Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures

Francesco Flammini[1 2], Andrea Gaglione[2], Nicola Mazzocca[2], Concetta Pragliola[1]

[1] ANSALDO STS - Ansaldo Segnalamento Ferroviario S.p.A.
Via Nuova delle Brecce 260, Naples, Italy
{flammini.francesco, pragliola.concetta}@asf.ansaldo.it
[2] Università di Napoli "Federico II"
Dipartimento di Informatica e Sistemistica
Via Claudio 21, Naples, Italy
{frflammi, andrea.gaglione, nicola.mazzocca}@unina.it

Abstract. Scientists have been long investigating procedures, models and tools for the risk analysis in several domains, from economics to computer networks. This paper presents a quantitative method and a tool for the security risk assessment and management specifically tailored to the context of railway transportation systems, which are exposed to threats ranging from vandalism to terrorism. The method is based on a reference mathematical model and it is supported by a specifically developed tool. The tool allows for the management of data, including attributes of attack scenarios and effectiveness of protection mechanisms, and the computation of results, including risk and cost/benefit indices. The main focus is on the design of physical protection systems, but the analysis can be extended to logical threats as well. The cost/benefit analysis allows for the evaluation of the return on investment, which is a nowadays important issue to be addressed by risk analysts.

Keywords: Security, Quantitative Approaches, Risk Analysis, Cost/Benefit Evaluation, Critical Infrastructure Protection, Railways.

1. Introduction

Risk analysis is a central activity in the security assurance of critical railway transportation infrastructures and mass transit systems. In fact, the results of risk analysis are needed to guide the design of surveillance and protection systems [11].

Risk analysis is commonly performed using qualitative approaches, based on expert judgment and limited ranges for risk attributes (e.g. low, average, high) [10]. However, model-based quantitative approaches are more effective in determining the risk indices by taking into account the frequency of occurrence of threats (e.g. considering historical data) and analytically determining the consequences (damage of assets, service interruption, people injured, etc.). This allows for a fine tuning of the security system in order to optimize the overall investment.

Usually, analysts refer to Risk Assessment as the process of measuring the expected risk as a combination of threat occurrence probability, system vulnerability and expected damage. Risk Management (or mitigation) is instead used to indicate the process of choosing the countermeasures and predicting their impact on risk reduction. The overall process (which can be iterative) is often referred to as risk analysis. While it does not seem to exist a generally accepted taxonomy, this is the meaning we will give to such terms in this paper.

This paper concentrates on quantitative risk analysis approaches. There exist several issues related to the choice of implementing quantitative, analytical or model-based approaches: one is the availability of source data; another is the methodology to be used for the analysis, which is not straightforward.

Several approaches to the risk analysis of critical infrastructures are available in the literature (see e.g. references [1]-[6]), but no one seems to precisely fit the specific application, since they are either qualitative, too much general (hence abstract) or tailored to different applications. In this paper we present the core of a quantitative framework based on a reference mathematical model (partly derived from [8]) supported by a specifically designed software tool. In particular, we have extended the classical risk equation in order to precisely evaluate the impact on risk indices of parameters related to protection mechanisms. This allows to achieve a balance between the investment on security technologies and the achieved risk mitigation. The method has been developed and experimented considering a railway transportation domain, but it is general enough to be adopted for the analysis of other types of critical infrastructures. At the moment, we have implemented a full working prototype of the tool to be adopted for risk evaluation and to support the design of security systems.

The rest of this paper is organized as follows. Section 2 presents the method used for the analysis. Section 3 describes the aim and the features of the software tool we have developed. Section 4 provides an example application of quantitative risk analysis using the tool. Finally, Section 5 draws conclusions and provides some hints about future developments.

2. The method

With reference to a specific threat, the quantitative risk R can be formally defined as follows:

$$R = P \cdot V \cdot D \ . \tag{1}$$

Where:

- P is the frequency of occurrence of the threat, which can be measured in [events / year];

- *V* is the vulnerability of the system with respect to the threat, that is to say the probability that the threat will cause the expected consequences (damage);
- *D* is an estimate of the measure of the expected damage occurring after a successful attack, which can be expressed in euros [€].

The vulnerability V is an adimensional parameter, since it represents the conditional probability:

$$P(success \mid threat) \ . \tag{2}$$

Therefore, a quantitative way to express the risk associated to a specific threat is to measure it in lost euros per year: [€ / year]. The overall risk can be obtained as the sum of the risks associated to all threats.

Despite of the simplicity of (1), the involved parameters are not easy to obtain. The analysis involves both procedural and modeling aspects. Procedural aspects include brainstorming sessions, site surveys, design review, statistic data analysis, expert judgment, etc. Formal modeling languages which can be used to analytically compute P, V and D include Attack Trees, Bayesian Networks, Stochastic Petri Nets and possibly other formalisms which are able to take into account the uncertainty inherently associated to the risk as well as the possibility of strategic attacks [7]. In fact, the three parameters feature an inter-dependence which should be modeled, too.

Protection mechanisms are able to reduce the risk by having three main effects:

- Protective, aimed at the reduction of *V*
- Deterrent, aimed at the reduction of *P*
- Rationalizing, aimed at the reduction of *D*

Therefore, by quantifying the listed effects it is possible to estimate the risk mitigation, considering any combination of threats and protection mechanisms.

A possible way to compute risk mitigation is to associate threats and protection mechanisms by means of threat categories and geographical references, namely sites. A site can be considered as a particular kind of critical asset (actually, an aggregate asset), sometimes defined as “risk entity”. Each threat happens in at least one site and, homogonously, each protection mechanism protects at least one site. For a railway infrastructure, a site can be an office, a bridge, a tunnel, a parking area, a platform, a control room, etc.

In the assumption that:

- Threat *T* belongs to category *C*;
- Threat *T* happens in (or passes through) site *S*;
- Protection *M* is installed in site *S*;
- Protection *M* is effective on threat category *C*;

then it can be affirmed that *M* protects against *T*.

Basing on the above definitions, it is possible to express the overall risk to which the system is exposed as follows:

$$R_T = \sum_i R_i \cdot \prod_j (1 - E_{Pji} \cdot COV_j) \cdot (1 - E_{Dji} \cdot COV_j) \cdot (1 - E_{Rji} \cdot COV_j) \ . \quad \textbf{(3)}$$

Where:

- R_T is the total mitigated risk;
- R_i is the initial risk associated to threat *i* (computed according to (1));
- E_{Pji} is an estimate of the protective effect of mechanism *j* on threat *i*;
- E_{Dji} is an estimate of the deterrent effect of mechanism *j* on threat *i*;
- E_{Rji} is an estimate of the rationalizing effect of mechanism *j* on threat *i*;
- COV_{ji} is a measure of the coverage of mechanism *j* (e.g. percentage of the physical area or perimeter of the site).

The values of parameters expressing coverage and effectiveness are in the range [0..1]. The formula can be validated by attempts using sample data and boundary analysis: for instance, when both the coverage and one of the effectiveness parameters are set to 1, the risk is mitigated to 0, as expected; on the opposite, if either the coverage or all the effectiveness parameters are set to 0, the risk is not mitigated at all. Fig. 1. reports an example risk evaluation based on (3) using sample data. In such evaluation it is assumed that a single protection mechanism is used and all the other data is kept constant.

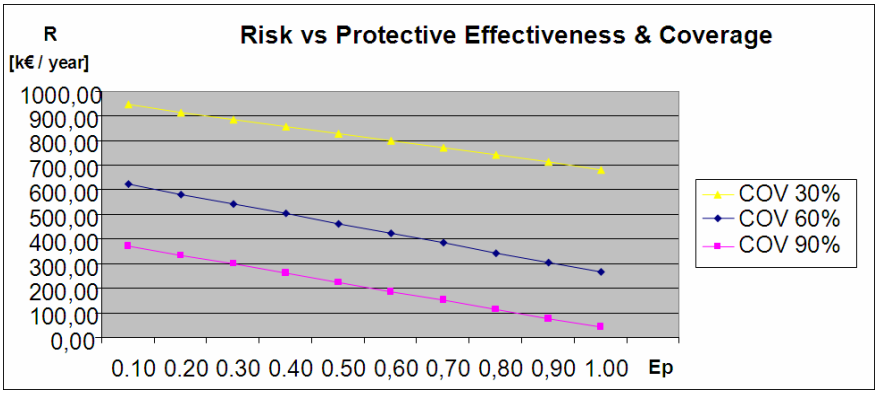

Fig. 1. Risk evaluation using sample data.

The cost/benefit index can be defined simply as the balance between the investment on security mechanisms and the achieved risk mitigation:

$$EB = \text{risk reduction} - \text{total investment in security} = (\mathrm{R_T} - \sum_i R_i) - \sum_{\mathrm{j}} \mathrm{C_j} \ . \quad \textbf{(4)}$$

Where:

- *EB* is the Expected Benefit, which can be positive or negative;
- $\mathrm{C_j}$ is the cost of the protection mechanism *j*, obtained considering all the significant costs (acquisition, installation, management, maintenance, etc.).

Therefore, the return on investment can be obtained from the expected benefit EB considering the cost of the invested capital (which depends on the rate of interest, the years to pay-off, possible external funding, etc.).

Expressions (3) and (4) need to be computed starting from a database of attack scenarios, sites, protection mechanisms and related significant attributes. The management of such data and the computation of results are performed by an automatic tool which will be described in detail in next section.

3. The tool

A tool has been developed which automatically manages risk data and evaluates risk and benefit indices starting from input data. The tool has been named simply Q-RA (Quantitative Risk Analysis), to be pronounced as [kura] (sounding like the Italian for “cure”).

In particular, the inputs of the tool are:

- A list of threats, characterized by:
  - Threat identifier;
  - Short description of the attack scenario (including the adversary category, required tools, etc.);
  - Threat category (e.g. vandalism, theft, sabotage, terrorism, flooding, etc.);
  - Initial estimated *P*, *V* and *D;*
  - Site (geographical reference).
- A list of protection mechanisms, characterized by:
  - Protection mechanism identifier;
  - Short description of the mechanism;
  - List of threat categories on which the mechanism is effective;

- Expected protective (E_{Pji}), deterrent (E_{Dji}) and rationalizing (E_{Rji}) effectiveness;
- Estimated coverage (*COV*);
- Site (geographical reference);
- Annual cost (acquisition, management, maintenance, ecc.).

A database is used in order to store and correlate the input data. Data referring to economic aspects is also managed (number of years to dismiss, rate of interest, etc.). The tool provides features allowing the user for inserting the inputs, updating them to modify some parameters (i.e. frequency of threats) and finally removing them.

Parameters can be chosen using average or worst case considerations. Sensitivity analysis can be performed acting on input data ranges in order to evaluate the effect of uncertainty intervals upon the computed results and possibly defining lower and upper bounds.

The tool elaborates data according to the relationships defined in the database (in particular, using the common attributes of site and threat category) and the mathematical models of (3) and (4), providing:

- The risk associated to each threat (R_i) and the overall risk (R_T);
- The total risk reduction considering all the threats;
- Annual cost of the single protection mechanism and of the whole security system;
- Annual cost/benefit balance (*EB*).

The points listed above are part of the informal functional requirements specification. Application specific requirements have also been added, like the possibility of specifying a day/night attribute for both threats (some scenarios can not happen when the service is interrupted, e.g. a subway station is closed to the public) and protection mechanisms (some mechanisms, e.g. motion detection, can be activated only when the service is interrupted). Non functional requirements of the tool include user friendliness, data import / export facilities using standard formats (e.g. CSV, Comma Separated Values), platform independence and use of freeware software (possibly), user identification and rights management (still to be implemented).

Some implementation details are reported in the following. The software design has been performed using an object-oriented approach based on the Unified Modeling Language (UML) and the Java programming language. In order to guarantee the persistence of objects (threats, protection mechanisms and sites), a relational database (based on MySQL) has been designed starting from Entity Relationship (E-R) diagrams. The GUI (Graphical User Interface) of the tool is web-based, exploiting JSP (Java Server Page) and Apache Tomcat technologies.

As an example, the conceptual class diagram related to the specific domain is reported in Fig. 2, where the attributes and interrelationships of the entities described in the previous section are graphically shown.

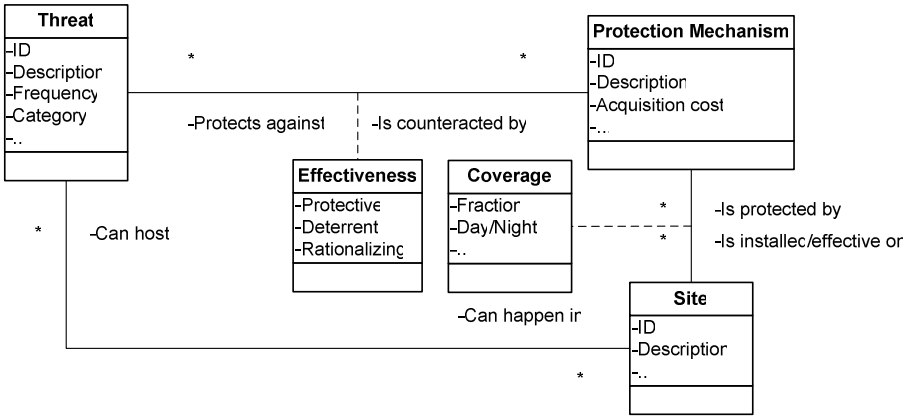

Fig. 2. Conceptual class diagram.

4. Example application

Let us consider a case-study of a railway or subway station. The following threats against the infrastructure should be considered:

- Damage to property and graffitism (vandalism);
- Theft and aggressions to personnel and passengers (micro-criminality)
- Manumission and forced service interruption (sabotage)
- Bombing or spread of NBCR[1] contaminators (terrorism)

Let us consider the example scenarios reported in Table 1 and the protection mechanisms listed in Table 2, both referring to a specific station. It is assumed that the values are obtained by analyzing historical data of successful and unsuccessful attacks before and after adopting specific countermeasures (such data is usually available for comparable installations). The expected damage relates to the single attack and it is computed by predicting the expense needed to restore the assets and the possible consequences of service interruption (no human injury or loss is considered). The estimated annual cost of the protection mechanisms also accounts for maintenance and supervision, while acquisition and installation costs are accounted separately. Please note that the effect of protection mechanisms may vary according to threat category. Furthermore, all the specified values should not be

[1] Nuclear Bacteriologic Chemical Radiologic.

considered as real. The choice of real values would require an extensive justification, possibly via a model-based analysis, which is not in the scope of this paper.

Fig. 3 reports a screenshot of the GUI representing the input mask for the attributes of protection mechanisms, while Fig. 4 reports the results of the example application computed by the tool. In the assumptions of the example, the positive expected benefit resulting from the adoption of the protection mechanisms clearly justifies the investment, the total benefit being 36722 €/year.

Table 1. Attack scenarios considered in the example application.

THREAT ID	THREAT DESCRIPTION	THREAT CATEGORY	SITE	EST. P [# / YEAR]	EST. V_{INIT}	EXP. ASSET D [K€]	EXP. SERVICE D [K€]
1	GRAFFITISM	VANDALISM	STATION EXT.	60	0.9	0.5	0
2	THEFT OF PCS	THEFT	TECH. ROOM	4	0.8	8	6
3	GLASS BREAK	VANDALISM	STATION EXT.	12	1	0.5	0
4	BOMBING	TERRORISM EXPL.	PLATFORM	0.01	1	600	300
5	HACKING	SABOTAGE	TLC SERVER	2	0.8	0	10
6	GAS ATTACK	TERRORISM CHEM.	PLATFORM	0.01	1	10	150
7	FURNITURE DAMAGE	VANDALISM	HALL	70	1	0.1	0
			PLATFORM	50	1	0.1	0
8	INFRASTRUCT. DAMAGE	PHYSICAL SABOTAGE	PLATFORM	4	0.9	5	0

Table 2. Protection mechanisms considered in the example application.

PROT. ID	COUNTERMEASURE DESCRIPTION	ACQ. COST [K€]	MANAG. COST [K€ / YEAR]	SITE	COV	THREAT CATEGORIES	E_P	E_D	E_R
1	ALARMED FENCE	10	1	STATION EXT. STATION INT. (NIGHT)	0.9	VANDALISM THEFT P. SABOTAGE	0.9 0.9 0.9	0.3 0.3 0.3	0.2 0.2 0.2
2	VOLUMETRIC DETECTOR	5	1	TECH. ROOM	1	THEFT	0.8	0.6	0.2
3	VIDEO-SURVEILLANCE (INTERNAL)	150	20	HALL, PLATFORM	0.95	VANDALISM THEFT SABOTAGE TERRORISM EXPL. TERRORISM CHEM.	0.4 0.6 0.6 0.4 0.4	0.6 0.6 0.6 0.3 0.3	0.3 0.3 0.8 0.6 0.6
4	CHEM. DETECTOR	50	2	PLATFORM	0.9	TERRORISM CHEM.	0.6	0.2	0.4
5	INTRUSION DETECTION SYSTEM	1	0.5	TLC SERVER	1	L. SABOTAGE	0.9	0	0
6	EXPLOSIVE DETECTOR	50	2	STATION INT. (*)	1	SABOTAGE TERRORISM EXPL.	0.8 0.8	0.4 0.1	0.1 0.1

(*): detectors are physically installed near turnstiles, but the protection is effective on the whole station internal.

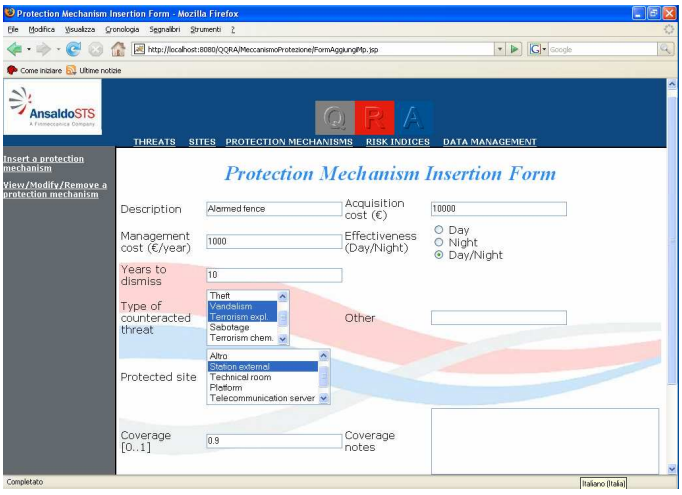

Fig. 3. The Q-RA input data mask for protection mechanisms.

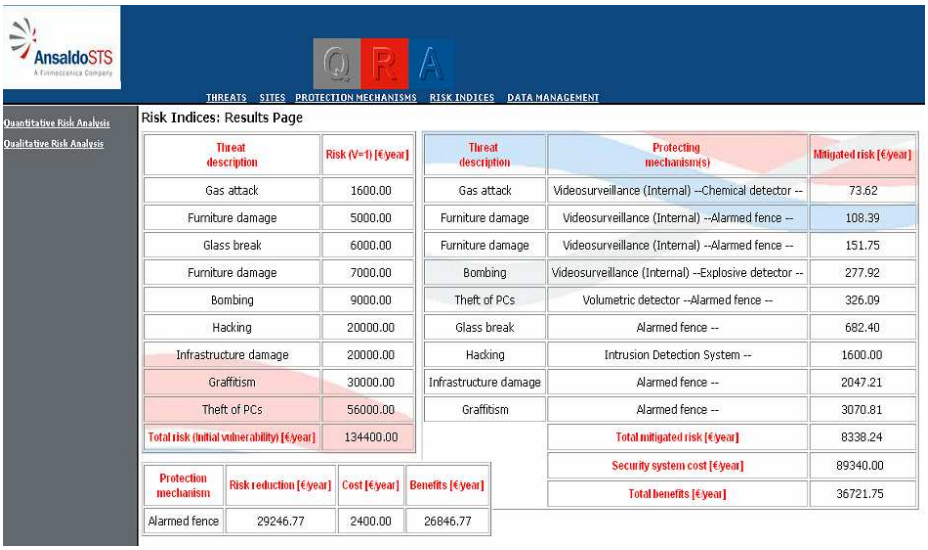

Fig. 4. Q-RA output data presentation for the example application.

5. Conclusions

In this paper, a method and a support tool for the quantitative security risk analysis of critical infrastructures have been described. The method has been developed to address the risk management of railway infrastructures mainly considering physical threats. However, we believe that the considerations on the base of the method do not limit its application to a specific infrastructure neither prevent the analysis of logical security. For instance, a site can be thought of as a logical point in which a hacker attack can be performed by exploiting one or more flaws.

For attacks involving persons (injury or kill), a quantification of consequences, though possible, is not generally accepted. Therefore, qualitative approaches can be applied separately to such classes of threats. The Q-RA tool is also intended for the integration of qualitative analysis by means of associative tables [10].

The automation provided by the tool also eases the analysis of parametric sensitivity in order to assess how error distributions in the input values affect the overall results.

Finally, it is possible to extend the tool with functionalities of cost/benefit optimization (e.g. by genetic algorithms), considering limited budget constraints. In such a way, the optimal set of protection mechanism minimizing the risk can be automatically determined.

References

1. Asis International: General Security Risk Assessment Guideline http://www.asisonline.org/guidelines/guidelinesgsra.pdf (2008)
2. Broder, J.F.: Risk Analysis and the Security Survey. Butterworth-Heinemann (2006)
3. Garcia, M.L.: Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann (2005)
4. Lewis, T.G.: Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. John Wiley (2006)
5. Meritt, J. W.: A Method for Quantitative Risk Analysis, http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf (2008)
6. Moteff, J.: Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. CRS Report for Congress, The Library of Congress (2004)
7. Nicol, D.M., Sanders, W.H., Trivedi, K.S.: Model-based evaluation: from dependability to security. In Dependable and Secure Computing, IEEE Transactions on, Vol.1, Iss.1, pp. 48-65 (2004)
8. SANDIA National Laboratories: A Risk Assessment Methodology for Physical Security. White Paper, http://www.sandia.gov/ram/RAM%20White%20Paper.pdf (2008)
9. Srinivasan, K. Transportation Network Vulnerability Assessment: A Quantative Framework. Southeastern Transportation Center – Issues in Transportation Security (2008)
10. U.S. Department of Transportation: The Public Transportation Security & Emergency Preparedness Planning Guide. Federal Transit Administration, Final Report (2003)
11. U.S. Department of Transportation: Transit Security Design Considerations. Federal Transit Administration, Final Report (2004)
12. Wilson, J. M., Jackson, B.A., Eisman, M., Steinberg, P., Riley, K.J.: Securing America's Passenger-Rail Systems. Rand Corporation (2007)