International Journal of Transportation
Vol.2, No.3 (2014), pp.95-116
http://dx.doi.org/10.14257/ijt.2014.2.3.06

Strategic Concept for the Protection of Regionally Interconnected Surface Transportation Networks

George Leventakis[1], Athanasios Sfetsos[2,] Nikolaos Moustakidis[2*], Nikitas Nikitakos[3]

[1]Dept. of Information & Communication Systems Engineering, University of Aegean, Center for Security Studies (KE.ME.A.)
[2]Environmental Research Laboratory, Institute for Nuclear and Radiological Sciences, Energy, Technology and Safety, NCSR "Demokritos"
[3]Department of Shipping Trade and Transport, University of Aegean
gleventakis@kemea.gr, **ts@ipta.demokritos.gr, nmoustakidis@gmail.com, nnik@aegean.gr*

Abstract

Surface transportation systems crucially define the daily functionality and operations of modern societies: they are utilised by millions of commuters worldwide, on a daily basis. As such, they are open and freely accessible by design and in the past have been exploited for malicious purposes and have also been severely disrupted by natural phenomena. Like many modern critical infrastructures, multimodal and heterogeneous transportation networks are interconnected as integral part of larger synergistic systems forming a "network of networks".

The present manuscript introduces a holistic concept for the protection of heterogeneous transportation networks that is applicable on a strategic level. The basis of the proposed model is the concept that security incidents may be propagated between assets of interconnected networks. The proposed methodology emphasizes the strategic level protection both from the perspective of the network operator and the emergency responder, linking all phases of the disaster cycle into a unique concept of operations.

Keywords: *Surface Transport, Network of Networks, strategic protection*

1. Introduction

Transportation is at the heart of everyday life of citizens and a fundamental aspect of the modern economy. Based on UITP data [1] 60 billion passenger journeys were made by public transport in 2008 in the EU-27. Worldwide, terrorists have targeted the transportation sector in more than half of the total intended attacks [2] and major incidents in the EU during the last decade (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.

Historically, the design and operation of transportation systems accounts for natural and accidental failures, but place little or no emphasis on protection against security incidents [3]. 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.

ISSN: 2287-7940 IJT

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 protection 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 protection 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.

The unification of the crisis phases, Figure 1, will ensure effective and faster response: Early awareness from multiple fused data sources, increased readiness, education and training, reduced risk to emergency responders by providing accurate and timely coherent information relating to hazards and risks. The proposed work however is focused on the development of a consolidated risk assessment and risk management plan for interconnected transportation systems linked to coherent contingency planning.

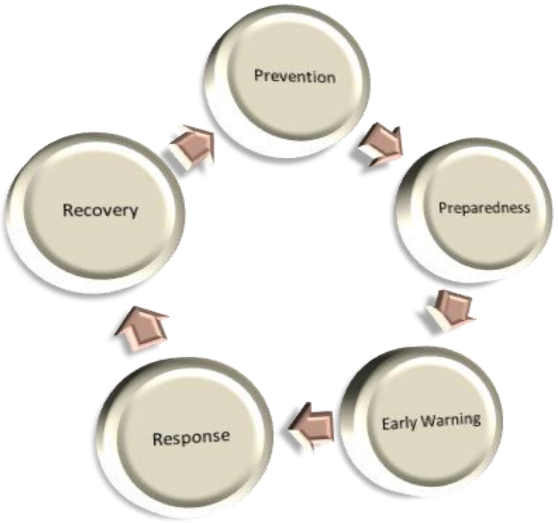


Figure 1. Phases of the Crisis Cycle

Risk Analysis is a continuously adaptive process where threats are evolving and more sophisticated technological solutions are used to exploit system vulnerabilities. The US Department of Transportation [4] employed a vulnerability assessment methodology, based on identifying critical assets and associated risk scenarios. Countermeasures to deter, detect and delay the possible attacks were developed and compared based on their estimated costs. Haimes [5] 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.

In recent years, many researchers have tried to accommodate the complex interconnections of modern critical infrastructures and cascading events into a holistic risk analysis process.

Earl *et al.*, [7] and Rosato *et al.*, [8] applied complex network theories, whereas the introduction of not only abstract interdependencies but also selected properties of infrastructure types such as buffering of resources were proposed. Sandmann [9] proposed stochastic models of networks covering a broad field of models and tools that might be applicable to (inter-) dependency modelling. Eusgeld *et al.*, [10] emphasized the importance of potential failure propagation among infrastructures leading to cascades affecting all supply networks, presenting a systems-of-systems (SoS) approach. A Complex Network theory based topology-driven method was presented [11] to comprehensively analyze the vulnerability between interdependent infrastructures.

Haimes *et al.*, [12] proposed the inoperability input-output model for the analysis of the manner in which perturbations (*e.g.*, intentional 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 [13] was developed as an analysis tool of sparse data which can be used to infer extreme event likelihoods and consequences using hierarchical coordination. Pant and al [14] 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 [15] 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.

Casalicchio *et al.*, [16] proposed an agent-based modelling and simulation solution for critical interdependence modelling. The approach, named Federated-ABMS, relies on discrete agent-based modelling and simulation and federated simulation. It provides a formalism to model compound complex systems, composed of interacting systems, as federation of interacting agents and sector specific simulation models. Balducelli [17] developed interacting agents for modelling the discrete event simulation as a tool to approach interdependencies analysis and evaluation for critical infrastructures.

The DECRIS model [18, 19] drew upon the experience obtained from the application of 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 [20] EU funded project. A generic security guide was developed which was 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. Additionally, EURAM [21] built a basic common methodology for the analysis of interdependencies between Critical Infrastructures (CI) of the same sectors and between CI of different sectors and different countries.

The above approaches are very useful within their particular scope and frame of application. However, a gap that becomes visible is the lack of a generic and widely applicable risk assessment framework that can incorporate the concept of asset interconnection (and consequently the concept of network interoperability) into a holistic and integrated semi-empirical approach capable of being bringing together a broad range of networks (transport, energy, cyber, etc.), infrastructures (including critical ones) and response policies.

The specific objective of the present work is to develop a comprehensive Strategic Risk Assessment Framework for interconnected 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.

2. Strategic Risk Analysis Framework

The process to derive the strategic risk analysis framework (RAF) is presented schematically in Figure 2. Its general principles follow a well-established path that has been followed in related literature, *e.g.*, [12, 17, 18, 19], and in related funded studies (*e.g.*, COUNTERACT [20], EURAM [21]).

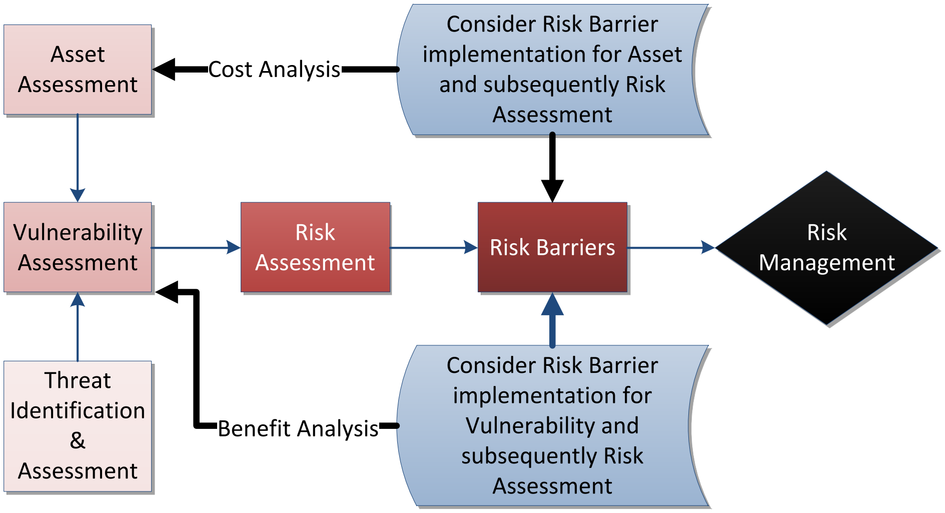

Asset Assessment
Cost Analysis
Consider Risk Barrier implementation for Asset and subsequently Risk Assessment
Vulnerability Assessment
Risk Assessment
Risk Barriers
Risk Management
Threat Identification & Assessment
Benefit Analysis
Consider Risk Barrier implementation for Vulnerability and subsequently Risk Assessment

Figure 2. Generic Strategic Risk Assessment Framework

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. 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 that could allow for optimal routing algorithms, evacuation routes and replacement services.

Phase 4: Risk mitigation, which includes a determination is to identify countermeasure / 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.

The main benefit of the proposed framework in comparison to existing approaches is the combination of the below elements:

- A risk analysis and assessment methodology for ground transports at a strategic level.

- Response measures and procedures integration.
- Transition from a single infrastructure modelling to a holistic "network-of-networks" model.
- Compatibility with the EU Directive 114/2008 regarding the European Critical Infrastructure Protection Programme.
- Extendibility to various types of critical infrastructures.
- Ability to incorporate framework to a risk assessment IT tool.

3. 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.

In response to this approach, a conceptual framework for categorizing assets within any transportation network is proposed comprising of:

- 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. An important step in understanding and consequently modelling that relationship is to first identify all possible expressions and variations of the so-called "interdependencies" which link together assets. All interdependencies can be categorized in he proposed RAF, based on the medium which each connection utilizes in order to manifest itself. These categories according to [22] are:

- ✓ **Physical Interdependency**: Two networks / assets are physically interdependent if the state of one is dependent on the material output(s) of the other. This sort of interdependency is realized when a physical linkage between the assets exists.
- ✓ **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.

4. 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. In order for the attack or incident to inflict a measured impact on the transportation network, certain vulnerabilities of the assets (*e.g.*, security flaws, operational, functional, by design) must be exploited. These, on a second stage, should be exhaustively analysed by the security officers and risk managers of the transportation network, and be used to define appropriate countermeasures and security policies that would considerably reduce the risk impacts.

Within the proposed RAF, a threat-risk 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 1a/b). 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.

Table 1a. Intentional Incidents: Threat Categorization, Related Risks

Threat category	Threat subcategory	Risk
Organized and non-organized criminal activity	Terrorism internal and international	Bombing
		Armed assault
		Robbery
		Kidnapping
		Arson
		Sabotage
		Hacking
		Dangerous mail
		CBRN
		Suicide missions
	Anarchism	Assault
		Bombing
		Arson
		Sabotage
		Kidnapping
		Seizure
	Organized and common crime	Kidnapping
		Seizure
		Homicide
		Riots
		Robbery
		Smuggling
		Infrastructure damage (direct/indirect)
	Anti-social behaviour	Infrastructure damage

		Suicide
		Violence
		Hoaxes – Threats
Mass Public Demonstrations/Strikes (as a means of protest)	Demonstrations / public gatherings / strikes that turn violent	Seizure
		Violence
Accidents/Random Events	Environmental accidents	Pollution
	Technological accidents	Fire
		System failures
	Transportation accidents	Vehicle accidents
	Collapse of infrastructure due to:	Natural Disasters
		Problematic infrastructure
		Error
		Intentional harm
Technological intrusion	Communication or computer hacking	Tampering
		Loss of communication
		Viruses
		System Failure
Other	Abandoned objects (usual)	Losses
	Abandoned objects (hazardous materials)	Presence of hazardous material
	Resources deficiency	Lack of personnel
		Lack of equipment
		Lack of resources
	Panic without important cause (e.g., due to spreading of false news)	Injury
		Spoilage of operator property
		Business continuity loss
	Panic due to emergency (e.g., fire, earthquake)	Rescue obstruction

Table 1b. Non-Intentional Incidents & Accidents: Threat Categorization, Related Risks

Natural disasters	Extreme weather effects	Damage due to weather
	Geological effects	Damage from geological incidents
	Hydro-geological effects	Flooding
	Biological	Illness spread
Physicochemical disasters (Fires)	Fires (depending on the asset at risk)	Fire
	Wildfires	

5. Risk estimation

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 3 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. The utilized subjective classification may be relying on expert judgment judgment and/or assessment based on records of past incidents.

- **A numeric scale**; which is deployable in cases where extensive quantifiable data regarding the incident are available.

The advantage of the proposed approach is that for the estimation of risk, any type of information may be employed combining related scales in order to accurately estimate risk.

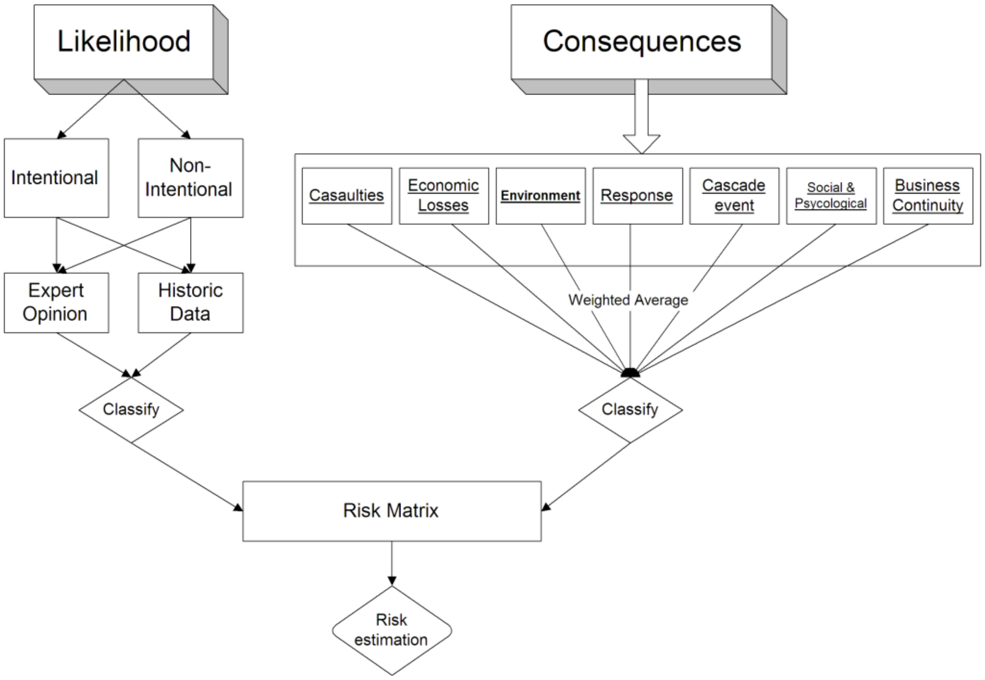


Figure 3. General Risk (Single Asset) Assessment Framework Methodology

5.1. 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.

The proposed framework has an additional advantage of a common quantification of different threats, under a common scale. This was deduced from the frequency of occurrence depending on whether the threat under examination was a result of intentional (or not) human activity or a naturally occurring hazard. Finally a set of 5 different likelihood classes has been employed in the proposed RAF, described in Table 2.

Table 2. Likelihood Categories and Classification under RAF

Category	Very low	Low	Medium	High	Certainty
Scales	**Intentional acts**				
Ordinal	Attack would require virtually unlimited resources	Attack very difficult to perform needing conjunction of 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
Cardinal	Never or once	Handful during the operation	Occasionally during the operation	Once a week	Once a day
	Untargeted attacks or accidents				
Ordinal	Extremely Unlikely. There is no history in the sector / environment.	Not likely. It is very limited in the sector / environment.	Likely Similar events have been reported in other organizations of the sector / environment.	Very likely. Most of the sector / environment has already suffered such situations.	The event will happen in the organization in the immediate future.
Cardinal	Can occur only in rare / special occasions	1 occurrence every 5-10 years	1 occurrence every year	1 occurrence every 6 months	1 occurrence every 3 months

5.2. 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. A detailed analysis of the consequences is presented in the work of Leventakis *et al.*, [23].

5.3. Business Continuity

According to [24], business continuity planning is the process of identifying critical systems, identifying reasonable threats, and creating a long-term strategy for reducing the impact of interruptions to the business and stabilizing critical business functions. It consists of several tasks that together constitute a set of integrated procedures to minimize the impacts of a security incident, ensuring operations remain viable. For the purposes of the proposed RAF, the business continuity approach is multi-dimensional meaning that consequences have been accounted for:

1. Damage to the asset, quantified in the linguistic terms.
2. Loss of service, quantified numerically, which can be associated with
3. Impact on personnel, that are incapable of participating in the business as usual operation
4. A numeric indicator of passengers unable to use the asset at risk
5. The impact on the network flow evaluated in relative terms

Table 3. Proposed Quantification of Business Continuity Impacts

	Damage	Loss of service	Impact on personnel	% unable to use asset	impact on flow	Service replacement
Negligible	Negligible	less than 1 hour	Negligible	Few	Business as usual	None
Small	Very small damage	1 hour - 6 hours	20-50% up to 15 days	5 - 10%	Short delays	Within 1 hour
Medium	Small damage	6 hours - 1 day	20-50% up to 1 month	10 - 20%	Severe delays	Within 6 hours
High	Partial damage / severe damage	Up to 1 month	20-50% up to 2 months	20 - 50%	Route alteration / replacement	Within days
Severe	Collapse / permanent damage	1 year	More than 50% for 2 months	More than 50%	evacuation / out of service	Special arrangements

The proposed surface transportation risk analysis framework has the inherent ability to propagate risk in interconnected assets, employing the proposed Impact Propagation Matrix (IPM) which will be extensively analysed in Section 6. However, there is the additional capability to account for the impact (i) in the network operation containing the asset at risk and (ii) in the entire “network of networks” of a region employing a similar perspective as the one summarized in Table 3, displayed in Figure 4.

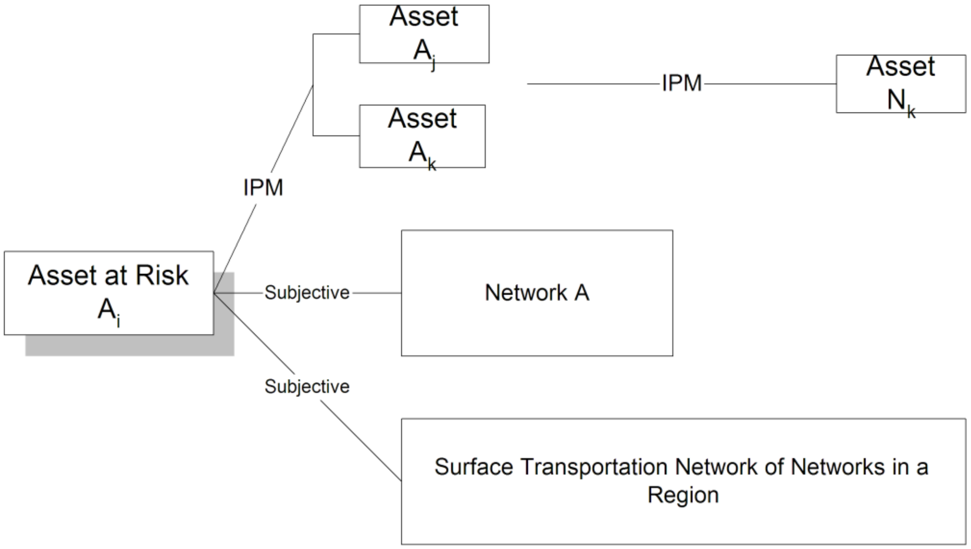


Figure 4. Schematic Alternatives for Risk Estimation

5.4. Risk Estimation

The Risk Assessment Matrix is a classic tool to conduct semi-quantitative risk assessment, widely applied in many different frameworks [25, 26]. Some basic principles that were adopted within the present RAF that 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, respectively, with qualitative descriptions and scales (Tables 4,5).

Table 4. Final Risk Classes

Very Low	Low	Medium	High	Critical

Table 5. Risk Matrix

	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

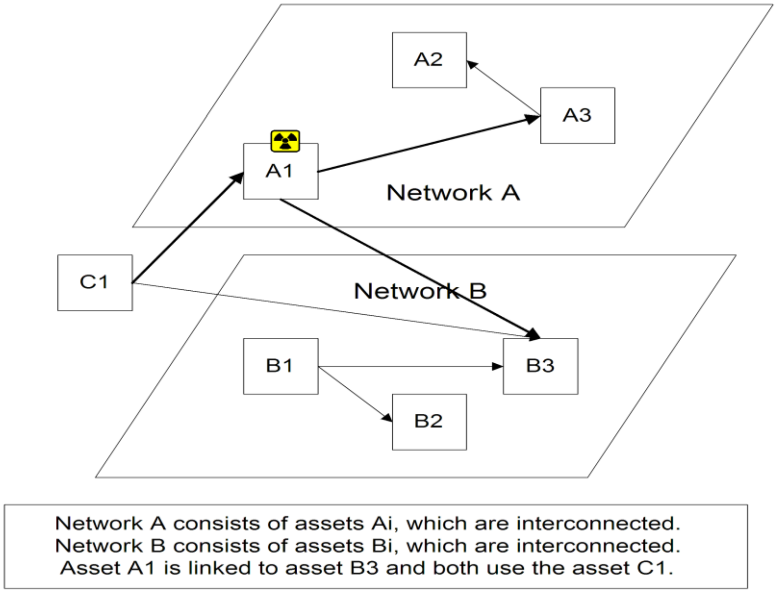
<Table 5>

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. A subjective assignment of weights (wi, summing to 100%) can be assigned to the different classes based on their presumed significance, whilst some maybe be ignored. By assigning individual impact rating to ordered numbers (xi) the final value may be estimated as $R_i = \frac{\sum_i w_i x_i}{\sum_i w_i}$.

6. 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. 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 5, presents an example of the interconnected transportation network assets (which in generalization A and B may be heterogeneous transportation networks), to aid in understanding of the defined process.



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

Figure 5. Example of Assets within Interconnected Networks

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

First and foremost, it is important to define the initial incident(s) in terms of the nature, likelihood and possible impact as proposed in the risk analysis framework. Let us make the assumption that the security incident occurs in Asset A1. More specifically:

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}

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

This process involves the estimation of the Risk in the Asset A1from the Risk Matrix based on the inputs A1{L} and A1{C}.

Step 3: Apply the response procedures to the asset at risk

These will be enforced in order to account for the optimal response to the asset-at-risk, ensuring that disruptions to the network services are minimized. They can be classified into:

i. **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) the optimal routing of the responding entities from their initial locations to the incident which may require blockage / prioritizing of roads, (iii) definition of the traffic cordon surrounding the incident area where all traffic is suspended, (iv) optimal routing to nearest hospitals for treating of injured citizens.

ii. **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. In order to achieve this, it would acceptable to suspend a part of the network operations or adapt to the rapidly changing conditions.

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. Within the proposed framework these tasks are aided by the introduction of the VISTA Dynamic Traffic Assignment model.

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. The new set of assets-at-risk, i.e. those linked to A1 by any type of linkage, will be determined by (i) the type and nature of the initial incident, (ii) the type and characteristics of the interconnection between the assets. Thus the proposed approach is described from the following terminology: “security incidents in an asset can trigger incidents in interconnected assets”. This concept also accounts for the geographically interconnected assets defined in the previous step accounting for the response procedures. 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).

Additionally, due to the highly interconnected properties and functionality of the operation of the network asset, it is anticipated that the security incident in any asset, may trigger a different security incident in the same asset, thus establishing a self-interconnection.

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.

The matrix contains either continuous probability values in the range of [0,1] or a five class likelihood values in every cell indicating the likelihood of triggering an incident in an interconnected asset (column) caused by the incident affecting the initial asset (row). These probabilities 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 in based entirely upon the original incident and not any previous incidents preceding it as shown in the definition below:

P (Incident k occurring at asset l after incident i has previously occurred at interconnected asset j) = $P_{(kl)(ij)}$ = $P_{ijkl.}$

P_{ijkl} = F(Pairings of assets, Security incidents, Interconnection type, Asset characteristics)

As triggered incidents are occurring at interconnected assets the likelihood of subsequent incidents is calculated based on the probability of the previous incident multiplied by the probability of the current incident occurring, given that the previous incident has already occurred. This is based on the definition of the conditional probability formalized as such: $P(B \cap A) = P(B|A)P(A)$.

Where A is the generating incident and B is the current incident considered to happen, P(B∩A) is the probability of both A and B occurring and P(B|A) is the conditional probability of B occurring after A. In order for this principle to be applicable in cases where 5-level scale likelihoods are used we introduce the "Likelihood Matrix" which is the tool used to map the probabilities of the initial incident and the conditional probability found in the IPM to the probability of both incidents occurring.

Table 6. Likelihood Matrix

Likelihood Category	Very Low	Low	Medium	High	Certainty
Very Low	Very Low	Very Low	Very Low	Very Low	Very Low
Low	Very Low	Very Low	Very Low	Low	Low
Medium	Very Low	Very Low	Low	Low	Medium
High	Very Low	Low	Low	Medium	High
Certainty	Very Low	Low	Medium	High	Certainty

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 4**.

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.

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

The introduction of a suitable methodology may lead to a combined approach for (i) optimise the use of resources, (ii) determining the effectiveness and costs of different control options, (iii) improving the overall decision-making process and (iv) providing a basis for allocating resources in the most effective manner. The risk assessment process should provide the following in relation to control measures:

a) identification or clarification of existing and potential control measure options;

b) evaluation of effects of control measures on risk levels (likelihood / impact / interconnection);

c) basis for selection or rejection of control measures and the associated justification of adequacy; and

d) basis for defining performance indicators for selected control measures.

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. Table 7 introduces a non-exhaustive list of risk control options currently applied in surface transportation systems.

Table 7. Risk Control Measures

Design Principles

- Transparency (i.e. clear sightlines)
- Clearing out (e.g. by removing unnecessary furniture, vending machines, etc.)
- Improvement of lighting levels
- Etc.

Equipment
Fire protection (including direct fire protection, ventilation, etc.)
Operational standards/Instructions/Guidelines
Collaboration agreements
Line of communication • Internal • External
Crisis communication
Overall preparedness plan as well as Contingency planning with detail
Crisis management group/structures
Evacuation • Rules & procedures • Training & exercises
Training/Education of operational staff
Exercises (tabletop / real)

7.1. Risk Barrier Modelling

In order to incorporate the notion of Risk Control Measures (RCM) in the overall risk assessment process a Risk Mitigation Matrix (RMM) was introduced into the framework. This is a two-way matrix used to adjust the initial likelihood and/or consequence estimation of a threat on an asset based on the available pro-active measures in place that can lower the likelihood of a threat, its consequences or both. The columns of the matrix represent the different levels of effectiveness of the overall risk control measures and range from "Ineffective" to "Very Effective". The initial level estimated for the likelihood or consequence (rows) may be decreased by a varying number of levels based on the effectiveness of the risk control measures. The output of the matrix (cells) represents the revised likelihood or consequence level estimation for the specific threat on the asset in question taking into account all relevant risk control measures.

Table 8. Likelihood / Consequence Mitigation Matrix (LMM/CMM)

	Risk Control Measures Effectiveness					
Initial Likelihood / Consequence Estimation		Very Effective	Effective	Somewhat effective	Limited effectiveness	Ineffective
	Certainty	Very Low	Low	Medium	High	Certainty
	High	Very Low	Very Low	Low	Medium	High
	Medium	Very Low	Very Low	Very Low	Low	Medium
	Low	Very Low	Very Low	Very Low	Very Low	Low
	Very Low	Very Low	Very Low	Very Low	Very Low	Very Low

7.2. Risk Propagation with Barriers

A similar approach is applied but the previously mentioned but the specifically selected mitigation measures are applied either on the asset at risk either at any asset of the network of networks.

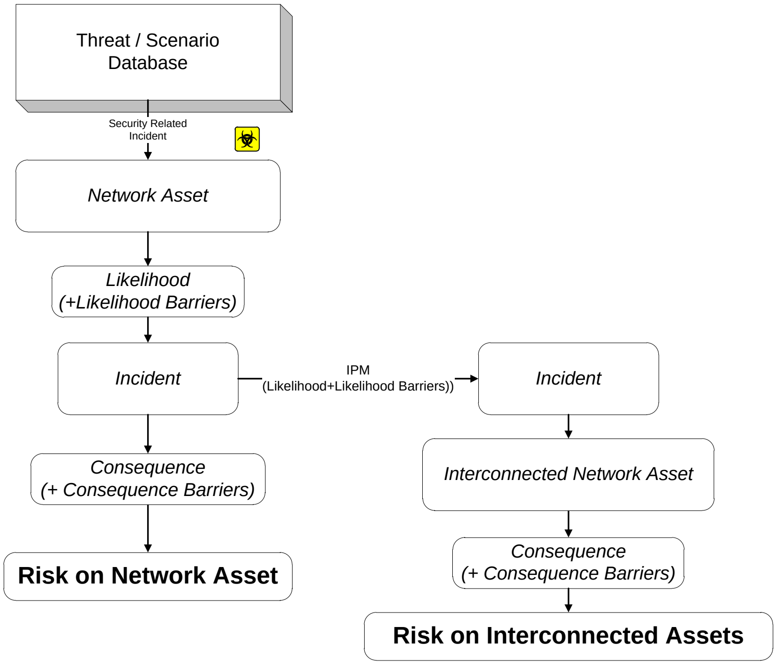

Threat / Scenario Database
Security Related Incident
Network Asset
Likelihood (+Likelihood Barriers)
Incident
IPM (Likelihood+Likelihood Barriers))
Incident
Consequence (+ Consequence Barriers)
Interconnected Network Asset
Risk on Network Asset
Consequence (+ Consequence Barriers)
Risk on Interconnected Assets

Figure 6. Risk Mitigation Introduction in the Risk Assessment Process

Step 1: Scenario outline definition and description of risk mitigation measure (if applicable).

First and foremost, it is important to define the risk mitigation in terms of its properties, (effectiveness, costs) as proposed in the risk analysis framework. Once these are defined then the likelihood mitigation matrix will be estimated

Obtain a five class estimate of the likelihood AM1{L} which is found from the product of the initial matix A1{L} and the likelihood mitigation matrix

$AL1\{L\} = A1\{L\} \times LMM$

The consequences of the incident on asset A1 will be modified with the Consequence Mitigation Matrix, provided that the respective risk control measure influences at least one consequence category

$AM1\{CL1\} = A1\{C\} \times CMM$

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

The Risk is estimated from the Risk Matrix based on the inputs AM1{L} and AM1{C}.

Step 3: Apply the response procedures to the asset at risk

Step 4: Determine the Assets that are interconnected to A1

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

Step 6: Estimate Risk in interconnected asset

Again the IPM will be modified according to the LMM so that probabilities to have an updated value based on the parameters that define the risk control option. This process is applicable only if a suitable control measure is selected.

Step 7: Incident termination

8. Case Study

The following section introduces the application of the developed framework on a case study concerning a major transportation hub in the region of Attica Greece. The hub features a suburban railway station, an underground metro station and multiple bus stops. The incident used 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”, without any further specifications. The duration of the incident was approximately 3 hours.

8.1. Example Scenario

Therefore, both metro and suburban stations are presumed to be the assets-at-risk. The Likelihood level of the incident has been denoted as MEDIUM, 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 7 presents a synthesis of consequences occurring from this scenario, which fall under the VERY LOW category. The total risk is classified as LOW and not any further risk propagation occurs to interconnected assets.

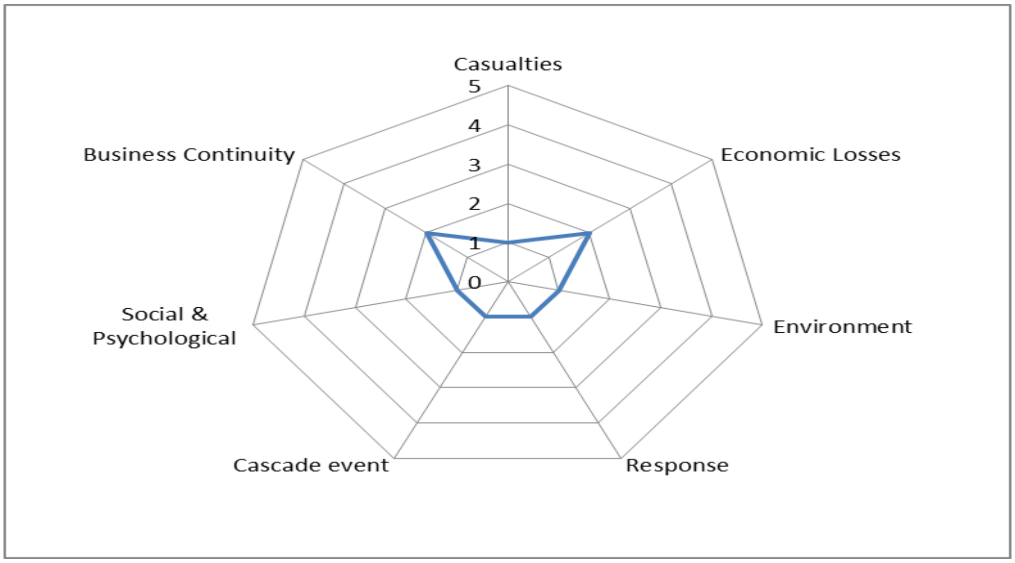


Figure 7. Risk Estimation in Metro & Suburban Stations using Classic Approach

Proposed Method

The weighted average of Consequences (Figure 8) resulted in the total estimate as a MEDIUM class and the application of the Risk Matrix under these categories returned an overall Risk as MEDIUM.

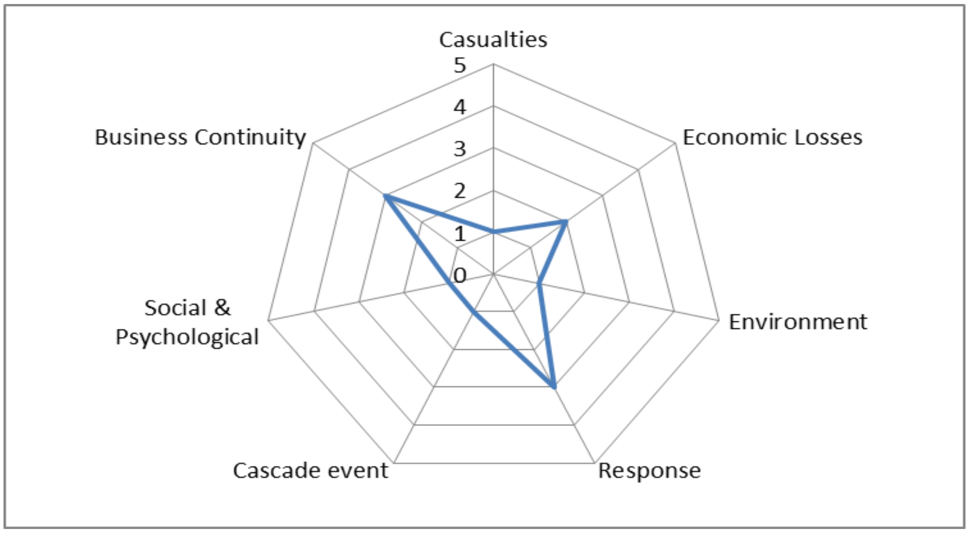
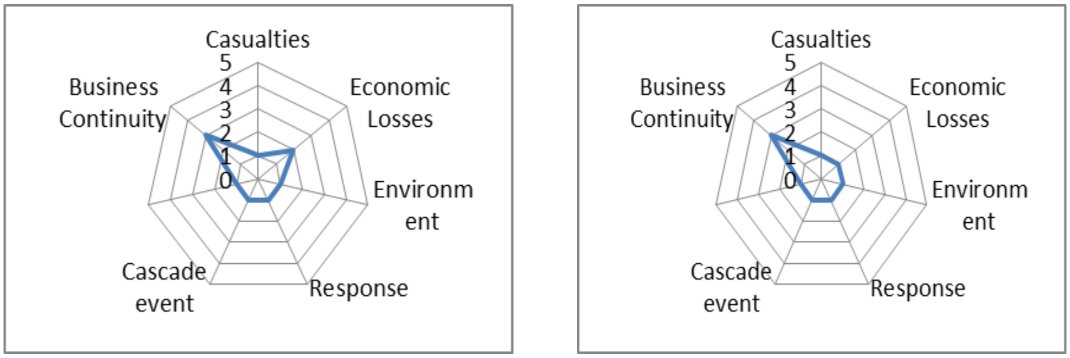


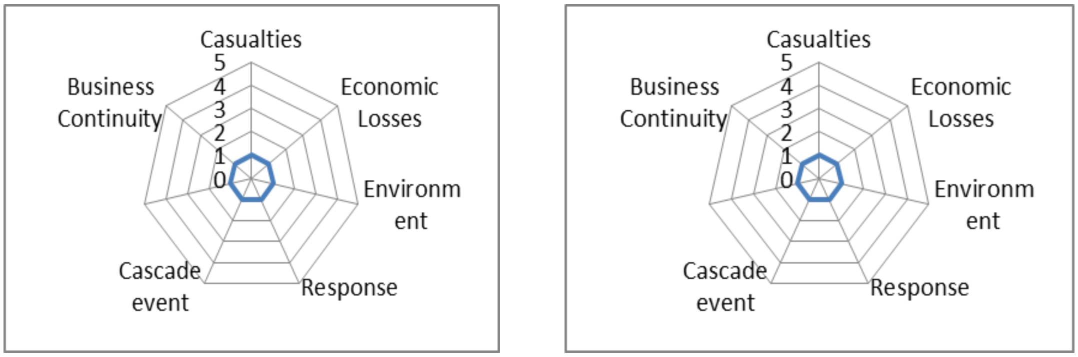
Figure 8. Risk Spider Plot for Metro / Suburban Stations

The Incident Response Procedures were initiated. Based on the IPM constructed for this scenario, the physically connected assets of the metro and suburban rail (*i.e.*, tunnels and suburban rails) have been closed, in order to isolate the assets at risk thus suspending all flow there in (Figure 8a), thus following the Table 6 (with CERTAIN category) we obtain also a MEDIUM likelihood on the interconnected assets. The impacts are due to the establishment of a traffic cordon are that bus stops (Figure 8b) could not be approached and consequently a bus rerouting must be designed in order to ensure the maximum possible bus service towards the citizens (Figure 8c). Additionally, as a 2nd order effect people panicking at the Metro station and abandoned objects may occur, but these have a LOW likelihood to occur, thus according to the LM (Table 6) have an overall likelihood category VERY LOW. The consequences are VERY LOW to all categories, thus establishing a final VERY LOW risk for this 2nd order effect.



(a) Metro tunnels / Suburban rails

(b) Bus stops



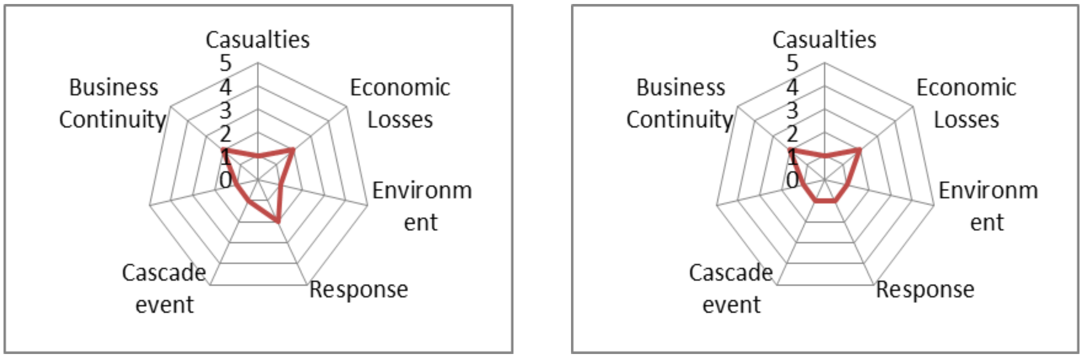
(c) Bus Lines

(d) Metro 2^{nd} order effect

Figure 9. Risk spiders in Interconnected Assets and 2nd Order Effects In Metro Station

Risk analysis with mitigation measures

The risk analysis options considered with this scenario include the installation of real-time sensors as precursors to explosive devices. Owing to these measures, which are characterized with limited efficiency (Table 7), the CONSEQUENCES has been fallen to VERY LOW, resulting in a final risk of VERY LOW. Similar considerations have been made for the interconnected tunnels (Figure 9).



(a) Metro station

(b) Metro tunnels

Figure 10. Risk spiders in interconnected assets and 2nd order effects in Metro station

9. Conclusions

The present paper introduced a strategic risk analysis methodological approach that is applicable on surface transportation networks. The innovation aspect of the introduced approach in comparison to standard risk assessment methodologies 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. These additions complement traditional risk assessment techniques and improve modeling capacity by incorporating various realistic concepts (risk barriers, risk propagation, asset interconnections, *etc.*,) that add up to a multi-faceted and holistic framework. Furthermore, and in order to provide concrete decision support to the critical infrastructures operators risk mitigation options have been introduced. These are coupled with state of the art dynamic traffic assessment tools (VISTA model) that will aid in the maximization of the contingency planning of all involved organizations:

- Optimal path of emergency response vehicles to / from incident area
- Traffic flow simulations under restricted conditions (traffic blockage cordons)
- Surface transport minimization of disruption alternatives (*e.g.*, bus rerouting)

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.

Acknowledgements

The authors acknowledge partial funding by the EC FP7 under Grant Agreement No 225594 (STAR-TRANS).

References

[1] UITP 2010, International Association of Public Transport, http://www.uitp.org/mos/positionspapers/95-en.pdf [accessed on 20/1/2011].

[2] M. Leung, J. H. Lambert and A. Mosenthal, "A Risk-Based Approach to Setting Priorities in Protecting Bridges Against Terrorist Attacks", Risk Analysis, vol. 24, **(2004)**, pp. 963–984.

[3] NRC, Improving Surface Transportation Security: A Research and Development Strategy. A report by the Committee on R&D Strategies to Improve Surface Transportation Security. National Research Council. Washington, DC: National Academy Press, **(1999)**.

[4] U.S. Department of Transportation Surface Transportation Vulnerability Assessment. Research and Special Programs Administration and Office of Intelligence and Security, Washington DC, **(2001)** October.

[5] Y. Y. Haimes, "Risk Modeling, Assessment and Management", New York: Wiley, 2004, B. Ezell, J. Farr, I. Wiese, Infrastructure Risk Analysis Model, Int. J. of Infrastructure Systems, vol. 6, **(2000)**, pp. 114-117.

[6] E. L. Earl II, J. E. Mitchell and W. A. Wallace, "Restoration of services in interdependent infrastructure systems: a network flows approach", IEEE Tr. on Systems, Man, and Cybernetics—Part C: Application and Reviews, vol. 37, **(2007)**, pp. 1303-1317.

[7] V. Rosato, L. Issacharoff, F. Tiriticco and S. Meloni, "Modelling interdependent infrastructures using interacting dynamical models", Int. J. of Critical Infrastructure, vol. 4, **(2008)**, pp. 63–79.

[8] W. Sandmann, "Rare Event Simulation Methodologies and Applications", Simulation, vol. 83, **(2007)**, pp. 809-810.

[9] I. Eusgeld and C. Nan, "Creating a simulation environment for critical infrastructure interdependencies study", IEEE Int. Conf. on Industrial Engineering and Engineering Management, **(2009)**, pp. 2104-2108.

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

[11] Y. Y. Haimes, J. Santos, K. Crowther, M. Henry, C. Lian and Z. Yan, "Risk analysis in interdependent infrastructures", E. Goetz and S. Shenoi (eds) Critical Infrastructure Protection. Springer, Boston, **(2007)**, pp. 297-310.

[12] Z. Yan, Y. Y. Haimes and M. Waller, "Hierarchical coordinated Bayesian model for risk analysis with sparse data", Society of Risk Analysis, Annual Meeting, **(2006)**.

[13] R. Pant, K. Barker, F. H. Grant and T. L. Landers, "Interdependent impacts of inoperability at multi-modal transportation container terminals", Transportation Research Part E: Logistics and Transportation Review, vol. 47, **(2011)**, pp. 722-737.

[14] P. Zhang and S. Peeta, “A generalized modeling framework to analyze interdependencies among infrastructure systems”, Transportation Research Part B: Methodological, vol. 45, **(2011)**, pp. 553-579.

[15] E. Casalicchio, E. Galli and S. Tucci, “Agent-based modelling of interdependent critical infrastructures”, International Journal of System of Systems Engineering, vol. 2, **(2010)**, pp. 60-75.

[16] C. Balducelli, S. Bologna, A. Di Pietro and G. Vicoli, “Analysing interdependencies of critical infrastructures using agent discrete event simulation”, International Journal of Emergency Management, vol. 2, **(2005)**, pp. 306-318.

[17] I. B. Utne J. Vatn and P. Hokstad, “A structured approach to modeling interdependencies in risk analysis of critical infrastructures”, Reliability, Risk, and Safety Theory and Applications, eds (C. Guedes Soares , Radim Briš , and Sebastián Martorell), CRC Press, **(2010)**.

[18] I. B. Utne, P. Hokstad and J. Vatn, “A method for risk modeling of interdependencies in critical infrastructures”, Reliability Engineering and System Safety, vol. 96, **(2011)**, pp. 671-678.

[19] Couneract, Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities, EC Contract Number SSP4/2005/TREN/05/FP6/S07.48891.

[20] EURAM, Generating a European risk assessment methodology for critical infrastructures, Funding through EC Directorate General for Justice, Freedom and Security, **(2006)**.

[21] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, “Identifying, understanding and analyzing Critical Infrastructure Interdependencies”, IEEE Control Systems Mag., vol. 21, **(2001)**, pp. 11-25.

[22] G. Leventakis, A. Sfetsos, N. Moustakidis, V. Grizis and N. Nikitakos, “The development of a strategic risk analysis framework for interconnected surface transportation systems”, International Journal of Critical Infrastructures, vol. 7, no. 3, **(2011)**, pp. 177-199.

[23] D. J. Landoll, “The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments”, Auerbach Publications, **(2005)**.

[24] B. Ruge, “Risk Matrix as Tool for Risk Assessment in the Chemical Process Industries”, ESREL, **(2004)**.

[25] A. S. Markowski and S. M. Mannan, “Fuzzy risk matrix”, Journal of Hazardous Materials, vol. 159, **(2008)**, pp. 152–157.