Abstract No. 025-0353

QRA and RBD techniques to evaluate the cost-effectiveness of transport security systems

Luca Urciuoli

Dept. Industrial Management and Engineering, Engineering Logistics, Lund University, Box 118, SE-221 00 Lund, Sweden
luca.urciuoli@tlog.lth.se

Cross-border Research Association, Ave d´Echallens 74, CH-1004 Lausanne, Switzerland

luca@cross-border.org

POMS 23rd Annual Conference

Chicago, Illinois, U.S.A.

April 20 to April 23, 2011

1 Introduction

Security has become a major concern for transport stakeholders as well as our communities. Statistics showing increasing trends in cargo crime, past terror attacks that struck transportation networks, as well as upcoming mandatory programs issued by governments worldwide (i.e. C-TPAT, AEO, ISPS etc.) are requiring transport and terminal operators to increase their security degrees.

The challenge faced by managers as well as by the authorities issuing certifications is to specify and choose among diverse levels of security by assembling together security measures. However, it is still difficult to compute with a good reliability the cost-benefits of the security measures. Main difficulties consist of the lack of reliable statistical data telling how well a security measure or a security system (i.e. a combination of diverse security devices) performs against specific threats. This implies the necessity for techniques and tools to perform choices among wide sets of security solutions by trading off costs and impacts on security.

Very little has been done by previous research analysed within this study. Available literature, focusing on security, highlights the importance of introducing security measures for combating cargo theft and even complying with mandatory programs as the C-TPAT or the AEO initiative. Diverse authors suggest the implementation of managerial strategies as substitution, hedging, burden shifting, collaboration and outsourcing etc., while others bring to light the importance of technical systems as access control, biometrics, satellite based track and trace etc. (Anderson, 2007; Badolato, 2000; Rice and Spayd, 2005; Abbott et al., 2003; Sheffi, 2001). Some of these investigations expound that investments in security should not only be traded off with costs but with the benefits brought to the supply chain. Rice and Spayd (2005) explain that investing in security brings "*collateral benefits*" as trade facilitation, asset visibility and tracking, faster

standard development etc. The same concept of "*collateral benefits*" is sustained by Sheffi (2001), Peleg-Gillai et al. (2006) and Closs and McGarrell (2004). Likewise Willys and Ortiz (2004) emphasize that efficiency and security in supply chain transport are closely interrelated, since higher security may reduce customs delays so as the higher transparency of information of goods flows may reduce shipping costs and time. These studies underline the importance to determine the trade-off of security with costs and benefits; however they don't propose any model to quantitatively compute this trade-off. Only few researchers try to quantify the impact of security solutions. Lee et al. show that RFID tags can save time during containers' inspections and ensure costs savings between $2,000 and $4,000 per container (Lee and Whang, 2005). However, in this study the real effect of the security technology on cargo crime remains unveiled. Urciuoli (2011) exploits the quantitative risk assessment approach combined with expert's judgements and monte carlo simulation to compute B/C ratios and NPV of security devices. However, in this study the impact given by the combination of security devices is not assessed.

Hence, the scope of this paper is to develop further the methodology in Urciuoli (2011) and show how it could be improved to determine the cost-effectiveness of security measures. In particular, this paper proposes to combine the QRA approach with Reliability Block Diagram, and Monte Carlo simulation.

This study has been developed within the CASSANDRA project that is developing risk based approaches for supply chain management to couple with a data sharing concept that allows an extended assessment of risks by both business and government (CASSANDRA, 2011). Security is one of the main risks considered in the CASSANDRA project and therefore the methodology

proposed in this paper is a valuable contribution to be taken into consideration for further development.

This paper is split into 7 sections: first of all a literature review is provided to expound the theoretical foundation of the QRA approach, system reliability theory and reliability block diagrams. Thereafter, according to the experience developed in Urciuoli (2011), merits and limits of the QRA to handle security threats are discussed. Next, we present how the technique of Reliability Block diagrams may be more appropriate. Next, the method is applied to a hypothetical case consisting of security threats against truck transportation and a numerical example is given to explain how the impact of security technologies may be quantified. Finally the results are discussed highlighting the pros and cons of the approach as well as need for future research.

2 The QRA Approach

Risk can be traditionally defined as a combination of three factors: a scenario, the likelihood of the scenario, and its consequences. Thus, performing a risk analysis consists of answering three main questions (Kaplan 1997; Kaplan and Garrick 1981; Haimes, 1998):

1. What can happen? (scenario)
2. How likely is it? (likelihood)
3. If it does happen, what are the consequences? (consequences)

The quantitative estimation of risks, in which numerically specified levels of exposures are coupled with probabilities of response, is known as the Quantitative Risk Assessment (QRA). This approach has been widely used to determine the effect of safety measures in nuclear power plants or to assess the impact of fire fighting measures (Kaplan, 1997; Haimes, 1998; Johansson,

2003). According to the figure below (Figure 1), the QRA approach consists of three main phases: identification of scenarios, collection of body of evidence and scenario quantification.

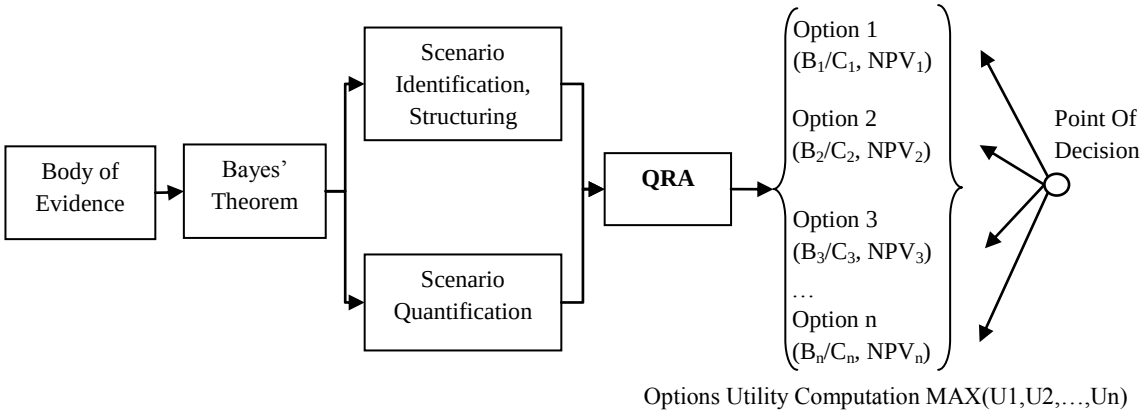

Figure 1: The Quantitative Risk Assessment (QRA) approach (Kaplan 1997).

Scenario Identification. The identification of scenarios is meant to determine the possible attacks against a system. Designing the possible risk scenarios to be analysed is difficult and depends on the degree of complexity of the system analysed. Kaplan (1997) suggests to consider any risk scenario, S_i, as a deviation from the normal conditions specified by the analyst in an initial scenario S_0 (Figure 2).

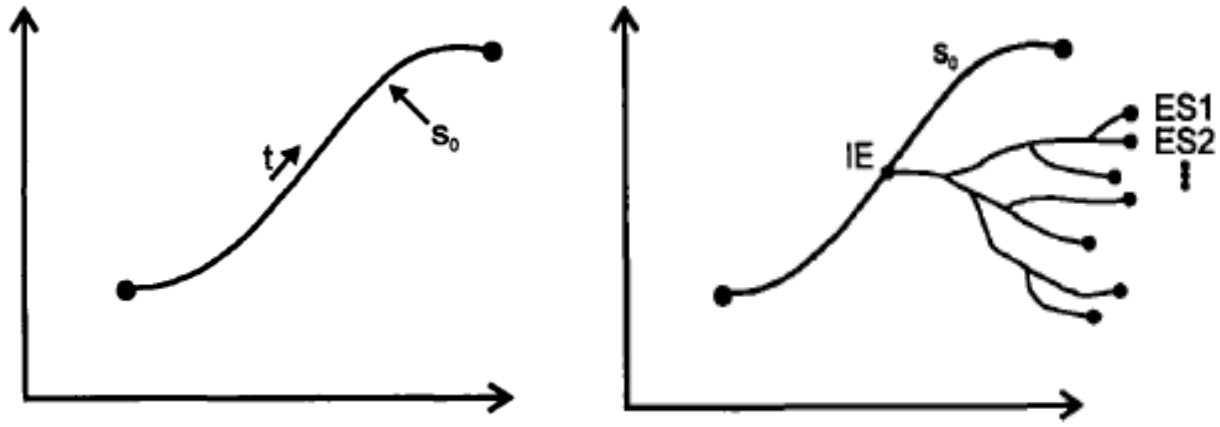

Figure 2: on the left scenario S_0 as a trajectory in the state space of the system, and on the righ tidentification of Initial Events and End States from the trajectory (Kaplan, 1997).

As it is depicted in the above figure (Figure 2), all the departures from this trajectory starts from an Initial Event (IE) and end in an End State (ES).

Collection of Body of Evidence. During this phase, statistics data and experts panels may be exploited to gather evidence of possible security incidents (Kaplan, 1997). To enhance the accuracy and reliability of the data it is recommended to combine different data sources, i.e. databases, experts' judgements, secondary data etc. The probability of the evidence is then given by the sum or integral below:

In this case the Bayes' theorem may be applied according to the equation below (Apostolakis, 1986; Kaplan, 1997):

$$p(E) = \int_0^\infty p(\phi)p(E|\phi)d\phi$$

Where

$$p(\phi|E) = p(\phi)\left[\frac{p(E|\phi)}{p(E)}\right] \quad (1)$$

$p(\phi|E)$ is the probability we assign to ϕ after having evidence *E*, posterior probability.

$p(\phi)$, is the prior probability assigned to ϕ before having evidence *E*.

$p(E|\phi)$ is the probability to observe evidence *E* if the frequency is ϕ.

Scenario Quantification. Once experts' judgements are gathered, scenarios are quantified, and costs, benefits and risks can be simulated and assessed in form of probability curves. To generate probability curves, Monte Carlo simulation may be exploited. This is done by generating pseudo-random numbers. In this way, likelihoods of occurrence can be assigned to the simulation outcomes and enable the evaluation of security solutions according to the statistical dispersions of the output variables, i.e. benefits-costs ratios or net present values etc. (Shina and Labi, 2007).

3 Merits and Limitations of QRA

The implementation of the QRA to assess the impact of transport security solutions has diverse merits and limitations. The major merit of the QRA approach is to overcome the lack of statistical data by using experts' judgements, together with causal modelling and computer simulations. It is well known that often transport and supply chain operators have a tendency not to record or show statistics concerning security attacks against their assets. This comes mostly because of the fear that the statistics could be accessed by their customers or by their insurers that could raise the premiums (Urciuoli, 2011). At the same time, in the few cases where statistics is collected it is very rare that operators store and monitor data showing how well a security device perform or even how criminals react when security systems are introduced.

Despite this, in Urciuoli (2011), it was unveiled that the feasibility and reliability of techniques based on experts' judgements depend on the number of security systems to be evaluated. In particular, this drawback affects the capability of the QRA to evaluate combination of security devices.

For instance, if one wants to evaluate n threats and m security solutions, the total number of scenarios to be evaluated by an expert grow according to the linear relationship $n \times m$. It is

evident that when the combination *n x m* grows, the usage of experts' judgements is not practical anymore. If the analyst wants to take into consideration also the combination of security solutions against the *n* threats, the process may become unfeasible even before, since this time the number of experts' judgements needed grows exponentially. According to combinatorial mathematics, the number of experts' judgements may be calculated according to the following formula:

$$EJ = n \cdot C_k^m = n \cdot \sum_k \frac{m!}{k!\,(m-k)!}$$

Where EJ is the variable representing the amount of experts' judgments, C_k^m is the amount of combinations of *m* security devices in groups of *k* un-ordered collections (in this case k=m). In Figure 8, it is shown how rapidly the number of experts' judgements increase when the number of security devices, *m*, to be combined in groups of *m* un-ordered collections is incremented from 1 to 10. In the same figure, it is also possible to depict how this process may become even less feasible when the number of threats, *n*, is increased from 2 to 8. For example, an analyst willing to evaluate the combination of 5 security technologies against 6 types of threats would require 186 judgements to be collected from the experts.

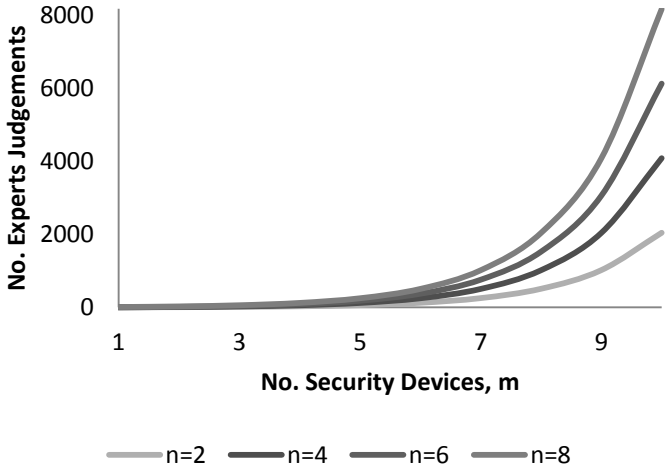

Figure 3: relationship between number of security devices and experts judgements for n=2,4,6,8 security threats.

Hence, it is clear that an analyst willing to consider the impacts of the combination of security devices the collection of experts' judgements becomes an impractical operation. In addition, performing so many judgements may overexert the assessors and degrading the quality of their judgements.

4 The implementation of Reliability Block Diagrams

Reliability Block Diagrams consist of a technique developed within the System Reliability Theory. Smith (1997) as well as Lakner and Anderson (1985) define components reliability as: "*the probability that an item will perform a required function under stated conditions for a stated period of time"*. This definition is rather similar to the definition provided by ISO8402 (1986): "*the ability of an item to perform a required function, under given environmental conditions and for a stated period of time*". In both the definitions the item is any component, subsystem or system that may be considered an entity; while the function of the item may be a single function or a combination of functions that are necessary to provide a service (Rausand and Høyland, 2004).

According to Rausand and Høyland (2004), a Reliability Block Diagram (RBD) is a success-oriented network illustrating how various functional blocks (elements of a system, whether it is a component or a large subsystem) work together to secure that the final system function is fulfilled. The logical interconnections among the functional blocks in a Reliability Block Diagram can be mathematically formalized by structure functions to allow the computation of system reliability indices.

Figure 4 depict a system made of one component *i*. The functions of a component could be diverse, for instance it could be a safety shutdown valve installed in a pipeline or a pressure controller valve installed in a steam boiler system. In any case, whenever the component *i* works correctly it is assumed that there is a connection between end points *a* and *b*. In addition, separate reliability block diagrams have to be built for each of the functions of the system. Hence it is important to specify the function of the system as well as to label each component with a brief description of its function.

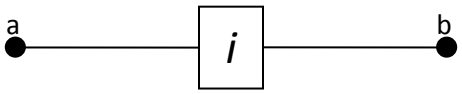

Figure 4: Component *i* illustrated by a block.

The components of a system may be interconnected in reliability block diagrams by means of *series* and *parallel structures*. A system is represented in *series diagrams* if it works as long as all of its *n* components function (Figure 5). As shown in the figure below, the connection between the end points *a* and *b* is achieved if and only if the connection through the *n* blocks representing the components is achieved.

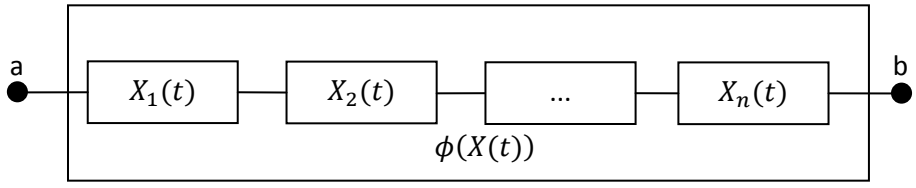

Figure 5: Reliability block diagram of series system (Bergman and Klefsjö, 2004).

In the figure above, it is depicted a system made of *n* components numbered consecutively for *i = 1 to n*. Hence, the state of each component *i, i = 1, 2, ..., n* can be described by a binary stochastic variable $X_i(t)$ that is time dependent. The binary state variables $X_i(t)$ for *i = 1,2,...,n*, take the value of 1 if the component is working, or 0 if the component is in a failed state. Thus, the expected value of each single state variable represents the reliability function of each component in the system analysed:

$$E[X_i(t)] = 0 \cdot \Pr(X_i(t) = 0) + 1 \cdot \Pr(X_i(t) = 1)$$
$$= R_i(t), for\ i = 1,2, \dots, n$$

Similarly the state of the system is described by a stochastic structure function $\phi_s(X(t)) = \phi_s(X_1(t), X_2(t), \dots, X_n(t))$. Consequently, the system reliability at time *t*, $R_s(t)$, is given by the expected value of the stochastic structure function $\phi_s\big(X(t)\big)$.

$$R_s(t) = E(\phi_s\big(X(t)\big))$$

The structure function depends on time as well as on the logical interconnections among the components of the system: series and parallel structures. The structure function and system reliability of a system in which the components are interconnected in series structures, as illustrated in Figure 5, is given by the following equations:

$$\phi_s(X(t)) = X_1(t) \cdot X_2(t) \cdots X_n(t) = \prod_{i=1}^{n} X_i(t)$$

$$R_s(t) = E\left(\phi_s\big(X(t)\big)\right) = E\left(\prod_{i=1}^{n} X_i(t)\right) = \prod_{i=1}^{n} R_i(t)$$

The typical graphical representation of components in parallel is depicted in Figure 6. According to the figure, the connection between the end points *a* and *b* is achieved if it at least one of its components is functioning. The system will stop working only when all the components in parallel will fail. The next equations depict in order the structure function and reliability of a system (Bergman and Klefsjö 2004):

$$\phi_s(X(t)) = 1 - (1 - X_1(t))(1 - X_2(t)) \dots (1 - X_n(t)) = 1 - \coprod_{i=1}^{n} X_i(t) = \coprod_{i=1}^{n} X_i(t)$$

$$R_s(t) = E\left(\phi\big(X(t)\big)\right) = E\left(1 - \coprod_{i=1}^{n} X_i(t)\right) = \coprod_{i=1}^{n} (1 - R_i(t))$$

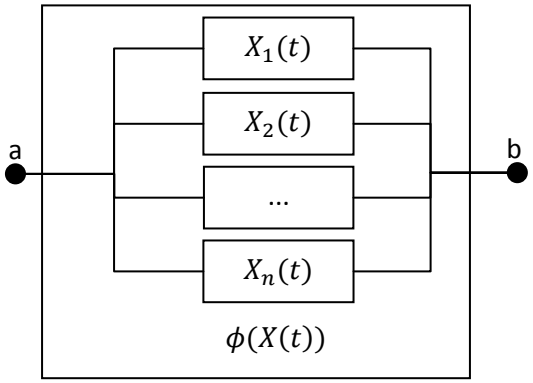

Figure 6: Reliability block diagram of a parallel structure (Bergman and Klefsjö, 2004).

In this paper we propose to perform the estimation of the impacts of security devices on threats by first letting the experts evaluate *n x m* scenarios and thereafter by automating the computation of systems in which the devices are combined. This could be done by exploiting the logic interconnections of the RBD diagrams between the security devices. The logic of the interconnections, to be established among the security devices, is exactly the same explained in the previous section for safety systems. The only difference is that, in a security context, the

failure of the system is provoked by an intentional attack against one or more single components of the security system. This failure determines the interruption of the connection between the end points of the RBD. A system could react to an attack according to which security device is targeted by perpetrators and also whether the device is in series or in parallel in the system.

Devices in series. When security devices are in series structures an intruder will be able to make the security system fail just by successfully attacking one of its components. In other words when security devices are put into series structure the system is as secure as the least secure of its components. In mathematical terms this may be expressed as:

$$R_s(t) \leq min_i(R_i(t))$$

Hence, given a series structure we define the insecurity of a system *s* made of components in series in the following equation:

$$IS_s = 1 - R_s(t) = 1 - E\left(\phi_s\big(X(t)\big)\right) = 1 - \prod_{i=1}^{n} R_i(t)$$

Where

$IS_s = Insecurity\ of\ System\ s$

$R_s(t) = Reliability\ or\ Security\ of\ the\ system$

$R_i(t) = Reliability\ or\ Security\ of\ components\ i\ in\ the\ security\ system$

Devices in Parallel. When security devices are drawn in parallel it implies that an intruder will need to deceive all the devices in the system to successfully perpetrate an attack. As for the series structures, the insecurity of parallel structure of security devices may be formalized as it follows:

$$IS_s = 1 - \ R_s(t) = 1 - \prod_{i=1}^{n}(1 - R_i(t))$$

5 Transportation Case Study

Identification of Scenarios

The case considered in this investigation is a road transportation assignment in which a container loaded with generic cargo is moved between two warehouses (Figure 7). By following the recommendations given by Kaplan (1997), this case may be considered as the S_0 scenario from which Initial Events and End States are going to be identified.

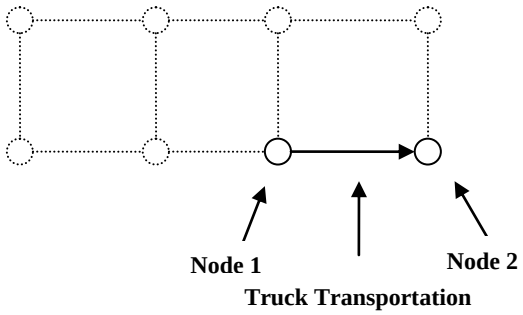

Figure 7: The hypothetical transportation assignement considered in this study (Scenario S_0).

The initial events considered in this case and deviating from the initial scenario S_0 consist of theft attacks against the truck moving between node 1 and node 2. The cargo theft attacks can be mathematically formalized into a vector $\overline{\mu} = \{\mu_1, \mu_2, \mu_3, \dots, \mu_n,\}$ where μ_n is the generic *modus operandi* in the set of cargo theft attacks M ($\mu_n \in$ M). A more detailed description of the *modus operandi* considered in this analysis is given in Table 7 in the appendix of this paper. As it is shown in the figure below, the *n modus operandi* correspond to *n x 2* possible deviations from the initial scenario (Figure 8). Indeed, each of the *n* deviations may lead to two end states: cargo stolen or cargo not stolen.

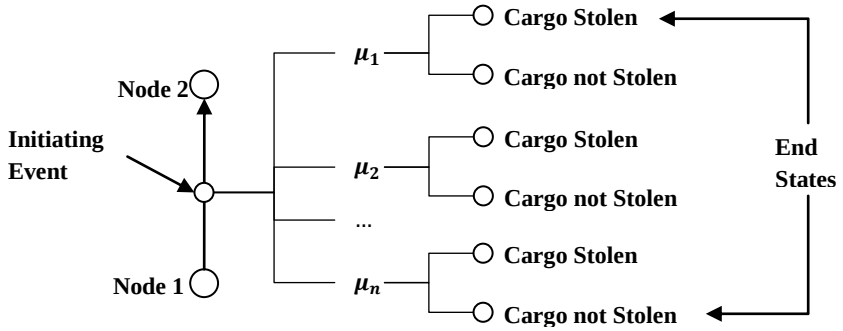

Figure 8: Scenario identification from initiating events to end states.

In addition to the above scenarios, the implementation of security measures implies the development of further scenarios, in which the introduced security systems are coupled with the *modus operandi*. The set of technologies considered in this analysis are also mathematically formalized into a vector $\overline{\rho} = \{\rho_1, \rho_2, \rho_3, \dots, \rho_m\}$, where ρ_m is a generic technology in the set of security measures P ($\rho_m \in$ P). Hence, the new scenarios to be considered are those given by the combination of the *n modus operandi* with the *m* technologies (μ_n, ρ_m) (Figure 9). This implies that a total of $(n \times m + n) \times 2$ scenarios are going to be considered in the analysis. A security measure may be a routine, a managerial strategy or a technical system.

Collection of Body of Evidence

The body of evidence used in this study consists of cargo theft statistics, the costs of security measures, the impact of the security measures on the cargo theft scenarios, and the average annual shipments carried out in Sweden. The data have been collected from primary and secondary sources: hence by means of interviews, statistics data stored in electronic databases and experts' judgements.

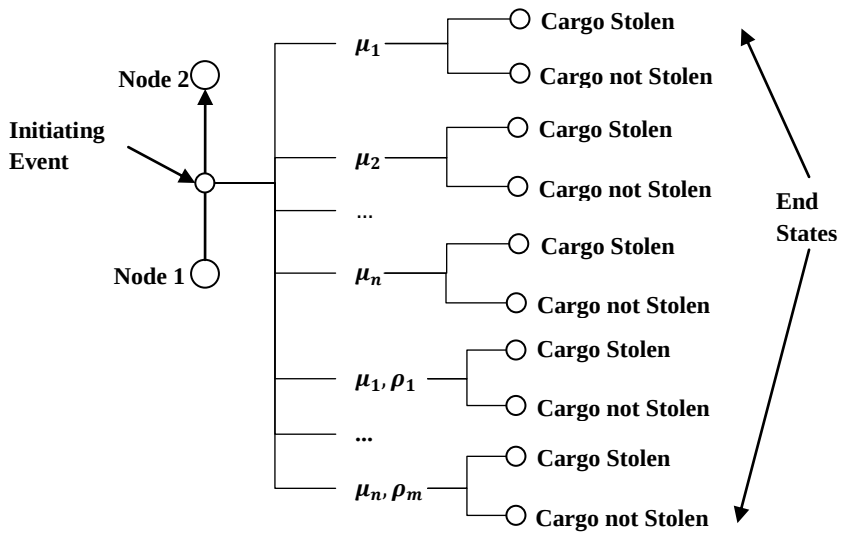

Figure 9: Scenario identification from initiating events to end states.

Cargo Theft Statistics

Statistical data were gathered to determine the frequency of theft attacks against transport operations. This was performed by gathering data corresponding to theft incidents from 2006 to 2007 available from the Swedish HOBIT database, built and provided by the Swedish Law enforcement agency, and the TAPA EMEA (Transported Assets Protection Association) Incident Information System (IIS).

Table 1: modus operandi and corresponding frequency of theft (n=6).

	Modus Operandi	Frequency
μ_1	Burglary (Container)	$7{,}39*10^{-6}$
μ_2	Burglary (Vehicle)	$2{,}77*10^{-6}$
μ_3	Fraud (Vehicle/Container)	$9{,}23*10^{-7}$
μ_4	Hijacking (Vehicle/Container)	$3{,}23*10^{-6}$
μ_5	Robbery (Container)	$9{,}24*10^{-7}$
μ_6	Robbery (Pallets)	$1{,}52*10^{-5}$

Costs of Security Measures

Interviews were used to gather the costs of the security solutions considered in this study. First of all, a set of nine security systems was selected among those that are mostly used by transport operators. Thereafter, companies developing these systems were selected and interviewed to find out the costs of the solutions. The costs have been mathematically formalized in a total cost vector $\overline{TC_\rho} = \{TC_{\rho 1}, TC_{\rho 2}, TC_{\rho 3}, \dots, TC_{\rho m}\}$, where the generic element is given by the sum $TC_{\rho m} = FC_{\rho m} + VC_{\rho m}, \forall\, \rho \in$ M, and $FC_{\rho m}$ and $VC_{\rho m}$ are respectively the fixed and monthly variable costs of a generic technology ρ_m. The collected costs are illustrated in the table below (Table 2). The names of the companies interviewed are not provided for privacy concerns.

Table 2: security solutions and associated fixed and variable costs (m=9).

	Security Solutions	Fixed Costs (€)	Variable Costs (€)
ρ_1	Track & Trace	1 000	15
ρ_2	ID Tag + Readers + Sensor (E-SEALS)	52 000	0
ρ_3	Active RFID Tags + Readers	52 766	0
ρ_4	Active RFID Tag + Reader + GPS + GPRS/GSM	55 000	15
ρ_5	Passive RFID Tags + Readers (gates)+WIFI	53 336	0
ρ_6	Sound Barrier	665	5
ρ_7	Mechanical Locks	300	0
ρ_8	Vehicle Immobilizer	720	15
ρ_9	Reinforced Trailers	500	0

Impact on Cargo Theft Scenarios

The impact of the selected security measures on the cargo theft scenarios has been measured by means of experts' judgements and in form of proportion of theft attacks that could be stopped by a security measure. Hence, to enhance the accuracy of the data to be gathered, a group of experts was chosen among security managers working in logistics and transportation companies as well as among representatives from the law enforcement agency with direct experience of cargo theft. All the experts were chosen from

a convenience sample of representatives joining a Scandinavian project dealing with transportation security that was run from 2005 to 2008.

Table 3: Summary of the experts judgements collected.

	μ_1	μ_2	μ_3	μ_4	μ_5	μ_6
ρ_1	0	0,31	0,33	0,39	0,388	0,008
ρ_2	0,01	0	0,06	0,06	0,06	0,202
ρ_3	0,004	0	0,06	0,06	0,06	0,172
ρ_4	0,5	0,5	0,56	0,56	0,58	0,5
ρ_5	0,002	0	0	0	0	0,162
ρ_6	0,39	0,18	0,12	0,15	0,12	0,29
ρ_7	0,3	0,06	0,02	0,04	0,02	0,17
ρ_8	0	0,38	0,62	0,44	0	0
ρ_9	0,44	0	0,002	0	0,004	0,006

Scenario Quantification

In the scenario quantification phase a mathematical model, Visual Basic scripts (developed in the Excel macro development environment) and Monte Carlo simulations are exploited to estimate the impact of the security solutions on transportation in form of investment indexes. The table below (Table 4) presents a summary of the variables that have been used in the model. According to the table, the input variables are: the theft statistics (μ_n), the interest rate (ir), the loss value or value of shipment transported (C_{loss}), and the impact given by the introduction of security solutions (security solutions impact). The impact of the security solutions is assumed to be an exogenous variable defined by three values to be used to generate random data from triangular distribution (an interval range and a mean value, respectively $[\alpha_\rho, \beta_\rho, \chi_\rho]$). The remaining input parameters are fixed and set by the analyst.

Table 4: Model variables.

Variable	I/O variable	Type	Symbol
Theft Statistics	Input	Fixed	μ_n
Interest Rate	Input	Fixed	ir
Loss Value	Input	Fixed	C_{loss}

Security Solutions Impact	Input	Exogenous	$[\alpha_\rho, \beta_\rho, \chi_\rho]$
B/C	Output	Endogenous	$\left[\frac{B}{C}\right]_\rho$
NPV	Output	Endogenous	NPV_ρ
Risk	Output	Endogenous	δR_ρ

The endogenous variables constituting the output parameters of the mathematical model are the capital investment indexes (the B/C ratio and the Net Present Value) and the risk reductions. These parameters are calculated according to the equations below.

$$\left[\frac{B}{C}\right]_{\rho_m} = \frac{\sum_{t=0}^{T}\left[\delta R_{\rho_m} \cdot (1+ir)^{-t}\right]}{\sum_{t=0}^{T} TC_{t\rho_m} \cdot (1+ir)^{-t}}, \rho_m \in \bar{\rho} \quad (4)$$

$$NPV_{\rho_m} = \sum_{t=0}^{T}\left[\left(\delta R_{\rho_m} - TC_{t\rho_m}\right) \cdot (1+ir)^{-t}\right], \rho_m \in \bar{\rho} \quad (5)$$

$$\delta R_{\rho_m} = \sum_{\mathrm{M}} \left(\mu_n \cdot F_{Z\rho_m}^{-1}(\mathrm{r}) \cdot \Psi\right), \forall\, \mu_n \in \bar{\mu}, \rho_m \in \bar{\rho} \quad (6)$$

Where

$F_{Z\rho_m}^{-1}(\mathrm{r})$, is the inverse of the cumulative triangular distribution function generated with the experts' judgements (see appendix).

δR_{ρ_m}, is the risk reduction of a generic security solution ρ_m.

$\left[\frac{B}{C}\right]_{\rho_m}$, is the Benefit-Cost ration of the generic security solution ρ_m.

NPV_{ρ_m}, is the Net Present Value of the generic security solution ρ_m.

$\Psi = \mathrm{C_{loss}} \times \frac{\mathrm{J_{avg}}}{\mathrm{T_{op}}}$, is the yearly average value shipped by a generic transport operator in Sweden.

RR_{ρ_m}, is the proportion of risk reduction estimated for the security solution ρ_m.

T, is the calculation period of the investment.

t, time measured in years.

To determine the impacts of hybrid security solutions on cargo threats, the set of security solutions identified in this study are combined in series and parallel systems. Therefore, mechanical locks, reinforced trailers and electronic seals can be put in series, since defeating one of them would cause the system to fail. On the contrary the sound barrier, the GPS based Track & Trace, the Vehicle Immobilizer and the Identification based solution can be put in parallel. Even if one of them is deceived by thieves, the system can still defeat an attack (Figure 10).

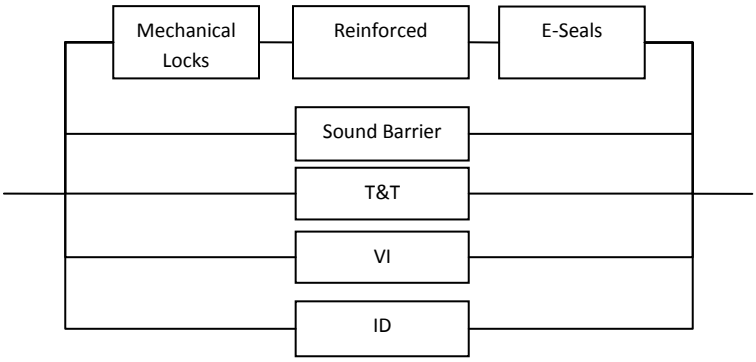

Figure 10: The identified security solutions in series and parallel systems.

To determine the Success Rate (risk reduction factor) of the security systems identified in the previous phase, the reliability block diagram in Figure 5 can be generalized and mathematically formalized in equation below.

$$SR_{S_c} = \left[1 - \left(\prod_{\rho \in \mathrm{P}_{\mathrm{par}}} \left(1 - F_{Z\rho}^{-1}(\zeta)\right) \cdot \prod_{D_s} \left(1 - \prod_{\rho \in \mathrm{P}_{series}} \left(F_{Z\rho}^{-1}(\zeta)\right)\right)\right)\right]$$

In the above, P_{par} and P_{series} are subsets of P containing respectively technologies working in parallel and series fashion, while D_s represents the set of devices put in series in the diagram. S_c is the generic element of the vector $\overline{S} = \{S_1, S_2, S_3, \ldots, S_c,\}$, where $c = \sum_{k=1}^{m} \frac{m!}{k!(m-k)!}$ is the number of possible permutations of the *m* security solutions in *k* un-ordered collections.

6 MODEL RUN

In the next tables the first ten security systems are depicted by sorting the simulation results first on the B/C ratio and then on the NPV (Table 5 and Table 6).

The table below shows the first ten security systems sorted on the B/C ratio (Table 5). The highest B/C ratio is still given by the mechanical locks, followed by the parallel combination of sound barrier and mechanical locks, reinforced trailers, the sound barrier, the combination of sound barrier and reinforced trailers etc. The first solution showing devices in series ranks on the 6th place and is made up of the combination of a sound barrier, a reinforced trailer and a mechanical lock installed on the trailer's doors.

Table 5: First ten security systems sorted on B/C ratio.

	SS	B/C	NPV (€)	RISK (δR_ρ, %)	Security System
1	7	17,42	4 928	-9,30%	Mechanical Lock
2	40	7,90	10 102	-28,65%	Sound Barrier and Mechanical Lock
3	9	7,65	3 328	-7,63%	Reinforced Trailer
4	6	7,03	7 028	-16,72%	Sound Barrier
5	42	6,32	8 867	-18,64%	Sound Barrier and Reinforced Trailer
6	127	4,51	6 910	-14,16%	Sound Barrier, Reinforced Trailer and Mechanical Lock
7	126	3,85	10 510	-28,66%	Sound Barrier, Mechanical Lock and Vehicle Immobilizer
8	68	3,52	10 015	-32,52%	Track and Trace, Sound Barrier and Mechanical Lock
9	128	3,41	9 358	-30,02%	Sound Barrier, Vehicle Immobilizer and Reinforced Trailer
10	43	3,28	5 759	-17,88%	Mechanical Lock and Vehicle Immobilizer

The next table shows the first ten scenarios sorted on the NPV index (Table 6). The highest NPV is given by the combination in parallel of the sound barrier, mechanical lock and vehicle immobilizer. The scenario that follows adopts a similar solution but without the vehicle immobilizer. The first solution, that present devices in series, ranks on the 10th place and is made up of sound barrier, mechanical lock, Vehicle Immobilizer and reinforced trailer. None of the RFID solutions appears in the tables (above or below).

Table 6: First ten security systems sorted on NPV.

	SS	NPV (€)	B/C	RISK (δR_ρ, %)	Security System
1	126	10 510	3,86	-28,66%	Sound Barrier, Mechanical Lock and Vehicle Immobilizer
2	40	10 103	7,90	-28,65%	Sound Barrier and Mechanical Lock
3	68	10 015	3,53	-32,52%	Track and Trace, Sound Barrier and Mechanical Lock
4	182	9 472	2,53	-34,91%	Track and Trace, Sound Barrier, Mechanical Lock and Vehicle Immobilizer
5	128	9 359	3,41	-30,02%	Sound Barrier, Vehicle Immobilizer and Reinforced Trailer
6	42	8 867	6,33	-18,64%	Sound Barrier and Reinforced Trailer
7	70	8 858	3,13	-25,43%	Track and Trace, Sound Barrier and Reinforced Trailer
8	184	8 412	2,32	-34,95%	Track and Trace, Sound Barrier, Vehicle Immobilizer and Reinforced Trailer
9	41	7 529	3,23	-21,74%	Sound Barrier and Vehicle Immobilizer
10	255	7 408	2,77	-23,62%	Sound Barrier, Mechanical Lock, Vehicle Immobilizer and Reinforced Trailer

7 Discussion

In this paper a methodology for the quantification of security investments is proposed by taking advantage of existing methods as the Quantitative Risk Assessment (QRA), experts' judgements,

the Reliability Block Diagrams and Monte Carlo simulations. The QRA approach combined with the experts' judgements is necessary because of the absence of statistical evidence regarding the effect of security measures on cargo threats. The collection of experts' estimations can become an unfeasible operation if the dimensions of the sets of security solutions and cargo threats increase, especially if analysts want to consider the impacts of hybrid security systems. Hence, by following the method of System Reliability Analysis, hybrid security systems can be designed and their impact estimated by means of reliability block diagrams (series and parallel diagrams). Finally, Monte Carlo simulation is necessary since the judgements of the experts are uncertain and are represented by probability curves.

Results from a hypothetical transportation case study shows the possibility to apply the methodology and also prove that the amount of experts' judgements may be sensitively reduced, improving the feasibility of the study.

Practitioners may benefit from the tool developed as they will be able to enhance their decision making processes and select the most cost-effective solution among a hugher amount of security systems. At the same time, this paper contributes to the scientific world with a mathematical model to compute the impact of security solutions on transport networks.

8 References

Abbott, G., Thomas, R., and Brandt, L. (2003), 'Commercium Interrupts: Supply Chain Responses to Disaster', *Acquisition Policy*, Fort McNair, Washington, D.C. 20319-5062.

Anderson, B. (2007), 'Securing the Supply Chain – Prevent Cargo Theft', *Security*, Vol. 44, No. 5, pp. 56-58.

Apostolakis, G. (1986), 'On the use of judgments in probabilistic Risk Analysis', *Nuclear Engineering and Design*, Vol. 93, N° 2-3, pp. 161-166.

Badolato, E.V. (2000), 'Smart moves against cargo theft', *Security Management*, Vol. 44, No. 7, pp. 110-115.

Broder, J.F. (2006), *Risk Analysis and the Security Survey*, 3rd Edition, London: Elsevier Butterworth-Heinemann.

CASSANDRA, (2011), Improving security through visibility, http://www.cassandra-project.eu/

CBP (2008), C-TPAT: Customs Trade Partnership Against Terrorism, http://www.cbp.gov/xp/cgov/trade/cargo_security/ctpat/, [accessed 01/03/2008].

Closs, D. and McGarrell, E. (2004), 'Enhancing Security Throughout the Supply Chain', IBM Centre for the business of government.

CP3 Group (2006), AEO Guidelines, http://www.cp3group.com/attachments/AEO%20guidelines.pdf, [accessed 01/02/2007].

Driels, M.R., and Shin, Ý.S. (2004), Determining the number of iterations for Monte Carlo simulations of weapon effectiveness, Naval Post-graduate School, Monterey, California.

Devore, J. and Farnum, N. (1999), *Applied Statistics for Engineering and Scientists*, London: International Thomson Publishing.

ECMT (2002), *Crime in road freight transport*, OECD Publication Service, Paris.

Ekwall, D. (2009), 'The displacement effect of cargo theft', *International Journal of Physical Distribution and Logistics Management*, Vol. 39, No. 1, pp. 47-62.

EU Commission (2007), Authorized Economic Operators – GUIDELINES, TAXUD/2006/1450, [accessed 29/06/2007].

European Parliament (2007), Security - Protection of persons, of assets and the facilities, http://ec.europa.eu/dgs/energy_transport/security/intermodal/, [accessed 22/08/2007].

Haimes, Y.Y. (1998), *Risk Modeling, Assessment, and Management*, John Wiley & Sons.

Hall, S. and Frank, H. (2003), A CCTV system designed to cut the Influx of Drugs and Theft, International Association of Professional Security Consultants.

Hintsa, J. (2011). Post-2001 Supply Chain Security - Impacts on the Private Sector. Lausanne: HEC University of Lausanne.
http://www.techforesight.ca/Publications/CanadianStrategicSecurityChallenges2015.pdf.

ISO8402 (1986), Quality Vocabulary, International Standards Organization, Geneva.

Johansson, H. (2003), *Decision Analysis in Fire Safety Engineering - Analysing Investments in Fire Safety*. PhD Thesis. Lund 2003.

Kaplan, S. (1997), 'The Words of Risk Analysis', *Risk Analysis*, Vol.17, No. 4.

Kaplan, S. and Garrick, B.J. (1981), 'On the Quantitative Definition of Risk', *Risk Analysis*, Vol.1, No. 1

Kaplan, S., Haimes, Y.Y. and Garrick, B.J., (2001), 'Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk', *Risk Analysis*, Vol. 21, No. 5, pp. 807 – 819.

Kotz, S. and Van Dorp, J.R. (2004), *Beyond Beta - Other Continuous Families of Distributions with bounded support and applications*, World Scientific Publishing Company.

Lakner, A.A. and Anderson, R.T. (1985), *Reliability Engineering for Nuclear and Other High Technlogy Systems*, Elsevier Applied Science, London.

Law, A.M. and Kelton, W.D., (2000), *Simulation Modelling and Analysis*, 3rd edition, McGraw Hill Higher Education.

Lee, H.L. and Whang, S. (2005), 'Higher Supply Chain Security with lower cost: lessons from Total Quality Management', *International Journal of Production Economics*, Vol. 96, No. 3, pp. 289-300.

Lumsden, K. (2006), *Logistikens Grunder*, 2nd Ed., Poland: Studentliteratur.

Peleg-Gillai, B., Bhat, G., and Sept, L. (2006), 'Innovators in Supply Chain Security - Better Security Drives Business Value', *Stanford University - The Manufacturing Institute*, The Manufacturing Innovation Series.

Peterson, C. and Miller, A. (1964), 'Mode, Median, and Mean as Optimal Strategies', *Journal of Experimental Psychology*, Vol. 68, N°4, pp. 363 – 367.

Purpura, P.P. (2008), *Security and Loss Prevention: An Introduction*, 5th Edition, London: Elsevier Butterworth-Heinemann.

Rausand, M. and Høyland, A. (2004), *System Reliability Theory – Models, Statistical Methods, and Applications*, 2nd Ed., Wiley Series in Probability and Statistics, New Jersey.

Rice, J.B. Jr., and Spayd, P.W. (2005), 'Investing in Supply Chain Security: Collateral Benefits', IBM Center for Business of Government.

Rodwell, S., Van Eeckhout, P., Reid, A., and Walendowski, J. (2007), Study: Effects of counterfeiting on EU SMEs and a review of various public and private IPR enforcement initiatives and resources, http://ec.europa.eu/enterprise/enterprise_policy/industry/doc/Counterfeiting_Main%20Report_Final.pdf, [accessed 31/08/2007].

Sheffi, Y. (2001), 'Supply Chain Management under the Threat of International Terrorism', *The international Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11.

Shina, K.C., and Labi, S. (2007), *Transportation Decision Making – Principles of Project Evaluation and Programming*, New Jersey: Jon Wiley & Sons.

SIKA Institute (2008) Lastbilstrafik, http://www.sika-institute.se/Templates/Page____66.aspx, [accessed 16/03/2008].

Smith, D.J. (1997), *Reliability, maintainability and Risk*, 5th Ed., Butterworth Heinemann, Oxford, UK.

Stöth, G. (2004), *Transport- och Logistikrätt*, 2nd Edition, Sundbyberg: Industrilitteratur.

Talas, R., and Menachof, D., (2009), 'The efficient trade-off between security and cost for sea ports: a conceptual model', *International Journal of Risk Assessment and Management*, Vol. 13, No.1, pp. 46 – 59.

TAPA EMEA (2008), TAPA EMEA Transported Asset Protection Association, http://www.tapaemea.com/, [accessed 01/02/2008].

Urciuoli, L. (2011), Investing in transport security solutions: using the quantitative risk assessment (QRA) approach, International Journal of Risk Management and Assessment, Vol. 15, No.4, pp. 275-298.DOI: 10.1504/IJRAM.2011.042669

Wandel, S. (1985), 'A Schematic Model of Experiments with Mathematical Models applied to production control', *Engineering Costs and Production Economics*, Vol. 9, pp. 321 – 337.

Whyte, J.L. (1993), 'The freight transport market: buyers-sellers relationships and Selection Criteria', *International Journal of Physical Distribution and Logistics Management*, Vol. 23, No. 3, pp. 29-37.

Willys, H.H., and Ortiz, D.S. (2004), 'Evaluating the Security of the Global Containerized Supply Chain', *RAND Corporation*, Santa Monica, CA.

Winkler, R.L., and Murphy, A.H. (1968), ‚Good Probability Assessors', *Journal Appl. Meteor.*, Vol. 7, N°5, pp. 751 – 758.

APPENDIX

Table 7: Threats against road transport operations and assets.

	Threat	Description
μ_1	**Burglary (Trailer)**	The thieves break into or enter a trailer without the confrontation of drivers or other operators. The stolen cargo is loaded onto another container and driven away to a specific location.
μ_2	**Burglary (Vehicle)**	The thieves break into or enter the vehicle's cabin without the confrontation of drivers or other operators. The stolen vehicle is driven to a specific location where the cargo is loaded onto another trailer.
μ_3	**Fraud (Vehicle)**	A vehicle and its cargo are stolen with intentional deception. By making false statements, concealing or omitting material facts, criminals manage to take possession of the vehicle and its cargo and drive it to another location where the cargo is unloaded.
μ_4	**Hijacking (Vehicle)**	Force (armed or unarmed), threat or intimidation are used to kidnap drivers in order to take possession of the vehicle and its cargo. The vehicle is driven to a specific location where the trailer's cargo is loaded on another truck and driven away.
μ_5	**Robbery (Trailer)**	By means of force (armed or unarmed), threat or intimidation a driver is coerced to hand over the trailer to criminals. These couple the trailer with another truck tractor and drive it to a specific location where cargo is unloaded.
μ_6	**Robbery (Pallets)**	By means of force (armed or unarmed), threat or intimidation a driver is coerced to open the container/trailer and hand over the pallets to criminals. Goods are loaded into another truck and driven to a specific location.

Table 8: Solutions to secure road transport operations and assets.

	Security Solution	Description
ρ_1	**T&T**	The basic track & trace solution is a unit placed on the trailer in which the following sensors are integrated: a GPS and a wireless communication unit (GSM/GPRS). Positioning information is sent to a central server according to an updating frequency of 30 minutes. A basic computer application is installed to monitor the shipment
ρ_2	**ID Tag + Readers + Sensor (E-SEALS)**	The solution is equipped with specific sensors to detect opening/closing activities of the trailer's doors. This information is stored in an active tag integrated in the solution. Finally the information on the tag is read at three key locations where RFID readers are placed. A basic computer application is installed to monitor the shipment.
ρ_3	**Active RFID Tags + Readers**	Active tags are placed on the pallets (a shipment of ten pallets is considered) and a reader is installed in the trailer to identify the cargo. Information about the cargo and communicate it to external readers placed in nodes of the transport network (i.e. warehouses, intermodal terminals, etc.). A basic computer application is installed to monitor the shipment.
ρ_4	**Active RFID Tags + Reader + GPS + GPRS/GSM**	Active tags are placed on the pallets (ten pallets) and a reader is installed in the trailer to identify the cargo. Information about loaded/unloaded pallets in the trailer is sent together with GPS position to a remote server where a basic computer application is installed to monitor the shipment. If pallets are unloaded from the truck outside specific locations defined by the user, an alarm is automatically triggered.
ρ_5	**Passive RFID Tags + Readers (gates) + WIFI**	Passive RFID tags are installed on pallets (ten pallets) and short range readers are placed on trailer's doors to read entering and exiting goods. Short range readers are placed in nodes of the transport network to read the trailer's content. A basic computer application is installed to monitor the shipment.
ρ_6	**Sound Barrier**	The sound barrier is a siren installed in the trailer that is activated by an intrusion detection sensor. This unit produces a disturbing noise that forces thieves to abandon the target.
ρ_7	**Mechanical Locks**	Mechanical locks include padlocks and bolt container seals to lock trailers' gates. In this study a bolt container seal in stainless steel is considered.
ρ_8	**Vehicle Immobilizer**	The vehicle immobilizer is an electronic mechanism that can be remotely activated to immobilize the truck tractor. The solution includes a GPS and a GSM modem. A remote operator can monitor the truck's position and immobilize it via SMS communication.
ρ_9	**Reinforced Trailers**	Trailers curtains are reinforced by rigid ones to obstacle criminals trying to break in through the walls.