Securing Ground Transportation Infrastructures

A. Di Febbraro, F. Papa, and N. Sacco
DIME – University of Genoa, Genoa, Italy
Email: {angela.difebbraro, Federico.papa, nicola.sacco}@unige.it

***Abstract*—Global strife and the perception of injustice create suitable conditions for terrorists, as well for saboteurs, thieves and vandals, to recruit and raise support. In addition, as Countries modernize, they increasingly depend on technologies, and the interconnections among systems, such as energy distribution, telecommunication and transportation systems, are becoming increasingly strong. Such networks of Critical Infrastructures (CIs) represent, in many cases, the targets to the above cited adversaries.**
Taking into account the above considerations in this paper, the "second step" results of a project aiming to design an effective tool for risk analysis are described, focusing on the problem of evaluating the global risk of ground transportation infrastructures, such as highways and railways, after the introduction of some suitable protections in some the elements making it up.
The paper is organized as follows: after a brief literature review, the main characteristics of the considered tool architecture are recalled. After this brief introduction the new modules are described, focusing on the enhancements they provide to the whole architecture. Finally, a case study is described with the aim of showing the capabilities of the proposed architecture.

***Index Terms*—Physical protection systems design, risk analysis, transportation systems security.**

I. Introduction

Global strife and the perception of injustice create suitable conditions for terrorists, as well for saboteurs, thieves and vandals, in a word "adversaries", to recruit and raise support.

In addition, as Countries modernize, they increasingly depend on technologies, and the interconnections, often operated by computers, among systems, such as energy distribution, telecommunication and transportation systems, and so on, become increasingly strong. Such networks of Critical Infrastructures (CIs) represent, in many cases, the targets to the above mentioned adversaries.

In this framework, a CIs network may be thought of as a set of different networks gathering transportation systems, like those for the energy distribution, telecommunications networks, and so on, that are characterized by elements whose damages can lead to the failure of other systems, thus provoking significant disruptions and losses.

A significant example of such interconnected networks is represented by the railway transportation network, whose normal operations are supported by dedicated telecommunication and energy distribution subsystems.

The vulnerability of these two subsystems could represent an attractive way to stop trains, in order to perform a specific attack, or to damage the image of the railway system and increase the level of fear of people.

Maximizing the security of such networks has become a problem of primary importance for all the Countries. Then, in recent years institutions [1]–[4] and researchers [5]–[7] have devoted their efforts to:

1. Define more and more accurate norms for increasing controls, harmonizing the rules of different Countries, planning investments for securing them;
2. Design risk mitigation technologies and risk analysis methodologies that are:
   - *Easy-to-use*, that is, suitable for practical applications, even on large networks;
   - *Reliable*, that is, minimizing the effects of such human subjectivity that sometimes affects the security risk analysis process, where the estimation of some characteristics of assets are left to the opinions and experiences of the risk assessor;
   - *Optimization oriented*, that is, able to provide indications on the most effective investments, in term of cost/benefit, to be realized to secure infrastructures.

Moreover, it is worth saying that, due to their intrinsic characteristics, securing transportation networks represent a key problem to tackle with. In fact, such networks are:

- *Vital*, because in many cases represent the backbone connection among different geographical areas of a Country, or among different Countries;
- *Highly geographically distributed*, so that controlling them at any time is, practically, infeasible;
- *Very heterogeneous*, from both the points of view of the constituting civil structures and technological devices;
- *Critical*, because in most cases no redundancy is possible;
- *Open*, because almost the whole infrastructure is easily reachable by anyone;
- *Highly populated* in some locations, where a large number of vehicles and/or people are gathered together, such as in railway stations.

In this framework, transportation networks need a particular attention because they have often shown their

Manuscript received December 25, 2012; revised January 25, 2013.

doi: 10.12720/jtle.1.2.141-147

vulnerability (New York, 2001 – Madrid, 2004 –London 2005, just to cite some sadly known events).

Then, in this paper, to cope with the problem of minimizing the risk the of ground transportation infrastructures, such as highways and railways, the "second step" results of a project aiming to design an effective tool for risk analysis, are described. The proposed general architecture refers to the one proposed in [9], where the specifications of each element of the proposed tool have been discussed.

Therefore, in this work the attention is focused on the definition of:

- *Qualitative/Quantitative Filters (QQF)*, based on Fuzzy Logic, that elaborate the (qualitative) information describing the quality of Physical Protection Systems (PPS), the attractiveness of assets, the adversaries characteristics and tactics, and provide the relevant (quantitative) numerical estimations;
- An optimization problem aiming to support the selection of the best intervention, or configuration of securing interventions, to be realized for minimizing risk.

The paper is organized as follows: after a brief literature review, the main characteristics of the considered tool architecture are recalled. Therefore, the new modules are described, focusing on the enhancements they provide to the whole architecture. Finally, a case study is described with the aim of showing the capabilities of the proposed architecture.

II. Literature Review

In this section, a brief literature review, mainly focused on transportation systems, fuzzy logic and its application to risk analysis, is described.

The analyzed literature on security essentially tackles with the following problems:

1. Identify what can go wrong: "which are the possible malicious attacks?" ([6] and the references therein);
2. Estimate its likelihood: "how much are they probable, or frequent?" ([7]–**[9]** and the references therein);
3. Identify and estimate what are the consequences of an attack ([7]–**[**10], and the references therein);
4. Take the most appropriate decisions about the investments for improving the protection of assets [12], or to plan secure transportation [13].

In addition, a complete guideline for the design of physical protection systems may be found in [14], which also provides a detailed description of the state of the art of technologies, and of the profiles of the categories of possible adversaries.

As regards Fuzzy Logic [15], [16], some references about the application of this formalism to risk analysis processes have been examined. Then, while FL is quite known in risk analysis [17]–[19] no explicit applications to security risk analysis have been found in the considered scientific literature.

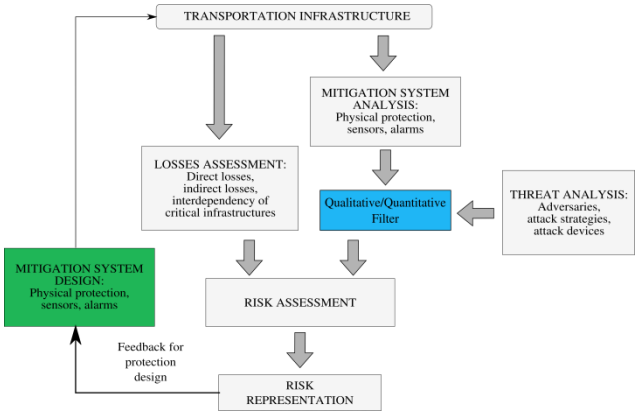

Figure 1. Tool architecture.

III. The Proposed Tool Architecture

In this section, the modular architecture of risk analysis tool is described. In doing so, it is worth saying that it represents a further development the one proposed in [7], where also the specifications of the inputs and outputs of each module have been introduced.

Then, consider the scheme reported in Fig 1 where the different modules, depicted in light grey in the diagram, have the following meanings, or perform the following tasks:

- The *Transportation Infrastructure (TI)* block represents the ground transportation infrastructure, whose risk has to be assessed, and the relevant PPS has to be designed.
- The *Losses Assessment (LA)* module performs the computation of the damages generated by a security incident, not only quantifying the direct losses represented by the costs of all the assets destroyed or damaged by the attack, but also performing an analysis aimed at estimating the costs of its consequences, also in terms of interdependence of infrastructures [10], [11];
- The *Mitigation System Analysis (MSA)* module is devoted to analyze, classify, and evaluate the quality of the already existent PPS in the considered infrastructure. A typical output of this module consists of a list of the already operative PPS devices, as well as their performances and effectiveness evaluation;
- The *Threat Analysis (TA)* module performs the identification of the possible adversaries, taking into account the relevant characteristic (tactics, tasks, weapons, knowledge, and so on. A typical output consists of a list of the possible adversaries together with the most probable assets that could be attacked by each of them. In an architecture without the Fuzzy Logic filter described in the following, this module also estimates the attack likelihood;
- The *Risk Assessment (RA)* module represents the core of the whole architecture, and is devoted to the assessment of the risk for any asset of the considered transportation infrastructure. As inputs, it needs the losses, which are provided by the

above LA module, and the attack likelihood for any class of adversary, which is provided by the MSA and TA modules, throughout the new QQF described in the following;

- The *Risk Representation (RR)* module represents the part of the tool intended to depict, in a suitable graphical way, the risk associated with each asset of the considered infrastructure. Its output corresponds to the so called "risk piffle".

Note that the information provided by some the above modules (TA and MSA) consists of qualitative descriptions of some characteristics, such as, for instance, the quality of protections or the attractiveness, whereas the other modules require that the same characteristics are expressed as quantitative evaluations (LA, VARA, RR).

Then, the need of designing proper QQF in order to make the inputs and the outputs of each module compatible, and the relevant "conversion" objective and reliable, rises. Therefore, the first improvement of the above scheme consists of the introduction of such filters, depicted in blue in Fig. 1, and whose design will be described in the following section.

A second enhancement of the proposed architecture is represented by the introduction of the *Mitigation System Design (MSD)* module, depicted in green in Fig. 1. Such a module states a optimization problem for the identification of the best investment in PPS among all the possible ones, given the characteristics of the considered ground transportation system to be secured. The module will be described with more details in the following section.

IV. The Quantitative/Qualitative Filters and Optimization Modules

In this section the above cited filters and optimization modules for the considered architecture are described. In order to cope with this task, a brief introduction of Fuzzy Logic fundamentals will be first given.

A. Basics on Fuzzy Logic

Fuzzy Logic (FL), which first formulation was introduced in the sixties by Zadeh [15], is a multi-valued logic that allows to introduce "intermediate" values between the conventional concepts like true/false, yes/no, and so on. In addition, FL permits to associate numerical quantities with them.

In this framework, qualitative and subjective notions like "rather high" or "very fast", can be associated to numerical values, in suitably chosen scale, and then processed by numerical algorithms. The process of associating numbers to such "fuzzy" concepts consists, first, of defining a set of *membership functions* $\mu_i \to [0,1]$, $\forall i \in I$, that is, for each of the qualitative concepts like the above exemplified, and gathered in the set I. Then, each value x to be *fuzzyfied* is processed by each membership function, thus obtaining a set of values $\mu_i(x)$, $\forall i \in I$.

Evidently, the values assumed by the membership functions strongly depend on the shape of the functions themselves, which have, indeed, to be carefully identified, possibly by means of a set of reliable data.

Coming back to the security risk assessment problem, the characteristic of FL appears to be particularly useful because, once carefully defined the membership functions. This formalism allows to:

1. Define suitable scales (for instance from 0 to 10) for representing qualitative concepts, such as goodness of protection, attractiveness, and so on, and calibrate them;
2. Weight the values given for a particular characteristic of an asset on the basis of the assessments given, in similar cases, by other risk assessors or experts. This approach reduces the "subjectivity" of any particular risk assessor itself.

Summing up, FL represents a useful way for modeling the "vagueness" of those "non-numeric" parameters, while ensuring, at a time, that human creativity and intuitively, which is an essential ingredient for successful risk analysis, is still taken into account.

In the following, FL will be used for designing the qualitative/quantitative filters in Fig. 1. In doing so, it is worth saying that the shapes of the membership functions have been obtained by means of data gathered throughout questionnaires on test cases compiled by a group security experts.

B. Qualitative/Quantitative Filter Design

The proposed risk analysis tool, whose specifications are reported in [7], has been designed to be used directly in the process of site inspection, so as to facilitate the risk assessment of large transportation networks. Then, consider the architecture depicted in Fig. 1, where it is possible to note that the risk is computed on the base of data about potential damages and losses, which are expressed as numerical evaluations, and data about characteristics of adversaries (tactics, objectives, etc.) and of the protection systems (site of valuable materials, kind of detecting sensors, kind of physical protections, number of controlled accesses, etc.), which are, on the contrary, often expressed in a mixed qualitative/quantitative form.

As a consequence, the QQF have to transform the input data from qualitative descriptions to quantitative evaluations, in order to allow to the RA module to elaborate numerical values of the risk.

Then, the first step to be performed by the QQF is to collect the information about valuable assets, presence of people, and, in general, about the importance of the asset, so as to identify the most probable targets of adversaries, that are:

1. The locations with valuable materials, when thieves are considered;
2. The sites gathering many people, or those whose failures would have an impressive impact on the public opinion, when terrorists are considered;

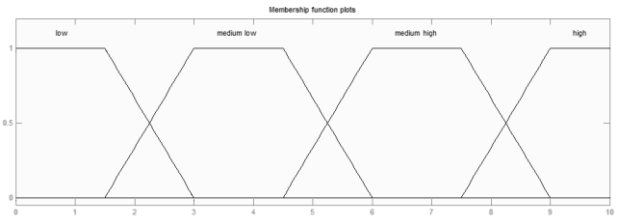

Figure 2. Membership function for "attractiveness of an asset".

3. The vital areas gathering those equipment whose failure or damage could make the systems services unavailable, when saboteurs are considered;
4. Isolated or unguarded places, when vandals are considered.

The risk assessor is expected to give a qualitative score, indicated as $a_i^{k,in}$, in a scale between 0 and 10, and expressing the attractiveness of the k^{th} asset with respect to the i^{th} class of adversary. Then, the value $a_i^{k,in}$ is processed throughout the membership functions μ_{low}, μ_{ml}, μ_{mh}, and μ_{high}, associated with the different qualitative values expressing the attractiveness of an asset (resp., *low*, *medium low*, *medium high*, *high*), whose shapes are reported in Fig. 2.
More in detail, the QQF compute the value

$$a_i^{k,out} = [\mu_{low}(a_i^{k,in}) + \mu_{ml}(a_i^{k,in}) + \\ +\mu_{mh}(a_i^{k,in}) + \mu_{high}(a_i^{k,in})]a_i^{k,in} \quad (1)$$

which represents a "calibrated", more objective, value of $a_i^{k,in}$, that takes into account, in some way, the experience of the experts that collaborated to define the membership functions.

Then, the second operation performed by the QQF filter consists of the identification of the so-called "adversary path" [14], that is the sequence of PPS to be overcome by an adversary to reach its goal.

Such task is reached by collecting the scores of the risk assessor about the kind of fences (walls, metal, and so on), the kind and the number of accesses (gates, doors, windows), the presence of open areas, and so on, together with the relevant protection devices effectiveness (kind of CCTV, of intrusion detection sensors, access control measures, and so on). In analogy with the attractiveness of an asset, the "quality of protection" parameters is calibrated by means of the relevant membership functions. Following the proposed approach, each value $q_i^{j,k,in}$ assigned by the risk assessor to the j^{th} PPS of the k^{th} asset, with respect to the i^{th} class of adversaries, is calibrated on the basis of the membership functions, thus obtaining a more objective value $q_i^{j,k,out}$.

Then, once individuated the sequence S_k of the $|S_k|$ global evaluation of the quality of protection is computed as

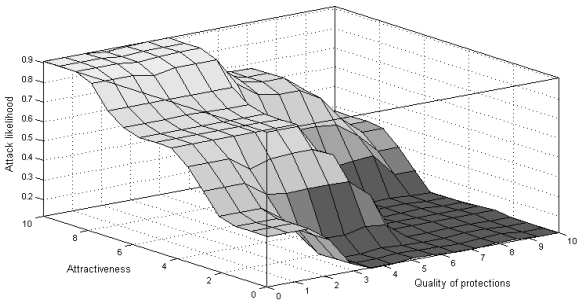

Figure 3. Attack likelihood for a generic class of adversary, computed with Matlab Fuzzy Logic Toolbox.

$$q_i^k = \frac{1}{|S_k|}\sum_{j \in S_k i} q_i^{j,k,out} \ . \quad (2)$$

Finally, by means of the Matlab Fuzzy Logic Toolbox, the QQF filter computes the attack likelihood. To do so, a set of functions similar to the one reported in Fig. 2 are calibrated, again by means of the questionnaires, for each class of adversary. The functions relate the calibrated attractiveness $a_i^{k,out}$ of the k^{th} asset and the relevant quality of protection q_i^k, giving the attack likelihood $Pa_i^k(a_i^{k,out}, q_i^k)$.

Note that these values have to be multiplied for the so-called "a-priori probabilities" of attack, that is, for the generic probability that an attack to the asset is considered. In general, these probabilities do not depend on the asset characteristics and express the fact that, in some Countries, attacks of terrorists or saboteurs are more frequent than in others; that vandals and thieves are more active in some cities than in the others, and so on. In particular, they depend on the general Homeland risk level of a Country, from the general crime level of a city, and so on.

C. The Risk Assessment Module

As said above, the RA module combines the information provided by the LA module and by the TA and MSA modules (the last throughout the QQF) and computes the risk value for each asset of the considered infrastructure.

To do so, a spatial discretization of the elements of the network is necessary, so as to refer risk to precisely geo-located sites. This discretization is driven by the following homogeneity criterion: each site, whose extension may reach few kilometers, gathers assets with the same characteristics, or different assets "collaborating" to perform a unique task. Finally, sites consisting of the same kind of assets, have be differentiated by their surrounding landscape (hills, plans, valleys), by the presence of trees or houses, and so on, that are characteristics greatly influencing the attractiveness and the protection effectiveness.

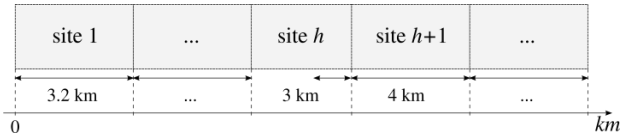

Figure 4. Example of site discretization.

Examples of sites are: tunnels, bridges, open air track stretches, passenger stations, toll gates, and so on. A graphical example of discretization of a highway or railway stretch is depicted in Fig. 4.

Then, the risk R_i^k of the k^{th} asset with respect to the i^{th} class of adversaries, is simply given by the relation

$$R_i^k = Pa_i^k \cdot D_i^k , \tag{3}$$

where D_i^k is the mean loss generated by an attack of an adversary of the i^{th} class of adversaries, and provided by the LA module.

Finally, the risk of the generic h^{th} site is assumed to be, for any class of adversaries, the maximum among the risks of all the assets in the site, that is

$$R_i^h = \max_{\forall k \in S_h} R_i^k , \tag{4}$$

where S_h is the set asset gathered in the h^{th} site.

In principle, the risk R_i^k of any generic k^{th} asset, and, more in general, the risk R_i^h of any generic h^{th} site, depends not only on the characteristics of the asset and site themselves, but also on the risk of all the other assets and sites. This mutual dependence is mainly due to the interaction between the attractiveness and the quality of protection due to the following phenomenon: securing the asset, or the site, with the highest risk often makes the other assets, or sites, more "attractive" for adversaries, thus increasing their risk level.

Then, to cope with this problem the investments should be carefully evaluated so as to globally reduce the risk level of the entire considered infrastructure. To do so, in the following, an optimization problem will be stated in order to reduce the risk of all the CI, in opposition to the problem of considering each asset of the CI independently. Such a task is performed by the PSD.

D. The Mitigation System Design Module

In this section, the second improvement to the proposed risk assessment tool architecture is described. This enhancement consists of the definition of an optimization problem for the choice of the best investment, or configuration of interventions, to make the whole considered transportation network, hereafter referred as N, globally more secure.

To do so, it is possible to state a minimization problem that considers, at a time, the risk of all the asset of the infrastructure, and takes into account the above described interactions between the attractiveness and quality of the protections of each asset.

Formally, the problem may be state as

$$\max_{C} J \tag{5}$$

with

$$J = \sum_{\forall i \in I} \alpha_i \sum_{\forall h \in N} R_i^h = \sum_{\forall i \in I} \alpha_i \sum_{\forall h \in N} \max_{\forall k \in S_h} R_i^k , \tag{6}$$

where:

- C is the set of all the possible configurations of interventions:
- I is the set of all the classes of adversaries;
- α_i is a suitable weighting term introduced to differentiate importance of the different classes of adversaries.

Note that the correlation among the risks of all the assets is hidden in the risk R_i^h, and, in particular, in the attack likelihood making it up.

As regards the problem constraints, they consist of two classes of constraints:

1. The class of *Technological Constraints* gathering the technological limitations to the interventions, such as the availability of certain kinds of sensors or physical protections, their maintainability, and so on;
2. The class of *Budget Constraints* gathering the budget limitations to the investments, both in terms of physical protections, devices, etc., and of procedures involving human operators.

At this, step, the solution of this problem consists of the definition of the set C of all the possible configurations satisfying the above constraints, and then of choosing the best one. In doing so, it is worth saying that, while in general, the set C is too large (2^n possible configurations with n possible interventions), so as to make the enumeration approach not applicable in practice. Work is in progress to apply genetic algorithms to solve it.

V. Case Study

In the first part of the section, the result of a risk assessment procedure on a case study is described. In the second part of the section, the effects of the investments in PPS in the considered network are discussed, with the aim of pointing out the importance of the optimization problem defined in Eq. (5) and Eq. (6).

A. Case Study Risk Assessment

In this section a case of study represented by a short railway stretch is presented. In particular, in the first part of the section, the risk of the considered railway stretch is assessed, whereas, in the second part, the effects of the introduction of protection systems are analyzed. Finally, some considerations about the application of the above optimization problem will be given.

TABLE I. TABLE I: SITES MAKING UP THE CONSIDERED RAILWAY STRETCH.

Section	Length of section [m]
Tunnel	500
Bridge	100
Open air section	300
Passenger station	600

Then, consider a railway stretch characterized by the following sequence of sites: tunnel – bridge – open air track – passenger station, whose characteristics are reported in Tab. I.

For these assets no particular PPS for security risk mitigation are considered, whereas, as regards the adversaries, the attention will be focused on three kinds of adversaries: Terrorists (Te), Thieves (Th), and Vandals (V).

Then, the information given for the considered sites by the risk assessor are reported in Tab II, where also the attack likelihood, computed by the QQF as above described, is reported.

As regards the highest attack likelihood values, it is worth saying that:

- Bridges are extremely vulnerable because of the easiness for vandals to make graffiti on pillars;
- Thieves may act undisturbed in open track (copper stealing is frequent along railways);
- Passenger stations represent very attractive sites for thieves, thus making their attack likelihood high;
- Passenger stations represent very attractive sites for terrorists, due to the concentration of many people.

Finally, by taking into account the average direct and indirect damages caused by the considered classes of adversaries to the considered assets, it is possible to compute the risk and build the risk profile depicted in Fig. 5, where the risk value is expressed in monetary costs.

B. Case Study Risk Mitigation

As mentioned, the proposed tool allows to evaluate and optimize, by means of the MSD module, the performances achievable with the introduction of a set of interventions able to globally reduce the risk of all the considered railway stretch. Then, by means of a feedback process, the risk value may be computed again and compared with the former one.

Then, consider the new risk values computed after having introduced a CCTV plant for monitoring the station, the bridge pillars and the tunnel access. Consider that it is not possible to design an economic CCTV plant able to control the whole open air track site (budget constraint violated), which remains, indeed, unchanged. In addition it should be taken into account that the new PPS could be seen by anyone. In effect, it is well known [14] that the visibility of the PPS may significantly influence the attractiveness of a site. In fact, the visibility of the CCTV devices discourages adversaries to attack. In Fig. 6 a comparison between the risk before and after the introduction of the CCTV is reported.

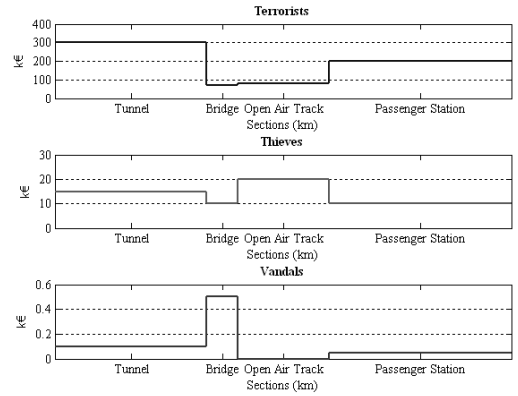

Figure 5. Level of risk of each section for each type of adversary.

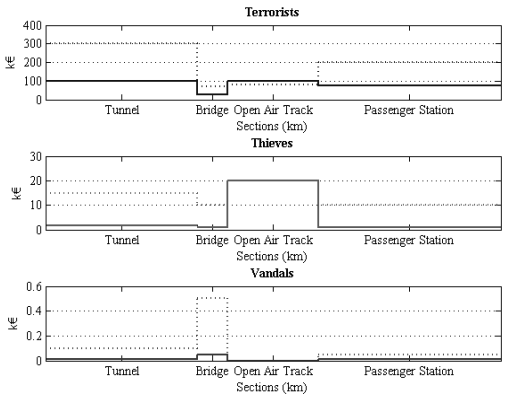

Figure 6. Comparison of the risk profiles before (dashed lines) and after (continuous lines) the introduction of a CCTV.

In such a figure it is easy to observe that, for what concerns the attacks of terrorists, the introduction of the considered PPS reduces, on one hand, the risk in three of the sites, but increases, on the other hand, the risk of the open air track. In effect, making the other sites less attractive increase the relative attractiveness of the remaining one, which does not appears to be protected. Analogously, the risk computed with respect of thieves and vandals, is reduced in the protected sites, but remains unchanged, although the last one is negligible, in the open air track site. This effect shows a well-known dynamic in PPS design: securing a single asset does not necessarily make all the entire line globally more secure, because the mitigation actions only "move" the interest of adversaries towards a less protected asset. In terms of the cost function defined in Eq. (6), having chosen $\alpha_i = 1,\ \forall i \in I$, the entire risk decreases from 705.65k€ per year to 323.57k€ per year.

The proposed architecture capability of correlating the effects of changes on individual assets and "reassessing" the level of security of the whole infrastructure, combined with the possibility of trying different kinds of securing interventions, is suitable for the best choice of investment. This aspect ensures the possibility of performing, in a short time, a reliable cost-benefit analysis, or even an

optimization stage, as the one proposed for the MSD module.

TABLE II. Characteristics of the sites and attack likelihood.

Section	Attractiveness			Quality of protections			Attack Likelihood (times/year)		
	Te	Th	V	Te	Th	V	Te	Th	V
Tunnel	6	6	2	6	6	6	10E-8	10E-6	10E-4
Bridge	2	2	7	3	3	1	10E-9	10E-8	8
Open air section	2	7	2	1	1	1	10E-5	10E-1	10E-5
Passenger station	9	1	1	9	9	1	10E-3	3	10E-9

VI. CONCLUSIONS

In this paper, the development of the tool for risk analysis and physical protection design of distributed infrastructures has been presented. The reported results represent a "second step" of a project aiming to design a tool for an easy-to-use risk analysis tool for distributed ground transportation infrastructures, such as highways, railway, and so on.

In addition, it is worth remarking that, although the kind of information provided by the new toll architecture are similar to those provided in [7], the reliability of this information is greatly improved due to the here introduced QQF. The model now is not influenced by the perception of who is inserting the data, whose opinions and experiences are "filtered" by means of the experience of the experts that have contributed to calibrate the tool. As regards the future improvement of the tool, work is in progress to apply genetic algorithms to the solution of the described optimization algorithm.

REFERENCES

[1] "Final report," U.S. Department of Transportation. Transit Security Design Considerations, 2004.

[2] Presidency and CT Coordinator, "The European Union Counter-Terrorism Strategy," pp. 1-17, 2005.

[3] EU Commission, "Directive 2008/114/CE on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection," 2008.

[4] T. G. Lewis, *Critical Infrastructure Protection in Homeland Security – Defending a Networked Nation*, Wiley Interscience, 2006.

[5] T. Macaulay, *Critical Infrastructures*, CRC Press, 2008.

[6] B. J. Garrick, J. E. Hallb, M. Kilgerc, J. C. McDonaldd, T. O'Toolee, P. S. Probstf, E. Rindskopf Parkerg, R. Rosenthalh, A. W. Trivelpiecei, L. A. Van Arsdalej, and E. L. Zebroskik, "Confronting the risks of terrorism: making the right decisions," *Reliability Engineering & System Safety*, vol. 86, n. 2, pp. 129-176, 2004.

[7] A. Di Febbraro, F. Papa, and N. Sacco, "A Tool for Risk Analysis and Protection Design of Railway Infrastructures," in *Proc. of 89th TRB Annual Meeting*, 2010.

[8] J. N. Hood, T. Olivas, C. B. Slocter, B. Howard, and D. P. Albright, "Vulnerability Assessment Through Integrated Transportation Analysis," in *Transportation Research Record No. 1822*, pp. 18-23, 2003.

[9] C. N. Y. Fink, "Antiterrorism Security and Surface Transportation Systems - Review of Case Studies and Current Tactics," in *Transportation Research Record No. 1822*, pp. 9-17, 2003.

[10] G. E. Apostolakis and D. M. Lemon, "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism," in *Risk Analysis*, vol. 25, n. 2, pp. 361-376, Wiley, 2005.

[11] A. Di Febbraro and N. Sacco, "A Petri-Net based approach for the interdependence analysis of Critical Infrastructures in transportation networks," in *Proc. 12th World Conference on Transportation Research*, 2010.

[12] J. H. Lambert and M. W. Farrington, "Cost-benefit functions for the allocation of security sensors for air contaminants," *Journal of Reliability Engineering & System Safety*, vol. 92, n. 7, pp. 930-946, 2007.

[13] D. Brand, S. R. Mehndiratta, and T. E. Parody, "Options Approach to Risk Analysis in Transportation Planning," in *Transportation Research Record No 1706*, pp. 54-63, 2000.

[14] M. L. Garcia. *The Design and Evaluation of Physical Protection Systems*, Elsevier 2001

[15] L. A. Zadeh, "Fuzzy algorithms," in *Information and Control*, 1968.

[16] J. K. George, B. Yuan, *Fuzzy Sets and Fuzzy Logic*, Prentice Hall PTR, 1995.

[17] V. Ravi, P.J Reddy, H. Zimmermann, "Fuzzy global optimisation of complex system reliability," *IEEE Transactions on Fuzzy Systems*, vol. 8, n. 3, pp. 241–248, 2000.

[18] A. Pillay and J. Wang, "Modified failure mode and effects analysis using approximate reasoning," in *Reliability Engineering and Systems Safety*, vol. 79, pp. 69-85, 2003.

[19] C. Johnson and C. M. Holloway, "A survey of logic formalisms to support mishap analysis," in *Reliability Engineering and System Safety*, vol. 80, pp. 271–291, 2003.

Angela Di Febbraro was born in Ronco Scrivia, Italy, on November 23rd, 1963. She received the Laurea degree in Electronic Engineering in 1987, and the Ph.D. Degree in Computer Science and Electronic Engineering in 1992, both at the University of Genoa.

Her main research interests are in modeling, optimization, and control of freeway, interurban, and urban transportation systems, and of logistic systems. She has been Assistant Professor at the University of Genoa, and Associate Professor at the Polytechnic of Turin, Italy. Since 2005 she is Full Professor of Transportation at the University of Genoa.

Prof. Di Febbraro is member of EURO Working Group on Transportation, and has been co-editor of different special issues of international scientific journals, and reviewer of both international scientific books, and papers submitted to different journals and periodic international conferences, especially for IEEE and IFAC.

Federico Papa was born in Genoa, Italy on January 25th, 1985. In 2009, he received the Laurea Degree in Transportation and Logistics Engineering, with a dissertation on the design and the development of an innovative tool for assessing the security of rail infrastructures.

Since 2010, he has been at University of Genoa as a grant holder for a research on critical analysis of systems to mitigate the risks related to vandalism and terrorism attacks to railway assets.

Currently, Eng. Papa is a Ph.D. student and is involved in European research projects aiming to improve railway safety and security.

Nicola Sacco was born in Borgosesia, Italy, on December 4th, 1976. He received the Laurea degree in electronic engineering and the Ph.D. degree in Automatics and Computer Sciences for Transportation Systems at the Polytechnic of Turin, Turin, Italy, in 2000 and 2004, respectively. His main research interests include Petri nets, modeling, control, and optimization of hybrid systems, with special applications to intelligent transportation systems and environmental systems.

He currently is a Assistant professor at University of Genoa.

Dr. Sacco is member of EURO Working Group on Transportation, and reviewer of both national and international scientific books, and papers submitted to different journals and periodic international conferences.