato & Newton, 2015);

- Demand for the cooperation of actors with responsibilities in the transportation system itself and those who deal with security issues in and around transportation modes;
- Improve the quality of joint collaborative work between actors involved in providing security;
- Develop a consistent and integrated threat detection approach for all modes of transport;
- Improve data sharing between modes and across nations;
- Implement security management systems.

Implementation timescale

- Urgent (1 year), short-term (2-5 years).

6.4 Challenge #4 – Remote detection of explosives and other materials

Recent developments in explosive remote detection are based on advanced optic technology. A laser system can precisely identify the atomic and molecular structure of the explosives, and the device can rapidly and remotely scan the steering wheel or the door of a vehicle (also applicable to luggage and opaque containers) and pick up trace residue. This technology was identified with the potential to be applied to maritime transportation.

Moreover, remote detection of other threats (*e.g.,* radioactive materials) should be considered. Remote detection of radioactive materials is an emergent critical issue since personnel working in airport cargo are exposed to this risky material (no real-time detection).

Benefits for cross-modal implementation

- Remote detection of threats is of high relevance for cross-modality;
- Highly inclusive across modes of transport since it is a transversal topic;
- Capability to detect explosives sensitively, accurately, and rapidly could have great benefit to national and international security;
- Rapid detection of materials in a non-invasive way can serve as an indicator for identifying attempts at concealed assembly or transport of explosive materials and devices (Wynn *et al.*, 2008).

Challenges for cross-modal implementation

- Need for urgent reliable, and affordable detection technologies that meet the specific requirements of land transportation;
- Gap between the need to identify threats and the technologies commercially available;
- Technologies and measures need to be implemented without passengers' disturbances;
- Need for high-resolution technologies in imaging and profiling;
- Applicability for civil aviation requires and depends on the reliable detection of small amounts of explosives in a short time;
- Urgent need for real-time detection of radio-active materials (since air mode staff is exposed to these materials);
- The need to be done without disturbing the passengers;

- Passenger experience and acceptance are significant (*e.g.,* the concept of Smart Security Solutions);
- New technologies and advances in technology are too expensive and not cost-efficient since the input of information to users implies specialized staff;
- Lack of control of the objects carried by passengers; lost and found objects are a problem (given the frequency and the amount), and there are no rapid analysis methods.

Steps to implementation

- Investment in social aspects since profiling is mainly based on psychical and demographic characteristics (*e.g.,* education);
- More reliable knowledge/research production;
- Research should cover multi-risk situations by aiming the combination of detection data (different substances and individual behaviour) and long-distance detection;
- False alarms must be reduced to a minimum;
- Increase the use of profiling and digital identification technologies as a means of threat detection.

Implementation timescale

- Short-term (2-5 years).

6.5 Conclusions

Transport and mobility represent the essential elements of any economy and society. Moreover, across all modes, global transport directly impacts the quality of life of people and their travelling. For this reason, ensuring and enhancing safe and secure transport across all modes is paramount.

During WP3 development, many technologies, methodologies, and approaches from all considered domains, with capabilities to improve transport safety and security, were identified and categorised in areas and concepts. In this phase, the results of multiple rounds of stakeholders' consultations on these technologies and approaches are summarised, resulting in a list of topics to address the cross-modal challenges related to security.

In this sense, the security-related cross-modal challenges are:

1) Cybersecurity;
2) Ensuring security in transit environments while maintaining the privacy demands of passengers;
3) Crime prevention through environmental design;
4) Remote detection of explosives and other materials.

Each identified challenge is addressed with a specific topic. The topics are predominantly from the infrastructure and technology domains; nevertheless, governance and user domains are intricately intertwined in all the topics, as regulation and user acceptance are two of the most important factors influencing the implementation of any technology or solution. The topics detailed described in this report emphases the benefits and challenges of cross-modal implementation, as well as identify the necessary steps towards implementation, and the implementation time scale.

The next step is to set common research themes across WP topics, transport modes and domains, which will serve as input to the roadmap for the implementation of the FORx4 initiative, incorporated into the final deliverable of the project (D5.4). The resulting roadmap represent an investment strategy for crucial infrastructure funders, including European, national, and regional public bodies and private infrastructure investors, to be used in specific developments.

Lisbon, LNEC, December 2022

APPROVED

The Head of the Acoustics, Lighting, Building Components and Facilities Unit

Jorge Patrício

The Head of the Urban and Territorial Studies Unit

João Branco Pedro

João Branco Pedro

The Director of the Buildings Department

Grandão Lopes

Jorge M. Grandão Lopes

AUTHORS

MargaridaRebelo

Margarida Rebelo
Assistant Researcher

Paulo Machado

Paulo Machado
Assistant Researcher

References

AIRPORTS COUNCIL INTERNATIONAL, 2012 – **Realizing Europe's vision for aviation Strategic Research & Innovation Agenda (Volumes 1 & 2)**. http://www.aci.aero/media/aci/file/aci_priorities/safety/aci_policies_and_recommended_practices_seventh_edition_5.pdf, Last accessed 2nd December 2015.

BURBIEL, Joachim; GRIGOLEIT, Sonja; GHAZEL, Mohamed, 2016 – **Creating an Agenda for Research On Transportation Security. Research Agenda for Security Issues in Land Transport (CARONTE)**. Deliverable D6.2.

BURBIEL, Joachim; GRIGOLEIT, Sonja; KOCHSIEK, Joachim, 2016 – **Assessment Of Existing And Possible Approaches And Solutions. Creating An Agenda For Research On Transportation Security (CARONTE)**. Deliverable D6.1.

CECCATO, Vania; NEWTON, Andrew, 2015 – **Safety and Security in Transit Environments**. London: Palgrave Macmillan. ISBN 9781137457653.

CRIME CONCERN, 2004 – **People's conceptions of personal security and their concerns about crime on public transport: research findings**. Department of Transport, London

CROWLEY, John, 2003 – Uses of Governance and Governmentality. **Critique Internationale, vol. 21, no. 4, pp. 52-61.**

DEPARTMENT FOR TRANSPORT (DfT), 2012 – **Security in Design of Stations (SIDOS) Guide**. London: British Government.

EUROPEAN COMMISSION, 2009 – **A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations**. Brussels, EC.

EUROPEAN COMMISSION, 2011 – **Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system**. Brussels, EC.

FARRINGTON, D. P., WELSH, B. C., 2010 – Preventing delinquency and later criminal offending. In J. M. Brown & E. A. Campbell (Eds.), **The Cambridge handbook of forensic psychology** (pp. 376–383). Cambridge University Press. https://doi.org/10.1017/CBO9780511730290.047.

HEDDEBAUT, Marc; SOUHEIR, Mili; SODOYER, David; JACOB, Eduardo; AGUADO, Marina; ZAMALLOA, Christian; LOPEZ, Igor; DENIAU, Virginie, 2014 – **Towards a resilient railway communication network against electromagnetic attacks**. 2014 Transport Research Arena Conference. DOI 10p. ffhal-01061258f.

KERKDIJK, Richard; MEIJERINK, Michael, 2015 – Ahead of the Threat - Enhancing Cyber Intelligence Communities. **European Cyber Security Perspectives**, pp. 44-48. https://www.thehaguesecuritydelta.com/media/com_hsd/report/34/document/European-Cyber-Security-Perspectives-2015.pdf, Last accessed 19th November 2015.

MTRS3, 2012 – **Compendium of technologies for designing safety and security (SECURESTATION).** Deliverable 3.2. URL: http://securestation.eu/documents/securestation_d2_3.pdf, Last accessed 19th November 2015.

NEWTON, Andrew, 2014 – Crime on Public Transport. **Encyclopedia of Criminology and Criminal Justice**, pp. 709–720. London: Springer.

PLANAS, Eulalia; PASTOR, Elsa; PRESUTTO, Franck; TIXIER, Jerome, 2008 – Results of the MITRA project: Monitoring and intervention for the transportation of dangerous goods. **Journal of Hazardous Goods, 152(2): 516-526**. DOI 10.1016/j.jhazmat.2007.07.032.

POOLE, Robert, 2008 – **Towards Risk Based Aviation Security Policy**. Organization for Economic Co-operation and Development (OECD), Discussion Paper Nr. 2008-23. https://www.itf-oecd.org/sites/default/files/docs/dp200823.pdf, Last accessed 19th November 2015.

PROTECTRAIL, 2014 – **High-speed track and tunnel experimentation with SNCF/RFF accessed**.http://www.protectrail.eu/IMG/pdf/01-prail_20140527_thales_villecresnes_demo.pdf, Last accessed 19th November 2015.

RESTRAIL PRACTICAL GUIDE, 2014 – **Reduction of Suicides and Trespasses on Railway Property - How to prevent suicide and trespass on the railways and mitigate the consequences?**. http://www.restrail.eu/IMG/pdf/restrail_book.pdf, Last accessed 19th November 2015.

SECRET PROJECT, 2015 – **Security of Railways against electromagnetic attacks**. http://www.secret-project.eu/, Last accessed 19th November 2015.

SECUREMETRO, 2012a – **WP3 - Design Solutions for Fire and Firebombs**. Deliverable D3.01 Critical inventory of technologies for firebomb mitigation. http://securemetro.inrets.fr/fileadmin/depository/PublicDocuments/WP3/D3.01%20-%20Final%20Version.pdf, Last accessed 19th November 2015.

SECUREMETRO, 2012b – **WP3 - Design Solutions for Fire and Firebombs**. Deliverable D3.02 Practical and Operational Implementation of Firebomb Mitigation Technologies. http://securemetro.inrets.fr/fileadmin/depository/PublicDocuments/WP3/D3.02%20Final%20Version.pdf, Last accessed 19th November 2015.

SEVENTH FRAMEWORK PROGRAM, 2012 – **Compendium of technologies for designing safety and security** Deliverable D2.3. http://securestation.eu/documents/securestation_d2_3.pdf, Last accessed 19th November 2015.

THALES, 2014 – SECUR-ED **Final Report. Secured Urban Transportation – European Demonstration**. Deliverable D01.11. http://www.secur-ed.eu/wp-content/uploads/2014/12/D01.11_SECUR-ED_Final_Report.pdf, Last accessed 19th November.

THE ENGINEER, 2012 – **Improved carriage design could reduce bomb-related injuries**. http://www.theengineer.co.uk/sectors/rail-and-marine/news/improved-carriage-design-could-reduce-bomb-related-injuries/1015305.article, Last accessed 19th November 2015.

VU, Van-Thinh; BREMOND, François; DAVINI, Gabriele; THONNAT, Monique; QUOC-CUONG, Pham; ALLEZARD, Nicolas; SAYD, Patrick; ROUAS, Jean-Luc; AMBELLOUIS, Sébastien; FLANCQUART, Amaury, 2006 – **Audio-video event recognition system for public**

transport security. Conference on Crime and Security. London: IET. DOI: 10.1049/ic:20060345.

WELSH, B.; FARRINGTON, D.; O'DELL, S., 2010 – **Effectiveness of Public Area Surveillance for Crime Prevention: Security Guards, Place Managers and Defensible Space**. Stockholm: Swedish National Council for Crime Prevention.

WYNN, Charles; EDWARDS, Brian; KUNZ, Rod; ZAYHOWSKI, John; PALMACCI, Stephen; ROTHSCHILD, Mardechai, 2008 – **Novel method for remotely detecting explosives**. SPIE Newsroom. DOI: 10.1117/2.1200805.1179.

WU, G. Y., JIAO, L., WANG, Y-F, CHANG, E. Y., 2003 – **Multi-camera Spatio-temporal Fusion and Biased Sequence-data Learning for Security Surveillance**. 11th ACM Int. Conf. on Multimedia, pp. 528-538.

ANNEXES

ANNEX I
List of technologies, measures, and best practices on the security of people and goods

1. SECURITY Concept – Measures to prevent criminal activity

1.1. European Security Research and Innovation Agenda

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		European Security Research and Innovation Agenda		
MODE		AIR, RAIL, ROAD, WATER		
MATURITY		New development, future initiatives, EU		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, RAIL, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/ POTENTIAL PROJECTS (IF KNOWN)		European Security Research and Innovation Agenda; European Security Research and Innovation Forum (ESRIF) – composed by 64 members from 31 countries (assisted by 600 experts) to define future trends on security research agenda (2009).		
PROVIDE INFO REGARDING:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	--------------------	--------------------	--------------------
	INFRASTRUCTURE	--------------------	--------------------	--------------------
	GOVERNANCE	Maritime: EU strives for the application and enforcement of high standards of safety, security, environmental protection and working conditions, and for eliminating piracy. Road: Halving road casualties by 2020. Make sure that the EU is a world leader in safety and security of transport in all modes. Promote SESAR, ERTMS and ITS technology deployment. • Promote improved screening methods • Promote effective and privacy-friendly technologies and solutions. • Define common detection performance standards and certifications procedures for detection equipment. • Clean, safe and silent vehicles for all modes. Promote land transport security by working with Member States on the security of land transport (permanent expert group on land transport security; focus on urban security). Promote “end-to-end” security. • Joint Security Assessment (all modes). • Preparation of mobility continuity plan integrates the effects of terrorism. • International cooperation in the fight against terrorism and other criminal activities.	--------------------	--------------------
	CUSTOMER	--------------------	--------------------	--------------------
Sources European Commission (2009). “A European Security Research and Innovation Agenda - Commission's initial position on ESRIF's key findings and recommendations”. Brussels, December 2009 European Commission (2011). White paper – “Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system”, Brussels, March 2011 www.caronte-project.eu/wp-content/uploads/2015/06/Mid_Term_Conference_V0.6-FINAL.ppt http://www.caronte-project.eu/wp-content/uploads/2014/10/Caronte-Newsletter-FINAL-March-2015.pdf				

1.2. Security in transit environments

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Security in transit environments		
MODE		RAIL, ROAD, WATER		
MATURITY		State-of-the-art		
CONCEPT POSSIBLY APPLICABLE TO:		AIR		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/ POTENTIAL PROJECTS (IF KNOWN)		Public transit systems security (transit environments); refers to crime, security from bodily injury and to rude behaviour. Six categories of crime evident on PTNS: 1. crimes against passengers (theft, robbery and assault); 2. crimes against employees; 3. vandalism, 4. graffiti; 5. antisocial behaviour; 6. line of route crimes (offenses along routes that cause delay or affect safety).		
PROVIDE INFO REGARDING:		STATUS OF DEVELOPMENT (reference to TRL) Security in transit environments concerns the statistical risk of being a victim of crime and is dependent on several factors regarding to an individual's characteristics and lifestyle and factors associated with the environments of exposure (bus stops, stations, and interchanges) and also on the move (subways, buses, trains).	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION Lack of consensus provided by the authors regarding the definition of transit crimes. Most adopt a simple definition of transit crime (TC), as crime within transit environments or settings. Research shows that crime is a result of two dimensions: the environment of the transport node itself (*e.g.,* design of platforms, CCTVs, dark corners, hiding places) and social interactions that take place in these environments (*e.g.,* poor guardianship, crowdedness) (Ceccato et al., 2013). Factors that may influence security: • Passenger density; • Offender proximity and familiarity with a setting/area; • Guardianship; • Design and management; • User proximity, familiarity, and feelings of security; • The relative position within the network; • Type of security concern; • Time of day, day of week and season.	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION Literature suggests that multi- or interdisciplinary approach is adequate to tackle transit security, as reality demands more integrated, holistic and cross-disciplinary research, particularly methods that are capable of guiding and dealing with an ever-increasing volume of space and time data.
DOMAINS	TECHNOLOGY	--------------------	--------------------	Increased role played by technological innovation n transit journeys - significant improvements in travel information in real time, assisting a traveller in complex transit systems but no guaranties that increased information reduces passengers' security concerns. As information becomes mobile, there are new opportunities for crime. Two theoretical framings: 1. Crime forecasting – security aspects should be included in the design phase of new product development, not added afterwards; 2. Exponentially growing cybercrime – the difference between cyber-enabled crime and cyber-dependent crime is that the first are traditional crimes which can be committed without the use of ICT but have become enhanced through the rapid exponential growth of ICT (*e.g.,* fraud) and the latter are crimes which can only be committed using ICT. This nomenclature could be adapted to transit security.
	INFRASTRUCTURE	Analysis of the uses and processes, as well as their status of development within the concept Transit settings and environments include transport hubs, the immediate vicinity of transport stops and stations (transport environs), and travel 'en route, onboard different modes of transport.	--------------------	--------------------
	GOVERNANCE	--------------------	--------------------	--------------------
	CUSTOMER	Analysis of the travel behaviour regarding the deployment of technologies or transport policies	--------------------	--------------------
Sources: Newton, A. (2014) Crime on Public Transport. Encyclopedia of Criminology and Criminal Justice. London: Springer, 709–720 Ceccato, V & Newton, A. (2015) (Eds.). Safety and Security in Transit Environments. London, Palgrave Macmillan.				

1.3. Security in design of stations (SIDOS)

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people and goods		
CONCEPT		Security in design of stations (SIDOS)		
MODE		ROAD		
MATURITY		The maturities of technology, infrastructure and governance measures discussed are a mixture of current practice and future opportunities.		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, RAIL		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Relevant to roads and rail stations		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	--------------------	--------------------	--------------------
	INFRASTRUCTURE	Security in design of stations (SIDOS): There is considerable scope in the design and planning of station infrastructure to include proven and effective security measures that will prevent, mitigate or deter attacks from terrorists. This could also be applicable for airports and ports. The following measures can be implemented: • Mitigating effects of blast – Implementation of appropriate physical and procedural security measures which should be 'designed in' at all stages of station development. • Operational Requirement Process – This includes containing (where possible) building services and power supplies, locating public car parks as far away from station buildings as practically possible and creating a distinct separation with other 'crowded places'. • Station approaches – Increase stand-off using landscaping and road design features such as traffic calming chicane measures, but also consider emergency vehicle access. • Station building structure – A quantifiable degree of blast resistance should be used. Any glazing should be Polyvinyl Butyral laminate. • Internal facilities – Reduction of flat-topped structures and waste management facilities located away from entrances and main concourses.	--------------------	Security in design of stations (SIDOS): Security is just one element in station design, and it is important to take a holistic approach considering all aspects including passenger access, health and safety and creating a place that is functionally usable.
	GOVERNANCE	--------------------	--------------------	--------------------
	CUSTOMER	--------------------	--------------------	--------------------
Sources Department for Transport (DfT) (2012). "Security in Design of Stations (SIDOS) Guide", British Transport Police and CPNI				

2. SECURITY Concept – Measures to reduce opportunities for criminal activity

2.1. Anti-terrorism Aviation security policy

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Anti-terrorism Aviation security policy		
MODE		AIR		
MATURITY		State-of-the-art		
CONCEPT POSSIBLY APPLICABLE TO:		RAIL, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Public transport Operators; Public transport, Closed infrastructure		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL) After 9/11 2001 terrorist attacks, EU, Canada and USA have adopted the cost-effective measures, implemented a number of additional aviation security measures, among them strengthened (and locked) cockpit doors, 100% screening of checked baggage, more thorough screening of passengers and their carry-on baggage, increased use of on-board security officers, increased attention to air cargo, and greater attention to airport access control and perimeter control.	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION Low risk assessment investment. Absence of a real benefit-cost analysis on security measures implementation.	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	New defensive technology systems “must be designed with terrorist counter-technology behaviours and past successes in mind”	--------------------	Security reinforcement to levels equivalent to air mode.
	INFRASTRUCTURE	--------------------	Strong necessity of adaptive measures (procedures to check the entry of passengers and baggage) and huge adaption works, highly expensive.	Opportunities for the modernization and rehabilitation of the existing infrastructure.
	GOVERNANCE	Difficulty of conducting overall benefit/cost analysis of anti-terrorist strategies; Ambiguity in who is responsible for security;	Target-hardening approaches, which have been placed at the air mode of transport, especially since 9/11, are much more difficult to implement on other transport modes, because of the costs.	Security reinforcement could be taken to levels equivalent to air mode.
	CUSTOMER	Less positive reaction from passengers considering protective measures too much intrusive;	Possible low acceptance to screening and other control procedures, namely by its time consuming and greater security guard presence in terminal lobby areas and outside the terminal.	Opportunities for modernization and rehabilitation of the existing infrastructures.
Sources: Poole, R.W. (2008) “Towards risk based aviation security policy”, Organization for Economic Co-operation and Development (OECD), Discussion Paper No. 2008-23, http://www.internationaltransportforum.org/jtrc/discussionpapers/DP200823.pdf, Last accessed 2nd December 2015				

2.2. Aviation security practices

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people and goods		
CONCEPT		Aviation security		
MODE		AIR		
MATURITY		Current practice, USA, EU		
CONCEPT POSSIBLY APPLICABLE TO:		RAIL, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Passenger and cargo airplanes, some of the security procedures especially for security of cargo can be transferrable to other modes (rail, road, water)		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	--------------------	--------------------	--------------------
	INFRASTRUCTURE	--------------------	--------------------	Since April 2011 the "One Stop Security" arrangement has in principle been extended to passengers originating from US airports with the potential to create an even wider area of passenger facilitation and security. Eliminating duplication within the EU and for flights from 3rd Countries with equivalent security standards is essential to stop the progress in security related costs while allowing Member States together with airlines and airports to better focus security measures to achieve further reductions in risk to civil aviation.
	GOVERNANCE	Currently EU rules for aviation security apply to outbound flights from the EU – the principle of 'Host State responsibility', as well as to all EU carriers. However, it may be appropriate to review this approach and consider whether it is desirable to also require as mandatory certain levels of security for all (or some) inbound flights into the EU. In any event, the EU should pursue the achievement of the necessary standards of security through robust rules adopted in the binding framework of ICAO and implemented based on a high performing universal audit programme. EU level baseline security standards would provide a common and adequate level of protection to rail transport to the benefit of businesses and passengers and would ensure consistency of approach across borders. This would avoid risks of duplication and incompatibility of rules associated with the implementation of local or national systems, thus in turn assisting the good functioning of the Single Market.	The Commission has started a process of consultation to examine proposals to make security controls more effective in more efficient ways. Together with Member States and stakeholders, it is looking into the use of technologies and methods for risk-based, differentiated, and unpredictable controls. The role and responsibility of the operators have also been examined. Specific risk-based security by aviation security agencies is already being applied for air cargo. A system of supply chain security allows faster treatment of cargo from trusted partners. The development of the AEO programme is one example of how to proceed: a system created to secure and facilitate the handling of cargo by customs also offers benefits as regards targeting security controls in both the aviation and maritime sectors.	There are considerable merits in continuing the work already commenced in the aviation and maritime sectors in developing specific measures on transport security at the EU level. The benefits could include: • A higher overall level of security for citizens in the EU • Lower levels of theft and other crimes – with consequential cost savings • Simplification for transport operators by having common security requirements – with consequential cost savings • Simplification for security providers – both equipment and personnel – by having common performance requirements and having a stronger voice in international forum
	CUSTOMER	Transport security policy is a sensitive topic, and full account must be taken of the implications it can have for public authorities as well as for the fundamental rights of the individual. Respecting the subsidiarity principle is particularly important.	Customer's acceptance (lack of it). A lot of new rules and tight safety regulations are aimed at increasing passenger and cargo safety, but on the same hand, bring more restrictions and limit the number of things that can be brought on board the planes.	Cooperation of passengers and cargo operators to abide by security standards.
Sources Airports Council International (ACI) (2012) "Realizing Europe's vision for aviation Strategic Research & Innovation Agenda Volume 1 and 2, ACARE", September 2012. http://www.aci.aero/media/aci/file/aci_priorities/safety/aci_policies_and_recommended_practices_seventh_edition_5.pdf, Last accessed 2nd December 2015				

2.3. Cybersecurity

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people + Security of goods		
CONCEPT		Cybersecurity		
MODE		AIR, RAIL, WATER		
MATURITY		State-of-the-art		
CONCEPT POSSIBLY APPLICABLE TO:		ROAD		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Surface transportation electronic devices such as: hacks on DMS, TMC and Signalling, Transit system, airports, airplanes, trains, tramways, passenger and cargo vessels.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	Cybersecurity is necessary for transportation mobility and safety. Cyber-attacks on transport infrastructure are nowadays becoming an increasing problem. Potential vulnerabilities in transport infrastructure and vehicles need to be mitigated by security protocols and plans ahead of time. Goals: systems safety, security, reliability and resilience	All the technology related with electronic data transfer can be affected by cyber hacking attacks. Technology such as electronic devices, software, hardware, and communications backbone (listed under infrastructure) is vulnerable and subject to cyber safety threats.	It is necessary to understand critical systems, interdependencies and importance of cyber physical control systems, traffic control and operations management systems, safety management systems, traveller and operator services such as 511, e-commerce, e-payment.
	INFRASTRUCTURE	Increasing dependence on digital infrastructure is observed in every mode of transport, in-vehicle devices are e-enabled, and their operating systems can be easily broken in if proper security procedures are not implemented. Communications infrastructure and channels include satellite, cellular, Wi-Fi, radio, DSCR, Blue Tooth &RF, Wireless sensors, CD &MP3,	Intermodal ports can be affected include the specific elements include: • Container terminal operations and management • Automated gates • Physical security (CCTV surveillance cameras) • Crane monitoring and control • Wireless devices and tracking Transit vehicles are e-enabled, some systems that can be affected include: Control domain: Vehicle Controls, Vehicle Diagnostics, Traffic Signal Priority, Video Surveillance Duress Alarms, Vehicle Immobilizers Operations domain: Automated Dispatching Vehicle Location, Route/Schedule Status Passenger Counters, Stop Annunciation Electronic Payments Infotainment Domain: Customer use of Wi-Fi and WiMAX Real-time Travel Info & Trip Planning Vehicles are also e-enabled, specific systems that can be affected include electrically assisted power steering, breaks, active suspension, fuel injection, etc.	Create a Cybersecurity ecosystem to (incorporate security into the design process, SMS's & the safety culture). • Identify systems, connections & interdependencies • Assess vulnerabilities and risks • Identify and use best practices and standards • Include Cybersecurity in design specs and acquisitions • Collaborate with IT, physical security & other groups • Develop policies and procedures for c • Motivate employees with training, exercises & "hot triggers" • Make sure that systems and operations are resilient (*i.e.*, layers, detection, incident response, COOP) • Develop an organisation-wide strategic plan linked to funding
	GOVERNANCE	Security needs to be built into the process to ensure the resilience of the overall system specific elements include: • Risk assessments • Standards • Design practices • Certification • Maintenance & Ops	--------------------	Understanding and risk mitigation requires collaboration (using best practices approach) of the following institutions/entities: • Designers & manufacturers • Equipment suppliers • System integrators • Expert consultants • University & government researchers • Testing organizations • Users: airlines, automobile users • Infrastructure operators • Standards organizations • Certifiers and regulators
	CUSTOMER	Customers need to be aware of cybersecurity threats: proper public outreach campaigns need to be conducted by the government and public safety organizations.	Customers can be affected via each of the 4 transport modes, but the most vulnerable is aviation. It is necessary to mention security in e-commerce applications frequently used by multimodal users.	Safety/security campaigns, culture and cooperation is important in understanding cybersecurity threats. Specific contingency plans should be available to public to provide procedures how to deal with potential cybersecurity issues and threats.
Sources EC Staff Working Document on Transport Security, Brussels 2012 ECTA, EPCA and CEFIC, (2003). "Guidelines for Transportation Security", http://www.ecta.com/media/1042/8_transportation_security.pdf, Last accessed 2nd December, 2015				

3. SECURITY Concept – Transportation safekeeping

3.1. Monitoring and intervention for the transportation of dangerous goods (MITRA)

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of goods		
CONCEPT		Monitoring and intervention for the transportation of dangerous goods (MITRA)		
MODE		RAIL		
MATURITY		--------------------		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Professional transport of dangerous goods; Motorway; Railway		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	A new operational system for monitoring the transportation of dangerous goods in Europe based on regional responsibilities. This concept, based on systems used in air traffic control, aims to provide civil security centres with real-time knowledge of the position and contents of dangerous vehicles circulating in their area of responsibility, and, in the event of a dangerous situation, to issue warnings, alerts and crisis management information, thereby allowing intervention teams to react immediately with maximum safety. This concept, derived from the air traffic control domain, provides civil security centres with the following: • The location of dangerous goods circulating in their area of responsibility: real-time knowledge of the position and contents of vehicles (electronic cargo identification) • Warning and alert display in the event of dangerous situations • The system can prevent accidents by allowing preventive measures to be taken • Crisis-management information that allows quicker, safer, and more efficient intervention, including precise knowledge of the situation and its potential consequences; this can protect the lives of both citizens and intervention forces	For water mode: It is possible that for Water and Air, a similar system may already be in place.	The system is already considered for rail. As an example, part of the system would be installed in the locomotive & wagons (on-board sensors and terminal for monitoring of the dangerous goods). To be investigated for water mode.
	INFRASTRUCTURE	MITRA's innovation is the integration of satellite navigation systems, telecommunications networks, geographic information systems, risk-knowledge databases and risk-propagation models in a single system. The MITRA prototype system relies on the following main components: • On-board terminal (OBT) • Communication server (CS) • Data exchange infrastructure (DEI) • User monitoring terminal (UMT) • Risk-knowledge platform (RKP)	--------------------	--------------------
	GOVERNANCE	--------------------	--------------------	--------------------
	CUSTOMER	This system can provide institutional authorities with the necessary tools to improve emergency response by providing knowledge of the characteristics of dangerous goods and of the associated risks and effects. More importantly, it will provide real-time expertise and support to decision-makers and emergency teams.	--------------------	--------------------
Sources Planas E., Pastor E., Presutto F., Tixier, J. (2008) "Results of the MITRA project: Monitoring and intervention for the transportation of dangerous goods", In Journal of Hazardous Goods, Vol. 152, Issue 2, 1st April 2008, Pages 516-526, in http://www.sciencedirect.com/science/article/pii/S0304389407010084, Last accessed 4th December 2015				

3.2. Reduction of suicides and trespasses on railway property

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Reduction of Suicides and Trespasses on RAILway property (RESTRAIL)		
MODE		RAIL		
MATURITY		Reduction of Suicides and Trespasses on RAILway property (RESTRAIL): identifying the various available prevention and mitigation measures and analysing their conditions for success in the rail environment – toolkit of the most relevant and cost-effective measures and recommendations at European level		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Rail and urban transport, Open infrastructure, Tunnel and stations.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	An evaluation of existing measures and recommendations for the reduction of suicides and trespasses on railway property identified the most relevant techniques (in terms of technology): • Warnings sings and posters • Video enforcement and sound warning • Forward Facing CCTV in trains	The possibility of employing these technologies (video and sound warning, forward facing CCTV) for road/water transport needs more investigation.	Road transport could benefit from the security approach developed for reduction of suicides and trespasses in railway properties
	INFRASTRUCTURE	Evaluation of existing measures and recommendations for the reduction of suicides and trespasses on railway property identified the most relevant techniques (in terms of infrastructure): • Mid-platform fencing • Gatekeeper programme • Gatekeeper programme • Computer based training	The other transportation modes' infrastructure needs more investigation (for *e.g.,* where these techniques can be implemented).	These infrastructures techniques could be relevant for the reduction of suicides and trespasses, especially on road transport.
	GOVERNANCE	Evaluation of existing measures and recommendations for the reduction of suicides and trespasses on railway property identified the most relevant techniques (in terms of governance): • Railway safety education programme • Education in schools for 8–11-year-old children • Societal collaboration to prevent railway suicide	The possibility of employing various technologies, from the ELSA (Ethic, legal and social aspects) point of view, needs to be investigated.	There could be potential to develop guidelines that demonstrate or encourage the application of this technology.
	CUSTOMER	Need to increase the perceived customer security using staff presence and new technology.	Needs of customer's collaboration with the staff during exercises or interventions and respect of information management system.	There could be potential to trained and educated customer for the security of persons.
Sources Restrail Practical Guide (2014): "Reduction if Suicides and Trepasses on RAILway property. Practical guide. How to prevent suicide and trespass on the railways and mitigate the consequences?". URL: http://www.restrail.eu/IMG/pdf/restrail_book.pdf , Last accessed 19th November 2015.				

3.3. Technology and measures for railway security against electromagnetic attacks

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Technology and measures for security of railways against electromagnetic attacks (SECRET)		
MODE		RAIL		
MATURITY		The European project SECRET (SECurity of Railways against Electromagnetic aTtacks) aims to assess the real risks concerning EM attacks on rail networks, to identify areas for strengthening and to develop a detection and management system for EM attacks that is integrated into the rail infrastructure, making it an architecture resilient to any EM attack.		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Rail transport, Open infrastructure, Tunnel and stations.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	SECRET addresses the protection of railway infrastructure against Electro-Magnetic attacks. The objective of SECRET; among others, is to develop detection systems for electromagnetic attacks on the rail infrastructure, as well as to develop a resilient communication architecture against EM attacks. Current ERTMS/ETCS (European Rail Traffic Management Systems) use the GSM-Rail communication platform and need a permanent communication path between the trackside and the train. Detection systems (employing dedicated sensors) allow for detection in real-time for EM attacks. A Multipath Communication System ensures that even if one or several paths fail, the communication needed for ERTMS is maintained.	--------------------	Road/air/water transports could benefit from the security approach technologies developed for railway infrastructure specially EM attack detection and protection devices and processes; and protection rules and recommendations to ensure infrastructure resiliency and potential contribution to standards.
	INFRASTRUCTURE	EM attack detection solutions.	The road/air/water infrastructure needs more investigation regarding dynamic solutions.	Potential to share the EM attack detection solutions.
	GOVERNANCE	IEC and ETSI standards need more collaboration for EMC purpose.	The possibility of employing various technologies, from the ELSA (Ethic, legal and social aspects) point of view needs to be investigated.	Potential to set common or to share the guidelines/standards
	CUSTOMER	--------------------	--------------------	--------------------
Sources Heddebaut, M., Souheir, M., Sodoyer, D., Jacob, E., Aguado, M., Zamalloa, C., Lopez, I., Deniau, V. (2014): “Towards a resilient railway communication network against electromagnetic attacks”. In Transport Research Arena Conference Proceedings. Paris. Secret Project (2015): “Security of Railways against electromagnetic attacks”. URL: http://www.secret-project.eu/, Last accessed 19th November 2015.				

3.4. Specific technologies and measures for secured urban transportation

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Specific technologies and measures for Secured Urban Transportation (SECUR-ED)		
MODE		RAIL		
MATURITY		SECUR-ED's rationale was to create a global European improvement in mass transportation security through the development of packaged modular solutions		
CONCEPT POSSIBLY APPLICABLE TO:		ROAD		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Urban transport, Open infrastructure, Tunnel and stations.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	The project provides a toolkit to improve urban transport security in medium to large-scale cities. Demonstration in four major urban European cities – Madrid, Paris, Milan and Berlin – using technologies and systems: • CCTV and video analytics are very interesting tools to improve security in public transport (intrusion, tracking, crowd assessment and face recognition) can help investigate incidents • Network and communications systems are crucial elements in security concepts. Reliable communication helps to enhance dilation and reactivity in case of accidents and incidents	The following items are identified for future development: • Crisis passenger information doctrine and additional uses of (passenger) mobile applications to support security and operations • Geolocation tools for underground infrastructures • Integrated and scalable training approach using simulations & mobile applications to train staff • "Safety and security together" (network shared, an infrastructure shared) Cybersecurity and cyber resilience in Public Transport.	Road/air/water transport could benefit from the security approach developed for public transport; these technologies can be useful for evacuation (coordination, reactivity) in case of incidents/accidents or latter for the investigations. Simulation is a relevant, reliable, and cost-effective approach to address design of complex systems.
	INFRASTRUCTURE	Rail infrastructure needs to be prepared to facilitate crisis management.	The others transport mode's infrastructure also needs to be prepared to facilitate crisis management.	Mature developed tools (*e.g.*, construction and air conditioning) are also applicable to assess resilience of infrastructures to security threats.
	GOVERNANCE	• Cybersecurity is a growing concern; the business process needs to be reviewed to identify the most relevant threats and countermeasures for implementation • Information management; tools to collect relevant information can help to make the best decision • Training is confirmed as the most effective security safeguards The following standardization activities have been identified as crucial to support accelerated growth and innovation in the Transportation sector: • Standard mapping format of underground and 3D infrastructures to be initiated through ISO Geographical groups • CCTV standards to be continued on IEC 62676 (TC79) and ISO 22311 (TC292), with a special focus on a dedicated public transport profile, metadata and interoperability with operators for crisis management • Contributions to the rail-on-board standards (IEC TC9) will continue, with contributions to IEC 62580-1 and IEC 62580-2 (onboard CCTV)	The possibility of employing various technologies, from the ELSA (Ethic, legal and social aspects) point of view, needs to be investigated. The identified standardization activities' contributions to road/air/water standards need to be investigated for their possible implementation.	There could be potential to develop guidelines that demonstrate or encourage the application of this technology. The guidelines and the standardization activities can accelerate innovation in the transportation sectors and facilitate the development of cross-modal transport systems.
	CUSTOMER	Need to increase customers' perceived security by using staff presence and new technology.	Needs more customer collaboration with the staff during exercises or interventions and respect for the information management system.	Potential to train and educate customers regarding the security of persons in other transport modes.
Sources Thales (2014): "SECUR-ED Final Report. Secured Urban Transportation – European Demonstration (SECUR-ED). Deliverable D01.11". URL: http://www.secur-ed.eu/wp-content/uploads/2014/12/D01.11_SECUR-ED_Final_Report.pdf , Last accessed 19th November. SECUR-ED Youtube Channel: [Several Videos containing information about SECUR-ED]. Retrieved from: https://www.youtube.com/channel/UCkgup8VreaTBtW8v_7hHe1A/videos, Last accessed 19th November 2015.				

3.5. Technology and measures for blast resistant and fire safe metro vehicles

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Technology and measures for blast resistant and fire safe metro vehicles (SECUREMETRO)		
MODE		RAIL		
MATURITY		The goal of this research project is to develop validated materials selection and design strategies for building metro vehicles with intrinsic security features. The Securemetro project will consider threats from conventional explosives and firebombs		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Rail transport, vehicle, Tunnel and network.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	The results of the Securemetro projects allowed improvements of the resilience of the metro vehicle, the passenger and staff in the following ways: • Improved resistance of the windows that cleanly separate from the body and do not shatter, thanks to the use of protective film and bonding; this results in the absence of broken glass flying towards the platform in case of blast in a station • Improved resistance of the ceiling panels and light/speaker/heavy elements using retaining cables to the main vehicle (primary) structure: the ceiling does not fall on the passengers and does not cover the ground which would make egress difficult and hazardous • Improved lights using LEDs, which have been showed to keep performing throughout the trial and after. This is an important point to improve the possibility to enter and egress the carriage, walk safely, assess the damages, and bring rescue • Recommendation to reinforce the driver's bulkhead • Use of flexible backing layer on certain key elements of the secondary structure to improve flexibility under blast loading	The results of Securemetro project suitability in term of the metro vehicle, the passenger and staff resilience and their adaptability/implementation need more investigation for Road/air/water transports.	The results of Securemetro project suitability in term of the metro vehicle, the passenger and staff resilience and their adaptability/implementation need more investigation for Road/air/water transports.
	INFRASTRUCTURE	--------------------	--------------------	--------------------
	GOVERNANCE	Possible improvements to the existing standards, deserving consideration for enclosure in the standards. No current standard exists to consider the emerging need to address the behaviour of metro vehicles facing a blast attack. The partners of the project therefore used existing standards applicable in other domains such as weaponry or found inspiration in the existing standards addressing different issues, notably crash worthiness [EN12663, EN15227, GM/RT1230]. The lack of existing common practice in the domain was particularly notable in two domains: appropriate test and measurement techniques, and design taking blast resilience into consideration.	The emerging needs identified in rail transport for standardization activities need to be investigated to evaluate their possible contributions to road/air/water transport standards or guidelines.	There could be potential to develop guidelines that demonstrate or encourage the application of this technology. The potential common practices in various transport domains can facilitate the development of cross-modal transport system by setting appropriate standards.
	CUSTOMER	Need to increase customers' perceived security by using staff presence and new technology.	Need more customers' collaboration with the staff during exercises or interventions and respect of information management system.	Potential to trained and to educated customer for the security of persons.

Sources
SECUREMETRO (2012b): "WP 3 – Design Solutions for Fire and Firebombs– DELIVERABLE: D3.02 Practical and Operational Implementation of Firebomb Mitigation Technologies". URL: http://securemetro.inrets.fr/fileadmin/depository/PublicDocuments/WP3/D3.02%20Final%20Version.pdf , Last accessed 19th November 2015.
SECUREMETRO (2012a): "WP 3 – Design Solutions for Fire and Firebombs– DELIVERABLE: D3.01 Critical inventory of technologies for firebomb mitigation". URL: http://securemetro.inrets.fr/fileadmin/depository/PublicDocuments/WP3/D3.01%20-%20Final%20Version.pdf, Last accessed 19th November 2015.
The Engineer (2012): "Improved carriage design could reduce bomb-related injuries". URL: http://www.theengineer.co.uk/sectors/rail-and-marine/news/improved-carriage-design-could-reduce-bomb-related-injuries/1015305.article, Last accessed 19th November 2015.
Images:
SECUREMETRO (2012b): "WP 3 – Design Solutions for Fire and Firebombs– DELIVERABLE: D3.02 Practical and Operational Implementation of Firebomb Mitigation Technologies". URL: http://securemetro.inrets.fr/fileadmin/depository/PublicDocuments/WP3/D3.02%20Final%20Version.pdf , Last accessed 19th November 2015.
The Engineer (2012): "Improved carriage design could reduce bomb-related injuries". URL: http://www.theengineer.co.uk/sectors/rail-and-marine/news/improved-carriage-design-could-reduce-bomb-related-injuries/1015305.article, Last accessed 19th November 2015.

3.6. Station and terminal design for safety, security and resilience to terrorist attacks

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Station and terminal design for safety, security and resilience to terrorist attack (SECURESTATION)		
MODE		RAIL		
MATURITY		--------------------		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Urban transport, Open infrastructure, Tunnel and stations.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	The focus of the SECURESTATION project is producing the necessary tools to build safer and more secure passenger stations/terminals against terrorist bomb blast, CBRN attacks involving particle dispersion, and fire events, whilst providing maximum operating resilience. A compendium of technologies, means, materials and engineering techniques for safety, security and operational uses in passenger terminals, which can be implemented as a basis for the development of the Constructive Design Handbook have been proposed: • CCTV and video analytics tools to improve security in public transport (intrusion, tracking, crowd assessment and face recognition) can help investigate incidents • Access control system (ACS) for help points, announcement facilities, signage, vehicle management, intrusion and materials detection, alarm systems • Smoke, flame and fire detection and protection systems (devices and control panels) • The use of matured tools: blast attack simulations, Fire Dynamic Simulator, Fire & smoke, and evacuation modelling Development of the risk management (assessment) in passenger terminal methodology: SEST-RAM – a set of Excel spreadsheets – from methodology to software-based tool.	The results of SECURESTATION project suitability and adaptability for implementation need more investigation, especially in term of the road/water transports passenger stations/terminals security against terrorist bomb blast and CBRN attacks regarding the four objectives.	The others transport modes could benefit from the security approach developed for public transport. Some relevant techniques/technologies could be implemented for the other transport stations/terminals as help points, alarms and announcement facilities, signage, access management controls, vehicle management, threat detection systems (screening, materials detection), Intrusion detection systems, tracking applications. Road transport could benefit from the security approach developed for public transport.
	INFRASTRUCTURE	The Design Guidelines for Railway Station Security provide guidance for the design or operation of stations and identify the security features and best practice which should be considered at each stage: Design Guidelines for Railway Station Security are broken down into three main items: • General Station Design Principles • Risk Identification and Mitigation • Design Guidelines for Station Security A passenger terminal design guidelines (handbook) describes: • Building automation and energy management systems: the need of backup power generation, emergency lighting and plumbing devices • Construction techniques and material to be used	The possibility of employing various technologies, from ELSA (Ethic, legal and social aspects) point of view needs to be investigated for the road/water transport.	Potential to share the guidelines, design principles and risk identification and mitigation process. The others transport modes stations/terminals could benefit from techniques like station furniture, access controls and barriers, indoor and outdoor systems, perimeter protection, fencing, walls, gates, equipment, people and vehicles design and implementation.
	GOVERNANCE	--------------------	--------------------	--------------------
	CUSTOMER	--------------------	--------------------	--------------------
Sources MTRS3 (2012): “D2.3 – Compendium of technologies for designing safety and security”. URL: http://securestation.eu/documents/securestation_d2_3.pdf, Last accessed 19th November 2015.				

4. SECURITY Concept – Surveillance

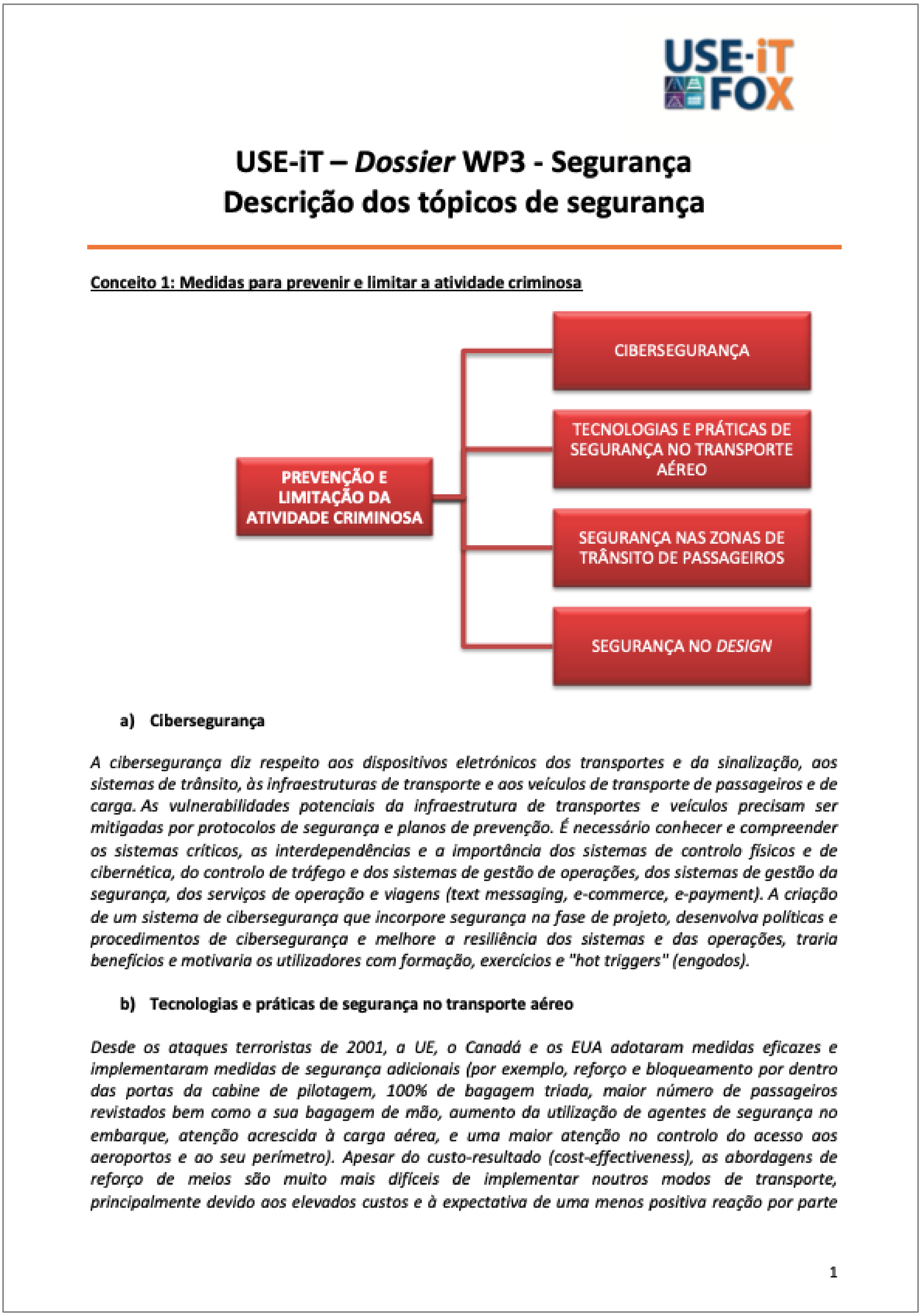
4.1. Technology and measures for Integrated Security of Rail Transport

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people		
CONCEPT		Technology and measures for Integrated Security of Rail Transport (PROTECTRAIL)		
MODE		RAIL		
MATURITY		--------------------		
CONCEPT POSSIBLY APPLICABLE TO:		AIR, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Rail transport, Open infrastructure, Tunnel and stations.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	Network communication. Train to wayside communication system (TWCS), form a crucial subsystem in delivering diversified railway security. This TWCS make use of existing commercial telecom infrastructure (*i.e.*, LTE, HSPA+, HSPA, etc) and optionally, it combines these networks with private wireless technologies (*i.e.*, 802.11 n Wi-Fi). Modern and practical approaches to video and video-based analytics. Several video analytics solutions have reached a reasonable level of maturity, such as video tracking, face recognition, intrusion detection and crowd detection.	Objective might be adapted and limited to highways, tunnels entrances, stations or bridges for the others transport modes.	Road/air/water transports could benefit from the security approach developed for rail transport: • Detect human/animals trespassing by automatic intrusion detection or tunnel entrance intrusion to minimize unnecessary traffic interruptions and maintenance
	INFRASTRUCTURE	--------------------	--------------------	--------------------
	GOVERNANCE	• Cybersecurity is of growing importance for the railway sector. The railway industry needs to establish security standards and best practices for information security management like the ISO 27000 series. In this context security technologies like VPN for secure collaboration in distributed locations and MPLS for high-performance routing in large networks and redundant network connections in case of a failure or an attack, virtual LANs for a secure segregation and guarantee a quality of service for safety related applications • Information management. Tools to collect relevant information can help to make the best decision • Training is confirmed as the most effective security safeguards	The possibility of employing various technologies, from ELSA (Ethic, legal and social aspects) point of view needs to be investigated.	There could be potential to develop guidelines that demonstrate or encourage the application of this technology.
	CUSTOMER	Need to increase costumers' perceived security by using staff presence and new technology.	--------------------	--------------------
Sources PROTECTRAIL (2014): "High speed track and tunnel experimentation with SNCF/RFF accessed". URL: http://www.protectrail.eu/IMG/pdf/01-prail_20140527_thales_villecresnes_demo.pdf, Last accessed 19th November 2015.				

4.2. Total Airport Security System

PROJECT		USE-IT		
WP TITLE		WP3 Safety and Security		
AREA		Security of people + Security of goods		
CONCEPT		Total Airport Security System (TASS) – a multi-segment, multi-level intelligence and surveillance system		
MODE		AIR		
MATURITY		New development, Future opportunities SAMSIT project – FP7 (2010-2014) SAMSIT (Système d'Analyse de Médias pour une Sécurité Intelligente dans les Transports publics) aims at developing an audio-video surveillance platform able to automatically recognize high level human behaviors involving individuals using both audio and video information.		
CONCEPT POSSIBLY APPLICABLE TO:		RAIL, ROAD, WATER		
SPECIFY LOCATION, TYPE, PLACEMENT LIST EXISTING/POTENTIAL PROJECTS (IF KNOWN)		Airports and other public transport infrastructure are large areas to be monitored. TASS (Total Airport Security System) is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on integrating different types of selected real time sensors &amp; sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions.		
PROVIDE INFORMATION REGARDING TO:		STATUS OF DEVELOPMENT (reference to TRL)	BARRIERS TO DEVELOPMENT OR IMPLEMENTATION	OPPORTUNITIES AND BENEFITS FROM DEVELOPMENT AND IMPLEMENTATION
DOMAINS	TECHNOLOGY	"TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities. The TASS concept is based on integrating different types of selected real time sensors &amp; sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions. TASS divides the airport security into six security control segments (environmental, cargo, people, airplanes, vehicle-fleet &amp; facilities) each of them being monitored by various technologies that are fused together, creating a multisource labyrinth fusion logic enabling situational and security awareness of the airport anytime and anywhere. These fused control segments will be accessed through the TASS WEB-based portal by running a suite of applications making the airport security control centralized to all airport authorities. Information will be shared and synchronized between all of them in order to generate a comprehensive, real time, security overview for the airport C2, providing all the necessary features to assure a total "no breach" security environment. The integration will include the use of in-place technologies that will result in a cost-effective solution.	• Technological, mainly due to modelling as pre-classification framework, which must be adapt to different transport scenarios and operating conditions. • Environmental, especially due to lightning conditions, both natural as artificial inside transport vehicles. • Economic, considering the high-technology used and time-spent	This is a very promising technology that combines different audio and video scenario recognition. The possibility of having a pre-modelling social interaction scenarios within transport vehicles, as well as pre-defined disruptive events (individual or group misconduct events), including pre-recognition of criminals, combined with recording just in time real situations could be useful to better protect vehicles and passengers from anti-social behaviour.
	INFRASTRUCTURE	--------------------	Adaptations have to be implemented within a scenario of migration from an infrastructure as an airport to another one, such a rail station or an urban public transport hub. Potential threats can also differ.	Direct and indirect contribution to a full understanding of real threats upon transport facilities.
	GOVERNANCE	Situational awareness allied with less time-consuming and reduced potential for human error	The integration of technology will include the use of in-place technologies that will result in a cost-effective solution, probably high for most of the transport infrastructures stakeholders and owners (public or private)	--------------------
	CUSTOMER	Diminishing nuisance alarm occurrences to ensure minimal effect on the passenger flow while providing a high degree of security, taking into consideration all potential threats. Friendly technology to end-users and customers. Expectedly, customers will felt an increased level of security knowing that there is a very sophisticated means of surveillance that protects the possibility of events that offend their safety.	Although the literature is silent as to customers' acceptance, the necessary identification of the existence of the system inside the vehicles can bring some constraints.	Smooth passengers flow. Increased real security. Higher feeling of security. In a situation of full exploitation of this combined technology, with the possibility of interoperability between different modes of transport, the transport system would be quite a shielded for use by individuals with antisocial and harmful behaviour and would greatly increase the feeling of insecurity among customers.
Sources Vu, V.-T., Bremond, F., Davini, G., Thonnat, M., Quoc-Cuong Pham, Allezard, N., Sayd, P., Rouas, J.-L., Ambellouis, S. and Flancquart, A (2006) "Audio-video event recognition system for public transport security", In The Institution of Engineering and Technology Conference on Crime and Security, IET, ISBN 0-86341-647-0, London, June 2006				

ANNEX II
Flyer presented during the interviews with security stakeholders



USE-iT FOX

USE-iT – *Dossier* WP3 - Segurança
Descrição dos tópicos de segurança

Conceito 1: Medidas para prevenir e limitar a atividade criminosa

PREVENÇÃO E LIMITAÇÃO DA ATIVIDADE CRIMINOSA

CIBERSEGURANÇA

TECNOLOGIAS E PRÁTICAS DE SEGURANÇA NO TRANSPORTE AÉREO

SEGURANÇA NAS ZONAS DE TRÂNSITO DE PASSAGEIROS

SEGURANÇA NO *DESIGN*

a) Cibersegurança

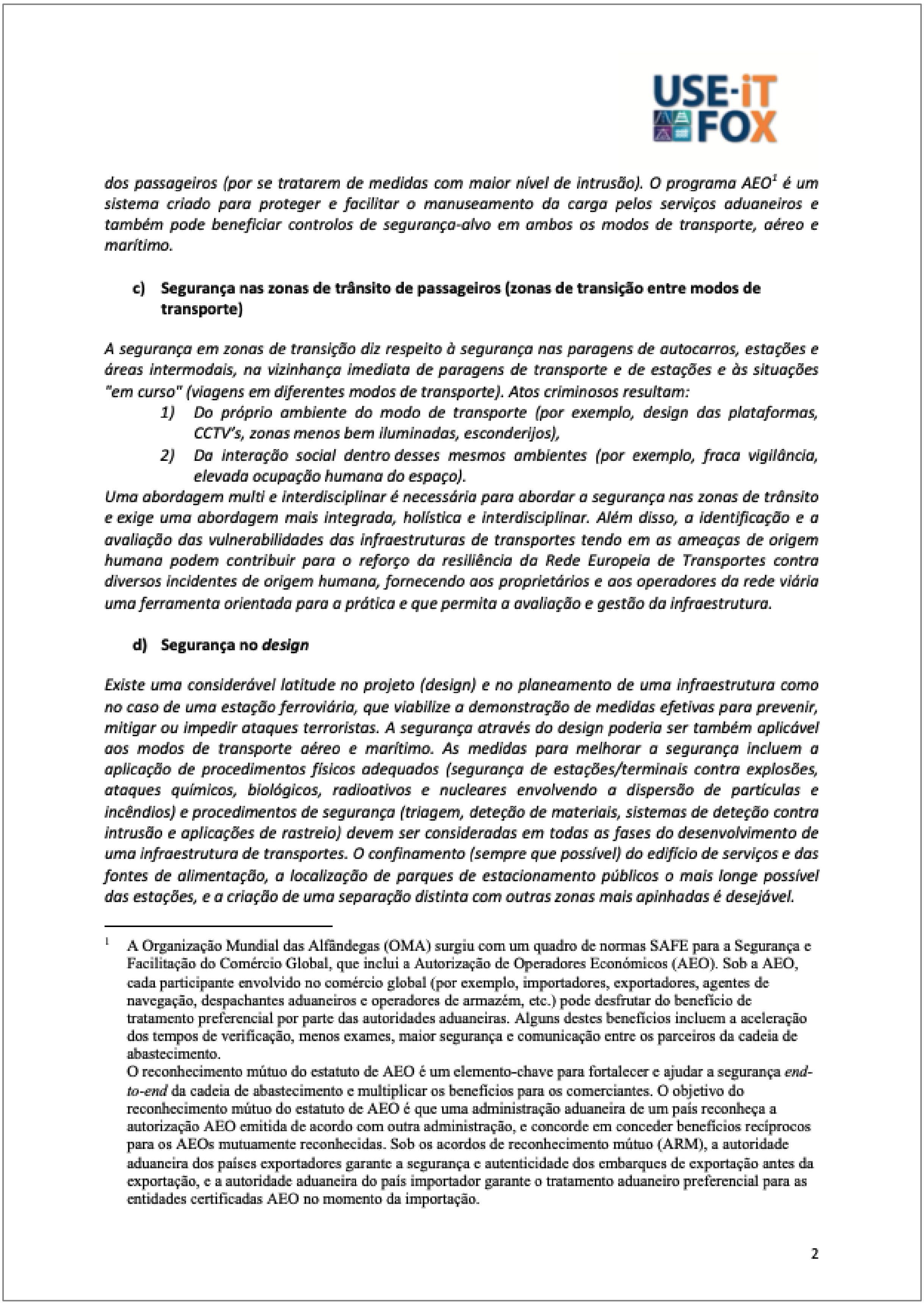
A cibersegurança diz respeito aos dispositivos eletrónicos dos transportes e da sinalização, aos sistemas de trânsito, às infraestruturas de transporte e aos veículos de transporte de passageiros e de carga. As vulnerabilidades potenciais da infraestrutura de transportes e veículos precisam ser mitigadas por protocolos de segurança e planos de prevenção. É necessário conhecer e compreender os sistemas críticos, as interdependências e a importância dos sistemas de controlo físicos e de cibernética, do controlo de tráfego e dos sistemas de gestão de operações, dos sistemas de gestão da segurança, dos serviços de operação e viagens (text messaging, e-commerce, e-payment). A criação de um sistema de cibersegurança que incorpore segurança na fase de projeto, desenvolva políticas e procedimentos de cibersegurança e melhore a resiliência dos sistemas e das operações, traria benefícios e motivaria os utilizadores com formação, exercícios e "hot triggers" (engodos).

b) Tecnologias e práticas de segurança no transporte aéreo

Desde os ataques terroristas de 2001, a UE, o Canadá e os EUA adotaram medidas eficazes e implementaram medidas de segurança adicionais (por exemplo, reforço e bloqueamento por dentro das portas da cabine de pilotagem, 100% de bagagem triada, maior número de passageiros revistados bem como a sua bagagem de mão, aumento da utilização de agentes de segurança no embarque, atenção acrescida à carga aérea, e uma maior atenção no controlo do acesso aos aeroportos e ao seu perímetro). Apesar do custo-resultado (cost-effectiveness), as abordagens de reforço de meios são muito mais difíceis de implementar noutros modos de transporte, principalmente devido aos elevados custos e à expectativa de uma menos positiva reação por parte

1

Note: translation under author's responsibility.



dos passageiros (por se tratarem de medidas com maior nível de intrusão). O programa AEO[1] *é um sistema criado para proteger e facilitar o manuseamento da carga pelos serviços aduaneiros e também pode beneficiar controlos de segurança-alvo em ambos os modos de transporte, aéreo e marítimo.*

c) Segurança nas zonas de trânsito de passageiros (zonas de transição entre modos de transporte)

A segurança em zonas de transição diz respeito à segurança nas paragens de autocarros, estações e áreas intermodais, na vizinhança imediata de paragens de transporte e de estações e às situações "em curso" (viagens em diferentes modos de transporte). Atos criminosos resultam:

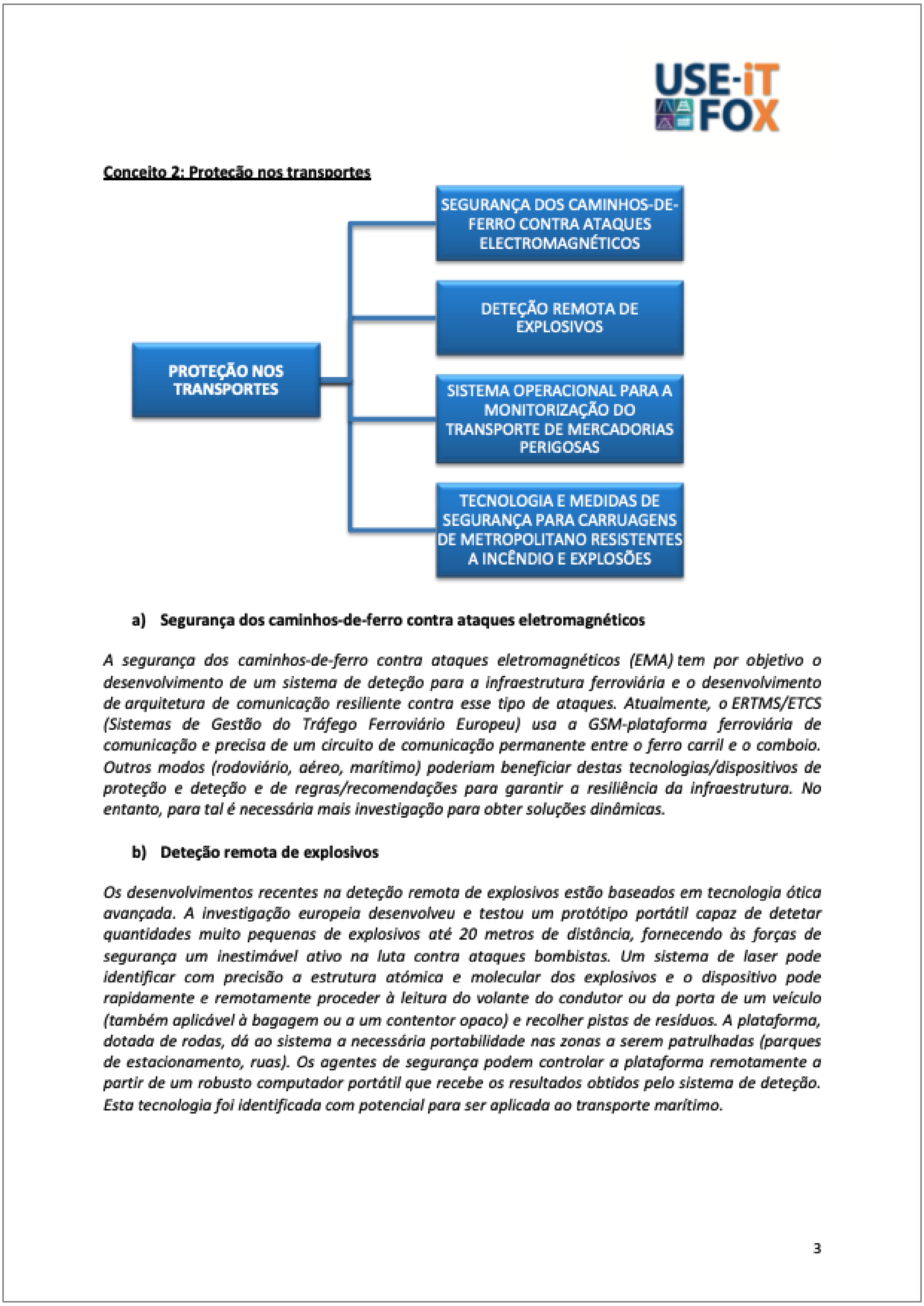
1) *Do próprio ambiente do modo de transporte (por exemplo, design das plataformas, CCTV's, zonas menos bem iluminadas, esconderijos),*
2) *Da interação social dentro desses mesmos ambientes (por exemplo, fraca vigilância, elevada ocupação humana do espaço).*

Uma abordagem multi e interdisciplinar é necessária para abordar a segurança nas zonas de trânsito e exige uma abordagem mais integrada, holística e interdisciplinar. Além disso, a identificação e a avaliação das vulnerabilidades das infraestruturas de transportes tendo em as ameaças de origem humana podem contribuir para o reforço da resiliência da Rede Europeia de Transportes contra diversos incidentes de origem humana, fornecendo aos proprietários e aos operadores da rede viária uma ferramenta orientada para a prática e que permita a avaliação e gestão da infraestrutura.

d) Segurança no *design*

Existe uma considerável latitude no projeto (design) e no planeamento de uma infraestrutura como no caso de uma estação ferroviária, que viabilize a demonstração de medidas efetivas para prevenir, mitigar ou impedir ataques terroristas. A segurança através do design poderia ser também aplicável aos modos de transporte aéreo e marítimo. As medidas para melhorar a segurança incluem a aplicação de procedimentos físicos adequados (segurança de estações/terminais contra explosões, ataques químicos, biológicos, radioativos e nucleares envolvendo a dispersão de partículas e incêndios) e procedimentos de segurança (triagem, deteção de materiais, sistemas de deteção contra intrusão e aplicações de rastreio) devem ser consideradas em todas as fases do desenvolvimento de uma infraestrutura de transportes. O confinamento (sempre que possível) do edifício de serviços e das fontes de alimentação, a localização de parques de estacionamento públicos o mais longe possível das estações, e a criação de uma separação distinta com outras zonas mais apinhadas é desejável.

[1] A Organização Mundial das Alfândegas (OMA) surgiu com um quadro de normas SAFE para a Segurança e Facilitação do Comércio Global, que inclui a Autorização de Operadores Económicos (AEO). Sob a AEO, cada participante envolvido no comércio global (por exemplo, importadores, exportadores, agentes de navegação, despachantes aduaneiros e operadores de armazém, etc.) pode desfrutar do benefício de tratamento preferencial por parte das autoridades aduaneiras. Alguns destes benefícios incluem a aceleração dos tempos de verificação, menos exames, maior segurança e comunicação entre os parceiros da cadeia de abastecimento.
O reconhecimento mútuo do estatuto de AEO é um elemento-chave para fortalecer e ajudar a segurança *end-to-end* da cadeia de abastecimento e multiplicar os benefícios para os comerciantes. O objetivo do reconhecimento mútuo do estatuto de AEO é que uma administração aduaneira de um país reconheça a autorização AEO emitida de acordo com outra administração, e concorde em conceder benefícios recíprocos para os AEOs mutuamente reconhecidas. Sob os acordos de reconhecimento mútuo (ARM), a autoridade aduaneira dos países exportadores garante a segurança e autenticidade dos embarques de exportação antes da exportação, e a autoridade aduaneira do país importador garante o tratamento aduaneiro preferencial para as entidades certificadas AEO no momento da importação.



USE-iT FOX

Conceito 2: Proteção nos transportes

PROTEÇÃO NOS TRANSPORTES

SEGURANÇA DOS CAMINHOS-DE-FERRO CONTRA ATAQUES ELECTROMAGNÉTICOS

DETEÇÃO REMOTA DE EXPLOSIVOS

SISTEMA OPERACIONAL PARA A MONITORIZAÇÃO DO TRANSPORTE DE MERCADORIAS PERIGOSAS

TECNOLOGIA E MEDIDAS DE SEGURANÇA PARA CARRUAGENS DE METROPOLITANO RESISTENTES A INCÊNDIO E EXPLOSÕES

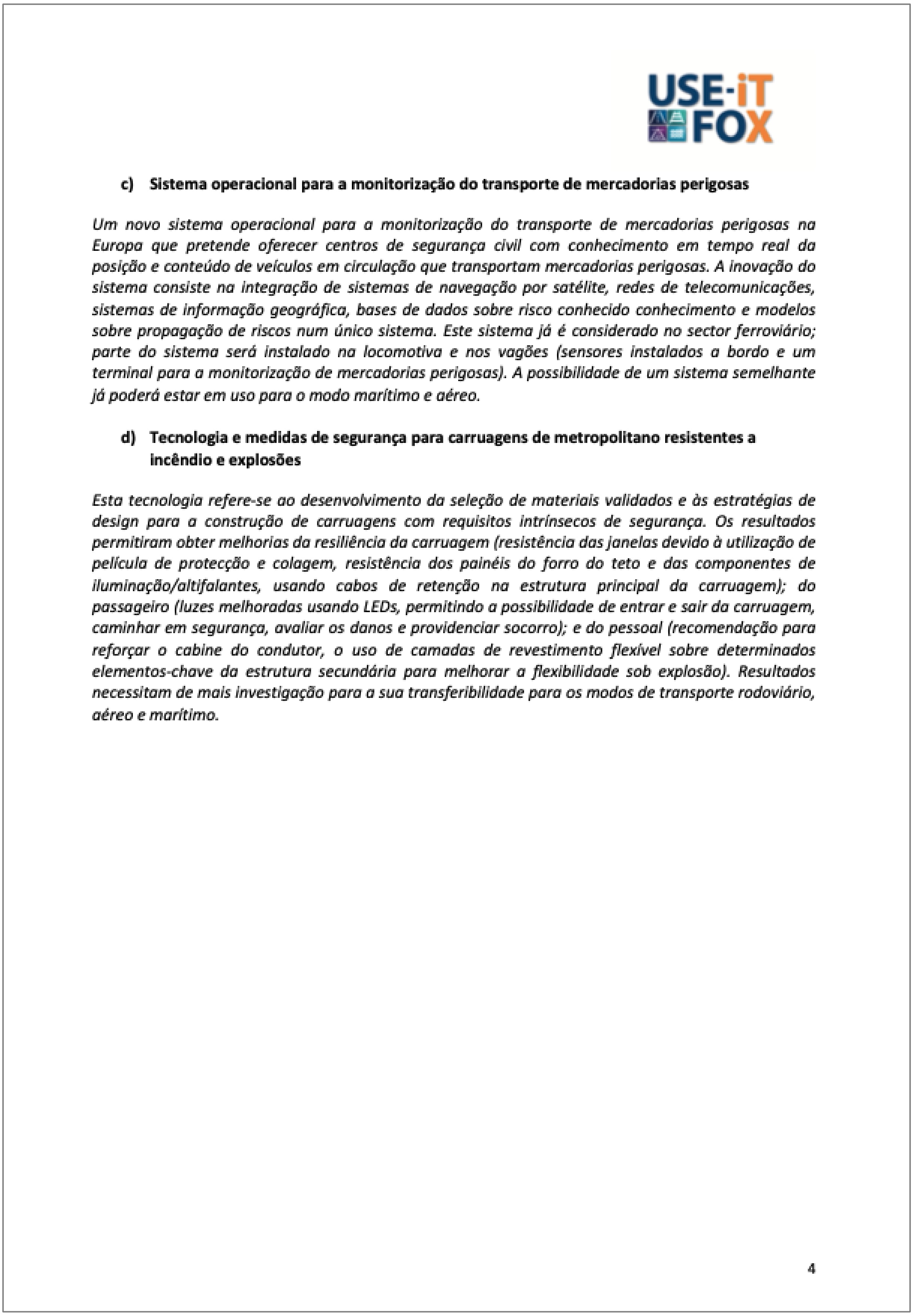
a) Segurança dos caminhos-de-ferro contra ataques eletromagnéticos

A segurança dos caminhos-de-ferro contra ataques eletromagnéticos (EMA) tem por objetivo o desenvolvimento de um sistema de deteção para a infraestrutura ferroviária e o desenvolvimento de arquitetura de comunicação resiliente contra esse tipo de ataques. Atualmente, o ERTMS/ETCS (Sistemas de Gestão do Tráfego Ferroviário Europeu) usa a GSM-plataforma ferroviária de comunicação e precisa de um circuito de comunicação permanente entre o ferro carril e o comboio. Outros modos (rodoviário, aéreo, maritimo) poderiam beneficiar destas tecnologias/dispositivos de proteção e deteção e de regras/recomendações para garantir a resiliência da infraestrutura. No entanto, para tal é necessária mais investigação para obter soluções dinâmicas.

b) Deteção remota de explosivos

Os desenvolvimentos recentes na deteção remota de explosivos estão baseados em tecnologia ótica avançada. A investigação europeia desenvolveu e testou um protótipo portátil capaz de detetar quantidades muito pequenas de explosivos até 20 metros de distância, fornecendo às forças de segurança um inestimável ativo na luta contra ataques bombistas. Um sistema de laser pode identificar com precisão a estrutura atómica e molecular dos explosivos e o dispositivo pode rapidamente e remotamente proceder à leitura do volante do condutor ou da porta de um veículo (também aplicável à bagagem ou a um contentor opaco) e recolher pistas de resíduos. A plataforma, dotada de rodas, dá ao sistema a necessária portabilidade nas zonas a serem patrulhadas (parques de estacionamento, ruas). Os agentes de segurança podem controlar a plataforma remotamente a partir de um robusto computador portátil que recebe os resultados obtidos pelo sistema de deteção. Esta tecnologia foi identificada com potencial para ser aplicada ao transporte marítimo.

3



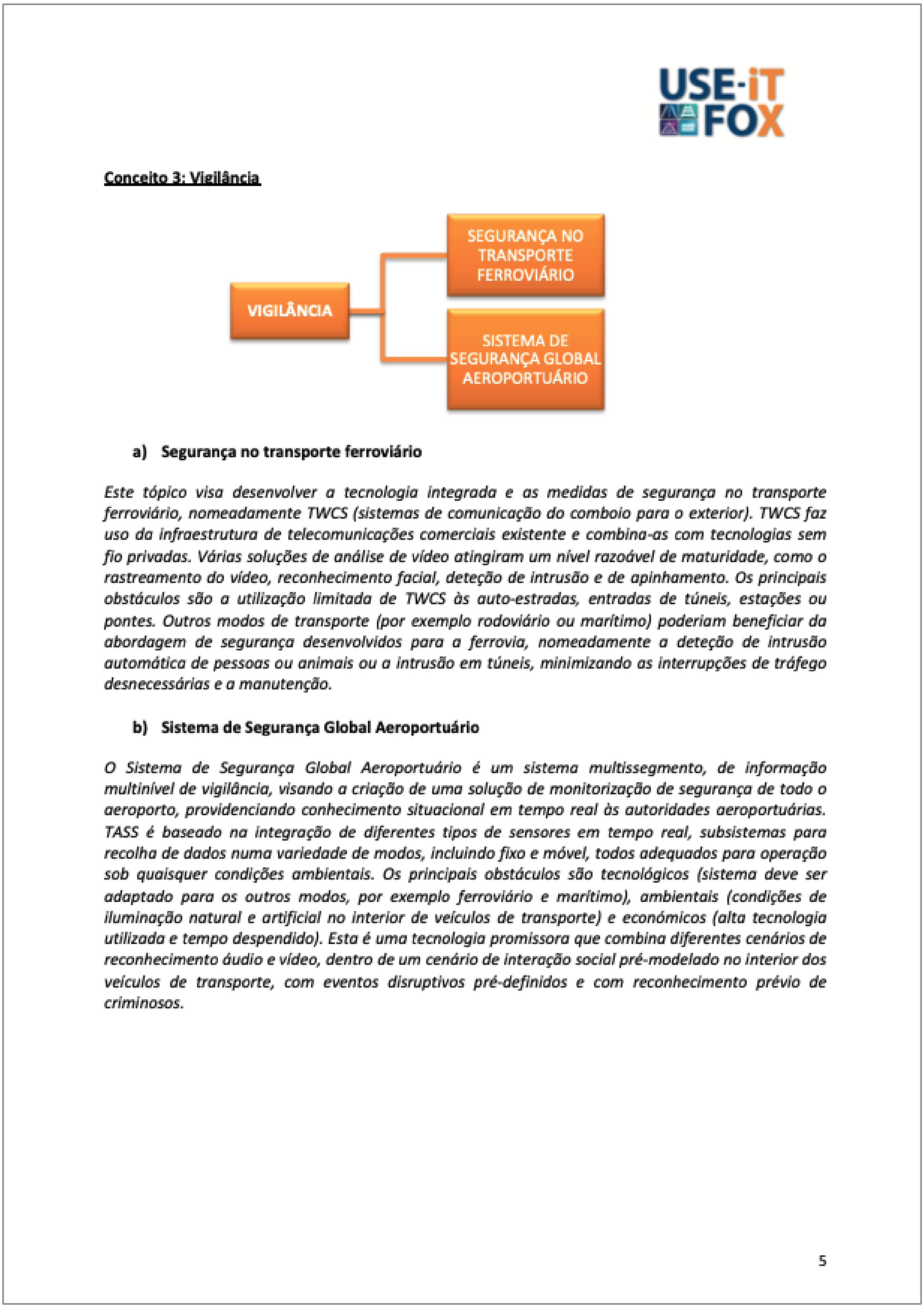
USE-iT FOX

c) Sistema operacional para a monitorização do transporte de mercadorias perigosas

Um novo sistema operacional para a monitorização do transporte de mercadorias perigosas na Europa que pretende oferecer centros de segurança civil com conhecimento em tempo real da posição e conteúdo de veículos em circulação que transportam mercadorias perigosas. A inovação do sistema consiste na integração de sistemas de navegação por satélite, redes de telecomunicações, sistemas de informação geográfica, bases de dados sobre risco conhecido conhecimento e modelos sobre propagação de riscos num único sistema. Este sistema já é considerado no sector ferroviário; parte do sistema será instalado na locomotiva e nos vagões (sensores instalados a bordo e um terminal para a monitorização de mercadorias perigosas). A possibilidade de um sistema semelhante já poderá estar em uso para o modo marítimo e aéreo.

d) Tecnologia e medidas de segurança para carruagens de metropolitano resistentes a incêndio e explosões

Esta tecnologia refere-se ao desenvolvimento da seleção de materiais validados e às estratégias de design para a construção de carruagens com requisitos intrínsecos de segurança. Os resultados permitiram obter melhorias da resiliência da carruagem (resistência das janelas devido à utilização de película de protecção e colagem, resistência dos painéis do forro do teto e das componentes de iluminação/altifalantes, usando cabos de retenção na estrutura principal da carruagem); do passageiro (luzes melhoradas usando LEDs, permitindo a possibilidade de entrar e sair da carruagem, caminhar em segurança, avaliar os danos e providenciar socorro); e do pessoal (recomendação para reforçar o cabine do condutor, o uso de camadas de revestimento flexível sobre determinados elementos-chave da estrutura secundária para melhorar a flexibilidade sob explosão). Resultados necessitam de mais investigação para a sua transferibilidade para os modos de transporte rodoviário, aéreo e marítimo.



Conceito 3: Vigilância

VIGILÂNCIA

SEGURANÇA NO TRANSPORTE FERROVIÁRIO

SISTEMA DE SEGURANÇA GLOBAL AEROPORTUÁRIO

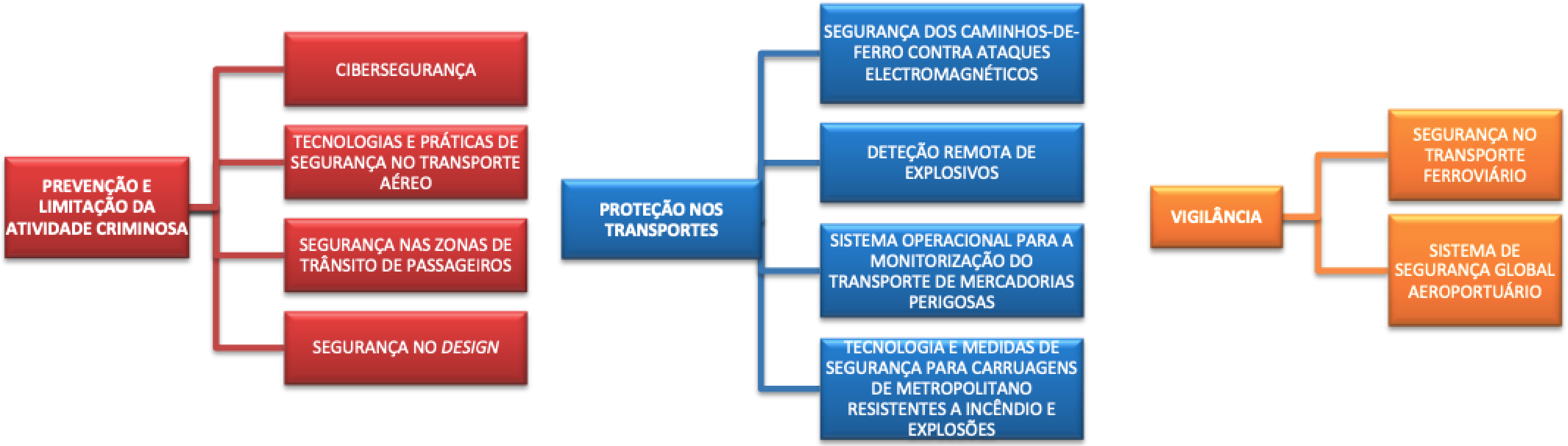
a) Segurança no transporte ferroviário

Este tópico visa desenvolver a tecnologia integrada e as medidas de segurança no transporte ferroviário, nomeadamente TWCS (sistemas de comunicação do comboio para o exterior). TWCS faz uso da infraestrutura de telecomunicações comerciais existente e combina-as com tecnologias sem fio privadas. Várias soluções de análise de vídeo atingiram um nível razoável de maturidade, como o rastreamento do vídeo, reconhecimento facial, deteção de intrusão e de apinhamento. Os principais obstáculos são a utilização limitada de TWCS às auto-estradas, entradas de túneis, estações ou pontes. Outros modos de transporte (por exemplo rodoviário ou marítimo) poderiam beneficiar da abordagem de segurança desenvolvidos para a ferrovia, nomeadamente a deteção de intrusão automática de pessoas ou animais ou a intrusão em túneis, minimizando as interrupções de tráfego desnecessárias e a manutenção.

b) Sistema de Segurança Global Aeroportuário

O Sistema de Segurança Global Aeroportuário é um sistema multissegmento, de informação multinível de vigilância, visando a criação de uma solução de monitorização de segurança de todo o aeroporto, providenciando conhecimento situacional em tempo real às autoridades aeroportuárias. TASS é baseado na integração de diferentes tipos de sensores em tempo real, subsistemas para recolha de dados numa variedade de modos, incluindo fixo e móvel, todos adequados para operação sob quaisquer condições ambientais. Os principais obstáculos são tecnológicos (sistema deve ser adaptado para os outros modos, por exemplo ferroviário e marítimo), ambientais (condições de iluminação natural e artificial no interior de veículos de transporte) e económicos (alta tecnologia utilizada e tempo despendido). Esta é uma tecnologia promissora que combina diferentes cenários de reconhecimento áudio e vídeo, dentro de um cenário de interação social pré-modelado no interior dos veículos de transporte, com eventos disruptivos pré-definidos e com reconhecimento prévio de criminosos.

USE-iT – WP3 - Segurança
Descrição dos tópicos de segurança



PREVENÇÃO E LIMITAÇÃO DA ATIVIDADE CRIMINOSA

- CIBERSEGURANÇA
- TECNOLOGIAS E PRÁTICAS DE SEGURANÇA NO TRANSPORTE AÉREO
- SEGURANÇA NAS ZONAS DE TRÂNSITO DE PASSAGEIROS
- SEGURANÇA NO *DESIGN*

PROTEÇÃO NOS TRANSPORTES

- SEGURANÇA DOS CAMINHOS-DE-FERRO CONTRA ATAQUES ELECTROMAGNÉTICOS
- DETEÇÃO REMOTA DE EXPLOSIVOS
- SISTEMA OPERACIONAL PARA A MONITORIZAÇÃO DO TRANSPORTE DE MERCADORIAS PERIGOSAS
- TECNOLOGIA E MEDIDAS DE SEGURANÇA PARA CARRUAGENS DE METROPOLITANO RESISTENTES A INCÊNDIO E EXPLOSÕES

VIGILÂNCIA

- SEGURANÇA NO TRANSPORTE FERROVIÁRIO
- SISTEMA DE SEGURANÇA GLOBAL AEROPORTUÁRIO

6

ANNEX III
Interviews with security stakeholders

Systematisation of the content of the interviews to security stakeholders

STAKEHOLDER TYPE	MODES	ANSWERS
TOPIC: General – Security Q1: What are the new/innovative techniques/methodologies to increase security that you have newly introduced in your organization in the last 5 years?		
TRANSPORT OPERATOR	RAIL	NO. In the last 5 years technological innovations in the security area have not been implemented. Existing systems were maintained and / or strengthened as determined by operational needs.
TRANSPORT OPERATOR	ROAD	NO. Criminal activity prevention by design is an example of what is now made in terms of security (on the past the USA norm suggested long corridors which are not friendly neither secure). Today, metro stations are built up with central atrium stations and former models/design of an atrium at the end was abandoned.
TRANSPORT OPERATOR	RAIL	YES. The company started to operate with innovative technologies and standards. Electronic security has been the most sensitive area deriving from the use of a critical infrastructure (bridge). Regular contacts with national intelligence for terrorist actions. The company use electronic surveillance systems and human surveillance and work directly with the security forces (police). The company introduced operating rules including the work of the security forces before trains circulation. The main core of the company activity in security terms is the combat to fraud and vehicles vandalism by using system alarms associated to CCTV system; There are no CCTV inside the trains; only in the hot spots of the infrastructure (stations and hubs).
TRANSPORT OPERATOR	RAIL	YES. In the year 2016 it has been implemented a spring system (technology developed specifically for us taking into account the existing space in the terminal) into a given terminal. The installation of this system was made to ensure the damping in the event of a collision to ensure the safety of employees and passengers inside the vehicle. In terms of methodologies, our company has developed close contacts with civil protection agents for action optimization, emergency planning into operation and some safety procedures were updated.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	YES. Introduction of surveillance cameras in stations (rail); Creation of the department of security road-rail; Procedural changes in the administrative conduct of the criminal situation/criminal reporting.
INFRASTRUCTURE PROVIDER	RAIL	YES. Special firewalls and software solutions against cyber-attacks; Video monitoring systems at railway stations and terminals; Regular trainings with security forces.
RESEARCH PROVIDER	AIR	YES. Risk assessment based on 3 D modelling of area to be protected, using drone and photogrammetry; Near real-time standoff detection of explosives; Wide area of surveillance capability at distances of about 30 m; Remote, stand-alone system; Non-contact; Short-wave infrared hyperspectral imaging by liquid crystal tunable filter.
RESEARCH PROVIDER	RAIL	YES. Research on cybersecurity in order to improve systems and operations resilience.
NATIONAL AUTHORITY	AIR	YES, the ones derived from annex 17 of ICAO that are of critical importance to the future of civil aviation and to the international community at large to prevent and suppress all acts of unlawful interference against civil aviation. Human factor – all stakeholders must have mandatory training; Update and knowledge recycling; Differentiated update and training according to the access levels to the airport infrastructure.
NATIONAL AUTHORITY	AIR	YES. New equipment (evaluation of security scanners, multiplexed x-rays, ACBS, …), work on “security culture” and an innovation programme to develop airports partnerships (“Vision Sûsete”).

STAKEHOLDER TYPE	MODES	ANSWERS
GOVERNMENT	RAIL, ROAD	YES. Crisis management based on quantitative indicators assessing systems resilience (the ability to cope with disruptions/ failures/ faults, etc.) and the identification of systems weakness, vulnerabilities.
OTHER	AIR	YES. LAG-screening technology included new SW and new processes; ETD-screening technology for different cross-checks for Pax and Handbag; Use of new generation of body scanners for pax screening.
OTHER	AIR	N/A
TRANSPORT OPERATOR	RAIL	N/A
TOPIC: General – Security Q2: Do you think that these techniques/methodologies have the potential to be transferred to other transport modes?		
TRANSPORT OPERATOR	ROAD	Transferability of CCTV and thermal cameras (infrared) to water mode.
TRANSPORT OPERATOR	RAIL	YES, to water and road modes.
TRANSPORT OPERATOR	RAIL	The spring system can be interesting, since it is designed to absorb the energy of the vehicle's crash at the end of the line in a short journey. The existing models needed a larger space so as to absorb the necessary energy.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	No, they are very mode-specific; we have introduced changes and technologies already adopted by other modes
INFRASTRUCTURE PROVIDER	RAIL	It would be very useful to share our experiences if other transport modes do not have such solutions.
RESEARCH PROVIDER	AIR	Methodology can be used for developing a 3D model of airport, harbour, central bus depot, and railway station.
NATIONAL AUTHORITY	AIR	Very difficult to implement on other modes (high costs, research need, service time constraints) but with potential to maritime (long distance cruises) and highspeed railway (intercountry).
NATIONAL AUTHORITY	AIR	Yes
GOVERNMENT	RAIL, ROAD	Yes, for technological level, but need more communication and consultation between all transport modes for cross-modal implementation as aviation security technologies and practices are very particular.
OTHER	AIR	“All new screening technologies are single-solutions, there is no integration in the complete process-chain! Out of the aviation-industry are demands in the transportation & logistic industry”
TOPIC: General – Security Q3: If there are no innovative techniques to be reported please let us know if any norms or procedures have been changed using the same techniques and technologies since the last five years.		
TRANSPORT OPERATOR	RAIL	Technology has evolved tremendously in the last five years and became more effective and useful, but not necessarily friendly or cheaper. The systems and security procedures were maintained to operate, much like the existing form and “attention / vigilance” regarding security was strengthened.
TRANSPORT OPERATOR	ROAD	The situation could be described as follows: the rules do not dictated practices, and these were not justified because the degree of threat was null or negligible.
TRANSPORT OPERATOR	RAIL	N/A
TRANSPORT OPERATOR	RAIL	Changes that existed were in the procedures regarding the speed set on the line and the optimization of contacts/joint work with civil protection agents.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	N/A
NATIONAL AUTHORITY	AIR	N/A
INFRASTRUCTURE PROVIDER	RAIL	Alarm systems with defined tasks for our staff
RESEARCH PROVIDER	AIR	N/A

STAKEHOLDER TYPE	MODES	ANSWERS
OTHER	AIR	All new equipment for process and procedures in Security are certified in different regulations by ECAC, ICAO, FAA and national Regulations!
NATIONAL AUTHORITY	AIR	N/A
GOVERNMENT	RAIL, ROAD	N/A
RESEARCH PROVIDER	RAIL	N/A
OTHER	AIR	N/A
TOPIC: Our concepts and topics in Security Q4a: Presentation of our list of topics and concepts, along with explanations and ask for approval, additional comments, scoring/rating		
TRANSPORT OPERATOR	RAIL	Presently, security issues should not be thought separately, but in a complementary and subsidiary way, attending the emerging threats. The resilience will be achieved with the use and implementation of various systems and crossing of different technologies and approaches. Threats are no longer linear. It requires to reflect about what are the threats and risks and what the value of the property to protect, and then think what is accurate. Obviously, the more systems are functioning the better (at least this is my perception based on observation and participation in different working groups and security platforms that I belong to). The question is how we will analyse such information. So, the most important is to have an interface that aggregates all these technologies and systems and display the information the way we want, that is to give the "alerts" that is configured.
TRANSPORT OPERATOR	ROAD	The securisation of a transport system (whatever the mode considered) must be understood globally, from access ports, traffic corridors, to existing public furniture, and includes visibility from LEAs (law enforcement authorities). The dialogue between LEAs and transport operators is critical. Very important is also the security training, which should be valued.
TRANSPORT OPERATOR	RAIL	We consider relevant the information / knowledge sharing management on the evolution of the security demands versus the evolution of security solutions regarding the variuos transport modes. The difficulty that organizations / companies have in addressing this issue results from the vulnerability / difficulty in managing the "unknow" or the "insufficiently know". The current global context will bring short-term challenges on this field and organizations / companies will have greater a difficulty to overcome if this issue is not resolved/decreased.
TRANSPORT OPERATOR	RAIL	OK. No additional comments on the topics and concepts.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	OK. No additional comments on the topics and concepts.
INFRASTRUCTURE PROVIDER	RAIL	OK. No additional comments on the topics and concepts.
RESEARCH PROVIDER	RAIL	OK. No additional comments on the topics and concepts.
RESEARCH PROVIDER	AIR	OK. No additional comments on the topics and concepts.
NATIONAL AUTHORITY	AIR	OK. No additional comments on the topics and concepts.
NATIONAL AUTHORITY	AIR	OK. No additional comments on the topics and concepts.
GOVERNMENT	RAIL, ROAD	OK. No additional comments on the topics and concepts.
OTHER	AIR	OK. No additional comments on the topics and concepts.
OTHER	AIR	OK. No additional comments on the topics and concepts.
TOPIC: Our concepts and topics in Security Q4b: What are the Top 3 concepts?		

STAKEHOLDER TYPE	MODES	ANSWERS
TRANSPORT OPERATOR	RAIL	Surveillance systems with video analytics and operators trained in behavioral analysis, must be crossed with kinotechnical teams on the ground, as well as vigilant and various sensors (chemical and not only) can detect and warn in time, beyond that the computer network has to be monitored and be safe from cyber-attacks, otherwise it will be complicated to have confidences in electronic systems.
TRANSPORT OPERATOR	ROAD	Cybersecurity, Security by design, Remote detection of explosives
TRANSPORT OPERATOR	RAIL	"Design by security, Security in transit environments, Total airport security system"
TRANSPORT OPERATOR	RAIL	The most important from the perspective of light rail transit systems is security in transit environments, total airport security system and security technologies and practices in air transport.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	Cybersecurity, Security by design, Security of railway transportation
NATIONAL AUTHORITY	AIR	Cybersecurity, Security by design, Surveillance (all technologies), Remote detection of explosives
TOPIC: Our concepts and topics in Security Q5: Are the topics relevant in their mode?		
TRANSPORT OPERATOR	RAIL	As mentioned in the previous question, I consider a mistake try to isolate areas or separate them: a security system should be seen holistically. For example, I would say that systems such as CCTV with video analytics and operators trained in behavioral analysis, must be crossed with dog teams on the ground, as well as vigilant and various sensors (chemical and not only) can detect and warn in time. In addition to the computer network safeguard has to be monitored and be safe from cyber-attacks; otherwise, it will be complicated to have confidence in electronic devices.
TRANSPORT OPERATOR	ROAD	Cybersecurity
TRANSPORT OPERATOR	RAIL	Total airport security system because turns face recognition work less time consuming, Security on railway transportation, Security against electromagnetic attacks (rail mode), Remote detection of explosives"
TRANSPORT OPERATOR	RAIL	The lack of control of the objects carried by passengers. Existing systems are too open and difficult to implement security measures. In our opinion, the lost and found objects are a problem (given the frequency and the amount) and there are no rapid methods of analysis of lost and found objects. Another issue of concern is the safe areas in passenger traffic because they are not designed taking into account these concerns and joint management is not made between the various transport modes. In this topic, the introduction of common procedures would help to more effective preventive and controlled occurrences. Another worrying issue is the CCTV, given the difficulties of implementation (both legally and technically). The implementation of these systems should be improved as often installed systems do not serve to fulfill the goals (*e.g.,* are not directed to sites that could allow a more effective identification of offenders)."
INFRASTRUCTURE PROVIDER	RAIL, ROAD	YES, specifically CCTV because it is beneficial for the prevention and containment of insecurity occurrences and for the detection of intruders/intrusions
INFRASTRUCTURE PROVIDER	RAIL	These topics are completely relevant in their modes
RESEARCH PROVIDER	AIR	N/A
NATIONAL AUTHORITY	AIR	YES, mainly cybersecurity, surveillance and remote explosives detection.
OTHER	AIR	N/A
TOPIC: Our concepts and topics in Security Q6: Are there any specific needs with regard to research (knowledge gaps)? Please specify how those knowledge gaps could be overcome.		

STAKEHOLDER TYPE	MODES	ANSWERS
TRANSPORT OPERATOR	RAIL	Systems that can be scaled / customized to produce early warnings. Creating interfaces / systems “layers” that can produce these alerts.
TRANSPORT OPERATOR	ROAD	Cybersecurity culture implementation is not achieved at the various decision-making levels. The use of nanotechnologies applied to security is underused. People's awareness in general for security issues (flyers, schools, etc.)
TRANSPORT OPERATOR	RAIL	User willingness to pay (considering the transferability of air security technologies and procedures to rail mode), data protection. One of the problems that affect organizations / companies refers to new forms of crime (terrorism) and the information management process / knowledge on this subject. Support / enhance knowledge produced by research, a wider dissemination of the research and consequent increase of awareness to the problem of security among the different players, definition of strategies to improve the approach to the problem and enhance the development of interactions and partnerships for implementing mitigation solutions.
TRANSPORT OPERATOR	RAIL	There are some shortcomings such as the lack of communication between the various agents, a greater sharing of experience and know-how allowing a more efficient joint action. Legislation should also follow the existing needs in the area of security, which often does not permit an effective action.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	It is necessary to contradict the idea that rail mode is safe to the practice of criminal acts; the presence of security forces even though has the constraint to affect the service (delay on trains) can increase objective security and the security perceptions among users. Inefficiency in communicating crime occurrences in transport modes. Many security procedures are still made in a ““handmade way”“, *i.e.*, lack of systematic procedures and rules for registry and data treatment. Research, awareness programs to users, especially the younger generations; joint work between security forces and infrastructure operators, improve the record of criminal occurrences in different transport modes.
NATIONAL AUTHORITY	AIR	Body and baggage scanning, Quality control improvement which may involve changes in the training of staff, Enlargement of the procedures allowing security forces staff to fly with weapons Use of dogs as explosive detectors, extension of the list of prohibited articles and absence of a security culture
OTHER	AIR	The detection of explosives must be done remotely. The challenge is how to do it without disturbing the passengers. Radioactive material detection will come, and the airports will have to install it. Currently, radio-active material is being transported a lot. The personnel working in airport cargo is exposed to that. There is no real-time detection.
TOPIC: Multi-modal involvement Q7: Have you been involved in any cross-modal activities in this area (security)? If yes, please elaborate or specify.		
TRANSPORT OPERATOR	RAIL	Yes
TRANSPORT OPERATOR	ROAD	Long experience in Portugal as well as abroad, note exclusively on rail mode.
TRANSPORT OPERATOR	RAIL	Yes, road mode.
TRANSPORT OPERATOR	RAIL	Our multi-modal involvement refers to the management of security in the implementation of various events such as local festivals, marathons and other operations where there is a joint coordination of means and procedures between the various transport modes, civil protection agents and municipal services. There are also partnerships at the level of emergency management, with common emergency plans and simulation actions with the various transport modes.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	Yes, with road.
INFRASTRUCTURE PROVIDER	RAIL	Regular meetings and know-how transfer with road administration

STAKEHOLDER TYPE	MODES	ANSWERS
NATIONAL AUTHORITY	AIR	STAC approached by other modes (*e.g.,* railway) for the use of explosive detection dogs"
NATIONAL AUTHORITY	AIR	Yes, mainly with rail (metro hub + airport) and road.
RESEARCH PROVIDER	RAIL	Just research activities in different transport modes
RESEARCH PROVIDER	AIR	Designing integrated bomb-explosion detection systems for critical infrastructure.
GOVERNMENT	RAIL, ROAD	Road and railway video surveillance data treatment and systems resilience assessment
OTHER	AIR	N/A
TOPIC: Multi-modal involvement Q8: What do you think are the common challenges to increase security across modes?		
TRANSPORT OPERATOR	RAIL	Having a set of available tools that can increase system's resilience, either technological tools or others, as well as spreading them by all transport system, so that they can be used and that the monitoring clearance to be effective, through the technologies already available to the end-users (provided that there is money to buy such equipment, which does not seem to be the case).
TRANSPORT OPERATOR	ROAD	YES. Specific training of the security forces to increase security in public transport; extracurricular training on regulations and security procedures associated with each mode.
TRANSPORT OPERATOR	RAIL	Cybersecurity and Anti-terrorism preventive action
TRANSPORT OPERATOR	RAIL	The main challenge is to work together in order to define a common security policy involving the public security forces and public and private transport companies. Besides, the introduction of CCTV in the vehicles and data disclosure. Information on the entry of problematic passengers should be shared with other modes in order to allow the response readiness.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	YES, at recording crime data occurrences in different transport modes (statistics production and analysis).
NATIONAL AUTHORITY	AIR	Background checks of candidates, adequate training, delineation of areas and more CCTV access control
TOPIC: Multi-modal involvement Q9a: Have you been involved in any cross-modal activities in this area (security)?		
TRANSPORT OPERATOR	RAIL	Yes
TRANSPORT OPERATOR	ROAD	Long experience in Portugal as well as abroad, note exclusively on rail mode.
TRANSPORT OPERATOR	RAIL	Yes, road mode.
TRANSPORT OPERATOR	RAIL	Our multi-modal involvement refers to the management of security in the implementation of various events such as local festivals, marathons and other operations where there is a joint coordination of means and procedures between the various transport modes, civil protection agents and municipal services. There are also partnerships at the level of emergency management, with common emergency plans and simulation actions with the various transport modes.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	Yes, with road.
INFRASTRUCTURE PROVIDER	RAIL	Regular meetings and know-how transfer with road administration
NATIONAL AUTHORITY	AIR	STAC approached by other modes (*e.g.,* railway) for the use of explosive detection dogs"
NATIONAL AUTHORITY	AIR	Yes, mainly with rail (metro hub + airport) and road.
RESEARCH PROVIDER	RAIL	Just research activities in different transport modes
RESEARCH PROVIDER	AIR	Designing integrated bomb-explosion detection systems for critical infrastructure.
GOVERNMENT	RAIL, ROAD	Road and railway video surveillance data treatment and systems resilience assessment
OTHER	AIR	N/A

STAKEHOLDER TYPE	MODES	ANSWERS
TOPIC: Multi-modal involvement Q9b: If yes, please elaborate or specify.		
TRANSPORT OPERATOR	RAIL	SECUR-ED project, among others, *vd.* http://www.uic.org/Security-Reseach-Projects#SECRET-SECurity-of-Railways-against-Electromagnetic-aTtacks
TRANSPORT OPERATOR	ROAD	YES, with security forces and other modes operators.
TRANSPORT OPERATOR	RAIL	The company is not yet at that level (cross-modal activities regarding security), *i.e.*, there is no cooperation between entities both public and private.
TRANSPORT OPERATOR	RAIL	We have tried to implement a project together with the public security forces based on the “Liverpool Model” which was based on the common management of events, but there was a great difficulty by the security forces in providing adequate resources.
INFRASTRUCTURE PROVIDER	RAIL, ROAD	YES, with road.
INFRASTRUCTURE PROVIDER	RAIL	Not yet
NATIONAL AUTHORITY	AIR	YES
NATIONAL AUTHORITY	AIR	N/A
RESEARCH PROVIDER	AIR	Threat assessment for metro- and bus transportation system in Middle East.
RESEARCH PROVIDER	RAIL	N/A
GOVERNMENT	RAIL, ROAD	Level crossings safety and security Improvement
OTHER	AIR	N/A
OTHER	AIR	N/A
TOPIC: Multi-modal involvement Q10: What opportunities do you think there are for cross-modal research in enhancing transport security?		
TRANSPORT OPERATOR	RAIL	Several. There are projects funded by the EU in this area, very interesting and that were never implemented. It would be a good idea to start by listing those projects and try to understand what could be done with those who have potential.
TRANSPORT OPERATOR	ROAD	Greater integration between the security forces and critical infrastructures operators.
TRANSPORT OPERATOR	RAIL	Aviation anti-terrorism procedures and technologies should be implemented in high-speed rail; Conventional solutions are harder to implement in urban and suburban rail transport because of discomfort to the user and so opt for less intrusive measures of policing and surveillance; Digital footprint is important to trace criminal activity; Cooperation between public and private entities in combating urban crime”
TRANSPORT OPERATOR	RAIL	N/A
INFRASTRUCTURE PROVIDER	RAIL, ROAD	The hubs of greater interoperability (different transport modes) because they are more complicated to manage due to the high influx of users and the impact they have in terms of operation.
NATIONAL AUTHORITY	AIR	Implementation of a security culture at society level using education system and training to form the younger generations on security topic (*e.g.,* like what has been done regarding some environmental behaviors such as recycling of waste) Improvement of the AVSEC for all modes, that is, appropriate regulation + adequate training of human resources + technology improvement.”
INFRASTRUCTURE PROVIDER	RAIL	Safer and better communication and common training sessions for all transport modes
TOPIC: Multi-modal involvement Q11: Would your organization be interested in practical involvement for transferring best practices across modes? If yes, please elaborate		
TRANSPORT OPERATOR	RAIL	The company is always willing to cooperate in an area as sensitive as this, always depending on its possibilities and limitations.
TRANSPORT OPERATOR	ROAD	YES, mainly with water mode.

STAKEHOLDER TYPE	MODES	ANSWERS
TRANSPORT OPERATOR	RAIL	YES, through work partnerships with other modes representatives, security forces and intelligence agencies.
TRANSPORT OPERATOR	RAIL	N/A
INFRASTRUCTURE PROVIDER	RAIL, ROAD	YES, mainly with road and maritime.
INFRASTRUCTURE PROVIDER	RAIL	YES, at societal level (education institutions, security forces, other modes).
NATIONAL AUTHORITY	AIR	Cybersecurity, surveillance systems and training methods
RESEARCH PROVIDER	AIR	International Security Competence Centre GmbH (ISCC, Austria) is interested in using SOTA technologies to create security systems for cross-modal transport components, based on combining SOS and VAS.
OTHER	AIR	We are active in the Aviation Industry and started in the Transportation & Logistic Industry. We have international experience and references in Aviation Security.
GOVERNMENT	RAIL, ROAD	Yes. Already working on level crossings safety and security improvement (for road and railway systems)

ANNEX IV
USE-iT WP3 Stakeholders Workshop #2 – Security Handouts

USE-iT WP3 Stakeholders Workshop #2 – Security Handouts (Page 1)

Security challenges

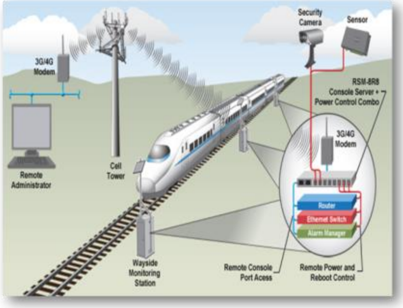
1. Cybersecurity
2. Reduction of suicides in railway transport
3. Ensuring security in transit environments while maintaining privacy demands of passengers
4. Crime prevention through environmental design
5. Lack of cooperation between operators, law enforcement, managers and technicians
6. Efficient threat detection (e.g. explosives, terrorism, etc.)
7. Assessment of potential vulnerability in cases of criminal acts or intentional disasters

Description of main research topics for Security

Source: http://security.cs.umass.edu/

Cyber security – collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Cyber security affects surface transportation electronic devices and signalling, transit systems, transport infrastructure, passengers and cargo vehicles. The potential vulnerabilities in transport infrastructure and vehicles need to be mitigated by security protocols and plans ahead of time. It is necessary to understand critical systems, interdependencies and the importance of cyber physical control systems, traffic control and operations management systems, safety management systems, traveller and operator services (511, e-commerce, e-payment). The creation of a cyber security system that incorporates security into the design process, develop policies and procedures for cyber security and improving systems and operations resilience, would bring benefits and motivate users with training, exercises & "hot triggers".

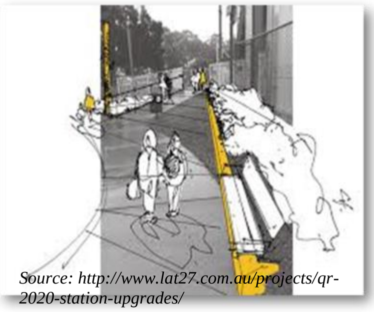

Security Camera
Sensor
3G/4G Modem
RSM-8R8 Console Server + Power Control Combo
3G/4G Modem
Remote Administrator
Cell Tower
Router
Ethernet Switch
Alarm Manager
Wayside Monitoring Station
Remote Console Port Acess
Remote Power and Reboot Control

Source: http://www.wti.com/t-managing-network-devices-in-wayside-railroad-applications.aspx

Security of railway transport – This topic aims at developing integrated technology and measures for railway transport security, namely TWCS (train to wayside communication systems).

TWCS makes use of existing commercial telecom infrastructure and combines them with private wireless technologies. Several video analytics solutions have reached a reasonable level of maturity, such as, video tracking, face recognition, intrusion detection and crowd detection. The main barriers are the limited use of TWCS to highways, tunnels entrances, stations or bridges. Other modes (e.g. road, water) could benefit from the security approach developed for rail, namely human/animals trespassing by automatic intrusion detection or tunnel entrance intrusion minimizing unnecessary traffic interruptions and maintenance.

USE-iT WP3 Stakeholders Workshop #2 – Security Handouts (Page 1)



Source: http://www.lat27.com.au/projects/qr-2020-station-upgrades/

Security by design – There is a considerable scope in the design and planning of station infrastructure to include proven and effective security measures to prevent, mitigate or deter attacks from terrorists.

The measures to improve security include the implementation of appropriate physical secure stations/terminals against bomb blast, CBRN (Chemical, Biological, Radiological and Nuclear) attacks involving particle dispersion and fire events); security procedures (screening, materials detection, intrusion detection systems, and tracking applications) should be considered at all stages of station development. The containment (where possible) of building services and power supplies, locating public car parks as far away from station buildings, creating a distinct separation with other 'crowded places' are examples of possible measures.

Security in transit environments – refers to the security of buses stops, stations and interchanges, to the immediate vicinity of transport stops and stations and to the 'en route' travel (on board of different modes).

Criminal acts are a result of 1) the environment of the transport node itself (e.g., design of platforms, CCTVs, dark corners, hiding places) and, 2) the social interaction within those environments (e.g., poor guardianship, crowdedness). A multi- and interdisciplinary approach is required to tackle transit security and demands more integrated, holistic and cross-disciplinary approach. Also, the identification and assessment of transport infrastructure vulnerabilities regarding man-made threats can contribute to the strengthening of the resilience of the European Transport Network against various man-made hazards, by providing road owners and operators with an easy to manage, practice-oriented tool for the assessment of the infrastructure.

Remote detection of explosives – Recent developments on explosive remote detection are based on advanced optic technology.

Source: https://www.tangerinetravel.com/How-to-Expedite-Getting-Through-Security

A laser system can precisely identify the atomic and molecular structure of the explosives and the device can rapidly and remotely scan the steering wheel or the door of a vehicle (also applicable to luggage, opaque container) and pick up trace residue. The wheeled platform gives the system the necessary portability to the areas to be patrolled (car park, street). Security agents can control the platform remotely from a portable ruggedized lab-computer that receives the results obtained by the detection system. This technology was identified with potential to be applied to maritime transportation.

www.lnec.pt

AV DO BRASIL 101 • 1700-066 LISBOA • PORTUGAL
tel. (+351) 21 844 30 00
lnec@lnec.pt **www.lnec.pt**