A RISK ASSESSMENT APPROACH FOR INLAND CONTAINER TERMINALS

Manfred Gronalt[(a)], Hans Häuslmayer[(b)], Werner Jammernegg[(c)], Edith Schindlbacher [(a)], Monika Weishäupl[(c)]

[(a)] University of Natural Resources and Applied Life Sciences Vienna, Feistmantelstraße 4, 1180 Vienna, Austria
[(b)] h2 projekt.beratung, Obere Viaduktgasse 10/7, 1030 Vienna, Austria
[(c)] Vienna University of Economics and Business Administration, Nordbergstraße 15, 1090 Vienna, Austria

[(a)]manfred.gronalt@boku.ac.at, edith.schindlbacher@boku.ac.at, [(b)]hh@h2pro.at,
[(c)]werner.jammernegg@wu-wien.ac.at, monika.weishaeupl@wu-wien.ac.at

ABSTRACT
Inland container terminals are, due to their operational daily business and environmental conditions faced with several risks having different degrees of consequences. Current risk assessment methods for terminals just consider dramatic events like terrorist attacks. We present a new method for the assessment of risk and vulnerability of inland container terminals, also including terminal internal and environmental factors.

Keywords: risk assessment methodology, inland container terminals, risk profile

1. INTRODUCTION

Ever more frequent disturbances and irregularities in the flow of goods in transport chains and transport systems reflect the importance of evaluating supply chain risk potentials. Disturbances in the supply chain can be caused by an act of sabotage on transport chains or their infrastructure, as well as by natural hazards, including flooding or earthquakes. Specifically in Austria natural hazards like storms, heavy rains, avalanches and floods are of great importance.

A supply chain can be defined as a "network of organisations that are involved, through upstream and downstream linkages, in the different processes and activities that produce value in the form of products and services in the hands of the ultimate consumer" (Christopher, 1992). An intermodal supply chain is a multi-element transport chain consisting of pre-carriage of cargo to a terminal, the transhipment to another means of transport and the following actual change of location on that modus. The transportation process ends after a further transhipment and the on-carriage of the goods or containers. Container terminals thereby represent the essential infrastructure for the turnover process.

The German authority Federal Office for Information Security defines critical infrastructure as "organisations or facilities of key importance to public interest whose failure or impairment could result in detrimental supply shortages, substantial disturbance to public order or similar dramatic impact", which includes transportation and traffic (Hellström, 2007). Austrian inland container terminals can be considered as critical infrastructure, because major industry branches depend on container transport logistics. As a consequence, the terminal nodes are crucial hubs for intermodal (rail, truck, ship) container turnover in logistics networks.

In contrast to numerous national and international security guidelines and initiatives for seaports, there exist no obligatory legal guidelines for inland terminals.

A longer persisting disruption of a certain stage - respectively a node - of a supply chain can cause massive damages which are hard to quantify. Such an incident can affect the whole supply chain, i.e. from suppliers, who no longer can deliver their goods, up to the customers, who don't receive them.

The remainder of the paper is organized as follows. In Chapter 2 we highlight related works in supply chain risk assessment and classification. Chapter 3 gives a presentation and critic of the pro and cons of a risk assessment method for terminals developed by the International Union of combined Road-Rail transport companies (UIRR). In Chapter 4 we then present a new risk assessment approach, developed in a field study of Austrian inland terminals. Furthermore, we show the differences of our developed risk assessment approach to the mentioned industry guidelines and give reasons for our modifications. In addition to that, we illustrate our method, using a real-world example of an Austrian inland terminal. We conclude in Chapter 5 with the identification of future research needs.

2. RELATED WORKS

Supply chains can be exposed to many forms of risks, which emphasises the importance of research. Minor (2005) points out four major reasons why intermodal supply chains are especially prone to risks. First, supply chains today are time-sensitive. If supply chains are just-in-time, disruptions have more severe effects, than if there would be a time buffer. Second, there exists a massive reliance on non-standardised or tailored inputs. If goods are tailored to exact specifications, a new supplier would take weeks or even months to reengineer

its supply lines. Third, most companies rely on single- or limited-source supplies – the reliance on tailored goods indicates, inherently, a limited-source supply chain. The last point Minor mentions, is the reliance of (producing) companies on single geographies - sometimes one country is simply the best supplier for a good.

Therefore, the handling of risks and complex processes is gaining importance in managing supply chains. Risks in supply chains generally can be classified in several ways. Out of many approaches there are several that are adequate for inland container terminals. A distinction between market risks and operational risks is proposed by Chopra and Sodhi (2004). Market risks comprise demand and exchange rate risks; operational risks can be subdivided in acquisition and process risks. Christopher and Peck (2004) use the "point of origin" approach which could be used to classify risks for terminals. On the one hand, there are process and control risks arising within the regarded organisation. On the other hand, there are supply and demand risks emanating from supply chain partners. In addition to that, environmental risks can occur due to socio-political or macroeconomic reasons or natural disasters.

An overview on supply chain management with an account to risk is presented by Kersten et al. (2006). Supply chain management includes the corresponding risk and complexity management, since various stages are obliged to co-operate. Thus, risk assessment is also considerably relevant for each individual company involved. The authors also show that there is a difference in assessing sources of risks between producing companies and logistics firms.

A framework of risk assessment and characterisation of risks in supply chains is presented by Deleris and Erhun (to appear). Their analytical process starts by defining the considered system and performance value using expert opinions and flow charts. In the next step they identify possible risks and show how they interdependently influence each other. This step is based on statistics and expert opinions. The last two stages of the framework are risk quantification and risk management.

A lot of work on risk assessment in supply chains has been undertaken by many authors. Research concerning risk and transportation infrastructure is presented for example by Knoflacher et al. (2002), Riley (2004) or the Volpe National Transportation Systems Center (2003). As well, considerable work has been done in the topic of container security, focusing on the transport loading unit itself (for example Seidelmann, 2007). The International Labour Organization and the International Maritime Organization present a framework for port security assessment (ILO/IMO, 2003). To the best of our knowledge, except for the UIRR guidelines, which we present in the following chapter, no corresponding work for inland container terminals exists.

3. UIRR METHOD OF RISK ASSESSMENT FOR COMBINED TRANSPORT TERMINALS

The need to develop a method of risk analysis for inland container terminals evolved on the basis of the reviewed literature and guided framework interviews, expert opinion polls and on-site-inspections at several Austrian inland terminals.

Among others, the method and guidelines for the risk analysis of combined transport terminals, provided by the International Union of combined Road-Rail transport companies - UIRR, (UIRR, 2007a and 2007b), were a starting point for our risk analysis approach. In the UIRR's view an exposure to threats of a terminal is given by the mean and possibility of destructing the terminal itself, or the mean of affecting the natural or technical infrastructure surrounding the site.

The first step of the UIRR analysis is the identification of possible threats, starting with a framework of possible malicious terrorist operations. Questions asked in this context are for example, why a terminal could be the target of an attack, and how this could happen. Basically, the analysis distinguishes here between three scenarios. First, the attempt to destroy the terminal or parts of its contents, second, the use of the terminal as a source for products or material for the later deployment for an attack, and third, the usage of the terminal as starting point or transit facility for concealed persons or material in a loading unit.

The second step of the analysis presents the evaluation of the sensitivity of the terminal. The susceptibility and the location of the terminal are considered as the two main factors of vulnerability. A measure for the susceptibility is the presence of dangerous substances on the site. This represents the key role for a feasible terrorist interest in combined transport terminals. The location of a terminal is of importance in case of nearby densely populated areas or crowded areas like schools, hospitals, stadiums etc. or the closeness to critical infrastructures like air ports, transport corridors, chemical plants or other facilities.

In order to estimate the sensitivity of the terminal site, two other factors - on the one hand already taken precaution measures to ensure the security, and on the other hand the state of alert as published by public authorities - have to be considered. Eventually, risks can be defined on the basis of the threats to which a terminal is exposed to, and its specific vulnerabilities in combination with the possible consequences of a terrorist act for the terminal in question and its surrounding environment.

The UIRR itself criticises some points of its method of risk analysis. One of them is the difficulty of estimating probabilities of occurrence for actions of terror. For these cases no statistic argumentation is possible. Moreover, distances between the terminal and its surrounding infrastructure and environment are specified arbitrarily for the determination of the area of vulnerability, thus, a (negative) discrimination of terminals can happen. In addition, no domino effects are

considered in the evaluation of the consequences of a possible act.

According to our opinion, the method of the UIRR is a further general framework for risk analysis and doesn't give concrete suggestions for the computation of the potential risks of a terminal and therefore, its vulnerability. Furthermore, the view of the risks, a terminal can encounter, refers purely to possible threats of terrorism. This focus is understandable, considering the world-wide developments in the last years. However, operational risks and risks to the terminal, emanating from the surrounding infrastructure and from environmental conditions play an important role as well. In general, effects of these risks are considered to be less dramatic than a terrorist attack, but a much higher frequency and probability of occurring can be assumed.

For this reasons, the method of the UIRR did not seem appropriate enough to cope with the situation of Austrian intermodal supply chains. As a consequence, we developed our own approach for the classification of risks and vulnerability assessment for intermodal transport nodes.

4. A NEW APPROACH FOR RISK AND VULNERABILITY ASSESSMENT OF INLAND TERMINALS

The structuring of risk sources builds the basis for our directed identification and analysis. Risk categories, including their subclasses for inland container terminals, can best be illustrated by using a three-step process, which is oriented towards the framework of Deleris and Erhun (to appear). In the first step a complete description of the terminal regarding its operations and all other risk assessment factors is developed. It is also arranged according to the three risk dimensions identified by Christopher and Peck (2004). In the second step, we picture the point of origin of all possible disturbance events to a terminal, corresponding to the aforementioned description. The following impacts of these disturbance events are classified in the third step. Thus, a logically consistent path is guaranteed.

4.1. Risk Identification and Classification

Step 1: Terminal description

The elements describing a terminal are classified into the three main-categories "terminal internal factors", "network factors" and "surrounding conditions". The components of the first sub-category (see Table 1) are specified in more detail through another sub-categorisation. For example, a terminal is described through the internal factor "yard", which is characterised by the storage area, the empty-container storage and the storage area for dangerous goods. A further description of the singular subcategories is realised in additional stages.

Step 2: Risk identification and classification

The classification of the potential risks for a terminal is undertaken by the determination of their point of origin. The categories of risk sources are: "diminished availability", "capacity overload", "accidents", "failures and communication failures", "acts of sabotage and attacks", "natural disasters and weather" and "economical and political incidences". These sources are appropriately assigned to the three main-categories corresponding to the terminal description.

Table 1: Terminal Description

Categories	Factors
terminal internal factors	workforce
	external persons at the site
	turnover
	yard
	edificial facilities
	equipment
	rail-road-waterway infrastructure
	ICT
	security facilities
	risk management
	backup facilities
network factors	network-role of the terminal
	transport connection
	network ICT
surrounding conditions	natural environment
	technical environment
	economical and political situation

In this context it is important to be aware of the fact that the sources designated in this classification could be the cause of a risk, but also concurrently the result, respectively the consequence of a cause, which denotes the mutual relationship.

The link between the first and the second step of the method is given by the elements of the first sub-category of the description of the terminal and the second sub-category of the risk classification (see Table 1 and Figure 1). For a better understanding we give a few examples in the following:

- *Terminal operations* are negatively affected through a *diminished availability* of the *workforce*, caused through *absenteeism*.
- *Terminal operations* are negatively affected through a *high utilisation* in the *network*, specifically a *capacity overload of the rail track*, which belongs to the *network connection.*
- *Terminal operations* are negatively affected through an event in the *surrounding conditions* of the terminal, more precisely an attack on the *technical environment*, with the result of a *fire* and consequently a *blockade of the motorway intersection.*

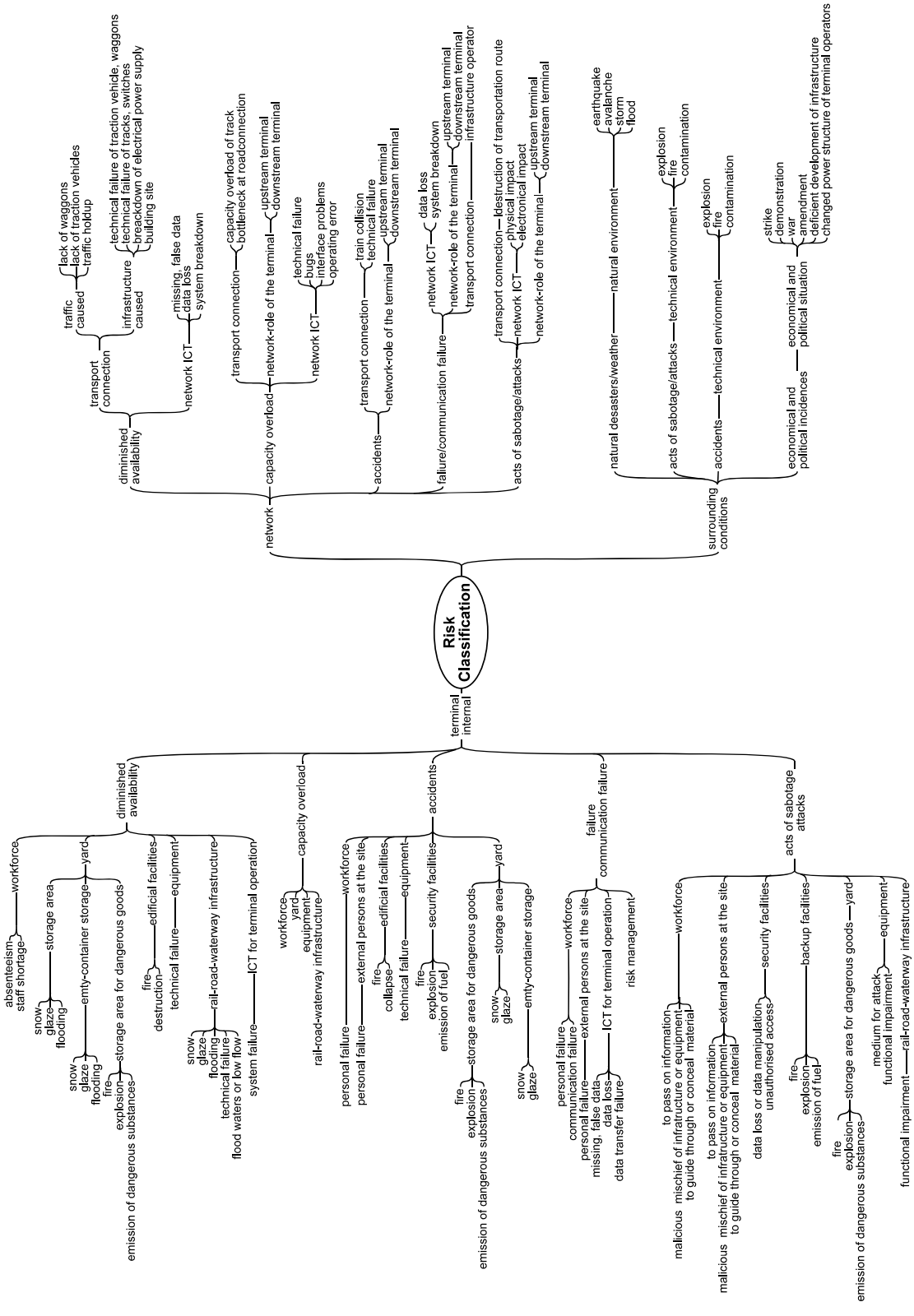

Figure 1: Risk Classification

The intuitive simple form of presentation in a mind map of the risk classification in Figure 1, is selected intentionally for getting an easy overview to the extensive components. The outermost branches are exemplary for concrete scenarios, and therefore don't represent an exhaustive enumeration.

To describe a scenario in more detail, one can use the terminal description from step 1, and hence, specify the description of the elements by the use of the conjunctive layer between step 1 and step 2.

For more information about the terminal description, please contact the authors.

Step 3: Assignment of consequences

The third step in our risk analysis approach subdivides the possible consequences of feasible disturbances or disruptions of terminal operations. We try to estimate the extent and the duration of impact, as well as its intensity. Effects of disruptions can concern the incoming and outgoing of loading units through road-, rail- and/or waterways, and as a consequence reduce the total performance of the terminal (see Table 2).

Table 2: Structure of Consequences

Consequence			Extension (yes / no)	Duration	Intensity 0-100 %
Throughput	Rail	Incoming			
		Outgoing			
	Road	Incoming			
		Outgoing			
	Waterway	Incoming			
		Outgoing			

4.2. Analysis of vulnerability

The next step after the identification of all possible risks, a terminal and its operations can face, is to conduct a vulnerability assessment on the level of the particular factors describing a terminal. For this purpose, we developed a set of several two-dimensional matrices, which only take into consideration the decisive elements for causing potential vulnerabilities to disruption or disturbance, out of all the describing elements of a terminal from step 1. We assess the susceptibility to suffer a disturbance, and in a second instance, the ability to react adequately to a negative event happening in these decisive elements.

Assigned to the matrix is a scale with five grades, ranging from "strongly negative" to "positive" in concern to terminal vulnerability. In case of multiple applicable categories, the terminal is classified by the most negative one. Primarily, the assessment is performed with a view to terminal operations, and secondarily it considers other risk sources, like the possibility of natural hazards or acts of sabotage.

For example, a terminal is assessed by risk and vulnerability resulting from its workforce. The dimensions of evaluation are the workforce structure and its utilisation. The structure of the workforce is characterised by the cumulative job tenure of the own staff, and by the employment of leased staff. The extent of the job tenure allows implications on the qualification and routine of the workforce. (Short time) leased staff generally is less familiar with terminal operations than the permanent staff. Performing the evaluation, we assume that a highly skilled own staff is able to compensate flaws caused by temporary employees. Figure 2 shows the result for the factor "workforce" for one of the analysed Austrian terminals, classified in the way depicted above.

Another, very significant factor for inland container terminals is the transhipment equipment. Regarding this factor, the vulnerability is evaluated by the utilisation of the equipment and the ad-hoc availability of potential substitutes. In the event of a breakdown, equipment can thus be replaced by other existing equipment of the same or of another type. For the evaluation, we assume that in the latter case larger constraints emerge in the transhipment process. Moreover, the overall utilisation considerably affects the substitutability. It defines the free capacities of the remaining functional equipment (see Figure 3).

A framework with the same procedural method for all factors of the terminal description (see Table 1) was developed.

Scale: Assessment of vulnerability

strongly negative	negative	slightly negative	neutral	positive

WORKFORCE	Structure			
Utilisation	leased staff, short job tenure of company's staff	just company's staff, short job tenure	leased staff, long-time job tenure of company's staff	just company's staff, long-time job tenure
full				
high				X
normal				
low				

Figure 2: Assessment of Workforce

EQUIPMENT	Substitutability			
Utilisation	no substitutability	possible through other type of equipment	possible through same type of equipment	possible through other and same type of equipment
full		X		
high				
normal				
low				

Figure 3: Assessment of Equipment

The overall picture of a terminal's vulnerability evolves from the depiction of the evaluated complete set of factors in a vulnerability profile. Hence, the identified weaknesses are visible at a glance. Figure 3 shows the vulnerability profile of one of the analysed Austrian terminals. The marked area indicates the non-critical factors in the terminal.

With such a vulnerability profile a clear form for contrasting different terminals against each other is provided, and an extensive reflexion of the vulnerability of a terminal network, respectively a supply chain network, is possible.

5. CONCLUSION AND NEED FOR FUTURE RESEARCH

We have shown that inland container terminals as important nodes of international supply chains face more and ever more complex risks. Not only dramatic terrorist events can pose a challenge and risk to supply chains (even though not a single incident in the last years of terrorists attacks on supply chains or container terminals is known – one can only speculate on the reason for this). Other risks, emanating from the daily business, the structure of terminal operations, its environment or surrounding infrastructure can be named and are often much more frequent, and sometimes even

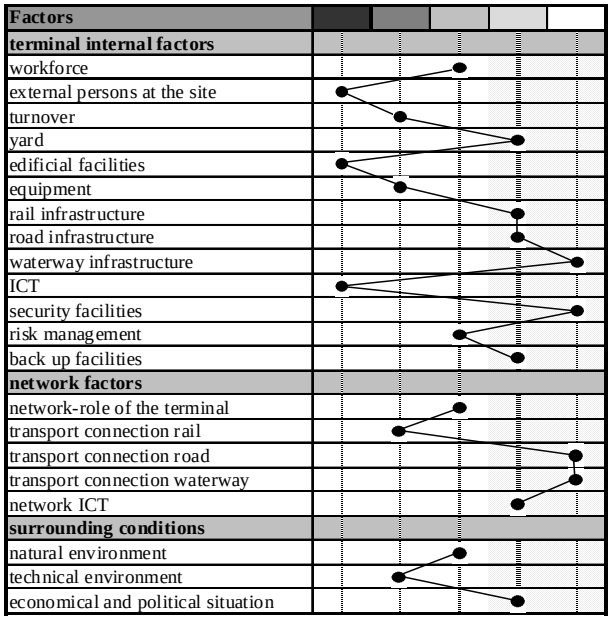

Figure 3: Vulnerability Profile of a reference terminal

as severe as terrorists attacks. Therefore, we developed a methodology and framework to undertake more comprising risk and vulnerability assessment of inland container terminals.

As container terminals just constitute the nodes in intermodal supply chains, an extension of our research will focus on the several carriers and modes of transportation in such multimodal supply chains. Further, as a chain is ever only as weak as its weakest link, the assessment of the nodes can only be one part in a comprising risk assessment of supply chains. Hence, we intent in further research to take an unagitated look on the matter of risk assessment of the different possible edges between the nodes in intermodal supply chains.

ACKNOWLEDGMENTS

This research was funded by a grant of the Austrian Security Research Programme KIRAS of the Federal Ministry for Transport, Innovation and Technology, managed by the Austrian Research Promotion Agency (FFG).

REFERENCES

Chopra, S., Sodhi, M.S., 2004. Managing Risk To Avoid Supply-Chain Breakdown. *MIT Sloan Management Review* 46(1): 53-61.

Christopher, M., 1992. *Logistics and supply chain management*. London: Pitman Publishing.

Christopher, M., Peck, H., 2004. Building The Resilient Supply Chain. *International Journal of Logistics Management* 15(2): 1-14.

Deleris, L.A., Erhun, F., to appear. Quantitative risk assessment in supply chains: a case study based on engineering risk analysis concepts. In: Kempf, K., Keskinocak, P., Uzsoy, R., eds. *Handbook of Production Planning*. Boston: Kluwer Academic Publishers.

Hellström, T., 2007. Critical infrastructure and systemic vulnerability: Towards a planning framework. *Safety Science* 45: 415-430.

ILO/IMO, 2003. *Code of practice on security in ports*. International Maritime Organization. Available from: http://www.imo.org/includes/blastDataOnly.asp/data_id%3D9179/ILOIMOCODEDRAFTmesshp-cp-aEnglish.pdf [accessed 7 May 2008].

Kersten, W., Böger, M., Hohrath, P., Späth, H., 2006. Supply Chain Risk Management: Development of a Theoretical and Emperical Framework. In: Kersten, W., Blecker, T., eds. *Managing Risks in Supply Chains, How to built reliable collaboration in logistics.* Berlin: Erich Schmidt Verlag GmbH & Co, 3-18.

Knoflacher, H., Pfaffenbichler, P.C., Nussbaumer, H., 2002. Quantitative risk assessment of heavy goods vehicle transport through tunnels – the Tauerntunnel case study. *Proceedings of 1st International Conference Tunnel Safety and Ventilation*, NA. April 8-10 (Graz, Austria).

Minor, J., 2005. *Protecting Supply Chains Against Political Risks*. Aon Political Risk Service, Aon Trade Credit. Available from: http://www.aon.com/about/publications/pdf/issues/Supply_Chain_Risk_2005.pdf [accessed 23 October 2007].

Riley, J., 2004. *Terrorism and rail security*. RAND Corporation. Available from : http://www.rand.org/pubs/testimonies/CT224/index.html [accessed 20 March 2008].

Seidelmann, C., 2007. Developing and Implementing global interoperable standards for container security. In: Bichou, K., Bell, M.G.H., Evans, A., eds. *Risk management in port operations, logistics and supply-chain security*. London: Informa, 55-60.

UIRR, 2007a. *UIRR Risk Analysis, Guidelines for Combined Transport Terminals.* International Union of combined Road-Rail transport companies. Available from: http://www.uirr.com [accessed 12 July 2007].

UIRR, 2007b. *UIRR Recommendations on improving Security in Combined Transport.* International Union of combined Road-Rail transport companies. Available from: http://www.uirr.com [accessed 12 July 2007].

Volpe National Transportation Systems Center, 2003. *Risk assessment and prioritization*. Volpe Center: Volpe Journal 2003. Available from: http://www.volpe.dot.gov/infosrc/journal/2003/pdfs/chap1.pdf [accessed 14 May 2008].