# A Risk Assessment Framework For Interconnected And Interdependent Surface Transport Networks

George Leventakis
Dept. of Information & Communication Systems Engineering, University of Aegean; Center for Security Studies (KE.ME.A.)
gleventakis@kemea.gr

Athanasios Sfetsos
Environmental Research Laboratory, Institute for Nuclear and Radiological Sciences, Energy, Technology and Safety, NCSR "Demokritos"
ts@ipta.demokritos.gr

Nikolaos Moustakidis
Environmental Research Laboratory, Institute for Nuclear and Radiological Sciences, Energy,Technology and Safety, NCSR "Demokritos"
nmoustakidis@gmail.com

Nikitas Nikitakos
Department of Shipping Trade and Transport, University of Aegean
nnik@aegean.gr

DOI 10.5592/otmcj.2013.3.6
Research paper

**Keywords**

Critical Infrastructure, Interdependencies, Risk Assessment, Network of Networks

THE FUNCTIONING AND VIABILITY OF MODERN SOCIETIES IS HEAVILY DEPENDED UPON THE CONTINUOUS AND UNINTERRUPTIBLE OPERATION OF CRITICAL INFRASTRUCTURES. Surface transportation systems are in the heart of the daily lives of millions of citizens globally. As such, they are open and freely accessible by design and in the past have been exploited for terrorism attacks.

Like many critical infrastructures, different multimodal and heterogeneous transportation networks are interconnected as integral part of larger synergistic systems forming a "network of networks". These underlying and often concealed interconnections between network assets enable adverse effects to manifest at assets that are initially unaffected by a security incident. The present paper introduces a holistic Risk Assessment Framework for heterogeneous, transportation networks that is applicable at a strategic level, where risk is propagated between interconnected networks through an "Incident Propagation Matrix" taking into account the nature of the interconnection and the type of threat. The proposed methodology views and models the risk analysis process from the perspective of the network operator and emergency responders and emphasizes the reduction of the impacts on business continuity.

## Introduction

Transportation is at the heart of everyday life of citizens and a fundamental aspect of the modern economy. Based on recent data from (UITP, 2010) 60 billion passenger journeys were made by public transport in 2008 in the EU-27. Worldwide terrorist incidents involve the transportation in more than half of the total number (Leung et al., 2004) and major incidents in the EU (such as the terrorist attacks on the Madrid commuter rail network in March 2004 and the London underground and bus bombings of July 2005) serve to emphasize the simple fact that assets of the transportation system are extremely attractive targets: largely prominent, carry large numbers of commuters, and very accessible. Networks of buses, trains, light rail and metros are increasingly physically integrated with each other, with other transport modes such as main lines rail and air travel, and with other economic activities and support the uninterrupted progress of mass events, forming synergistic "network of networks", that are combined in the transport of passengers and good. An attack on a specific transportation asset is likely to impact the entire "network of networks" within which it resides, since it can have swelling-effects and cascading failures.

Despite the fact that surface transport security issues are very similar across all counties, there is a remarkable gap in the derivation of a commonly agreed risk assessment framework and a common concept of operations. Following the EC Critical Infrastructure Protection Programme (Directive 114/2008/EC), and an initial reaction, security provisions in surface transportation systems have returned to being a limited priority. The proposed strategic risk analysis framework could be considered a small yet decisive step towards the development of a common and harmonized security risk assessment process for surface transportation systems.

Risk Analysis is a continuously changing process where threats are evolving and more sophisticated technological solutions are used to exploit system vulnerabilities. Furthermore, risk analysis becomes increasingly more complicated given the increased interconnectivity between heterogeneous critical infrastructures. In the vast majority of cases the number of such risks is large enough for the need for aggregation, filtering and ranking to arise (Berdica, 2002 and Morgan, 2000). (Haimes, 2004) proposed a Hierarchical Holographic Model (HHM) to account for the interdependencies of the highway transportation system: Emergency Response and Recovery (ERR), Intermodal, Physical, Economic, Functional, and Users, pertaining to industry sectors that depend on the transportation infrastructure. (Ezell et al., 2000) augmented the HHM, considering a multitude of mathematical and conceptual models, each of them devoted to represent a particular aspect of the system: hierarchy, functions, components, operations etc.

(Haimes et al. 2001 and 2007) proposed inoperability input-output model for the analysis of how perturbations (e.g., willful attacks, accidental events, or natural disasters) to a set of initially affected sectors impose adverse impacts on other sectors, due to their inherent interdependencies. The Hierarchical Coordinated Bayesian Model (Yan et al., 2006) was developed as an analysis tool of sparse data inferencing extreme event likelihoods and consequences using hierarchical coordination. (Pant and al., 2011) described the interdependent adverse effects of disruptive events on inter-regional commodity flows resulting from disruptions at an inland port terminal, using a risk-based Multi-Regional Inoperability Input-Output Model. (Zhang and Peeta, 2011) proposed a generalized modeling framework that combines a multilayer network concept with a market-based economic approach to capture the interdependencies among various infrastructure systems with disparate physical and operational characteristics.

The DECRIS model (Utne et al., 2001) utilized experience from risk analyses within different critical infrastructures, to develop an all-hazard generic methodology suitable for cross-sector infrastructure analysis. A similar approach was derived in the COUNTERACT (COUNTERACT Consortium, 2009) EU funded project. Generic security guidance was developed, focused exclusively on terrorist threats, using a human intent specific method to assess risks, based on harm (effect) and availability (vulnerability/threat). The approach lacked a mechanism to transfer the results of multiple risk assessments into a higher (hierarchical) level, in addition to the interconnected aspect of different infrastructures.

The objective of the present work is to develop a comprehensive Strategic Risk Assessment Framework for surface transportation system taking into consideration that (a) interdependent and heterogeneous networks are interconnected and (b) that risk is propagated between them. The proposed framework attempts to build upon the existing operational risk analysis frameworks of transportation operators and from the organization of major events. It is designed to estimate risk in interconnected transportation networks and finally the estimation of a holistic risk in the network of networks.

## Strategic Risk Analysis Framework

The process to derive the strategic risk analysis framework (RAF) is presented schematically in Figure 1.

The proposed framework is comprised of four main phases:

**Phase 1: Assessment of present situation**, which includes the detailed specification and description of the interconnected transportation network (or network of networks) that is at risk.

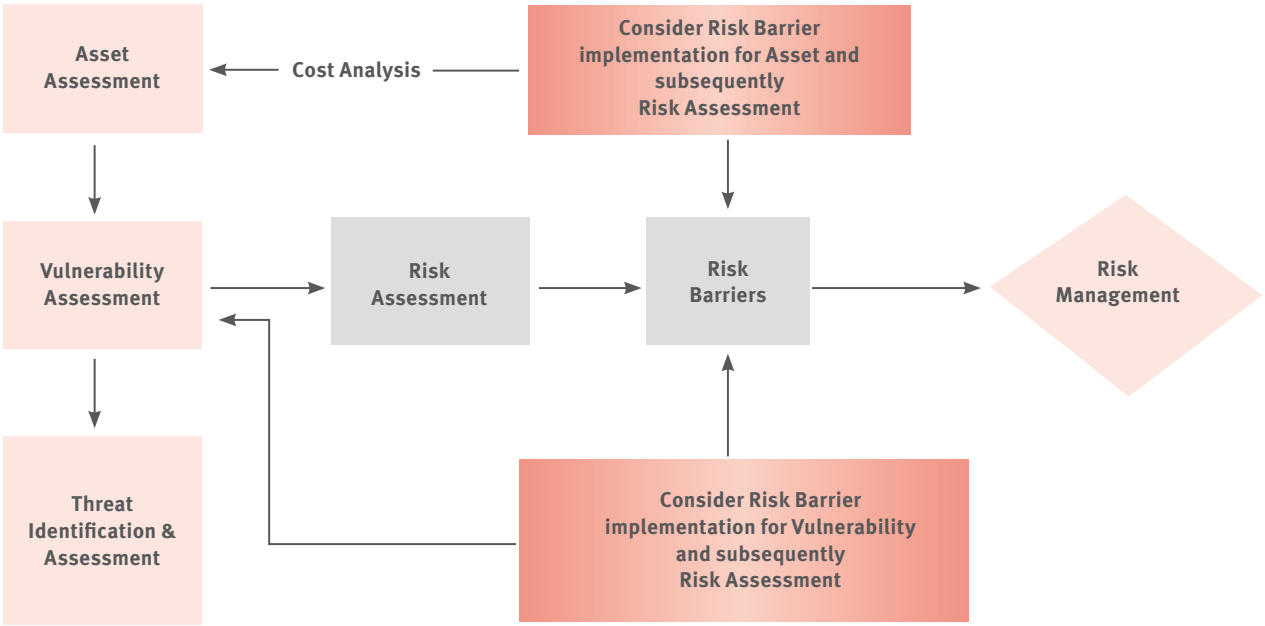



Figure 1. **Generic Strategic Risk Assesment Framework**

This is complemented by an exhaustive list of threat identification and assessment, and a vulnerability analysis to determine how these threats may be realized.

**Phase 2: Risk Assessment**, which will be determined by an estimation of the likelihood and consequences of an event. Using input from Phase 1, the risks will be propagated to interconnected transportation network assets, thus reaching

**Phase 3: Response procedures**, which includes specifying emergency response and business continuity operations.

**Phase 4: Risk mitigation**, which includes a determination to identify countermeasures and security upgrades that will lower the various levels of risk. These may include monitoring equipment, extending security perimeter, improving training of personnel, etc. A cost benefit analysis could be applied on an iterative process with the specified risk mitigation options to determine optimal ones.

## Network assets

The identification of the network assets is the first introductory step as it builds the foundations upon which relevant methodologies will be applied. Under the scope of the proposed RAF, an asset is considered as the basic unit of any transportation network, and in general the following basic principle is assumed: Each network will be decomposed into assets, i.e., objects with specific and easily recognized roles. A conceptual framework for categorizing assets within any transportation network is proposed:

**Direct assets**

- Passengers, goods, services relating to the motivation to transport
- Transport media (movable assets)
- Transport Infrastructure

**Indirect assets**

- Utilities, e.g. electricity, water
- Information, e.g. signals

**Auxiliary assets**

The major source of complexity in heterogeneous transport systems is defined by the way each asset affects the others as well as the intensity of that effect. All interdependencies can be categorized in he proposed RAF, based on the medium which each connection utilizes in order to manifest itself. These categories are (Rinaldi et al., 2001):

- ✓ **Physical Interdependency:** Two networks / assets are physically interdependent if the state of one is dependent on the material output(s) of the other.
- ✓ **Systems Interdependency:** Two networks / assets have a systems interdependency, if its state depends on the properties of a system transmitted through another asset.
- ✓ **Geographic Interdependency:** Networks / assets are geographically interdependent if an incident in an asset may impact the state of assets in a defined spatial proximity.
- ✓ **Logical Interdependency:** Two networks / assets are logically interdependent if the state of each depends on the state of the other via a mechanism that does not fall into any of the above.

## Threat definition

A threat is any factual or probable condition (incident, fact or occurrence) that can inflict harm or death to passengers, personnel, damage or loss of transport equipment, property or/and facility as well as undermining the positive image or prestige of the operator. Within the proposed RAF, a threat-risk

| Threat category | Threat subcategory | Threat category | Threat subcategory |
|---|---|---|---|
| Organized and non-organized criminal activity | Terrorism internal and international | Other | Abandoned objects (usual) |
| | Anarchism | | Abandoned objects (hazardous materials) |
| | Organized and common crime | | Resources deficiency |
| | Anti-social behaviour | | Panic without important cause (e.g., due to spreading of false news) |
| Mass Public Demonstrations/ Strikes (as a means of protest) | Demonstrations / public gatherings / strikes that turn violent | | Panic due to emergency (e.g., fire, earthquake) |
| Accidents/Random Events | Environmental accidents | Natural disasters | Extreme weather effects |
| | Technological accidents | | Geological effects |
| | Transportation accidents | | Hydro-geological effects |
| | Collapse of infrastructure | | Biological |
| Technological intrusion | Communication or computer hacking | Physicochemical disasters (Fires) | Fires |
| | SCADA | | Wildfires |

Table 1. **Threat categorization, related risks**

matrix composed of the vast majority possible risks for a certain type of threat that could adversely affect the transport network operation, has been identified (Table 1). For each identified risk a series of security incidents may be derived that would be the initiating mechanism of the proposed RAF, but are not introduced here due to space limitations.

## Risk assessment

Within the proposed framework, risk is evaluated from an iterative process assessing the probability of occurrence of the threat (Likelihood) and the Consequences in the event of a realization occurs. Figure 2 presents an analytical description of the proposed RAF, taking into consideration the main categories of Likelihood (Section 5.1) and Consequences (Section 5.2). The RAF has been designed to process diverse sources of information on:

- **An ordinal scale of 5 categories,** as is widely used in similar studies and operational procedures.
- **A numeric scale**; which is deployable in cases where extensive quantifiable data regarding the incident are available.

| Category | Very low | Low | Medium | High | Certainty |
|---|---|---|---|---|---|
| Scales | Intentional acts | | | | |
| Ordinal | Attack would require virtually unlimited resources | Attack very difficult to perform needing expert skills and money | Attack not easy but possible with expert skills and reasonable investment in time & effort | Attractiveness, lack of protection and attacker resources making the attack perfectly feasible | Attractiveness, lack of protection and, attacker resources making the attack ordinary |
| | Untargeted attacks or accidents | | | | |
| Ordinal | Extremely Unlikely. There is no history in the sector. | Not likely. It is very limited in the sector / environment. | Likely Similar events have been reported. | Very likely. Most of the sector has already suffered. | The event will happen in the organization in the immediate future. |

Table 2. **Likelihood categories and classification under RAF**

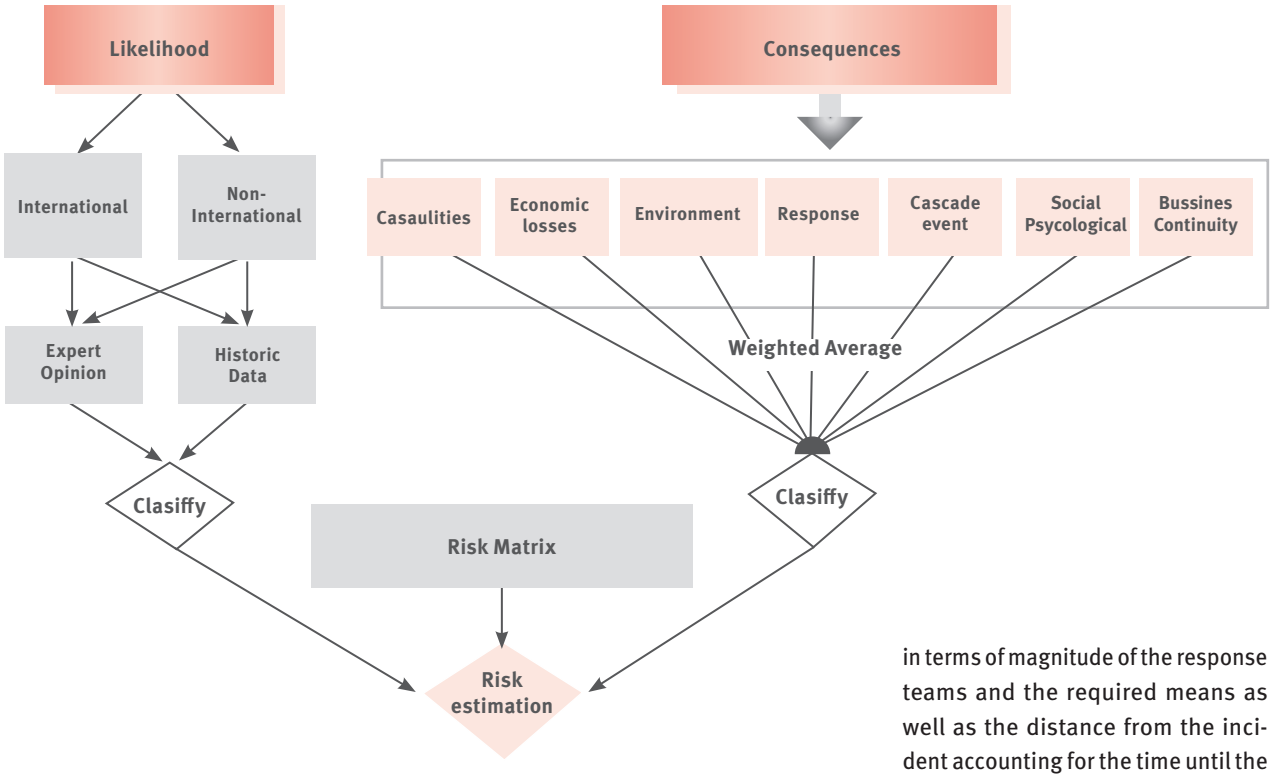



Figure 2. **General Risk (single asset) Assessment Framework Methodology**

## Likelihood

Likelihood is the frequency of occurrence of a particular threat. In a more generic approach it is expressed by the generic formula: *Likelihood = Intention to harm X Capability,* which is directly related to the carrier of the threat as well as the vulnerability of the target. Regarding the source of the threat, a distinction has been made between targeted/intentional and untargeted attacks. Finally a set of 5 different likelihood classes has been employed in the proposed RAF, described in Table 2.

## Consequences

Consequences are the result of the realization of a threat and defined as the harmful or damaging effects and can comprise physical harm, injury, death, loss, damage to property or revenue as well as loss in reputation and credibility of the company and of the transport system in general. The proposed approach estimates the consequences building upon a two level hierarchy. Level 1 is a generic category of consequences, quantified in a 5 class system (Negligible, Small, Medium, High, Severe), whereas Level 2 may have numerical / logic / categorical / binary / etc. values. In summary, the proposed consequence hierarchy is described in the following sections:

- **Casualties** include fatalities and injury to passengers, employees of the transport network and people in the affected area
- **Economic Losses** are estimated from a twofold impact that any security incident will have, (i) on the transportation network and (ii) on the economic activity levels that are affected by the incident on the transport network
- **Environmental / ecological impacts** that can be expressed in terms of the size of the impacted area, an indication of severity based on recovery time needed to fully restore the state of the environment in its previous state and as an indicator of the ecosystem and biodiversity at-risk.
- **Response to the incident**, assessed in terms of magnitude of the response teams and the required means as well as the distance from the incident accounting for the time until the units are deployed and become fully operational.
- **Cascading effects**, to interdependent critical infrastructures, the urban environment and even initiate natural hazards such as forest fires and flooding.
- **Social & Psychological impacts**, originating from the synthesis of factors affecting the capacity of society, as a whole, to operate at its normal level. It is composed by three distinct features: (i) the political impacts, (ii) reputation of the transport network and (iii) the psychological impact on the citizens and employees.
- **Business continuity**, accounting for: asset damage, loss of service, impact on personnel, etc

## Risk Assessment

The Risk Assessment Matrix is a classic tool to conduct semi-quantitative risk assessment, widely applied in many different frameworks (Markowski and Mannan, 2008). The output risk index is determined only by the mapping of the consequences and the likelihood to a single risk level, all of which can be divided into different levels.

| Very Low | Low | Medium | High | Critical |
|---|---|---|---|---|

Table 3. **Final risk classes**

| | Consequences | | | | |
|---|---|---|---|---|---|
| **Likelihood** | **Negligible** | **Small** | **Medium** | **High** | **Severe** |
| **Certainty** | Low | Medium | High | Critical | Critical |
| **High** | Very Low | Medium | Medium | High | Critical |
| **Medium** | Very Low | Low | Medium | Medium | High |
| **Low** | Very Low | Very Low | Low | Low | Medium |
| **Very Low** | Very Low | Very Low | Very Low | Very Low | Low |

Table 4. **Risk matrix**

Aggregating the risk between different levels is a crucial task that significantly tests the validity of the proposed approach. Although a variety of different options can be applied, the one selected here as returning the most reliable estimates is the Weighted Mean.

## Risk propagation

The core idea of the approach developed for modeling risk propagation in the framework is that a user defined security scenario which originates in an asset of any transportation network can cause diverse impacts and affect other interconnected assets or networks as shown in Figure 3.

**It builds upon the fundamentals of Markovian chain process, so that the state of a transportation asset will be dependent upon its previous state and/or the states of its interconnected assets.** The state of an interconnected asset (Xn) is thus a result of the nature of the incident affecting the originating asset, the characteristics of the asset under consideration (risk countermeasures, means of immediate response, etc.) and the type of interconnection between the assets.

Figure 4 presents an example of the interconnected transportation network assets to aid in understanding of the defined process. Here, there are two difference networks (A and B e.g. Metro and Tram) along with their respective assets (A1, A2, A3 and B1, B2, B3). There is also an additional asset (C1) which is a separate from the two networks (e.g. Power plant).

▶ **Step 1**: Scenario outline definition and description of the initial incident(s) that occur(s).

- The likelihood will be estimated depending on the nature of the incident (intentional or untargeted act/accident) to a five class estimate A1{L}.

- The consequences of the incident on the asset A1 will be defined using the proposed approach on the Level1/Level 2 hierarchy. A1{CL2} → Expert rules → A1{CL1} → weighted average → A1{C}

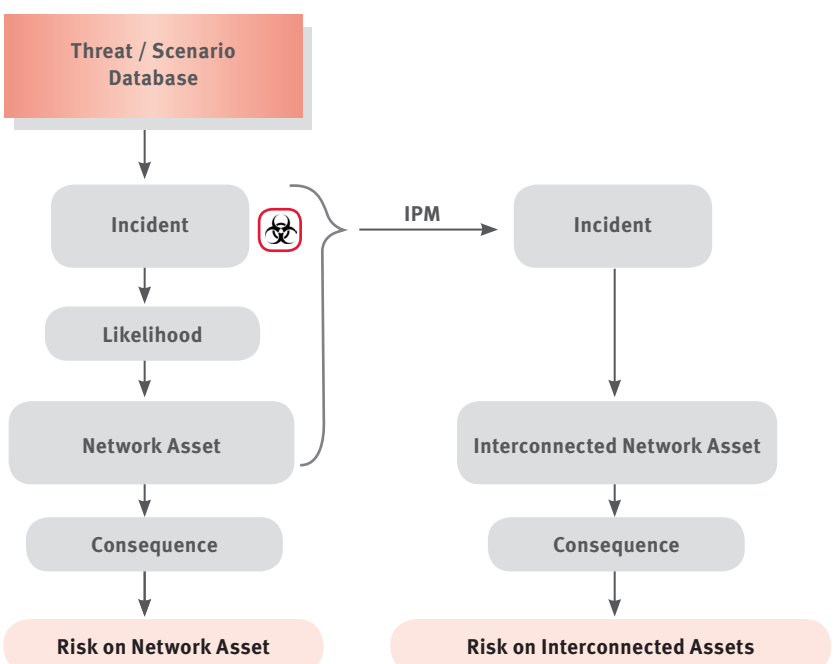
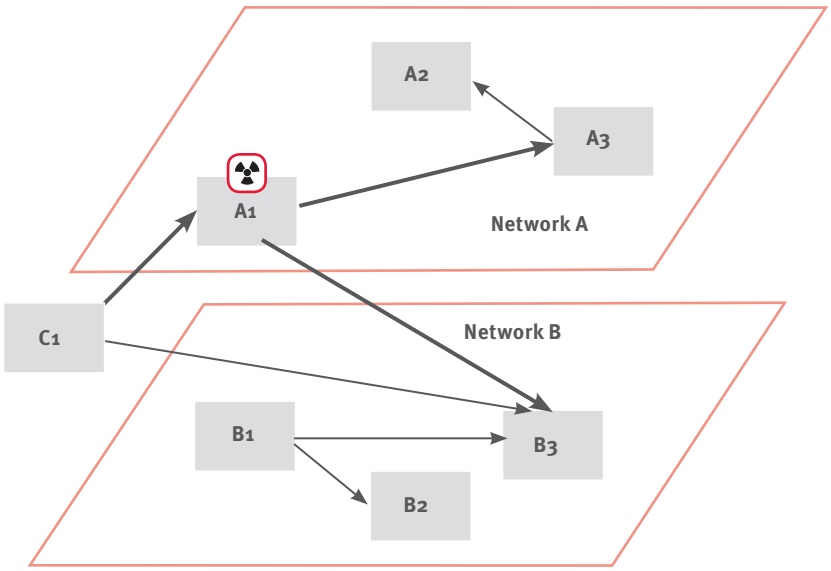



Figure 3. **Risk propagation process of the proposed approach**




Network A consists of assets Ai, which are interconnected.
Network B consists of assets Bi, which are interconnected.
Assets A1 is linked to asset B3 and both use the asset C1.

Figure 4. **Example of assets within interconnected networks**

▶**Step 2**: Estimate Risk of incident in the Asset A1.

This process involves the estimation of the Risk in the Asset A1 from the Risk Matrix based on the inputs A1{L} and A1{C}.

▶**Step 3:** Apply the response /business continuity procedures to the asset at risk

1. **Emergency response**. In order to account for the optimal response to the incident the following parameters must be defined: (i) the number and magnitude of responding teams, (ii) definition of the traffic cordon surrounding the incident area where all traffic is suspended
2. **Business Continuity**. The main target of the network operator and those closely affected by the security incident occurring at the asset at risk (A1) is to ensure the maximal possible continuation of the network operations.

Both procedures described will result in several assets of the network being considered as non-operational and a geographical interconnection established to the asset at risk.

▶**Step 4:** Determine the Assets that are interconnected to A1

The next step involves the process of identifying those Assets that will be affected by the impacts of the incident in asset A1. Thus the proposed approach is described from the following terminology: **"security incidents in an asset can trigger incidents in interconnected assets"**. In addition to interconnected assets, secondary incidents can be triggered on the same asset as well. To that end a separate Incident Propagation Matrix will be designed for each type of interconnection (Physical/System/Geographical/Logical).

▶**Step 5:** Estimate the probability of incident initiation at interconnected assets

This will be modeled through the definition of an Incident Propagation Matrix (IPM) which will evolve through a Markov chain process into the risk assessment procedure. Conceptually, the Incident Propagation Matrix (IPM) is a probabilistic input / output matrix where **inputs are the** security incidents and **output(s) are also security incidents,** on the immediately interconnected asset, with the exception of geographically linked assets. It shows in a consolidated form the probability of incidents triggering in linked assets resulting from the initial security incidents. These are derived from a stochastic process endowed with the Markov "memory-less" property in the sense that the possibility of subsequent incidents occurring on interconnected assets.

▶**Step 6:** Estimate Risk in interconnected asset

The Risk in the interconnected / linked asset(s) is estimated using the main approach (Steps 1 and 2). However, it has to be noted that: **The likelihood of the cascading incident equals to the defined probability value of the Markovian process estimated in step 5.**

▶**Step 7:** Incident termination

Subsequent incidents related to non-zero probabilities can never be brought down to zero since they are multiplied by also non-zero probabilities. This can cause an endless loop which practically serves no purpose other than overloading the system with insignificant incident occurrences. In order to alleviate this we set a probability threshold under which the calculated probabilities are considered to be practically zero and thus the incident propagation from that incident is effectively terminated.

## Risk Barriers

The effective risk assessment should consider a range of control measures (mitigation strategies) and additionally provide a basis for the selection of control measures. Risk control measures are relevant in all security phases, before, during and after a potential threat may be executed, i.e.

- **Preparedness** before a potential threat may be executed including preventive measures;

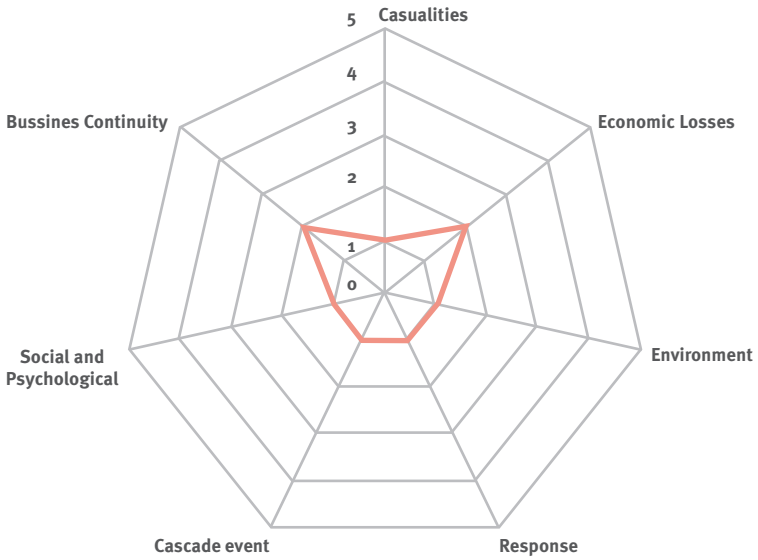



Figure 5. **Risk assessment in Metro & Suburban stations using classic approach**

- Capacity for **response**, relief and mitigation, during an incident;
- Capacity for **recovery** after an incident has occurred.

The most common control measures that should be evaluated in terms of

**a) Viability** that relates to the practicability of implementing the control measure within the facility; and

**b) Effectiveness** which is related to the effect of the control measure on the level of risk. For example, the reliability and availability of control measures influence the likelihood of an incident occurring, while the functionality and survivability of the control measures during the incident influence the consequences.

The evaluation of options for control measures within the proposed risk assessment framework should allow the determination of additional benefit gained from introducing additional or alternative control measures. The proposed approach is build on the capability to search for gaps in the existing control regime, where the introduction of further control measures may seems appropriate.

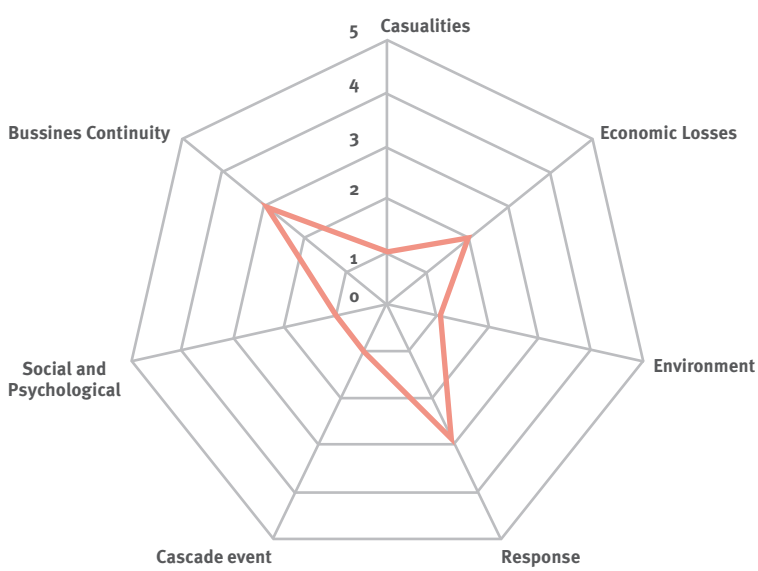



Figure 6. **Risk Spider plot for Metro / Suburban stations**

## Case Study

▶**Step 1:** Scenario outline definition and description of the initial incident that occurs: The incident is a "False bomb call" that can be classified in the Risk category "Hoaxes – Threats" further belonging in the "Man-made; Organized and non-organized criminal activity, Anti-social behaviour" category of threats. The incident was a "verified and assessed false bomb threat in the Plakentia station". The duration of the incident was approximately 3 hours.

▶**Step 2:** Estimate Risk of incident in the Asset A1: Therefore, both the metro (A1) and the suburban station (B1) in the Plakentia region are presumed to be the assets-at-risk. The Likelihood level of the incident has been denoted as MEDIUM (A1{L}), judging from historic data and opinion of experts.

Concerning the Consequences, the non Negligible categories were determined as: Response: three different response teams were called upon to intervene, Business Continuity : the stations were out of service for ~ 2 hours, and all passengers and transport flow were halted and stations were evacuated.

### *Classic Analysis*

Under the conventional analysis, the risk would have been estimated only in the asset / transport network at risk in a single step. Under a similar categorization in used for the assessment of risks, Fig 6 presents a synthesis of consequences occurring from this scenario, which fall under the NEGLIGIBLE category. The total risk is classified as VERY LOW and not any further risk propagation occurs to interconnected assets.

▶**Step 3:** Apply the response /business continuity procedures to the asset at risk:

*Proposed Method*

The weighted average of Consequences (Figure 6) resulted in the total estimate as a SMALL class and the application of the Risk Matrix under these categories returned an overall Risk as LOW.

▶**Step 4** Determine the Assets that are interconnected to A1: Asset B1 is interconnected to A1 through a physical interconnection.

▶**Step 5** Estimate the probability of incident initiation at interconnected assets: It is estimated through expert opinion that the probability of the hoax impacting B1 **after** it has already affected A1 is HIGH for assets that are physically interconnected. So using the same principle as in the Risk Matrix we combine the MEDIUM probability of A1{L} with the HIGH probability of B1|A1{L} into a MEDIUM probability for B1{L}.

▶**Step 6** Estimate Risk in interconnected asset: Repeat the same process as in step 2 and 3 for asset B1.

▶**Step 7** Incident termination:

No other interconnections or incidents of non-zero probability are considered for this example and so the incident terminates here.

## Conclusions

The present paper introduced a strategic risk analysis methodological approach that is applicable on surface transportation networks. The main advantage of the introduced approach lies with its inherent ability to estimate risk in interconnected and heterogeneous transportation networks based on a repetitive process of risk evaluation and assessment of severity, taking into account the Likelihood of occurrence and the Consequences on each interconnected asset. Furthermore, and in order to provide concrete decision support to the critical infrastructures operators risk mitigation options have been introduced.

The estimation of the Risk in assets either located away from the area where the incident occurred or belonging to a different transport network is a major advantage of the proposed approach, extending similar approaches found in the literature and are employed as operational by many transport operators.

The proposed approach is analytic enough to contain an exhaustive list of threats pertaining to transportation and also has an inherent framework to estimate the propagation of risk to interconnected transportation assets. Furthermore the developed approach is easily programmable in XML and/or UML languages and can easily provide interfaces for exporting data in GIS or other related formats.

## References


Berdica, K. (2002), "An introduction to road vulnerability: what has been done, is done and should be done", Transport Policy, Vol. 9, Iss. 2, pp. 117-127.

COUNTERACT Consortium (2009), "Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities", available at http://trainingsecurity.uitp-events-expo.org/sites/default/files/pdf/COUNTERACT%20Guidelines_lr.pdf/ (accessed 10 May 2012).

Ezell, B., Farr, J. and Wiese, I. (2000), "Infrastructure Risk Analysis Model", International Journal of Infrastructure Systems, Vol .6, Iss. 3, pp. 114-117.

Haimes, Y., J. Santos, K. Crowther, M. Henry, C. Lian and Yan, Z. (2007), "Risk analysis in interdependent infrastructures" in Goetz, E. and Shenoi, S. (Ed.), Critical Infrastructure Protection, Springer, New York, NY, pp 297-310.

Haimes, Y.Y. (2004), Risk Modeling, Assessment and Management, Wiley, New York, NY.

Haimes, Y.Y. and Jiang, P. (2001), "Leontief-based model of risk in complex interconnected infrastructures", Journal of Infrastructure Systems, vol. 7, pp. 1-12.

International Association of Public Transport, Financial and Economic Crisis - UITP (2010), "The Situation of the Public Transport Sector in EU 27" available at http://www.uitp.org/mos/positionspapers/95-en.pdf (accessed on 20/1/2011).

Leung, M., Lambert, J.H. and Mosenthal, A. (2004), "A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks", Risk Analysis, Vol. 24 No. 4, pp. 963–984.

Markowski, A.S. and Mannan, S.M. (2008), "Fuzzy risk matrix", Journal of Hazardous Materials, Vol. 159, pp. 152–157.

Morgan, M. G., Florig H. K., DeKay M. L. and Fischbeck, P. (2000). "Categorizing risks for risk ranking", Risk Analysis, Vol. 20 No. 1, p. 49.

Ouyang, M., Hong, L., Mao, Z., Yu, M. and Qi, F. (2009), "A methodological approach to analyze vulnerability of interdependent infrastructures", Simulation Modelling Practice and Theory, vol. 17, pp. 817–828.

Pant, R., Barker, K., Grant, F.H. and Landers, T.L. (2011), "Interdependent impacts of inoperability at multi-modal transportation container terminals", Transportation Research Part E: Logistics and Transportation Review, vol. 47 No.5, pp. 722-737.

Rinaldi S.M., Peerenboom, J.P. and Kelly T.K. (2001), "Identifying, understanding and analyzing Critical Infrastructure Interdependencies", IEEE Control Systems Magazine, Vol. 21, pp. 11 – 25.

Sandmann, W. (2007), "Rare Event Simulation Methodologies and Applications" Simulation, Vol. 83, pp. 809-810.

Utne, I. B., Hokstad, P. and Vatn, J. (2011), "A method for risk modeling of interdependencies in critical infrastructures", Reliability Engineering and System Safety, vol. 96 No. 6, pp. 671-678.

Yan, Z., Haimes Y.Y. and Waller, M. (2006), "Hierarchical coordinated Bayesian model for risk analysis with sparse data" presented at the Society of Risk Analysis, Annual Meeting, 3-6 December, Baltimore, Maryland, USA.

Zhang, P. and Peeta, S. (2011), "A generalized modeling framework to analyze interdependencies among infrastructure systems", Transportation Research Part B: Methodological, Vol. 45 No. 3, pp. 553-579.


## Acknowledgements


The authors acknowledge partial funding by the EC under Grant Agreement No 225594 (STAR-TRANS).