3rd International Workshop on Critical Information Infrastructures Security
CRITIS'08
October 13-15 2008, Frascati (Rome), Italy

F. Flammini, A. Gaglione, N. Mazzocca, C. Pragliola

Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures

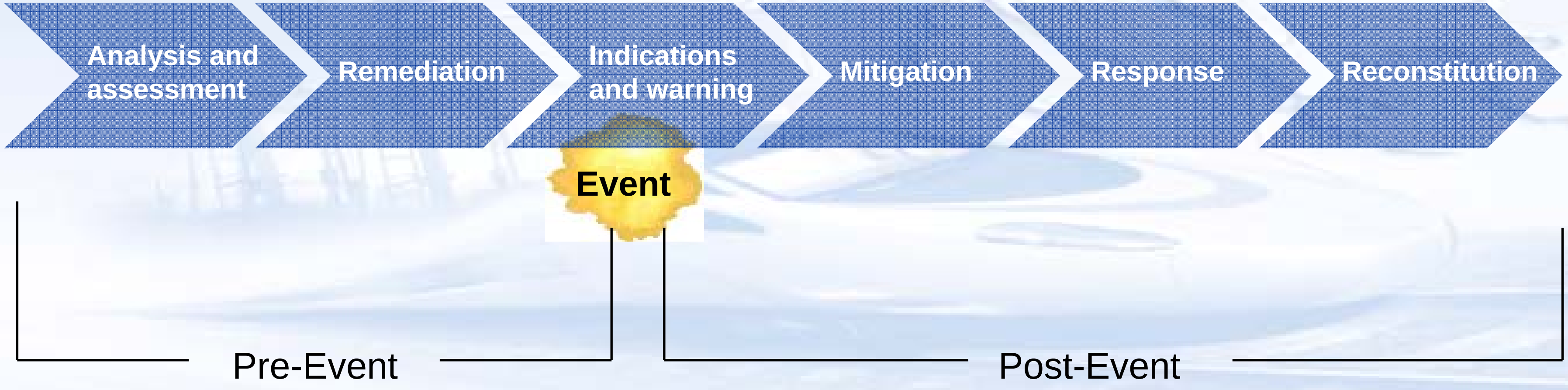
presented by

Francesco Flammini

Ansaldo STS Italy – Business Innovation Unit
University Federico II of Naples – Department of Computer and Systems Engineering

Critical Infrastructure Security

- Railway and Subway transportation systems are exposed to threats ranging from vandalism to terrorism
- CIP life-cycle:



Risk Analysis

- Risk Analysis
  - Qualitative
  - Quantitative
- Iterative steps
  - Risk Assessment
  - Risk Mitigation
- Main objective of traditional (qualitative) approaches
  - Evaluation of most relevant vulnerabilities
- Advantages of quantitative approaches
  - More precise results
  - Support the design of protection mechanism
  - Evaluation of the return on investment

Quantitative Definition of Risk

$$R = P \cdot V \cdot D$$

- *P* : threat frequency [events / year]
- *D* : expected damage [€]
- *V* : system vulnerability w.r.t threat (adimensional)

$$P(success \mid threat)$$

Therefore, the Risk can be expressed in [€ / year] (monetary loss)

Effect of Protection Mechanisms

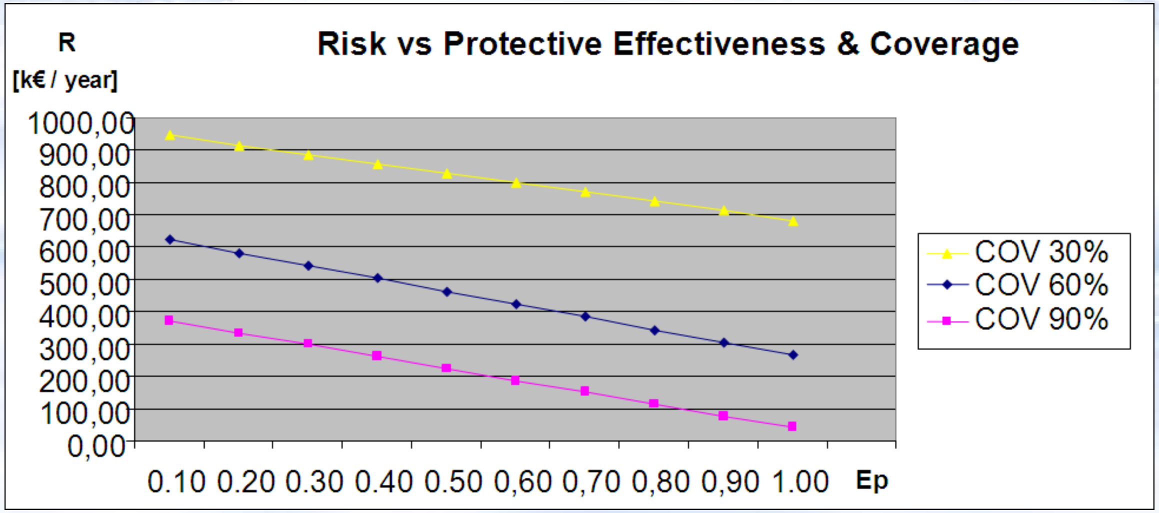
- Protection mechanisms are able to reduce the risk by having three main effects:
  - Protective, aimed at the reduction of V
  - Deterrent, aimed at the reduction of P
  - Rationalizing, aimed at the reduction of D
- In the assumption that:
  - Threat T belongs to category C
  - Threat T happens in (or passes through) site S
  - Protection M is installed in site S
  - Protection M is effective on threat category C

then it can be stated that <u>M protects against T</u>

Extensive Risk Formula

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

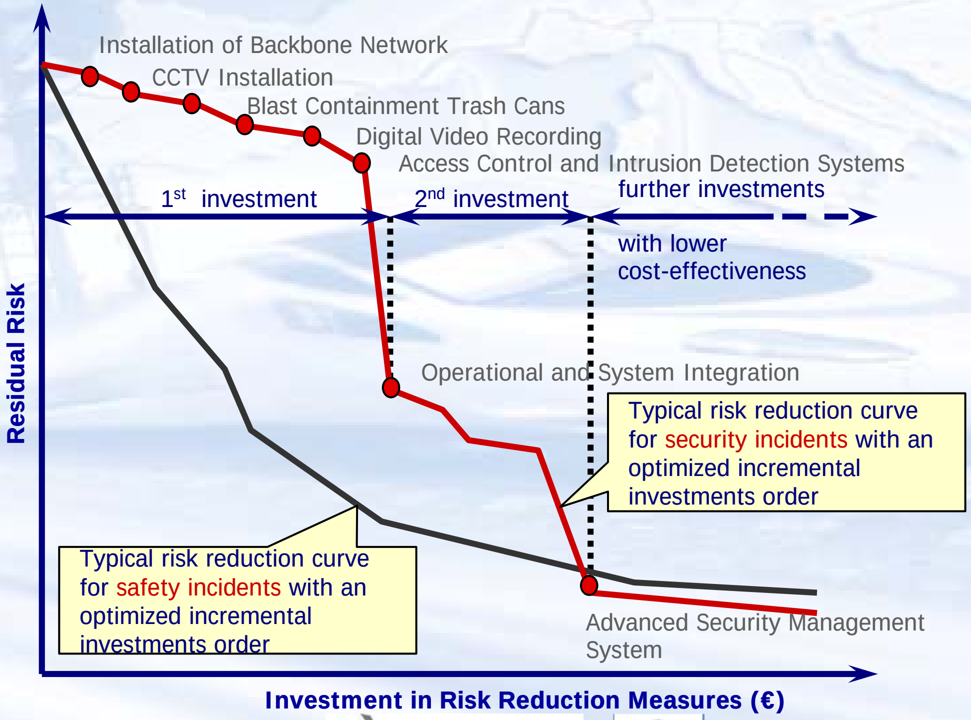
- *Rt* is the total mitigated risk
- *Ri* is the initial risk associated to threat *i*
- *Epji* is an estimate of the protective effect of mechanism *j* on threat *i*
- *Edji* is an estimate of the deterrent effect of mechanism *j* on threat *i*
- *Erji* is an estimate of the rationalizing effect of mechanism *j* on threat *i*
- *COVji* is a measure of the coverage of mechanism *j* (e.g. percentage of the physical area or perimeter of the site)



Return on investment

$$EB = \text{risk reduction} - \text{total investment in security} = (\mathrm{R_T} - \sum_i R_i) - \sum_j \mathrm{C_j}$$

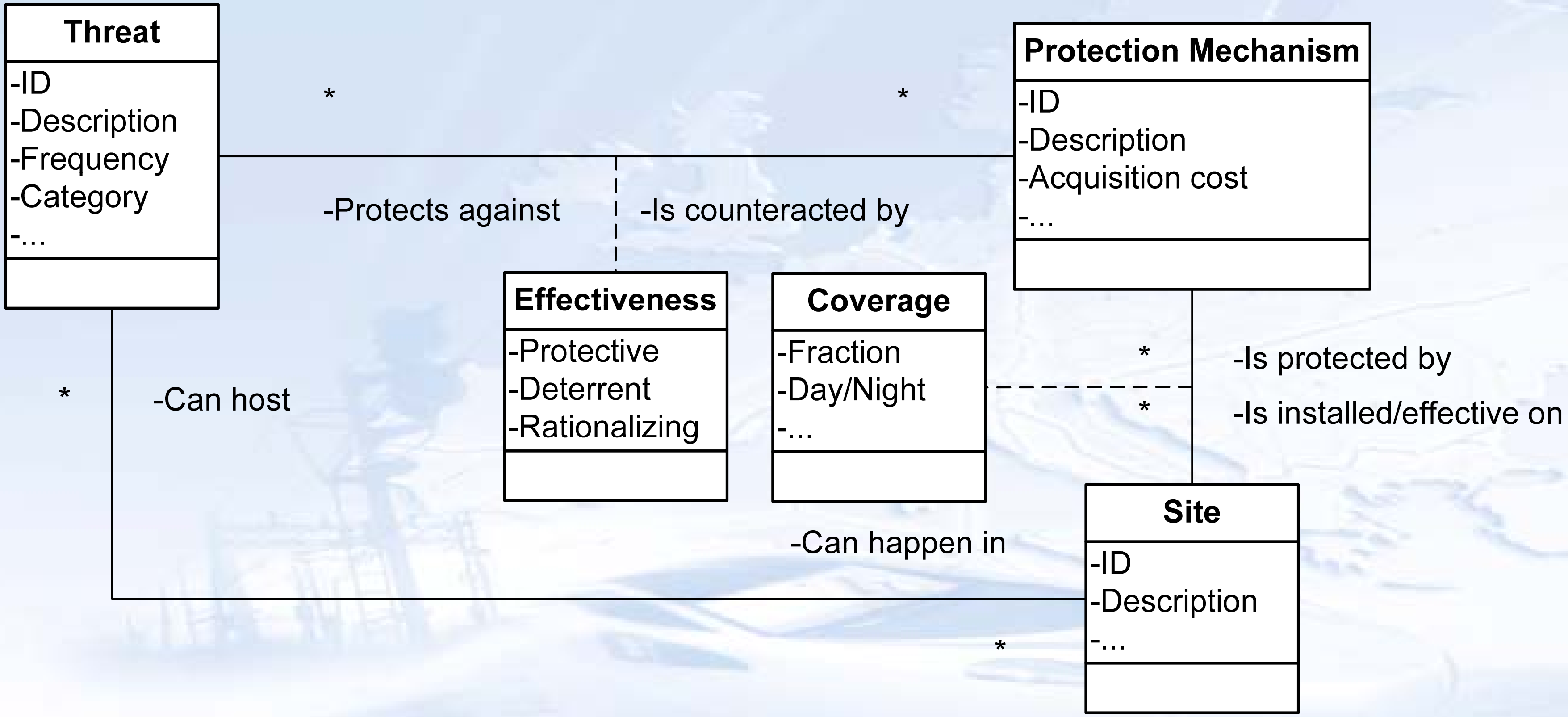
- *EB* is the Expected Benefit, which can be positive or negative
- *Cj* is the cost of the protection mechanism *j*, obtained considering all the significant costs (acquisition, installation, management, maintenance, etc.)



Typical risk reduction curve for security incidents with an optimized incremental investments order

Typical risk reduction curve for safety incidents with an optimized incremental investments order

The Q-RA tool: software architecture



Threat
-ID
-Description
-Frequency
-Category
-...

Protection Mechanism
-ID
-Description
-Acquisition cost
-...

Effectiveness
-Protective
-Deterrent
-Rationalizing

Coverage
-Fraction
-Day/Night
-...

Site
-ID
-Description
-...

-Protects against

-Is counteracted by

-Can host

-Is protected by

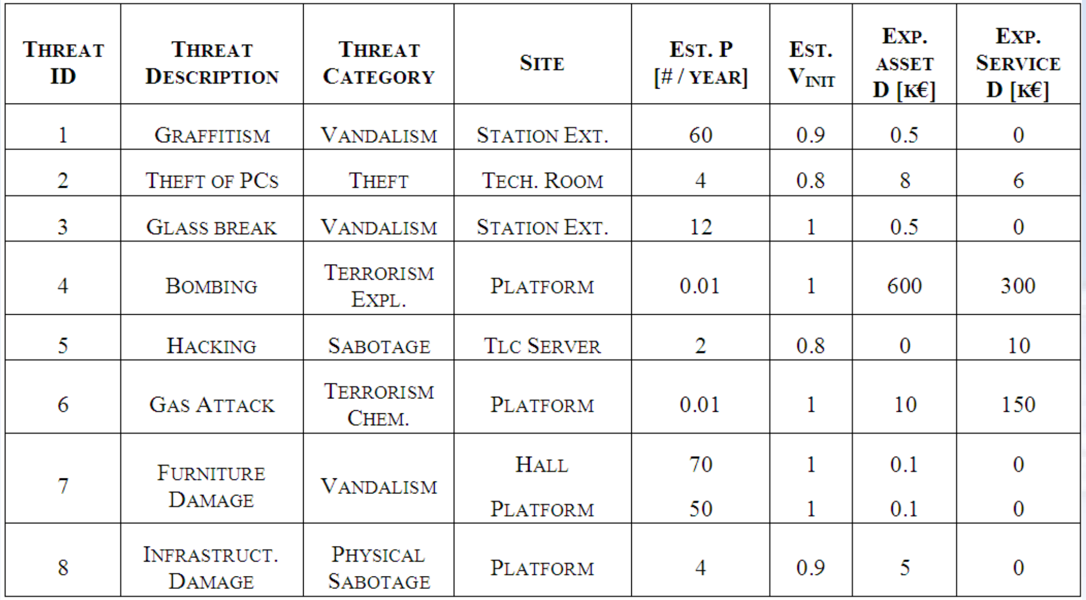
-Is installed/effective on

-Can happen in

*

- Languages / technologies employed in design and implementation of the tool:
  - UML, MySQL, JSP, Apache Tomcat

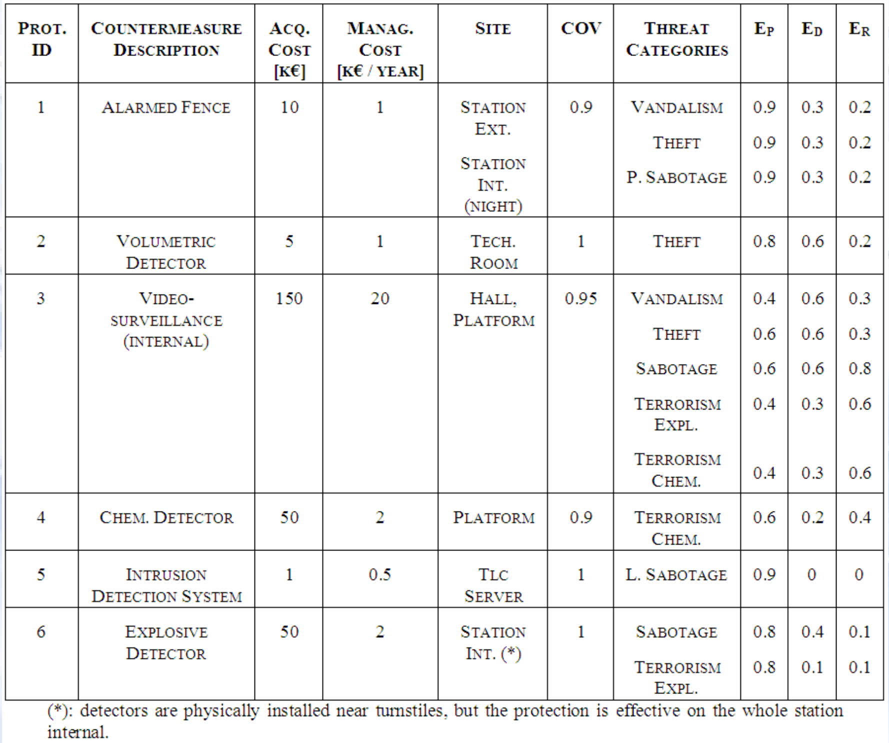
Example application



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

THREATS

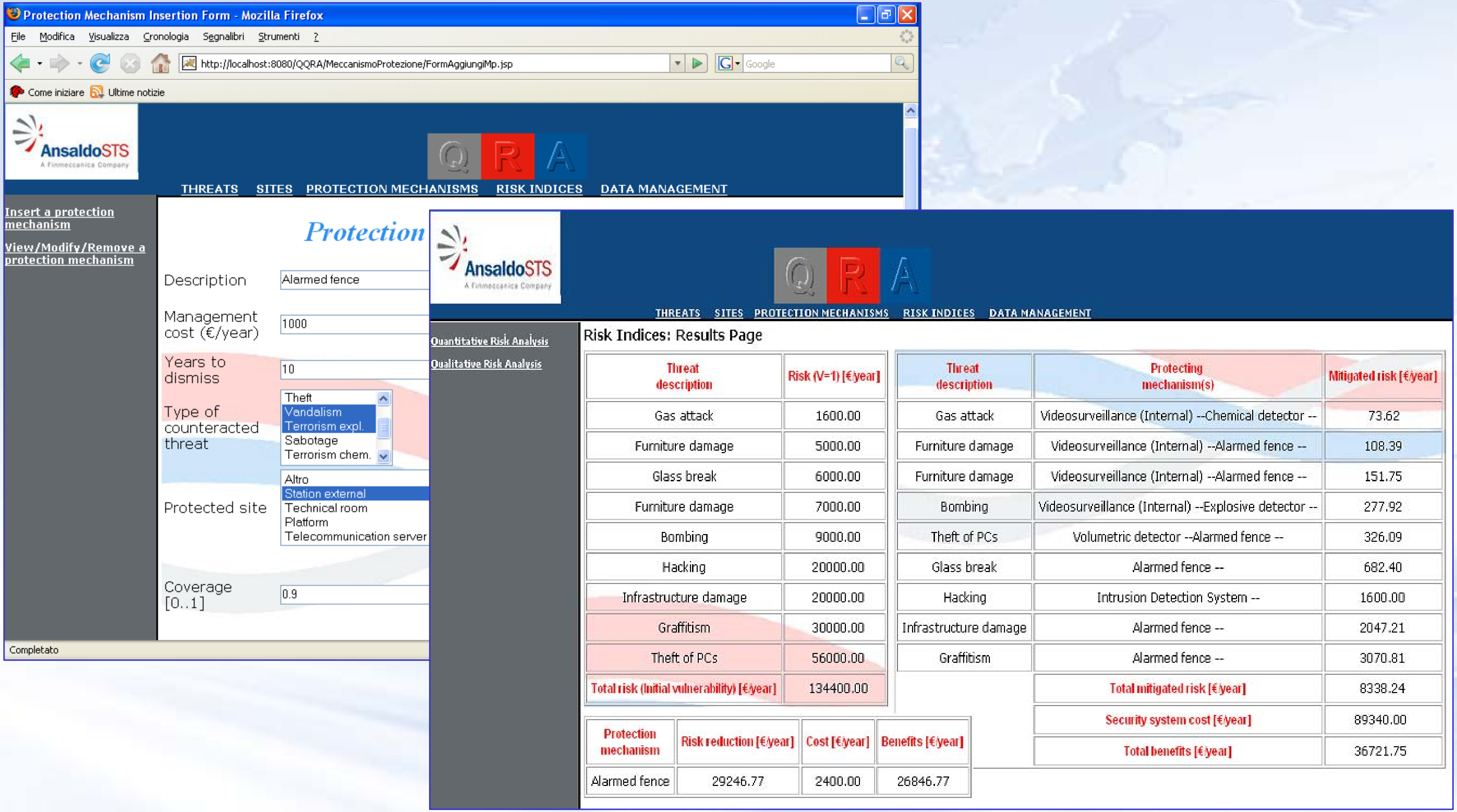
PROTECTION MECHANISMS



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	0.9	0.3	0.2
						Theft	0.9	0.3	0.2
						P. Sabotage	0.9	0.3	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	0.4	0.6	0.3
						Theft	0.6	0.6	0.3
						Sabotage	0.6	0.6	0.8
						Terrorism Expl.	0.4	0.3	0.6
						Terrorism Chem.	0.4	0.3	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	0.8	0.4	0.1
						Terrorism Expl.	0.8	0.1	0.1

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

Q-RA GUI: example inputs and outputs


Protection Mechanism Insertion Form - Mozilla Firefox
File Modifica Visualizza Cronologia Segnalibri Strumenti ?
http://localhost:8080/QQRA/MeccanismoProtezione/FormAggiungiMp.jsp
Google
Come iniziare Ultime notizie
AnsaldoSTS
A Finmeccanica Company
QRA
THREATS SITES PROTECTION MECHANISMS RISK INDICES DATA MANAGEMENT
Insert a protection mechanism
View/Modify/Remove a protection mechanism
Protection
Completato
Quantitative Risk Analysis
Qualitative Risk Analysis

Description	Alarmed fence
Management cost (€/year)	1000
Years to dismiss	10
Type of counteracted threat	Theft Vandalism Terrorism expl. Sabotage Terrorism chem.
Protected site	Altro Station external Technical room Platform Telecommunication server
Coverage [0..1]	0.9

Risk Indices: Results Page

Threat description	Risk (V=1) [€/year]
Gas attack	1600.00
Furniture damage	5000.00
Glass break	6000.00
Furniture damage	7000.00
Bombing	9000.00
Hacking	20000.00
Infrastructure damage	20000.00
Graffitism	30000.00
Theft of PCs	56000.00
Total risk (Initial vulnerability) [€/year]	134400.00

Threat description	Protecting mechanism(s)	Mitigated risk [€/year]
Gas attack	Videosurveillance (Internal) --Chemical detector --	73.62
Furniture damage	Videosurveillance (Internal) --Alarmed fence --	108.39
Furniture damage	Videosurveillance (Internal) --Alarmed fence --	151.75
Bombing	Videosurveillance (Internal) --Explosive detector --	277.92
Theft of PCs	Volumetric detector --Alarmed fence --	326.09
Glass break	Alarmed fence --	682.40
Hacking	Intrusion Detection System --	1600.00
Infrastructure damage	Alarmed fence --	2047.21
Graffitism	Alarmed fence --	3070.81
	Total mitigated risk [€/year]	8338.24
	Security system cost [€/year]	89340.00
	Total benefits [€/year]	36721.75

Protection mechanism	Risk reduction [€/year]	Cost [€/year]	Benefits [€/year]
Alarmed fence	29246.77	2400.00	26846.77

Conclusions & future works

- A methodology and a tool for the quantitative risk analysis have been developed which allow to compute the return on investment of security protection mechanism.
- The tool has been designed and experimented for the physical protection of rail-based mass transit systems; however, it is suited to logical threats and other classes of critical infrastructures
- 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.
- 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. Q-RA is also intended for the integration of qualitative analysis by means of associative tables
- 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.
- The evaluation of parameters involved in the risk formula can be performed by adopting model-based approaches. See:

  F. Flammini, V. Vittorini, N. Mazzocca, C. Pragliola: "A Study on Multiformalism Modelling of Critical Infrastructures". In: *Proc. 3rd International Workshop on Critical Information Infrastructures Security*, CRITIS'08, Frascati (Rome), Italy, October 13-15, 2008.

  …later, during the poster session.

AnsaldoSTS

Thank you for your kind attention.

Any questions?

AnsaldoSTS