A Security Risk Analysis Framework for Interconnected Transportation Systems

G. Leventakis
Dept. of Information & Communication Systems Engineering, University of Aegean, Karlovassi, Samos, Center for Security Studies (KE.ME.A.), Athens, Greece
gleventakis@kemea.gr

A. Sfetsos
Environmental Research Laboratory, INTRP
NCSR Demokritos, Athens, Greece
ts@ipta.demokritos.gr

N. Moustakidis
Environmental Research Laboratory, INTRP
NCSR Demokritos, Athens, Greece
nmoustakidis@gmail.com

V. Gkrizis
Center for Security Studies (KE.ME.A.)
Athens, Greece
vgrizis@kemea.gr

S. Andronopoulos
Environmental Research Laboratory, INTRP
NCSR Demokritos, Athens, Greece
sandron@ipta.demokritos.gr

N. Athanasiadis
Research Innovations Development
INTRASOFT International S.A.
Athens, Greece
Nikolas.Athanasiadis@intrasoft-intl.com

A. Ramfos
Research Innovations Development,
INTRASOFT International S.A.
Athens, Greece
antonis.ramfos@intrasoft-intl.com

S. Tönjes
Fraunhofer-Institut für Verkehrs- und Infrastruktursysteme (IVI)
Dresden, Germany
Stefan.Toenjes@ivi.fraunhofer.de

D. Zisiadis
Centre for Research & Technology Hellas,
Thessaloniki, Greece
dkzisiadis@gmail.com

S. Kopsidas
Centre for Research & Technology Hellas,
Thessaloniki, Greece
kopsidas@iti.gr

N. Nikitakos
Dept. of Shipping Trade and Transport
University of Aegean, Mytilene, Greece
nnik@aegean.gr

ABSTRACT

The present paper introduces a comprehensive Transportation Security Risk Assessment Framework for assessing related risks and provides cohered contingency management procedures in interconnected, interdependent and heterogeneous transport networks. The proposed approach includes elements, methodological tools and approaches found in the literature, in addition to operational experience from the organization of major events.

Keywords

Risk assessment, heterogeneous transport networks, asset interconnections, transportation network analysis, threat likelihood, impact assessment, GIS modeling of network dependencies.

Reviewing Statement: This short paper has been fully double-blind peer reviewed for clarity, relevance and significance.

INTRODUCTION

The objective of the present work is to develop a comprehensive Transportation Security Risk Assessment Framework for assessing related risks and provide cohered contingency management procedures in interconnected, interdependent and heterogeneous transport networks. The approach incorporates methodological tools and approaches found in the literature, like the Hierarchical Holographic Model (HHM) and the extended Risk Filtering, Ranking and Management (RFRM) methodology, in addition to operational experience from existing transportation assets and major events, and most importantly spells a methodological framework for estimating risks in assets of interconnected transportation networks.

The main issue with existing tools and frameworks is that they are found somewhat lacking in their ability to capture and model asset interconnections in a way that enables impact propagation among them and consequently their respective networks. However, a combination of the above components can be useful in the development of a framework that will cope with the aforementioned weakness yet still be generic enough to retain its applicability to any kind of network which can be described on an asset-interconnection-asset basis such as the one described below.

To this end, the components which we chose to incorporate into our approach consist of:

- **The risk matrix**: The main ingredient in many risk assessment/analysis frameworks in the literature, used to summarize the likelihood and impact of a risk into a single risk level by applying the formula

  Risk = Likelihood x Impact

- **Interconnection taxonomy**: In order to define the variant ways that assets are weaved into a network interconnection web we adopt the taxonomy which was found to be the most fitting with regard to simplicity, generality and inclusivity. (Rinaldi, Peerenboom, 2001) offer such a taxonomy which is actually the one implemented in the relevant section of the interconnection analysis.

The basis upon which the proposed framework is built mainly comprises empirical findings and case study analyses and is thus presented as an alternative method of using inherent interconnections among assets of different networks in order to model cascading effects and indirect/secondary impacts on interdependent systems.

TRANSPORTATION STRATEGIC RISK ANALYSIS FRAMEWORK

The security process involves the selection of a scenario from the threat / scenarios database that was built (Section 5) and its application on an asset of the transport network.

Risk in the asset is defined as the outcome of the likelihood of the incident and its imposed impacts on the network asset. The possible impacts on the interconnected assets of the same or any other network are defined through the so called Impact Propagation Matrix (IPM).

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 incident matrix composed exhaustively of every possible risk incident that could adversely affect the transport operator, has been identified. The incidents have been classified based on their respective type of threats/threat category and finally subcategory to form a comprehensive threat pool.

Network Assets

The basic principle of the proposed Risk Analysis Framework is that:

- *Each network will be decomposed into assets, i.e., objects with specific and easily recognized roles.*

With that principle in mind the proposed conceptual framework for categorizing assets comprises of:

- *Direct assets (passengers, goods, services/transport media/transport infrastructure)*
- *Indirect assets (utilities, information)*
- *Auxiliary assets*

The major source of complexity in heterogeneous transport systems is 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 based on the medium which each connection utilizes in order to manifest itself. These categories according to (Rinaldi, Peerenboom, 2001) are:

Physical Interdependency: Two or more 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 or more 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 or more 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.

RISK ASSESSMENT

A generalized and common Risk Analysis Framework (RAF) is defined for 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.

Likelihood

Likelihood is the frequency of occurrence of a particular threat. In a more generic approach it is expressed by the formula: Likelihood = Intention to harm X Capability to succeed. The levels of Likelihood are classified into a five category system (Very low-Low-Medium-High-Certainty) and are calculated using two main sources of information: Historical records and Expert opinions.

Consequences

Consequences (Impacts) are the result of the realization of a threat and defined as the harmful or damaging effects of a possible or realized emergency or threat. The proposed approach estimates the consequences building upon a two level hierarchy. Level 1 is a generic taxonomy of consequences summarizing effects in fundamental categories such as Casualties, Environment, Response procedures, Cascade events, Social & Psychological impact and Business Continuity, whereas Level 2 goes into finer detail in the form of Level 1 subcategories. The total, Level 1 and Level 2 (sub)categories impact is assessed using 5 impact levels: Negligible-Small-Medium-High-Severe.

Risk Estimation

Finally, Risk is estimated using a five category system, in accordance to the previous classification of likelihood and consequences through the use of a Risk Matrix which produces a risk estimation level (Very low-Low-Medium-High-Critical) when provided with a Likelihood and a Consequence level value.

RISK PROPAGATION

The core idea of the approach developed for modelling risk propagation in the framework of STAR-TRANS 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. The entire process is described in a series of steps that are discussed in the next part of the section.

The steps taken towards the realization of the STAR-TRANS framework are described below:

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

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

Assuming that the security incident occurs in Asset A1

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

The **consequences** of the incident **on the asset A1** will be defined using the proposed approach on the Level 2 hierarchy. A1{C_{L2}} → Expert rules → A1{C_{L1}} → weighted average → **A1{C}**

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

Risk estimation on Asset A1 by the Risk Matrix based on the inputs A1{L} and A1{C}.

Estimate Likelihood A1{L}

Estimate & Aggregate Consequences A1{C}

→ Estimate Risk **A1{R}**

Step 3: Determine the Assets that are interconnected to A1

Identification of affected Assets by (i) the type and nature of the initial incident, (ii) the type and characteristics of the interconnection between the assets and (iii) the magnitude of the consequences. Thus the proposed approach can be summarized with the phrase: "**impacts from security incidents in an asset can trigger incidents in interconnected assets**".

The "triggering" of incidents is modelled with the help of an Impact Propagation Matrix (IPM). Conceptually, the Impact Propagation Matrix (IPM) is an input / output matrix where **inputs are the consequences** of a security incident (on a hierarchy level 2) and **output(s) are security incidents,** on the immediately interconnected asset, with the exception of geographically linked assets. It shows in a consolidated form the incidents that may be triggered in linked assets from the consequences of security incidents.

The matrix contains "**1**" and "**0**" values in every cell indicating respectively the triggering or not of an incident in an interconnected asset (column) caused by the impact affecting the initial asset (row).

Multiple IPM matrices are defined for different: pairings of transportation assets, security incidents, interconnection types and characteristics of transportation assets.

It must be stressed that IPM *does not provide a unique "1 to 1"* representation of impacts and incidents, in the sense that an impact may trigger multiple incidents. Also different impacts may result in the same incident.

Step 4: 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 likelihood of the initial incident. Thus in symbolic terms **A1{L} ⇔ A3{L} ⇔ C1{L} ⇔ B3{L}**.

CONCLUSIONS

A generalized and common Risk Analysis Framework (RAF) is defined for 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.

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. Therefore it allows the estimation of a holistic risk in many varied contexts:

FUTURE WORK

In order to further experiment with, test and solidify the proposed framework extensive test cases are programmed to be studied and fitted with the framework presented in order to identify possible incompatibilities with certain types of networks (constraint exploration) as well as test the plausibility of the underlying risk modelling process.

The proposed generic risk analysis framework has been transcribed into a UML based modelling language termed as "Impact Assessment Modelling Language" that describes the elements of the introduced framework: network, assets, asset dependencies, incidents, incident likelihood, incident consequences and incident propagation.

Finally, all the components will be integrated into the STAR-TRANS Impact Assessment Tool. The proposed architecture of the IAT will be built on Web 2.0 technologies and characteristics, required by any modern and state-of-the-art rich internet application (RIA) thus providing enhanced user experience.

Acknowledgements

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

REFERENCES

1. Berdica, K. (2002), An introduction to road vulnerability: what has been done, is done and should be done, *Transport Policy*, 9, 2, 117-127.
2. Carr M. J., Konda S. L., Monarch I., Ulrich F. C. and Walker C. F. (1993), Taxonomy-Based Risk Identification, *SEI Technical Report* SEI-93-TR-006, Pittsburgh, PA: Software Engineering Institute.
3. Di Gangi, M. (2005), Transportation Network Vulnerability Indicators for Risk Evaluation and Exposure Reduction, Proceedings of the European Transport Conference (ETC 2005), Strasbourg, France.
4. Haimes, Y. Y. (1998), Risk modelling assessment, and management, John Wiley & Sons.
5. Haimes, Y.Y., Lambert, J.H., Kaplan, S., Pikus, I., and Leung, F (2002), A Risk Assessment Methodology for Critical Transportation Infrastructure, Government report (FHWA A/VTRC 02-CR5), Virginia Transportation Research Council, Richmond.
6. Morgan, M. G., H. K. Florig, M. L. DeKay, and P. Fischbeck (2000), Categorizing risks for risk ranking, *Risk Analysis*, 20, 1, 49-58.
7. Rinaldi S.M., Peerenboom, J.P., Kelly T.K. (2001), Identifying, understanding and analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine*, 21, 6, 11-25.
8. U.S. Department of Transportation (2001), Surface Transportation Vulnerability Assessment, Research and Special Programs Administration and Office of Intelligence and Security, Washington DC.
9. Webler, T., H. Rakel, O. Renn, and B. Johnson (1995), Eliciting and classifying concerns: A methodological critique, *Risk Analysis*, 15, 3, 421-436.