European Commission




Research Theme Analysis Report

Transport Security

COMMUNICATING TRANSPORT RESEARCH AND INNOVATION

www.transport-research.info

Mobility and Transport

This report was prepared by:
Claudia de Stasio, Cosimo Chiffi, Alessio Sitran, Riccardo Parolin, Silvia Maffii, Raffaele Vergnani (TRT),
Claus Doll, Lucia Mejia-Dorantes, Katharina Wachter (Fraunhofer),
Gareth Horton, Marius Biedka (Ricardo Energy & Environment),
Hana Bruhova (CDV), Ian Skinner (TEPR)

Coordinated and guided by:
Robert Missen
DG MOVE – Head of Unit B3 (Innovation & Research)

Dimitrios Vartis
DG MOVE – Unit B3 (Innovation & Research)

Design and layout by:
Ricardo Energy & Environment

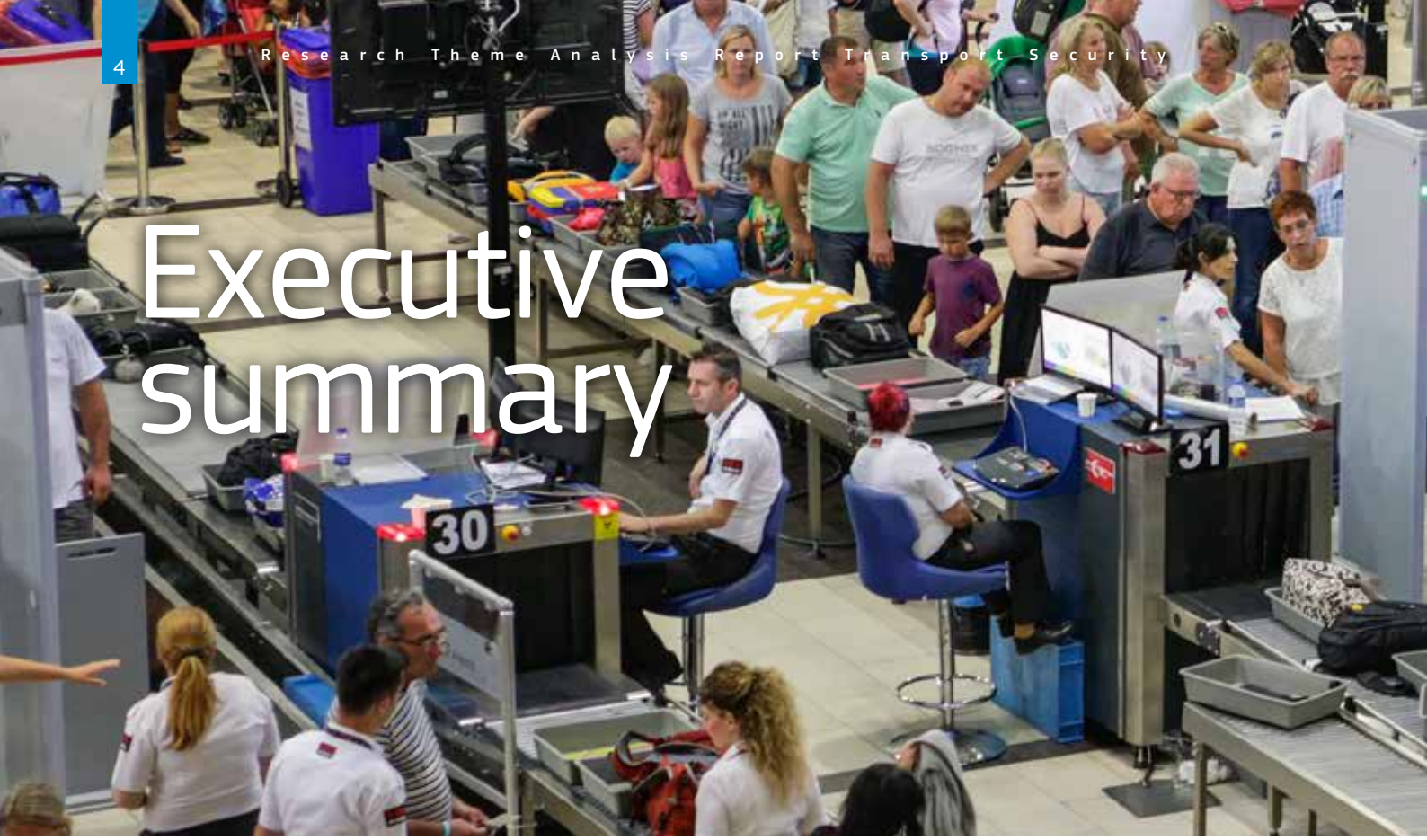
More information on the European Union is available on the Internet (http://europa.eu)

Cover photographs: © Shutterstock
Internal photographs: © Shutterstock

Research Theme Analysis Report

Transport Security

Contents



Executive summary

This is the fourth Research Theme Analysis Report produced under the Transport Research & Innovation Portal (TRIP) Continuation project for the European Commission's Directorate-General for Mobility and Transport (DG-MOVE), which began in November 2014. It covers the research theme Transport Security.

The purpose of TRIP is to collect, structure, analyse and disseminate the results of European Union (EU) supported transport research, research financed nationally in the European Research Area Network (ERA-NET) and selected global research programmes. The TRIP web portal can be found at www.transport-research.info.

The purpose of this Research Theme Analysis Report is to provide an overview of research performed (mostly) in the EU collated by TRIP, providing a view across many projects that fall under the theme. It reports a robust and thorough assessment of the reported results from the research projects, giving scientific and policy perspectives.

For the purpose of this review, the theme of Transport Security has been divided into six sub-themes and the assessments have been performed within each sub-theme and across the complete theme. The sub-themes considered are:

- threat detection and prevention;
- crisis management;
- cyber security, privacy and information and communications technology (ICT) systems;
- staff security training;
- cargo security;
- passenger security.

The key findings from a scientific perspective are:

- A lot of the research on transport security has developed approaches, methodologies and guidelines or focused on the development and testing of technologies that have the potential to facilitate improved security, reduce casualties or improve the resilience of the passenger transport system. In many cases, the involvement of operators and industry representatives (e.g. vehicle manufacturers or terminal operators) suggests that the results of the research will have informed relevant procedures and design specifications.
- The training of staff and passengers in security procedures can provide significant benefits in enhancing security. Research projects have developed more effective training courses by using the latest technology. It is important that training is kept up to date to ensure it continues to be relevant to emerging threats.
- Cyber security is an emerging focus for research projects. Future research in this domain should continue to focus on the deployment, compatibility and privacy protection of different information technology (IT) systems, while increasing the cooperation of different stakeholders and actors. A particular focus might be on the land transport sector. This will have particular relevance as road transport (in particular) begins to exploit emerging technologies and domains such as the Internet of Things (IoT), cloud computing and connected vehicles.

The key findings from a policy perspective are:

- Policy on passenger security needs to continue to develop at different administrative levels to reflect changing security threats. The results of EU research needs to be disseminated and integrated into policy making, as appropriate. The results of research relating to vehicle design could be integrated into EU standards, or communicated internationally if it applies to aviation or international maritime transport. Findings relating to terminal design or safety procedures could be integrated into guidance at the appropriate level, which could range from global or EU guidelines to local design guides, depending on the mode and subject matter.
- Future policy development should take account of the need for a more universal and integrated approach to transport security across transport modes.
- The definition of standards and processes as well as the cooperation between actors is to be underpinned with clear rules and guidelines. This need is particularly evident in the rail and public transport sectors where local operators have a key role.
- Research in the domain of transport security has shown beneficial implications for cross-border intra-EU and international freight and passenger transport. Work is required to transfer the results of research into EU and national policy frameworks.
- In the aviation and maritime sectors, the legislative framework has evolved rapidly in recent years. Although the Port Security Directive (2005/65/EC) is still to be fully implemented in most Member States, the introduction of security standards has led to improved organisation of key nodes such as seaports and airports. Research projects demonstrated that the level of security in railway and metro stations can be improved.
- The need for EU-wide security requirements and standards for road and rail transport is something that cannot be postponed. Research should support the development of EU legislation addressing land transport security.

The priority research gaps identified are:

- Research will continue to be needed in response to the ever-changing nature of the security threat that faces the EU's passenger transport networks. The technology that is used to counter these threats is developing rapidly. Research must ensure that developments in ICT are applied for transport security purposes, including monitoring, threat prevention and for dealing with emergencies as they occur. Research into scanning technologies that might be applied on different modes in a way that does not greatly inconvenience passengers needs to be taken forward.
- Further research in the crisis and emergency management domain is needed for the development of more integrated solutions across all modes of transport that would make it possible to overcome sectoral approaches. The use of 'big data' for better management of crisis situation and improvements to humanitarian logistics are also aspects that deserve broader investigation.
- The system-wide approach to the design and evaluation of airport check-in systems should be also be applied to the different aspects (including behavioural elements) of the security surrounding all passenger transport modes. There is a big potential for the development and use of new technologies to counter threats and monitor security on board passenger trains. Research is required on how best to transfer the concepts from airports to the particular circumstances of vehicle boarding in other transport modes.

1 Introduction

This is the fourth Research Theme Analysis Report produced under the Transport Research & Innovation Portal (TRIP) continuation project for the European Commission's Directorate-General for Mobility and Transport (DG-MOVE), which began in November 2014. It covers the Transport Security research theme.

The purpose of TRIP is to collect, structure, analyse and disseminate the results of European Union (EU) supported transport research, research financed nationally in the European Research Area Network (ERA-NET) and selected global research programmes. The TRIP web portal can be found at www.transport-research.info.

This Research Theme Analysis Report gives an overview of research performed (mostly) in the EU collated by TRIP, providing a view across many projects that fall under the theme title. It provides an assessment of the reported results from these projects and offers perspectives from scientific and policy points of view.

This assessments aims to consider:

- overall trends in transport security, including key results;
- overall trends in the funding for transport security research;
- the alignment of the research with current policy;
- policy implications of the results from the research;
- any gaps within the research theme.

The theme for this analysis was decided in consultation with DG-MOVE.

The assessments for this analysis have been performed on six sub-themes within the theme of Transport Security. The set of sub-themes, selected following initial assessments of the projects and in consultation with DG-MOVE, consists of:

- threat detection and prevention;
- crisis management;
- cyber security, privacy and information and communications technology (ICT) systems;
- staff security training;
- cargo security;
- passenger security.

The projects identified have been clustered under these sub-themes. The analyses of the trends and gaps have been performed across the projects in these sub-themes and across the full Transport Security theme. The assessments of trends and gaps are mainly based on selected projects within the TRIP database.

Projects funded by the European Commission align with EU policy through the funding and selection process. As such, the trends identified from these projects may not necessarily be representative of those from further afield.

Section 2 of this report presents the policy context of transport security and Section 3 describes the scope of this theme analysis. The subsequent sections then present reviews of the individual sub-themes (as specified above), the research environment and development, and the research activities and outcomes. Conclusions and recommendations are then presented at the end of the report.

The preparation of this report has involved the analysis of a large number of projects related to the Transport Security theme. Most were identified from the TRIP database, others were identified from other sources. To enhance readability, the text of this report refers to projects by their standard acronyms (where an appropriate one exists). More details of the projects, including the full titles, are given in the tables at the end of each sub-theme section.

2 Policy context

2.1 Transport security in European transport policy

Transport systems have always been subject to illicit acts against passengers, freight, infrastructures and vehicles. Such acts include anything from relatively minor criminal damage on the premises of transport providers, graffiti on vehicles, crimes against passengers or cargo thefts from lorries to major acts of piracy, hijacking and terrorism that have higher physical and psychological costs. Cyber attacks to information and communications technology (ICT) systems and on passengers' privacy are also unlawful acts. These are increasing in frequency and may have a major impact on the functioning of transport systems and on people's confidence in using new electronic devices – especially having their personal data recorded.

Transport security is a highly sensitive issue and has an important international dimension. The free movement of people and cargo, and the extra-European Union (EU) cross-border dimension of international trade and transport need actions to be taken at the EU level and in coordination with transport security policies developed at global, national and local levels.

In its 2011 Transport White Paper[1], the European Commission set the ambitious objective of becoming a world leader in the safety and security of transport in all transport modes by 2050. The Commission places transport security at the top of the EU's agenda, looking particularly at the land transport sector. Here, common requirements and standards are absent and not comparable to those already existing in the aviation and maritime sectors, which were developed in accordance with the International Civil Aviation Organization (ICAO), the International Maritime Organization (IMO) and in close cooperation with third countries.

The policy context for aviation, maritime transport and land transport security policies is presented in the following sections.

2.1.1 Aviation

Prior to 11 September 2001, aviation security in the EU was the responsibility of each EU Member State. Following the terrorist attacks in the United States of America (USA) in 2001, the EU decided to develop a common EU aviation security regime aimed at protecting people and goods from unlawful interference with civil aircraft.

Therefore, common rules were established in 2002 with the adoption of framework Regulation (EC) No 2320/2002 of the European Parliament and of the Council. This was largely based on international standards for aviation security as laid down in Annex 17 of the Chicago Convention[2] and further developed through ICAO. However, in the following years, a more detailed harmonisation of the European rules became necessary. This was driven by the need for more flexibility in adopting security measures to meet evolving risks and to allow new technologies to be introduced. The initial Regulation was replaced by Regulation (EC) No 300/2008 of the European Parliament and of the Council.

Common basic standards at the EU level comprise:

- screening of passengers, cabin baggage and hold baggage;
- airport security (access control, surveillance);
- aircraft security checks and searches;
- screening of cargo and mail;
- screening of airport supplies;
- staff recruitment and training.

Since 2009, several supplementary regulations entered into force as regards liquids, aerosols and gels; the use of security scanners; the adoption of alternative security measures; controls of air cargo domestically and internationally; the specifications of national quality control programmes; and procedures for conducting Commission inspections in the field of aviation security. In 2016, the whole set of previous implementing legislation was updated with Commission implementing Regulation (EC) No 2015/1998 that indicated detailed measures for implementing the common basic standards on aviation security.

The European aviation security policy is defined in close collaboration with Member States and various stakeholders, but also working with ICAO, third-country partners and regional organisations. The overall aim is to ensure the proper balance between the security and other important aspects, such as travel convenience, privacy and protection of personal data, and other operational factors.

1 Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system (COM(2011)144), European Commission, 2011.
2 Convention on the International Civil Aviation signed on 7 December 1944.

In recent years, the efforts to achieve this balance and improve the overall EU civil aviation security policy focused on:

- the general use of security scanners at EU airports;
- the replacement of the ban on liquids, aerosols and gels with secure screening procedures;
- the security of EU-bound cargo and mail departing from airports outside the EU;
- the transparency, cost-relatedness and non-discrimination when levying charges at airports.

For passenger screening, the eligible methods and technologies as laid down in the European legislation are:

- hand search;
- walk-through metal detection equipment;
- hand-held metal detection equipment;
- explosive detection dogs;
- explosive trace detection.

Following an attempted terrorist attack on an aircraft that departed from Amsterdam on 25 December 2009, which involved explosives concealed on a passenger, the Commission worked on improving the legislative framework by introducing the use of security scanners at EU airports. In June 2010, a Commission Communication on the use of security scanners was released, together with a related impact. The Communication confirmed security scanners as being a valid alternative to the approved screening methods as they are capable of detecting metallic and non-metallic items carried by a person. The EU legal framework on security scanners, integrated into the Implementing Regulation (EU) 2015/1998, was adopted in November 2011.

In March 2013, the Commission adopted the first necessary legal changes to implement a stepped approach for replacing the restriction on the carriage of liquids, aerosols and gels with technological screening. Phase 1 started in January 2014 with passengers being able to carry duty-free liquids, liquid medicines and liquids needed for special dietary requirements as long as they are screened by dedicated equipment. An impact assessment study carried out after some months concluded that there was no operational impact from this first phase. However, a subsequent study revealed potential negative impacts on throughput and cost for EU airports if passengers were permitted to carry bottled water as well. Therefore, the Commission decided to postpone the introduction of the second phase of lifting the liquid restrictions.

The EU has a robust and well-established air cargo and mail security regime that requires all cargo and mail to be physically screened or come from a secure supply chain before being loaded onto an aircraft. Since 1 February 2012, additional rules require air carriers carrying cargo and mail into the EU from non-EU airports to ensure security standards are complied with prior to loading.

Air carriers that fly air cargo or mail into the EU from a non-EU airport are required to comply with the EU 'Air Cargo or Mail Carrier operating into the Union from a Third Country Airport' (ACC3) programme for inbound cargo and mail. Only air carriers that comply with this programme can be designated as ACC3 and may carry cargo or mail into the EU. ACC3s must ensure that all cargo and mail is physically screened according to EU standards or comes from an EU aviation security validated secure supply chain. These rules have been mandatory since 1 July 2014.

An interface between the European Organisation for the Safety of Air Navigation (Eurocontrol) information technology (IT) systems and the 'Union database on supply chain security' has been also established. This enables Member States to identify aircraft arriving from airports located in third countries where the air carrier has not been designated as an ACC3.

2.1.2 Maritime transport

The EU regulatory framework dealing with maritime security is based on Regulation (EC) No 725/2004 on enhancing ship and port facility security and the so-called Port Security Directive (2005/65/EC).

Regulation (EC) No 725/2004 provides a basis for the harmonised interpretation, implementation and European Community monitoring of the special measures to enhance maritime security adopted by the IMO in 2002. This amended the 1974 International Convention for the Safety of Life at Sea (SOLAS Convention) and established the International Ship and Port Facility Security Code (ISPS Code). The Regulation makes mandatory a number of recommendations introduced into Part B of the ISPS Code.

The security measures introduced by Regulation (EC) No 725/2004 have been complemented by the Port Security Directive, so making an entire port subject to a security regime and enhanced security measures. The objective of the Port Security Directive is to improve security in areas of ports not covered by Regulation (EC) No 725/2004 and to ensure that the enhancement of port security can support the security measures taken under the Regulation. The Port Security Directive provides for mechanisms to implement these measures and check their conformity. The legislation also requires that ships and port facilities have plans for three levels of security, giving different levels of readiness in response to the perceived threat level.

The Commission has been given the obligation by the European Parliament and the European Council to monitor the implementation by Member States of Regulation (EC) No 725/2004 and the Port Security Directive, and to verify the effectiveness of national maritime security measures, procedures and structures. To fulfil this task, the Commission adopted Regulation (EC) No 324/2008 on procedures for conducting Commission inspections in the field of maritime security.

The Regulatory Committee for Maritime Security (MARSEC) was established by Regulation (EC) No 725/2004 to assist the Commission in its functions and activities, and consists of experts representing all Member States. Best practices and indications on national instructions have been shared in this forum. Recently, it was agreed to create a mechanism for secure mutual information sharing where each Member State could insert sensitive information (e.g. security levels adopted, threat evaluations and others topics relevant for the security of European shipping). Also, a Stakeholder Advisory Group on Maritime Security (SAGMaS) has been established where members can express their views on the work of MARSEC.

In 2013, the Commission released a second assessment report, covering the period 2009-2013, on progress made in implementing the Port Security Directive. The report shows that the measures needed to implement all provisions of the Directive in full still need to be improved in most Member States. However, the legislative framework allowed an improved level of prevention of security breaches in ports and achieved adequate protection for maritime and port activities. The introduction of security measures has often led to a review of the organisation of ports, such as the movement and storage of goods, the control of access to different areas of the port and the definition of restricted areas.

A study on the technical aspects of port area security (TAPS II) and the implementation of the Port Security Directive was carried out in 2011 by the European Commission's Joint Research Centre's[3] (JRC) Institute for the Protection and Security of the Citizen. The objective of the study was to help establish common criteria for meeting the objectives of the Port Security Directive by drawing up minimum standards, recommendations and guidelines; and collating best practices. A methodology with two successive stages of checks was developed – one defining port facilities and characteristics forming part of the port, and the other identifying, by means of a risk analysis, the port boundaries so as to establish the most efficient port security.

In the area of international trade in goods, customs authorities in the EU apply a risk-based approach to security threats based on the Community Risk Management Framework, the Community Risk Management System and the EU Authorised Economic Operator (AEO) Programme. EU customs authorities receive, in advance, cargo information for risk analysis purposes on all cargo coming from or going to third countries. Economic operators certified as an AEO that voluntarily invest in improving the security of their supply chains on international trade routes are entitled to some facilitation benefits.

In 2010, in response to the resurgence of acts of piracy, the European Commission adopted a Recommendation (2010/159/EU) on measures for self-protection, and the prevention of piracy and armed robbery against ships. A best management practice scheme to deter piracy in the Gulf of Aden and off the coast of Somalia was developed to assist companies and ships in avoiding piracy attacks, deterring attacks and delaying successful attacks.

3 European Commission's science and knowledge service.

2.1.3 Land transport

Unlike the aviation and maritime sectors, and except for dangerous goods movement, there is no EU legislation addressing land transport security.

The Commission's 2011 Transport White Paper indicated the need to find an appropriate European approach to land transport security in those areas where EU action has an added value. This is also underlined in the Commission Communication 'The EU Internal Security Strategy in Action: Five steps towards a more secure Europe'. This states that there is scope and justification for a more active European approach to the broad and complex area of land transport security and, in particular, to the security of passenger transport.

EU transport ministers have, to date, not requested the Commission to bring forward any legislation for EU security requirements for road or rail transport.

As recommended in the Transport White Paper, a permanent EU Expert Group for Land Transport Security (LANDSEC)[4] was set up in 2012 to provide a forum to discuss issues with Member States and stakeholders, and to exchange relevant experience, policies and practices between Member States and the various parties involved.

At the same time, the Commission adopted a Staff Working Document on Transport Security[5], which provided an overview of potential areas for the development of EU land transport security policies. In particular, the document highlighted the need to focus on:

- multimodal transport interchanges and mass transit security, including rail/metro stations and car parks at airports;
- EU-wide security standards for the high-speed rail network and security features to be incorporated into the design of rail and metro rolling stock, and infrastructure;
- training staff working in land transport (mandatory training for security staff and awareness training for all people working in the land transport domain);
- contingency planning for the aftermath of an incident and transport recovery plans;
- pre-defined standards for transport security technology and equipment;
- research on transport security;
- better communication and sharing of classified information (i.e. similar to the exchange of threat and risk information now in place in the air cargo and mail security domain);
- security of the supply chain and secure lorry parking;
- cyber crime against transport;
- inland waterway transport.

The Staff Working Document also included an overview of projects funded under the 7th Framework Programme for Research and Technological Development (FP7) that have transport security relevance organised by mode of transport.

After the attack on the Brussels metro and airport on 22 March 2016, metro and rail security has been added to the LANDSEC agenda.

4 http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2821

5 'Commission Staff Working Document – Transport Security', SWD(2012) – 143 final, https://ec.europa.eu/transport/sites/transport/files/themes/security/doc/2012-05-31-swd-transport-security.pdf

2.2 Transport security in European research programmes

Past and ongoing EU research projects have been scrutinised during the preparation of this Research Theme Analysis Report. The screening revealed that a very limited number of transport-related projects focused on transport security prior to FP7. In line with the EU legislation on maritime and aviation sectors, projects focused mainly on these two areas.

The topic of secured maritime and cargo 'black boxes' was analysed in two projects in FP4 and FP5. Some FP6 projects focused on monitoring and information services, and on infrared sensing assistance to clandestine weapon surveillance (e.g. FP6 – Aerospace).

In FP7, EU-funded research started to pay attention to civil security (anti-terrorism and crisis management) under the specific programme 'Cooperation' and a budget of EUR 1.4 million was allocated. The research aimed to generate new knowledge and promote the application of new technologies in the field of civil security. In particular, it addressed the areas of:

- security of citizens (technology solutions for civil protection, bio-security and protection against crime and terrorism);
- security of infrastructure and utilities (examining and securing infrastructure in areas such as information and communications technology (ICT), transport, energy, and services in the financial and administrative domain);
- intelligent surveillance and border security (technologies, equipment, tools and methods for protecting Europe's borders (e.g. land and coastal borders));
- restoring security and safety in case of crisis (technologies and communication, and coordination in support of civil, humanitarian and rescue tasks);
- security systems integration, interconnectivity and interoperability (information gathering for civil security, protection of confidentiality and traceability of transactions);
- security and society (acceptance of security solutions; socio-economic, political and cultural aspects of security; ethics and values; social environment and perceptions of security);
- security research co-ordination and structuring (co-ordination between European and international security research efforts in the areas of civil, security and defence research).

The Horizon 2020 Programme marked the security topic as one of its main priorities ('making transport and transport systems seamless: better mobility, less congestion, greater safety and security') and identified security as a dedicated research area. The Horizon 2020 Programme specifically addresses security topics in the Challenge 'Secure societies – Protecting freedom and security of Europe and its citizens' (budget EUR 1.7 million). This Challenge is aimed at:

- enhancing the resilience of society against natural and man-made disasters – ranging from developing new crisis management tools to ensuring communication interoperability and developing novel solutions for the protection of critical infrastructure;
- fighting crime and terrorism – ranging from developing new forensic tools to protecting against explosives;
- improving border security – ranging from improved maritime border protection to supply chain security and supporting the EU's external security policies (including conflict prevention and peace building);
- providing enhanced cyber security – ranging from secure information sharing to new assurance models.

Over the last 5 years, the JRC has launched several projects related to maritime and aviation transport. In the maritime sector, the JRC contributed to the development of the European Border Surveillance System (EUROSUR) and the Common Information Sharing Environment. In addition, the JRC developed the ConTraffic[6] research project to provide information on container routes and risk assessment services to customs and security authorities.

As part of JRC's expansion into the field of aviation security and explosives detection, it is developing its experimental capacity, which is intended to establish a large-scale testing facility that will equip the European Commission with an in-house, independent capability to test aviation security detection technologies. The JRC is also studying the feasibility of deploying new technologies, such as the use of composite materials fitted with embedded sensors that can detect possible threats and wirelessly communicate their status to competent authorities, easing customs operations. These activities are condensed into the European Reference Network for Critical Infrastructure Protection (ERNCIP) and its project platform,[7] and the Disaster Risk Management Knowledge Centre in the areas of crisis management.

6 https://contraffic.jrc.ec.europa.eu/
7 https://erncip-project.jrc.ec.europa.eu/

3 Scope of the Transport Security theme

Security is a major factor that can affect the regular functioning of passenger and freight transport systems and operations; and the attitude of transport users, providers of transport services and policy makers.

People should have the right to travel without fear of being a victim of any criminal act and preventive actions against cargo theft should be enforced to reduce the growing economic and social costs of transport crime.

The EU has experienced a number of terrorist attacks on transport, including the bombs in the Saint-Michel metro station in Paris (1995), the attacks on the urban rail nodes in Madrid (2004) and London (2005), and the suicide bombings that occurred at the airport and Maalbeek metro station in Brussels on 22 March 2016. The high number of passengers in the aviation and rail sectors and the relative 'openness' of the networks demonstrate that transport systems are difficult to protect.

The approach to this Transport Security thematic review was to cluster research projects under a number of limited, but relevant, sub-themes to focus on emerging issues (e.g. cyber security and staff security training) and more traditional topics such as developing new technologies for threat detection and prevention, and crisis management.

The selected sub-themes are:

- **Threat detection and prevention** – the ability of the transport system to detect and prevent criminal acts, cargo theft on transported cargo, acts of piracy (physical or hijacking) and terrorist attacks is largely linked to the protocols, procedures and technologies able to limit such risks. Therefore, this sub-theme includes all those projects dealing with monitoring and surveillance systems (such as closed-circuit television (CCTV) and sensors), physical interfaces (at gates or land checkpoints) and solutions to detect risks. The sub-theme considers projects linked to long-distance detection, multi-hazard approaches and risk assessment.
- **Crisis management** – in case of a major disruption, attack or an emergency situation, the transport system must be able to manage its own functioning (e.g. at reduced operations or primarily to rescue passengers and protect goods during the crisis). Therefore, this sub-theme includes all those systems, technologies and procedures able to accomplish such crisis operations.
- **Cyber security, privacy and information and communications technology issues** – the rising dependency of transport on functioning IT systems needs security to be strictly embedded in the design of such systems, thus preventing threats from cyber attacks. The aspect of cyber resilience is also relevant (i.e. the capability of IT systems to operate transport infrastructure and services in case of a failure, and procedures for re-establishing control in case of attacks). Last, but not least, privacy issues are relevant in case of personal data management with implications for ethics and transparency.
- **Staff security training** – having skilled and well-trained staff is a fundamental component of every security system. In addition to regular training programmes, specific education and training procedures can be conducted when new technologies or solutions are introduced. This sub-theme is partly devoted to the analysis of projects dealing with the training of staff (not only specialised security staff or rescue teams but, in particular, staff working in transport operations that might face critical situations). It also considers how training issues (contents and frequency of training) are taken into account in projects dealing with threat detection and prevention, and crisis management.
- **Cargo security** – this sub-theme is focused on all those improvements in vehicles, aircraft, vessels, cargo units and the efficiency of the supply chain that have impacts on freight protection in transport systems. It also includes non-technological aspects such as regulations, standards and framework conditions.
- **Passenger security** – this sub-theme aims to analyse innovations and security provisions for passenger vehicles, aircraft and vessels; and advancements and security provisions at airports, railway stations and transport interchanges in general. It also encompasses studies on passenger behaviour.

4 Sub-theme assessments

This section describes the assessments of each of the sub-themes in turn. For brevity, when discussing individual projects, the descriptions refer to those projects by their acronym (particularly for projects funded by the European Union (EU), which commonly have an acronym as well as a full project title). Further information on the projects that are relevant to the sub-theme, including the full project title, is given in the tables at the end of each sub-theme section.

4.1 Threat detection and prevention

4.1.1 Introduction to the sub-theme

Threat and vulnerability identification and detection are the starting points of the threat-protection process. This sub-theme reviews research projects aimed at developing methods, processes and tools to identify threats and risks, and to detect identified threats. Through early detection, threats might be neutralised or mitigated. Therefore, new technological developments are used to support threat detection and, consequently, prevention. Notably, sections of the transport network are vulnerable to different threats and prevention measures, and tools have been developed to this effect. Furthermore, the transport network is an integral part of the built environment and requires international cooperation on threat detection and prevention. Projects addressing these topics are also included in the analysis.

A total of 78 research projects were identified under this sub-theme. Of these, 71 were funded by EU research programmes, while 7 were funded by national programmes. Table 4 1 (section 4.1.4) provides a summary of these research projects with their duration and source of funding. It should be noted that a considerable number of projects under this category are either nearing completion or ongoing. Therefore, detailed information is not yet available on their outcomes. Nevertheless, short profiles (from the Transport Research & Innovation Portal (TRIP)) are used here to identify project objectives with the aim of gaining insight into the direction of current and future research. Finally, the sub-theme includes projects whose outcomes could also be applied in security detection and prevention.

4.1.1.1 Overall direction of European-funded research

The EU-funded research on security threat detection and prevention has witnessed very substantial development efforts aimed at creating and using new intelligent and innovative technologies. Several research projects funded by the European Commission have been identified under this sub-theme and cover a variety of topics. In addition, threat detection and prevention is part of wider security systems that have been analysed and developed in a number of projects. Research efforts may be categorised with respect to their scope or their particular emphasis on a specific sector responding to particular needs. Research focused on risk/threat identification, assessment and management has been delivered over many years. Notably, as the nature of threats has changed, the emphasis has also widened to incorporate new developments. New technologies have been developed for use in threat detection and prevention. Finally, given the international dimension of transport security, support projects and activities have also been initiated through EU-funded initiatives.

Figure 4-1 shows the distribution of these project categories over time, based on the year they were awarded. The figure indicates the continuing interest in risk assessment and management, as well as support activities to raise awareness and streamline approaches. The figure also shows the continuous effort in the development of new technologies for threat detection, while the importance of improving efficiency and introducing seamless controls has recently become more important.

Figure 4-2 shows the evolution over time of projects that address needs in specific sectors. Security in air transport has been the prominent sector of research over the years. However, as the vulnerability of other sectors is identified, research has extended to address the needs in security threat detection and prevention in them. In recent years (e.g. through the Horizon 2020 research programme), all transport sectors have been included in the research programme, including critical infrastructure. Notably, there is a challenge in transferring knowledge, good practices and applications from one sector to another, especially with respect to checkpoints and screening of passengers and goods. Finally, a recent focus on ethics and social impacts of security measures has been identified.

4.1.1.2 Overall direction of nationally funded projects

A total of seven national research projects were identified under this sub-theme – Czech Republic (one project), Slovakia (one project), Portugal (one project), Spain (one project), Switzerland (two projects) and the UK (one project). These covered a wide range of issues targeted at different transport modes/sectors. No overarching trend can be seen. As a general observation, projects that were completed in the middle of the last decade involved nationally driven initiatives with a focus on theoretical analyses to improve procedures for the safety and security of passengers (e.g. rail, parking). However, a shift to technological solutions to detect risk in security systems and telecommunications infrastructure is evident in most recently completed projects. As with EU-funded research, ongoing projects focus on more sophisticated solutions for radio communication, and on integrating risk assessment and management processes into the functionality and resilience of critical infrastructure.

Figure 4-1 Evolution of the number of threat detection and prevention projects per scope

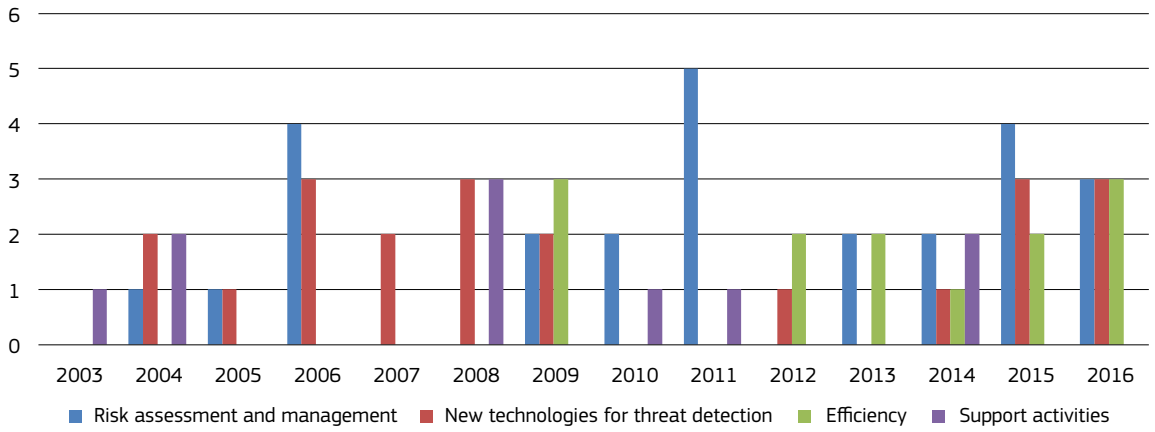
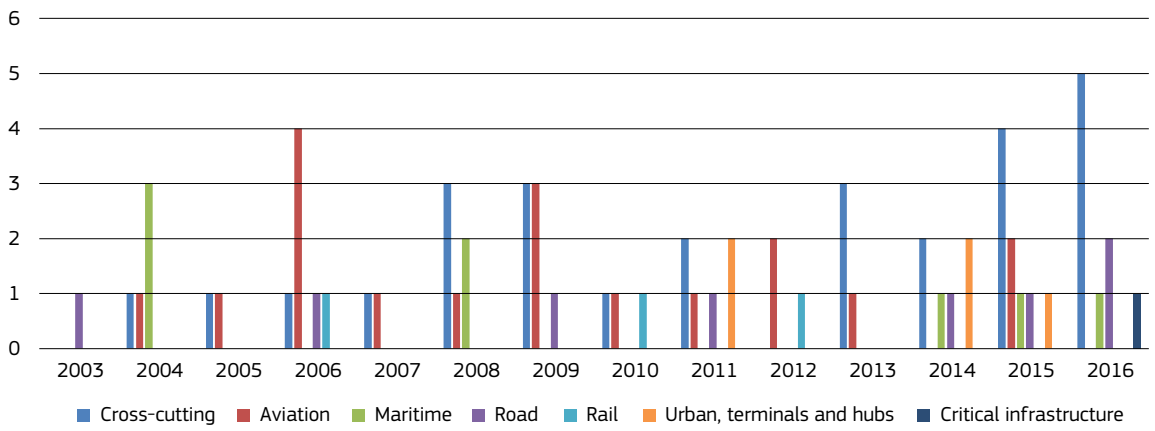


Figure 4-2 Evolution of the number of threat detection and prevention projects addressing specific sectors



4.1.2 Research activities

4.1.2.1 Risk/threat identification, assessment and management

For a significant number of research projects (27 EU-funded and 5 nationally funded), the preliminary scope included identifying, assessing and managing threats facing the transport system and providing the assessment frameworks and guidance. Projects identified include:

- COUNTERACT (2006-2009) – this aimed to assess the state-of-the-art, and identify, prioritise and assess the needs for security policies and concrete measures within the transport and energy sectors. The project focused on the protection of critical transport infrastructure, public transport passengers and goods.
- SeRoN (2009-2012) – this aimed to develop an innovative hazard analysis methodology for possible terrorist attacks on critical road transport networks, or parts thereof, and evaluate planned protection measures for critical road transport infrastructure, including their impact on security and cost-effectiveness.
- STAR-TRANS (2009-2012) – this aimed to develop a holistic transportation security risk-assessment framework for critical infrastructure and apply it to a wide range of international transport infrastructure. The project included analysing and assessing common issues for risks, threats and vulnerabilities; identifying possible interdependencies; and assessing the impact of failures on interconnected infrastructure.
- AllTraIn (2013-2015) – this aimed to develop a comprehensive, structured, all-hazard guide for critical transport infrastructure in Europe.
- Process model of critical infrastructure safety and protection in the transport sector (2015-2018) – a national project (Slovakia) that aimed to develop a hierarchical model for the classification of management safety levels and the effective protection of critical infrastructure elements in the transport sector.

The ECOSSIAN (2014-2017) project plans to develop a holistic system for incident detection and management at all levels. The prototype system will facilitate preventive functions such as threat monitoring, detection of early indicators and real threats, alerting, support of threat mitigation and disaster management. In addition, the CIPSEC (2016-2019) project will create a unified security framework that orchestrates state-of-the-art heterogeneous security products to offer high levels of protection in information technology (IT) and operational technology departments of critical infrastructure.

With regard to resilience, the RESOLUTE (2015-2018) project will conduct a systematic review and assessment of the state-of-the-art of the resilience assessment and management concepts as a basis for the development of a European Resilience Management Guide (ERMG). The IMPROVER (2015-2018) project will develop a cross-sectoral methodology on risk evaluation that will include combinations of social, organisational and technological resilience concepts providing input to standardising the security of infrastructure.

The SIAM (2011-2014) project developed a decision-support system to simplify the process of assessing security measures and technologies, so providing a systematic approach for measuring their potential impact. The ASSERT (2013-2014) project developed tools and methodologies to measure the social impact of security research. Finally, acknowledging the need for a deeper understanding of organised crime and terrorist networks, the TAKEDOWN (2016-2019) project aims to generate novel insights into these areas.

While the above projects may apply across all transport sectors, many others are focused on specific needs concerning:

- Aviation:
  - The TASS (2010-2014) project aimed to create an entire airport security monitoring solution, providing real-time accurate situational awareness to airport authorities at several levels, modes and segments.
  - The FLYSEC (2015-2018) project will complement the efforts by the Airports Council International (ACI) and International Air Transport Association (IATA) to develop and demonstrate an innovative integrated and streamlined security process for passengers, from landside to airside and into the boarding gates.
  - The COPRA (2011-2013) project dealt with the continuing technological evolution and proliferation of civil aviation threats and the respective security procedures and new technologies. The project released the Aviation Security Research Roadmap compiling more than 350 possible security measures and over 50 conceptual ideas for overarching approaches for cargo, passenger and external security concepts.
  - The FLYSAFE (2005-2009) project was the first decisive big step towards 'VISION 2020' produced by the Advisory Council for Aviation Research and Innovation in Europe (ACARE) for safety in flight operations. Its novelty lies in the design, development, testing and validation of a complete Next Generation Integrated Surveillance System (NG ISS), focusing particularly on the main types of accidents around the world – loss of control, controlled flight into terrain, and approach and landing accidents.
  - The VULCAN (2006-2010) project investigated the vulnerability of composite and hybrid structures to blasts and fire incidents. It also considered possible reinforcing measures and novel aircraft materials with the aim of improving the resilience of current aircraft.

- Maritime:
  - The national Security tool for risk analysis in harbour installations (2008-2009, Spain) project produced a uniform and global solution that is applicable to all port installations in security and risk management matters, and facilitates the integration of all security technologies in use to enable the establishment of common procedures in every seaport.
  - The main objective of the MARNIS (2004-2008) project was to improve safety; the protection of the environment; security; efficiency and reliability; and the economic, legal and organisational aspects of sea transport.
- Road:
  - A number of projects focused on road safety affected by impaired driving under the influence of alcohol and substances (such as the DRUID (2006-2011) project), and on the prevention of suicides (such as the Suicide prevention on bridges Fundamentals (2004-2006) and RESTRAIL (2011-2014) projects).
- Rail:
  - The PROTECTRAIL (2010-2014) project attempted to improve the interoperability of asset-specific solutions for ensuring railway security. It aimed to conceive and design a modular architectural framework into which each asset-specific solution can be 'plugged' to provide a streamlined and integrated system of security solutions.
  - The RAILPROTECT (2006-2009) project aimed to reduce the vulnerability of rail station infrastructure and rolling stock to explosions by assessing this vulnerability via numerical simulations of the blast effects.
- Urban transport, terminals and hubs:
  - The SECURESTATION (2011-2014) project aimed to improve passenger station and terminal resilience to terrorist attacks and safety incidents through the use of enhanced technologies and design methodologies to reduce impacts.
  - The SECUR-ED (2011-2014) project aimed to set up a pan-European improvement in mass transportation security through the development of packaged modular solutions validated through demonstration and made available to the full community of operators.
  - The PANDHUB (2014-2017) project will create an integrated toolbox to aid transport operators and relevant actors in major transport hubs in the development of their current pandemic and dangerous pathogen preparedness and response plans.
  - The Reducing Crime at Rail Stations in Socially Excluded/ High Crime Locations (2005) project was a UK national project with respect to the assessment of risks/threats in rail stations.
  - The Safety and comfort of car parks (2001-2005) and BIRDWATCH (2015) projects dealt with threat detection in parking facilities.
- Critical infrastructure:
  - The RESILIENCE (2015-2019) project aims to conduct research focusing on a dynamic correlation evaluation of significant sectors in the EU (energy, transport and information and communications technology (ICT)). The analysis will include descriptions of the synergistic effects of these systems, their failure mechanisms and a dynamic evaluation of these failures on the resilience of critical infrastructure.
  - The SmartResilience (2016-2019) project aims to benchmark best-practice solutions by identifying new 'smart' resilience indicators, based on which new advanced resilience assessment methodology and related tool is developed.

4.1.2.2 Exploitation of technology advances

Monitoring and surveillance systems lie at the core of threat detection. A total of 21 EU-funded and 2 nationally funded projects focused on technology applications to provide real-time information on infrastructure status. These systems are often integrated with emergency management systems, such as the one designed by the ISTIMES (2009-2012) project. This exploits distributed and local sensors for non-destructive electromagnetic monitoring to provide fast and reliable multi-hazard and risk-management monitoring and damage assessment due to multiple-technology integration. Other technologies developed include:

- thermal infrared hyperspectral sensing for clandestine weapon surveillance (the HAWKEYE (2005-2009) project);
- a transportable system making use of optical technologies for the stand-off detection and identification of explosives in real scenarios at long distances (the OPTIX (2008-2013) project);
- a novel network of sensors incorporating a disruptive technology known as controlled magnetic field that are easily camouflaged (the WARDIAM PERIMETER (2016) project);
- turning street lighting fixtures into multipurpose electronic cells that can facilitate data transmission between traffic participants and data centres, increasing the security of traffic and public places (the Intelligent Infrastructure for Modern City (2012-2014) project);
- overcoming the drawbacks of classical, centralised surveillance by offering a prompt and wide coverage (space and time) system for the unattended surveillance of public transport, maritime transport and other public spaces (the ASPIS (2008-2011) project).

A recent promising technological development that is highly applicable in this field is the use of 'drones' or unmanned aerial vehicles (UAV), which are destined to replace human resources. Therefore, related projects strive to realise the niche application for the technology. Accordingly, the ADS (2015) project addressed these challenges by using a system that controls operations of small 'multicopters' and a network of landing/recharging stations. The system controls navigation, video feeds from the drones and the operation strategy. The EXTREMDRON (2016) project focused on creating a next-generation UAV for aerial monitoring applications in extreme operating environments (fires, radiation/nuclear, hazardous chemicals). The SURVEIRON (2016-2018) project will investigate the use of a set of intelligent robots, embedded inside a fleet of UAVs to provide an intelligent surveillance and decision-making system for critical situations. In addition, the main goal of the INOUI (2007-2010) project was to provide a roadmap for the future of UAVs in the air traffic management (ATM) context, but also to complement Single European Sky ATM Research (SESAR) activities related to the operational concept and architecture.

Notably, all the above outcomes may be applied across most transport sectors.

- Aviation:

Focusing on the landside of airports, a number of projects demonstrate the use of advances in technology:

- The e-Airport (2015-2017) project aims to develop an airport operations monitor application based on European global navigation satellite systems (GNSS) to increase the efficiency, safety and security of aircraft services and cargo processes.
- The OPTAG (2006-2009) project developed a system that enables the immediate location of delayed or missing checked-in passengers. This reduces passenger-induced delays, and enhances (suspicious) passenger identification and threat assessment systems.
- The SKY-Scanner (2007-2010) project aimed to develop a novel laser-tracking technology to detect and track aircraft up to at least six nautical miles from the aerodrome traffic zone (ATZ), thus improving the aircraft security and communications.
- The Slovakian national 'Speaker verification as an add-on element of the Air Traffic Management security' (2015-2017) project is also expected to contribute to this topic.

Regarding aircraft resilience to security threats, SAFEE (2004-2008) envisaged the construction of advanced aircraft security systems designed to prevent on-board threats and to ensure fully secure flights, while influencing security bodies at national, European and global level. As a continuation of the SAFEE work, the SOFIA (2006-2010) project designed architectures for integrating the frequency-response function (FRF) system into several types of avionics for civil transport aircraft. The project developed one of these architectures, validated the FRF concept and the means to integrate it in the current ATM system, and assessed the safety of FRF at aircraft and operational levels.

The CASAM (2006-2009) project designed and validated a closed-loop, laser-based, directed infrared counter measure module for jamming shoulder-launched infrared guided missiles (man-portable air-defence systems (MANPADs)) that complies with the constraints of commercial air transportation, including the aircraft flight profile.

- Maritime:

Key projects dealing with monitoring and surveillance technological solutions include:

- the MERSEA (2004-2008) project that developed an ocean monitoring and forecasting system;
- the SECTRONIC (2008-2011) project that developed and launched a new and revolutionary 'command and control security system' that was designed to protect maritime and land-based assets by automatically creating an intuitive situational awareness picture for detecting, tracking, classifying and deterring security threats;
- the SMARTER (2015) project dealt with marketing the light detection and ranging (LADAR) sensor (developed in recent previous projects), which is able to survey and monitor the surface layer surroundings of vessels, platforms and coastal infrastructure.

- Road:

The EFFISEC (2009-2014) project aimed to provide border officers with up-to-date technologies to enable systematic in-depth checks on travellers, luggage and vehicles (including passengers inside vehicles) through the use of automatic gates and portable identity check and scanning equipment.

- Rail:

Regarding rail transport, the SECRET (2012-2015) project addressed the protection of railway infrastructure against electromagnetic attacks.

- Urban transport, terminals and hubs:

The HOLOSCAN (2014-2015) project proposed a novel approach to high-throughput millimetre wave screening to allow real-time safe screening of large numbers of people moving simultaneously towards the entrances of buildings, public transport or public places.

4.1.2.3 Efficiency in transport security threat detection and prevention

Much research has taken place to reduce delays in traffic imposed by the need to prevent threats through the control of passengers and goods. A number of these projects take into account human behaviour and make respective assessments. For example, the main goal of the Gait Biometrics 3 (2015) project was to create a prototype of a novel biometric solution for highly reliable identification of people, based on the characteristics of their walk.

Most of these efforts were focused on airports and passenger management, such as:

- the Intelligent Luggage (2008-2011, Portugal) project that aimed to develop technology to track luggage items by using embedded smart tag systems;
- the AIR-SEAL (2009-2011) project that investigated the development of an advanced radio frequency identification (RFID) security seal to monitor the integrity of an aircraft galley trolley or transportation vehicle;
- the ATOM (2009-2012) and the SOS (2012-2015) projects that focused on developing innovative surveillance systems able to detect hidden hazardous materials and/or tools and their possessors;
- the XP-DITE (2012-2017) project that will develop and validate a comprehensive, passenger-centred approach to the design and evaluation of integrated security checkpoints at airports.

More recently, considerable emphasis has been placed on facilitating controls at border checkpoints. Recently completed and ongoing projects aim to deliver more efficient technological equipment for threat detection and prevention to land border authorities. These include:

- the iCROSS (2016-2019) project that will design and implement a system to enable faster through-border control for third country nationals crossing EU borders;
- the PROTECT (2016-2019) project that will develop an enhanced biometric-based person identification system to work across a range of border crossing types by adopting strong user-centric features;
- the MobilePass (2014-2016) project that focuses on the research and development of technologically advanced mobile equipment at land-border crossing points that incorporates new technologies needed in mobile scenarios and embeds them in the actual border-crossing workflow to speed up control procedures;
- the BODEGA (2015-2018) project that will investigate and model human factors in border controls to provide innovative socio-technical solutions for enhancing border guards' performance of critical tasks, support border management decision-making and optimise travellers' border-crossing experience;
- the FastPass (2013-2017) project that is investigating combinations of different technologies and advances (biometrics, document authentication and video surveillance) to enhance the security and efficiency of border crossings.

Similarly, in the maritime sector, SafeShore (2016-2018) aims to cover existing gaps in coastal border surveillance by developing a core solution for detecting small targets that fly at low attitude that is integrated with existing systems to create a continuous detection line along the border.

Finally, addressing the human factor:

- the BEMOSA (2009-2012) project improved security by producing a training programme for airport authority personnel to enhance their ability to correctly detect potential security hazards, and by revising and updating their safety and security skills and procedures;
- the ACROSS (2013-2016) project aims to develop, integrate and test new flight-deck solutions and cockpit-based technologies to improve passenger safety by facilitating the management of the peak workload situations that can occur during a flight, so reducing stress for pilots and the number of crew required to operate safely in unpredictable situations.

4.1.2.4 Support actions

In recognition of the international nature of security of the transport network and the need for actors to cooperate and endorse a common approach, some coordination and support actions were funded. Those that may be considered as cross-cutting include:

- the SUPPORT (2010-2014) project that engaged representative stakeholders to guide the development of next-generation solutions for upgraded security capabilities in European ports, encompassing legal, organisational, technological and human factors;

- the GMOSS (2004-2008) project that brought together Europe's civil security research to acquire and nourish the autonomous knowledge and expertise on global monitoring using satellite-based earth observation;
- the HERMES (2011-2014) project that established a common portal for accessing information from databases of past and ongoing research projects in the field of transport technologies in the EU and their counterparts around the world;
- the ESTEEM (2008-2009) project that aimed to enhance and strengthen the links between the Maghreb transport-related research system and three neighbouring EU countries (Italy, France and Spain), focusing on the theme of safety and security of transport systems and infrastructure.

Other actions focused on specific sectors, such as:

- Aviation:
  - The ICOA.10.09 (October 2009) was a two-day international conference on airports and their challenges. It was organised by the Air and Space Academy and held in Paris.
- Maritime:
  - The objective of the OPERAMAR (2008-2009) Support Action was to provide the foundations for pan-European Maritime Security Awareness, as prescribed by the Maritime Policy, by addressing the insufficient interoperability of European and national assets, and generating unified data models for seamless exchange.
  - The EU CISE 2020 (2014-2017) project aims to develop a European test bed for the maritime Common Information Sharing Environment in a 2020 timeframe.
  - The GRAND (2004-2006) project developed a network of regional alliances to coordinate the efforts of states around the world in implementing a global ocean observing system (GOOS).

Also, under the area of support actions, the VERA2 (2003-2004) project, stemming from driver violations at border crossings, resulted in the preparation of a possible future directive on cross-border enforcement, among others.

Finally, the goal of the CARONTE (2014-2016) project was to create an agenda for research on land transport security and provide answers to the question of what type of security-related projects should be planned in the future, considering the current state-of-the-art and existing research projects.

4.1.3 Research outcomes

4.1.3.1 Achievements of the research under this sub-theme

Figure 4-3 presents this sub-theme's project distribution based on year of (expected) completion. It is noticeable that there is a continuous flow of outcomes with respect to risk/threat assessment and management, and the endorsement of advanced technologies in threat detection and prevention. More recently, emphasis has been placed, also using advancements in science and technology, on making threat detection and prevention procedures more efficient and less disturbing to traffic flow, especially with respect to passengers. Finally, while support actions have always been present, it is noticeable that these are soon to be concluded.

Notably, emphasis on research for the detection and prevention of threats is continuous over the years and responds to the increasing number of threats to, and the vulnerabilities of, transport systems. Hence, the assessment of risks/threats and management methodologies requires a continuous adjustment and responsiveness, and a focus on the particular vulnerabilities of each transport system. Moreover, research was initially focused on aviation, although, more recently, threats and vulnerability of other transport systems have been included (with results expected within the forthcoming years).

Another consideration concerns the exploitation of advances in science and technology in other sectors, which find potential for applications for the detection and prevention of threats in transport. While monitoring and surveillance are their primary domain of implementation, technologies derived from developments in other fields have also been used to reduce the burden of controls and their disturbance to traffic flows.

With regard to individual transport modes, aviation is a major focus in this sub-theme. Related research has long focused on a variety of monitoring and surveillance systems targeted at aircraft, airports, passengers and luggage. However, the direction of current research has shifted towards novel ATM concepts and, in parallel, towards the need for integrated solutions for airport security systems.

An additional novelty is the focus on an ethical framework, social behaviour and security decision making during security threats.

Research on threat detection and prevention in maritime transport was primarily addressed in the wider spectrum of information exchange services in terms of achieving a secure, controlled data-sharing process for the security of vessels, port operations and port environment. Recently, research has been targeted at creating surveillance technology with the scope of detecting, tracking and deterring security threats to provide an intuitive situational awareness.

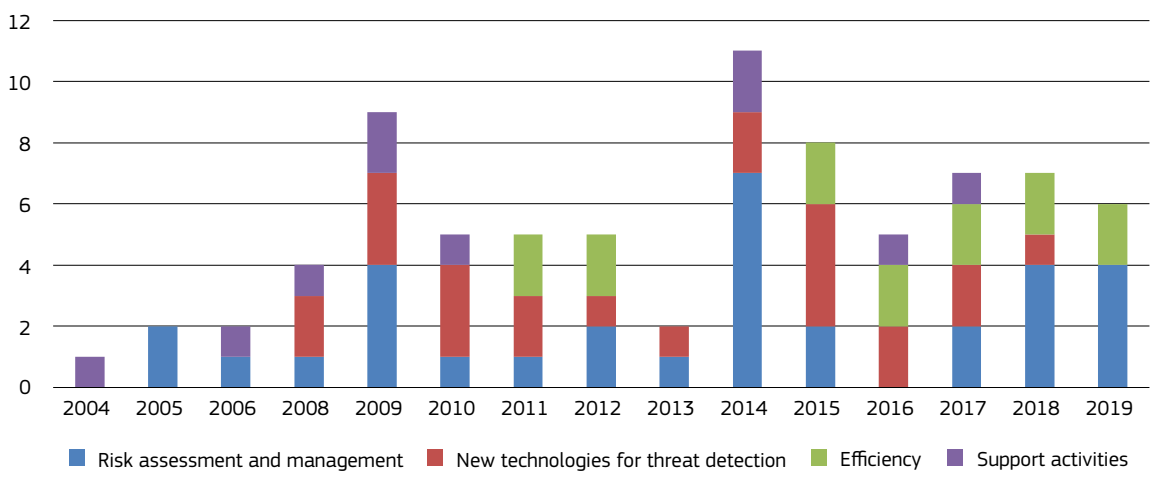
The majority of projects related to land transport were completed recently and cover a variety of topics. Nevertheless, a focus on urban transport is evident in the wider context of increasing security in mass transport systems. Research is directed towards innovative and integrated systems for the unattended surveillance of public transport (vehicles, stations), and technologies and methodologies enabling appropriate design of stations and terminals to reduce the impact of any security incident and/or attack.

Research has also recently been directed towards the protection of critical infrastructure. An evident trend that arises is the need for a holistic approach, integrating functionalities at all critical infrastructure levels (i.e. individual, across interdependent critical infrastructure and across borders). Moreover, because of prohibitive costs, the need for protection against extreme events is expanding and now also encompasses the concept of resilience addressed by ongoing projects.

4.1.3.2 Transferability from research to practical use

The majority of research outcomes from this sub-theme may be considered as being immediately applied in practice. There are two main drivers in this respect: the acknowledged need to detect and prevent threats, and the cooperation of transport service users to this effect. Moreover, many of the projects (being) implemented concerned applications of other research outcomes which, in practice, increased the maturity of the initial technology.

Figure 4-3 Distribution of threat detection and prevention projects by completion date



4.1.3.3 Indications for future research

As threats to the transport system become all the more pronounced, detection and prevention of threats becomes all the more important in sectors, such as land transport, which previously placed little attention to their vulnerability and potential threats. However, given the advancement in sectors such as aviation and airports, there is scope and potential to transfer expertise, applications and research findings to other sectors (e.g. maritime) where little research has been concluded in this respect.

In addition, the need to implement threat detection and prevention measures more widely is also coupled with the need to apply these measures 'seamlessly'. Therefore, there will be a more pronounced need for long-distance monitoring and surveillance and more efficient and effective control points.

4.1.3.4 Implications for future policy development

As transport networks are highly connected, there is a need for a more universal approach to threat detection and prevention. This calls for a continuous emphasis on support and coordination actions, which will allow actors from different levels of system operation and across systems to collaborate, exchange experience, develop a common understanding and co-innovate.

4.1.4 List of projects

Table 4-1 lists the projects included in this sub-theme assessment.

Table 4-1 Projects reviewed in the threat detection and prevention sub-theme

Project acronym	Project name	Project duration	Source of funding
ACROSS	Advanced Cockpit for Reduction Of StreSS and workload https://goo.gl/jycauA	2013-2016	EU (FP7[8]–TPT)
ADS	Autonomous Dronistics for Security (ADS): optimized services with fleets of flying robots https://goo.gl/9zhphW	2015	EU (Horizon 2020)
AIR-SEAL	An Innovative RFID Security SEAL for Aircraft Galley Trolleys https://goo.gl/Eey37B	2009-2011	EU (FP7–SME)
AllTraIn	All-Hazard Guide for Transport Infrastructure https://goo.gl/4zvQGp	2013-2015	EU (CIPS)
ASPIS	Autonomous Surveillance in Public transport Infrastructure Systems https://goo.gl/w3rZ9w	2008-2011	EU (FP7–SST)
ASSERT	Assessing Security Research: Tools and Methodologies to measure societal impact https://goo.gl/KfaJQI	2013-2014	EU (FP7–SEC)
ATOM	Airport detection and tracking of dangerous materials by passive and active sensors arrays https://goo.gl/7qyx90	2009-2012	EU (FP7–AAT)
BEMOSA	Behavioral Modeling for Security in Airports https://goo.gl/C4QzSN	2009-2012	EU (FP7–TPT)
BIRDWATCH	The first integral and modular mobility and security solution for smart parking management https://goo.gl/xvmIfG	2015	EU (Horizon 2020)
BODEGA	BOrDErGuArd – Proactive Enhancement of Human Performance in Border Control https://goo.gl/Yjui02	2015-2018	EU (Horizon 2020)
CARONTE	Creating an Agenda for Research ON Transportation sEcurity https://goo.gl/OmI7RW	2014-2016	EU (FP7–SEC)

8 Seventh Framework Programme for Research and Technological Development.

Table 4-1 (Continued) Projects reviewed in the threat detection and prevention sub-theme

Project acronym	Project name	Project duration	Source of funding
CASAM	Civil Aircraft Security Against MANPADs https://goo.gl/IWeMSS	2006-2009	EU (FP6–Aerospace)
CIPSEC	Enhancing Critical Infrastructure Protection with innovative SECurity framework https://goo.gl/7HxT91	2016-2019	EU (Horizon 2020)
COPRA	Comprehensive European Approach to the Protection of Civil Aviation https://goo.gl/7UI33R	2011-2013	EU (FP7–SEC)
COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities https://goo.gl/sOL8if	2006-2009	EU (FP6)
DRUID	Driving Under the Influence of Drugs, Alcohol and Medicine https://goo.gl/b3YBIp	2006-2011	EU (FP6–SUSTDEV)
e-Airport	Increase airport capacity, safety and security using European GNSS https://goo.gl/EMfmoS	2015-2017	EU (Horizon 2020)
ECOSSIAN	European Control System Security Incident Analysis Network https://goo.gl/KQYCMA	2014-2017	EU (FP7–SEC)
EFFISEC	Efficient Integrated Security Checkpoints https://goo.gl/7PxMlg	2009-2014	EU (FP7–SEC)
ESTEEM	Enhancing Safety and Security Aspects in Transport Research in the Euro-Mediterranean Region https://goo.gl/F91ahn	2008-2009	EU (FP7–TPT)
EU CISE 2020	EUropean test bed for the maritime Common Information Sharing Environment in the 2020 perspective https://goo.gl/mAQwLP	2014-2017	EU (FP7–SEC)
EXTREMDRON	Unmanned aerial vehicle for vigilance, control and critical urban infrastructure protection https://goo.gl/pQkGFi	2016	EU (Horizon 2020)
FastPass	A harmonized, modular reference system for all European automated border crossing points https://goo.gl/BWdlsH	2013-2017	EU (FP7–SEC)
FLYSAFE	Airborne Integrated Systems for Safety Improvement, Flight Hazard Protection and All Weather Operations https://goo.gl/c9VCkZ	2005-2009	EU (FP6–Aerospace)
FLYSEC	Optimising time-to-FLY and enhancing airport SECurity https://goo.gl/9rIJQe	2015-2018	EU (Horizon 2020)
Gait Biometrics 3	Main goal of the project is to create a prototype of the software, which will be able to identify people just based on the way how they walk. https://goo.gl/OexYEU	2015	EU (Horizon 2020)
GMOSS	Global Monitoring for Security and Stability https://goo.gl/yTClUJ	2004-2008	EU (FP6–Aerospace)
GRAND	GRAND GOOS Regional Alliances Network Development https://goo.gl/SjQkVO	2004-2006	EU (FP6–SUSTDEV)

Table 4-1 (Continued) Projects reviewed in the threat detection and prevention sub-theme

Project acronym	Project name	Project duration	Source of funding
HAWKEYE	Thermal infra red hyperspectral sensing assistance to clandestine weapon surveillance under working conditions linking fixed airborne or space borne systems https://goo.gl/eid6su	2005-2009	EU (FP6–Aerospace)
HERMES	Establishing a CompreHEnsive transport Research information Management and Exchange System https://goo.gl/18VG54	2011-2014	EU (FP7–TPT)
HOLOSCAN	Holographic Scanner for Safe Real-Time High Throughput Screening of People and Their Bags https://goo.gl/wGDQFN	2014-2015	EU (Horizon 2020)
ICOA.10.09	International Conference on Airports, October 2009 Paris https://goo.gl/C4M5xQ	2008-2010	EU (FP7–TPT)
iCROSS	Intelligent Portable ContROl SyStem https://goo.gl/xZTWnI	2016-2019	EU (Horizon 2020)
IMPROVER	Improved risk evaluation and implementation of resilience concepts to critical infrastructure https://goo.gl/qxsWzf	2015-2018	EU (Horizon 2020)
INOUI	Innovative Operational UAV Integration https://goo.gl/pKYevH	2007-2010	EU (FP6–Aerospace)
ISTIMES	Integrated System for Transport Infrastructures surveillance and Monitoring by Electromagnetic Sensing https://goo.gl/OBLNfj	2009-2012	EU (FP7–SEC)
MARNIS	Maritime Navigation and Information Services https://goo.gl/Ehy8yD	2004-2008	EU (FP6–SUSTDEV)
MERSEA	Marine Environment and security for the European Area https://goo.gl/m8uuYr	2004-2008	EU (FP6–Aerospace)
MOBILEPASS	A secure, modular and distributed mobile border control solution for European land border crossing points https://goo.gl/sZuDOi	2014-2016	EU (FP7–SEC)
OPERAMAR	An Interoperable Approach to European Union Maritime Security Management https://goo.gl/00S2mk	2008 -2009	EU (MIP-MAP)
OPTAG	Improving Airport Efficiency, Security and Passenger Flow by Enhanced Passenger Monitoring https://goo.gl/uz5Jao	2006-2009	EU (FP6–Aerospace)
OPTIX	Optical Technologies for the Identification of Explosives https://goo.gl/OkpiBD	2008-2013	EU (FP7–SEC)
PANDHUB	Prevention and Management of High Threat Pathogen Incidents in Transport Hubs https://goo.gl/LcnuM4	2014-2017	EU (FP7–SEC)
PROTECT	Pervasive and UseR Focused BiomeTrics BordEr ProjeCT https://goo.gl/2bfvYT	2016-2019	EU (Horizon 2020)
PROTECTRAIL	The Railway-Industry Partnership for Integrated Security of Rail Transport https://goo.gl/dndj29	2010-2014	EU (FP7–SEC)

Table 4-1 (Continued) Projects reviewed in the threat detection and prevention sub-theme

Project acronym	Project name	Project duration	Source of funding
RAILPROTECT	Innovative Technologies for Safer and more Secure Land Mass-Transport Infrastructure under Terrorist Attacks https://goo.gl/FM3k5q	2006-2009	EU (JRC)
RESILIENCE	Dynamic Resilience Evaluation of Interrelated Critical Infrastructure Subsystems https://goo.gl/AvPhL9	2015-2019	National (Czech Republic)
RESOLUTE	RESilience management guidelines and Operationalization appLied to Urban Transport Environment https://goo.gl/muQTzw	2015-2018	EU (Horizon 2020)
RESTRAIL	Reduction of Suicides and Trespasses on RAILway property https://goo.gl/1GbxNV	2011-2014	EU (FP7–TPT)
SAFEE	Security of Aircraft in the Future European Environment https://goo.gl/30dt1n	2004-2008	EU (FP6–Aerospace)
SafeShore	System for detection of Threat Agents in Maritime Border Environment https://goo.gl/Mr4URb	2016-2018	EU (Horizon 2020)
SECRET	SECurity of Railways against Electromagnetic aTtacks https://goo.gl/SHvmUN	2012-2015	EU (FP7–SEC)
SECTRONIC	Security System for Maritime Infrastructures, Ports and Coastal Zones https://goo.gl/6Bc6cr	2008-2011	EU (FP7–SEC)
SECUR-ED	Secured Urban Transportation – European Demonstration https://goo.gl/xjcr8s	2011-2014	EU (FP7–SEC)
SECURESTATION	Passenger station and terminal design for safety, security and resilience to terrorist attack https://goo.gl/Ghmpfo	2011-2014	EU (FP7–SST)
SERON	Security of Road Transport Networks https://goo.gl/77YUnP	2009-2012	EU (FP7–SEC)
SIAM	Security Impact Assessment Measure – A decision support system for security technology investments https://goo.gl/lg46YV	2011-2014	EU (FP7–SEC)
SKY-Scanner	Development of an Innovative LIDAR Technology for New Generation ATM Paradigms https://goo.gl/BNv2EC	2007-2010	EU (FP6–Aerospace)
SMARTER	Surveillance of Maritime Surroundings through Laser Technology https://goo.gl/rmrpLX	2015	EU (Horizon 2020)
SmartResilience	Smart Resilience Indicators for Smart Critical Infrastructures https://goo.gl/X7YU6s	2016-2019	EU (Horizon 2020)
SOFIA	Safe Automatic Flight Back and Landing of Aircraft https://goo.gl/H9A0YI	2006-2010	EU (FP6–Aerospace)
SOS	Sensors system for detection and tracking Of dangerous materials in order to increase the airport Security in the indoor landside area https://goo.gl/04E2Yn	2012-2015	EU (FP7–People)

Table 4-1 (Continued) Projects reviewed in the threat detection and prevention sub-theme

Project acronym	Project name	Project duration	Source of funding
STAR-TRANS	Strategic Risk Assessment and Contingency Planning in Interconnected Transport Networks https://goo.gl/glkMcj	2009-2012	EU (FP7–SEC)
SUPPORT	Security UPgrade for PORTs https://goo.gl/GKM5SG	2010-2014	EU (FP7–SEC)
SURVEIRON	Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures https://goo.gl/HSCtYB	2016-2018	EU (Horizon 2020)
TAKEDOWN	Understand the Dimensions of Organised Crime and Terrorist Networks for Developing Effective and Efficient Security Solutions for First-line-practitioners and Professionals https://goo.gl/9jzJsE	2016-2019	EU (Horizon 2020)
TASS	Total Airport Security System https://goo.gl/LKlZxv	2010-2014	EU (FP7–SEC)
VERA2	Video Enforcement for Road Authorities 2 https://goo.gl/tWkiOm	2003-2004	EU (FP5–Growth)
VULCAN	Vulnerability Analysis for Near Future Composite/Hybrid Air-Structures: Hardening via New Materials and Design Approaches Against Fire and Blast due to Accidents or Terrorist Attacks https://goo.gl/x6Rqx7	2006-2010	EU (FP6–Aerospace)
WARDIAM PERIMETER	WARDIAM PERIMETER https://goo.gl/tEmw04	2016-2016	EU (Horizon 2020)
XP-DITE	Accelerated Checkpoint Design Integration Test and Evaluation https://goo.gl/DMI8jo	2012-2017	EU (FP7–SEC)
N/A	Intelligent Infrastructure for Modern City https://goo.gl/n2MlQW	2012-2014	National (Czech Republic)
N/A	Intelligent Luggage https://goo.gl/pILup5	2008-2011	National (Portugal)
N/A	Process model of critical infrastructure safety and protection in the transport sector https://goo.gl/AEJhkW	2015-2018	National (Slovakia)
N/A	Reducing Crime at Rail Stations in Socially Excluded/High Crime Locations https://goo.gl/9XsxZM	2005	National (United Kingdom)
N/A	Safety and comfort of car parks (VSS2000/454) https://goo.gl/rE74Ka	2001-2005	National (Switzerland)
N/A	Security tool for risk analysis in harbour installations https://goo.gl/jVVVFd	2008-2009	National (Spain)
N/A	Speaker verification as an add-on element of the Air Traffic Management security https://goo.gl/1rVWAA	2015-2017	National (Slovakia)
N/A	Suicide prevention on bridges: Fundamentals (AGB2003/013) https://goo.gl/xBLPr1	2004-2006	National (Switzerland)

4.2 Crisis management

4.2.1 Introduction to the sub-theme

Transport systems are vital for the functioning of regions, industries and societies, and constitute costly and durable assets covering large land areas. They have always been exposed to and are sensitive to the effects of natural and man-made hazards (e.g. earthquakes, extremes of weather, acts of sabotage and armed conflicts). Even with good preparation, not all such events can be prevented or mitigated successfully. In cases where transport systems, settlements or industries are hit by external threats, crisis management needs to reduce the most immediate, medium and long-term impacts for people, assets, cities and regions.

This sub-theme considers research on how the impact of external events can be reduced during or after they occur. The review is organised along three levels or phases of crisis management research:

- studies on emergency management – developing or demonstrating response mechanisms, resilience guidance and staff training curriculums;
- resilience planning – going a step further and researching how crisis management strategies, in case of an impact, are to be embedded in broader strategies from crisis preparation, through emergency management and to the after treatment of the event;
- strategy development – aiming to provide general guidance on the options that institutions may take and on open issues to be clarified.

4.2.1.1 Overall direction of European-funded research

In total, 31 projects on the topic of crisis management were identified in the TRIP database – 26 of these were European projects. Of the projects reviewed, 10 started in 2014 or later and 17 of the remainder started between 2007 and 2013 (i.e. during the Seventh Framework Programme for Research and Technological Development (FP7)). The topic areas of the projects reviewed were emergency management (11), resilience planning (4) and strategy development (16).

From the aims and results of the projects, the linking of various information sources for a cross-sectoral, cross-border and cross-institutional coordination of actors (including public and private bodies) for enhanced crisis management can be identified. Moreover, novel technologies, such as new monitoring systems and computer-aided situation assessment for evacuation purposes, have emerged. Looking at the modal distribution, nearly half (14) of the 31 projects reviewed deal with intermodal issues. The remaining studies are devoted to aviation (7), rail (6), road (3) and shipping (3).

4.2.1.2 Overall direction of nationally funded projects

The review of the projects in TRIP identified only five nationally funded projects relevant to this sub-theme. As a result, it was not possible to identify any trends or specialisation in the research activities.

4.2.2 Research activities

Selected projects are presented in the following sections to provide a snapshot of the research activities performed. Projects are structured around the most relevant topics with regard to crisis management. First, there is the question on how crises affecting the transport system can best be prevented. Second, there are projects that strive to support the various actors in dealing with the crises that occur, despite the efforts to prevent them. Third, there are overarching projects that focus on the resilience of transport systems, thereby striving to improve the mechanisms to prevent and mitigate crises, and to reconstruct the systems after they happen.

4.2.2.1 Emergency management

Crisis mitigation makes reference to how best to handle crises once they have occurred. Here there are, on the one hand, some mode-specific projects that focus, for example, on the evacuation of passenger ships. On the other hand, there are projects that cover several transport modes and the corresponding infrastructure to enable comprehensive crisis mitigation in the case of extreme and cross-modal crises.

In the HELI4RESCUE (2012-2014) project, the possibility of using large air-transport systems at crisis sites was analysed. This focused on those systems that are used in military operations and their potential for civil use. As a result, requirements and functional specifications were generated for large air-transport systems for civil use. These were complemented by a feasibility assessment and a roadmap for a common European approach regarding the use of large air-transport systems for crisis mitigation.

With regard to ships, the LYNCEUS2MARKET (2015-2018) project is concerned with operational system for evacuating passengers from large passenger ships, which is based on innovative technologies for locating people in emergency situations. The project follows on from the LYNCEUS[9] (2012-2014) project, in which the proposed systems were tested in laboratory settings. The LYNCEUS2MARKET project focuses on the implementation of the tested system and its dissemination.

The MICRODIS project (2007-2011) is an overarching project which strives to strengthen the preparation, mitigation and preparedness for extreme events, and their impact on social communities. The aim of the project is to achieve this through a better understanding of the events and their impacts on society. The focus of the project is not only on Europe, but also includes Asian partners.

9 http://cordis.europa.eu/project/rcn/103573_en.html

There are various other projects that attempt to support the mitigation of crises. These include the AIRBEAM (2012-2015), CRISIS (2010-2013), GETAWAY (2011-2014), IMPACT (2015-2017) and SAFEGUARD (2009-2012) projects. Nationally funded projects include the Finnish eCall-hyöty (2005) project, the Italian project on the 'guidelines for evacuation plans' (2004-2005) and the Spanish project focusing on 'optimisation models applied to the robust planning and management of Metropolitan Public Transport services in cases of emergency' (2008-2009).

4.2.2.2 Resilience planning

The projects focusing on crisis resilience are working to develop measures to enable transport systems to cope with crises better. This involves reducing the impacts of crises, effectively and efficiently dealing with crises, and recovering from them. These projects mainly focus on developing the relevant processes and management schemes.

Standardisation is at the core of the ResiStand (2016-2018) project as it enables the interoperability of different systems. To this end, the gaps in standardisation are identified from the point of view of the main stakeholder groups (standardisation organisations, end-users and suppliers). The aim is to develop a pre-standardisation process that is then used by all stakeholders to ensure that promising research results may be implemented in crisis management procedures.

How infrastructure can withstand, adapt and recover from crises is the main focus of the RESILENS (2015-2018) project. To this end, a European resilience management guideline, a resilience management matrix and an audit toolkit are to be developed. These should then help to operationalise the theoretical concept of resilience for critical infrastructure. Finally, a RESILENS decision-support platform is proposed, which will be based on an e-learning platform to familiarise critical infrastructure providers and guardians, first responders and civil protection personnel with resilience measures. In a similar context, the RESOLUTE (2015-2018) project focuses on developing management guidelines for the resilience of the urban transport environment and supporting their implementation.

Lastly, a project on 'process management tools ensuring security and functionality of crisis infrastructure with emphasis on the area of transport' (2015-2018) is being funded by the Czech Republic. The project is intended to develop software that will enable the user to apply the tools that have been developed directly and to follow the defined steps in the event of a crisis.

4.2.2.3 Strategy development

With regard to crisis prevention, a large body of knowledge already exists for specific fields, modes or occasions. Thus, the projects in this area focus on combining the existing knowledge and/or to give an overview of the project and knowledge landscape.

In this sense, the CARONTE (2014-2016) project provides a roadmap regarding necessary future research to increase the security of land transportation. The basis is a thorough analysis of Europe's land transport security to identify potential weaknesses; the project builds on the results of relevant previous projects. Attention is paid to passenger and freight transport. As a result, the outcome of this project is a research agenda including all relevant threats and security aspects of the land-based transport modes.

The GMOSS (2004-2008) project focuses on the combination of knowledge regarding security and stability. Therefore, a network was set up to bring together Europe's civil security research to develop a satellite-based Earth observation system. Thanks to the multidisciplinary team working on the project, political, social and economic aspects of the satellite monitoring were acknowledged as were technical issues.

In contrast, the DEMASST (2009-2010) and RANGER (2016-2019) projects focus on crisis prevention for specific transport modes. With regard to rail and road transport, the DEMASST project focused on elaborating adequate and well-accepted security measures for mass transportation in Europe. This is of special importance as the operators cannot employ security measures similar to those at airports due to the many entry and exit points of land-based mass transportation systems. The focus of the RANGER project is on securing the European maritime border areas. To this end, a surveillance platform is planned that will enable suspicious vessels to be detected, recognised, identified and tracked. Therefore, it draws on novel radar systems, namely an over-the-horizon radar, combined with a multiple input, multiple output (MIMO) radar and an early warning system.

Other projects funded by the EU in this context include AIDER (2001-2005), ASSIST (2005-2007), COUNTERACT (2006-2009), ECOSSIAN (2014-2017), PANDHUB (2014-2017), PROTECTRAIL (2010-2014), SECRET (2012-2015), SECUR-ED (2011-2014), SUBITO (2009-2011) and TASS (2010-2014). In addition, there are various nationally funded projects such as those from the Czech Republic that focus on the 'virtual simulation of pedestrian evacuation and transport processes' (2012-2014) and the 'Utilisation of Crisis Management, Risk Management, Systems Engineering Tools and Modern Technologies to Improve Security at International Airports in the Czech Republic' (2013-2015).

4.2.3 Research outcomes

4.2.3.1 Achievements of the research under this sub-theme

The majority of projects in this sub-theme are concerned with the organisation of crisis and emergency management, rather than with technological questions. Apart from many good practices and guidelines for specific situations, the overarching recommendation of the projects is that the intelligent linking of information sources and actors is key to successful crisis management.

A number of projects dealt with the protection of European borders. This aimed to coordinate European Member States towards joint operations, and standardised procedures and technologies. The interoperability of procedures and technologies, which needs to be ensured before actual missions, can support good emergency management. However, research results also point to the regional and cultural aspects in reacting to hazardous situations, which must not be ignored.

4.2.3.2 Transferability from research to practical use

Transferability of research outcomes in this sub-theme is quite common as many of these projects are very close to practical implementation and, in some cases, operational guidelines for crisis management have been developed.

4.2.3.3 Indications for future research

Big-data applications should be exploited further for better management of critical situations, such as the evacuation of passengers and customers from terminals.

Humanitarian logistics appeared on the agenda of aid organisations in the early 2010s, but never received much attention by research. Given the many crises in the vicinity of Europe, this aspect of crisis and emergency management deserves broader investigation.

Cross-sectoral research on cascade effects should be deepened to minimise risks to actual crisis and emergency management. Recent events, such as the terrorist attacks in Paris and Brussels, revealed that social media constitute core means of communication, but mobile networks may get overloaded. Power failures outs may add further serious problems to successful crisis management and recovery. Research on multiple sector impacts during hazardous situations exists, but its practical relevance seems limited.

One of the most recent roadmaps that took into consideration crisis and emergency management research is provided by the CARONTE project. The roadmap highlights that a lot of research for single solutions of good crisis management has been already carried out, but more research is needed for integrated solutions. Also the need for more staff training and awareness raising was stressed.

4.2.3.4 Implications for future policy development

Future policy developments related to crisis management should take into consideration:

- defining communication standards and processes to be used in crisis situations;
- cooperation between actors is to be clarified and is to be underpinned with clear rules and guidelines;
- integrating novel technologies in crisis management processes.

4.2.4 List of projects

Table 4-2 lists the projects included in this sub-theme assessment.

Table 4-2 Projects reviewed in the crisis management sub-theme

Project acronym	Project name	Project duration	Source of funding
AIDER	Accident Information and Driver Emergency Rescue https://goo.gl/voOPLr	2001-2005	European Union (FP5–IST)
AIRBEAM	AIRBorne information for Emergency situation Awareness and Monitoring https://goo.gl/dI58aW	2012-2015	European Union (FP7–SEC)
ASSIST	Alpine Safety, Security and Informational Services and Technologies https://goo.gl/fPmky9	2005-2007	European Union (FP6–Aerospace)
CARONTE	Creating an Agenda for Research ON Transportation sEcurity https://goo.gl/OmI7RW	2014-2016	European Union (FP7–SEC)
COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities https://goo.gl/sOL8if	2006-2009	European Union (FP6)
CRISIS	CRitical Incident management training System using an Interactive Simulation environment https://goo.gl/hdaJtl	2010-2013	European Union (FP7–SEC)
DEMASST	Security of critical infrastructures related to mass transportation https://goo.gl/P6VLQz	2009-2010	European Union (FP7–SEC)
eCall-hyöty	Impacts of an automatic emergency call system on accident consequences https://goo.gl/p3gP7d	2005	Finland
ECOSSIAN	European Control System Security Incident Analysis Network https://goo.gl/KQYCMA	2014-2017	European Union (FP7–SEC)
GETAWAY	Generating simulations to Enable Testing of Alternative routes to improve WAYfinding in evacuation of overground and underground terminals https://goo.gl/Iy0Dx6	2011-2014	European Union (FP7–TPT)
GMOSS	Global Monitoring for Security and Stability https://goo.gl/yTClUJ	2004-2008	European Union (FP6–Aerospace)
HELI4RESCUE	Heavy Payload Helicopter for Last Mile Rescue https://goo.gl/gxzeIV	2012-2014	European Union (FP7–SEC)
IMPACT	Impact of Cultural aspects in the management of emergencies in public Transport https://goo.gl/tL6Mqm	2015-2017	European Union (Horizon 2020)
LYNCEUS2MARKET	An innovative people localisation system for safe evacuation of large passenger ships https://goo.gl/EM85py	2015-2018	European Union (Horizon 2020)
MICRODIS	Integrated health, social and economic impacts of extreme events: Evidence, methods and tools https://goo.gl/Gdb27w	2007-2011	European Union (FP6–SUSTDEV)
PANDHUB	Prevention and Management of High Threat Pathogen Incidents in Transport Hubs https://goo.gl/LcnuM4	2014-2017	European Union (FP7–SEC)
PROTECTRAIL	The Railway-Industry Partnership for Integrated Security of Rail Transport https://goo.gl/dndj29	2010-2014	European Union (FP7–SEC)

Table 4-2 (Continued) Projects reviewed in the crisis management sub-theme

Project acronym	Project name	Project duration	Source of funding
RANGER	Radars for long distance maritime surveillance and SAR operations https://goo.gl/SsVZRY	2016-2019	European Union (Horizon 2020)
RESILENS	Realising European resilience for critical infrastructure https://goo.gl/anpqJ3	2015-2018	European Union (Horizon 2020)
ResiStand	Increasing disaster resilience by establishing a sustainable process to support standardisation of technologies and services https://goo.gl/AX3Fgw	2016-2018	European Union (Horizon 2020)
RESOLUTE	RESilience management guidelines and Operationalization appLied to Urban Transport Environment https://goo.gl/muQTzw	2015-2018	European Union (Horizon 2020)
SAFEGUARD	Ship Evacuation Data and Scenarios https://goo.gl/ZRaoU4	2009-2012	European Union (FP7–TPT)
SECRET	SECurity of Railways against Electromagnetic aTtacks https://goo.gl/SHvmUN	2012-2015	European Union (FP7–SEC)
SECUR-ED	Secured Urban Transportation – European Demonstration https://goo.gl/xjcr8s	2011-2014	European Union (FP7–SEC)
SUBITO	Surveillance of Unattended Baggage and the Identification and Tracking of the Owner https://goo.gl/1IoDuI	2009-2011	European Union (FP7–SEC)
TASS	Total Airport Security System https://goo.gl/LKlZxv	2010-2014	European Union (FP7–SEC)
N/A	Guidelines for evacuation plans by simulation of transport systems in emergency conditions https://goo.gl/Hy1vrk	2004-2005	Italy
N/A	Optimisation models applied to the robust planning and management of Metropolitan Public Transport services in cases of emergency https://goo.gl/lxhKVn	2008-2009	Spain
N/A	Process management tools ensuring security and functionality of crisis infrastructure with emphasis on the area of transport https://goo.gl/eF2pMH	2015-2018	Czech Republic
N/A	Utilisation of Crisis Management, Risk Management, Systems Engineering Tools and Modern Technologies to Improve Security at International Airports in the Czech Republic https://goo.gl/fe4y1b	2013-2015	Czech Republic
N/A	Virtual simulation of pedestrian evacuation and transport processes https://goo.gl/oFWwln	2012-2014	Czech Republic

4.3 Cyber security, privacy and ICT issues

4.3.1 Introduction to the sub-theme

Modern society is heavily dependent on data collection, processing and usage for a wide range of IT technologies and devices. Even roads, which in the past were simply made with asphalt and concrete, depend more and more on data for their operation. This implies that when the operating systems fail, transport systems cannot work effectively (or only with an unacceptably higher risk of accident) or not at all.

The ongoing trend is to eliminate human presence (and risks of human mistakes) in traffic control by introducing ICT systems that can replace operators, pilots, metro drivers and, in the near future, drivers in general. The benefits of ICT systems are clear and understandable, but their security has to be ensured and transport systems need to be protected against attacks by terrorists or hackers.

Ensuring the security of transport requires not only the protection of transport structures against destruction (e.g. bomb attacks), but also the protection from abuse of the devices and software which control the traffic on those transport structures. The same protection has to be guaranteed for the personal data produced by many devices that people use in their daily lives.

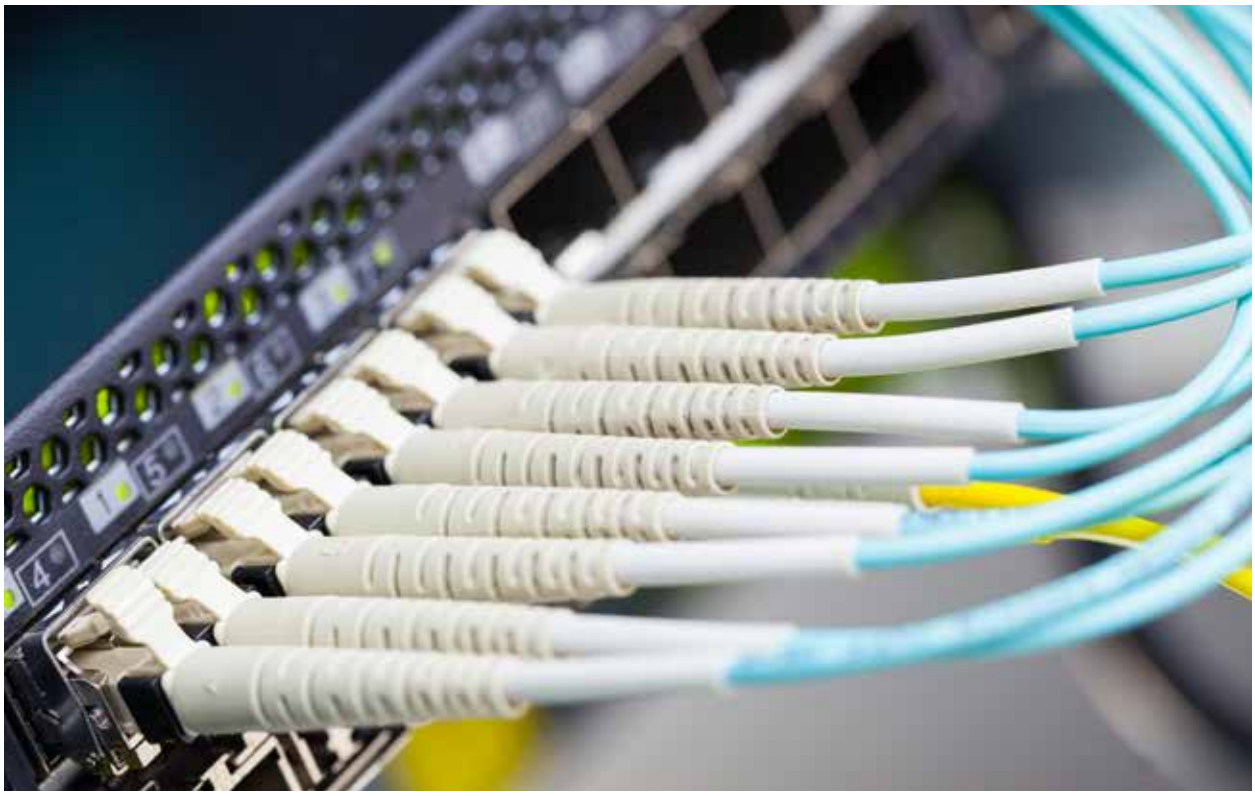
4.3.1.1 Overall direction of European-funded research

The European Commission has funded several projects focused on cyber security, privacy and ICT issues during the last two decades. Aviation was the dominant theme, followed by road and rail transport.

Air transport research has been focused on:

- the improvement of European airspace and traffic management infrastructure, and to increase worldwide competitiveness (the INTERVUSE (2001-2004) project);
- the needs of alternative communications systems in air transport (e.g. applying multi-carrier (MC) technology for aeronautical communications in the very high frequency (VHF) band for a future MC broadband VHF (B-VHF) system (as in the B-VHF (2004-2006) project));
- the enhancement of aircraft system monitoring by developing concepts based on new wireless technologies and integrated sensing solutions (the WISE (2005-2008) project);
- improvements to the ATM in different areas and conditions (the NUP2 (2004-2007) project);
- developing novel laser-tracking technology (the SKY-Scanner (2007-2010) project);
- safe automatic flight back and landing of aircraft (the SOFIA (2006-2010) project).

In the maritime sector, the interrelated projects CYSM (2013-2014), MITIGATE (2015-2018) and MEDUSA (2010-2014) specifically target the protection of the maritime supply-chain IT infrastructure. The projects provided a sound basis for moving leading-edge risk management frameworks (and their accompanying tools) for maritime and port critical information infrastructures (CIIs) from the realm of research and development to commercial application.



Unlike aviation and maritime security, the threats and risks to land transport are diverse, so research topics are more case-specific. However, there are a few European projects combining ICT with cyber security and privacy topics, for example:

- safety improvement in road and rail tunnels using advanced information technologies was studied by the SIRTAKI (2001-2004) project;
- preparing secure vehicle-to-everything (V2X) communication systems was dealt by the PRESERVE (2011-2014) and ICSI (2012-2015) projects.

There have been more projects supported by the EU that focused on anti-terrorist activities and/or planning (e.g. COUNTERACT (2006-2009), STAR-TRANS (2009-2012), CITYMOBIL2 (2012-2016) and AINARA (2015-2017)). However, these projects have not widely covered cyber security, privacy and ICT issues.

The CARONTE (2014-2016) project created an overview about the priority research topics on transport security, within which cyber and ITC security were considered as top priority topics.

4.3.1.2 Overall direction of nationally funded projects

Nationally funded projects connected to the topic of cyber security, privacy and ICT were carried out in Spain, Norway and the Czech Republic. Spain supported the Security tool for risk analysis in harbour installations (2008-2009) project. The Norwegian Public Roads Administration supported the Data Protection and Privacy Implication in Road Safety (2008-2010) project. The Czech Republic supported the Universal radio gateway for IP communication in dispatch systems (2014-2017) and Using related GNSS safe applications for elimination safe and security risk by transport dangerous goods at different kind of transport infrastructure' (2012-2014) projects that were partly linked to the topic under consideration. The first project investigated the universal integration of internet protocol (IP) radio gateway for implementation into complex integration or dispatching systems including the unified voice and data communication into channels for internal and external subsystems (communication, security, information, etc.). The second project was aimed at the use of ICT for improvements to the safety and security of the transport of dangerous goods.

4.3.2 Research activities

The most relevant projects of the sub-theme of cyber security, privacy and ICT have been identified and analysed according to their focus on vehicles and networks, and on personal identity and privacy protection.

4.3.2.1 ICT for transport vehicles

The EVITA (2008-2011) project complemented other e-safety related projects that focused on the protection of the V2X communications by intra-vehicle communication.

The project objective was to design, verify and build a prototype architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise when transferred inside a vehicle.

The goal of PRESERVE was to bring secure and privacy-protected V2X communication closer to reality by providing and field testing a security and privacy subsystem for V2X systems. It aimed to provide comprehensive protection, ranging from the vehicle sensors, through the on-board network and vehicle-to-vehicle (V2V)/vehicle-to-infrastructure (V2I) communication, to the receiving application. Another strategic objective of PRESERVE was to contribute to the ongoing harmonisation and standardisation efforts on the European level. PRESERVE combined and extended results from earlier research projects, integrating and developing them to a pre-deployment stage by enhancing scalability, reducing the cost level and addressing open deployment issues.

The WISE project was related to air transport. It aimed to accelerate and improve structural repairs on aircraft. In the current market organisation, structural repairs require on-site specialised expertise. As experts are not available at every airport, they often have to be flown to the site and this creates costly delays. Instead of physically moving the experts, WISE brought expert assistance to the on-site teams through an advanced augmented reality communication system. The WISE project stemmed from repeated requests from customers, providing a challenge to devise a device capable of bringing world-class expertise to their on-site general maintenance teams.

4.3.2.2 ICT for transport network

Adequate response to detected threats is also relevant for secure transport infrastructure. With the increasing number of remote, centrally controlled networked infrastructures and big- data computing, the central systems should have adequate tools to detect and react to potential risks.

The protection of the national infrastructure is one of the main issues for national and international security. While the MICIE (2008-2011) project has proved that increasing cooperation among infrastructure increases their level of service and predictive capability, it is not enough to effectively counteract threats such as cyber attacks. Such attacks could be performed by blocking communication from central supervisory control and data acquisition (SCADA) to local equipment, or inserting fake commands or measurements in the communications between SCADA and field equipment (as happened with STUXNET – a malicious computer worm). The paradox is that critical infrastructure relies heavily on the newest interconnected (and vulnerable) ICT technologies, while the control equipment is typically old legacy software and hardware. Such a combination of factors may lead to very dangerous situations that expose systems to a wide variety of attacks.

To overcome such threats, the CockpitCI (2012-2014) project continued the work done in MICIE by refining and updating the on-line risk predictor used in the SCADA centre and provided a form of intelligence to field equipment. This enables the equipment to perform local decisions to self-identify and self-react to abnormal situations induced by cyber attacks. It is necessary to operate at the SCADA control centre and at the field equipment levels because it is very dangerous to let field components operate autonomously. To address this issue, a hybrid validation system was implemented. At the control centre level, an 'Integrated On-line Risk Predictor' provided the operator with qualitative and quantitative measurements of near future level of risk, integrating data coming from the field, from other infrastructure and from smart detection agents monitoring possible cyber attacks. At the field level, the system is complemented by a smart software layer for field equipment and a detection system for the telecommunication network. The system can be used, for example, in traffic light control or tunnel fire protection systems and tunnel ventilation. It will be validated on real equipment and scenarios provided by Israel Electric Corp.

The first project to consider security issues alongside the maritime CII was CYSM. The overall aim of CYSM was to develop significant enhancements to the protection of the ports' CIIs, on the basis of a holistic approach, which took their dual cyber-physical aspects into account. The whole spectrum of CII threats to ports was analysed. Furthermore, a dynamic risk management methodology for ports' CII, which evaluated the physical and cyber risks against the requirements specified in the International Ship and Port Facility Security (ISPS) Code (physical) and ISO/IEC 27001 (cyber), was produced. The project also developed a web-based collaborative security management system. The follow-up project, MITIGATE, aims to improve risk-management methodologies for the maritime sector to make progress towards a collaborative, evidence-driven, maritime-supply-chain risk assessment (MSRA) approach that alleviates the limitations of state-of-the-art risk-management frameworks. To this end, the MITIGATE project will integrate, validate and commercially exploit an effective, collaborative, standards-based risk management system for port CIIs. This will consider all threats arising from the supply chain, including those associated with interdependencies and associated cascading effects. In addition, the MEDUSA project aimed to reduce the gap between risk-assessment frameworks and various cascading effects that are associated with security incidents that arise from interacting entities.

The SISSDEN (2016-2019) project aims to enhance global cyber security in relation to transport by improving the cyber security posture of EU entities and end users through the development of situational awareness and sharing of actionable information. The core of SISSDEN is a worldwide sensor network. Its main goal is the creation of multiple, high-quality feeds of actionable security information that will be used for remediation purposes and for proactive tightening of computer defences. This will be achieved by developing and deploying a distributed sensor network based on state-of-the-art technologies and the creation of a high-throughput data processing centre. SISSDEN will provide in-depth analytics on the collected data and develop metrics that will be used to establish the scale of most important security issues in the EU and impact of the project itself.

4.3.2.3 Personal identity protection

One of the main issues in transport is traveller identity protection when ticketing by digital means – bank card use, national electronic identity (eID or e-Identity) card and biometrics. These newly deployed measures require safe and secure e-Identity to raise trust in digital ticketing use, and prevent fraudulent use and data loss. The ARIES (2016-2019) project intends to deliver a comprehensive framework for a reliable eID system. It will:

- comprise new technologies, processes and security features that ensure the highest levels of quality in eID;
- be based on trustworthy security documents and biometrics for highly secure and privacy-respecting physical and virtual identity management;
- have the specific aim of achieving a significant reduction in levels of identity theft, fraud and associated crimes.

ARIES will leverage virtual and mobile identification that is cryptographically derived from strong eID documents to prevent identity theft and related crimes in the physical (e.g. an airport) and virtual (e.g. eCommerce) domains. The derivation process and the derived identities will be unambiguously linked to citizens' biometric features, increasing the level of identity assurance when issuing credentials and during authentication. Highest data protection standards will be followed to provide digital privacy-preserving features. Thus, the project will provide a global approach for an eID system in Europe to address European-specific concerns to improve identity, trust and security.

The main focus of the LV-Pri20 (2015-2017) project is the formal and automatic analysis of privacy-preservation in today's ICT. LV-Pri20 will focus on the prevalent wireless media (e.g. RFID protocols, remote car unlocking, wearables, machine-to-machine communication in the Internet of Things (IoT)/ubiquitous computing), but it will not neglect wired environments (given their common cloud connection). LV-Pri20 will assess and automatically analyse privacy-sensitive applications in their standalone execution and in the more involved setting of multiple, concurrent executions. A new model of checking algorithms will be developed. These functions will be incorporated in automatic verification software, which has already proven efficient in analysing highly distributed systems, in line with, for example, the IoT applications envisaged by the project.

4.3.2.4 Data protection

Research was also carried out in the field of social sciences connected to the acceptance of the new ICT developments. Interesting outcomes were brought by the Norwegian Data Protection and Privacy Implication in Road Safety (2008-2010) project. A survey performed by the project showed that, for about half of the respondents, travelling anonymously without any processing of personal data connected to their trip is important. The concern about being exposed to misuse of personal data exceeds that of terror attacks. People are concerned about the possibility of different actors being able to connect data from several sources. However, two thirds trust that the methods used to transfer travel data are secure and that data processing is secure and confidential. About half of the respondents also trust the competence of transport companies and their routines for data deletion after use.

Another issue of concern is the new, fast-developing trend of IoT and cloud computing that can also provide potential threats to transport security. The ECRYPT-NET (2015-2019) project aims to develop advanced cryptographic techniques for the IoT and the cloud. It also aims to implement these techniques in systems that offer a high level of security and increased usability for a wide range of physical computation platforms. ECRYPT-NET will create advanced cryptographic solutions that will be available for commercial applications.

An emerging category of data protection that has been identified relates to the security of global positioning system (GPS) receivers. The risk consists of 'spoofing attacks' through the broadcast of incorrect GPS signals to a receiver.

There is little evidence of actual attacks of this nature having occurred in practice. Nonetheless, it has been identified as a risk, although no projects have been identified that have addressed the risk or how it might be overcome.

4.3.3 Research outcomes

4.3.3.1 Achievements of the research under this sub-theme

A range of results has been achieved in this field. Some results have already been transferred to practical use, especially in the air transport sector, to which the majority of projects were related.

The research outcomes show that aircraft operating costs and the costs of installing monitoring systems costs can be reduced. For example, instead of physically moving experts to carry out structural repairs, the system developed by the WISE project will bring expert assistance to the on-site teams through an advanced augmented reality communication system. Any maintenance site will then be able to benefit from the cumulated expertise, which provides better results than any individual expert and avoids the added inconvenience of delaying the repair. Air flight security will be improved and costs reduced.

Video cameras can provide a useful contribution to airport surveillance (the INTERVUSE project). The technology was developed that has the potential to be a gap-filler to complement surface movement radar (SMR). The INTERVUSE technology can achieve most of the performance requirements of the SMR. Specifically, the strengths of the system are no radiation, lower cost, provision of video and higher update rates.

The operational concepts addressed in the NUP2 project contribute to the improvement of the ATM in different areas and conditions. Improvements were obtained in different key performance areas (KPAs), such as environmental sustainability, efficiency, cost-effectiveness, predictability, safety, flexibility, capacity and security.

The development of an innovative technology to increase the traffic capacity of airports was reached through the SKY-Scanner project. The technology is based on a full laser control of ATZs and the related aircraft movements in a new generation ATM. Another project output is the development of a useful, innovative technology to achieve optimal operational performance of the aircraft-supporting infrastructure, seeking to reduce the number of transport fatalities.

Different procedures for managing aircraft in a security emergency being controlled by a flight reconfiguration function were defined by the SOFIA project. One of the project outcomes is a defined need of a ground authority and/or system (like a ground security decision system) at the European level to:

- take legal responsibility for decisions;
- generate and track the flight plan for the aircraft under the control of the 'Flight Reconfiguration Function';
- coordinate with national authorities, air navigation service provider (ANSP) and airports.

Some research outputs are connected with land transport. In particular, improvements have been made in the field of V2X communications.

The B-VHF project generated several valuable scientific results in terms of definitions of B-VHF system requirements; B-VHF functional scope, architecture and high-level system design; and the development of the B-VHF system operational concept.

The EVITA project established a standard for secure automotive sensor/actuator networks and attempted to assure a broad utilisation of the EVITA results in the automotive industry. The impact will be multiplied once vehicle manufacturers and electronics suppliers implement the secure architecture specification and protocols that were developed.

4.3.3.2 Transferability from research to practical use

Different projects developed software and/or secure architecture specification and protocols for uptake by industry. Technology developed in the INTERVUSE project has the potential to be a gap-filler to complement SMR. The PRESERVE project designed, implemented and tested a secure and scalable V2X security subsystem for realistic deployment scenarios. The B-VHF project generated a definition of the functional scope, architecture and high-level system design of the B-VHF concept for an advanced aeronautical communications system. It also developed a simulation framework, system operational concept, narrowband interference simulator and channel model to assist in the transfer of the technology to practical use.

The operational concepts addressed in the NUP2 project contribute to the improvement of ATM in different areas and conditions. The WISE project achieved improved aircraft monitoring by developing concepts based on new wireless technologies and integrated sensing solutions with autonomous sensor powering and low consumption. The SKY-Scanner project developed a demonstrator system, based on a rotating cylindrical laser range-finder array, capable of detecting and tracking aircraft up to at least 6 nautical miles from the ATZ. The SOFIA project has defined different procedures for managing aircraft in security emergency situations through control by a flight reconfiguration function. The development of a cost-efficient hardware security module (HSM) in the EVITA project will help many embedded applications to efficiently improve their security.

4.3.3.3 Indications for future research

It is important to monitor the current situation regarding the deployment and compatibility of systems, particularly in terms of road and rail traffic. An intensive collaboration of different stakeholders in cyber security, privacy and ICT should be supported. In addition, the phenomena of the IoT and cloud computing represents potential sources of near-future threats, as huge financial investments and human resources are now being committed. Their impacts on data mining, the reliability of information, the ability to deliver in-time discovery and response capabilities, and privacy protection should be priorities for future European research and development activities. Future requirements for automotive applications will include cyber security by design, communications through secure links and remote data storage.

Another issue which requires more attention in future research is industrial control systems (ICS). According to the European Union Agency for Network and Information Security (ENISA), a coordinated testing of capability at the EU level is needed to ensure the cyber security of transport ICS[10]. These systems are often outdated and have traditionally been designed as independent systems. Without sufficient security requirements, they are not prepared to deal with current threats.

Future research needs have been identified especially in the field of air transport. The WISE project demonstrated an energy density of vibration-based energy scavenging that is better than state-of-the-art performances. Further investigation in material use and size reduction can make this technology common in future applications. The WISE project further identified that future research or the development of a product for an aircraft systems application should address these issues to allow WISE technology to be fitted routinely to aircraft. Ongoing research is needed in a topic that was opened in the SOFIA project – to make aircraft more secure by themselves. This project also determined further research should be promoted to test the flight reconfiguration function software and tools on ground simulators in advance of flight trials. An integration of project results, mainly in the air transport area (tools, software, protocols or approaches), is especially desirable.

10 https://www.enisa.europa.eu/news/enisa-news/ics-without-sufficient-cybersecurity-controls-require-coordinated-testing-of-capability-at-eu-levels

4.3.3.4 Implications for future policy development

European policy and coordination should continue to devote special attention to digital security. This need was emphasised by the outcomes of the CARONTE project with cyber security indicated as a top priority.

The Norwegian 'Data Protection and Privacy Implication in Road Safety' project brought interesting outcomes that could influence future policy development. A web-based survey conducted as part of this project showed that the concern about being exposed to misuse of personal data exceeds that of terror attacks. The worry about misuse of personal data is on a level with that of being a victim of assaults or criminal behaviour when walking and cycling. People are concerned about the possibility of different actors being able to connect data from several sources. The concern is more prevalent in men than women and the concern grows with increasing age. Future policy development should take this into account and ensure cyber security and privacy have a high priority for transport users.

4.3.4 List of projects

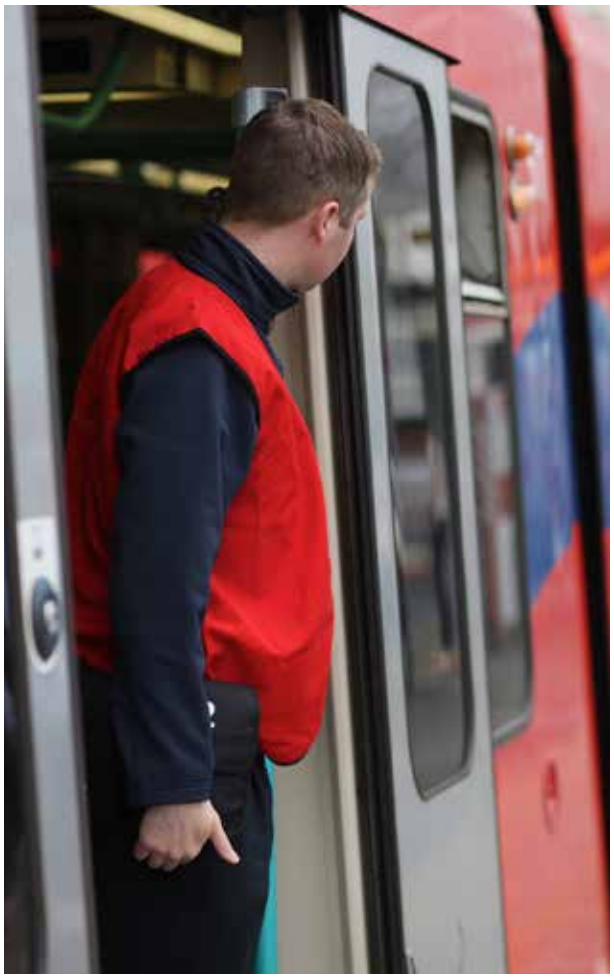
Table 4-3 lists the projects included in this sub-theme assessment.

Table 4-3 Projects reviewed in the cyber security, privacy and ICT sub-theme

Project acronym	Project name	Project duration	Source of funding
AINARA	Automation and Intelligence solutions for Automated Road transport systems https://goo.gl/0WXaDj	2015–2017	EU (Horizon 2020)
ARIES	reliAble euRopean Identity EcoSystem https://goo.gl/EQ6xXQ	2016-2019	EU (Horizon 2020)
B-VHF	Broadband VHF – Aeronautical Communications System Based on MC-CDMA https://goo.gl/Avn3iI	2004-2006	EU (FP6–Aerospace)
CARONTE	Creating an Agenda for Research On Transportation sEcurity https://goo.gl/OmI7RW	2014-2016	EU (FP7–SEC)
CITYMOBIL2	Cities demonstrating cybernetic mobility https://goo.gl/0s9MDR	2012-2016	EU (FP7–TPT)
CockPitCI	Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures https://goo.gl/Eo3TWE	2012–2014	EU (FP7–SEC)
COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities https://goo.gl/sOL8if	2006-2009	EU (FP6)
CYSM	Collaborative Cyber/Physical Security Management System https://goo.gl/9rxEb3	2013-2014	EU (CIPS)
ECRYPT-NET	European Integrated Research Training Network on Advanced Cryptographic Technologies for the Internet of Things and the Cloud https://goo.gl/MHO4bf	2015-2019	EU (Horizon 2020)
EVITA	E-safety Vehicle Intrusion proTected Applications https://goo.gl/NWIXSM	2008-2011	EU (FP7–ICT)
ICSI	Intelligent Cooperative Sensing for Improved traffic efficiency https://goo.gl/06EE82	2012-2015	EU (FP7–ICT)
INTERVUSE	Integrated Radar, Flight Plan and Digital Video Data Fusion for SMGCS https://goo.gl/iq2qmT	2001-2004	EU (FP5–IST)

Table 4-3 (Continued) Projects reviewed in the cyber security, privacy and ICT sub-theme

Project acronym	Project name	Project duration	Source of funding
LV-Pri20	Logic-based Verification of Privacy-Preservation in Europe's 2020 ICT https://goo.gl/9rHybE	2015–2017	EU (Horizon 2020)
MEDUSA	MEDUSA, a Meteorological Decision Support System for Aviation https://goo.gl/PvNRp8	2010-2014	EU (FP7–People)
MICIE	Tool for sistemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures https://goo.gl/fAltCU	2008-2011	EU (FP7–ICT)
MITIGATE	Multidimensional, IntegraTed, rIsk assessment framework and dynamic, collaborative Risk ManaGement tools for critical information infrAstrucTurEs https://goo.gl/oJFuF4	2015-2018	EU (Horizon 2020)
NUP2	North European ADS-B Network Update Programme Phase 2 https://goo.gl/OUwpQT	2004-2007	EU (MIP-MAP)
PRESERVE	Preparing Secure Vehicle-to-X Communication Systems https://goo.gl/qApUo6	2011-2014	EU (FP7–ICT)
SIRTAKI	Safety Improvement in Road & rail Tunnels using Advanced ICT and Knowledge Intensive dss https://goo.gl/aPxJG6	2001–2004	EU (FP5–IST)
SISSDEN	Secure Information Sharing Sensor Delivery event Network https://goo.gl/BLhAKq	2016–2019	EU (Horizon 2020)
SKY-Scanner	Development of an Innovative LIDAR Technology for New Generation ATM Paradigms https://goo.gl/BNv2EC	2007-2010	EU (FP6–Aerospace)
SOFIA	Safe Automatic Flight Back and Landing of Aircraft https://goo.gl/H9A0YI	2006-2010	EU (FP6–Aerospace)
STAR-TRANS	Strategic Risk Assessment and Contingency Planning in Interconnected Transport Networks https://goo.gl/gIkMcj	2009-2012	EU (FP7–SEC)
WISE	Integrated Wireless Sensing https://goo.gl/UXMWEo	2005-2008	EU (FP6–Aerospace)
N/A	Security tool for risk analysis in harbour installations https://goo.gl/jVVVFd	2008-2009	National (Spain)
N/A	Data Protection and Privacy Implication in Road Safety https://goo.gl/HVLlii	2008-2010	National (Norway)
N/A	Universal radio gateway for IP communication in dispatch systems https://goo.gl/Vaz2hP	2014-2017	National (Czech Republic)
N/A	Using related GNSS safe applications for elimination safe and security risk by transport https://goo.gl/I9n1ye	2012-2014	National (Czech Republic)



4.4 Staff security training

4.4.1 Introduction to the sub-theme

Having qualified security staff plays a key role in the protection of transport systems. Therefore, it is important that security staff have adequate levels of training to increase their preparedness to prevent and manage threats and possible terrorist attacks. Other staff in the transport sector should also be trained, according to their job requirements, in dealing with security issues. For staff not directly dealing with security operations, there should be training that provides basic information on how to respond to security threats. For example, the SECUR-ED (2011-2014) project prepared training courses in the security field for the following groups of people:

- front-line employees and passengers;
- security employees;
- operators in security command and control centres, and operational control centres;
- security managers.

Security training should be comprehensive enough to cover a wide range of jobs and situations and generic enough so that the numerous operators can easily adapt them to local conditions.

It is necessary to link training with technologies, including future developments and procedures. Security training should also ideally encompass the 'refresher' method (i.e. repetitive short training courses, drills, etc.) to strengthen the preparedness of the trained staff, and increase the preventive and remedial security capabilities in the transport sector. Furthermore, the skills, education and training procedures for security staff are different from country to country and even between companies in the same regions (e.g. the CARONTE (2014-2016) project).

Projects under this sub-theme should identify best practices for training and educating staff. They should take account of different levels of security needs (depending on transport purpose, region and type) and provide recommendations or standards for education and training procedures for general staff and security personal. Training should not only aim to improve the skills of staff, but also to assist in identifying gaps in security. It should provide staff with the skills to raise customers' security awareness without causing fear, to detect crisis situations at an early stage and to react in an appropriate manner. The training package should comprise a step-by-step set of modules necessary to provide a basic qualification for staff.

4.4.1.1 Overall direction of European-funded research

European-funded research projects dominate the sub-theme of staff security training (24 of the 28 projects analysed). Most of the projects focused on the preparation of staff education programmes, including applying innovative approaches to education (e.g. using interactive games that simulate different kinds of situations and threats (the CRISIS (2010-2013) and BEMOSA (2009-2012) projects).

Another research direction of this sub-theme focuses on providing information to decision makers and politicians with the aim of preventing criminal threats and of increasing security, such an example is the preparation of a decision support system (the SIAM (2011-2014) project). A further aspect is the establishment of a sound collaboration with police, security, emergency and military services including a framework for cooperation of public and private institutions (the COUNTERACT (2006-2009) project).

There is a clear trend towards:

- including modern technologies in the newest training programmes, which simulate a wide range of possible threats and situations;
- developing solutions that are independent of human operator interpretation;
- improving security and security management systems;
- minimising human errors.

Another apparent trend is developing complex management systems for emergency events that can coordinate all the respective groups of people using wide datasets and diverse data sources.

4.4.1.2 Overall direction of nationally funded projects

Of the 28 projects analysed under this sub-theme, only four were nationally funded and even these were only partially related to staff security training. More precisely, these projects focused on:

- air security (the Slovak Speaker verification as an add-on element of the Air Traffic Management security (2015-2017) and the Czech The Utilisation of Crisis Management, Risk Management, Systems Engineering Tools and Modern Technologies to Improve Security at International Airports in the Czech Republic (2013-2015) projects);
- the reduction of the probability that catastrophic events will happen and the reduction of the vulnerability of systems exposed to such events (the Italian Guidelines for evacuation plans by simulation of transport systems in emergency conditions (2004-2005) project);
- suicide prevention on bridges (the Swiss Suicide prevention on bridges: Fundamentals (AGB2003/013) (2004-2006) project).

It should be noted that the publicly funded projects dealing with staff security training form only part of the activities in this field. Commercial organisations in the transport sector (or industry organisations, such as the International Civil Aviation Organization (ICAO)) prepare their own training and other education programmes to increase the security knowledge of their staff.

4.4.2 Research activities

The research activities under this sub-theme include developing training methods that use modern technologies to reflect the current situation and threats. Their outputs of the projects are focused on staff of security and transport companies, on companies at transport terminals and on the general public, including decision makers and politicians (supported by decision-support systems). Some projects prepared training material to teach staff how to use new technologies and security management tools developed under these projects (e.g. the SUPPORT (2010-2014) project for ports, included a new port-security management system using e-learning, a manual for drills and exercises, together with an examination module). However, improvements in training content and methods are often relevant to all transport modes. Various systems for staff security training have been prepared for all transport modes.

The L4S (2009-2011) project focused on developing an innovative framework – the Advanced Collaboration in Crisis Management (ACCM) Framework. This addressed the effective development of collaboration competencies for the specific challenges of crisis management in the transport sector (including air and sea). The aim of L4S is to further extend and customise the platform to other critical infrastructure (such as energy, financial services and the food industry).

A set of ACCM simulation games represents widely deployable, advanced, interactive, technology-enhanced solutions that guarantee the effective understanding and internalisation of collaborative decision-making processes when:

- under extreme time pressure;
- facing the lack and uncertainties of information;
- dealing with the diversity and emotions of people.

The simulations developed effectively address the interpersonal dimension of speed-relationship building, and the trust and role definitions between crisis managers in the transport sector. They provide tools to train managers, organisations, employees and the public.

In sea transport, an on-board docking simulation was developed to improve crew and pilot training when manoeuvring a vessel. The simulation was designed to be modular and easily parameterised so that it can be applied to a wide range of vessels (the EC-DOCK (2002-2006) project). Another research activity focused on tug simulators, including a three-dimensional simulator that enables tug skippers to judge the distance to the assisted ship (the EFFORTS (2006-2009) project).

Regarding road transport, there have been research activities focusing on how to improve security against terrorist attacks, the specification of needs for education and training, and the preparation of a web-based tool for policy makers and stakeholders in public transport. Further research activities have focused on intermodal freight transport, energy production and transmission infrastructure (the COUNTERACT project) and training packages (staff training in best practices) to enhance the security of urban public transportation in medium and large cities (the SECUR-ED project). The LOGSEC (2010-2011) project offered security training and awareness building regarding crime related to the security of logistics and supply chains, including various types of theft, smuggling and violations of intellectual property rights. Another dimension covered is that of the risk and fear of terrorist attacks on, and the exploitation of, logistics systems.

In the field of air transport, training programmes for airport staff, based on a behaviour model that reflects the complex reality in airports, have been prepared (the BEMOSA and CRISIS projects).

The most recent projects in security (the SURVEIRON (2016-2018), BODEGA (2015-2018), MESMERISE (2016-2019) and IMPACT (2015-2017) projects) aim to develop systems that would provide support to security staff to prevent emergencies. The systems would work automatically, and independently collect and analyse a wide range of data provided by security cameras, telephone calls, social networks and mobile phones, data on travel behaviour and socio-cultural characteristics, etc. However, the quality of education and training in the security field remains an important factor in providing security in the transport sector.

The SKILLFUL (2016-2019) project focuses on all transportation modes and multimodal chains (which constitute a key trend for future transport concepts), and on all levels and types of workers to review the existing, emerging and future knowledge and skills requirements. It also aims to identify new business roles in the education and training chain.

4.4.3 Research outcomes

4.4.3.1 Achievements of the research under this sub-theme

The SECUR-ED project developed a mass transport security knowledge platform that enables industrial organisations to develop innovative security solutions and integrate them into an operator's legacy systems and organisational structures. In addition, it helps operators to set the right requirements for upgrading programmes. Training represents one of these integrated outputs. The different modules (made up of best practices, procedures, training, and hardware and software) were selected and packaged with standard interfaces and tested in various European cities including Madrid, Paris, Milan, Berlin, Brussels, Izmir, Lisbon and Bucharest. Training courses developed under this project include a security awareness course for front-line employees and passengers; a security course plus refresher training for security agents, operational control centre/closed-circuit television (OCC/CCTV) operators and security managers; and emergency and crisis preparedness training programmes.

The project analysed the existing training and learning activities in security and formulated the following shortcomings of these activities:

- the requirements in crisis situations that have an impact on competence are fuzzy;
- the competencies available to stakeholders are not clear;
- specific crisis situations and the specific competence needs of different stakeholders derived from them are too complex to cover with general training;
- the configuration of training and learning strategies follow no systematic logic or path, and are often unique activities that are not transferable to other crisis scenarios;
- training and learning activities, and a substantial improvement in competencies to cope with crisis situations are difficult to be measured in a meaningful way.

The lessons learned from the development of the SECUR-ED training are:

- Before implementation, all training lessons should be properly adapted to the relevant local conditions – language, country/regional regulations, transport modes and specific to company processes, etc.
- The text and the images (or other support tools used) of training lessons should be adapted to the local context of the trainees to help them better understand the lessons and to improve familiarisation with the public transport environment.
- The 'train-the-trainer' lessons (and kit) are highly appreciated because they help operators to do the training themselves. However, a significant challenge in this field is finding qualified people to deliver this course.
- In the lessons, try to strengthen the links with law enforcement and first responders so they are familiar with each other's protocols and to increase efficiency.
- Training should not only aim to improve staff training, but also to identify gaps in the general public transport operators' architecture.
- To tap the entire potential of the lessons, it is sometimes necessary to complement security training with other related subjects (e.g. training with (enhanced) psychological components).

The BEMOSA project developed a training programme that considers all the airport security stakeholders. Advanced software simulations to capture and predict social behaviour under stressful emergencies provide the platform for the training modules and training packages that can be readily, and at minimum cost, applied to airports across Europe. This leads to increased efficiency of air transport by decreasing false alarms, increased safety through training and increased coordination for all stakeholders in cases of emergency and security threat.

Under the CRISIS project, a critical incident management training system, using an interactive simulation environment in airport operational security, was developed. Using an interactive games concept, trainees are able to practise situation and cue assessment, problem diagnosis, decision making and action coordination in real-time in response to a critical incident. This allows staff to train individually against the system, as a team within an organisation, across organisations and at different levels of the command hierarchy. It adopts a three-stage development strategy that integrates, tests and iteratively evaluates user performance at each step of the way.

4.4.3.2 Transferability from research to practical use

Results under this sub-theme have a direct use in real cases and there are usually no serious barriers to applying the training programmes in practical use. Furthermore, a significant number of privately run training and education programmes have been prepared by commercial companies and by international organisations (including United Nations bodies such as ICAO) to enhance security.

4.4.3.3 Indications for future research

The research must:

- react to new developments in IT and mobile applications;
- study the possibilities of the additional use of these (passenger) applications to support security and operations, intelligent surveillance and decision-making service, automatic scanning and analyses;
- prepare training programmes that would be universal enough to cover various threats and possible terrorist attacks.

The training should further reflect demographical changes, immigration and other social development. Because of the rapid development of these factors, security training must be regularly updated and improved, and adjusted to the requirements of different staff roles. Another aspect for future research might include the use of modern technologies in training programmes (e.g. various simulation tools and models). Training programmes could use simulations and mobile applications to train staff, so reducing the need for dedicated in-person training. A specific field of research is needed on how best to communicate security messages to passengers and how to build up a society-wider security culture.

4.4.3.4 Implications for future policy development

The security threats faced by transport operators and users range from daily crime and anti-social behaviour (such as group violence, vandalism and graffiti) to serious crime (such as the use of arms and firearms, and terrorist activities involving explosives or toxic materials). These threats can lead to people being harmed, physical damage to transportation assets, service disruption or systems shutting down!

A key role is played by security staff, despite the growing importance of technology in this field. Transport companies and operators have established some prescribed interfacing and training, but the provision of further information to, and training of, passengers and the public is needed. The policy should support further training for new technologies, support cooperation so that various emergency teams can easily work together and share data and technologies. It is also important to coordinate research activities on staff security training between publicly funded projects and the outputs of private companies in the transport field.

4.4.4 List of projects

Table 4-4 lists the projects included in this sub-theme assessment.

Table 4-4 Projects reviewed in the staff security training sub-theme

Project acronym	Project name	Project duration	Source of funding
BEMOSA	Behavioral Modeling for Security in Airports https://goo.gl/C4QzSN	2009-2012	EU (FP7–TPT)
BODEGA	BOrDErGuArd – Proactive Enhancement of Human Performance in Border Control https://goo.gl/Yjui02	2015-2018	EU (Horizon 2020)
CARONTE	Creating an Agenda for Research ON Transportation sEcurity https://goo.gl/OmI7RW	2014-2016	EU (FP7–SEC)
COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities https://goo.gl/s0L8if	2006-2009	EU (FP6)
CRISIS	CRitical Incident management training System using an Interactive Simulation environment https://goo.gl/hdaJtl	2010-2013	EU (FP7–SEC)
EC-DOCK	Easy Controlled Docking https://goo.gl/8u06GX	2002-2006	EU (FP5–Growth)
EFFORTS	Effective Operation in Ports https://goo.gl/h1tLbR	2006-2009	EU (FP6–SUSTDEV)
IMPACT	Impact of Cultural aspects in the management of emergencies in public Transport https://goo.gl/tL6Mqm	2015-2017	EU (Horizon 2020)
L4S	Learning 4 Security https://goo.gl/XqRYdw	2009-2011	EU (FP7–SEC)
LOGSEC	Development of a Strategic Roadmap towards a Large scale Demonstration Project in European Logistics and Supply Chain Security https://goo.gl/BpN02G	2010-2011	EU (FP7–SEC)
MESMERISE	Multi-Energy High Resolution Modular Scan System for Internal and External Concealed Commodities https://goo.gl/SwgKJI	2016-2019	EU (Horizon 2020)
SECUR-ED	Secured Urban Transportation – European Demonstration https://goo.gl/xjcr8s	2011-2014	EU (FP7–SEC)
SKILLFUL	Skills and competences development of future transportation professionals at all levels https://goo.gl/nU1mNx	2016-2019	EU (Horizon 2020)
SIAM	Security Impact Assessment Measure – A decision support system for security technology investments https://goo.gl/lg46YV	2011-2014	EU (FP7–SEC)
SUPPORT	Security UPgrade for PORTs https://goo.gl/GKM5SG	2010-2014	EU (FP7–SEC)
SURVEIRON	Advanced surveillance system for the protection of urban soft targets and urban critical infrastructures https://goo.gl/HSCtYB	2016-2018	EU (Horizon 2020)

Table 4-4 (continued) Projects reviewed in the staff security training sub-theme

Project acronym	Project name	Project duration	Source of funding
N/A	Guidelines for evacuation plans by simulation of transport systems in emergency conditions https://goo.gl/Hy1vrk	2004-2005	Italy
N/A	Speaker verification as an add-on element of the Air Traffic Management security https://goo.gl/1rVWAA	2015-2017	Slovakia
N/A	Suicide prevention on bridges: Fundamentals (AGB2003/013) https://goo.gl/xBLPr1	2004-2006	Switzerland
N/A	The Utilisation of Crisis Management, Risk Management, Systems Engineering Tools and Modern Technologies to Improve Security at International Airports in the Czech Republic https://goo.gl/fe4y1b	2013-2015	Czech Republic

4.5 Cargo security

4.5.1 Introduction to the sub-theme

According to the European Commission[11], 90% of the world's cargo is transported in maritime containers, but only 2% is physically inspected by customs authorities. Moreover, it is estimated that around 40% of commercial exchanges internal to the EU are transported by sea. Therefore, it is evident that the risk for potential illicit activities – of various types – involving the content and integrity of maritime containers, and other general cargo has to be taken in consideration. These concerns also apply to land and air freight transport.

Further more, cross-border and international freight transport has increased substantially over the last decades. For this reason, an increasing number of regulations, initiatives and agreements between freight companies and Member States have been progressively implemented. The ISPS Code, a comprehensive set of measures to enhance the security of ships and port facilities, is just one example of those regulations that created the precondition for the further development of research and applications in supply chain and cargo security.

Technology development and digital innovation are playing a fundamental role in further improving the way that shipments are controlled, detected and monitored 'door-to-door' along the entire supply chain. The research and identification of common standards, and the pursuit of a wider and more effective interoperable system are also relevant for ensuring that high security standards are applied throughout European countries.

The challenges facing international intermodal freight logistics are efficiency and security. These apparently – and potentially – conflicting issues can be more effectively managed by means of well-timed and up-to-date management and visibility of supply chains, where data can be more easily shared between business and governments, and by integrating the solutions across the supply chain.

4.5.1.1 Overall direction of European-funded research

In total, 32 projects on the topic of cargo security were identified and reviewed in the TRIP database, of which 30 were European-funded projects. A wide set of projects and initiatives relating to this sub-theme have been carried out in FP4 to FP7 (i.e. from 1994 to 2013) and are running under the current Horizon 2020 Programme.

The Joint Research Centre (JRC) of the European Commission provides direct support to the Directorate-General for Taxation and Customs Union (DG TAXUD) in matters relating to risk management and security of the supply chain, underpinning the international agreements between the EU and international counterparts. In collaboration with the European Antifraud Office and DG TAXUD, the JRC developed the ConTraffic[12] project to provide information from customs and security authorities on container routes and risk assessment services to users.

4.5.1.2 Overall direction of nationally funded projects

Only two projects focusing on cargo security have been identified at a national level. These are from the Czech Republic and Hungary (the latter co-financed by the EU under the Trans-European Transport Network (TEN-T) initiative) and concern the management of the transport of dangerous goods.

The Czech project aimed to establish an international compatible information system (software, prototype, functional sample) based on GNSS to automatically monitor transport with high-risk dangerous goods. The Hungarian initiative focused on inland water transport, specifically on a section of the Danube River in the northern part of the country. This identified stretch of river has an increasing volume of dangerous goods being transported, so more effective safety and security measures and a fully operable pilot system between Vienna (Austria) and Százhalombatta (Hungary) were needed.

11 https://ec.europa.eu/jrc/en/research-topic/monitoring-container-traffic-and-analysing-risk
12 https://contraffic.jrc.ec.europa.eu/

The reasons behind the small number of national initiatives is probably linked to the international character of freight transport, and transport in general, meaning that technical standards and agreements need to be identified and harmonised at cross border and international levels. Wider forms of collaboration between customs operations, border controls and the police need to be established beyond a single state authority and jurisdiction to ensure overall high security standards.

4.5.2 Research activities

Most of the research activities and projects carried out on this sub-theme over the past two decades focused on waterborne transport (inland and overseas), including its supply chain and related facilities (such as seaports and terminals). Also, the aviation sector, specifically air cargo, played a role in developing solutions for threat detection and prevention (see Section 4.2). As previously indicated, this focus on waterborne transport is explained by the dominant transport of international freight by sea routes and by the presence of specific security legislation in air and maritime transport.

The research review below is organised along the topics of cargo security in:

- container and supply chain management;
- maritime transport and port management;
- aviation and road transport sectors.

4.5.2.1 Security of container and supply chain management

The definition and implementation of a 'cargo black box' as a tool to monitor and track a ship's route was one of the topical issues in the first projects implemented in the late 1990s and early 2000s.

The introduction of the maritime black box was intended to lessen the risks of accidents through a better knowledge of accident origins, so improving the education and training of seafarers, improving passenger safety, reducing costs of accident compensation and speeding up the resolution of related disputes. The MBB (1996-1999) project developed a standardised maritime voyage data recording system, whereas the S-CBB (2002) project aimed to accelerate the adoption and use of telematics applications to prevent fraud in export activities. It did so by developing a wide and comprehensive functional architecture of a secured cargo black box.

The advance in security through the introduction of the cargo black box led to wider attention being focused on the detection and continuous monitoring of supply chains. This allows the risk of cargo being interfered with, when in transit and far from inspection checkpoints or customs controls, to be limited to some extent. Therefore, several projects have developed and tested smart solutions. These take advantage of new technologies and solutions to check, in real-time, the content and amount of goods transported, and to track any possible unauthorised modification of the carriage. Some of them took the opportunity to undertake a wider range of actions, intended to integrate and manage freight flows better.

Some projects focused on the simplification and better overall management of cargo, through several approaches and specific procedures. The CHINOS (2006-2010) project developed a system intended to combine all three 'container status monitoring' parameters (identification, seal condition and damage documentation) into one single system and ensure that the overall system was compatible with the upcoming container traceability standard proposals. The INTEGRITY (2008-2011) project developed procedures and technologies allowing for supply chain visibility, security and predictability through real operational business and customs operations in door-to-door supply chains in the major trade corridor from China to the EU.

Although focused on the specific sector of postal operations, the SAFEPOST (2012-2016) project identified the main security threats, threat actors and security gaps in postal operations. The initiative led to the development of a 'postal security target operating model'. This is expected to enable postal operators, customs and other relevant actors to understand how to securely exchange information related to security and to optimise postal flows. The CORE (2014-2018) and IMCOSEC (2010-2011) projects put an emphasis on securing supply chains, specifically addressing the identification of security gaps.

The CONTAIN (2011-2015) project worked on the development of an EU surveillance system for shipping containers that could encompass regulatory, policy and standardisation recommendations; new business models; and advanced container security management capabilities The system would support transport security stakeholders in managing container security threats as part of an integrated approach to the management of transportation networks. The project established integration facilities between security agencies such as the European Border and Coast Guard Agency (FRONTEX), European Maritime Safety Agency and other EU platforms such as e-Customs and the vessel traffic monitoring and information system (SafeSeaNet). The EURIDICE (2008-2011) project conceived the 'intelligent cargo' concept, in which services can be instantly combined in relation to the capabilities of self-awareness, context awareness and connection through a global telecommunications network to support a wide range of information services. The platform simultaneously improved the logistics, business processes and public policy aspects of freight transportation by dynamically combining services at different levels.

The importance and number of IT solutions conceived and tested (data sharing, e-freight, cloud) has increased in recent years and has found applications in maritime shipping. For example, the use of e-freight technologies, which are becoming widespread to replace paper documents with electronic data and messages, was improved and made more efficient by the CASSANDRA (2011-2014) project. This was achieved through the development of a data-sharing concept that allowed for extended risk assessments by governments and companies. The COMCIS (2011-2013) project deepened the topic of interoperability between e-freight systems as a follow-up initiative to previous EU projects and others that were developed in commercial undertakings[13]. Many available data sources were aggregated, such as data from container security devices, port communities, logistics networks and terminal operators.

Solutions with a high innovation character were developed by further initiatives. The first one, developed by the CWT (2015-2016) project, aimed to improve the (not always high) correctness standards of custom declarations, which rely on manual and semi-manual processes carried out by importers and exporters. This project used a collaborative cloud platform that supported the process from export to import end-to-end.

The second was a much more specific innovation targeted at detecting cargo while on route. Taking account of the high risk of damage or vandalism of external antennas, the solution designed by the ISOTRACK (2008-2011) project was targeted at developing a robust composite container door that withstands typical operational loads and stresses and, most importantly, that is transparent to radio frequency (RF) radiation. It also incorporates electronic sensors to detect chemical explosives, radioactive substances or stowaways. The C-BORD (2015-2018) project is tackling the need to deploy comprehensive and more accurate, cost-effective container non-intrusive inspection (NII) solutions to potentially protect all EU sea and land borders, satisfying a large range of container NII needs. Since a single NII technology cannot cope with all different targets and potential illegal contents and substances transported, the toolbox that is being developed will include five complementary innovative detection technologies – improved X-rays, target neutron interrogation, photofission, sniffing and passive detection. Finally, the AXCIS (2013-2017) project is intended to develop a manufacturer-independent reference database of X-ray images of illegal and legitimate cargo, procedures and algorithms to harmonise X-ray images from different cargo scanners and measurement parameters. It will also develop a system for the automated identification of potentially illegal cargo. This kind of innovation appears to show promise and to have the potential for wider application.

4.5.2.2 Cargo security in maritime transport and port management

Ports represent the core area where cargos is handled, controlled and normally distributed to its final destination, often by other modes of transport (e.g. rail and road). Since ports are normally located close to densely populated areas and great urban agglomerations, security is of fundamental importance. This is even more so in recent years where the alert state, due to potential terrorist attacks, has been raised by many port authorities and police forces across EU Member States. Possible accidents and damage occurring in ports may result in appalling consequences in terms of human lives, financial costs necessary to repair the infrastructure and severe impacts on the overall economy, at regional and even national scales.

Security projects in port areas concerned several aspects. These included the overall management of security, the safe manoeuvring of cargo in harbours and ships (so minimising the risk of hard landings (the EC-DOCK (2002-2006) project)), navigation in ports and its organisation, the structural problems caused by the progressive and constant increase in ship size, and the unchanged availability of space and local facilities at ports (the EFFORTS (2006-2009) project).

Another relevant focus is associated with the protection of maritime infrastructure that is related to goods (and passenger) transport, energy supply and port infrastructure. Following the implementation of the Port Security Directive, there has been a set of initiatives, at various extents and with different objectives, to strengthen security in ports. The SECTRONIC

[13] It showed how the following e-freight systems would be integrated: Logit 4SEE (resulting from Freightwise), Smart-CM Neutral Layer and ICS-SEAP (from Smart-CM), SICIS (from Integrity), Port Community Systems (e.g. from Descartes) and commercial platforms (e.g. from DHL).

(2008-2011) project developed an integrated security system that is able to work at any time and in all weather conditions. It is able to communicate security information of significance to the infrastructure authorities in real time, aggregate reports and display any security-related information of significance in an intuitively understandable way.

Based on the progress achieved in recent years with the adoption of the ISPS Code, the SUPPORT (2010-2014) project developed formal specifications and tools based on open standards to aid security upgrades in EU ports. These were designed to be complementary to, and useable by, other European initiatives. The improvements were accomplished by setting up a participation process and seeking input from representative stakeholders concerning potential preventive and remedial security actions.

Other projects focused their attention at a policy level with the aim of providing clearer indications and renewed guidelines for further action for the whole sector. Following the accidents to the motor vessels Erika (1999) and Prestige (2002) that resulted in large spills of heavy fuel oil, the MARNIS (2004-2008) project, through a holistic and harmonised approach, focused its research activities into five thematic clusters:

- maritime information management concerning preventive information services to support traffic safety and efficiency;
- supporting technology for navigation, communication and information systems to improve safety and efficiency of maritime traffic;
- safety – remedial measures and the information services needed for preventive and remedial actions;
- information services for the efficiency of port operations and security in ports, as well as the preventive and remedial traffic information services in the port environment;
- on-board information services for improved safety, security and efficiency of traffic and transport.

The LOGSEC (2010-2011) project developed a strategic roadmap for a large-scale demonstration project in European logistics and supply chain security, characterised by adequate security for the benefit of business and governments, with short time delays and low cost implications.

However, the broader contribution in this sense was given by the MARPOS (2008-2010) project, which aimed to assist the European Commission in the implementation of the EU Maritime Transport Policy objectives by using the results of past research work in the field of maritime transport. The inputs were included in a user-friendly, searchable internet database through which all interested parties could find valuable information about the results of EU research since FP5. The projects included in the database are classified into five thematic areas, among which are safety and security – where new technologies and intelligent systems related to safety and security of people and infrastructure, and protection against unauthorised and unexpected actions of any kind, have been developed.

4.5.2.3 Cargo security in aviation and road transport sectors

The volume of air freight transport is constantly growing. In 2010, according to the Directorate-General for Internal Policies of the Union, 14.2 million tonnes of goods were transported across all EU airports, indicating an average annual increase of 4.8% in the sector between 2002 and 2010. In the future, the proportion of air freight transport may play an even more important role in the air transportation industry. Air cargo transportation systems are designed to provide fast and efficient shipment of goods. Because of its relatively high cost, air freight is competitive mainly for long distances and relatively light, high-value or perishable goods. These features make them highly vulnerable to potential security threats.

Research activities, some of them still ongoing, were channelled in two directions – innovative solutions and exchange information.

The FLY-BAG2 (2012-2015) project was a follow-up to the FP7 FLY-BAG project, which developed and demonstrated a blast-resistant, textile-based luggage container for narrow-body passenger aircraft. FLY-BAG2 aimed to exploit the knowledge gathered in the previous project to develop new containers for cabin (addressing the 'least-risk bomb location' requirements) and cargo environments, and to enlarge the experimental validation of the new concepts including full-scale tests on retired aircraft. The CITRIMACC (2015-2017) project has conceived a smart and secure cargo container and information exchange platform that can reduce screening costs and eliminate tampering risks. This will be achieved by combining advanced composite materials; secure PIN-code lock; electronic shipping documents; web-based software for data storage; and a 24-hour communications system based on GPS, general packet radio service (GPRS) and RFID technology for continuous real-time visibility. The project aims to validate such a system in real-life environments.

Similarly, the EUROSKY (2013-2017) project aims to provide facilitation measures to safeguard international supply chains and the security of citizens while fostering international co-operation and a broad stakeholder engagement. In particular, a wide cooperative model for air-cargo security and facilitation, including key performance indicators, was developed. The project also improved automated detection and alarm resolution solutions to provide faster and more accurate detection of dangerous substances with reduced rates of false positive indications. A technological infrastructure was also developed for electronically connecting air-cargo stakeholders together; and amplifying their security capabilities through faster communications, shared scans and intelligence, real-time optimisation, pooled resources and synchronised actions.

The TruckSecurity (2015) project developed and implemented an alarm system for road transport vehicles based on technology developed by the Norwegian company IDTEQ. Conventional car alarm systems are not designed to handle the specific threats of fuel theft or cargo theft, since their market focus is on cabin protection and vehicle tracking.

IDTEQ provides a leading technology for secure and reliable alarm detection in remote and noisy environments. The IDTEQ incident detection technology samples and analyses sound. Sensors and proprietary signal processing algorithms detect specific incidents and discard false incidents.

4.5.3 Research outcomes

4.5.3.1 Achievements of the research under this sub-theme

Many projects demonstrated the feasibility of improved supply chain visibility and security. Companies have at their disposal more tools to reduce administrative and planning errors along the supply chain, while public authorities can use data more efficiently, so improving the overall effectiveness of cargo security (as in the CASSANDRA and CORE projects) and through using open standards (the CWT project).

The MBB project paved the way for the mandatory equipping of commercial vessels with voyage data recording systems, defining a modular maritime black-box concept and prototype.

A higher level of interoperability between ICT systems used in transport and logistics services was achieved, along with the provision of a basis for semantic (i.e. content-related) standards in these sectors (the COMCIS project).

New and innovative tracking and alarm systems (the ISOTRACK, TruckSecurity and CORE projects) have been implemented on additional transport modes.

4.5.3.2 Transferability from research to practical use

A lot of research has been carried out on cargo and container management. This seems the most mature topic and the one that delivered some ready-to-use technologies and practices for operators and the market.

The CARONTE (2014-2016) project highlighted that many security solutions are already available on the market. However, they are frequently not easily implemented and integrated into transport applications – especially cargo transport – as it is a low-margin business with little tolerance for measures that do not bring immediate benefits. Confirmation of the benefits could indicate the need for applied research for more economical solutions or for activities that support the market entry of new solutions.

4.5.3.3 Indications for future research

Actions to improve the overall performance of port, road and rail freight transport security are still required.

Considering the continuous rising volumes of goods transported in the air cargo sector, further research and measures should be undertaken to ensure that the highest security standards are maintained.

4.5.3.4 Implications for future policy development

The European Commission, in its 'Europe's Seaports 2030: Challenges Ahead' memo[14], highlighted the strategic importance of seaports for future EU competitiveness, and the potential for job creation and to attract investment. Although a clear and direct reference to security aspects is not mentioned in this document, it is evident that a reorganisation and upgrade of ports management, including dedicated security systems facilities and security-related processes, will be needed in the medium term. This could be integrated into a possible upgrade of the Port Security Directive, aimed at providing new policy impetus and clearer and shared EU guidelines towards renewed security standards (e.g. risk of terror attacks).

The recent bankruptcy of the shipping company Hanjin[15] revealed additional security implications for containers and ships stuck at ports for longer than expected.

14 http://europa.eu/rapid/press-release_MEMO-13-448_en.htm
15 http://www.joc.com/special-topics/hanjin-shipping-bankruptcy

4.5.4 List of projects

Table 4-5 lists the projects included in this sub-theme assessment.

Table 4-5 Projects reviewed in the cargo security sub-theme

Project acronym	Project name	Project duration	Source of funding
ACXIS	Automated Comparison of X-ray Images for Cargo Scanning https://goo.gl/Jd1YTC	2013-2017	EU (FP7–SEC)
CARONTE	Creating an Agenda for Research ON Transportation sEcurity https://goo.gl/OmI7RW	2014-2016	EU (FP7–SEC)
CASSANDRA	Common assessment and analysis of risk in global supply chains https://goo.gl/dR8f5H	2011-2014	EU (FP7–SEC)
C-BORD	effective Container inspection at BORDer control points https://goo.gl/rw5kZa	2015-2018	EU (Horizon 2020)
CHINOS	Container Handling in Intermodal Nodes – Optimal and Secure https://goo.gl/WW3mAs	2006-2010	EU (FP6–SUSTDEV)
CITRIMACC	Circulation Pilot with Continuous Control of Multi-Modal Air Cargo Containers https://goo.gl/pc5pBI	2015-2017	EU (Horizon 2020)
COMCIS	Collaborative Information Services for Container Management https://goo.gl/fPAi7D	2011-2013	EU (FP7–TPT)
CONTAIN	Container Security Advanced Information Networking https://goo.gl/HVukQ6	2011-2015	EU (FP7–SEC)
CORE	Consistently Optimised Resilient Secure Global Supply-Chains https://goo.gl/sfQ3Fc	2014-2018	EU (FP7–SEC)
CWT	Clearview Trade – Cloud based collaborative custom system https://goo.gl/xMS0zc	2015-2016	EU (Horizon 2020)
EC-DOCK	Easy Controlled Docking https://goo.gl/8u06GX	2002-2006	EU (FP5–Growth)
EFFORTS	Effective Operation in Ports https://goo.gl/h1tLbR	2006-2009	EU (FP6–SUSTDEV)
EURIDICE	European Inter-disciplinary Research on Intelligent Cargo for Efficient, Safe and Environment-friendly Logistics https://goo.gl/MBUlsH	2008-2011	EU (FP7–ICT)
EUROSKY	Single European Secure Air-cargo Space https://goo.gl/0vs7CZ	2013-2017	EU (FP7–SEC)
FLY-BAG2	Advanced technologies for bomb-proof cargo containers and blast containment units for the retrofitting of passenger airplanes https://goo.gl/Ce3LFO	2012-2015	EU (FP7–TPT)
IMCOSEC	Integrated approach to IMprove the supply chain for COntainer transport and integrated SECurity simultaneously https://goo.gl/mm1hO1	2010-2011	EU (FP7–SEC)
INTEGRITY	Intermodal Global Door-to-door Container Supply Chain Visibility https://goo.gl/38zLf0	2008-2011	EU (FP7–TPT)

Table 4-5 Projects reviewed in the cargo security sub-theme

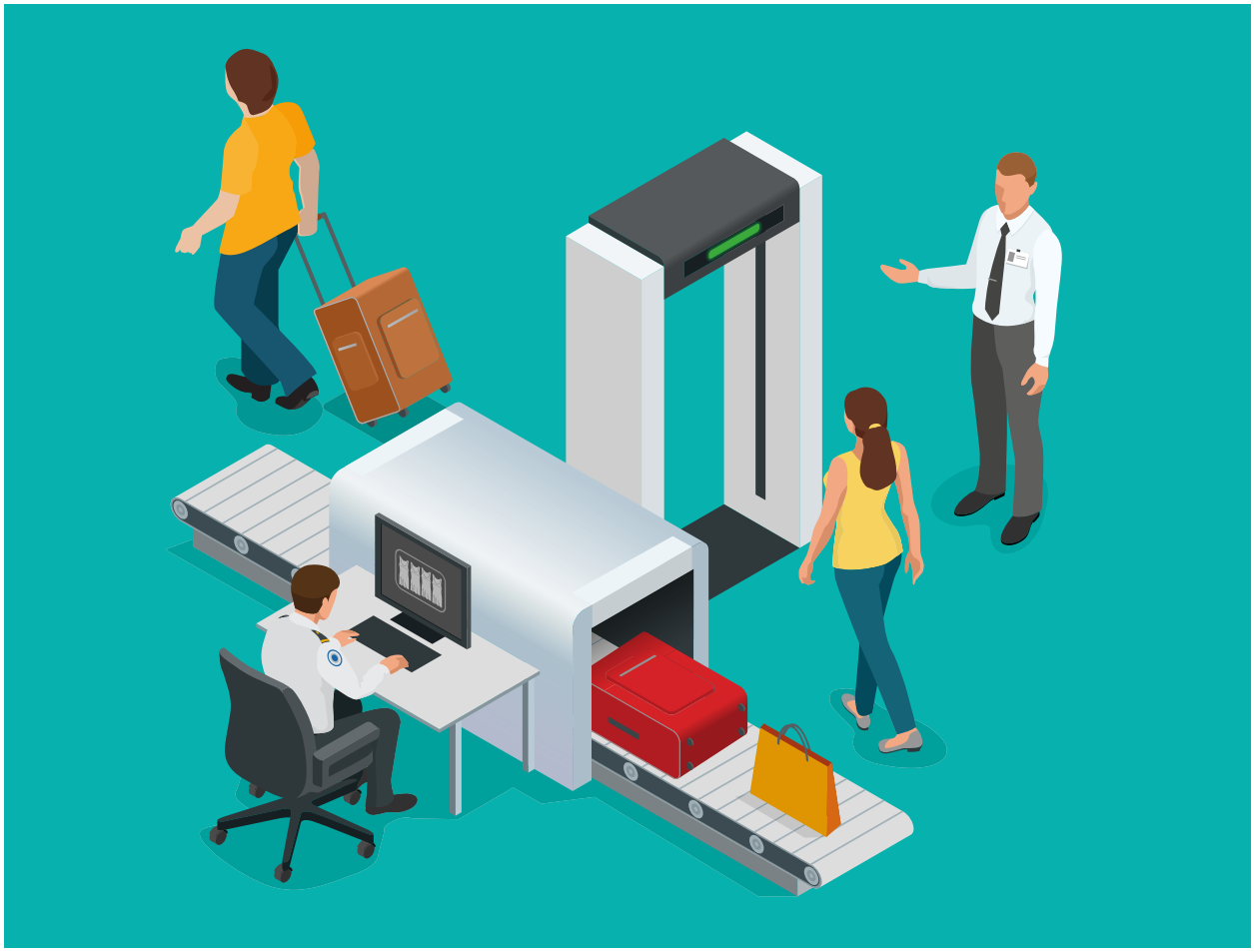
Project acronym	Project name	Project duration	Source of funding
ISOTRACK	ISO Shipping Container Tracking and Monitoring System https://goo.gl/pbr842	2008-2011	EU (FP7–SME)
LOGSEC	Development of a Strategic Roadmap towards a Large scale Demonstration Project in European Logistics and Supply Chain Security https://goo.gl/BpN02G	2010-2011	EU (FP7–SEC)
MARNIS	Maritime Navigation and Information Services https://goo.gl/Ehy8yD	2004-2008	EU (FP6–SUSTDEV)
MARPOS	Maritime Policy Support https://goo.gl/37FOYr	2008-2010	EU (FP7–TPT)
MBB	Maritime Black Box https://goo.gl/yUv5D3	1996-1999	EU (FP4–Transport)
SAFEPOST	Reuse and development of Security Knowledge assets for International Postal supply chains https://goo.gl/ogzNsg	2012-2016	EU (FP7–SEC)
S-CBB	Secured cargo Black Box https://goo.gl/QXRFre	2002	EU (FP5–Growth)
SECTRONIC	Security System for Maritime Infrastructures, Ports and Coastal Zones https://goo.gl/6Bc6cr	2008-2011	EU (FP7–SEC)
SUPPORT	Security UPgrade for PORTs https://goo.gl/GKM5SG	2010-2014	EU (FP7–SEC)
TruckSecurity	Truck Security – Fuel and cargo theft detection alarm system https://goo.gl/rA5Pdq	2015	EU (Horizon 2020)

4.6 Passenger security

4.6.1 Introduction to the sub-theme

The security of passengers travelling on EU transport networks is of the utmost importance. However, in taking measures to improve security, it is important to balance the need to protect passengers, while still enabling them to use transport networks without too much inconvenience and without incurring the associated costs. Inevitably, different transport modes face different challenges when it comes to security because of their different characteristics. While in the maritime and aviation sectors, the majority of passengers are transported between a relatively small number of ports and airports using a relatively small number of vehicles, the road transport sector has a large number of vehicles that use roads that dominate major towns and cities and reach the most remote areas. The rail sector has more in common with the aviation and maritime sectors in that passengers access the rail network through a limited, albeit much larger, number of points, while there is a relatively smaller number of dedicated trains.

Even within modes, the situation might be different because the security appropriate for an urban road or railway line might not be as relevant for interurban roads and railways. The international nature of much of the passenger and freight transport in the aviation and maritime sectors brings a different set of challenges because aircraft and ships travel outside the jurisdiction of the EU and are subject to different, sometimes less stringent, security regimes. The policy framework and research requirements for the security of passenger transport have tended to be developed in response to specific incidents, even though there is, arguably, scope for a more and more proactive approach. The scope of this sub-theme is the infrastructure and vehicles used by all modes (i.e. transport in the road, rail, aviation and maritime sectors).



4.6.1.1 Overall direction of European-funded research

FP6 began in 2006. This was after the terrorist attacks in New York, Madrid and London between 2001 and 2005, which highlighted the vulnerability of air travel and public transport to terrorist attacks. Research since has focused on various different elements of passenger security. For airports, one of the main issues has been on striking the right balance between security and inconvenience for passengers, and on improving the reliability of security controls. While identifying trends from a relatively small and varied selection of projects is difficult, the XP-DITE (2012-2017) project is taking a more systematic approach, whereas earlier projects focused more on the use of a particular technology (such as the OPTAG (2006-2009) project). There have been few projects that have mainly focused on passenger security on maritime transport, rather than on maritime security more generally. One relevant project that aimed to inform the International Maritime Organization (IMO) guidance on passenger evacuation was the SAFEGUARD (2009-2012) project.

The focus of research on the security of passengers using land-based transport has been on mass public transport, particularly in urban areas. Research has not been limited to the development and demonstration of different technologies, but has also focused on identifying risks (the COUNTERACT (2006-2010) and the MODSafe (2008-2011) projects) and developing appropriate procedures for responding to incidents if they were to occur (the DEMASST (2009-2010) and SECURED (2011-2014) projects). The use of technologies has been researched for the purpose of monitoring generally (the MORYNE (2006-2008) project), but also in relation to providing information in the immediate aftermath of an incident (the ASPIS (2008-2011) project). Again, identifying trends is difficult, but some of the more recent projects are considering different aspects of emergency management, such as how to deal with people from different cultural backgrounds (the IMPACT (2015-2017) project), rather than being more generic. Research has also looked at the design of and materials used in aircraft (the VULCAN (2006-2010) project) and metro trains (the SECUREMETRO (2010-2012) project), and the design of metro stations (the SECURESTATION (2011-2014) project). There have been few projects that focus on the security of private road transport. The projects that do exist also cover efficiency and safety concerns (the BIRDWATCH (2015) project).

4.6.1.2 Overall direction of nationally funded projects

Few national projects were identified that focused on the security of passengers. With respect to aviation and maritime transport, this is probably due to the international nature of these modes, which means that the issues and solutions are international in nature or, at least, need to take account of the realities of international transport and its associated politics. Hence, EU-level research is much more appropriate than national research in relation to the security of these modes. While land-based mass public transport is generally national or local by nature, the issues faced in different countries and cities are similar. Therefore, again, it makes sense for research to be undertaken at the EU level where different experiences and solutions can be discussed. The national projects that have been identified focus on issues that are, arguably, more appropriately dealt with at the national level (e.g. crime at railway stations and design standards for parking) as they will need to take account of wider national and, in many cases, local issues.

4.6.2 Research activities

4.6.2.1 Passenger security in the aviation and maritime sectors

Various research projects have been undertaken in relation to the security of passengers travelling by air, many of which have focused on security procedures at airports. There have been fewer projects focusing on the security of passengers using maritime transport. These projects are discussed in this section. The SAFEE (2004-2008) and COPRA (2011-2013) projects would contribute to passenger security, but are much wider in scope as they focus on threat prevention and detection more generally. They have been covered in Section 4.1.2.

The focus of the OPTAG project was on minimising delays at airports as a result of passengers turning up late at departure gates and, possibly, reducing the associated security checks. The aim of the project was to develop and demonstrate a system for tracking passengers at airports using an RFID tag. The project involved the development of the tag itself and the accompanying imaging system, software and user interface. These were then trialled at Debrecen airport in Hungary. As a result of the trial, the use of an RFID tag as a means of tracking passengers at airports was proven, although further development was needed (see Section 4.6.3).

Airport security was one of the topics discussed at the two-day 'International Conference on Airports' held in Paris in October 2009 (ICOA.10.09 (2009)). The conference brought together policy makers and operators from around the EU and from farther afield to discuss developments relating to airports, and to share innovative ideas about the future direction of the sector. In relation to passenger security, the conference's recommendations included that new airports should be constructed to a sufficient size to enable them to be adaptable to meet changing security needs and that relevant regulations should be harmonised at the European and international levels. It was also concluded that research was needed into new technologies that improve the reliability of security controls, while reducing the inconvenience for passengers. It was underlined that security procedures needed to reconcile two difficult requirements – efficiency and respect for individuals.

The development and testing of scanning technology to detect concealed objects is the subject of the CONSORTIS (2014-2017) project. The technology that is being developed in this project uses a combination of a 'submillimetre wave' video camera and a three-dimensional imaging radar system, together with image forming optics and scanning optomechanics. The system is designed to detect anomalies that may indicate a concealed object. Algorithms will be developed to automate the system and to protect privacy. While the technology will be tested at an airport, it is potentially applicable in other forms of mass transit. End users are also involved in the project to ensure that the results are acceptable from their perspective.

The aim of the XP-DITE project is to move beyond the current approach to airport security, which tends to focus on the performance of individual pieces of security equipment, to a more systems-based approach for the design and evaluation of airport checkpoints. This focus on the system as a whole should enable a more flexible approach to security, so minimising negative impacts such as costs and inconvenience, and thus ensure a more positive experience for passengers. The design of the approach will take account of the needs of security, operational requirements and passengers' perceptions. The subsequent framework will then be used to develop an integrated design tool for airport checkpoints, which will include an evaluation platform that will be tested at two airports, including Schiphol in Amsterdam.

The VULCAN project was concerned with analysing the new composite and hybrid materials that are increasingly being used in the manufacture of aircraft. The aim was to propose measures for reducing the potential damage to such materials from explosions or fires as a result of, for example, a terrorist attack. The project developed relevant material models, failure criteria and vulnerability maps for the materials in response to difference types of explosion and fire. On the basis of this work, strategies were then developed to improve the performance of composite and hybrid materials in explosions or fires, which were then tested on scaled aerostructures manufactured for this purpose.

There have been fewer projects that focus on passenger transport using ships and ferries. This is probably due to the fact that fewer people use the maritime sector for the purpose of passenger travel. Additionally, to date at least, maritime transport has not been the target of terrorist attacks to the same extent as passenger aircraft. However, EU funds have supported projects that would have benefits for passengers using maritime transport. Additionally, some projects (e.g. RANGER (2016-2019)) would benefit passenger security on maritime transport, but focus more generally on threat detection and prevention, so have been covered in previous sections (e.g. Section 4.1.2).

The aim of the SAFEGUARD project was to collate and analyse datasets on the response and assembly times of passengers when a ship needed to be evacuated. The project responded to a call from the IMO whose existing guidance in this area was not based on a sufficiently rich dataset. The datasets collated were used to develop a series of response time distributions that were then used to develop and test different scenarios. On the basis of this analysis, a validation protocol and acceptance criteria were developed, which it was proposed could be adopted by the IMO in revised guidance on ship evacuation.

4.6.2.2 Passenger security for land-based transport

While terrorism is still an issue for passenger security on land transport, particularly at major railway stations and on trains, security against criminal activity becomes more of an issue and so a focus of some research relating to passenger security on land transport.

Some projects (such as CARONTE (2014-2016)), focus on land transport generally, but have explicit implications for passenger security. CARONTE focused on addressing the two main challenges facing land transport from the perspective of security:

- avoiding interruptions to transport networks as a result of terrorist attacks;
- ensuring that transport does not become a means for an attack.

This area is relatively under researched, so the project developed a research agenda for the security of land transport to address the gaps that were identified.

The IMPACT project is investigating the role of cultural factors in managing safety and security issues relating to emergencies on public transport networks. This will include how best to communicate and deal with passengers from different socio-cultural backgrounds. The project will produce a cultural risk assessment methodology and identify solutions that can be used by operators to engage with people and take account of different cultural issues.

The aim of the COUNTERACT project, which was led by the International Union of Public Transport (UITP), was to improve the security of public transport against terrorist attacks in light of the attacks in the United States of America (USA) and Europe in the early 2000s. The project reviewed existing security policies, procedures and technologies, and identified gaps and proposed targeted solutions for addressing these. It brought together a range of relevant information in a knowledge centre. The conclusion was that there was a lack of consistency in terms of the provision of security across the EU and that there was no overarching security policy at the European level for any of the sectors covered. The project aimed to develop a generic methodology for risk assessment for public transport systems and recommended that there was a need to raise awareness of the risks among users of public transport.

The ASPIS project focused on a specific detail of the aftermath of a terrorist incident (i.e. the need to be able to undertake a quick assessment of the situation to plan the rescue operation to save the most lives). The project aimed to address this need through the development of a video 'black box' that was able to send videos recorded just after an event to rescue teams to help with the planning of the rescue. The black box might be used on public transport vehicles or in stations, or on ferries or cruise vessels. The development of the black box and the tests undertaken on it (in collaboration with the SECUREMETRO project (see below) proved to be successful.

The focus of the DEMASST project was on mass public transport. The project recognised that it was not possible, technically or economically, to replicate the security arrangement for air travel on mass public transport because of the increased number of access points. Hence, it aimed to identify the main challenges in relation to the security of passengers using mass public transport and the most promising integrated solutions for addressing these. The project developed a roadmap for a series of demonstration activities, which was taken forward in the SECUR-ED project[16].

The SECUR-ED project undertook a series of demonstration activities aimed at improving the security of mass public transport in the face of a range of different security challenges. While the main demonstration activities took place in Paris, Milan, Berlin and Madrid, some smaller cities around Europe were also involved. The themes explored in the project included the organisation of security, information management, video surveillance, telecommunications and cyber resilience, and the potential response to various types of possible terrorist attack. The results were condensed into a White Paper targeting public transport stakeholders.

The focus of the SECURESTATION project was to improve the resilience of railway stations in the face of a terrorist attack. The aim was to inform the design of new stations and the renovation of existing ones, including the structure of the station, the design of its interior and the design of associated services. Another objective was to ensure that the measures introduced would be cost-effective and so risk-analysis methodologies were harmonised and used to prioritise possible actions.

16 Chmel, S. et al (nd) 'DECOTESSC1 System Description'; see www.decotessc1.eu/DECOTESSC1_System_Description.pdf

The project had two main outputs – a risk assessment methodology focused specifically on passenger stations and a design handbook to support the construction and renovation of passenger stations to improve their resilience in the face of a terrorist attack.

The focus of the UK-funded 'Reducing Crime at Rail Stations in Socially Excluded/High Crime Locations' (2005) project was on crime rather than terrorism. The project was undertaken for the UK's Department for Transport and aimed to identify the reasons for crime at railway stations where it was common. Of particular interest was the extent to which crime was linked to issues associated with the station or whether it was a symptom of social exclusion more generally. The project also looked at existing methods of reducing crime at stations with the aim of identifying the most effective responses[17].

Safety and, to a lesser extent, security in the European guided-transport sector was the focus of the MODSafe project. Previously, this had been a relatively under researched area in which different requirements and certification schemes applied. The project involved major transport operators, including London Underground, Régie Autonome des Transports Parisiens (RATP) in Paris and Metro Madrid. In response to the challenges faced by urban operators of trams, underground and light rail systems, MODSafe aimed to provide a coherent analysis of the risks and hazards facing these systems. It brought together and tested existing knowledge to develop an agreed process and layout for safety systems of guided urban transport systems.

The use of mobile sensors to enhance the efficiency, safety and security of buses was the subject of the MORYNE project. The project developed and successfully demonstrated, using buses in Berlin, a monitoring system that used buses as elements of a mobile monitoring network. The buses that were fitted with the sensors were able to collect data about the environment in which they were operating and communicate this in real-time to a public transport management centre and a city traffic management centre. The information was used to make decisions about the management of public transport and the wider network more generally, which were then passed back to bus drivers as appropriate.

The aim of the SECUREMETRO project was to improve the resilience of metro carriages in the event of a terrorist attack, so reducing injuries to the public and speeding-up the subsequent recovery of the system. The project focused on the development and validation of design strategies – including the selection of materials – that would reduce injuries in the event of an explosion using conventional explosives or firebombs. The project involved a vehicle builder, a system operator and researchers to enable different options to be tested. The main results identified the importance of having windows that separated as a whole from vehicles (rather than shattering), improving the resistance of ceiling panels (so that these do not fall on the passengers or fall onto the ground, making escape difficult) and improving lighting so that it continues to work in the event of an explosion or fire.

17 DfT (2005) 'Reducing Crime at Rail Stations in Socially Excluded/High Crime Locations'; see www.transport-research.info/project/reducing-crime-rail-stations-socially-excludedhigh-crime-locations

The use of broadband services to access the internet for security purposes and the convenience of passengers is the focus of the NTR (2015-2018) project. The internet has the potential to be used to monitor incidents as they occur and provide important information to the driver and those responsible for the overall safety and security of the network. Different national operators are developing different systems for different national circumstances, potentially without sufficient consideration to international travel or, potentially, to the risks of using the internet for this purpose. The project aims to address such concerns.

While there are many projects concerned with the safety of private road transport, there are relatively few that focus on the security of private road transport. Those that do, often cover security as an element of a wider problem. For example, the BIRDWATCH project helped to develop a tool to help car park operators to manage car parks, and to assist with payments and security. The project was supported by Horizon 2020's SME Instrument and support was provided to the Spanish company Quercus to help with the development of the BIRDWATCH parking suite solution. The tool moves beyond the previous state-of-the-art in terms of parking management, as it links various technologies and focuses on linking the vehicle, identified using automatic number plate recognition technology, with other activities in the car park.

The Swiss 'Safety and comfort of car parks' (2001-2005) project also covered security in addition to other factors. The aim of the project was to develop standards for the design and operation of car parks as no such standards previously existed – internationally or nationally. The intention was to inform the planned renovation of some major car parks in Swiss cities. The research was based on surveys and engagement with the main stakeholders to develop standards that could be applied nationally. These covered all elements of the design and operation of car parks, including the access and movement of vehicles and people, service areas (e.g. ticketing and toilets), the size of parking spaces, and the necessary safety and security elements[18].

4.6.3 Research outcomes

4.6.3.1 Achievements of the research under this sub-theme

An important achievement of many of the research and innovation projects on passenger security has been the engagement of the relevant actors, particularly major operators. Projects, such as COUNTERACT, MODSafe and SECUR-ED have all involved operators of public transport networks from major European cities, which suggests that the areas being supported are of relevance to such important stakeholders. A number of the projects, including those mentioned already, but also projects such as SECURESTATION and SAFEGUARD, have developed similar approaches, methodologies and guidelines that might be more widely applied and so bring benefits to operators that were not directly involved in the projects. More recent projects have begun to take more system-wide approaches (e.g. the design of airport check-in areas as in the XP-DITE project or the management of passenger security checks, such as dealing with people from different cultural backgrounds, as in the IMPACT project). Such projects will contribute to the understanding and implementation of ways to improve the security of passenger transport throughout the EU.

Other projects have focused more on the development and testing of technologies that might be used to facilitate improved security, reduce casualties or improve the resilience of the passenger transport system. These technologies can be varied, ranging from those that focus on monitoring to facilitate decision-making (such as the ASPIS and MORYNE projects) to those that develop safer or more resilient materials for transport vehicles (including the VULCAN and SECUREMETRO projects). Other projects aimed to maximise the potential of the rapid developments in communications technologies (e.g. the NTR and BIRDWATCH projects). Such research will have informed the development of technology that has the potential to improve the security of the passenger transport system.

4.6.3.2 Transferability from research to practical use

It is likely that many of the findings of the research projects have been used to at least inform practice in the real world. The fact that major cities were involved in the DEMASST and SECUR-ED projects suggests that their findings will have informed the practice in these cities at least. Similarly, the involvement of relevant operators and manufacturers in projects such as MORYNE, MODSafe and SECUREMETRO suggests that their findings are likely to have influenced the activities of the various operators. One of the operators involved in the ASPIS project, RATP from Paris, was interested in potentially using the resilient communication architecture that was developed in the project.

It is difficult to identify the extent to which the design guide for improving the resilience of railway stations in the face of a terrorist attack produced by the SECURESTATION project has been used in practice. However, one of the project partners, an architects' practice, has been involved in the renovations of some of the major railway stations in London and has mentioned the SECURESTATION project in the context of these renovations[19]. The findings of the SAFEGUARD project were presented at a seminar at the UK's Royal Institution of Naval Architects in November 2012[20]. However, no evidence of these being taken on board in a revised IMO circular, which was the intention of the project, was identified.

---

18 Swiss State Secretariat for Education and Research (2001-2005) 'Safety and comfort of car parks'; see www.transport-research.info/project/safety-and-comfort-car-parks-vss2000454

19 Whitelaw, J. (2014) 'The Euston opportunity: HS2 brings the most exciting design opportunity for decades', Infrastructure Intelligence; see www.infrastructure-intelligence.com/article/apr-2014/euston-opportunity-hs2-brings-most-exciting-design-opportunity-decades

20 World Maritime News (2012) 'RINA to Present SAFEGUARD Project at Passenger Ship Evacuation Seminar (UK)'; see http://worldmaritimenews.com/archives/67126/rina-to-present-safeguard-project-at-passenger-ship-evacuation-seminar-uk/

The support to Quercus that assisted with the development of the BIRDWATCH parking suite has led to the commercialisation of the solution, which was launched at the Intertraffic Amsterdam Exhibition in April 2016[21]. The findings of the Swiss 'Safety and comfort of car parks' project served as the basis of a new Swiss Standard (SN 640 285) on the 'Design and equipment of car parks'. As the UK 'Reducing Crime at Rail Stations in Socially Excluded/High Crime Locations' project was undertaken for the UK's Department for Transport, it might be expected that it informed subsequent policy making or guidance.

The findings of some research projects have been taken forward in other projects. For example, the DEMASST project developed a strategic roadmap for the demonstration of measures to improve the security of mass public transport, which was taken forward in the SECUR-ED project. Similarly, the use of RFID for airport security, as demonstrated by the OPTAG project, has been taken forward at a larger scale in more recent research projects (e.g. TASS (see Section 4.1.2)).

4.6.3.3 Indications for future research

From the behavioural perspective, the direction indicated by projects such as XP-DITE might suggest a way forward for future research needs. This project aims to undertake a system-wide approach to the design and evaluation of airport check-in systems. It could prove beneficial to take similar approaches to the design, implementation and evaluation of different aspects of the security surrounding all passenger transport modes. Projects such as IMPACT, which focuses on dealing with people from different cultural backgrounds in the case of emergencies, also provide a different insight on how different people should be treated. It might be worth further exploring the way in which different people respond when faced with an emergency situation to develop more nuanced responses. Research will also need to reflect the ever-changing nature of the terrorist threat. Therefore, research projects responding to improved knowledge and information gaps resulting from the security responses to new terrorist attacks will also be important.

The technology that could be used to counter threats faced by passenger transport is also changing rapidly, so research needs to ensure that it focuses on the needs most relevant from the perspective of EU added value. Potential areas include using developments in ICT for the purposes of monitoring and sharing information to prevent threats from materialising, and for dealing with emergencies when they occur, in the way that the NTR project is exploring the potential use of the internet for monitoring security on-board trains. Additionally, as the amount of passenger information that is collected increases, particularly as a result of the EU's Passenger Name Record Directive[22], research is needed into how this information might be linked to other information, such as that available on social media, to potentially differentiate the security approach taken for different passengers.

While passenger air travel has the most extensive security checks, mass public transportation faces similar threats, which are less easy to counter as a result of the higher number of access points, higher frequencies of use and shorter journeys. Hence, research could explore the potential to develop scanning technologies that might be more suitable for use on public transport – at stations and on-board vehicles, without greatly inconveniencing passengers. Research could also explore scanning technologies that might be used on vehicles and passengers boarding ferries. The potential to further use CCTV on public transport vehicles and at public transport stations for the purposes of security should also be explored (e.g. by analysing behaviours or identifying individuals through facial recognition).

4.6.3.4 Implications for future policy development

One of the main challenges for policy is to ensure that learning from research projects is taken into account by all of the relevant actors. Within the EU, this means ensuring that the results of research are disseminated and integrated into EU and national policy making, as appropriate. The extent to which it is necessary to integrate the approaches, methodologies and guidelines developed by various projects into EU or national policy framework will depend on the detail of the respective documents and of the importance of widely implementing their findings. As the nature of the threat and, thus, the necessary response, varies by mode and by location, it might be more efficient for approaches and guidelines to be adopted – to the extent necessary – by local operators or by authorities responsible for passenger transport security in different localities. Research on the design of vehicles could be integrated into EU standards, as appropriate.

Research that has implications for international aviation and maritime passenger transport could have implications for the design and construction of ships and airports outside of the EU. In this respect, it will be important to work through the appropriate international channels, such as IMO and the ICAO, or potentially directly with regulators in other countries where there are similar security threats.

21 Quercus (2016) 'Quercus launches powerful BirdWatch Parking Suite', Daily News of Intertraffic Amsterdam (2016), page 44, Route One Publishing.

22 DIRECTIVE (EU) 2016/681 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, http://eur-lex.europa.eu/eli/dir/2016/681/oj

4.6.4 List of projects

Table 4-6 lists the projects included in this sub-theme assessment.

Table 4-6 Projects reviewed in the passenger security sub-theme

Project acronym	Project name	Project duration	Source of funding
ASPIS	Autonomous Surveillance in Public transport Infrastructure Systems https://goo.gl/w3rZ9w	2008-2011	EU (FP7–SST)
BIRDWATCH	The first integral and modular mobility and security solution for smart parking management https://goo.gl/xvmIfG	June to November 2015	EU (Horizon 2020)
CARONTE	Creating an Agenda for Research ON Transportation sEcurity https://goo.gl/OmI7RW	2014-2016	EU (FP7–SEC)
CONSORTIS	Concealed Objects Stand-off Real-time Imaging for Security https://goo.gl/r3slgA	2014-2017	EU (FP7–SEC)
COPRA	Comprehensive European Approach to the Protection of Civil Aviation https://goo.gl/7UI33R	2011-2013	EU (FP7–SEC)
COUNTERACT	Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities https://goo.gl/s0L8if	2006-2009	EU (FP6)
DEMASST	Security of critical infrastructures related to mass transportation https://goo.gl/P6VLQz	2009-2010	EU (FP7–SEC)
ICOA.10.09	International Conference on Airports, October 2009 Paris https://goo.gl/C4M5xQ	2008-2010	EU (FP7–TPT)
IMPACT	Impact of Cultural aspects in the management of emergencies in public Transport https://goo.gl/tL6Mqm	2015-2017	EU (Horizon 2020)
MODSafe	Modular Urban Transport Safety and Security Analysis https://goo.gl/vCEBPQ	2008-2011	EU (FP7–TPT)
MORYNE	Enhancement of public transport efficiency through the use of mobile sensor networks https://goo.gl/PXZ9X2	2006-2008	EU (FP6–IST)
NTR	New technology railway to boost on-board internet, video surveillance and connection services https://goo.gl/2vxgF5	2015-2018	EU (MOBI.Europe)
OPTAG	Improving Airport Efficiency, Security and Passenger Flow by Enhanced Passenger Monitoring https://goo.gl/uz5Jao	2006-2009	EU (FP6–Aerospace)
RANGER	Radars for long distance maritime surveillance and SAR operations https://goo.gl/SsVZRY	2016-2019	EU (Horizon 2020)
SAFEE	Security of Aircraft in the Future European Environment https://goo.gl/30dt1n	2004-2008	EU (FP6–Aerospace)
SAFEGUARD	Ship Evacuation Data and Scenarios https://goo.gl/ZRaoU4	2009-2012	EU (FP7–TPT)

Table 4-6 Projects reviewed in the passenger security sub-theme

Project acronym	Project name	Project duration	Source of funding
SECUR-ED	Secured Urban Transportation – European Demonstration https://goo.gl/xjcr8s	2011-2014	EU (FP7–SEC)
SECUREMETRO	Inherently SECURE blast resistant and fire safe METRO vehicles https://goo.gl/UFGPWM	2010-2012	EU (FP7–TPT)
SECURESTATION	Passenger station and terminal design for safety, security and resilience to terrorist attack https://goo.gl/Ghmpfo	2011-2014	EU (FP7–SST)
VULCAN	Vulnerability Analysis for Near Future Composite/Hybrid Air-Structures: Hardening via New Materials and Design Approaches Against Fire and Blast due to Accidents or Terrorist Attacks https://goo.gl/x6Rqx7	2006-2010	EU (FP6–Aerospace)
XP-DITE	Accelerated Checkpoint Design Integration Test and Evaluation https://goo.gl/DMI8jo	2012-2017	EU (FP7–SEC)
N/A	Reducing Crime at Rail Stations in Socially Excluded/High Crime Locations https://goo.gl/9XsxZM	2005	UK
N/A	Safety and comfort of car parks https://goo.gl/rE74Ka	2001-2005	Switzerland

5 Conclusions and recommendations

5.1 Research environment and development

The theme of transport security started to appear in research funded by the European Union (EU) with the 7th Framework Programme for Research and Technological Development (FP7). The Secure Societies Challenge in Horizon 2020 has given a definitive boost to fully deploy the potential of research activities and transfer into practice a wide number of solutions, technologies and methods for more secure transport systems in Europe. Following the terrorist incidents in Europe in recent years, research in the field of transport security has widened its scope from the aviation and maritime sectors to land modes of transport. This is the trend that emerges from the distribution over time of the research projects analysed as well as from the range of topics covered in recent and ongoing projects.

There are very few nationally funded research projects in this review and this might be seen as a consequence of the international nature of security of transport networks. Indeed, the need for actors to cooperate and endorse a common approach is confirmed by a number of coordination and support actions funded by the European Commission that were carried out over recent years. Among the more significant projects on this aspect are CARONTE and COPRA, in particular for their research roadmaps in the land and air transport sectors respectively.

Research projects have been clustered into six sub-themes – threat detection and prevention; crisis management; cyber security, privacy and information and communications technology (ICT) systems; staff security training; cargo security; and passenger security.

Threat detection and prevention is one of the sub-themes that witnessed substantial development efforts in recent years aimed at deploying innovative technologies. New approaches using monitoring and surveillance systems (e.g. local sensors, electromagnetic, infrared and optical sensing) have been widely tested, particulary in the aviation sector, following the evolution of EU legislation. In parallel, within the same sub-theme, projects were devoted to studying ways to increase the efficiency of detection and prevention systems to reduce traffic delays imposed by passenger and goods inspections.

In the area of crisis management, research moved towards the development of emergency response mechanisms, resiliency planning and strategy development. Also, cyber security, privacy and ICT issues have evolved considerably over the last two decades.

The aviation sector benefited significantly from research achievements that improved, in particular, the European airspace and traffic management infrastructure, the availability and use of alternative communication and monitoring systems (e.g. multicarrier broadband very high frequency (VHF) systems or global navigation satellite system (GNSS) applications) and technologies for automatic flight back and landing of aircraft. These aspects focused essentially on ICT improvements and combined security with more prominent safety issues.

In the land transport sector, the issue of combining ICT with cyber security and privacy topics is now in the early stages. Importantly, the current research framework, Horizon 2020, has dedicated special attention to these aspects with cyber security having now a predominant role in the Secure Societies Challenge. As already mentioned, security issues in passenger and freight land transport received more attention in recent years, particularly in addressing the security of metro stations and railway hubs.

5.2 Research activities and outcomes

In the area of threat detection and prevention, a significant number of EU and nationally funded research projects focused on the identification, assessment and management of threats facing the transport systems. The efforts resulted in different risk assessment methods, tools and methodologies to analyse critical infrastructure and needs for security policies. In addition, decision support systems were applied across all transport modes and, specifically, for each sector.

Improved security procedures were largely developed especially in the aviation sector, but a significant number of projects were also carried out in road transport (e.g. prevention of suicides on bridges, threat detection in parking facilities), and rail and urban terminals.

In threat detection and prevention research, the exploitation of advancing technologies in monitoring and surveillance systems progressed significantly. These included:

- the use of optical technologies for the stand-off detection and identification of explosives in real scenarios at long distances;
- identifying the location of suspicious, delayed or missing passengers in airports and stations;
- the use of unmanned aerial vehicles (UAV) and sensors able to monitor the surface layer surroundings of vessels, platforms and coastal infrastructure.

Technologies have also been developed for real-time safe screening of large numbers of people moving simultaneously towards the entrances of buildings, public transportation or public places and for protecting railway infrastructure from electromagnetic attacks. At the same time, research focused on the efficiency of threat detection and in the facilitation of controls for passengers and goods at checkpoints.

With regard to crisis mitigation and management (i.e. how to best handle crises once they have occurred), projects investigated operational systems and procedures (e.g. evacuation of passengers from large ships) and vehicle/infrastructure intrinsic security features to mitigate the impacts of extreme crisis. Resilience of critical infrastructure and strategic prevention rather than technological advancements characterised this research area.

Digital security is closely linked with the primary objective of improving safety conditions of transport, but also to guarantee data protection and privacy for a wide number of emerging technologies. In this sense, research complemented other cooperative intelligent transport systems (C-ITS) projects especially in the road transport domain (e.g. protection of the vehicle-to-X communication and sensitive data protected against compromise when transferred inside a vehicle). In particular, research addressed the protection from cyber attacks in a remotely controlled critical infrastructure, thus allowing for a predictive capability and the proper response of supervisory control and data acquisition (SCADA) equipment and field units.

Cryptographic techniques for the Internet of Things (IoT) and the cloud were also developed as well as implementations that increased security levels and usability for a wide range of physical computational platforms.

Research in the field of social sciences connected to the acceptance of new ICT developments (e.g. the Norwegian project 'Data Protection and Privacy Implication in Road Safety') was also included in the analysis. A comprehensive framework for reliable e-identity systems for highly secure and privacy-respecting physical and virtual identity management was tested. Current research is addressing the automatic analysis of privacy-preservation in today's ICT.

As part of the staff security training sub-theme, the qualification and preparedness of security staff was addressed by the development of new training methods in combination with modern threat detection technologies. To this end, existing training and learning approaches have been integrated with interactive simulations and web-based tools. In this area, a number of decision support systems, analysis of behavioural aspects and collaborative framework among different bodies (police, security, emergency and military services) have been developed.

In the sub-theme of cargo security, innovations in tracking, alarm systems and black boxes have increased the level of security in harbours and ships, and on aircraft. Research devoted to the enhancement of interoperability between ICT systems has improved security along the entire supply chain.

An important achievement of many of the research and innovation projects on passenger security has been the engagement of the relevant actors, particularly major operators. National and European projects carried out demonstration activities aimed at improving the security of mass public transport in a range of different security challenges.

5.3 Indications for future research

Detection and prevention of threats to the infrastructure and operational systems are very relevant elements of transport security in all sectors. It is important that expertise, applications and research findings in some domains, such as aircraft and airports in particular, are transferred to other areas. Within this context, it is also relevant to continue to study solutions that are able to improve efficiency and effectiveness of passenger and freight security controls.

Further research in the crisis and emergency management domain is needed for the development of more integrated solutions across all modes of transport that would make it possible to overcome sectoral approaches. The use of 'big data' for better management of crisis situation and improvements to humanitarian logistics are also aspects that deserve broader investigation.

In parallel with the study of innovative technologies and procedures, there continues to be a need to constantly upgrade and improve the security training of transport staff, perhaps with the support of simulation tools.

Future research in the cyber security, privacy and ICT domains should continue to focus on the deployment, compatibility and privacy protection of the different IT systems while increasing the cooperation of different stakeholders and actors especially in the land transport sector. Also, the impacts on data mining, reliability of information, in-time discovery, and response and privacy protection should be a focus of future pan-European research and development. They have a particular relevance to the emerging and sensitive domains of the IoT and cloud computing and to allow the normal operational functioning of transport systems in the event of a cyber attack. The protection from cyber attacks and hackers becomes even more relevant considering the development of transport systems where mobility is based on vehicles connected among each other and with the infrastructure.

Actions to improve the overall performance of port security and the security in road and rail freight transport are expected outputs from a number of ongoing projects. A transfer of knowledge, solutions, standards and practices from the shipping and supply-chain management sectors to road freight transport has to be promoted as well.

The system-wide approach to the design and evaluation of airport check-in systems should also be applied to the different aspects (including behavioural elements) of the security surrounding all passenger transport modes. There is big potential for the development and use of new technologies to counter threats and monitor security on passenger trains. Scanning technologies suitable for use on public transport that could also be used on vehicles and passengers embarking onto ferries have to be further explored.

5.4 Implications for future policy development

Future policy development has to consider the need for a more universal and integrated approach to transport security across transport modes.

The role of research support and coordination actions should be reinforced, and aligned with activities and discussions within existing policy and research platforms at EU level. These should include the Regulatory Committee for Maritime Security (MARSEC), the established stakeholders and expert advisory groups in maritime and land-transport, and the networks and efforts put in place by the European Commission's Joint Research Centre (JRC). In particular, the JRC could facilitate a more direct transfer of research achievements into the work of the competent EU bodies dealing with security issues and responsibilities in the transport sector (e.g. the European Organisation for the Safety of Air Navigation (Eurocontrol), customs and maritime border authorities).

The definition of standards and processes and the cooperation between actors should be underpinned with clear rules and guidelines. This need is particularly evident in the public transport sector where local operators have a key role.

Research in the domain of transport security has been shown to have beneficial implications for cross-border, intra-EU and international freight and passenger transport. Efforts at a policy level should aim to systematise and disseminate the results of research into EU and national policy frameworks.

The legislative framework for the aviation and maritime sectors has evolved rapidly in recent years. Although the Port Security Directive (2005/65/EC) is still to be fully implemented in most Member States, the introduction of security standards has led to improved organisation of key nodes such as seaports and airports. Research projects have also demonstrated that the level of security in railway and metro stations can be improved.

The need for EU-wide security requirements and standards for road and rail transport should be addressed urgently. Research can complement the path for introducing EU legislation addressing land transport security.

6 References/bibliography

European Commission

European Commission. (2013).
Second report assessing the implementation of the Directive on enhancing port security [COM(2013) 792]

European Commission. (2012).
Commission staff working document on Transport Security. SWD(2012) 143 final. Brussels: European Commission

European Commission. (2011).
WHITE PAPER Roadmap to a Single European Transport Area. Towards a Competitive and Resource Efficient Transport System, COM(2011) 144 final. Brussels: European Commission

European Commission. (2011).
Commission staff working document. Impact Assessment on the possible use of security scanners at EU airports COM (2011): European Commission

European Commission. (2010).
Communication on the Use of Security Scanners at EU airports COM(2010) 311/4. Brussels: European Commission

European Commission. (2010).
Commission Recommendation of 11 March 2010 on measures for self-protection and the prevention of piracy and armed robbery against ships [2010/159/EU]

European Commission. (2010).
Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe (COM(2010) 673 final of 22.11.2010)

European Commission. (2009).
Report assessing the implementation of the Directive on enhancing port security [COM(2009) 2]

European Commission. JRC. (2009).
Technical Aspects of Port Area Security (TAPS II)

European Commission. (2008).
Commission Regulation (EC) No 324/2008 of 9 April 2008 laying down revised procedures for conducting Commission inspections in the field of maritime security

European Commission. (2006).
Report from the Commission to the Council and the European Parliament on transport security and its financing [COM/2006/0431 final]

Other documents

Directive.
2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security

Regulation.
(EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 and its implementing acts lay down measures for the implementation of the common basic standards on aviation security

Regulation.
(EC) No 324/2008 of the European Parliament and of the Council on procedures for conducting Commission inspections in the field of maritime security

Regulation.
(EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security

Regulation.
(EC) No 2320/2002 of the European Parliament and of the Council of 16 December 2002 establishing common rules in the field of civil aviation security

ICAO.
Convention on International Civil Aviation – Doc 7300. (1944).

International Convention for the Safety of Life at Sea.
(SOLAS Convention). (1974)

Whitelaw, J. (2014).
'The Euston opportunity: HS2 brings the most exciting design opportunity for decades', Infrastructure Intelligence

Wallis. (2009).
Economic Development Benefits of Transport Investment. Land Transport New Zealand Research Report 350

World Maritime News (2012).
'RINA to Present SAFEGUARD Project at Passenger Ship Evacuation Seminar (UK)'

Quercus (2016).
'Quercus launches powerful BirdWatch Parking Suite', Daily News of Intertraffic Amsterdam (2016), page 44, Route One Publishing

7 Glossary

The following abbreviations have been used in this review.

ATM	Air traffic management
ATZ	Aerodrome traffic zone
CCTV	Closed circuit television
EU	European Union
GNSS	Global navigation satellite system
ICAO	International Civil Aviation Organization
IMO	International Maritime Organization
IoT	Internet of Things
ISPS Code	International Ship and Port Facility Security Code
IT	Information technology
JRC	Joint Research Centre
RFID	Radio frequency identification
V2X	Vehicle to everything

www.transport-research.info

Publication: Research Theme Analysis Report Transport Security
Luxembourg: Office for Official Publications of the European Union

ISBN: 978-92-79-63149-8
DOI: 10.2832/074992
Catalogue: MI-04-16-975-EN-N