SEVENTH FRAMEWORK PROGRAMME

THEME [SEC-2013.2.2.1]

[A Research Agenda for security issues on land transport – Coordination and Support Action (Coordinating Action)]

Final project report

Tables and figures

Project acronym: **CARONTE**

Project full title: **Creating an Agenda for Research On Transportation sEcurity**

Date of preparation of this version:	**28/04/16**
Authors:	**Joachim Kochsiek – Fraunhofer IML**
Status (F: final; D: draft; RD: revised draft):	**F**
File Name:	**CARONTE_Tables_Figures_Final_Reporting.docx**
Version:	**1.0**

The research leading to the results of the project has received funding from the European Union Seventh Framework Programme (FP7/2013-2016) under grant agreement n° 606967.

CONTENT

List of tables:

List of figures:

Table 1: Research needs for topic "Staying operational in the event of a cyber-incident"

Category		Research Needs
Infrastructure	Protocols	There is a need for research to develop a comprehensive general protocol to be applied in a case of a cyber-event in transport specifically.
	Cooperation	Strong need for research into increasing cooperation among the actors in case of an event. That could include cross-border cooperation.
	Training	Research is needed on to how to raise the security awareness of ICT staff in land transport so they are prepared to act in the event of a cyber-attack.
ICT	ICT systems	Research projects are needed which look at making control systems specific to land transport (rail in particular) more resilient to attack and to develop early warning systems.
	Innovation	Research to address ICT priorities specifically in the land transport sector and how to maintain or re-establish aspects of systems in the event of an attack, such as trustworthy network and service infrastructures, user-centric identity and privacy management, and advanced biometrics.

Table 2: Identified research needs for a "timely and efficient threat detection"

Passenger Transport		Research Needs
Detection of illegal substances		• research, development and standardisation of detection technologies (video, infrared, laser, acoustic, sniffers) • fast, robust, reliable, affordable detectors which do not disturb business continuity • non-hindering sensors • stand-off detection • detection of all or more types of explosives • multi-hazard approach • coherent technologies (able to screen for different things in one go) • interoperability and network application of detection devices • improving the presentation of detection results • - miniaturising detection equipment
	Biological substances	• - non-specific B-detection
	Radioactive and nuclear material	• detection and identification of difficult to detect radioactive sources and nuclear material • detection and identification of masked and shielded sources • address the problems of “innocent” or false alarms • detection and location of radiation sources in large crowds • electronic tracking systems for radioactive sources • improving detection software • enhance mobility and portability of detection solutions
	Electromagnetic attacks	
Detection of concealed objects		
Situation assessment		• research, development and standardisation in the area of CCTV (linear camera, thermo camera, video comm., laser) • future usage of CCTV (in a proactive way) • fusion of different detection data • algorithms for data fusion and processing • algorithms for data analysis
Abnormal behaviour detection		
Other		• surveillance of connecting infrastructures • monitoring of staff (rail, bus drivers, etc.) • CBRNE detection in busses

Cargo Transport		Research Needs
Detection of illegal substances and hidden persons		See Passenger transport.
	Biological substances	
	Radioactive and nuclear material	
Container monitoring systems		• security awareness and risk management • authentication, certification and data protection • - physical transportation security and cargo monitoring
Surveillance of critical infrastructure (detection of intruders)		• secure and intelligent surveillance, alarm and access systems at freight distribution centres and park & ride areas • reliable and tamper-proof alarm systems that detect malice intrusion in vehicles, cargo compartments and containers using various types of sensing technologies (e.g. infrared, ultrasonic, microwave, vibration, narcotic gas detectors, etc.) with close-to-zero false alarm ratio and automatic emergency message to the police

Table 3 Threats to the land transport sector

Physical risks	Personal risks	Cyber risks

• Crime
• Rising violence in cargo theft
• Rising organisation of crime
• Bombing (often by suicide attackers or with the help of vehicles) is the most important mean of terrorists (followed by sabotage, and arson)
• Very low, up to no, reporting of dirty bombs, or poison
• Attractive targets are junctions, tunnels, and bridges
• Also important passenger trains (especially metros, as frequently seen in Russia or Belarus)
• Aging or poorly maintained infrastructure in some countries can cause more vulnerabilities, as robustness, bypassing possibilities or the likelihood or easiness to cause failures rises
	• Staff as a target of criminals or terrorists
	• Staff as an enabler for terrorists and criminals
	  • Force / extortion
	  • Corruption
	  • Lack of knowledge (IT-Security, security recommendation)
	  • Careless
	  • Lack of acceptance due to complexity of use regarding IT and IT Security
	• Lack of education and training in security and in use of modern technologies, processes and IT
	• Lack of motivation
	• Each private end device which has access to a network could be a security risk
		• 'Internet of things' introduces new communication between items with new potential gates for attacks
		• Software errors multiply with the number of connected systems
		• Open information flow in logistic systems also offers gates for criminals and terrorists
		• IT-Systems with different levels of security, especially quickly aging software or hardware in connected systems introduces weak points to a chain
		• Access to web based communication systems with unsecured end devices (esp. private devices with lower security standard and not hardly manageable security policies)
		• Rising interconnection and interdependency of traffic management and control systems also with relation to safety (automatic train control)
		• Outsourcing of IT-Systems also for traffic control with new interfaces and actors and uncertain security measures
		• Spoofing of information / signals
		• Disturbing of information / signals
		• As vehicles communicate between each other spoofing of information or infiltration of wrong information can cause high risks in transport
		• New dangers due to increasing ICT and connectivity in more and more automatic and autonomous cars

Table 4: Top gaps and requirement from matrix analysis

Gap & requirement title – matrix analysis
Cybersecurity and cybercrime
Commune standards and protocols
Detection and Monitoring Technology
Prevention: developing tools in risk assessment
Crisis Management
Physical Protection
Organizational protection in case of attack and hijacking (staff, passenger, vehicle and logistic)
Security personnel
Complete security chain in case of attack, hijacking (staff and vehicle) and manipulation from staff.
Closed loading units (seals) in case of attack (logistic, cargo and vehicle), manipulation and theft.

Table 5: Top ten gaps and requirements from questionnaires

Gap and requirement title - questionnaire
Financial support of authorities to implement security measures
Ethical and Regulation concerns stop technologies
Detection and Monitoring Technology
Budget to develop technologies
Coordination - Lesson Learned share between all actors in land transport chain
Cybersecurity and cybercrime
Lack of awareness
Prevention: developing tools in risk assessment (proactive assessment of possible vulnerabilities)
Training
Commune standards and protocols

Table 6: Top ten gaps and requirements from expert workshop

Gap and requirement title
Lessons learned or existing solutions from other sectors (i.e. aero, safety process) to transport sector
Open Systems
Education and Training (TTP - Tactics, techniques & procedures)
Logistics - Cyber Protection
Interface Port - Cyber protection - Power Supply
Cyber Security integrate into Infrastructure Risk assessment
Communication between countries & organization’s in emergency situation (e.g. Mont 'Blanc)
Awareness
Standards & Rules
Rising threat from terrorism or organized crime

Figure 1: Tentative roadmap for FCT (the blue items relate to railway security, the orange items relate to threat detection, the purple items relate to balancing security and privacy, the green items relate to other domains)

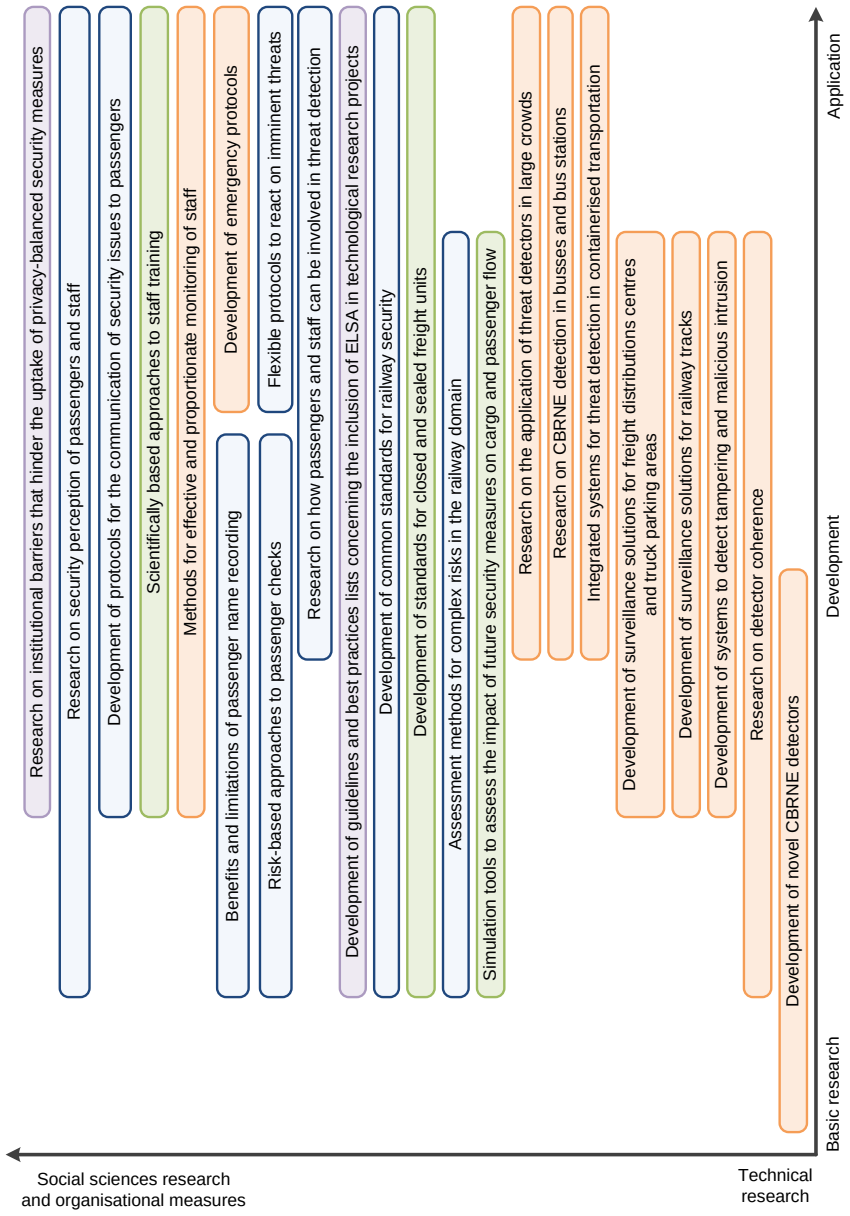


Figure 2: Tentative roadmap for CIP and DRS (the blue items relate to incident prevention and threat mitigation, the orange items relate to crisis management)

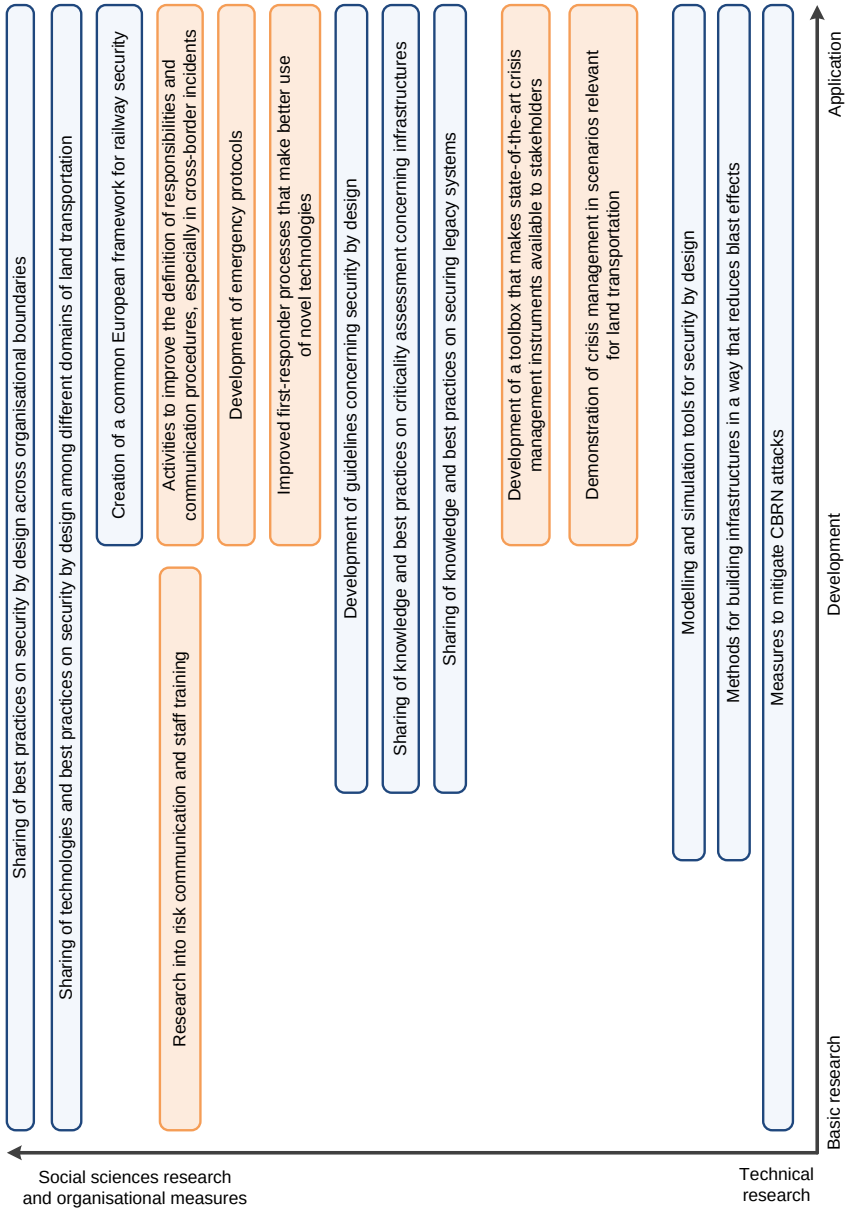


Figure 3: Tentative roadmap for the Digital Security Focus Area (the blue items aim at securing existing systems, the orange items aim at securing future systems)

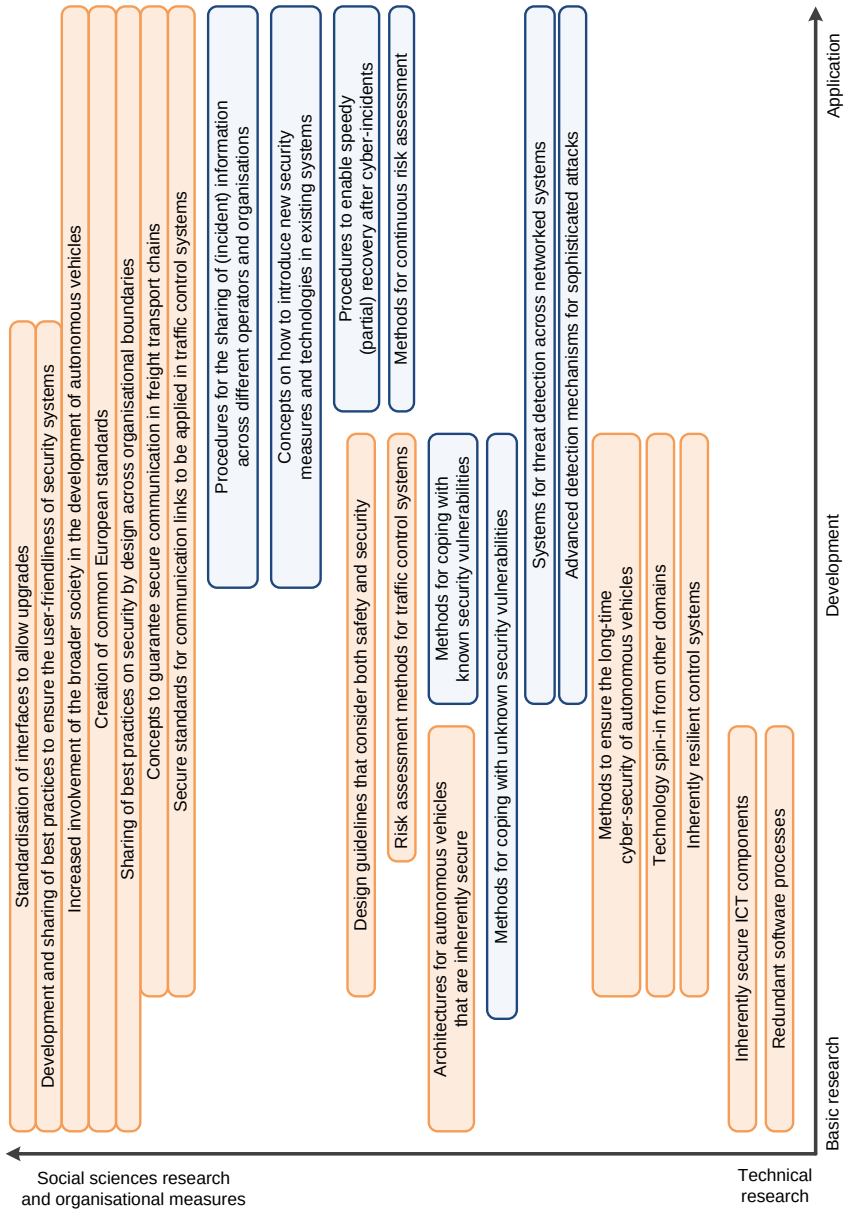


Figure 4: Share of security activities[1]

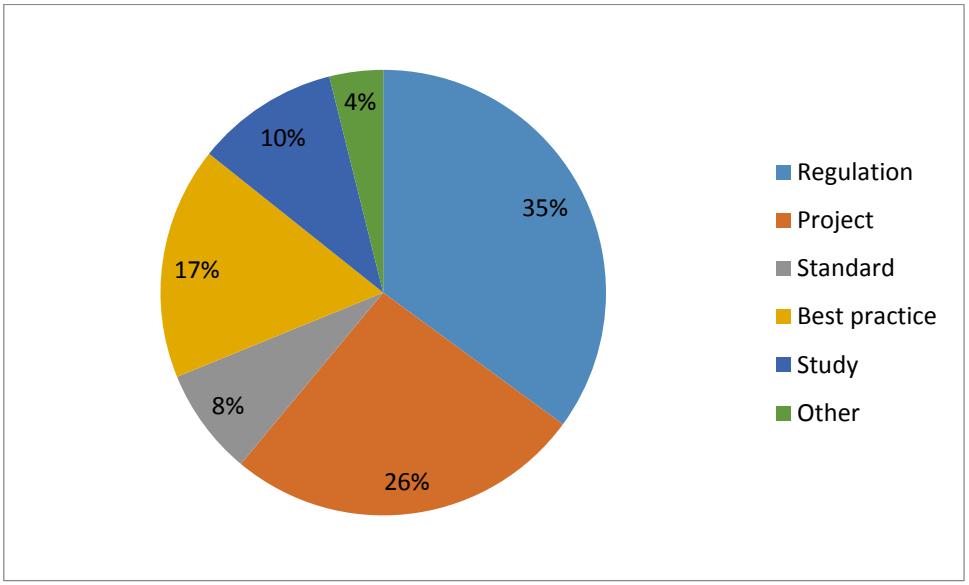
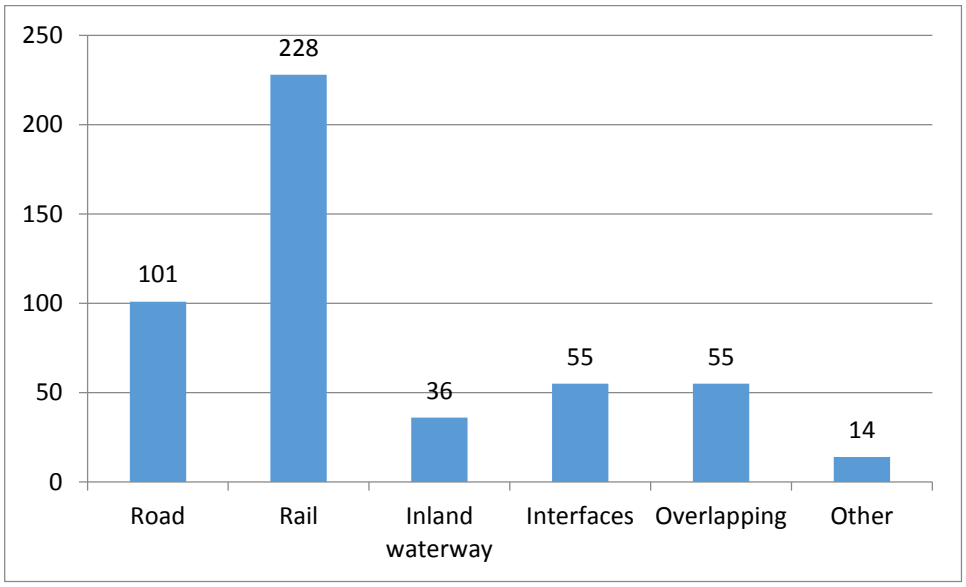


Figure 5: The number of identified activities up to end of December 2014 concerning the various transport modes[2]



[1] Source: CARONTE Deliverable 2.1
[2] Source: CARONTE delivery 2.1