

**EUROPEAN COMMISSION**  
**DG TREN**

**SIXTH FRAMEWORK PROGRAMME**  
**THEMATIC PRIORITY 1.6**  
**SUSTAINABLE DEVELOPMENT, GLOBAL CHANGE & ECOSYSTEMS**  
**INTEGRATED PROJECT – CONTRACT N. TREN-06-FO6TRS07.70077-**  
**S07.69821**



# **RETRACK**

**REorganization of Transport networks by advanced RAil freight Concepts**

<b>Deliverable no.</b>	D 7.3
<b>Dissemination level</b>	Public
<b>Work Package</b>	WP 7
<b>Author(s)</b>	Marika Kolbenstvedt and Astrid Amundsen
<b>Co-author(s)</b>	
<b>Status (F: final, D: draft)</b>	D.7.3 FINAL for revision 4.6.2010.
<b>File Name</b>	D7.3-Public-Rail Freight Security Challenges and Strategies in Rail Cargo Security in Europe-Final-v4.6.2010-Kolbenstvedt-04062010.pdf
<b>Project Start Date and Duration</b>	01 May 2007 – 30 April 2011

# Rail freight security practises

## Challenges and strategies in rail cargo security in Europe and for RETRACK

### Contents

<b>1. Background and scope</b> .....	<b>4</b>
<b>1.1 Introduction to RETRACK</b> .....	<b>4</b>
<b>1.2 Security in RETRACK</b> .....	<b>4</b>
1.2.1 The security concept.....	4
1.2.2 Security integrated in several WPs.....	5
1.2.3 WP 7 purpose: Stimulating security consciousness .....	5
1.2.4 Definition of focus and issues to be addressed.....	7
<b>1.3 Contents of the report</b> .....	<b>8</b>
<b>2. Methods</b> .....	<b>9</b>
<b>2.1 Literature review – WP7.1</b> .....	<b>9</b>
2.1.1 Sources and search words .....	9
2.1.2 Limitations by the theme .....	9
<b>2.2 Security survey – WP7.2</b> .....	<b>10</b>
2.2.1 Short questionnaires on eight themes .....	10
2.2.2 Special questionnaires to six types of stakeholder .....	11
2.2.3 Partners responsible for conducting the survey .....	11
2.2.4 Change of strategy .....	12
2.2.5 Low response rate.....	12
<b>3. Problem areas – facts and figures</b> .....	<b>13</b>
<b>3.1. Risk in rail transport</b> .....	<b>13</b>
3.1.1 Risk differences between rail and other transport modes.....	13
3.1.2 Major accidents in public/passenger transport.....	14
3.1.3 Accidents vs. terrorist attacks.....	15
3.1.4 Rail accidents by type of accident .....	16
<b>3.2 Transport of hazardous materials (hazmat)</b> .....	<b>17</b>
3.2.1 Many vulnerable points and large consequences.....	17
3.2.2 Cargo visibility and integrity - technological development.....	18
3.2.3 Identification and Authorisation Measures .....	19
3.2.4 Cost efficiency vs. security.....	19
<b>3.3 Criminal activities and vandalism</b> .....	<b>20</b>
3.3.1 Thefts and smuggling .....	20
3.3.2 Challenges in preventing crime.....	21
<b>3.4 Terrorist threats to security</b> .....	<b>21</b>
3.4.1 Trends in terrorist attacks on rail.....	21
3.4.2 Areas attacked in terrorist actions .....	22
3.4.3 Use of technologies.....	22
3.4.4 Use of measures not originally security-based.....	23
<b>3.5 Balancing security with other concerns</b> .....	<b>24</b>

<b>4. Results from RETRACK Security Survey</b> .....	<b>26</b>
<b>4.1 Security standards and procedures</b> .....	<b>26</b>
<b>4.2 Security assessment</b> .....	<b>27</b>
4.2.1 Threat assessment.....	27
4.2.2 Inspections - awareness.....	27
<b>4.3 Personnel and training</b> .....	<b>27</b>
4.3.1 Dedicated and trained staff.....	27
4.3.2 Security checks of employees.....	28
<b>4.4 Emergency preparedness and response</b> .....	<b>28</b>
4.4.1 Tracking of shipments, dangerous goods .....	28
4.4.2 Communication failures.....	29
<b>4.5 Customs control</b> .....	<b>30</b>
<b>4.6 Security incidents</b> .....	<b>30</b>
4.6.1 Security related incidents in 2008.....	30
4.6.2 Reporting incidents .....	30
<b>4.7 Security challenges</b> .....	<b>31</b>
4.7.1 Main weaknesses.....	31
4.7.2 Vulnerable links in the chain.....	32
<b>4.8 Security measures with most potential</b> .....	<b>33</b>
<b>4.9 Concluding remarks</b> .....	<b>34</b>
<b>5. Elements in a common security strategy</b> .....	<b>35</b>
<b>5.1 Baselines for risk management</b> .....	<b>35</b>
5.1.1 A model for understanding accidents.....	35
5.1.2 A system perspective.....	36
5.1.3 Anticipation and Resilience.....	37
5.1.4 Strategies at different levels .....	37
<b>5.2 Special challenges for rail freight security efforts</b> .....	<b>38</b>
5.2.1 Rail as an open system .....	38
5.2.2 Cross-border security planning involves many stakeholders....	39
5.2.3 Coupling to other factors – conflict or synergy? .....	39
5.2.4 Cross modality and risk migration.....	40
5.2.5 Basic security principles for rail freight.....	41
<b>5.3 Regulations and feedback processes</b> .....	<b>41</b>
5.3.1 The EU safety directive – a baseline.....	41
5.3.2 National support and feedback loops.....	42
<b>5.4 Security research – a field of growing importance</b> .....	<b>43</b>
5.4.1 Meeting the Challenge – a research agenda.....	43
5.4.2 Main findings on security from RETRACK WP 2 .....	44
5.4.3 Findings on strategy from RETRACK Security Survey, WP 7.2	45
5.4.4 The need of a research road map .....	46
<b>6 Conclusions for RETRACK</b> .....	<b>48</b>
<b>6.1 RETRACK must cope with general challenges</b> .....	<b>48</b>
<b>6.2 Security actions for the RETRACK project</b> .....	<b>48</b>
<b>6.3 Specific experiences from the RETRACK project</b> .....	<b>50</b>
<b>7. References</b> .....	<b>52</b>

# 1. Background and scope

## 1.1 Introduction to RETRACK

The European Commission (EC) aspires to achieve a sustainable modal shift of freight traffic from road to rail to achieve a market share of 15% by 2020, an aspiration also supported by the European Rail Research Advisory Councils (ERRAC). Along with this aspiration the main objective of the RETRACK project is to develop, demonstrate and implement an innovative and market-tested rail freight service along the East-West trans-European corridor from Romania to the Netherlands through Hungary, Austria and Germany.



The rail freight ventures in the RETRACK project exploit business opportunities created by EC rail liberalisation and the ongoing work on removal of operational, institutional and technical fragmentation between the national railway systems through standardisation of infrastructure, IT systems and rolling stock.

## 1.2 Security in RETRACK

### 1.2.1 The security concept

In general terms *security* is defined as “Freedom from risk or danger; doubt, anxiety or fear.” Security is thus something that assures safety and confidence; it is the quality or state of being secure. Security strategies to protect and ensure critical functions in society involve many aspects (i.e. economic, physical, cyber (IT) and human aspects (cf. for instance the US National Infrastructure Protection Plan (NIPP) 2006). Protection encompasses deterring threats, mitigating vulnerabilities and minimising consequences.

In transport, safety is concerned with the prevention of unintended incidents i.e. accidents, while security deals with willed incidents like criminal acts, vandalism, terrorism and the like. But when discussing safety vs security natural hazards will often be found in the latter group. This is probably due to the fact that security is related to society's vulnerability.

The strategies for deterring threats will differ between safety and security policies, while mitigating vulnerabilities and minimising consequences to a great extent will be the same for both themes. A well developed safety policy will probably reduce security threats and vice versa. It is thus pointless to make sharp distinctions between safety and security concept and strategies.

### **1.2.2 Security integrated in several WPs**

Safety and security are important aspects of all transport modes, but especially challenging in cross-border transport through several countries and at a period of time when many new threats occur. The RETRACK project and concept has thus included and integrated this aspect in several Work Packages, especially in WP2 "*State of the art of current rail services*" and WP6 "*Development of efficient rail infrastructure and interoperability*" services, and has also defined a special security work package; WP 7 "*Security practises in rail cargo transport*". The latter is presupposed to take advantage of results from other WPs mentioned and also to deliver input to WP 5 "*Development of an ICT goods control centre*" and WP8 "*Pilot demonstration of new rail freight service concept on Trans-European corridor(s)*".

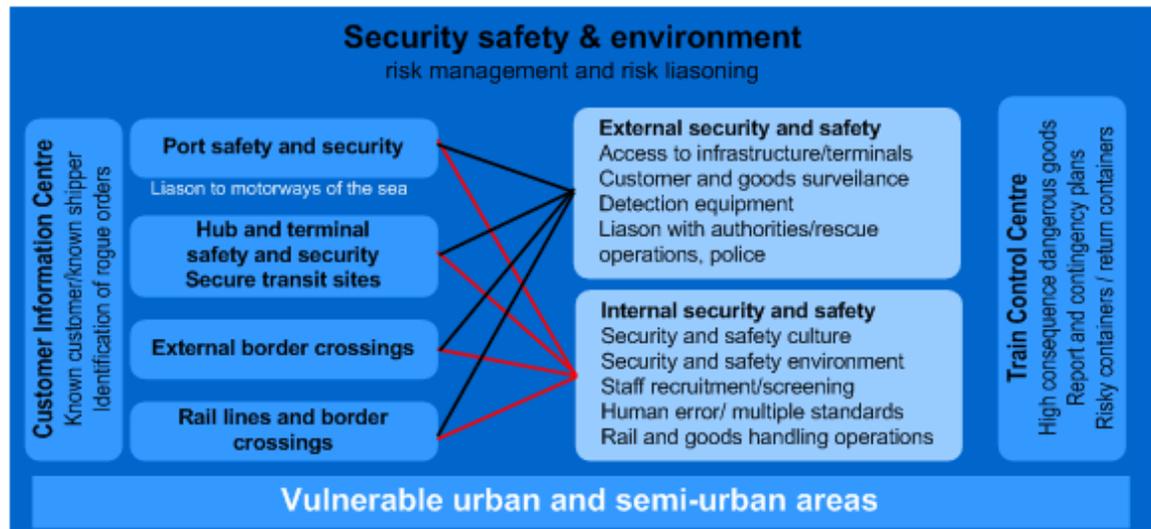
### **1.2.3 WP 7 purpose: Stimulating security consciousness**

The original objective of WP7, titled *Safety and Security*, was to: "*Implement security, safety and environmentally conscious business practices in all part of the business case demonstration project including the goods information centre and customer information centre.*" The proposed WP7 comprised six tasks and had a budget of 51 Man Months (MM). With a strong focus on implementation this WP should result in concrete master plans, blueprints and presentation of critical stretches and areas of operations for corridors, hubs, ports and border crossings, systems for reporting incidents, identification of human errors that can lead to accidents and establish liason routines with relevant authorities and stakeholders across nations involved. (See RETRACK 2005 and RETRACK Technical Annex 2006 for details on objectives and activities.)

During the contract negotiations and the distribution of the budget, due to increased focus on the demonstration project, WP7 was reduced to 27 MM. Later it was agreed to further reduce the scope of WP7 and the budget was downsized to 9 MM. Accordingly the purpose and content too was rescaled. Thus the purpose became to stimulate rather than to directly implement security consciousness by for instance building an organisation, set up screening systems, establish registration systems for incidents and making risk charts for the corridor. The purpose of WP7 was also narrowed by cutting safety and environment out of the objective.

The content, number of tasks and description of WP7 in chapter 6 in the Technical Annexes was accordingly changed (RETRACK 2008). It still contains the picture of all the elements included in security work, but the rescaled – and limited - focus is precisely given:

“The figure below (from the original WP7 application) fully illustrates the complexity of the security theme and the many parts of the cargo business, as well as in the external surroundings, that should ideally be encompassed in a security practices overview. However the objective of the current WP7 is strictly limited to experiences found in current European literature and among the RETRACK consortium partners.” (RETRACK 2008)



**Figure 1:** Risk management and risk liaisoning overarching external and internal security concerns. Source: RETRACK 2008.

The new WP7 should focus on : **Security practices in rail cargo transport** and was given the following objective: “WP 7 will contribute to a security-aware business practice by collecting and distributing information on practices and experiences among the members, and by discussing security strategies among the partners. Knowledge on security is necessary – though not alone sufficient – for prevention and management of high-level risks. Discussions on the information given by WP7 will contribute to the continuous work on security performed by the partners and operators along the corridor.” (European Commission 2008, Technical Annex for RETRACK contract 038552)

WP7 had three tasks:

- Task 7.1: Overview Key Questions in literature on security practices for prevention/management of risks, cf. delivery D7.1
- Task 7.2: Survey on security practice and experiences executed by RETRACK partners, cf. delivery D.7.2
- Task 7.3: Summary of survey, discussion and recommendations, the theme of this report

The connections to other WPs have been less developed than presupposed due to market problems influencing the operational plans of RETRACK. This fact has both resulted in other WPs being delayed and reduced the partners' capacity to deliver contributions to WP7, cf. chapter 2.2. However, the findings and conclusions from WP2 “*State of the art of current rail services*” has been an important baseline for WP7 (Dellimnger & Kotsikos 2008, .

### 1.2.4 Definition of focus and issues to be addressed

The RETRACK WP7 project deals with practices in cross-border rail freight business. The work package addresses security issues related to operating in international multi-standard environments where new norms, new organisations, new responsibilities and new equipment pose additional challenges to national projects. Table 1.1 gives an idea of where the emphasis of WP7 should be found.

Table 1.1: Overview of focus issues and themes not focused in WP7. RETRACK Security Survey 2009 .

<b>Focus</b>	<b>Not in focus</b>	<b>Remarks</b>
<i>Security Civic society</i>	<i>Military security</i>	<i>Given by RETRACK's objective</i>
<i>Rail freight</i>	<i>Passenger mass transport</i>	
<i>Cross-border cargo</i>	<i>Nasjonal cargo</i>	
<i>Transport; terminal and cargo handling stakeholders</i>	<i>Infrastructure, signalling, power supply</i>	<i>Recommendation from WP2</i>
<i>Practises</i>	<i>Regulations</i>	
<i>Security</i>	<i>Safety</i>	<i>Result of downscaling of WP7</i>

Practises for WP7 encompasses the whole chain from defining risk to implementing internal security procedures and a broad range of activities like staff screening and training, incident reporting and planning of organisational security. Experiences from collaboration with customs, police, terminal/hub, port authorities, industrial organisations, and other relevant authorities on minimising external and internal sources/consequences of risks should or could be included. Themes to be given special focus were not defined from the start, but were to be defined in dialogue with the partners, cf. sub-chapter 2.2.1.

Following the conclusions of and recommendations on the scope of the security theme made by the RETRACK partners in relation to WP7.2.4, WP7 should review *the transport component* related to transported goods and not infrastructure, signalling, power supply etc. This does not mean that a system perspective on security is excluded, but that detailed studies of infrastructure-related security measures are not in focus (Dellinger & Kotsikos 2008).

Justified by the stakeholder's responsibility as well as an estimation of where there already exist sufficient regulation or control systems, questions related to regulations on hazardous cargo were also excluded in the RETRACK Security study. Hazardous cargo is assumed to be governed by existing regulations, protocols with international standards (RID, ADR) and national reinforcements. This is somewhat contradictive to the initial objectives set for WP7, stating that "*Special focus will be on handling high-consequence goods and high-risk containers*". EC regulations governing rail transport are handled in other RETRACK WPs and thus not taken into account in the literature review, but regulations as a strategy is included the survey.

In any case we did not find any national or international regulation governing security in transport as a whole. The US new "*Rail and public transport security act*" that was heard by Congress in 2007/2008 never became law (GovTrack.us.2010). In Europe common regulation governs the transport of dangerous goods, and the RIPs (Railway Infrastructure Packages) govern

European cross-border rail transport. Some of the measures proposed in the “Safety Directive” (European Commission, Directive 2004/49/EC) will also improve security. Appendix I in D.7.1 gives an overview of relevant regulations.

### **1.3 Contents of the report**

This report summarises the survey and literature, pinpoints questions for discussion among the partners and identifies certain challenges to consider when developing strategies for security along the RETRACK corridor. Chapter 2 describes the *methods used* and the limitations of WP 7.1 (The literature review) as well as those of WP7.2. Chapter 3 looks at some *facts and figures on the prevalence* of accidents and security-related incidents and gives some detail on the different security problems identified by the literature review and the state-of-the-art description from WP1.

Chapter 4 is a summary of the *results from the security survey*. Security practices in the different countries are presented, together with summaries of the main challenges in national and international rail (freight) security as they are perceived by different stakeholders. As the RETRACK Security Survey is not a quantitative survey aimed at describing the actual prevalence of such challenges, the presentation also gives themes for forthcoming research.

The results from WP7.1 and WP7.2 were initially supposed to be summarised in the form of recommendations on critical issues that RETRACK and other cross-border rail cargo enterprises must address. Given the limitations of the study, we find it difficult to give strong recommendations. As a *base for further strategic thinking*, chapter 5 discusses some causal models, the special challenges of rail freight and cross-border transport and the potential of measures as expressed by the RETRACK Survey respondents. In addition the summary in chapter 6 pinpoints challenges and recommended actions especially for RETRACK.

## **2. Methods**

### **2.1 Literature review – WP7.1**

WP 7.1 should summarise and assess knowledge on security practices by drawing on available experiences from the literature dealing with the European Railway system and in particular border-crossing goods transport.

#### **2.1.1 Sources and search words**

The search for literature and other relevant information concerning rail freight security was done using different search machines, and viewing specific web-pages. To look for relevant information about rail freight security we used TRIS (National Transportation Library by TRB), ISI, ScienceDirect and Google.

We also viewed information on the following web-pages: European Commission DG Energy and Transport, Eurostat, the European Railway Agency, US Department of transport – Federal Transit Administration, Homeland Security (US), Association of American Railroads and International union of railways (UiC).

Searching of literature databases was done using the following search words: “rail freight security”, “rail terror”, “security rail”, “rail security European regulations”, “rail security plan”, rail security management”, “container security”, “rail cross border security”, “railway terrorism”, “rail container dangerous goods”, “rail hazemat” and “rail terror dangerous goods”.

Material from RETRACK WP2 on “Safety and security issues” (Dellinger and Kotsikos 2008) made a good basis for seeing the results in light of the RETRACK project.

#### **2.1.2 Limitations by the theme**

The RETRACK literature study (Kolbenstvedt and Amundsen 2008) failed to identify many references from studies on security practises in rail freight transport, on experiences with the consequences of different strategies, evaluation of tested measures, etc. Security in rail freight obviously is not a big area in transport research. Most documents found concern “bureaucratic” aspects related to planning, preparing laws, describing measures used, and technologies developed, and do not give research-based knowledge on their effects, cost/benefit etc.

We have, due to linguistic and economic capacity, only looked at publications written in English and published mainly since 1995. Given this limitation most publications come from Europe or the US. The US has had an increased focus on security, especially following the 9/11 terrorist attacks, and much of the literature on rail security is therefore American. In Europe there has been an increased focus on security, but safety remains the main concern.

A limitation imposed by the security theme itself is that the willingness to publish experiences and detailed descriptions of strategies against incidents caused by willed human actions will be less than for matters concerning accidents and traffic safety. It is not desirable to broadcast your secret strategies or the weaknesses

and strengths of your “weapons” (your technological and organisational measures) to your “enemies”.

And parallel to this - along with deregulation and privatisation - there is a shift from public to private stakeholders, the latter being less inclined to publish their commercial strategies, assets or weaknesses. Rail cargo transport as a theme is not strongly represented in the academic transport publication databases. We find far more material on rail passenger security, and have looked at some of those with a generic relevance that could be of interest also for rail freight.

With respect to technical equipment the literature mostly concerns technology related to security in cross-border transport (terminals and border stations), and more precisely tracking devices to find and control certain cargo during shipment. There are more descriptions of what “might be useful technology” than empirical tests or systemised experiences. In the absence of evaluation of techniques, we have chosen not to go into detail here.

## **2.2 Security survey – WP7.2**

One main purpose of WP7 was to collect information about security challenges affecting international rail freight operations by interviewing different stakeholders in the countries working with the RETRACK rail pilot, i.e. Romania, Hungary, Germany, Austria and the Netherlands. Task 7.2 should formulate and distribute a questionnaire on security practices and experiences to RETRACK partners. Each partner was to collect answers from their own country.

Frequent shifts of partners as well as severe market problems for the RETRACK pilot made it necessary to try other strategies. These have not given the desired outcome, a fact which demands a careful interpretation of the results in chapter 4.

### **2.2.1 Short questionnaires on eight themes**

The content of the questionnaire was based on central themes found in task 7.1 and discussed with the RETRACK partners. Eight themes were included:

- The prevalence of security standards
- Experience with security assessment
- Personal training plans
- Site security inspections
- Emergency preparedness
- Custom control
- Incident reporting systems
- Perceived security challenges

The questionnaires presented respondents with predefined answer categories, making it possible for both interviewing partners and respondents to answer without too much effort. For some questions though, the respondents could fill in their own remarks. The purpose was to collect information on respondent experiences with security practices and to capture unforeseen aspects of the security theme.

The questionnaire was made as short as possible to ease the collection of data. Due to limited economic resources, the standard questionnaire was written in English thus supposing that the RETRACK partners who were to ask the questions could handle a possible simultaneous translation.

## 2.2.2 Special questionnaires to six types of stakeholder

The survey was to include the following six types of respondents:

1. Ministry of Transport (1 per country)
2. Railway inspectorate or similar (1 per country)
3. Infrastructure/terminal management (1-2 per country)
4. Police and other emergency authorities (1-2 per country)
5. Major rail freight transport companies (1-2 pr country)
6. Customs (1 in Hungary and 1 in Romania)

To make the survey as effective as possible we designed six different questionnaires, one for each type of stakeholder. Table 2.1 indicates which themes each type of respondent had to answer. The number of questions varied from 13 – 22 for different stakeholders. The questionnaires can be found in D.7.2 (Kolbenstvedt and Amundsen 2009).

*Table 2.1: Overview of the stakeholders who were to answer the different questions. The shaded (light blue) cells indicate the type of questions asked to the specific respondent. RETRACK Security Survey 2009 .*

Question Theme	Infrastruc-ture Terminal manager	Rail cargo transport company	Ministry of Transport	Railway inspec-torate	Police, emergency authorities	Customs
Security Standards						
Security checks assessment						
Personnel, training						
Site security, inspections						
Emergency preparedness						
Custom control						
Incidents, reporting						
Security challenges						
<b>Number of questions:</b>	<b>22</b>	<b>20</b>	<b>15</b>	<b>13</b>	<b>15</b>	<b>18</b>

## 2.2.3 Partners responsible for conducting the survey

To conduct the security survey one elected partner of the RETRACK partnership was asked to carry out the necessary interviews in their respective country, cf. the RETRACK TA. These partners were responsible for collecting answers concerning their country from the different type of stakeholders included. Each elected partner was thus responsible for 5-10 interviews. The questionnaires were to sent by e-mail to the respondent, with a follow up phone call. The respondent could then choose if they wanted to answer the questionnaire themselves by e-mail, or in an interview during the phone call.

The questionnaires elaborated by TØI was sent to each partner several times and also distributed at meetings where the partners were encouraged to fulfil the contracted task. Due to shift of partners, market and other operational problems in RETRACK this strategy did not succeed. Even the stakeholder type well represented in the RETRACK consortium, i.e. rail freight company partners, did not answer “their own” questionnaire. The outcome was a complete set of questionnaires from the Netherlands, collected by Delta Rail, and none from other countries.

### 2.2.4 Change of strategy

At this stage we decided to change strategy and redistribute responsibility for the interviews. TØI was to carry out interviews in Romania, Hungary and Austria, while Delta Rail were to take care of the German part of the study.

To find persons responsible for security in rail freight transport among the six types of stakeholders chosen, cf. table 2.1 in the three countries of Romania, Hungary and Austria, we first asked the RETRACK partners to send us any relevant contact names, e-mail addresses or phone numbers they might have. This request did not give any results.

We then used web searching and follow-up phone enquiries, as well as other personnel contacts in the targeted countries. In this way we gathered a list of possible contact persons at different authorities or stakeholders, including their e-mail address and telephone number. Although we had this list it was very difficult to reach the right persons and get the questionnaires answered by e-mail or by phone. Typical problems were:

- People we contacted claimed that they were not the right person, for instance due to the fact that the organisation had changed staff, so that our contacts did not have the duties we expected. They sometimes promised to forward our questionnaire to relevant persons, but there was often no subsequent reply.
- Even when we found the right person on phone and afterwards sent the questionnaire to them by e-mail, there was no guarantee that we would receive the questionnaire. We called every person several times to remind them about the questionnaire, but they said that they were very busy and we had to wait. In most cases there was no ultimate answer.
- In all three countries, it was difficult to communicate in English, especially in Romania. After a long process of calling different sections of the relevant authorities in Romania, we finally found two people (at the Inspectorate of Romanian Transport Police and the Railway Inspectorate) that could answer us in English, and fortunately they filled in the questionnaires and returned them to us.

### 2.2.5 Low response rate

In total we received 12 answered questionnaires. This left us with a response rate of 44%. No questionnaires were received from Germany. A final try with revised questionnaires, only containing fixed categories, did not result in further responses.

Table 2.2: Respondents in the RETRACK Security Survey 2009.

Questionnaires/ Respondent	Answers from	Planned min. nr	Achieved number
Ministry of Transport	The Netherlands, Hungary	5	2
Railway Inspectorate	Hungary, The Netherlands, Romania	5	3
Terminal/railway managers	The Netherlands	5	1
Rail freight companies	Austria,	5	1
Police/Emergency Authorities	Austria, The Netherlands, Romania	5	3
Customs	Hungary, The Netherlands	2	2
<b>SUM</b>		<b>27</b>	<b>12</b>

## **3. Problem areas – facts and figures**

### **3.1. Risk in rail transport**

Though focussing on security, it is important to have the relative dimensions of the different problems as well as the links between them in mind when formulating strategies and allocating resources. According to Bech (1992) people in modern society are less willing to accept any kind of risk, and this raises doubts about whether “Vision Zero” will ever be realised. In fact there will always be accidents or fatal incidents while every natural hazard, willed action or mismatch between human, technical and organisational components cannot be foreseen.

The security concept can encompass different phenomena and threats. The common trait of these threats is often that they are intended, there is a human evil intention involved. As shown in WP2, willed threats to rail freight transport encompass several factors. WP2 defines theft, damage in transit, smuggling (people, weapons and substances) as major security threats.

#### **3.1.1 Risk differences between rail and other transport modes**

There are no data sources which give us a complete and updated global or European overview of accidents and fatal incidents which could make it possible to compare losses in the transport safety- and security-arenas respectively. Overviews of safety and risk in different transport modes are also lacking, as is knowledge about the differences between public rail transport and rail freight transport. It would be an extensive work to establish such an overview. It would be necessary to combine data from a lot of sources more or less defective in different ways.

Eurostat (European Communities, Panorama of Transport 2007) has some figures. Rail transport in Europe has a significantly lower risk per million inhabitants than road transport, 3 fatalities vs. 90. Also air and maritime transport shows higher risk figures than rail transport. Yearly ca. 3000 persons in Europe are injured in rail transport, and approximately half of them are killed. Due to the rarity of fatalities in railway accidents, one must of course be very careful when comparing and interpreting data.

In a Norwegian study (Amundsen and Elvik 2006) on safety of rail freight in Norway, safety of rail freight was compared to the safety of road freight. In this study the risk level of the two modes were calculated per million vehicle kilometres, and based on actual accidents in the period from 2000 to 2004. The calculation showed that the risk of fatality was about 14 percent higher for road freight than rail freight. If the two transport modes had been compared taking the ton-kilometre into account, the difference would have been higher. The same conclusions were reached by a study on transporting hazardous material like aircraft fuel (Elvik and Erke 2006).

Figure 3.1 gives a picture of the prevalence of different incidents in rail vs. bus transport as experienced by 100 US stakeholders (agencies interviewed by Taylor et. al. (2005)). We find no significant differences between the two modes.

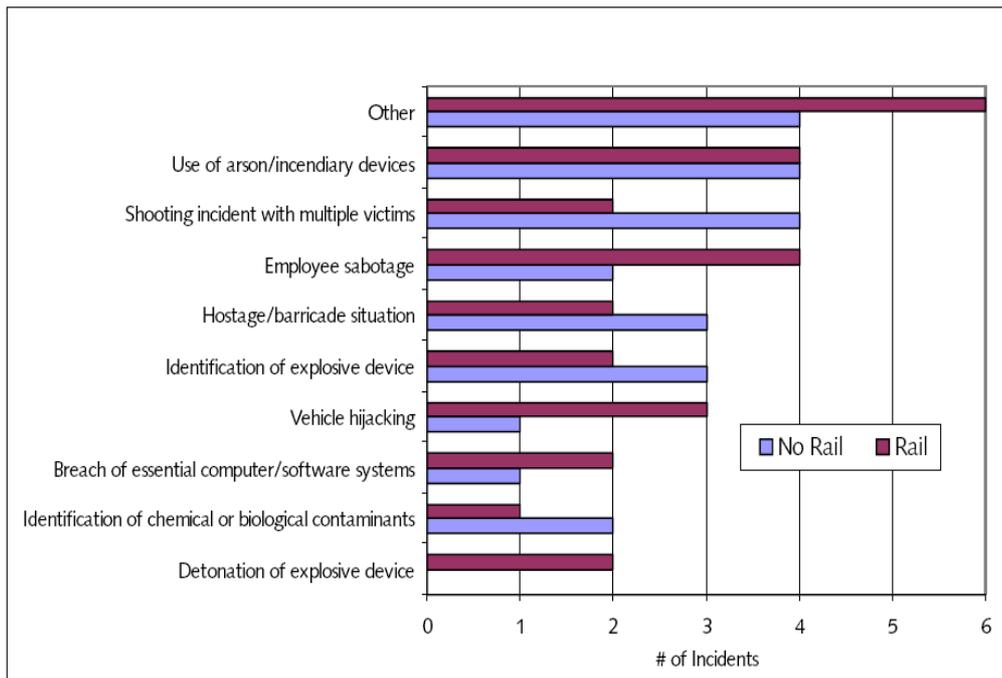


Figure 3.1: Incidents experienced in rail and bus transport. Interviews with 100 US stakeholders. Source: Taylor et. al. 2005.

### 3.1.2 Major accidents in public/passenger transport

Though it is by far the most risky transport mode, road transport has few major accidents (defined as accidents with more than five fatalities). Rail transport is involved in fewer major accidents than other transport modes, see Table 3.1. In Europe during the period 1991-2003, there were 56 rail accidents in passenger transport, compared to 102 air transport accidents. Air transport also has the largest number of fatalities related to accidents.

Table 3.1 also suggests that transport in Europe is safer than in the rest of the World. Table 3.1 shows that 20% of the major accidents were registered in Europe, but only 13% of the fatalities.

Table 3.1: Major accidents in passenger/public transport globally and in Europe 1991-2003. Road transport not included. (Major accidents = more than 5 fatalities, waste material or environmental damages. Here only fatalities are counted).

Transport mode	World		Europe	
	All accidents	No. fatalities	No. accidents	No. fatalities
Air	504	21347	102	2923
Maritime	294	13009	57	1828
Rail	272	7950	56	751
<b>Total</b>	<b>1070</b>	<b>42306</b>	<b>215</b>	<b>5502</b>

Source: Elvik & Olsen 2004)

Figure 3.2 shows the development over time. In the period 1991-2003 we find a decreasing tendency in Europe, yearly estimate of 6.8%. We have no similar data for rail freight transport.

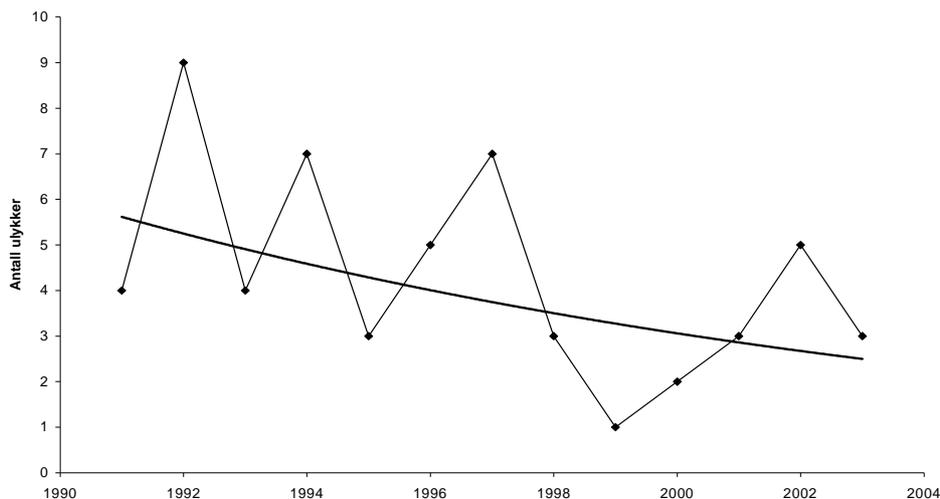


Figure 3.2: Development of major passenger rail transport accidents in Europe in the period 1991-2004. Source : Elvik & Olsen 2004.

### 3.1.3 Accidents vs. terrorist attacks

Most of the data on security issues are connected to a possible terrorist attack. Terrorist attacks have mainly been directed on passenger transport (Jenkins and Gerston 2000, Taylor et. al. 2005), but we find an increased focus on the possibility of hazardous materials (hazmat) used as potential terrorist targets.

We have not found tables depicting differences in fatality risk, country etc between accidents, terrorist attacks and other willed actions for rail freight transport - or for rail transport totally. Taylor et. al. (2005) did put together material on 800 separate incidents of terrorist attacks and other criminal incidents involving public transportation by rail and busses worldwide between 1972 and 2005. The extensive material collected by Jenkins and Gerston (2000) from newspapers and other sources was included.

With reservations for weaknesses in data, due to different and insufficient reporting, this material makes it possible to make rough comparisons with accidents and to depict some trends in transit terrorism, see Table 3.2 and Figure 3.3.

Table 3.2: Major accidents and terrorist attacks in passenger/public rail transport globally and in Europe 1991-2003. All rail accidents in 2005. Based on material from Taylor et. al. (2005), Elvik&Olsen (2004) and ERA (2007).

Transport mode	World			Europe		
	All accidents	No. fatalities	Fatalities per acc	No. accidents	No. fatalities	Fatalities per acc
Rail major accidents (> 5 fatalities)	272	7950	29.2	56	751	13.4
Rail - all sign. accidents - 2005 only and EU 25				7023	1464	0,2
Terrorist attacks	261	1098	4,2	85	108	1,3

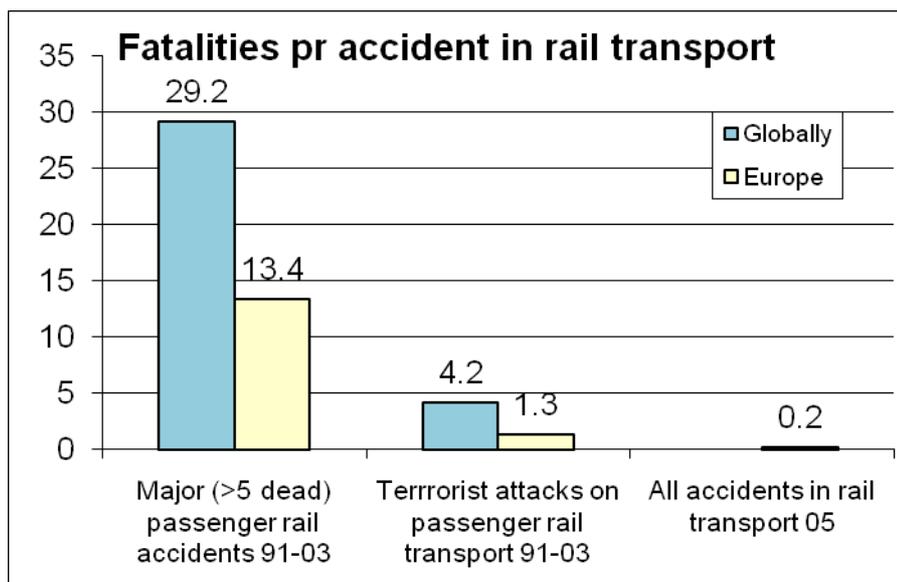


Figure 3.3: Fatalities per accident in major accidents and terrorist attacks in passenger/public rail transport globally and in Europe 1991-2003 and all rail accidents in 2005. Based on material from Taylor et. al. (2005), Elvik&Olsen (2004) and ERA (2007).

Table 3.2 and Figure 3.3 clearly show that - so far - major rail accidents are far more lethal than terrorist attacks. This applies both globally and in Europe. The fatality risk is higher globally than in the European countries.

Looking at all railway accidents however, terrorist actions are more dangerous. An explanation here is that freight transport affects fewer persons and thus accidents normally result in fewer fatalities.

### 3.1.4 Rail accidents by type of accident

Of those mortalities in European rail transport (1517 persons in 2007) only 5% are passengers. The most common type of accident by far were those caused by rolling stock in motion. This category encompasses: 1) people trespassing and walking on the line and 2) level-crossing users.

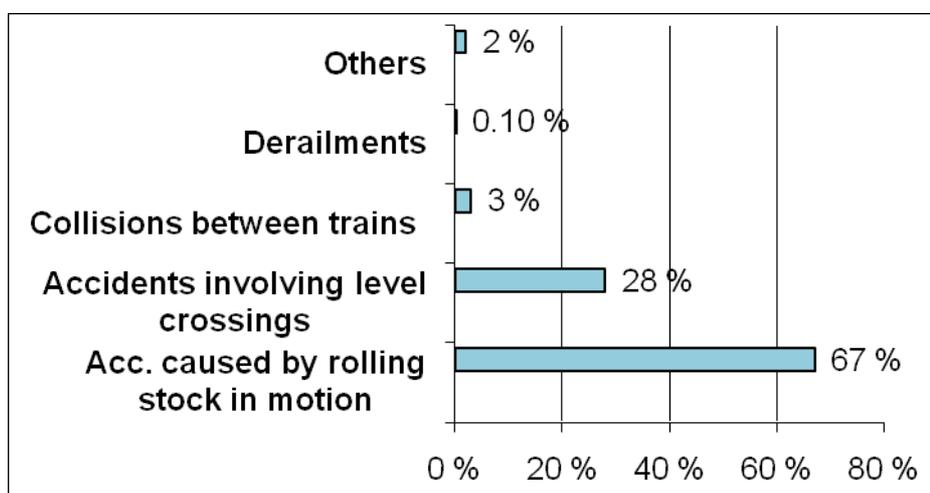


Figure 3.4: Persons killed in rail transport by type of accident in Europe 2005 (EU 25). Source: Eurostat, EU Panorama of transport 2007.

In 2008 there were 52 accidents involving dangerous goods in the EU. 38 of these were accidents where dangerous goods were released to the environment (Eurostat, EU Panorama of transport 2010). There are large differences between countries, probably due to different reporting practices.

## 3.2 Transport of hazardous materials (hazmat)

### 3.2.1 Many vulnerable points and large consequences

Each year huge amounts of dangerous goods are transported by rail. The number of ton-km and the number of access points make it impractical to screen all goods and all employees. There are too many points of vulnerability to ensure full security during hazmat transportation. Main challenges are related to the general safety system. Even small deviations from this and lack of ordinary safety barriers can have enormous consequences given that the cargo passes urban conglomerations, environmentally important areas etc, cf. the Lillestrøm near-BLEVE-accident in 2000 (NOU 2001). Terminals and borders are especially crucial points in the logistics chain, and this is a focus of security plans.

Table 3.3 gives an overview of the amount of cargo and hazardous materials carried by freight rail in different European countries.

Table 3.3: Goods transport in European countries in 2006. Ton-km and total tons of cargo on rail. Percentage of cargo that is potentially hazardous material. RETRACK corridor countries are shaded. Source: Eurostat Database 2009.

Country	Ton - km (mill ton-km)	Total ton of cargo (1000 tons)	Hazardous materials (% of total ton)
Belgium	8 572	62 188	14
Bulgaria	5 225	21 183	40
Czech Republic	15 779	97 491	47
Denmark	1 885	7 300	2
Germany	107 007	346 118	34
Estonia	10 418	61 284	88
Ireland	205	1 245	-
Greece	662	3 884	13
Spain	11 105	24 935	16
France	40 924	108 333	18
Italy	20 868	70 604	5
Latvia	16 831	48 731	80
Lithuania	12 896	50 225	66
Luxembourg	441	12 133	8
Hungary	9 279	46 777	29
Netherlands	5 341	30 655	30
Austria	17 871	86 161	17
Poland	44 331	156 400	53
Portugal	2 430	9 775	23
Romania	14 431	64 218	63
Slovenia	3 373	17 052	20
Slovakia	9 988	52 449	23
Sweden	22 271	64 944	4
Finland	11 060	43 560	15
Croatia	3 305	15 395	29
Turkey	9 544	19 745	21
Norway	3 251	24 144	2

1) Hazardous materials here defined as different types of petroleum products, chemicals.

The amount of hazardous materials carried by rail differs greatly from country to country, from 2% to 88% of the total tons of cargo transported by rail. Among the RETRACK countries the variation is from 17% to 63%. The data are collected from the database Eurostat (theme; Railway Transport, Accidents, Transport of Hazmat). For some countries data are lacking, causing some uncertainty about the percentage of hazardous materials reported in the table. Some of the materials we have defined as hazardous might not be, but it is difficult to be more exact due to the categories of cargo in the statistics.

One can consider whether transport of hazardous materials by road or by rail is safest. The risk of an accident is higher on roads, but the amount of material carried by train is usually higher, so the potential consequences of an accident are higher for rail. In addition one has to take the track location and the character of the surroundings into account.

### **3.2.2 Cargo visibility and integrity - technological development**

The security discussion concerning cargo transport is mainly focused on the possible use of dangerous goods as target (that the train can be used as a "Trojan horse"). It is important to be able to track a given shipment and its content at any time. Regulation of information on border-crossing cargo and technical devices for cargo visibility and integrity (i.e. that the container contains the same cargo from the moment it is sealed to the moment it arrives) are crucial elements in achieving this.

There are several measures under development, especially in the US (Peterman, Elias & Frittelli 2007 in their report to Congress). In spite of a rapid development of devices over the last few years, there is still a long way to go before optimal solutions can be identified in this field, but we will mention some of the regulations and devices on test in the USA;

- Smart-box technology (palm-sized tracking devices) that could be mounted on an interior wall of a container has been tested on selected routes. But in the short term shippers and carriers still favour using the best container seals currently in use.
- At the border crossing with Canada and Mexico, gamma ray technology is used to scan one entire rail carriage at a time. The gamma ray source and detectors are stationary, and the trains move through the system. Today, where the equipment is installed *100% of the rail carriages are scanned*. Some argue that 100% scanning will bottleneck terminal operations. It has also been found that the current scanning equipment is not accurate enough and could be easily circumvented by terrorists (Peterman et. al. 2007).
- In the US truckers and railroad operators from Canada and Mexico must report their contents 0.5 and 2.0 hours respectively before arriving at the border. Customs and Border Protection (CBP) analyses the cargo manifestations and other information to select which cargo to inspect physically, a critical process to keep terrorists and their weapons from being smuggled into the country.
- The Canadian and the US customs co-operate and send each other cargo information. They have also developed common principles for targeting, screening and examining cargo at the borders.

### 3.2.3 Identification and Authorisation Measures

Measures to screen admittance to the railway system can be found at different levels from individual workers to organisations or operators.

#### *AEO - Authorised Economics Operators in the EU*

The EU has established a certification system (Authorised Economics Operators) for rail operators. The operators must meet a certain security standard to be able to qualify for the certificate. An Authorised Economic Operator is an economic operator who is defined to be valid throughout the EU in the context of customs related operations, and therefore is entitled to enjoy benefits throughout the community. The holder of an AEO-certificate is entitled to (Commission of the European Communities 2007):

- easier admittance to customs
- fewer physical and document-based controls
- priority treatment if selected for control
- possibility to request a specific place for secure control

To qualify for an AEO-certificate the operator must fulfill different criteria on customs compliance, appropriate record-keeping standards, financial solvency, and maintaining appropriate security and safety standards.

#### *TWIC - Transportation Worker Identification Credential in the US*

Early in 2007 the TSA (Transport Security Agency) and the Coastguard agreed on the implementation of TWIC (Transportation Worker Identification Credential programme) at US ports (Peterman et. al. 2007). Under this programme Longshoremen, or truck drivers, merchant mariners and other maritime workers need to apply for a TWIC card to obtain unescorted access to port facilities or vessels.

The card will use biometric technology for positive identification, and TSA will conduct a security threat assessment on each worker before issuing a card. The security threat assessment has standards for examining criminal history, immigration status, mental capacity and terrorist activity. The implementation recommendations codify a special list of criminal offences that will disqualify a worker from getting the TWIC card.

### 3.2.4 Cost efficiency vs. security

A major challenge is to cost-efficiently increase security, especially for those threats posing the most danger to the public, and still meet the transportation requirements of commerce. Industry and government are gradually implementing “layered” systems of measures; this system involves incident prevention, preparedness and response.

Technical devices for tracking hazmat are not very well developed or tested. A particular challenge is that it might be very dangerous if hazmat information gets into the wrong hands.

Another dilemma surrounds the location of tracks and terminals. There are both pros and cons for routing hazmat through or around urban hubs. Shorter distance to customers and less road traffic transport might be good for the environment and safety – but if an accident with hazmat should occur in an urban setting the consequences would be far more serious than one occurring on the outskirts.

## 3.3 Criminal activities and vandalism

### 3.3.1 Thefts and smuggling

Theft of goods in transit costs billions of Euros each year (Commission of the European Communities 2003). A major part of the theft and smuggling is carried out by organised criminals (US Department of Transport 1999). Findings (US Department of Transport 1999) suggest that employees play a major part in theft, either directly or indirectly. In the US where the labour organisations have a strong hold, it is difficult to check the criminal record of persons they want to employ. Theft is considered a minor criminal activity, and cannot be asked about when interviewing new personnel (except security guards).

The penalties for theft or pilferage are low, and may not be enough to discourage further criminal activity. Some companies even declared that it was not worth investigating criminal activities on their premises, when the police investigation is either dropped or the sentencing is considered too lenient. The goods are insured, so why bother to prosecute or employ expensive security measures?

Cargo theft – this is carried out primarily as an *organised criminal act* (have substantial evidence on this). The US Department of Transport (DOT 1999) has summarised facts and findings on this theme. Often, criminals act on information given by transportation employees (inside information – or help). CIGNA Corporation (insurance company) reports that most cargo loss claims “involve cargo taken from transportation facilities *by personnel authorized to be there* and on vehicles controlled or similarly authorized by management”. Estimates indicate that “well over 80 percent of all theft and pilferage of transportation cargo is accomplished by, or with the collusion of, persons whose employment entitles them access to the cargo that is stolen”.

A majority of cargo theft occurs *at the terminals*. Methods used are:

- Opening the container – removing the goods – transporting them out in personnel automobile or delivery trucks.
- Falsely claiming that the cargo was hijacked
- Dismantling containers – removing key merchandise, resealing the containers
- Relying on an organised network for spotting, stealing, and fencing
- Driving off with the cargo with fraudulent paperwork
- Speeding through fences and security checkpoints
- Stealing loaded trucks off the street or from storage yards.

Other types of criminal acts can be:

- Smuggling of people, drugs, weapons, nuclear materials, hazmat etc.
- Thefts (personnel, private persons, organized criminals)
- Sabotage (to: vehicles, facilities, software, power supplies etc)
- Arson
- Vandalism
- Bomb threats and other threats
- Cargo tampering or disturbances
- Hijacking/piracy
- Civil disturbances

We have not found detailed data on the occurrence of different types of events and where we most often find the crucial weak link in the transport chain.

### **3.3.2 Challenges in preventing crime**

The transition to “just in time” deliveries make security more important than ever. Experiences and policy statements found in the literature review show that there are many challenges that must be handled;

- Rail transport is an open system. Terminals can be locked, but lines and stations not. After the cargo is sealed it can be shipped/transferred to a number of countries before it is opened.
- A growing volume of containers reduces the potential of discovery of threats. It is easy to conceal objects and far too labour intensive to inspect all containers (cannot check out all -take a sample). At most major container facilities less than 1% of the containers can be inspected each day (DOT 1999).
- Organised crime often involves employees. It has proven difficult to refuse to employ persons with criminal record (US labour and civil law provisions).
- Lack of adequate background investigations and standards for all personnel handling cargo. Different standards in different countries /companies e.g. not all requires to check for criminal records. In some cases it is enough to have a driving licence to get a job.
- Minimal impact if cargo is missing. Some employees were prosecuted – but received minimal or no punishment. Many organisations do not include thefts as a disqualifying element of a person’s record for employment purposes.
- Progress in conducting compliance inspections, but inspector’s role and missions have not been fully defined.
- Companies need to improve their communication with local authorities, in places where they ship dangerous chemicals. The firemen need to know what they are to confront.

## **3.4 Terrorist threats to security**

### **3.4.1 Trends in terrorist attacks on rail**

Terrorist actions are far more complicated to register and analyse than criminal actions and accidents. We have not found an international or European database for these events that could help with comparisons between transport modes.

Open access makes mass transit inherently vulnerable to attack and difficult to secure. Rail freight implies transportation of huge amounts of hazardous materials each year – raising concerns about terrorist attacks. Other problems are the number of stakeholders involved (can lead to communication challenges, duplications and confusion), funding for security actions and the inter-connectivity of the rail system.

There has been an increased focus on security across different transport modes, especially following the 9/11. A majority of the data are from the US In Europe the main focus is still safety, and implementation of the Safety Directive, but security is becoming an increasingly important focus here as well. Improvements since 9/11 are new security measures, increased frequency of inspections, risk assessments, emergency drills and development of security plans. In the US grants to support securing transport is a planned arrangement.

Some characteristics of passenger rail transport terrorism shown in or based on data from Taylor et. al. (2005) are;

- High lethality. While 20% of all terrorist incidents involve fatalities, 35% of the rail transport incidents result in fatalities.
- Two thirds of the attacks occur in countries with ongoing wars or terrorist campaigns.
- Transit crime generally reflects the level of crime of the larger urban area in which it is situated. This is also the fact for terrorist attacks.

We do not have equivalent information from rail cargo, but there are probably some similarities.

### **3.4.2 Areas attacked in terrorist actions**

Most of the terror attacks are directed at public transport in the major cities. Major attacks in the last decade are; 1995: Tokyo (subway- sarin), Paris (metro-bomb), 2000: Madrid (bomb) - 2004, Moscow (bomb)- 2004, London (bomb)- 2005. Trains, lines/tracks and stations are targets (Taylor et. al. 2005, Guerrero 2004). Targets on public surface transport system worldwide, from 1997-2000, were:

- Buses 41%
- Subways and trains 22%
- Subway and train stations 10%
- Tracks 8%
- Bus terminals 8%
- Tourist buses 5%
- Other 5%
- Bridges and tunnels 1%

The overview is thus that buses are attacked more often than trains.

### **3.4.3 Use of technologies**

A crucial issue is the possibility (or lack of) to track a specific cargo at a specific time. We have found a number of articles on technological developments related to screening/scanning cargo or GPS systems to follow specific cargo. It is impossible to get a 100% secure system. In the US they have three test sites at three different border stations to test the possibility of screening all cargo. There are expensive measures, and there is much discussion about who will take the costs.

Cargo can be scanned, but it is possible to disguise e.g. drugs or volatile materials so that it looks like something else. To detect these kinds of materials specially trained dogs is one solution – but it is impossible and far too expensive to check all containers in this way. New requirements in the cargo manifests for border crossings are also an important theme. Rail operators in the US must report their cargo manifest at least 2 hours prior to the border (30 min-1 hour for trucks and 24 hour for ships).

The most extensive used technology applied by the respondents Taylor et. al. (2005) interviewed is a Radio communication system. Such a technology is used by over 90% of the agencies. Figure 3.5 shows the different hardware technologies used by the respondents in this U.S study.

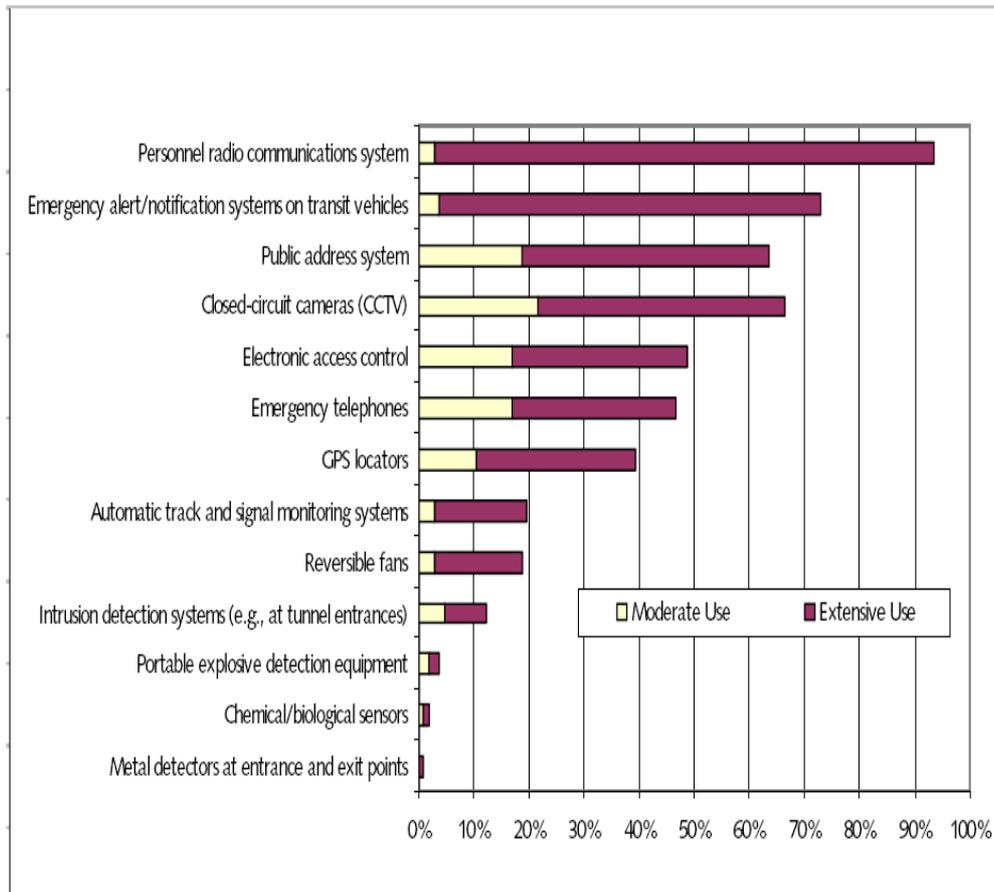


Figure 3.5: Security hardware Technologies and Strategies employed by Agencies. Source: Taylor et. al. (2005).

### 3.4.4 Use of measures not originally security-based

In all transport modes efforts exist whose primary aim is not to secure against terrorist attacks, but which nevertheless can be used to help unravel terrorist plans and prevent terrorist acts. One example of this is the use by British police of the system known as Automatic Plate Number Recognition (APNR) to track down one of the suspects of the car bombs at airport terminals in London and Glasgow in the summer of 2006.

Other measures open to exploitation by authorities for use in anti-terrorist activity include surveillance or registration of persons or vehicles, where the primary aim is to enforce speed limits or avoid petty crime; camera surveillance of terminals, vehicles, infrastructure and station areas (camera surveillance of public places is particularly widespread in Great Britain); automatic registration systems that register vehicle passes on toll spots (AutoPass); electronic tickets; intelligent speed adaptation (ISA); systems that automatically alert ambulance and police of road accidents (e-call); and automatic trip recorders in cars (“black boxes”). There are lots of new technological devices being developed and introduced to guide and control traffic Bjørnskau et. al. (2007), and it is not difficult to envisage their potential use in anti-terrorism efforts.

### 3.5 Balancing security with other concerns

Hamberger (2005) argues for a proper balance between protecting the assets/people, and providing a free flow of goods and promoting our international competitiveness. He quotes Norman Mineta, Former US Secretary of Transport: *"We do not want the checkpoints to become chokepoints"*.

Improvements from national authorities are needed on the following points:

- Unifying government policy regarding freight rail security and more effective coordination of the many governmental projects that affect rail safety
- Improving the current system of counter-terrorism information. It is important to tackle threats by providing timely and actionable information to enable efficient and effective deployment of limited resources
- Discuss the financial responsibility for cargo security. Advocates for public funding argue that homeland security is a national concern and therefore should be paid for by the general Treasury. Others argue that carriers are the direct beneficiaries of improved cargo security. (The US Department of Homeland Security provides grants for transit, passenger rail, freight rail security under the Urbanized Areas Security Initiative program, 400 mill \$ in 2008 (Peterman et. al. 2007).)

The many actors involved in container transport (not the same operator/authority have the responsibility from start to end line) makes organisational devices important. It is necessary to develop a shared security responsibility. Today railroad police literally work side-by-side with intelligence and security personnel at TSA and other agencies of the Homeland security.

Given the varying roles and mandates of the many stakeholders involved from private companies to different agencies of the central and local government, close coordination and cooperation are critical to effective transit security planning. A great challenge is to clearly define the roles and responsibilities of the different actors in the system, and to develop systems of sharing information and agree on common strategies and tactics.

An important benefit of improved coordination should be standardisation of emergency training, security audits, and disaster preparedness procedures, and the issue of common guidelines about security. Rail security standards have been slow in coming but Europeans can benefit from the US work in this field.

Taylor et. al. (2005) discuss the coupling of crime and terrorism. Given the uncertain effectiveness of anti-transit terrorism efforts, the greatest benefit of increased attention to and spending on transit security may be a reduction of criminal activity. Physical design of places can affect the likelihood of criminal activity. In the interviews Taylor et. al. (2005) describe, 80% of the respondents believed this to be a somewhat or very effective strategy in preventing terrorist attacks, ranking it alongside policing, security hardware and technology strategies.

It is also necessary to handle the conflict between security and the protection of privacy. The notion of the protection of privacy is associated with core democratic values such as civil rights and legal protection. It is concerned with the right to personal privacy and integrity, as stated in the European Convention on Civil Rights and in the EU Directive on the protection of personal data. The term

"privacy protection" is associated with the protection of personal integrity, whereas the term "data protection" connotes the protection of information of individuals being ever more important. Security checks challenge personal integrity and surveillance and registration challenges data protection rights (see Bjørnskau et.al. 2007). These are not only challenges to privacy and data protection but rather to our democratic legal tradition. Secret police with wide authority and a monopoly on information about terrorist threats is something we do not associate with democratic legal states. Thus we must ask whether actual threats can justify severe violations of privacy, data protection or legal rights.

Increased security efforts have so far been especially focused within aviation and shipping, where security has been on the agenda for a long time. It seems that the new terrorist threats have been given most attention in domains where there already existed high-profile security efforts. As of now (in the US) about 9 dollars is spent on aviation security for every cent on rail security (Kaplan 2007).

Another example of the differences in security focus in rail compared to air is the sheer number of governmental employees handling security issues. In the US about 550 persons spread across different governments (i.e. security officers rail safety inspectors) handle rail safety/security, while 45 000 government personnel are assigned to airport security (Hartong et. al. 2008). In 2004 the US federal government spent \$4.5 billion US dollars on airline safety, but only \$65 million on rail security. Homeland Security used only 2% of their "Critical Infrastructure Protection Grants" in 2006 on rail security, and those were earmarked for passenger rail (Hartong et. al. 2008).

To scale an appropriate effort for a problem that is difficult to quantify, such as terrorism, is tricky, c.f. Jenkins (2001). To find the optimal efforts for safety vs. security is also complicated. Using cost-benefit analysis would evidently not be very helpful. The risk of death from terrorism is so small and the expenditures for many measures so large, that costs would never match the economical benefits.

## 4. Results from RETRACK Security Survey

The RETRACK Security Survey is a qualitative study aiming to get experiences from different type of stakeholders engaged in rail cargo and also to pinpoint crucial problems or challenges to handle. Rather than a quantitative survey aimed at for instance describing the actual prevalence of such problems, the RETRACK survey aims to identify themes that ought to be studied more deeply in forthcoming projects as an important purpose.

In each of the five participating countries, 5-6 different questionnaires were to be answered by important stakeholders. In spite of intensive efforts to achieve this we only received 12 answers by February 2010, see Table 2.2. When we use general terms like e.g. “The ministry of Transport express...” it is thus important to remember that we only have one single representative of the stakeholders in some countries in mind, when reading.

When presenting the data in this chapter we have kept both the stakeholder and the country identification. Nevertheless we respect anonymity by not stating the name or position of the respondent.

### 4.1 Security standards and procedures

Respondents from the Ministry of Transport in the Netherlands and in Hungary both think that there is political support for security issues in their countries. In the Netherlands security issues are included in the national transport plan.

Most of the countries in RETRACK have developed national security standards concerning rail freight. In the Netherlands the specific standards for rail mainly cover dangerous goods. In Hungary the respondents perceive the situation in different ways.

*Table 4.1: Security standards in RETRACK countries. Answers on the question: Do your country have national security standards concerning rail freight? RETRACK Security Survey 2009.*

Stakeholder	Austria	Nederland	Hungary	Romania
Ministry of transport		Yes	No	
Railway Inspectorate		Yes	Yes	Yes
Terminal/railway managers				
Rail freight companies	Yes			
Police/Emergency Authorities	Yes	Yes		Yes
Customs		Yes	Don't know	

Certifications of operators as Authorised Economic Operators (AEO) has had a positive effect on customs security handling, mainly through simplification of procedures. After AEO certification fewer checks are necessary. This has speeded up the customs control to some degree. The two respondents from customs also state that their cooperation with other stakeholders (e.g. infrastructure holders, transport companies, police/emergency authorities, regional/local authorities, AEO certification authorities) engaged in rail freight security usually is good.

The police authorities were asked if they experienced any problems when cooperating with different authorities responsible for activities related to security in rail freight. In the Netherlands the police respondent reported that they had experienced some cooperation difficulties with international railway operators. These operators did not always understand the need for the security activities/measures implemented. In Romania the police reported some difficulties concerning cooperation with rail track managers, national railway operators and private security forces. One problem was that some private security forces do not respond immediately to requests from the police. There had also been some delays in the national railway operator reports to the police, and some gaps with regard to necessary technical data. The police authorities in Austria reported that there were no specific cooperation problems, but our respondent did not know if there was any problem with cooperation between the police and private security forces or with international railway operators.

## **4.2 Security assessment**

### **4.2.1 Threat assessment**

The respondents from police authorities both in the Netherlands and in Romania had conducted some kind of threat assessment for the transport sector. The threat assessments included crime-related, catastrophe-related and terrorist-related vulnerabilities. The police authorities in Austria had not conducted a threat assessment specifically for the transport sector.

### **4.2.2 Inspections - awareness**

In neither the Netherlands, Romania nor Hungary is rail freight security a specified part of the Railway Inspectorate's mandate. In the Netherlands this is only relevant regarding the RID requirements. Yearly (or more frequent) inspections are nevertheless conducted, e.g. on:

- Terminals
- Rail standards
- National and international rolling stock
- Certification systems/training systems
- Communication systems
- Monitoring systems

In the Netherlands these inspections have revealed a certain lack of awareness of security threats, and sites that could be easily accessed by intruders. In Hungary inspections of the rail infrastructure holders have revealed careless drivers at crossings, suicide by rail and thefts of cables.

## **4.3 Personnel and training**

### **4.3.1 Dedicated and trained staff**

Our one respondent from a transport company and our one respondent representing terminal managers both say that their companies have a person in charge of safety and security. The terminal management company has a specific person in charge of security. Both respondents state that key personnel receive security/emergency preparedness training. The terminal managers and the

transport companies were asked questions about their security/emergency preparedness training. The results are reported in Table 4.2.

*Table 4.2: Security Training. Answers to the question: What topics are covered in the security/emergency preparedness training? RETRACK Security Survey 2009.*

<b>Topic in emergency preparedness:</b>	<b>Austria</b>	<b>Nederland</b>
Security regulations	X	X
Company/institution procedures	X	X
Emergency procedures/evacuation routine	X	X
Hazardous material transport	X	X
First aid	X	X
Incident reporting	X	X
Explosive, chemical agent responses	X	X
Maintaining cargo integrity	X	X

The police and emergency authorities in Austria and the Netherlands have response teams specially trained to handle an emergency situation, in Romania they do not have this. In all three countries “staged scenarios” or field exercises on rail freight transport are performed yearly. In these exercises other emergency agencies also participate. Experiences from these exercises are mainly positive. One important outcome of these exercises is that more detailed information on chemicals is needed, and closer cooperation with chemical industry is desirable because of their detailed knowledge of dangerous goods handling.

### **4.3.2 Security checks of employees**

Site security is important and some studies report on employees involved in criminal activities. Of the different types of security breaks reported, tampering with the sealing of containers was most common. Trustworthiness and security awareness of the employees is thus of utmost importance.

We asked about security checks of the stakeholder’s own employees. In Austria rail companies are allowed to ask for a police report when considering new employees, so are terminal managers in the Netherlands. Independent security checks performed by authorised consultants are also used.

## **4.4 Emergency preparedness and response**

### **4.4.1 Tracking of shipments, dangerous goods**

In all the interviewed RETRACK countries it is possible to track down a specific shipment of cargo if necessary. How long it would take to locate a specific shipment varies from 1 second (terminal management in Netherland) to about 24 hours, according to the answers from our respondents.

The respondents from the Railway Inspectorates in Hungary, Romania and the Netherlands reported that it is always possible to follow the transportation of dangerous goods in their countries. They also stated that if an accident involving dangerous goods should occur, information about possible effects of these agents was available to all relevant authorities, see Table 4.3. The Ministry of Transport in the Netherlands and Hungary both state that the line of command in case of an emergency is clear in their countries. Our respondents in the police authorities and the railway company also state that information networks

(including phone numbers of contact persons) in case of a catastrophic event have been developed, and are kept up to date.

*Table 4.3: Information on dangerous goods. Answers on the question: "If an accident involving dangerous goods happens, can information on possible effects be easily accessed by the relevant authorities? RETRACK Security Survey 2009.*

Stakeholder	Austria	Nederland	Hungary	Romania
Ministry of transport		Yes	Yes	
Railway Inspectorate		Yes	Yes	Yes
Terminal/railway managers	Yes	Yes		
Rail freight companies				
Police/Emergency Authorities	Yes	Yes		Yes

Most data and information related to security threats are received either from the central authorities, the rail companies or the terminal managers, see Table 4.4.

*Table 4.4: Types and sources of security threats. Answers to the question: What kind of data do you receive, and from whom? RETRACK Security Survey 2009.*

Type of data:	Rail/terminal companies	Local authorities	Central authorities
Intelligence on possible terrorist cells			N
Terrorist threats			N
Evacuation routines/plans	N, R	N, R	R
Inf. effect on chemicals	N		R
Type of goods on the train	N, R		R
Routing of dangerous goods	N; R		R

N- Netherland, R- Romania

Information networks (including updated phone numbers) are usually also in place. In Netherland and Romania the authorities sometimes receive information on possible security threats against freight transport. In Romania more detailed information about CCTV coverage is desired. Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. Such a video monitoring and security system can be used to provide continuous traffic monitoring by the facility operator along the length of the facility. CCTV can also allow management to view and record high-risk areas to deter theft, control inventory, increase productivity and deter fraudulent

#### 4.4.2 Communication failures

The Railway Inspectorates in Romania and the Netherlands have not heard of any incidents involving "intruders" acquiring access to information they were not meant to have. In Hungary on the other hand, this has happened 2-3 times. There is no indication that this is an increasing problem in either country.

Neither the Inspectorate in the Netherlands and Romania has received any information about failures in communication systems on trains passing through their countries. The main communication problem is lack of language skills by some of the operators. In Hungary the Inspectorate states that there have been some problems; like lack of mobile phone/rail phones and some break in the security of the communication between train drivers and Traffic Management.

## 4.5 Customs control

We received questionnaires from customs in the Netherlands and Hungary. They receive information about dangerous goods, illegal drugs and illegal weapons. In Hungary the cargo manifest has to be delivered 30 minutes before border crossing, and in the Netherlands about 2 hours before the crossing.

The following criteria are important when deciding which containers to screen:

- Former experience with that specific customer
- Intelligence received from the police
- Information on which country the cargo has travelled through
- Tampered sealing on a specific container

In both countries it is possible to delay customs procedures until arrival in the hinterland (extended gateways).

## 4.6 Security incidents

### 4.6.1 Security related incidents in 2008

The respondents were asked to give an approximate number of the security incidents related to rail freight in their country (in 2008). Where the different respondents in a country have given different estimates of the number of incidents, we have used the highest number. Table 4.5 thus gives an estimate of the number of different types of incidents, and does not represent an exact overview of the situation in the different countries.

Theft and arson seem to be the most common incidents, followed by cargo tampering. Some of the countries have experienced terrorist threats, but no terrorist actions have occurred.

*Table 4.5: Prevalence of security incidents. Answers to the question: How many types of security related incidents related to rail freight occurred in your country in 2008? RETRACK Security Survey 2009.*

Type of incidents:	Nederland	Hungary	Romania
Accidents with hazmat rail	?	0	0
Smuggling	?	?	0
Terrorist attacks	0	0	0
Terrorist threats	1-10	0	1-10
Sabotage	0	0	1-10
Attacks by use of firearms	0	0	0
Theft	?	50+	50+
Use of arson	50+	?	?
Identification of explosive device	0	0	0
Hacking of computer/software system	0	0	0
Cargo tampering/destruction	?	26-50	?

### 4.6.2 Reporting incidents

The Ministry of Transport in Hungary states that security incidents are reported to Eurostat. The ministry of transport in the Netherlands does not report to Eurostat, but indicated that their Central Bureau for Statistic might do so.

In Hungary and Romania the Railway Inspectorate receives reports from infrastructure managers and transport companies on security incidents. The Inspectorate in the Netherlands does not receive this kind of information.

## 4.7 Security challenges

### 4.7.1 Main weaknesses

Most of the respondents are satisfied with security regulations, the security of the IT-systems, emergency preparedness and security training of personnel in their country. They do not define these items as weaknesses of the freight security system. The main weaknesses seem to be border control, site security, security checks and communication between different authorities, see Figure 4.1. Half of the respondents state that knowledge about security and possible threats are somewhat limited.

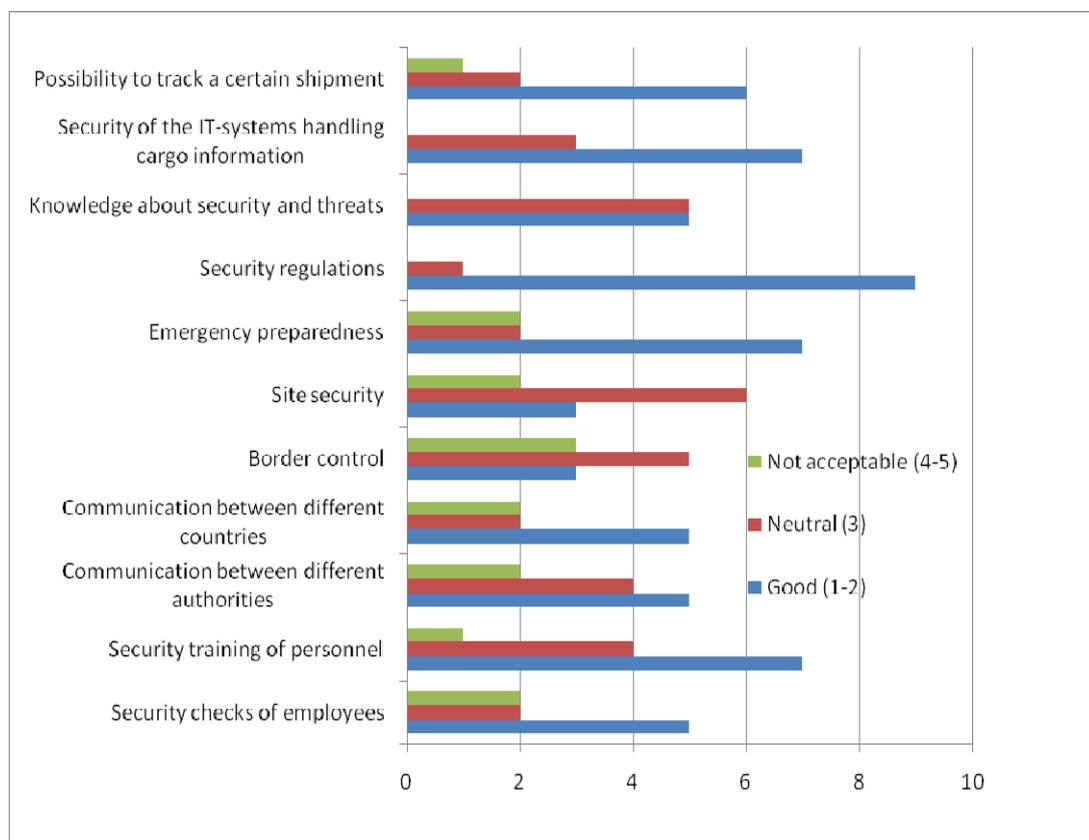


Figure 4.1: Evaluation of the weaknesses of different elements in the rail security system. Absolute numbers. RETRACK Security Survey 2009.

Even if most of our respondents do not regard IT-security as a main weakness, all three of our respondents from the police authorities grade this as a 3 on the 5-point scale. The police authorities also grade security training of personnel the same. Details on answers from countries and type of stakeholders are given in Table 4.6.

Table 4.6: Answers to the question: What is the main weakness in the freight security system? From different stakeholders in RETRACK countries. Graded from 1-5, were 1 is very good and 5 is not acceptable. RETRACK Security Survey 2009.

Weaknesses	1-2	3	4-5
Security checks of employees	A <sup>5</sup> , H <sup>2</sup> , N <sup>1</sup> , R <sup>2,4</sup>	A <sup>4</sup> , N <sup>3</sup>	H <sup>6</sup> , N <sup>4</sup>
Security training of personnel	A <sup>5</sup> , H <sup>2</sup> , N <sup>1,3,6</sup> , R <sup>2</sup>	A <sup>4</sup> , H <sup>6</sup> , N <sup>4</sup> , R <sup>4</sup>	H <sup>1</sup>
Communication between diff. authorities	A <sup>4</sup> , H <sup>2,6</sup> , N <sup>1</sup> , R <sup>2</sup>	N <sup>3,4,6</sup> , R <sup>4</sup>	A <sup>5</sup> , H <sup>1</sup>
Communication between diff. countries	H <sup>6</sup> , N <sup>1,3</sup> , R <sup>2,4</sup>	A <sup>4</sup> , H <sup>2</sup>	A <sup>5</sup> , N <sup>4</sup>
Border control	A <sup>4</sup> , H <sup>2</sup> , R <sup>2</sup>	A <sup>5</sup> , N <sup>4,6</sup> , H <sup>1,6</sup>	N <sup>1,3</sup> , R <sup>4</sup>
Site security	H <sup>1</sup> , N <sup>1,3</sup>	A <sup>5</sup> , H <sup>2,6</sup> , N <sup>6</sup> , R <sup>2,4</sup>	A <sup>4</sup> , N <sup>4</sup>
Emergency preparedness	A <sup>4,5</sup> , H <sup>2,6</sup> , N <sup>1,3,4</sup>	R <sup>2,4</sup>	H <sup>1</sup> , N <sup>6</sup>
Security regulations	A <sup>4,5</sup> , H <sup>2,6</sup> , N <sup>1,3,4</sup> , R <sup>2,4</sup>	H <sup>1</sup>	
Knowledge about security and possible threats	A <sup>4</sup> , H <sup>2,6</sup> , N <sup>1,3</sup>	A <sup>5</sup> , N <sup>4</sup> , H <sup>1</sup> , R <sup>2,4</sup>	
Security of the IT-systems handling cargo info	A <sup>5</sup> , H <sup>2,6</sup> , N <sup>1,3,6</sup> , R <sup>2</sup>	A <sup>4</sup> , N <sup>4</sup> , R <sup>4</sup>	
Possibility to track a certain shipment	A <sup>4</sup> , H <sup>2,6</sup> , N <sup>4</sup> , R <sup>2,4</sup>	A <sup>5</sup> , N <sup>3</sup>	N <sup>6</sup>

A -Austria, N- Netherland, H- Hungary, R- Romania

1- Ministry, 2- Inspectorate, 3- Terminal management, 4- Police , 5, Transport companies, 6- Customs

#### 4.7.2 Vulnerable links in the chain

The respondents were also asked to grade the vulnerability of different links in the freight transport system. Looking at all respondents together, it seems that bridges and tunnels as well as transport on the tracks are regarded as rather solid elements in the rail freight system. On the other hand we find that station areas and loading and unloading activities are vulnerable elements, see Figure 4.2 and table 4.7.

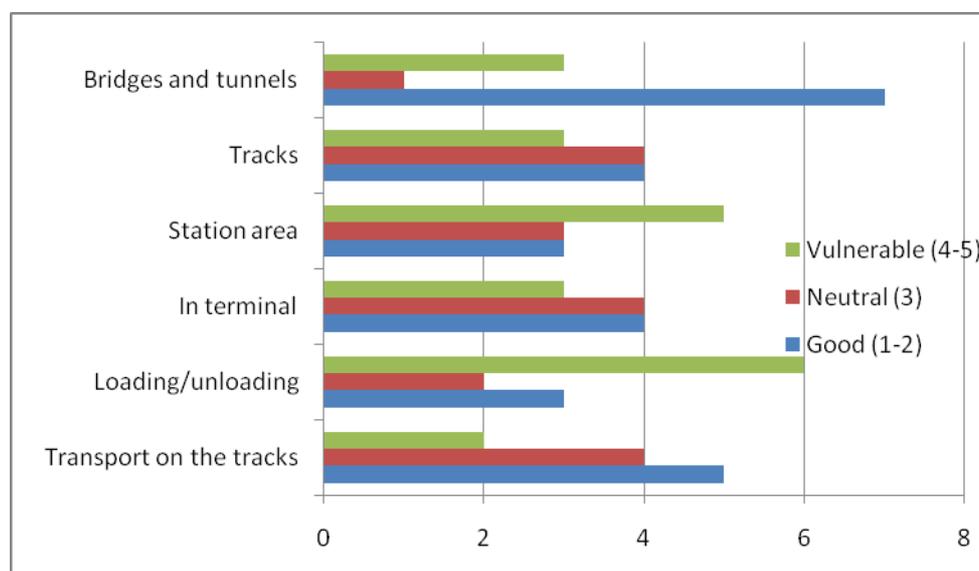


Figure 4.2: Degree of vulnerability of different links in the rail freight transport system. Absolute numbers. RETRACK Security Survey 2009.

The respondents in the different countries and in the different institutions do not agree on which link in the transport system that is most vulnerable. All the Austrian and Hungarian respondents agree that the cargo is vulnerable during unloading and loading, and that bridges and tunnels are quite secure. For answers from different stakeholders and countries see Table 4.7.

Table 4.7: Answers to the question: What is the vulnerability of different links in the freight transport system. Graded from 1-5, were 1 is very safe/secure and 5 is very vulnerable. RETRACK Security Survey 2009.

Links in the freight	Degree of security -vulnerability		
Transport system	1-2 very secure	3	4-5 very vulnerable
Transport on the tracks	A <sup>5</sup> , H <sup>1,6</sup> , N <sup>3,6</sup>	A <sup>4</sup> , N <sup>1</sup> , R <sup>2,4</sup>	H <sup>2</sup> , N <sup>4</sup>
Loading/unloading	N <sup>3,4,6</sup>	N <sup>1</sup> , R <sup>4</sup>	A <sup>4,5</sup> , H <sup>1,2,6</sup> , R <sup>2</sup>
In terminal	H <sup>2</sup> , N <sup>3,4,6</sup>	A <sup>4,5</sup> , H <sup>6</sup> , N <sup>1</sup>	H <sup>1</sup> , R <sup>2,4</sup>
Station area	H <sup>6</sup> , N <sup>3</sup> , R <sup>4</sup>	A <sup>4,5</sup> , N <sup>1</sup>	H <sup>1,2</sup> , N <sup>4,6</sup> , R <sup>2</sup>
Tracks	A <sup>4</sup> , H <sup>1,6</sup> , N <sup>3</sup>	A <sup>5</sup> , N <sup>1,6</sup> , R <sup>4</sup>	H <sup>2</sup> , N <sup>4</sup> , R <sup>2</sup>
Bridges and tunnels	A <sup>4,5</sup> , H <sup>1,2,6</sup> , N <sup>3</sup> , R <sup>2</sup>	N <sup>1</sup>	N <sup>4,6</sup> , R <sup>4</sup>

A- Austria, N- Netherland, H- Hungary, R- Romania

1- Ministry, 2- Inspectorate, 3- Terminal management, 4- Police , 5 - Transport companies, 6- Customs

## 4.8 Security measures with most potential

The respondents were also asked to mention the security measures with the most potential in their country, and internationally. It is obvious that the role of the respondent strongly influences their view on what could be an effective security measure, see table 4.8.

Table 4.8: Security measures with potential for increasing security. Answers to the question: Which security measures have most potential, nationally and internationally? Different stakeholders in RETRACK countries. RETRACK Security Survey 2009.

	Nationally	Internationally
Austria	<b>Transport Company:</b> Improvement of site and shunting yard security – infrastructure and manpower	<b>Transport company:</b> Stricter regulations and control of maintenance of railway cars
Netherland	<b>Ministry:</b> Better training of personnel, awareness training, CCTV <b>Terminal management:</b> Obligatory certificate for train drivers carrying dangerous goods, improvement of hand-over routines at borders, storage systems depending on type of dangerous goods <b>Police:</b> Dedicated freight lines <b>Transport Company:</b> Numbering of the containers should be obligatory, electronic systems, GPS	<b>Police:</b> Dedicated freight lines <b>Customs:</b> Smart systems – electronic system used to follow shipment from start to finish
Hungary	<b>Ministry:</b> Scaling of every wagon, operate independent security board <b>Customs:</b> Getting info. on the containers more than 30 min before arrival, info. on type of goods carried in the containers, info. on previous controls of container	<b>Ministry:</b> Scaling of every wagon, operate independent security board
Romania	<b>Police:</b> Implementation of CCTV systems, increased security training, increased number of security personnel	<b>Police:</b> Improving cross-border communication, more detailed security checks at borders

## **4.9 Concluding remarks**

None of our respondents know of any terrorist attack against freight rail in their country, but some terrorist threats had been received. Some of the countries had also experienced accidents involving dangerous goods. Of the incidents experienced in 2008, arson and theft are most common. This is line with other studies, cf. chapter 3.

To prevent possible future threats increased focus on security is desired. Increased number of security personnel, improved training of personnel, stricter regulation of rail carriage design, increased use of CCTV and GPS tracking of cargo are some of the main security measures recommended by our respondents.

Due to the low response rate, drawing any major conclusion based on the results presented here is not recommended. But it is possible to compare our results with those from other sources, and consider any common findings.

## 5. Elements in a common security strategy

A key aim of RETRACK WP7 was to give recommendations on a possible common security strategy. We do not find that the material collected forms the basis for strong security recommendations. This is especially so since the partners, due to the more pressing market challenges, did not fulfill the requirements of their part of WP7 i.e. both from interviewing others and from answering a questionnaire for their own enterprise or organisation. But the material from WP7 might all the same be fruitful as a basis for discussion among RETRACK partners and others, and thus contribute to the main purpose of enhancing security consciousness.

In this chapter we present some theoretical or reflective baselines for risk management thinking and discuss the special challenges of cross-border rail freight. We also discuss security as a research theme in the Community and present the potential of different measures as seen by respondents of the RETRACK Security Survey and the strategic conclusions on security from WP2.

### 5.1 Baselines for risk management

#### 5.1.1 A model for understanding accidents

Any strategy needs to be based on a model explaining the possible development of an undesired incident. Only a few undesired incidents result in accidents. (In 2003 the Norwegian Accidents Investigation Board investigated 145 unwanted events in air transport. Just 23 of these events were accidents, and only 10 of these were categorised as serious accidents (Accident Investigation Board Norway (AIBN) 2004). The key questions then are:

- What conditions cause an incident to develop into an accident and what can be done to prevent such a development?
- What conditions cause accidents develop into major accidents or catastrophes with large and widespread consequences and vice versa what can be done to prevent such an outcome?

Jersin (2004) discusses a model where one presupposes that safety or security barriers or defences can break off the process at every point of the event chain. Such defences can be technical, human or organisational. Defences can be measures that prevent deviances from a normal situation occurring, warn about deviances when they have occurred, correct deviances before they lead to severe consequences and finally limit the consequences after the undesired incident is a fact.

Both direct and indirect causes of accidents and their consequences are influenced by certain characteristics of the system in which they occur, such as:

- Large energy concentrations
- High energy speed
- Many vulnerable objects
- Lack of in-depth defence (few defences and low redundancy)
- Small tolerance for deviance and faults(cf. the concept of resilience)
- "Close couplings" (high interdependence)
- Causal circumstances of bad luck.

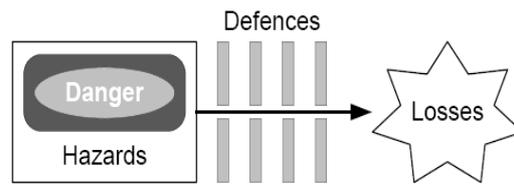


Figure 5.1: Connection between danger, defences and losses - a principle model of the event chain. Source: Jersin 2004.

The fact that some activities in today’s society take place in systems that make accidents inevitable led Perrow (1984) to launch the concept of “normal accidents”. Accidents will often take place in systems with high complexity, i.e. with many components and parts. Interactive feedback loops and closely connected couplings can make it difficult to discover and diagnose abnormal situations and to separate defences as well as to improvise solutions. These are definitely characteristics that could well describe security challenges for RETRACK and other rail freight cross border transport.

### 5.1.2 A system perspective

With many different causes at different levels a system perspective is necessary. A security strategy must encompass all elements in the rail freight system as well as its environment, i.e must encompass many different aspects: societal, organisational, economical, cultural and technical. This is called an MTO (Man Technique, Organisation) perspective. Elements in a risk management strategy are shown in Figure 5.2.



Figure 5.2: Elements in a risk managing strategy. Source: US Department of Homeland security 2006.

While technological innovation is necessary to tackle most safety and security problems it is not in itself sufficient. Even the most sophisticated technology will not solve the problem if the organisation lacks the necessary focus and mechanisms or if the actors on different levels are not motivated or concerned. Individual market players – consumers and businesses – must be motivated to stress safety and security questions and to find and eliminate barriers to the implementation of efficient measures.

A system approach could be defined like this “*The application of operating, technical, and management techniques and principles to the security of a facility throughout its life to reduce threats and vulnerabilities to the most practical level through the most effective use of available resources*” (DOT 1999).

### **5.1.3 Anticipation and Resilience**

When discussing a system perspective it is also necessary to discuss the balance between anticipation and resilience.

Anticipation is a mode of control where efforts are made to predict and prevent potential dangers before damage is done, while resilience is the capacity to cope with unanticipated dangers after they have been manifest, and learning to respond. Anticipation attempts to avoid hypothetical hazards, while resilience is concerned with those that have been realised (Wildavsky 2004, Nævestad 2010).

For a considerable number of uncertain situations, resilience is the preferable strategy. But for a substantial number of situations, anticipation (protecting the system against predictable forms of failure) seems more sensible (Wildavsky 2004). If the most serious risks come from unpredictable or low-probability sources, resilience is best. If danger on the other hand comes from reliable foreseeable sources, then anticipation is the best. The best way to secure a system is usually a combination of anticipation and resilience.

### **5.1.4 Strategies at different levels**

Railways (and other land based mass transit) are easy targets, thus some argue that the best way to stop a terrorist attack is to stop the terrorist before they want to and before they can strike (proactive focus). There are two - or maybe three - main strategies for security against terrorist acts. The responsible stakeholders for these strategies will be found on different levels;

1. Try to secure threatened objects and thus deter or prevent terrorist attacks.  
Level: *Transport sector*.
2. Securing against terrorist attacks by way of police methods such as surveillance of potential terrorist groups.  
Level: *Cooperation transport -governmental agencies*.
3. Policy actions that will decrease international conflicts that nurture terrorism.  
Level: *International*.

The first one is the main principle in aviation, where all persons and all luggage must pass strict security checks in order to make sure that illegal and potentially harmful objects are not brought onboard planes. This strategy is very restrictive, and so not as fit for an open transport system like rail as it is for aviation. The aim

of the second strategy is to take action against potential terrorists before they are able to attack. Such a strategy is more general than securing specific objects, and is not the responsibility for the railway stakeholders, even if they can contribute. Still more general is the third strategy mentioned.

For a better understanding of terrorist thinking and the complex reflections on cost/benefit of security see for instance papers from the Norwegian Coping with New Risks project (Ahktar, Bjørnskau and Veisten 2010 and Meyer 2010).

## 5.2 Special challenges for rail freight security efforts

### 5.2.1 Rail as an open system

Open access makes most land-based mass transit vulnerable to attack and difficult to secure. Railways (and other land-based forms of mass transit) are easy targets, so some argue that the best way to stop a terrorist attack is to stop the terrorists before they can strike (proactive focus). A rail system cannot be "closed". This is probably the nr. 1 challenge, illustrated by the following DGTREN Statement: *"The transport chain is only as secure as its weakest link"* (European Commission 2003).

A huge amount of hazardous materials are transported by rail each year – raising concerns about terrorist attacks. There are many different locations or arenas to focus on in rail freight; production areas, terminals, borders, tracks, urban agglomerations passed, personnel areas. Key questions in strategy formulation are;

- Where can threats be produced and where will they do most harm?
- Which areas are open and where can they most easily be closed?

Figure 5.3, though showing public transport and not freight, illustrate the difference between a closed and an open transport system.

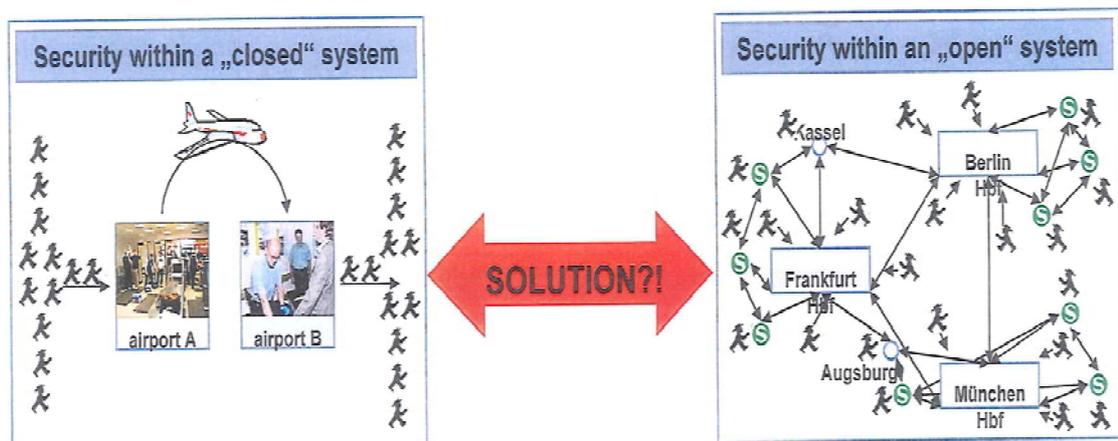


Figure 5.3 Security in closed vs. open systems – an illustration. Source: Puls, Deutsche Bahn AG, 2009.

A recent study in Norway documents that the differences between transport modes probably strongly influence the efforts used in security strategies (Bjørnskau et. al. 2007). E.g. urban mass transport has so many passengers, departures and stops/stations that it is practically impossible to adopt an aviation-style security regime. Aviation is characterised by centralised point-to-point traffic, where airports are placed outside of central junctions and thus much easier to secure physically than, for instance, railways and underground systems. Road traffic is characterised by open access and it is almost impossible to imagine security checks and control of access to the road system as a whole. Exceptions might be toll roads.

### **5.2.2 Cross-border security planning involves many stakeholders**

Transport systems are designed for accessibility and efficiency factors that make them highly vulnerable to terrorist attacks. To reduce risk/consequence one needs strategies and measures for emergency planning, vulnerability assessment, emergency response training of general personnel, medical emergency personnel, communication equipment and procedures and safety equipment. In addition it is necessary to increase the number of security personnel, video surveillance equipment in vehicles and on stations/terminals as well as random inspections with sniffer dogs.

RETRACK is a cross-border project aiming at “one single rail” in the corridor at stake. Such a cross-border concept must include work across;

- Nations
- Authorities
- Levels in the political system
- Transport modes
- Private/public stakeholders
- Transport and other parts of society

The large number of stakeholders involved evidently implies communication challenges and risks of duplications and confusion.

### **5.2.3 Coupling to other factors – conflict or synergy?**

Designing security programs for rail freight is not a sector specific activity with tight borders. On the contrary, several other factors and possible couplings must be taken into account, like;

- The psychology of terrorism, the value of feeling safe, the willingness to pay for risk-mitigating measures
- The possibility to integrate plans for criminal and terrorism prevention
- The possibility to integrate plans for safety and security
- Possible conflicts between our everyday life and security regimes
- Possible conflicts between economic goals and security work.

There are huge differences in risk acceptance between transport modes. Aviation deviates from the other modes in its very low level of risk acceptance and consequently high security costs. Bjørnskau (et. al. 2007) argues that safety for society as a whole would increase if resources were transferred from security measures in aviation to ordinary safety measures in road traffic. The same

complicated balance between willingness to pay for measures would probably be found between terrorist attacks and “normal” accidents.

The coupling between criminality and terrorism, and the options for a combined design for avoiding both threats is relevant for other stakeholders in the railway sector than those focused on in RETRACK, for instance the infrastructure, terminal and station managers. Situational crime prevention can be applied in this part of the transport chain. Situational crime prevention seeks to change the immediate environment, such that potential offenders perceive the opportunities as reduced and the risk as increased, and thus might decide against committing the specific crime (Clarke 1983). The situational crime prevention framework consists of 25 techniques organised into five main approaches for changing the decision-making process of the would-be offender (Clarke and Newman 2006). See Taylor et. al. (2005) and Smith and Cornish (2006) for detailed descriptions of applying situational crime prevention to public transportation.

It is also necessary to look for possible synergies between safety and security strategies to ensure an optimal use of resources. In both areas one needs three types of strategies, c.f. figure 5.1.

- Active - proactive strategies to eliminate risks as much as possible
- Passive - reactive strategies and defences to limit consequences of out-of-control situations
- Emergency preparedness to handle the situation and to reduce consequences

There will normally be larger differences between safety and security concerning the first two strategies, while the emergency handling will be the same.

A related aspect concerns the level of integration of the transport system with society and everyday life. Tram lines with frequent departures in Oslo are called “rolling pavements”, which illustrates how trams (and buses/underground) are perceived as an integrated part of city life. A massive security check of passengers would be perceived as incompatible with a vital city life.

And finally we have the couplings between economy, effectiveness and security work. The transition to “just in time” deliveries make security more important than ever. This requires a streamlined and effective control system, so that the goods are hindered as little as possible on their way to the receiver. There needs to be a proper balance between free flow of goods and security (Hamberger 2007), especially in the light of the competition between rail and truck/ship for the cargo transport. International requirements for increased security measures on rail transport might lead to a distortion of competition in favour of road transport. Environmentally speaking this may not be the best alternative.

#### **5.2.4 Cross modality and risk migration**

A special challenge for transport risk reducing strategies is the fact that both risk and transport migrates from one mode to another, cf. Grunnan et. al. (2008). Risk perception can move customers and passengers from one transport mode to another. Risk countermeasures can move terrorists or criminals activities from one arena to another.

A cross-modal policy involving the coordinated development of security and safety measures can help to reduce those unforeseen consequences inherent in traditional sector focused politics. Security measures developed with an intra-

modal focus, while intended to prevent accidents and potential incidents, may merely result in the migration of both risk factors and traffic to other modes. Vulnerability to new and old risks, cross-modal dependencies, and the challenges associated with New Public Management are further arguments for the cross-modal management of safety and security.

Achieving improved cross-modal security and safety includes stronger forms of governing through the use of uniform inspections, a stronger focus on safety and security in the management of subordinate agencies, and the establishment of a cross-modal working group. This is not only a recommendation for authorities, but might as well be a model for business partners, like the RETRACK consortium.

The threats of transit terrorism are probably not universal; most attacks in the developed world have been on the largest systems in the largest cities. But the risk might move down the system if security increases on the main lines/cities. The asymmetry of transit terrorist risk is at odds with a political system of public finance that favours distributing funding somewhat equally across jurisdictions.

### **5.2.5 Basic security principles for rail freight**

To sum up this short discussion of basic elements in a security strategy, we can use principles set up by Jenkins (2001). Slightly reformulated for RETRACK or other rail freight services they could be like this:

- Security cannot prevent terrorist attacks, but might influence terrorists to choose less "lucrative" or more feasible targets.
- Security must have two main goals; preventing casualties and reducing unnecessary shutdowns or disruptions influencing the economy and the market.
- Potential casualties can be reduced through the design of terminals, trains and containers and through effective and rapid response.
- Disruptions can be minimised with technologies and procedures that permit accurate diagnosis and rapid, well-rehearsed responses.

## **5.3 Regulations and feedback processes**

Cross-border freight will no doubt benefit from international cross-country regulations, national support systems, and feedback loops. We will give some examples.

### **5.3.1 The EU safety directive – a baseline**

The EU Safety Directive (European Commission 2004/49/EC) is evidently an important baseline for security planning in RETRACK. Article 4 demands that member states shall:

- Ensure that railway *safety* is generally maintained.
- Give priority to the prevention of serious accidents.
- Ensure that safety rules are laid down, applied and enforced in an open and non-discriminatory manner.
- Foster the development of a single European rail transport system.
- Take account of the need for a *system-based approach*.

- Ensure the *safe operation* of the railway system, and establish safety management systems.

There is a move towards mutual recognition and towards European harmonisation of the railway system, which is in fact RETRACK's starting point. The main security focus concerning freight rail transport in Europe is the transportation of dangerous goods. Tracking the goods, prevention of accidents, and knowledge on handling of different hazmat to reduce the threat to people and the environment has received most attention

### 5.3.2 National support and feedback loops

In the US they work with an extensive security planning system aimed at supporting all sectors in society (Homeland security 2006, 2007) with instructive descriptions of systems, actions and a logic process. Figure 5.4 shows the crucial steps in risk management as a continuous procedure.

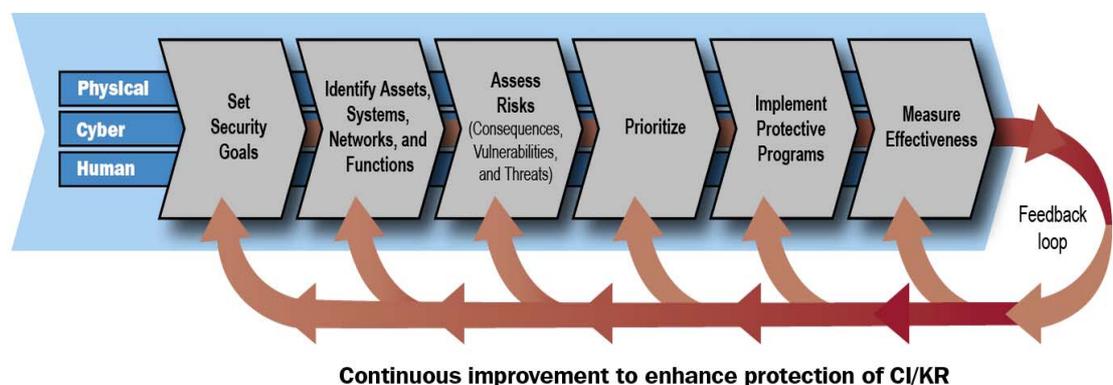


Figure 5.4: The US National Risk Management Framework. Source: US Dep. of Homeland security 2006.

In their proposed *Rail and public transportation security act of 2007*, (which did not pass into law), many strategic actions and measures of general interest were listed. Some examples from the documents connected to the proposed act are listed in RETRACK D.7.1 (Kolbenstvedt and Amundsen 2008) and table 5.1.

Homeland security and the House of representatives (transport committee) state that the main security challenges in freight rail transport in the USA are: possible threats including hazardous materials attacks (such as breaking a THI-tank), destruction or sabotage of freight rail bridges and tunnels, and cyber-attacks to the rail system that could disrupt or cause the degradation of railroad signalling and dispatching systems (Thompson et. al. 2009).

One other important challenge is for the federal agencies to find ways to protect the transport systems from potential terrorist attacks without compromising the accessibility and efficiency of rail (US Homeland security 2007b). The sheer numbers of shareholders involved can sometimes lead to communication challenges, duplication of efforts, and confusion about roles and responsibilities.

Technology improvements such as designing stronger tank cars, development of more real-time rail carriage tracking and monitoring systems (installing GPS on tank cars and track cars from origin to destination), and substituting highly

hazardous materials with less dangerous chemicals are American suggestions to some of the main challenges (Thompson et. al. 2009).

One of the United Nations (2010) Task Force on Rail Security's most prioritized activities now is to harmonise requirements concerning international railway transport.

*Table 5.1: Strategic actions and measures in Risk Management and National measures to support other stakeholders. Examples from the proposed US Rail and public transportation security act of 2007.*

Type of element and level	Examples
Standards	National standards for testing and use of technologies to improve security
Organisation, personnel	Establish a national preparedness consortium
	Establish a task force to review lists of crimes that disqualify individuals from certain transport-related employment.
	Establish protection response teams
Threat assessments	Increase number of security inspectors with at least 600 by 2010
	Train at least 100 extra dog teams per years.
	Carry out threat assessment screening programmes
	Threat assessment screening for transportation employees
Knowledge exchange	Evaluate prototype systems to detect nuclear or radiological materials on rail.
	Screening of in-bound rail shipment to the US for terrorist weapons of mass destruction
	Look at the possibilities of screening all cargo at international borders – implement alternative procedures to screen cargo where 100% screening is not possible
Protective programs	Conduct study on foreign rail security practices
	Assess likely methods of deliberate attacks against rail tank cars used to transport toxic-inhalation-hazard materials
	Develop an information sharing plan
Enhanced security measures for certain sensitive materials	Develop security training programmes, security exercises.
	Set forth civil penalties for violations of regulation and orders
	Enhanced security measures for certain sensitive materials

## 5.4 Security research – a field of growing importance

Our literature review from 2008 (cf. D.7.1) clearly demonstrated that, for the time being, we can find many lists and descriptions of strategic elements in rail freight security planning, but not so many scientific evaluations of best practices and their actual results. But, luckily enough, the situation is changing. In recent years the Community has strongly focused on this field with the result that Security is a theme in its own right in the 7<sup>th</sup> Framework Programme.

Here we will present some elements from work on the European Security Research showing that Security is given growing importance in Europe. We also present main research findings from Retrack WP2 (Dellinger and Kotsikos 2008) and from WP7 related to strategy measures.

### 5.4.1 Meeting the Challenge – a research agenda

In 2004 the European Parliament decided to establish a European Security Research Advisory Board, ESRAB. It was stated that this Board should draw the

strategic lines for European Security research and advise on security in the 7<sup>th</sup> Framework Programme. ESRAB presented their Agenda in 2006 (ESRAB 2006). The agenda was based on the contributions from 300 people, showing the complexity of the theme. ESRAB recommends three research paths;

1. Capability building
2. System development through integrated projects
3. Systems-of-systems demonstrations
  - a. Aftermath crisis management systems
  - b. European-wide integrated border control system
  - c. Logistic and supply chain security
  - d. Security of mass transportation
  - e. Integrated approach for CBRNE treatment

From a RETRACK perspective it is interesting to note that all the paths fit the RETRACK objectives or way of thinking, and that the demonstration programmes recommended, contain themes of evident importance for cross-border rail freight. At the same time the research agenda recognises that to enter many security techniques and strategies into service, numerous interrelated but independent systems and stakeholders must be connected. This is an argument for demonstrations especially focusing on security, and not handled as a small part of demonstrations with other main objectives.

Accordingly the EU established Security as a theme in its own right in the 7<sup>th</sup> Framework Programme. In CORDIS (database of EUs Framework Programmes) we can now find at least 14 research projects started in 2008 or 2009 that might influence rail transport security issues. Not all of the projects are rail-specific. Some of the results from these projects can be useful for further mapping of security challenges in European rail freight transport, and experiences of best practices for handling these issues. RETRACK has not given room for further literature studies, and the results from the FP-projects on security are not at hand yet. The projects are listed in Appendix I.

#### **5.4.2 Main findings on security from RETRACK WP 2**

The state-of-the-art study on Safety and Security of RETRACK WP2 concluded that rail transport security faces new threats from international terrorism which are not well defined. Nevertheless new rail freight service launching makes it mandatory, via an integrated approach, to address current security threats and to assess social as well as economic consequences. While providing reliable, cost-effective tools in assessing, preventing and combating the novel threats of international terrorism, different framework conditions and regional disparities have to be regarded. For further details see RETRACK D.2.4.

Some important recommendations from RETRACK WP2 (Dellinger and Kotsikos 2008) are that;

- The safety and security system should *identify terrorist and other threats and consequences* to new rail freight and promote threat-cost-benefit optimised solutions. The issues of cargo tampering, people and contraband smuggling and terrorism need to be assessed, and solutions evaluated based on a realistic freight “Risk” assessment associated with transport mode and local threat scenarios.
- There should be a *focus on border points* as high risk - with delay and train vulnerability exposed on a routine basis. Tracking of cargoes,

sensors to notify the operators of intrusion and performance of cargo control and protection must be evaluated to ensure security without harming the fluidity, productivity and cost-effectiveness of transport chain activities,.

- *An integrated approach* is necessary, i.e. linkage to all involved national bodies (customs, immigration, and security). The security is dependent on efficient cooperation and coordination among Public Authorities (in charge of threat identification), between countries concerned with the new service, the EU Institutions and the relevant stakeholders.
- There is a need to accept inspection and *cooperation beyond national borders* as well as driver integrity checks and access to trains. The priorities have changed from monitoring cross-border cargo and reducing international shipments of contraband, to *screening* for explosives, arms, dirty bombs and weapons of mass destruction.
- *The exchange of information should be enhanced*, disseminating best practices, establishing coordination mechanisms and taking joint actions on particular issues are important strategies.
- *Security checks etc. must be balanced against the transit freight system economy*. Security is expensive but this can be a product “plus” point, supporting the industries and transport operators' competitiveness. The challenge is rapid detection without disrupting the daily flow of goods.

A lot has already been achieved concerning the security of dangerous substances (HCDG like explosives, radioactive products, etc) both within Member States and at EU level. It is clear however that more can be done. The issues of cargo tampering, people and contraband smuggling and terrorism need to be assessed and solutions evaluated based on a realistic freight “Risk” assessment associated to « transport mode » and local threat scenarios.

#### **5.4.3 Findings on strategy from RETRACK Security Survey, WP 7.2**

The RETRACK Security Survey, cf. chapter 4, shows that security regulations, the security of IT-systems and security training of personnel are regarded as satisfactory by the respondents. The main weaknesses of the rail freight security system seem to be border control, security checks and communication between different authorities as well as different countries. Most respondents state that knowledge and awareness about security and possible threats are somewhat limited. Bridges and tunnels as well as transport on the tracks are regarded as rather solid elements in the rail freight system. On the other hand station areas and loading and unloading are vulnerable elements.

The respondents also listed which security measures they thought had the largest potential for increasing security nationally and internationally. The answers are shown in Table 5.3.

These suggestions are very much alike the best practices found in Hecker (2006), an overview of foreign security practices that was performed as a part of the US security effort. Some additional points from Heckers review might be:

- Increase the number and visibility of security personnel
- Employee training (e.g. using the HOT method, looking for packages that are Hidden, Obviously suspicious and not Typical of the environment)
- Design of infrastructure terminals and shunting yards
- Covert testing (training personnel on “staged events”)
- Overview of “best practices”

Table 5.3: Answers to the question: Which security measures have most potential, nationally and internationally? Type of stakeholder is given before the answer. RETRACK Security Survey 2009.

Stakeholder	Nationally	Internationally
<b>Transport company:</b>	Improvement of site and shunting yard security, infrastructure and manpower Numbering of the containers should be obligatory Electronic systems, GPS	Stricter regulations and control of maintenance of railway cars
<b>Ministry:</b>	Better training of personnel Awareness training, CCTV Scaling of every wagon Operate independent security board	Scaling of every wagon Operate independent security board
<b>Terminal management:</b>	Obligatory certificate for train drivers carrying dangerous goods, Improvement of hand-over routines at borders, Storage systems depending on type of dangerous goods	
<b>Police:</b>	Dedicated freight lines Implementation of CCTV systems Increased security training Increased number of security personnel	Dedicated freight lines Improving cross-border communication More detailed security checks at borders
<b>Customs:</b>	Getting information on the containers more than 30 min before arrival Information on type of goods carried in the containers Information on previous controls of container	Smart systems – electronic system used to follow shipment from start to endpoint

#### 5.4.4 The need of a research road map

Another European security research initiative is the European Security Research and Innovation Forum (ESRIF). They delivered their final report in December 2009. For two years the 64 members of the forum and 600 experts have analysed the present and long-term overall security challenges that the EU faces. The challenges range from natural disasters to major man-made incidents, from small-scale to those with potential mass disruption effects (ESRIF 2009).

One of the main findings is that to reach an interoperable, trust-embedded and resilient society, the EU needs a research and development roadmap. Consequently a European security research and innovation agenda has been defined.

Recommended research topics are (ESRIF 2009):

- Security cycle preventing, protecting, preparing, responding and recovering
- Countering of different means of attacks (detect and identify possible attacks/incidents etc)

- Securing critical assets (critical infrastructure, energy, water supplies etc.)
- Securing identity, access and movement of people and goods (border security, secure identity management)
- Cross-cutting enablers – the crucial role of information and communication technologies

Effective security must embrace interoperability, standardisation, certification, validation and communication with the public, education and training, exchange of best practices and consultations on privacy issues (ESRIF 2009).

Several of the above mentioned aspects are included in the objectives of the RETRACK security study. Due to different confounding problems one can question whether RETRACK will give good knowledge on these topics. Nevertheless they are still very relevant for further research planning.

## 6 Conclusions for RETRACK

In this chapter we sum up RETRACK WP7 by defining the core challenges for RETRACK, suggesting some security actions for the project and finally discuss the experience of security research in the RETRACK setting.

### 6.1 RETRACK must cope with general challenges

RETRACK as well as any other rail freight business must cope with – at least - three core security challenges, being:

1. Rail business being an open activity
2. The tricky balance between enormous consequences and few incentives.
3. Security strategies in rail freight cannot prevent terrorist attacks

Rail business is an open activity with good accessibility for the customers – both for cargo and public mass transport. The track as well as stations and terminals are often located near to important societal functions such as city centers, industrial concentrations and the like. It is probably difficult and not preferable to change the open character since accessibility is a key competitive advantage for rail transport.

With regards to the second point, few deviances in rail freight result in accidents. In addition “normal accidents” are responsible for more fatalities than terrorist attacks and other security problems. This is an enormous challenge when it comes to developing security consciousness and obtaining the resources for security work. To prevent risk, i.e. the probability multiplied by the consequences, one must define and identify risk drivers. Drivers increasing probability are that rail is an open system and that the system has many vulnerable links. Drivers giving large consequences are the large amounts of energy involved, that hazardous materials are transported, and that terrorist attacks difficult to foresee. The consequences from thefts, cargo tampering and vandalism are smaller.

The third point refers to the fact that it is necessary to engage in security strategies on several levels:

- *Transport sector responsibility:* Secure threatened objects, vulnerable areas. Control employees and goods.
- *Cooperation in transport - governmental agencies:* Ensure surveillance of potential terrorist groups.
- *International cooperation:* Develop policy to decrease international conflicts that pave the way for terrorism.

A single rail freight operation or transport company can evidently not handle security alone, especially not when operating across borders. They must rely on and cooperate with a lot of authorities and private stakeholders, both external and internal, national and international. But everyone can and must contribute and take responsibility for their part of the security work. Let's look at the RETRACK consortium and the RETRACK pilot. What could be done at this level?

### 6.2 Security actions for the RETRACK project

RETRACK is a pilot study meant to present an economic sustainable model for organization of other innovative crosscountry rail freight lines in Europa as well as

for extensions from Europe. With respect to security RETRACK gives some knowledge of qualities and vulnerabilities of elements in rail freight strategies in their country. Table 6.1 present an overall picture for RETRACK, and also some possible actions for the stakeholders. Details are given in chapter 4, see for instance figure 4.1 and 4.2.

*Table 6.1: Security qualities and challenges for RETRACK countries and possible security actions and measures . RETRACK Security Survey 2009.*

<b>Area of security</b>	<b>Quality today</b>	<b>Challenges</b>	<b>Possible actions for RETRACK</b>
The prevalence of security standards and security plans	<i>All RETRACK countries have standards.  AEO has had very good effects</i>	<i>All countries allng the corridor have not made special threat assessments for Transport in their national security plans.</i>	<i>Advise national authorities on the importance of such sector assessments.  Suggest special certificates for train drivers carrying hazmat.</i>
Inspections – national and local site inspections	<i>Experiences from inspections are good, they reveal treats and incease security consciousness.  Transport on tracks is perceived as secure.</i>	<i>Not a part of the Railway Inspectorates mandate – but probably under the National Emergency Agency.  Site inspections reveal stations and shunting areas as critical elements.</i>	<i>Raise the question of how national responsibility for security inspections should be organised.  Develop checklists for spotting undesired persons, goods etc. Design to make treats visible, and thus make terrorist to choose other targets.</i>
Security cooperation	<i>Mostly good</i>	<i>Police observes that some operators and private security forces do not understand the importance of security actions on request form the police</i>	<i>Establish regular meetings with the police authorities along the line</i>
Personell training plans and check of employees	<i>RETRACK partners have specific persons in charge of security, field exercises and also check employees before hiring them.</i>	<i>The survey only gave experiences from few coutries on this item.</i>	<i>Arrange/establish a forum for persons in charge of security along the line for exchange of experiences and mutual learning.</i>
Emergency preparedness and communication	<i>The lines of command for emergency seem clear and there are systems for info on hazmat in place. No sign that intruders get access to sensible information</i>	<i>Some wants more info on possible security treats and more detailed info on CCTV coverage.  Language skill is a problem and also lack of cellphones/rail phones.</i>	<i>Furnish the stakeholders along the line CCTV info.  Furnich all pilot trains with cell phones. Discuss which common language and codes to use in emergency situations</i>
Incident reporting and systems	<i>No terrorist actions reported</i>	<i>Thefts and cargo tampering the most frequent problem. Must be handled not to loose customers,  Different reporting routines to EU and locally.</i>	<i>Study effective locking systems and CCTV at terminals. Securirty could be developed to a competivie asset for  Establish a simple registration system for faults revealed along the line as basis for actions</i>

RETRACK partners and others involved in the Pilot project seem to be relatively satisfied with the state of art on security. They work along the national regulations given and find these mostly sufficient. From their practise in rail business they pinpoint several possible improvements on elements influencing rail freight security. Given the frames of the current project one could not expect the implementation of all such actions on a general basis. We will just give two recommendations:

- A dedicated cross-national security group should definitely be established as a part of the pilot project.
- If the pilot results in a permanent rail freight line and if other such lines are developed, one should obviously learn form the RETRACK survey and the experiences there enlightened.

### 6.3 Specific experiences from the RETRACK project

RETRACK is an integrated rail freight *research and demonstration* project with initially high ambitions – also for the security part of research.

When RETRACK submitted its application to the EUs 7<sup>th</sup> Framework Programme in December 2005 Rail Safety and Security was supposed to use 51 Man Months (MM), representing 10,1% of the total budget. At the time this disposition of resources and the research objectives listed was in line with the Communities focus on security rail freight research in 7.FP, especially so when considering that the consortium had many partners from the cargo business and that the researchers were in a minority. In the end, after contract negotiations and sequential changes of the Technical Annex one ended up with 9 MM, or 1,6 % of the total budget dedicated to security research.

In addition the partners did not fulfill the tasks they were contracted to in relation to WP7.2, the RETRACK Security Survey. Each one should have brought their experiences to the consortium and should help to gather other experiences and viewpoints on critical aspects of security related to the RETRACK corridor. Dialogue and cooperation was the key in achieving the objectives of WP7, namely to contribute to enhancing security consciousness. But it did not function exactly this way.

What were the reasons for this? Is security consciousness very low among the partners? Is security a low-priority issue for the partners and the Commission who decide on the downsizing of budgets? Or could there be other confounding explanations? We will look at some possible hypotheses like;

- Working across borders
- General economic crisis
- Shift in project focus
- No defined security actions

An important characteristic of RETRACK is huge amount av *border-crossing work*. RETRACK work not only across countries but also across local and national actor, across type of stakeholders and across praticians and researchers. Such work is obviously extremely demanding.

RETRACK starting in 2007, should plan and then from 2008 demonstrate a new railconcept at a time with severe *economic problems in Europe* and falling market share for rail all over the world. It is easy to understand that the partners found it

more important to work with paving the track for the pilot than with security consciousness.

The rescaling of the budget, cf. sub-chapter 1.2.3 and 1.2.4 was followed by a shift of focus *from implementation to stimulation of consciousness*. With less resources the objectives of WP7 were changed from practical implementation of strategies for organization, management, learning, control, scanning, detection, communication, technical operation etc (RETRACK Proposal to EC 2005) to contribution to stimulate the security consciousness among the partners. This should be done by more academic procedures (literature review and questionnaires). This research could thus seem far from the usual way of working among the partners and the many practical challenges related to the pilot. Engaging the partners in collecting data on security did not seem to function as a way to increase consciousness of the theme.

*No defined specific security actions* beyond collection and discussion of experiences were demanded from the partners. Psychologically this can influence priorities on this kind of perceived additional work, even if it was contracted and paid for. Especially so in a situation where security risk is low, the challenges are complicated to define exactly and you fulfill the requirements already given in national or international laws and regulations.

De facto, given from the budgets and the work with WP7, we can conclude that RETRACK gave low-priority to the security research work in the EU project. But we cannot conclude that the partners don't give security the priority demanded in their normal practical railway operations and business. We have not studied their security work in detail, and cannot give characteristics on this subject. We assume that the partners fulfill all regulations that are implemented on the European and national level. However given their situation, it is not to be expected that relative small independent operators shall push such issues beyond these demands.

Anyhow one very important general lesson from the priority process discussed above is that when economic matters are problematic themes like security – and safety – will easily be downsized with regard to consideration, engagement and resources. Given a WP in a research project this is not so important, but transferred to real life such a tendency could be critical and is worth discussing. If one believes that rail security and safety matters can do without attention for some time, the risk for incidents might obviously grow. Safety and security must always be main objectives and be given the necessary attention in any transport activity.

## 7. References

- Accident Investigation Board Norway (AIBN), 2004  
Annual report 2003.
- Amundsen, A. H. and Elvik, R. 2006  
El.avgift på frakt på bane – konsekvenser for trafikksikkerhet. Oslo,  
Transportøkonomisk institutt. Arbeidsdokument SM/1750/2006. (*In Norwegian*)
- Elvik, R. and Erke, A. 2006  
Sikkerhetsmessige konsekvenser av to transportløsninger for transport av flydrivstoff til  
Gardermoen. Oslo, Transportøkonomisk institutt. Arbeidsdokument SM/1788/2006. (*In Norwegian*)
- Beck, U. 1992.  
Risk society.
- Berrick, C. A. 2007  
Transportation security. Efforts to strengthen aviation and surface transport security  
are under way, but challenges remain. Director Homeland Security and Justice issues.  
Testimony before the Committee on Commerce, Science and Transportation, US  
Senate. GAO-08-140T. (October 2007)
- Bjørnskau, T., Gripsrud, M., Grunnan, T., Leite, T. and Wiese Schartum, D. 2007  
Transport security and the protection of privacy. Oslo, Institute of Transport  
Economics. TØI report 914//2007. (*English summary*)
- Clarke, Ronald V. 1983.  
Situational Crime Prevention: Its theoretical basis and practical scope.
- Clarke, Ronald V., and Graeme R. N., 2006  
Outsmarting the terrorists. Westport: Praeger Security International.
- Commission of the European Communities 2003  
Freight transportation security. European Commission, Directorate-General for Energy  
and Transport. Consolation paper.
- Commission of the European Communities 2005  
Green paper on a European Program for Critical Infrastructure Protection. Brussels,  
Commission of the European Communities. November 2005.
- Commission of the European Communities 2007  
Authorized economics operators. Guidelines. TAXUD/2006/1450.
- Dellinger, J. C. and Kotsikos, G. 2008  
Public safety and security, State of the art. WP2.4, RETRACK. Sixth framework  
programme, European commission.
- Grunnan, T., Bjørnskau, T. and Kolbenstvedt, M. 2008  
Cross-modal safety in the transport sector. Oslo, Institute of Transport Economics.  
TØI report 954/2008. (*English summary*)
- Elvik, R. and Olsen, S. F. 2004  
Major accidents in transport. Oslo, Institute of Transport Economics. TØI report  
748/2004. (*English summary*)
- ESRIF 2009  
ESRIF final report. European Security Research and Innovation Forum, December  
2009.
- European Commission, 2004  
“Safety Directive” (Directive 2004/49/EC)

- European Commission, 2006  
*Meeting the challenge: the European Security Research Agenda*. Luxembourg: Office for Official Publications of the European Communities, 2006.
- European Commission, 2007  
*Work programme 2008. Cooperation. Theme 10. Security, 2007*
- European Communities, 2007  
 Eurostat Statistical Books. Panorama of Transport, Edition 2007
- European Communities, 2009  
 Eurostat Statistical Books. Panorama of Transport, Edition 2009
- European Conference of Ministers of Transport 2005  
 Container transport security across modes. European Conference of Ministers of Transport (ECMT). OECD. ECMT 2005.
- ERA European Railway Agency, 2006  
 A summary of: 2004-2005 EU statistics on railway safety.
- ERA, European Railway Agency 2009  
 The Railway Safety Performance in the European Union.
- European Security Research Advisory Board, ESRAB, 2006  
 Meeting the challenge: the European Security Research Agenda.
- Evans, A. W. 2003  
 Transport fatal accidents and FN-curves: 1967-2001. London, Health and Safety Executive. Research Report 073.
- Guerrero, P.F. and Rabkin, N. J. 2004  
 Rail security. Some actions taken to enhance passenger and freight security, but significant challenges remain. Director of Physical Infrastructure issues and Managing Director of Homeland Security and Justice issues. Testimony before the Committee on Commerce, Science and Transportation, US Senate. GAO-04-598T. (March 2004)
- Haight, F. A.  
 What causes accidents – a semantic analysis. In Evans, L. (ed): *Accident Causation* Warrendale, Society of Automotive Engineers. Report SP-461.
- Hamberger, E. R. 2005  
 Hearing on: Railroad security. President and Chief executive officer of Association of American Railroads. Senate Commerce committee, October 2005.
- Hamberger, E. R. 2007  
 Hearing on: Rail and public transportation security act of 2007. President and Chief executive officer of Association of American Railroads. Before the US House of Representatives committee on Homeland Security, March 2007.
- Hartong, M. Goel, R. Wijesekra, D. 2008  
 Security and the US rail infrastructure. *International journal of critical infrastructure protection*. Vol 1, pp15-28.
- Hecker, J. Z. 2006  
 Passenger rail security. Evaluating foreign security practices and risk can help guide security efforts. GAO report GAO-06-557T
- Islam, D., Zunder, T. and Mortimer, P. 2008  
 State-of-the-art synthesis report on rail freight service on Rotterdam-Constanza corridor. Reorganization of transport networks by advanced rail freight concepts. WP2.10, RETRACK. Sixth framework programme, European commission.
- Jenkins, B. M. 1997  
 Protecting surface transportation systems and patrons from terrorist activities. San Jose, Norman Y. Mineta International Institute for Surface Transportation Policy Studies.

- Jenkins, B. M. 2001  
Protecting surface transportation against terrorism and serious crime: An executive overview. San Jose, Norman Y. Mineta International Institute for Surface Transportation Policy Studies. MTI Report 01-14.
- Jenkins, B. M. & Gerston, L. 2000  
Protecting Public Surface Transportation Against Terrorism and Serious Crime: Continuing Research on Best Security Practices. San Jose, Norman Y. Mineta International Institute for Surface Transportation Policy Studies.
- Jersin, E. 2004  
Katastrofepotensialet ved uønskede hendelser innen transport: hvilke faktorer avgjør om en hendelse utvikler seg til en storulykke. Trondheim, SINTEF teknologiledelse sikkerhet og pålitelighet. Rapport STF38 A04011. (*In Norwegian*)
- Jones, I. et. al. 2000  
Safety regulations and standards for European railways. Executive summary. A report for DG Energy and Transport. London, National Economic Research Associates.
- Kaplan, E. 2007  
Rail security and the terrorist threat. Council on Foreign Relations. March 2007.
- Kolbenstvedt, M. and Amundsen, A. H. 2008  
Rail freight security practices. Literature review and background for a RETRACK security survey. Deliverable 7.1. WP 7, RETRACK. Sixth framework programme, European commission.
- Kolbenstvedt, M. and Amundsen, A. H. 2009  
Rail freight security practices. Questionnaires to be used in the RETRACK security survey. Deliverable 7.2. WP 7, RETRACK. Sixth framework programme, European commission.
- Ludvigsen, J. 2009  
Security of mass Transportation. Policy for Implementation of Innovation. Contribution at Workshop in Berlin, 18. March 2009.
- Machenbach, P. and Coolen, M. 2005  
Study on the impact of possible European legislation to improve transport security. Impact assessment. DNV report 40008032-6-2
- Meyer, S. 2009: Aiming For Mass-killings: Explaining Terrorist' selection of targets in mass-transportation. (Submitted to American Political Science Review)
- Mihm, P. 2006  
Evaluation of the results from SAMRAIL and SAMNET projects. European Railway Agency. September 2006.
- Nævestad, T. O. 2010  
Culture, crisis and campaigns: examining the role of safety culture in the management of hazards in a high risk industry. Ph.D. dissertation. Oslo, Center for technology, innovation and culture, University of Oslo. (*submitted*)
- Norges offentlige utredninger 2001  
Lillestrøm-ulykken 5. april 2000. Oslo, Statens forvaltningstjeneste Informasjonsforvaltning. NOU 2001:9. (*In Norwegian*)
- Pasi, S. 2007  
Rail transport accidents in the European Union in 2004-2005. Statistics in focus, Transport, vol 34. Eurostat. Brussels, European Communities.
- Patacchini, A. 2007  
Experiences with safety management systems. Survey on existing SMS legislation practices in the railway sector and other critical sectors throughout the world. European Railway Agency. Safety unit.

- Perkuszewska, A. and Schiavi, F. 2007  
 Safety database report 2007. - significant accidents in 2006 – benchmarking and six-year trends. Paris, International Union of Railways.
- Perrow, C. 1984, 1999  
 Normal accidents. New York, BasicBooks.
- Peterman, D. R. 2006  
 Transport security: Issues for the 109<sup>th</sup> congress. CRS report to Congress. IB10135. June 2006
- Peterman, D. R., Elias, B. and Frittelli, J. 2007  
 Transport security: Issues for the 110<sup>th</sup> congress. CRS report to Congress. RL33512. August 2007
- Planas, E., Pastor, E., Presutto, F. and Tixier, J. 2008  
 Results from the MITRA project: Monitoring and intervention for the transportation of dangerous goods. *Journal of Hazardous Materials*, vol 152, issue 2, pp 516-626, 2008.
- Puls, J. 2009  
 Security of Mass Transportation. The Contribution of Deutsche Bahn AG, COLPOFER at Workshop in Berlin, 18 March 2009.
- Rausand, G. 2004  
 Storulykker innen passasjertransport globalt i perioden 1991-2003. Trondheim, SINTEF teknologiledelse sikkerhet og pålitelighet. Rapport STF38 A04406. (*In Norwegian*).
- Reason, J. 1997  
 Managing the risk of organizational accidents. Aldershot, Ashgate.
- RETRACK, 2005  
 Proposal for an Integrated Project in the 6<sup>th</sup> Framework Programme of the European Union, European Union, 2005
- RETRACK, 2006  
*SIXTH FRAMEWORK PROGRAMME Sustainable Development, Global Change and Ecosystems Sub-Priority 1.6.2: Sustainable Surface Transport FP6-2005-TREN-4. Annex I – “Description of work”, European Union 2006.*
- RETRACK, 2008  
*SIXTH FRAMEWORK PROGRAMME Sustainable Development, Global Change and Ecosystems Sub-Priority 1.6.2: Sustainable Surface Transport FP6-2005-TREN-4. Annex I – “Description of work”, European Union 2008*
- RETRACK, 2009  
*SIXTH FRAMEWORK PROGRAMME Sustainable Development, Global Change and Ecosystems Sub-Priority 1.6.2: Sustainable Surface Transport FP6-2005-TREN-4. Annex I – “Description of work”, European Union 2009*
- Smith, Martha J., and Derek B. Cornish, eds. 2006.  
*Secure and Tranquil Travel: Preventing Crime and Disorder on Public Transport.*  
 London: UCL Jill Dando Institute of Crime Science.
- Spraggins, H. B. 2005  
 Risk modelling of hazardous materials, rail movement to include a terrorist incident. *Journal of the Academy of Business and Economics*. March 2005.
- Taylor, B., Loukaitou-Sideris, A., Liggett, R., Fink, C., Wachs, M., Cavanagh, E., Cherry, C. and Haas, P. J. 2005  
 Designing and operating safe and secure transit systems: Assessing current practice in the United States and Abroad.. San Jose, Mineta Transportation Institute. MTI report 04-05.

Thompson, B., Oberstar, J., Mica, J., Brown, C., Shuster, B. and Cummings, E. 2009  
Freight rail security. Actions have been taken to enhance security, but the federal strategy can be strengthened and security efforts better monitored. GAO report GAO-09-243.

US Department of Homeland security 2006  
National Infrastructure Protection Plan (NIPP). Arlington, Transportation Security Administration.

US Department of Homeland security 2007  
Transportation systems. Critical infrastructure and key resources. Sector-specific plan as input to the National Infrastructure Protection Plan (NIPP). Arlington, Transportation Security Administration.

US Department of Homeland security 2007b  
Passenger rail security. Federal strategy and enhanced coordination needed to prioritize and guide security efforts. GAO report GAO-07-583T.

US Department of Transportation. 1999  
Intermodal cargo transportation : Industry best security practices. Research and Special Programs Administration. DOT-T-99-19

United Nations, Working party on rail transport 2010  
Report of the working party on rail transport on its 63 session. ECE/TRANS/SC.2/212.

Wildavsky, A. 2004  
Searching for safety. 3<sup>rd</sup> edition. New Brunswick (USA) and London (UK), Transaction publishers.

**Appendix I: Ongoing EU-projects including security related issues**

Acronyms	Projects names, and short description of aims.	Period
CAST	Comparative assessment of security-centered training curricula for first responders on disaster management in the EU.	2009-2011
DEMASST	Demo for mass transportation security: roadmapping study	2009-10
DETEC-TER	Detection technologies, terrorism, ethics and human rights To identify human rights and other legal and moral standards that detection technologies in counter-terrorism must meet, while taken into account the effectiveness of the technologies.	2008-2011
EFFISEC	Efficient integrated security checkpoints. Goal is to deliver border authorities more efficient technological equipment: that provides higher security level of identity and luggage control of passengers.	2009-2012
ERRAC	ERRAC Roadmap. WP04- Improving safety and security. Passengers and freight. Deliver roadmaps to guide rail research for the future. Enhance awareness and perform actions along key issues.	2009-2012
ERBORD	Border security issues in EU-Russia relations: challenges, perceptions and responses. Examine border security issues, and estimate the seriousness of border security challenges (drug-trafficking, illegal migration, smuggling etc.)	?
ESCoRTS	European network for the security of control and realtime systems. Cyber security of control and communication equipment in EU.	2008-2010
ESTEEM	Enhancing safety and security aspect in transport research in the Euro Mediterranean region. Coordination of research activities and policies between EU and the neighboring countries on transport issues.	2008-2009
FESTOS	Foresight of evolving security threats posed by emerging technologies. Identify and assess security threats posed by abuse or inadequate use of emerging technologies and new scientific knowledge. Propose means to reduce their likelihood.	2009-2011
ODYSSEY	Strategic pan-European ballistics intelligence platform for combating organized crime and terrorism. Aim is to create and develop secure interoperable situation awareness platform for the EU to combat organized crime and terrorism.	2008-2011
SAMURAI	Suspicious abnormal behavior monitoring using a network of cameras and sensors for situation awareness enhancement Develop and integrate an innovative intelligence surveillance system for monitoring people and vehicle activities at both inside and surrounding areas of a critical infrastructure.	2008-2011
SECRI-COM	Seamless communication for crisis management. Develop a reference security platform for EU crisis management operations. Use of secure encrypted mobile communication, creating recoverable networks and seamless connectivity, using trusted hardware enhancing the confidentiality of data and the privacy of users.	2008-2012
SKILLRAIL	Education and training actions for high skilled job opportunities in the railway sector. Based on knowledge and experience to create a high quality training and education activities suitable for further needs in the rail service.	2009-2011
TRACK-BOCS	Develop a tracking and security system for containers. Enabling tracking and security independently of fixed check point installation and satellite navigation systems.	2009-2011

