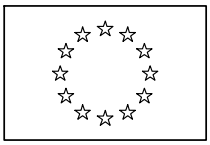

EUROPEAN COMMISSION

Brussels, 31.5.2012
SWD(2012) 143 final

COMMISSION STAFF WORKING DOCUMENT

on Transport Security

COMMISSION STAFF WORKING DOCUMENT

on Transport Security

1. INTRODUCTION

Effective transport systems are essential to Europe's prosperity, having significant impacts on economic growth, territorial cohesion, social development and the environment. At the same time, transport has always been subject to acts of unlawful interference, ranging from simple criminal acts on the premises of transport providers, to robberies of cargo when being transported, acts of piracy and hijacking, and terrorist acts[1].

The EU already has a sad history of terrorist attacks on transport[2]. The psychological cost of the loss of life and caring for the injured in deliberate unlawful acts against transport is incalculable.

However, security is not simply about terrorism or attacks on passengers. The economic cost of transport crime is high. For example, cargo theft from lorries in the EU is estimated to cost over €8 billion per year[3].

Security in a transport context seeks to prevent acts of unlawful interference against passengers, freight or the transport infrastructure. Security should give users confidence that they can use transport. Transport – and thus transport security - has also an important international dimension: in order to ensure security within the EU it may be necessary for transport security to be performed outside the EU before a journey to the EU commences.

The aim of this Staff working paper is to consider what can be done at the EU level to improve transport security, particularly in areas where putting in place common security requirements would succeed in making Europe's transport systems more resilient to acts of unlawful interference. Whilst there are European security requirements in the aviation and maritime sectors, such requirements do not exist for land transport. In this instance, the creation of an Advisory Group on Land Transport Security is necessary.

This working paper complements the Commission's 2011 White Paper on Transport[4] which identified the creation of a land transport security advisory committee as one of the priorities of EU transport policy.

This is also underlined in the Commission Communication "The EU Internal Security Strategy in Action: Five steps towards a more secure Europe" which 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[5].

---

1 Most recently, in October 2011, the railway system in Berlin was the target for bombs.

2 This includes 191 deaths in the 2004 Madrid rail bombings, 52 killed in the 2005 London tube and bus bombings, and 270 killed in the 1988 bombing of PanAm flight 103 over Lockerbie, UK.

3 Source: Transport Asset Protection Association (TAPA)

4 'Roadmap to a Single European Transport Area – towards a competitive and resource efficient transport system'. COM(2011) 144 final of 28.03.2011.

5 COM (2010) 673 of 22.11.2010, in particular pages 9 and 10.

In parallel, the EU Counter-Terrorism Coordinator has repeatedly drawn attention to the terrorist threat to transport security, and identified the value of EU action in promoting higher standards and better coordination.

2. ISSUES HINDERING TRANSPORT SECURITY

There are several reasons why transport security is not as well advanced in the EU as a whole as it could be.

For much of the transport sector security is not a positive selling feature that attracts customers or passengers[6] . Consequently, security can be perceived by some transport operators to be a negative cost, or even something that is not their responsibility to provide, taking into account that the return and effectiveness of investments in security is difficult to measure.

Mandatory requirements for transport security generally occur reactively following major incidents. Given the relative infrequency of such incidents there has not been a political urgency to develop pro-active mandatory security requirements.

While transport security for passengers is generally given a high profile, especially in the aviation sector, cargo has often been neglected (with the exception of aviation security where the risk is high of cargo being used as a means of placing a bomb on board an aircraft). One possible reason why cargo security has not been a priority for regulators is that criminal acts against cargo are perceived to be 'victimless crimes'. Clearly they are not.

Difficulties also arise with intermodal transport hubs where the cross-modal nature of operations may mean that the level of security is not consistent throughout the hub. For example a railway station at an airport may have a lower level of overall security than the airport building, yet may be just as attractive a target for terrorists.

The creation of a European Single Market and the application of Schengen Rules in the Member States led to the large-scale removal of border controls within the European Union. Whilst this has been beneficial to citizens and the economy as a whole, it has not been accompanied by sufficient efforts to deal with the possibilities for cross-border crime.

Finally, the attitude towards the risks from terrorist attacks against transport targets varies considerably throughout the EU. Whilst it can be argued that some Member States have a higher risk of being subject to terrorists acts than others, nobody can foresee what the motivation for tomorrow's cause may be.

3. THE ADDED VALUE OF ACTION AT THE EU LEVEL

Whilst transport security policy should be developed at national or local level under the principle of subsidiarity, a large proportion of transport operations occur among Member States and it is clear that there is an added value to certain actions being taken at the EU level.

Good EU-wide baseline levels of security are relevant to all Member States, especially with the free movement of persons and cargo. The risk of criminality has, potentially, a cross-

[6] the specialist sector dealing with the transport of valuable cargo is a notable exception

border dimension, therefore common approaches to ensure a good baseline level of transport security throughout the EU is desirable.

There is a 'force-multiplier' effect of EU27 acting together, rather than as individual Member States. This is particularly important in international fora, when investing in research, and in outreach in Third Countries. All of these issues are important in the field of transport security.

Finally, where the EU has no baseline standards for transport security there is a risk that those countries with low levels of security become the 'entry point' into the EU for security risks.

4. EU LAND TRANSPORT SECURITY POLICY: POTENTIAL AREAS FOR DEVELOPMENT

This section proposes areas where policy should be developed at the EU level to improve land transport security, and contrasts the sector with the aviation and maritime sectors where existing security policy already exists.

4.1. Land transport security: specific weaknesses at the EU level

It should firstly be stressed that not all weaknesses will apply throughout the EU as a whole. In parts of the EU the levels of land transport security are to the highest global standards. Rather, this section identifies where the absence of common approaches or standards throughout the EU leads to weaknesses, inconvenience or additional cost.

Land transport continues to be a major target for both criminals and terrorists. Yet the issues pertaining to land transport security are many and complex. The maritime and aviation sectors have already demonstrated the added value that comes from having policy and operational guidance and coordination mechanisms, in the form of Committees of Member State experts as well as from Stakeholder Advisory Groups.

To help in policy development on land transport security, as announced in the Transport White Paper, the Commission is establishing [in Decision xx/2012] an Advisory Group on Land Transport Security. The Group will provide a forum for Member State representatives responsible for land transport security policy and also law-and-order issues – usually the competences of different ministries – to discuss with the Commission topics where there would be added value for action at the EU level.

It is important that industry stakeholders have the possibility to give an input into policy development at the earliest possible stage. To this end the Member States' Advisory Group would be complemented by a Stakeholder Advisory Group on Land Transport Security, comprising of key stakeholder organisations representing transport operators, transport infrastructure managers, equipment manufacturers and transport user organisations at EU level.

4.1.1. Security of transport interchanges and mass transit security

Transport interchanges are potentially attractive targets for terrorist attacks, since they offer the possibility to cause havoc to more than one mode of transport. Furthermore, their intermodal nature may permit weaknesses in the security approaches followed. For example the level of security practiced at metro and railway stations located at airports may be lower

than that practised in the airport terminals themselves, yet an attack on an airport railway station will affect both the rail services and the airport operations.

In addition, it should be noted that the scope of EU legislation on aviation security is defined in such a way that the focus is on prevention acts of unlawful interference to aircraft. This means that airport car parks, airport railway stations and even the check-in areas of airports are not covered by existing EU aviation security requirements. In airport terminology they are considered to be 'landside'. It is therefore appropriate that the land transport security advisory group should look at the ways of developing better integrated security at multimodal transport interchanges, and consider if action at the EU level is needed.

4.1.2. Rail security

The development of a trans-European high-speed rail network has been a major European achievement. Furthermore, considerable work has been undertaken to harmonise safety requirements for the railway sector across the EU. However, no similar exercise has been done as regards railway security.

In the rail sector the Commission should consider setting EU-wide security standards for the high-speed rail network. The network has a European dimension, whilst high-speed rail is a potentially attractive target for terrorist acts.

Consideration should also be given to having EU legislation that requires security features to be incorporated into the design of rail and subway rolling stock and infrastructure. EU level baseline security standards would provide a common and adequate level of protection to rail transport to the benefit of businesses and passengers, and would ensure consistency of approach across borders. This would avoid risks of duplication and incompatibility of rules associated with the implementation of local or national systems, thus in turn assisting the good functioning of the Single Market.

4.1.3. Training of staff

A security system is only as good as the security staff that is employed to perform the task. It is important that security staff have adequate levels of training – both initially and recurrent. More work should be done to ensure that the standards are high and broadly equivalent throughout the EU so as to ensure a skilled EU-wide cadre of security staff in land transport.

But all staff working in land transport – and not just those with a security function – should contribute towards ensuring security. The shopkeepers and cleaners at railway stations and bus stations can provide additional pairs of eyes and ears to detect suspicious actions. To do this effectively a basic level of security awareness training is needed.

To address both issues the Commission should consider bringing forward mandatory requirements for training of security staff, together with mandatory security awareness training for all persons working in the land transport domain.

4.1.4. Planning for the aftermath of an incident

Transport security policy is primarily proactive in seeking to prevent security incidents from happening. However, it must be recognised that the concept of ‘perfect’ transport security does not exist. This is particularly relevant for the land transport sector which, due to its "open" operations, makes it more susceptible to security incidents.

If it is acknowledged that "perfect" security cannot be guaranteed in road and rail then transport operators and providers need to be prepared to react appropriately should a major security incident occur. Contingency plans covering likely security scenarios and the measures to be taken to mitigate the consequences would be a way to address this and EU legislation if necessary. Where appropriate such contingency plans should be cross-border.

For the most severe incident scenarios, for example the possibility of attacks using chemical, biological or radioactive weapons (CBR), planning should be done by national authorities, involving the transport operators.

Should a major incident occur then the ability of staff to react correctly can save lives. Transport staff will often be in the forefront before first responders[7] arrive. A legal requirement that all staff working in the public transport domain have basic training to deal with the initial aftermath of a major incident is desirable.

It is necessary that contingency plans are tried and tested by means of regular security exercises, to ensure that the plans work. Exercises are particularly important where many stakeholders are involved as they are a means of bringing the various actors together. The relationship between transport operators and first responders can be crucial in times of a major incident and performing security exercises – both desktop and live exercises – is a key way in ensuring a constructive, workable relationship[8] . Consideration should be given to obliging large transport operators and first responders to perform security exercises on a regular basis.

Transport recovery plans that can minimise the longer-term effects of an actual security incident are also needed. Planning should ensure how at least a core skeleton transport service can be provided swiftly after an incident. Lessons on transport continuity can also be learned from non-security incidents. For example the chaos faced in winter 2010 by rail and air passengers and cargo shippers as a result of snow demonstrated that the transport sector cannot always be relied upon to make continuity planning on a voluntary basis, even for something as predictable as bad weather.

Obligations to perform contingency planning, first aid training and recovery plans will have a cost, and this would be a factor to be evaluated before any legislative proposal would be brought forward. However, it should be noted that these are already done by many land transport undertakings for safety reasons. It thus should be feasible to combine some safety and security procedures at minimal cost.

4.1.5. Technology and equipment

Technology offers a variety of solutions to maintain both a secure and operationally efficient transport system. The EU security equipment industry is among the world leaders in this field. But the threat that equipment has to detect is constantly changing. Development costs are high. Manufacturers will invest in research and development only if they are confident that their product will be having free access to the market. Equally, purchasers of security equipment wish to have assurances that it will perform to a pre-defined standard. Such assurances can only be given by organisations mandated by governments. The lack of a

[7] First responders = those services (e.g. police, fire, ambulance) who are tasked with responding immediately to incidents.

[8] For an example of the importance of the relationship between transport operators and first responders see the UK Coroner's inquest into the London bombings of 7 July 2005.

coordinated system for the setting of standards, including the protection of fundamental rights, and conformity assessment of security equipment in the EU handicaps the well-functioning of the Single Market for security equipment. In order to address the problem, consideration should be given to having uniform performance standards and certification processes for security equipment, together with conformity assessment performed at the EU level.

4.1.6. Research on transport security

The Commission's research budget spends considerable sums on projects that are linked to transport security. Currently large parts of the projects are funded under a specific security theme in the Seventh Research Framework Programme (2007-13). [See Annex II for details]

Beyond 2013 EU security research will be funded by the "Horizon 2020" multiannual research and innovation instrument. It is important that the "Horizon 2020" Framework Programme for Research and Innovation allows for security-related research to remain closely linked to needs and developments in transport security policy, as well as complying with fundamental rights. Research on transport security should underpin policy, including competitiveness, not least in order to ensure "value-for-money". To achieve this, the annual work programme for research should clearly indicate the relevance of the proposals in terms of EU transport security policy.

In addition, there is a need for complementary tools that can swiftly address short-term needs for transport security research and innovation. As an example, following the EU ban of liquids on aircraft in 2006 there was no tool that enabled EU money to be targeted towards the swift development of security equipment for screening liquids (which, if successful, could have led to a prompt lifting of the ban).

4.1.7. Better communication and sharing of classified information

The need (and willingness) of national authorities to share information relating to types of security risk[9] – both terrorist and criminal - is of major importance. However, today's systems of communication are still overly dependent on personal networks that rely on the professionalism of individuals who are willing to provide information[10] . The air cargo security incidents of late 2010 did trigger a change, and a structured mechanism for the exchange of threat and risk information is now functioning in relation to air cargo and mail security involving the EU Situation Centre and relevant Member States' services. This approach should be broadened to land transport to ensure a network that can swiftly share key information at all times.

4.1.8. Security of the Supply Chain

For cargo requiring security it is desirable that it is performed at - or close to the point of shipment and its integrity maintained throughout the journey – end-to-end security. Given that much of the cargo in the supply chain passes via the road or rail sectors then it is clear that the

[9] Specifically, sharing information on types of action e.g. threat from home-made liquid explosives.

[10] As an example, a major (non-UK) urban transport operator informed the Commission that in the immediate aftermath of the 2005 London bombings it found it more efficient to use its own personal contacts in Transport for London in order to learn of the situation, rather than rely on its own Transport Ministry.

absence of common EU rules for supply chain security poses a weakness. Security measures could be better addressed at the start of the journey, rather than screening at airports or ports.

Of course, not all cargo transported by lorry needs to be subject to end-to-end security. Security requirements should be proportional to the risk and so obligatory requirements should be considered only for certain types of cargo, for example valuable cargo, or cargo transferred to aircraft.

Thus it would be desirable to promote existing best practices such as state-of-the-art logistics technologies that offer the possibility to not only track and trace cargo, but also to have the cargo store and/or communicate additional information about the supply chain. European companies are still among the world leaders in logistics and it is in the EU's interest to maintain this competitive advantage, whilst simultaneously improving security. To this extent, solutions provided by the intelligent cargo concept[11] or EU-funded projects like EURIDICE[12] or iCargo[13] should be considered.

Consideration should be given to having an EU standard for end-to-end security for transport operators. Such a standard could take the form either of a binding requirement for the transport of particular types of cargo or as a "Quality Standard" which transport providers would choose to adhere to.

4.1.9. Secure lorry parking

One area where EU action is desirable is in the provision of secure lorry parking. The absence of a coordinated EU-wide network of secure lorry parks – despite continued requests from many parties[14] is clearly noted. The proposal for a regulation on new TEN-T guidelines seeks to address the issue whilst the Directive on the framework for deploying Intelligent Transport Systems[15] provides for standards and decisions on information and booking systems. Consideration should be given to requiring the construction secure parking places at frequent intervals along TENs road networks, complemented by a requirement making available to lorry drivers 'real time' information about availability and quality of parking places in order to maximise their use.

The introduction of the EU-wide eCall system, providing a direct link to emergency services, can help to increase in particular the security of lorry drivers. Moreover, the use of an additional optional data set for heavy goods vehicles may also contribute to increasing the security of road transport freight.

4.1.10. Cybercrime against transport

A number of serious cyber-attacks have been recorded in recent years. Transport is particularly dependent on computerised management systems. For example port community systems are the key element in ensuring coordination of all port activities. With the eventual deployment of e-freight or e-maritime systems, a successful cyber-attack could for example close down one or several maritime or air ports for days with a substantial impact on supply

---

11 See Intelligent Cargo Forum http://www.intelligentcargo.eu/

12 See http://www.euridice-project.eu/

13 See http://www.i-cargo.eu/

14 E.g. a Resolution at the 3043rd meeting of the Justice and Home Affairs Council, on 8 & 9 November 2010

15 Directive 2010/40/EU. OJ L 207 of 06/08/2010 P.1

chains and the economy. The threat posed by cybercrime is a result alose relevant for land transport, which uses such systemsor could knock-on effects.

It is therefore important to ensure that transport is resilient to cyber-attacks. As part of the Commission's Internal Security Strategy, work has already commenced a feasibility study on the creation of a European Cybercrime Centre (ECC), which would be the future focal point in the fight against cybercrime at European level. Final results with recommendations are expected in early 2012 and a Communication is due to follow.

However, as with the security of transport interchanges it is a security threat that falls outside the current mandate of the EU legislation for aviation and maritime security.

If appropriate – and following the forthcoming Commission European Strategy for Internet Security - targeted actions for the transport sector should be considered. This could include requiring that transport operators have backup systems in place for computer systems that will allow swift recovery of core activities, especially relating to the safety of transport, should a cyber-attack occur.

4.1.11. Inland Waterway transport

Inland waterways operations is an area that does not neatly fit into either maritime or land transport operations. Inland waterway craft can operate in the same vicinity as sea-going ships, as well as providing intermodal services. Equally, inland waterways are used to transport large quantities of dangerous goods – often through urban areas - which could make them potentially attractive targets for terrorists. However, it is important to note that, to date, this sector has no security requirements at the EU level and this needs to be addressed.

4.1.12. International activity

The threat posed by terrorism is, like transport, often international in nature. Therefore, it is essential that measures to improve the resilience of transport to terrorist attack are taken whenever possible at the international level and that there is close cooperation with relevant third country partners.

Equally, there are facilitation reasons to have international norms for security. Given the international dimension of transport, it is important that transport can function as seamlessly as possible when crossing frontiers. Differing national requirements for security hinder this. In the domain of land transport there is no international body that sets standards for transport security. Thus, in the first instance, emphasis should be on the EU developing bilateral agreements with countries that have equivalent levels of transport security, with the two-fold aim of promoting the sharing of best practices, as well as ensuring that supply-chain security can be guaranteed.

4.2. Where other modes can lead by example

4.2.1. General

Since 2001, the Commission has developed extensive rules for EU aviation and maritime security, regularly updated to address evolving risks and threats, and developed in conjunction with actions at ICAO and IMO. In aviation, common EU rules are based on the principle that passengers, staff, baggage, cargo and mail must be subject to security controls before being allowed onto an aircraft. In maritime transport, common EU rules emphasise the application

of security controls to passengers, staff, vehicles and cargo entering ports or port facilities, or boarding a vessel. In both cases, the preparation of security plans is a core element of legislation.

The main aspects of EU transport security are:

- policy formulation and regulation;
- inspection activities by the Commission (of national competent authorities, airports, aircraft, ports, port facilities and ships) to ensure correct implementation;
- the obligation for Member States to ensure quality control by performing inspections on a regular basis, and
- feedback from inspections, leading to continuous review of legislative standards.

In principle, this "virtuous circle" ensures that EU legislation is correctly implemented by Member States and thus contributes to the security of citizens, and that legislation is continuously reviewed and, where appropriate, revised.

Furthermore, the possibility exists for Member States to set more stringent security measures. The EU rules are baseline standards. If a Member State has intelligence information about a particular threat then more stringent security measures may be imposed.

4.2.2. Maritime security

Regulation 725/2004 established as part of EC law the 2002 IMO International Ship and Port Security (ISPS) Code. The Regulation provides a basis for harmonised interpretation and implementation, as well as for monitoring special measures intended to protect shipping and port facilities against threats of intentional unlawful acts, so as to enhance maritime security.

In addition to the ISPS Code, the Regulation takes into account amendments to the 1974 International Convention for the Safety of Life at Sea (the SOLAS Convention). The Regulation is limited in scope to security measures on board vessels and at the immediate ship/port interface. Directive 2005/65/EC is complementary to Regulation 725/2004 as it extends the port security system to all port areas, and applies to all ports in which one or more port facilities governed by the Regulation are situated. The Regulation sets out modalities for the EU port inspection regime, operated by the Commission in cooperation with Member States.

Commission inspections cover national quality control systems and maritime security measures, procedures and structures, at each level of each Member State and of individual port facilities and relevant companies, and the implementation of Directive 2005/65.

The legislation also requires that both ships and port facilities have plans for three levels of security.

Piracy is a major problem for international shipping, and has significant consequences for the world merchant fleet, a large proportion of which is EU Member State flagged or owned.

The resurgence of acts of piracy led the Commission to address the situation and adopted in 2010 Commission Recommendation on measures for self-protection and prevention of piracy

and armed robbery against ships (Best Management Practice, "BMP". The sound implementation of BMP on EU Member States-flagged ships will be checked in the framework of Commission inspections.

For the maritime sector the volume of cargo means that, on the one hand, 100% security controls are not feasible whilst, on the other hand, the possibility of detection of items through random security controls is small. To this end a risk-based approach to security has been developed.

In the area of international trade in goods, customs authorities in the EU apply a risk-based approach to security threats, both on the flow of goods entering the customs territory of the EU as well as the flow of goods exiting this customs territory. The Community Risk Management Framework, the Community Risk Management System and the EU Authorised Economic Operator (AEO) Programme are constituent parts of this approach. EU customs authorities receive advanced cargo information for risk analysis purposes on all cargo coming from- or going to 3rd countries. Under the AEO programme, certified economic operators who voluntarily invest in improving the security of their supply chains to- and from 3rd countries are entitled to trade facilitation benefits.

As a further example of a risk-based approach the Commission has already undertaken a project entitled “ConTraffic” to automatically gather and analyse data on global maritime container movements to enable the identification of consignments that are potentially suspicious to customs. It has shown to be a viable way to target high-risk consignments and proceed with physical checks only where needed.

4.2.3. Aviation security

The original framework Regulation 2320/2002 was simplified through the adoption of the new framework Regulation 300/2008, which has been fully applicable since all implementing legislation was passed in April 2010. The concept of 'one-stop security' is applied within the EU. This means that any passengers (or baggage) arriving on a flight from within the EU does not need to be re-screened when transferring flights at an EU airport (since they are deemed to have been screened to the requisite standard at the first airport). Regulation 272/2009 extends the ‘one-stop security’ concept by allowing the EU to recognise the equivalency of measures taken by a Third Country and treat, for security purposes, any flight from that country to the EU as a domestic originating flight.

The Commission has started a process of consultation to examine proposals to make security controls more effective in more efficient ways. Together with Member States and stakeholders, it is looking into the use of technologies and into methods for risk-based, differentiated and unpredictable controls. The role and responsibility of the operators is also being examined. This approach should be pursued.

Specific risk-based security by aviation security agencies is already being applied for air cargo. A system of supply chain security allows faster treatment of cargo from trusted partners. The development of the AEO programme is one example of how to proceed: a system created to secure and facilitate the handling of cargo by customs also offers benefits as regards targeting security controls in both the aviation and maritime sectors.

Since April 2011 the “One Stop Security” arrangement has in principle been extended to passengers originating from US airports with the potential to create an even wider area of

passenger facilitation and security. Eliminating duplication within the EU and for flights from 3rd Countries with equivalent security standards is essential to stop the progress in security-related costs while allowing Member States together with airlines and airports to better focus security measures to achieve further reductions in risk to civil aviation.

Currently EU rules for aviation security apply to outbound flights from the EU – the principle of 'Host State responsibility', as well as to all EU carriers. However, it may be appropriate to review this approach and consider whether it is desirable to also require as mandatory certain levels of security for all (or some) inbound flights into the EU. In any event, the EU should pursue the achievement of the necessary standards of security through robust rules adopted in the binding framework of ICAO and implemented on the basis of a high performing universal audit programme.

5. CONCLUSIONS

Traditionally, policy in the field of transport security has been driven by incidents.

Yet inaction has a high price. Reactive measures taken after a major security incident are likely to be much more costly and/or intrusive than planned actions, whilst the absence of contingency planning or training to deal with security incidents exacerbates the effects. And policy development should not need as its impetus the deaths of citizens or major acts of criminality.

There are considerable merits in continuing the work already commenced in the aviation and maritime sectors in developing specific measures on transport security at the EU level. The benefits could include:

- A higher overall level of security for citizens in the EU
- lower levels of theft and other crimes – with consequential cost savings
- simplification for transport operators by having common security requirements – with consequential cost savings
- simplification for security providers – both equipment and personnel – by having common performance requirements, and
- having a stronger voice in international fora.

Nonetheless transport security policy is a sensitive topic, and full account must be taken of the implications it can have for public authorities as well as for the fundamental rights of the individual. The respect of the subsidiarity principle is particularly important.

The newly-formed land transport security advisory group will be invited to examine all the potential areas for development highlighted in Chapter 3. Their views, and that of stakeholders, on these topics (and others relating to transport security) will then be taken into consideration by the Commission when considering whether to bring forward legislative proposals in the field of land transport security. Where appropriate the views of the land transport security advisory group would be shared with the committees responsible for maritime and aviation security.

ANNEX I

CURRENT EU TRANSPORT SECURITY LEGISLATION

Transport security policy is a matter of shared competence between the EU and its Member States, based on Articles 91 and 222 TFEU. In the division of responsibility between Member States and the EU, action should take place at the level at which it can be most effective, whether local, regional, national or EU. In practice, the situation differs significantly between the different transport modes, according to their respective characteristics.

The following is a list of EU acts that have been adopted whose primary aim is to address transport security.

Aviation Security

Regulation (EC) No 550/2004 of the European Parliament and of the Council of 10 March 2004 on the provision of air navigation services in the single European sky

Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services

Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002.

Commission Regulation (EC) no 272/2009 of 2 April 2009 supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) no 300/2008 of the European Parliament and of the Council, as amended.

Commission Regulation (EU) No 1254/2009 of 18 December 2009 setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures.

Commission Regulation (EU) No 18/2010 of 8 January 2010 amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmes in the field of civil aviation security is concerned.

Commission Regulation (EU) No 72/2010 of 26 January 2010 laying down procedures for conducting Commission inspections in the field of aviation security.

Commission Regulation (EU) No 185/2010 of 4 March 2010 laying down detailed measures for the implementation of the common basic standards on aviation security, as amended. (The most recent amendments include cargo security rules for inbound cargo and mail to the EU and rules governing the use of security scanners at EU airports).

Commission Decision C(2010)774 of 13 April 2010 laying down detailed measures for the implementation of the common basic standards on aviation security containing information as referred to in Point (a) of Article 18 of Regulation (EC) No 300/2008, as amended.

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

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

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

Commission Recommendation (EU) No 2010/159 of 11 March 2010 on measures for self-protection and the prevention of piracy and armed robbery against ships

Land Transport Security

No specific legislative requirements exist at the EU level that primarily addresses security. However, Regulation (EC) no 1371/2007 of the European Parliament and of the Council of 23 October 2007 on rail passengers' rights and obligations does make reference to security.

Security of Inland Waterways Transport

No specific legislative requirements exist at the EU level

ANNEX II

OVERVIEW OF CURRENT EU-FUNDED RESEARCH INTO TRANSPORT SECURITY

An overview of activities funded under the 7th Framework Programme for Research that have transport security relevance:

Air transport-related

Project Acronym	Project Start Date	Project End Date	EC Financial Contribution	Project Total Cost
COPRA	01/09/2011	28/02/2013	986,382.00 €	1,303,301.80 €
CRISIS	01/05/2010	30/04/2013	3,495,612.00 €	4,593,444.66 €
ISTIMES	01/07/2009	30/06/2012	3,113,460.00 €	4,367,950.73 €
SIAM	01/02/2011	31/01/2014	2,168,640.00 €	2,777,307.68 €
SUBITO	01/01/2009	31/10/2011	2,581,052.60 €	3,897,587.20 €
TASS	01/04/2010	31/03/2014	8,986,696.15 €	14,544,276.60 €
XP-DITE			9,992,635.00 €	14,400,681.00 €
Total			31,324,477.75 €	45,884,549.67 €

Land & maritime transport-related

Project Acronym	Project Start Date	Project End Date	EC Financial Contribution	Project Total Cost
CASSANDRA	01/06/2011	31/05/2014	9,958,749.10 €	4,813,514.60 €
CONTAIN	01/10/2011	31/03/2015	10,044,904.00 €	15,600,818.55 €
DEMASST	12/01/2009	11/05/2010	956,558.96 €	1,840,549.50 €
IMCOSEC	01/04/2010	31/03/2011	930,718.00 €	1,142,591.00 €
ISTIMES	01/07/2009	30/06/2012	3,113,460.00 €	4,367,950.73 €
LOGSEC	01/04/2010	31/03/2011	753,372.32 €	800,047.14 €
PROTECTRAIL	01/09/2010	28/02/2014	13,115,064.00 €	21,775,289.80 €
SECTRONIC	01/02/2008	31/01/2012	4,496,106.41 €	6,948,326.42 €
SECUR-ED	01/04/2011	30/09/2014	25,468,072.00 €	40,187,354.70 €

SERON	01/11/2009	31/10/2012	2,246,110.00 €	2,942,113.00 €
STAR-TRANS	01/11/2009	30/04/2012	2,105,588.94 €	3,195,188.88 €
SUPPORT	01/07/2010	30/06/2014	9,920,607.00 €	14,629,279.69 €
Total			83,109,310.73 €	128,243,024.01 €

COPRA (= Comprehensive European Approach to the Protection of Civil Aviation)

Security has become a major factor in civil/commercial aviation. In recent decades, the number of threats to aviation security has grown significantly, especially after 9/11. This has led to ever more security regulations as the threats evolve. Security procedures have become exceedingly complex and invasive to passenger privacy; the number of security measures as well as personnel and therefore costs are growing steadily. At the same time passenger and cargo traffic are expected to double in the next 15 years. Already today, security is one of the main reasons for delayed take-off. It is clear that the current complex security system cannot be adapted to such a growth without a large rise in costs. It has already and will increasingly become a major market restraint. Therefore, the proposed project COPRA aims to answer two questions:

- How does the threat situation in civil aviation evolve in the future, taking into account both existing and new technologies and their continuing development and proliferation?
- Which opportunities arise from the development and proliferation of new technologies and security procedures to overcome the current complex and expensive security situation and to enable sustainable growth for the future?

COPRA's main objective is to answer both questions in a way that will constitute the optimal balance between security, privacy, public acceptability, mobility and costs, while providing ideas on how to increase flexibility and resilience of the whole aviation system against threats. To that aim COPRA brings together a well-balanced consortium of research organisations, industry and major air transport providers with a wide range of European stakeholders. End-users, technology providers, policy makers and think tanks will be involved in COPRA through the formation of expert groups. The involvement of these expert groups is essential to the success of COPRA's objectives.

Total project cost: €1 291 405.20	*EU Contribution €983 949.90*

CRISIS (= Critical incident management training system using an interactive simulation environment)

CRISIS is a 36 month project to research and develop an advanced critical incident management, interactive simulation environment for training security and emergency personnel in airport operational security. The prototype to be delivered will be distributed,

scalable, collaborative interactive simulation environment that will enable training of crisis managers and their staff at airports, at different levels of the organization.

The prototype system will avoid the simulation paradigm where the trainee selects one of a number of pre-set drill oriented choices at a predictable decision point. Instead, using an interactive games paradigm, the trainees will be able to practice situation and cue assessment, problem diagnosis, decision making and action coordination, in real-time in response to a critical incident. Currently, one key problem hindering the maintenance of a high level of preparedness in operational security organizations at airports is the long 2-year wait between major exercises. In CRISIS, we will enable organizations and individuals to train-on-demand, and as frequently as needed due to the innovations, such as end-user re-configurability of training scenarios. This will allow staff to train individually playing; against the system, as a team within an organization, across organizations, and at different levels of the command hierarchy. CRISIS will adopt a 3-stage development strategy, integrating, testing and iteratively evaluating user performance at each step of the way.

The CRISIS consortium brings together a powerful combination of expertise in User modelling and requirements engineering, Games and simulation, Software engineering, distributed systems, and security, Decision sciences and technology, User performance evaluation, to deliver capability for training and improving operational security preparedness at airports.

Total project cost: €4 591 760.99	*EU Contribution €3 495 611.99*

ISTIMES (= Integrated system for transport infrastructure surveillance and monitoring by electromagnetic sensing)

The aim of the proposal is to design, assess and promote an ICT-based system, exploiting distributed and local sensors, for non-destructive electromagnetic monitoring in order to achieve the critical transport infrastructures more reliable and safe. This has the overall aim to developing high situation awareness in order to provide real time and detailed information and images of the infrastructure status to improve decision support for emergency and disasters stakeholders.

The system exploits an open network architecture that can accommodate a wide range of sensors, static and mobile, and can be easily scaled up to allow the integration of additional sensors and interfacing with other networks. It relies on heterogeneous state-of-the-art electromagnetic sensors, enabling a self-organizing, self-healing, ad-hoc networking of terrestrial sensors, supported by specific satellite measurements. The integration of electromagnetic technologies with new ICT information and telestaff working papers systems enables remotely controlled monitoring and surveillance and real time data imaging of the critical transport infrastructures.

The proposal will be based on several independent non-invasive imaging technologies based on electromagnetic sensing. Sensor cross validation, synergy and new data fusion and correlation schemes will permit a multi-method, multi-resolution and multi-scale electromagnetic detection and monitoring of surface and subsurface changes of the infrastructure .

The architecture will be based on web sensors and service-oriented-technologies that comply with specific end-user requirements, including economical convenience, exportability, efficiency and reliability. The system will adopt open architectures and will make efforts to achieve full interoperability. The system will be tested on very challenging test beds such as: a highway-bridge and a railway tunnel.

Total project cost: €4 342 283	*EU Contribution €3 113 460*

SIAM (= Security impact assessment measures)

The SIAM decision support system will ease the complexity associated with the assessment of security measures and technologies. Where today decision makers have to oversee a wide range of relevant aspects from many different scientific fields and national as well as cultural interests SIAM will pass the needed information in a structured manner to the decision maker. It ties together those strands and reduces their complexity by providing a number of guidelines and a database for easy decision making.

One major impact is that SIAM will continue to close the gap between the perspective of preventing or disturbing criminal threats and the perspective of potential freedom infringements associated with many security measures and technologies. Furthermore by conducting four case studies (German, UK, Israeli airports plus London underground) featuring a significant level of security measures and technologies SIAM integrates the practical experience with such technologies into the decision support system. As it will be flanked by extensive literature reviewing and the gathering of the wisdom of Europes leading security and civil rights experts the practitioner perspective will be extended by state of the art knowledge. Beyond that SIAM is building an actor network to initialise the relationships needed for sustained cooperation and future fruitful interaction in the field of security. Participative elements such as stakeholder conferences open up the security field to a wider public and include more actors in the process.

Total project cost: €2 777 309.02	*EU Contribution €2 168 640*

STAR-TRANS (= Strategic risk assessment and contingency planning in interconnected transport networks)

STAR-TRANS aspires to develop a holistic risk assessment methodology for Critical Infrastructure and apply it to a wide panel of international transportation infrastructures to analyse and assess common issues for risks, threats and vulnerabilities and identify possible interdependencies assessing the impact of failures on interconnected transportation infrastructures. The successful project outcome will offer important aids for decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences (cost, timing, resources, etc.) of proposed actions.

The improvement of the response and management capabilities regarding assessment of incidences / failures in critical transport infrastructures will be achieved through the identification and closure of relevant knowledge gaps and through the development, validation and usage of computational modelling tools. STAR-TRANS aims at developing a

modelling formalism in which specification of the structure and associated assets of European transportation networks as well as the specification of the dependency types between the assets of interconnected and interdependent transportation networks is facilitated.

This modeling formalism will consider a transportation network of networks as consisting of nodes and links. In so doing, tools from network and graph theory and the systems area will be employed. A specialized software system will be developed that will support the end users, and network operators needs. The software tool will provide the technology to link together any relevant assets of interconnected and interdependent transport networks, such that risk managers, policy makers and others can, subsequently, be provided with the impact that a risk incident on an asset of a specific transportation network may have on the assets of other interconnected and interdependent transport networks.

Total project cost: €3 195 188.88	*EU Contribution €2 105 588.94*

SUBITO (= surveillance of unattended baggage and the identification and tracking of the owner)

The SUBITO programme has been developed to address Theme 10 - Security, specifically Topic SEC-2007-2.3-01 Detection of Unattended Goods and of Owner. It will focus on the automated real time detection of abandoned luggage or goods and the fast identification of the individual who left them and their subsequent path. The key design drivers will include an assessment of the situations faced in such scenarios, and the existing security equipment available that will support the automatic operation of such functionality. Automated processing will be developed to address the requirements, ultimately integrated to form part of a customer demonstration. To achieve the above, the SUBITO programme brings together; • Key technical expertise in state-of-the-art processing and detection and tracking algorithms • Industry leaders sensor data processing, sensor design and sensor systems integration • A consortium of End Users providing real knowledge of the threat and practical experience of the various operating environments.

Total project cost: €3 895 730	*EU Contribution €2 581 055*

TASS (= Total airport security system)

TASS is a multi-segment, multi-level intelligence and surveillance system, aimed at creating an entire airport security monitoring solution providing real-time accurate situational awareness to airport authorities.

The TASS concept is based on integrating different types of selected real time sensors & sub-systems for data collection in a variety of modes, including fixed and mobile, all suitable for operation under any environmental conditions. TASS divides the airport security into six security control segments (environmental, cargo, people, airplanes, vehicle-fleet & facilities) each of them being monitored by various technologies that are fused together, creating a multisource labyrinth fusion logic enabling situational and security awareness of the airport anytime and anywhere. These fused control segments will be accessed through the TASS WEB-based portal by running a suite of applications making the airport security control

centralized to all airport authorities. Information will be shared and synchronized between all of them in order to generate a comprehensive, real time, security overview for the airport C2, providing all the necessary features to assure a total no breach security environment. The integration will include the use of in-place technologies that will result in a cost-effective solution.

The TASS consortium consists of 3 main end users representing 16 airports and 16 technological partners, which bring together European SME s, industrial and academic partners, ranging from sensor design and electronic staff working papers through to civil airport protection. The technologies will be tested at 3 airports including the hub airport Heathrow, an Israeli domestic airport and Athens airport, in order to cover a wide range of needs at different levels of airport protection. The main test at Heathrow airport will involve scenarios including 2 connected to the upcoming 2012 Olympic Games in London ultimately resulting in a high & smooth passengers flow.

Total project cost: €15 544 276.60	*EU Contribution €8 986 696.15*

XP-DITE

The aim of the XP-DITE project is to develop, demonstrate and validate a comprehensive, passenger centred approach to the design and evaluation of integrated security checkpoints (CPs) at airports. The approach encompasses a variety of different types of requirements, relating to security, airport operations and societal aspects. An ethical framework will be defined which enables designers and operators to proactively introduce ethical factors in the checkpoint. The project team will identify and develop requirements and criteria at integrated system level. A key element of the project is the development of a design tool that allows the design of innovative new CPs and modification of existing CPs to meet changing threats. A major challenge comprises a validated set of protocols and tools for evaluating and monitoring the performance of the CP at the overall system rather than component level. The approach will be demonstrated in two integrated demonstration CPs at two airports. The activities are focussed towards aviation security but may be extended to mass transportation and other applications.

Total project cost: €9 992 635	*EU Contribution €14 400 681*

CASSANDRA (= Common assessment and analysis of risk in global supply chains)

CASSANDRA will:

•Facilitate the adoption of a risk-based approach in the supply chain, on the basis of integral monitoring data on cargo flows and container integrity,

•Build interfaces between existing visibility solutions, and visualisation tools, in an open architecture,

•Demonstrate the integration of data and risk assessment in supply chains in three major trading routes to and from Europe

•Evaluate the quality of the integral data with business and government.

•Facilitate a dialogue between business and government to gain consensus on the criteria for data sharing between business and government.

The project participants cover all relevant stakeholders, including some global players. This expertise will guarantee the successful adoption of the CASSANDRA solutions. The value drivers in CASSANDRA will include:

•Logistics efficiency benefits

•Security benefits for business as a result of the risk self assessment

•Security benefits for government as a result of the high quality and complete data for government risk analysis.

CASSANDRA will contribute to the priorities of DG TAXUD, will facilitate security and crime-fighting priorities of DG Enterprise and DG Justice, Liberty and Security, and enables priorities in the DG TREN Freight Logistics Action Plan, and builds on previous work in standardisation bodies.

The development of integral supply chain data that is the basis for risk-based supply chain management and the input for government supervision tasks, as envisaged in CASSANDRA, will set a new standard for global door-to-door goods flows to and from Europe: efficient & secure.

Total project cost: €14 813 514	*EU Contribution €9 958 749*

CONTAIN (= Container Security Advanced Information Networking)

CONTAIN will specify and demonstrate a European Shipping Containers Surveillance system which will encompass regulatory, policy and standardisation recommendations, new business models and advanced container security management capabilities. CONTAIN will:

1. Support transport security stakeholders in managing container security threats as part of an integrated approach to the management of transportation networks;

2. Provide a coherent set of technology options for screening and scanning plus container-integrated sensor, staff working paper and security technologies to monitor container movements and security related parameters in real time;

3. Enable ports to establish upgraded port container security processes and provide information feeds to port, community systems and national and European security databases;

4. Provide information gathering, validation, fusion and situation awareness services to establish dependable near real time ‘corridor container traffic maps’ and their integration into a EU Container Traffic Map for use by organisations and systems established to promote and implement an integrated EU surveillance policy;

5. Assist policy makers at national and EU level to benchmark container security performance and formulate improvement policies.

The project will:

1. Work actively on standardisation activities as a key enabler of cost effective solutions for shipping containers security with the ultimate goal to progress towards a single international shipping containers security standard.

2. Build on outputs from ongoing FP7 projects on security, freight transport and ICT and efforts to establish integration facilities between security agencies such as FRONTEX and EMSA and EU Platforms such as e-Customs and SafeSeaNet.

3. Demonstrate Secure Multimodal Corridor Design and Chain Monitoring & Control across international and European corridors at Interporto Bologna, Rotterdam /Amsterdam and Valencia.

Total project cost: €10 044 904	*EU Contribution €15 600 818.55*

DEMASST (= demo for mass transportation security: roadmapping study)

To develop adequate and well accepted security for mass transportation in Europe and the citizens affected by it, is a formidable task. The malicious threats, particularly those posed by terrorists, require a comprehensive approach: if security improvements are patchy, perpetrators are likely to find the loopholes left. With their open access points and interconnections, surface mass transportation systems are highly vulnerable, while it is technically and economically, impossible for the multiple operators to employ security measures similar to those used at airports.

With eight technology and security analysis RTOs, four transportation industries and system integrators and two transportation consultancies many with previous experience of working together in projects like SeNTRE and STACCATO DEMASST is exceptionally well prepared to take on the dual challenges of analysis and networking necessary to define and achieve commitment for the strategic roadmap for the Phase 2 Demonstration project.

DEMASST will develop a highly structured approach to the demonstration programme built on identifying the main security gaps and the most promising integrated solutions, utilising sufficiently mature technologies, for filling them.

In the type of Concept Development & Experimentation approach proposed the experiments must be designed and analysed so as to be maximally informative. Given the vast variation in mass transportation systems an effective demonstration programme must also identify synergies between demo tasks and use less costly methods than full scale demonstration whenever that helps a broader awareness. DEMASST proposes to build the methodological infrastructure for this.

But an optimal demo project design does not stop with finding scientific answers: the issue of turning demonstration into innovation is top on DEMASST's agenda. And this approach will have utility also beyond transportation.

Total project cost: €1 840 955	*EU Contribution €956 650*

IMCOSEC (= Integrated approach to improve the supply chain for container transport and integrated security simultaneously)

There are two contradicting trends in global transport (which are valid also for the segment of containers and other ILUs) that have to be aligned in the most efficient way assuring free trade and assuring transport security. Thus, it is essential that private end-users and public end-users work together on the improvement of supply chain security to ensure public safety and security as well as the efficient flow of goods.

IMCOSEC Integrated approach to improve the supply chain for container transport and integrated security simultaneously is a risk-based approach to identify and characterize the security gaps, preventive measures will be discussed and a guiding concept for demonstrations in phase II will be defined, with the aim to make the supply chains in their totality more secure without major negative impacts on their performance and without creating unjustifiable additional cost. An optimal solution will be creating win-win situations between industry and administration and will not imply as much security as possible, but as much security as needed and acceptable. Acceptance is one of the most important issues on the sustainability of the strategic roadmap to be developed. Therefore the consortium results will be discussed reflected and validated by a series of international workshops with stakeholders and the projects Advisory Board involving additional stakeholders from private end-users and public end-users. This will mainly contribute to European wide awareness and shall ensure that the target processes defined and technologies assembled will be applicable in the real world business.

The partners are well experienced in the sector either from its logistics or from its security angle. The Consortium includes international associations, security consultants and research institutions, experts from the maritime and inland/combined transport, as well as an operator of a container security platform.

Total project cost: €1 142 591	*EU Contribution €930 718*

ISTIMES (= Integrated system for transport infrastructure surveillance and monitoring by electromagnetic sensing)

The aim of the proposal is to design, assess and promote an ICT-based system, exploiting distributed and local sensors, for non-destructive electromagnetic monitoring in order to achieve the critical transport infrastructures more reliable and safe. This has the overall aim to developing high situation awareness in order to provide real time and detailed information and images of the infrastructure status to improve decision support for emergency and disasters stakeholders.

The system exploits an open network architecture that can accommodate a wide range of sensors, static and mobile, and can be easily scaled up to allow the integration of additional sensors and interfacing with other networks. It relies on heterogeneous state-of-the-art electromagnetic sensors, enabling a self-organizing, self-healing, ad-hoc networking of

terrestrial sensors, supported by specific satellite measurements. The integration of electromagnetic technologies with new ICT information and telestaff working papers systems enables remotely controlled monitoring and surveillance and real time data imaging of the critical transport infrastructures.

The proposal will be based on several independent non-invasive imaging technologies based on electromagnetic sensing. Sensor cross validation, synergy and new data fusion and correlation schemes will permit a multi-method, multi-resolution and multi-scale electromagnetic detection and monitoring of surface and subsurface changes of the infrastructure .

The architecture will be based on web sensors and service-oriented-technologies that comply with specific end-user requirements, including economical convenience, exportability, efficiency and reliability. The system will adopt open architectures and will make efforts to achieve full interoperability. The system will be tested on very challenging test beds such as: a highway-bridge and a railway tunnel.

Total project cost: €4 342 283	*EU Contribution €3 113 460*

LOGSEC (= Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security)

The goal of the LOGSEC project is to develop a strategic roadmap for a large scale demonstration project in European logistics and supply chain security, characterized by adequate security for the benefit of business and governments, on low time-delay and other cost implications.

A broad set of security policies, regulations, standards, technologies, procedural aspects, services, IPR-issues and links to other related projects will be assessed and evaluated during the project in close collaboration between the beneficiaries and business and governmental security end-users. Key technologies and procedural aspects covered by the project include: Container and goods/inventory, authentication, traceability, inspection and monitoring technologies; Risk assessment systems and models; Information transfer systems; Intermodal transport security; Modernization of customs procedures; Protection of supply chain infrastructure. As the main output, LOGSEC will identify the most relevant/promising research areas and research gaps, which should be addressed in the follow-up demonstration project. The LOGSEC project team consists of organizations with in depth experience in European and global supply chain security research and technology analysis and end-user partners representing a broad set of European shippers and logistics operators and customs administrations. The methodology consists of literature and project reviews; expert interviews; user surveys; user workshops.

Background theory will be drawn from supply chain and logistics management; security management; and crime prevention theories. Lessons learnt in other regions, including North and South America and Asia will be exploited during the course of the project. Links to key parallel projects will be established, including demonstrations in Integrated border management (Security) and China-EU secure trade lane (Transportation); related projects with the World Customs Organization and the World Bank amongst others.

Total project cost: €800 047	*EU Contribution €753 373*

PROTECTRAIL: the railway industry partnership for integrated security of rail transport

Facing the problem of enhancing the railway security with a systematic top-down approach (i.e. to search for an all-inclusive solution valid for all the conceivable threat scenarios) is judged by PROTECTRAIL members too ambitious even if it could generate potential economies of scale and effort rationalisation. The proposed PROTECTRAIL approach is therefore to split the problem of making the railway more secure into smaller asset-specific security problems (missions) for which it is easier to reach satisfactory solutions applicable and usable in different threat scenarios. Each sub-mission could be therefore better oriented to particularly significant areas of interest, resulting from risk analysis or from rail operator priorities. In a clear view of scope and performance goals, for each sub mission it will be easier to define research and develop solutions in terms of architectures, technology deployment, as well as the necessary procedures, organizations to manage the specific issue. The PROTECTRAIL challenge is therefore to make interoperable the single asset-specific solutions and to conceive and design a modular architectural framework where each asset-specific solution can be "plugged", that is the basis to assure a streamlined process of federation, integration and interoperability of respective solutions. The PROTECTRAIL project will address the following security sub-missions: protection of signal and power distribution systems against any terrorism act, track clearance, clearance of trains before and after daily use, staff clearance, luggage clearance control, passenger clearance control, freight clearance control, tracking and monitoring of rolling stock carrying dangerous goods, protection of staff working paper and information systems, stations, buildings and infrastructure protection.

Total project cost: €21 775 289.80	*EU Contribution €13 115 064*

SECTRONIC (= security system for maritime infrastructure, ports and coastal zones)

The SECTRONIC initiative addresses observation and protection of critical maritime infrastructures; Passenger and goods transport, Energy supply, and Port infrastructures. All accessible means of observation (offshore, onshore, air, space) of those infrastructures are exchanged via an onshore control centre. The end-users themselves or permitted third-parties can access a composite of infrastructure observations in real-time. The end-users will be able to protect the infrastructure by non-lethal means in the scenario of a security concerned situation.

The proposed system is a 24h small area surveillance system that is designed to be used on any ship, platform, container/oil/gas terminal or harbour. The initiative is an end-users driven R&D activity. The end-users represent the major market player in each of the three infrastructures: Passenger transport, Energy production, Energy transport, Commercial ports and combined military/commercial ports.

Total project cost: €7 080 433	*Total project cost: €7 080 433*

SECUR-ED (= secured urban transportation – European demonstration)

SECUR-ED Project federates, with a delegated management and in a balanced manner, major operators and top industrial integrators to enhance the security of urban public transportation in medium and large cities, through live demonstrations. Based on the best practices, in a very diverse societal and legacy environment, SECUR-ED will aggregate a consistent and interoperable mix of technologies and processes, covering all aspects, from risk assessment to complete training packages. SECUR-ED rationale is to create a global European improvement in mass transportation security through the development of packaged modular solutions validated through the demonstrations, and made available to the full community of operators. The process will follow a strict methodology to translate the threats into a system-of-systems architecture and interoperability language, as well as in assessing the results obtained. The different modules (made up of best practices, procedures, training and hardware and software) are selected and packaged with standard interfaces, ready to be integrated. Similarly standard interfaces are developed to host such modules in the legacy transport infrastructures. With a good coverage of the diverse priorities, integration is performed in the networks of four cities (Madrid, Paris, Milan and Berlin), validating the security enhancement packages, becoming a showcase of this unique European initiative. This is only the start point: a set of medium size cities will then use the above tool-kit to assess their risks and design their own solutions through adapted demonstrations, staff training to best practices, technical upgrades … To amplify the process, with the support of the professional associations, the Advisory Groups (Operators, First responders and Authorities) will conduct an active dissemination of the project results to the community of urban transport stakeholders in Europe

Total project cost: €40 187 354.70	*EU Contribution €25 468 072*

SERON (= Security of road transport networks)

The European road network, particularly TERN highways and TENT projects, is of major importance for the European economy and the mobility of the European citizens. A major task of highway owners and operators is to ensure a high availability of all important links. Even smaller disruptions due to traffic restrictions or failure of road network elements lead to severe traffic interferences resulting in high economic follow-up costs and negative environmental impacts.

Such infrastructures also constitute attractive terrorist targets due to their accessibility and great potential impact on human lives and economic activity. Attacks may cause considerable damage, including structural damage or demolition, substantial human casualties, socio-economic losses (unemployment, relocation of firms, reconstruction costs) and socio-political damage (public uncertainty, confidence loss) and even environmental consequences, each being accompanied by the related costs. Particularly bridges and tunnels, key elements of the road network, are highly vulnerable to terrorist attacks due to their bottleneck function. The SeRoN project will undertake a holistic approach both at individual infrastructure object and at road network level. Its main objectives are to investigate the impacts of possible terrorist attacks on the transport network, in particular the resulting regional and supra-regional impacts on transport links and their economic impacts.

SeRoN will focus on the development of a methodology which is to help owners and operators to analyse critical road transport networks or parts hereof with regard to possible

terrorist attacks. It will evaluate planned protection measures for critical road transport infrastructures concerning their impact on security and cost-effectiveness. Finally SeRoN will give adequate recommendations concerning possible current and future threat situations and the related most effective security measures.

Total project cost: €2 942 113	*EU Contribution €2 246 110*

STAR-TRANS (= strategic risk assessment and contingency planning in interconnected transport networks)

STAR-TRANS aspires to develop a holistic risk assessment methodology for Critical Infrastructure and apply it to a wide panel of international transportation infrastructures to analyse and assess common issues for risks, threats and vulnerabilities and identify possible interdependencies assessing the impact of failures on interconnected transportation infrastructures. The successful project outcome will offer important aids for decision-makers to determine priorities among multiple contingency alternatives by evaluating the consequences (cost, timing, resources, etc.) of proposed actions.

The improvement of the response and management capabilities regarding assessment of incidences / failures in critical transport infrastructures will be achieved through the identification and closure of relevant knowledge gaps and through the development, validation and usage of computational modelling tools. STAR-TRANS aims at developing a modelling formalism in which specification of the structure and associated assets of European transportation networks as well as the specification of the dependency types between the assets of interconnected and interdependent transportation networks is facilitated.

This modelling formalism will consider a transportation network of networks as consisting of nodes and links. In so doing, tools from network and graph theory and the systems area will be employed. A specialized software system will be developed that will support the end users, and network operators needs. The software tool will provide the technology to link together any relevant assets of interconnected and interdependent transport networks, such that risk managers, policy makers and others can, subsequently, be provided with the impact that a risk incident on an asset of a specific transportation network may have on the assets of other interconnected and interdependent transport networks.

Total project cost: €3 195 188.88	*EU Contribution €2 105 588.94*

SUPPORT (= Security upgrade for ports)

Port security remains of paramount importance for Europe both due to potential threats on passenger life and the potential for crippling economic damage arising from intentional unlawful attacks on port facilities. Challenges arise due to the complexity of operational modalities of sea and hinterland traffic and the lack of efficient organisational and technological interfaces linking ports to border control authorities, the police and other intervention forces, and transport-logistics operators. Considerable progress with port security has been achieved in recent years primarily associated with adoption of the International Ship and Port Facility Security (ISPS) Code. SUPPORT is aimed at building on these

achievements by engaging representative stakeholders to guide the development of next generation solutions for upgraded preventive and remedial security capabilities in European ports. The overall benefit will be the secure and efficient operation of European ports enabling uninterrupted flows of cargo and passengers while suppressing illegal immigration and trafficking of drugs, weapons and illicit substances all in line with the efforts of FRONTEX and EU member states. SUPPORT will deliver public formal specifications and open standards based tools that will aid security upgrade in EU ports and will be complementary to and usable by other EU projects and initiatives in this area. Emphasis will be given to bring together advances from research on security with results from the main EU projects in maritime and intermodal transport, specifically those concerned with security and interoperability issues. Thus, SUPPORT will address 'total' port security upgrade solutions encompassing legal, organisational, technology and human factors perspectives. These solutions should provide substantial improvements in the performance, reliability, speed and cost of European port security which will be demonstrated during the course of the project.

Total project cost: €14 629 279.69	*EU Contribution €9 920 607*

1.1. Transport security issues that could apply to more than one mode of transport

1. On preventative measures consideration should be given to:

 greater cross-border cooperation on intelligence sharing of potential threats;

 developing security measures that are more targeted, so as to be more resource-efficient and contain greater unpredictability.

 setting security outcomes, rather than prescriptive security requirements

2. On contingency planning to deal with the immediate effects of a security incident consideration should be given to:

 obliging all transport operators and providers to have contingency plans on how to react immediately to a security incident;

 requiring staff to have basic levels of security awareness training (for prevention of acts), as well as training to deal with the aftermath of security incidents;

 ensuring that transport operators undertake security training exercises;

3. On resilience and recovery planning consideration should be given to:

 making recovery planning mandatory in order to avoid that a security incident paralyses transport operations for a long period;

 greater coordination and development of EU critical infrastructure policy, noting that infrastructure policy needs to take fully into account both the needs of transport as well as the key role transport plays in alleviating problems;

 having better networks to ensure the swift sharing of information throughout the EU following major security incidents that may have an effect on transport;

 Ensuring that transport is resilient to cyber-attacks and, if an attack does occur, that backup systems are in place that will allow swift recovery of at least core activities, especially relating to the safety of transport. If appropriate – and following the forthcoming Commission Communication on cybercrime - targeted actions for the transport sector should be considered.

4. With regard to the well-functioning of the Single Market consideration should be given to:

 seeking further harmonisation at EU level of technical standards and conformity assessment for security equipment. A legal framework could be created to allow EU testing and approval of equipment by a single EU body;

 setting objective, measurable standards that could be used to measure people's abilities to perform security tasks, which could be used as a tool for recruitment policy for security staff;

1.2. Specific land transport security issues

5. With regard to land transport security consideration should also be given to:

 examining the need for EU-wide security standards to be set for the high-speed rail network;

 developing rules for end-to-end supply chain security that are proportionate and add value;

 greater use of logistics technologies to enhance security.

1.3. Develop further maritime security

6. With regard to maritime security, in addition to the continuous on-going work undertaken by means of the existing EU Committee for Maritime Security, consideration should also be given to:

 explicitly defining the Commission's mandate to develop EU policy on piracy, as well as specific EU actions to address piracy in the maritime sector;

 Developing more detailed EU security requirements for large cruise ships, as well as developing proportionate EU rules to enhance the security of ferries, in particular RoRo ferries.

1.4. Develop further aviation security

7. With regard to aviation security, in addition to the continuous on-going work undertaken by means of the existing EU Committee for Aviation Security, consideration should also be given to:

 reviewing the system governing the security requirements for inbound flights into the EU and, in particular, whether it would be prudent to lay down minimum security requirements for all or some inbound flights, beyond the current requirements for inbound cargo and mail

 ways of enhancing security by means of a more "risk based", differentiated and unpredictable, approach as opposed to the uniform screening of passengers and goods.

1.5. Funding of transport infrastructure and transport security research

8. With regard to the Commission's funding of transport security research and transport infrastructure the Commission will:

 ensure that the "Horizon 2020" Programme for Research allows for security-related research to be more closely linked to needs and developments in transport security policy. Consideration could be given to requiring that projects must successfully undertake a "policy impact assessment" to determine their relevance to policy needs.

 ensure that security issues are taken into consideration as a condition of EU funding of transport infrastructure.

1.6. External relations in the field of transport security

9. At the international level the Commission will consideration should be given to:

- further developments of bilateral mutual recognition agreements that can eliminate unnecessary duplication of security measures for international transport between countries which have equivalent levels of transport security as the EU;

- increasing the role of the EU in assisting Third Countries in capacity building in the domain of transport security. This could include clear budget lines for funding such actions;

- better ensuring common, coordinated positions of EU Member States on issues of mixed competence in the meetings of international organisations such as ICAO, IMO and WCO.

It is also important that requirements for transport security neither create a 'fortress Europe' nor that the EU rules actually handicap Europe's businesses by being too stringent. The European Commission is, therefore, working on a common EU transport security policy line with international organisations such as ICAO, IMO and WCO . It is important that the EU Member States speak with a common voice when developing policy in these fora. The combined resources of the Member States working together as the EU will always be far more effective at the international level than the individual Member States working in isolation.