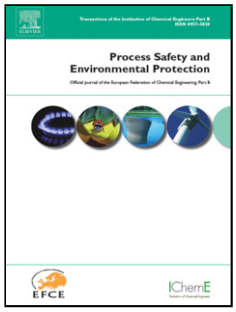
Accepted Manuscript



Title: Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities

Authors: Valeria Villa, Genserik L.L. Reniers, Nicola Paltrinieri, Valerio Cozzani

PII: S0957-5820(17)30089-7
DOI: http://dx.doi.org/doi:10.1016/j.psep.2017.03.023
Reference: PSEP 1014

To appear in: *Process Safety and Environment Protection*

Received date: 5-8-2016
Revised date: 11-3-2017
Accepted date: 15-3-2017

Please cite this article as: Villa, Valeria, Reniers, Genserik L.L., Paltrinieri, Nicola, Cozzani, Valerio, Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities.Process Safety and Environment Protection http://dx.doi.org/10.1016/j.psep.2017.03.023

Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities

Revised Version – March 2017

Valeria Villa[a], Genserik L.L. Reniers[b,c,d], Nicola Paltrinieri[e], Valerio Cozzani[a]

[a] *LISES – DICAM, Department of Civil, Chemical, Environmental and Materials Engineering, Alma Mater Studiorum, University of Bologna, via Terracini 28, 40131 Bologna, Italy*

[b] *Safety and Security Science Group, Faculty of Technology, Policy, and Management, TU Delft, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands*

[c] *ARGOSS, Faculty of Applied Economic Sciences, University of Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium*

[d] *CEDON, Faculty of Economics and Management, HUB-KU Leuven, Campus Brussels, Warmoesberg 26, 1000 Brussels, Belgium*

[e] *Department of Production and Quality Engineering, Norwegian University of Science and Technology NTNU, Trondheim, Norway.*

Abstract

Several recent events raised the attention toward possible major accidents triggered by external acts of interference in industrial facilities. In particular, a growing concern is present with respect to the intentional release of dangerous substances resulting in environmental and eco-terroristic attacks. Therefore, optimal selection and allocation of preventive security measures is becoming more important for decision-makers. Despite the existence of economic models supporting the decision-making process, their applications within the chemical industry security context are relatively limited. This study describes a specific model for economic analysis and selection of physical security measures, with respect to potential environmental and eco-terroristic attacks in chemical facilities. An example of application to a relevant case study is presented to show the model capabilities. Site-specific analysis of the baseline physical security system performance allows comparing the costs of different security upgrades with the benefits related to either prospective or retrospective losses, meanwhile accounting the uncertainties related to the threat probability. Selection of the most profitable security measures within budget constraints and definition of economic indicators are the main outputs of the model, in order to support decision-making processes for allocation of security barriers.

Keywords

Security Cost-effectiveness analysis; Physical security measures; Security decision-making; Chemical industry; Environmental accident.

1 Introduction

In the last years, chemical and process facilities have emerged as attractive targets for malevolent intentional actions, due to the potential consequences in terms of disruption of operations, destruction of property, environmental damages, health deterioration or loss of life (Bajpai and Gupta, 2007) with potential for cascading effects (Landucci et al., 2015). Two environmental security-related phenomena, named enviro-terrorism and eco-terrorism, emerged among security threats to tackle in chemical and process facilities and in hazardous material transportation routes worldwide. Enviro-terrorism and eco-terrorism are aimed at respectively triggering severe environmental damages and demonstrating radical environmentalism by means of unlawful set of actions within chemical facilities (Alpas et al., 2011). Comparison between the two has been reported in Table 1.

Table 1 Definitions and comparison of enviro-terrorism and eco-terrorism in industrial facilities, adapted from Alpas et al. (Alpas et al., 2011).

	ENVIRO-TERRORISM	ECO-TERRORISM
DEFINITION	Unlawful action or set of actions, committed by individuals or groups, leading to short or long term disruption of environmental resources and properties to deprive others of its use.	Severe damage/disruption to property, rare threat and/or harm against people, and/or nonviolent activism caused by individuals or groups protesting because of perceived harm/destruction to the environment and/or nature.
EXAMPLES	Sabotage or terroristic action w.r.t. industrial facilities containing large inventories of hazardous substances (e.g., chemical and process plants, nuclear installations, infrastructures involved in energy production) with the aim to trigger a major accident, with the worst environmental damages possible.	Arson actions against housing/industrial developments, targeting companies using animals for tests, theft and trespassing; demonstrative actions (e.g., machinery and vehicles sabotage) in industrial facilities perceived as pollutant.
MOTIVATION	Political, religious, personal, economic, etc.	Ideological (i.e., "very radical environmentalism")
TARGETS	Environment	Assets (e.g., equipment), rarely people (e.g., managers)
SCALE OF THE ACCIDENT/ CONSEQUENCES	Relevant environmental, health and assets losses, sometimes not confined within facility boundaries. The accident may cause the partial/complete interruption of operations for several hours/days and may contribute to the facility closedown. Severe environmental damages take place, generally requiring massive emergency intervention, causing health consequences to workers and, less often to the resident population (including injuries and/or casualties). Remediation costs and assets losses are relevant.	Generally, the consequences consist on minor assets losses, confined within facility boundaries that might cause a short and/or partial interruption of operations.

The importance of environmental losses in the context of security-related accidents has been highlighted by the results of an ARIA survey, regarding 850 malicious acts perpetrated within industrial facilities (mainly chemical industrial sites), in the period 1992-2015 (ARIA, 2015). Security-based accidents may be classified according to four main possible typologies of consequences: environmental, economic, social and human. For instance, the survey results highlight that 46% of security-based accidents resulted in severe environmental consequences (Figure 1A), leading also to economic consequences. For instance, economic consequences include internal damages necessitating repair expenses and production losses, as well as damages to third parties operations and properties. Environmental damages include soil, air, surface and ground water pollution. Moreover, release of hazardous or polluting substances occurred in almost half of security-based accidents (Figure 1B). However, as demonstrated by Figure 1, security-based accidents are complex phenomena, not limited only to environmental and economic damages, wherein social consequences (e.g., installation of safety perimeters and personnel redundancies) and human consequences

(e.g., casualties and morbidities) should be considered too. Therefore, an accurate monetary quantification of environmental damages within security-based accident losses, including intervention and remediation costs, may lead to a more realistic description of all the other accidents consequences.

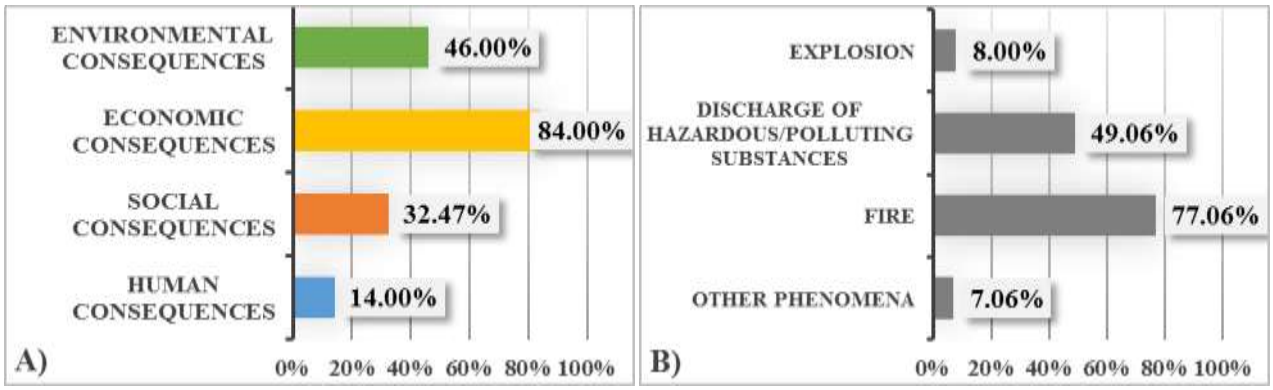


Figure 1 Overview on security accidents consequences in industrial facilities, based on ARIA survey regarding 850 accidents in the period 1992-2015 (ARIA, 2015). (A) General overview on consequences percentage composition according to four main consequence categories: environmental, economic, social and human. (B) General overview on security-based scenarios according to four main scenario categories: explosion, discharge of hazardous/polluting substances, fire and other phenomena. The consequences percentages in (A) and (B) are obtained with respect to the total number of accidents considered in the mentioned survey (i.e., 850). Consequences and scenario category percentages do not sum into 100% as a security-based accident may determine consequences and scenario belonging to more than one of the listed categories.

Within this context, reducing chemical plant vulnerabilities towards enviro-terrorism and eco-terrorism acts makes the investigation of intentional risks a relevant topic. Economic analyses, such as cost-benefit and cost-effectiveness analyses, may offer rational criteria for the selection and allocation of security measures within the decision-making process, as demonstrated by the application to other domains, as aviation (Stewart and Mueller, 2013, 2011, 2008) and navy facilities (Cox, 2009; Dillon et al., 2009). Table 2 summarizes recent contributions regarding theoretical, methodological and applicative aspects of economic analyses within the safety and security domain, referred to chemical and process industry installations. The analysis of research gaps highlighted that, despite the potential of economic analyses in establishing competitive business advantage within chemical process safety and security (Reniers, 2014), previous contributions are referred mostly to the selection and allocation of safety measures with respect to unintentional major and occupational accidents (i.e., safety-based accidents). No specific complete economic models and applications are yet available addressing the selection and allocation of preventive security measures, within the chemical and process industry domain.

The present study addressed the development of a model for cost-benefit and cost-effectiveness analysis of preventive security measures, with respect to potential environmental and eco-terroristic attacks, called ECO-SECURE, specifically addressing chemical and process facilities. The ECO-SECURE approach, starting from the analysis of the baseline physical security system, allows proposing security upgrades and accounting both for the performance improvements and the costs derived from their implementation. The model also includes the evaluation of benefits, considering avoided losses for different pertinent hypothetical scenarios. Thus, ECO-SECURE enables the comparison among different security upgrades and guides the choice of those economically feasible. Moreover, it determines the combinations allowing the maximum profits, according to different assumptions regarding the likelihood of the attack. The ultimate aim of the model is allowing a more rational allocation of security measures and supporting the decision-making process, within the context of chemical industrial activities. The model is specifically tailored for security measures aimed at the prevention of security-related events, as illustrated in Section 2, even if also the adoption of safety measures may offer sound support in the prevention, control and mitigation of security-based accidents (Aven, 2007; Reniers, 2010). ECO-SECURE was applied to an illustrative case study, freely adapted from a possible security-related environmental disaster that took place in Italy.

Table 2 Previous contributions on economic analysis, regarding safety and security aspects, within the chemical and process industry domain.

Keyword / Contribution	Reference accident/ measure typology	Elements of economic analysis				
		Measure performance/ risk reduction assessment	**Cost assessment**	**Losses/consequences assessment**	**Probability of attack/accident occurrence**	**Economic analysis**
(Ale et al., 2015)	Unintentional (safety-based) accidents/ safety measures	Not considered.	Discussion on hidden costs; no classification provided	Discussion on ethical issues; no classification provided	Not considered.	Cost-benefit analysis, budget limitations.
(Garcia, 2007, 2005)	Intentional (security-based) major accidents/ Physical security measures	EASI model; other models proposed	No classification provided	No classification provided	Deterministic approach	Qualitative discussion on cost-benefit analysis
(Gavious et al., 2009)	Unintentional (safety-based) accidents/ safety measures	Not considered	Not considered	Specific classification including categories, subcategories and formula	Not considered	Qualitative discussion on cost-benefit analysis
(HSE - Health and Safety Executive, 2016)	Unintentional (safety-based) accidents/ safety measures	Not considered	Discussion on costs; generic classification provided (no formula)	Discussion on benefit; generic classification provided (no formula)	Not considered	Cost-benefit analysis
(Janssens et al., 2015)	Unintentional (safety-based) major accidents (domino)/ safety measures.	Overall values; no classification provided	Overall values; no classification provided	Overall values; no methodology provided	Calculation of domino probabilities	Cost-effectiveness analysis
(Kyaw and Paltrinieri, 2015)	Unintentional (safety-based) major accidents/ safety measures	Not considered	Not considered	Calculation of reputational losses for notorious major accidents	Not considered	Qualitative discussion on the possible use within cost-benefit analysis
(Martinez and Lambert, 2012)	Unintentional (safety-based) major accidents/ safety measures	Layer of Protection Analysis	Overall values; no classification provided	Overall values; no classification provided	Deterministic approach	Cost-benefit analysis
(Paltrinieri et al., 2012)	Unintentional (safety-based) major accidents/ safety measures	Specific methodology for passive safety measures	Overall values; no classification provided	Overall values; no classification provided. Only human benefits considered	Deterministic approach	Cost-benefit analysis
(Reniers, 2014)	Intentional (security-based) and unintentional (safety-based) major accidents	Theoretical discussion on performance parameters	Theoretical discussion; no classification provided	Theoretical discussion; no classification provided	Not considered	Theoretical discussion on interactions between economic analyses and risk management

Table 2 (continued) Previous contributions on economic analysis, regarding safety and security aspects, within the chemical and process industry domain.

Keyword / Contribution	Reference accident/ measure typology	Elements of economic analysis				
		Measure performance/Risk reduction assessment	**Cost assessment**	**Losses/consequences assessment**	**Probability of attack/accident occurrence**	**Economic analysis**
(Reniers and Brijs, 2014a; Reniers and Van Erp, 2016)	Unintentional (safety-based) major accidents/ safety measures	Overall values; no methodology provided	Detailed classification specific for safety measures including categories, subcategories and formula	Classification for major accidents, including categories, subcategories and formula	Deterministic approach	Cost-benefit analysis, cost-effectiveness analysis
(Reniers and Brijs, 2014b)	Occupational accidents/ safety measures	Not considered	Not considered	Not considered	Not considered	Presentation of available cost-benefit analysis software/ methodologies
(Reniers and Sörensen, 2013)	Occupational accidents/ safety measures	Overall values	Overall values; no classification provided	Severity classes; no classification provided	Occurrence classes	Cost-effectiveness analysis
(Tappura et al., 2014)	Occupational accidents/ safety measures	Presentation of available models	Discussion on costs; no classification provided	Discussion on benefits; no classification provided	Not considered	Presentation of available cost-benefit analysis methodologies

2 Model description

2.1 General layout of the model

The ECO-SECURE model layout is shown in Figure 2. Definition of the site-specific adversary sequence of actions and assessment of baseline physical protection system (PPS) performance need to be carried out before the model application. This preliminary step was defined as module 0. Six steps are then required to complete the assessment:

- In Module 1 the risk variation achieved by implementing an additional security measure (or PPS) is evaluated.
- In Module 2 the overall costs of a specific security measure, $C_{Security,i}$, are assessed. This includes direct and indirect economic costs derived from the application and use of a security device.
- Module 3 defines the overall losses or consequences of either prospective or retrospective scenarios expressed in monetary values.
- Module 4 is aimed at defining the threat probability (i.e., the likelihood of the attack) within a chemical facility.
- Module 5 of ECO-SECURE allows defining the single security measures that are economically justified (by means of a cost-benefit analysis, indicated with the acronym CBA throughout the manuscript) with reference to a set of scenarios, according to deterministic and break-even approaches.
- Module 6 of ECO-SECURE provides the most profitable combination of security measures (by means of a cost-effectiveness analysis, indicated with acronym CEA throughout the manuscript) with reference to a set of scenarios, according to a deterministic and a break-even approach. Overall economic indicators are provided.

ECO-SECURE outputs are cost-benefit and cost-effectiveness indicators aimed at supporting the security decision-making process from an economic perspective. The model was developed extending a previous specific application of economic analysis to security-related decision making (Villa et al., 2016). In comparison with the previous work of the authors (Villa et al., 2016), the ECO-SECURE model presents a relevant number of improvements; in particular:

- Cost assessment and loss assessment were improved, introducing subcategories and expressions allowing quantitative assessment instead of applying empirical flat rates for each cost category.
- A coupled approach (i.e., deterministic and break-even), instead of a solely deterministic approach, was introduced for threat probability and cost-benefit analysis. The coupled approach allows including a sensitivity analysis within model application. A multi-scenario acceptability criteria was also added.
- An approach to cost-effectiveness analysis was introduced. The application of cost-effectiveness analysis is particularly important since it allows the allocation of the security budget on the most profitable combination of security measures. An original scoring system was also developed to provide overall economic indicators.

ECO-SECURE was implemented in Excel® version 2013, using 7 different datasheets, defined according to ECO-SECURE modules (i.e., from Module 0 up to Module 6). The single steps of the procedure are described in detail in the following.

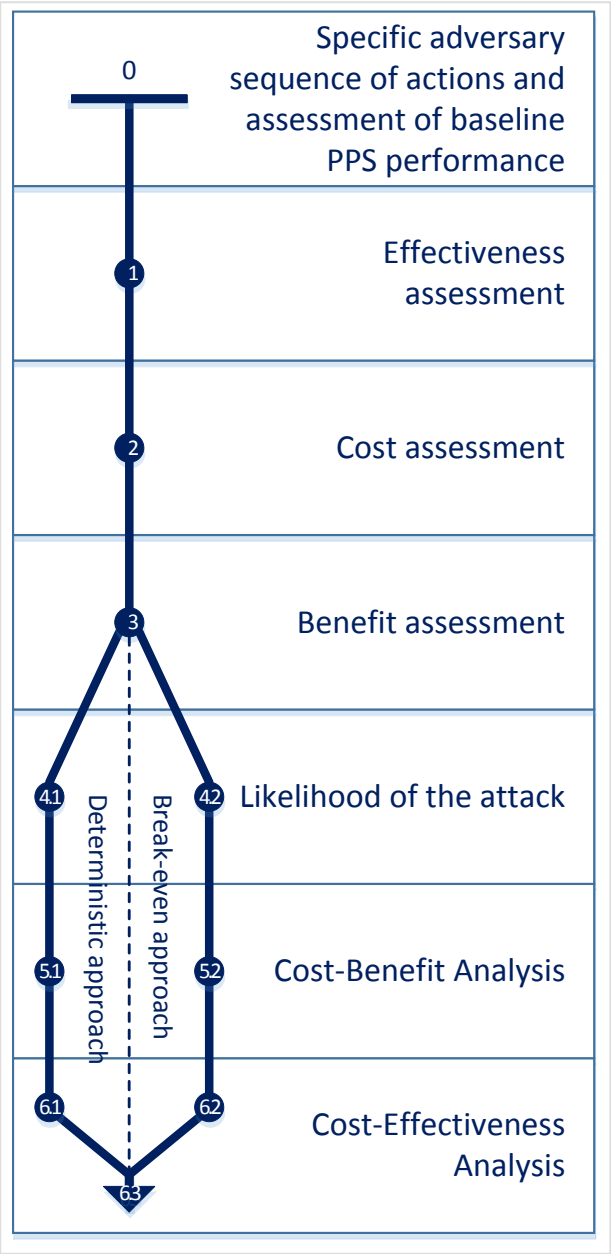


Figure 2 General layout of ECO-SECURE.

2.2 Module 0: Specific adversary sequence of actions and assessment of baseline PPS performance

Module 0 is the preliminary step for the application of ECO-SECURE: it provides the definition of the site-specific adversary sequence of actions and the assessment of baseline physical protection system performance. The selection of an adversary action sequence should be based on Adversary Sequence Diagrams and site-specific data. An Adversary Sequence Diagram is a graphic representation of the plant layout that should consider possible adversary starting points, distances up to the target(s), locations and typologies of security measures in place, and availability of security guards on site. Reasonable assumptions regarding the adversary mode of action (e.g., by foot or by car), tactic (e.g., stealth or deceit) and attack scope (e.g., triggering an explosion or stealing an asset) should be taken.

Several models may be used to determine the baseline physical protection system performance, whose principal indicator is its effectiveness (η_{PPS}) (Hester et al., 2010). In ECO-SECURE, Estimate of Adversary Sequence Interruption (i.e., EASI) model , developed by Sandia Laboratories (Garcia, 2007, 2005), was applied to determine physical protection system performance. Estimate of Adversary Sequence Interruption

(i.e., EASI) model, calculates the probability of interruption $(P_{I,p})$, referred to a single sequence of adversary actions aimed at theft or sabotage The probability of interruption expresses the conditional probability of an attacker's path of actions (i.e., indicated with p) being foiled, deterred or disrupted. EASI model requires the following input parameters: assessed detection and communication probabilities (i.e., indicated respectively with $P_{AD,i}$ and P_C), delay mean times of each protection element i (i.e., indicated with $t_{D,i}$ and expressing the mean duration time of a task), response force mean time (t_G) and standard deviations for the mentioned parameters (i.e., indicated respectively with $\sigma_{D,i}$ and σ_G). Standard deviation input values are required because the EASI model, applied for the calculation of the effectiveness, takes into account uncertainties regarding each task (e.g., presence of a lag time) by applying probability distribution. According to the conservative assumption on data dispersion of the model (Garcia, 2007), standard deviation values referred to the delay parameter for each security element and to the response parameter have been assumed as $3/10$ of the mean value.

According to EASI model, $P_{I,p}$ can be computed as follows with reference to a path p with l tasks:

$$\begin{cases} P_{I,p} = \left(1 - \prod_{i=1}^{k}(1 - P_{AD,i})\right) \cdot P_C \cdot \left(\int_0^T \left(1/\sqrt{2\pi(\sigma_D^2 + \sigma_G^2)}\right) \exp(-T^2/(\sigma_D^2 + \sigma_G^2))dT\right) \\ T = t_D - t_G \\ t_D = \sum_{i=k+1}^{l} t_{D,i} \\ \sigma_D = \sum_{i=k+1}^{l} \sigma_{D,i} \end{cases} \quad (1)$$

Details on the EASI model can be found elsewhere (Garcia, 2007, 2005); the suggested modelling environment is an Excel® datasheet. A sample Excel® datasheet of EASI model can be retrieved from the mentioned source (Garcia, 2007). In the evaluation of effectiveness, the neutralization probability is not accounted for, following the stated assumption that in industrial facilities the use of lethal force against an adversary is unlikely (Garcia, 2007).

Therefore, the baseline PPS effectiveness (i.e., $\eta_{PPS,old}$) can be assessed as follows, according to:

$$\eta_{PPS,old} = P_{I,p^*} = \min(P_{I,p}) \qquad with\ p = \{1, \dots, q\} \quad (2)$$

Where the path p^*, with the lowest $P_{I,p}$ (i.e., P_{I,p^*}) among q possible ones has been named critical path. P_{I,p^*} characterizes the baseline effectiveness of the physical protection system, according to the principles of EASI model (Garcia, 2007).

2.3 Module 1: Effectiveness assessment

This module is aimed at proposing security upgrades and determining the reduction in risk ΔR_i due to each security measure i. Following the assumption of adding one security device at a time, risk reduction due to the introduction of a generic security measure i in the existing Physical Protection System can be computed as:

$$\Delta R_i = \eta_{PPS,new\,i} - \eta_{PPS,old} \quad (3)$$

$$\forall i \in \{1, \dots, n\}, n \in Z$$

Where $\eta_{PPS,new\,i}$ expresses the probability of attacker's path of actions being foiled, deterred or disrupted in presence of each additional (i.e., "new") security measure i among the possible n security measures. It expresses the upgraded PPS effectiveness. On the other hand, $\eta_{PPS,old}$ represents the probability of attacker's path of actions being foiled, deterred or disrupted before the addition of a security measure, calculated in module 0. Thus, risk reduction (ΔR_i) requires the evaluation of PPS effectiveness. In order to define the effectiveness of upgrades, the EASI model is applied to the critical path for each of the security upgrades i, obtaining $\eta_{PPS,new\,i}$, $\forall i \in \{1, .., n\}, n \in Z$. Further details on effectiveness assessment by means of EASI

model are provided by Garcia (Garcia, 2007, 2005). It should be noted that EASI model, applied in ECO-SECURE for the calculation both of the baseline and of the upgraded system effectiveness specifically refers to physical security measures and cannot be generalized (i.e., it cannot be applied for safety measures performance evaluations). The choice of an appropriate pool of security upgrade should be based on the Organizational-Physical-Electronics-Reporting principle (i.e., OPER) (Reniers et al., 2015), which considers a complete PPS as a combination of the three security functions of detection, delay and response. Therefore, the range of choices should include at least one security measure belonging to each security function. Further details on security measures classification, based on security functions, are available elsewhere (CCPS - Center for Chemical Process Safety, 2003; Garcia, 2007). A detailed guideline on the possible security upgrades to be adopted is available elsewhere (Garcia, 2007), therefore it is not necessary to use a specific software for the selection of appropriate security upgrades within ECO-SECURE application.

2.4 Module 2: Cost assessment

This module provides the evaluation of costs for each risk-reducing security measure $(C_{Security,i})$. The cost assessment for a security device includes the direct economic costs of applying the device and the indirect costs associated with its use. Therefore, it may include general terms as purchase costs, personnel costs and running costs. On the other hand, also cost terms either specific for each category of PPS or site-specific might be determined. Six main cost categories have been considered. Among these, five are in close analogy with a similar cost evaluation referred to safety measures for the chemical and process industry (Reniers and Brijs, 2014a): i) initial costs; ii) installation costs; iii) operating costs; iv) maintenance, inspection and sustainability cost; v) other running costs; vi) specific costs. Despite the similarities with the cost classification applied to safety measures (Reniers and Brijs, 2014a), ECO-SECURE contains cost items specifically tailored for physical security measures, as described below.

Initial costs are the costs incurred during the investigation, selection and design phases of the project, involving furthermore the costs of materials, training and eventual guidelines changes (Campbell and Brown, 2003). Installation costs refer to the expenses sustained to put the security measure in place and ready for use (Campbell and Brown, 2003). The main difference with similar cost evaluations referred to safety measures (e.g. see (Reniers and Brijs, 2014a)) is the absence of a "Production loss cost" term and the different composition of the linked "Start-up cost". Installation of security measures usually does not interfere with the production rate of chemical plants, determining the necessity to neglect this term from the analysis. However, in some situations an integration of safety and security measures has been realized, allowing to extend the term "production loss cost" also to security measures. Operating costs are the expenses derived from the operation of the security measure, in terms of utilities consumption and labor (Campbell and Brown, 2003). The maintenance costs should incorporate also inspection and sustainability costs (e.g., renewing license and rental costs). Also, "other running costs" (e.g., cost of providing office furniture, transport, insurance, and stationery items) should be added as a separate category, due to its limited influence on the Overall costs (Campbell and Brown, 2003). The last category ("specific costs") includes all the cost features that are peculiar of a specific category of security measure or a site.

The Overall annual costs due to the implementation of one generic security measure $(C_{Security,i})$ can be calculated as the sum of the six mentioned contributions for each security measure i considered in the analysis:

$$C_{Security,i} = \left(C_{INITIAL,OV} + C_{INSTALL,OV} + C_{OPERATION,OV} + C_{MIS,OV} + C_{OR,OV} + C_{SPEC,OV}\right)_i$$

$$\forall\, i \in \{1,\dots,n\}, n \in Z \qquad (4)$$

Where: $C_{INITIAL,OV}$ is Overall initial costs, $C_{INSTALL,OV}$ is Overall installation costs, $C_{OPERATION,OV}$ is Overall operating costs, $C_{MIS,OV}$ is Maintenance, inspection and sustainability costs, $C_{OR,OV}$ is Other running costs and $C_{SPEC,OV}$ is Overall specific costs.

The expressions applicable to the calculation of each cost category in equation (4) were developed according to the fundamentals of CBA (Campbell and Brown, 2003) and reported in Appendix A.1 (Table A1). In order to calculate each cost category, the costs pertaining to each subcategory identified in Table A1 need to be added:

$$C_C = \sum_{i=1}^{n} C_{SC,i} \quad (5)$$

Where C_C is the cost category of interest, and $C_{SC,i}$ is the i-th cost subcategory identified in Table A1.

The expressions reported in Table A1 allow the calculation of the single cost terms for a generic security device. Grouping them into the six mentioned cost categories, the total annual cost due to the implementation a security measure can be computed. The cost estimation can be extended to more than one security device. All the cost terms should be expressed in coherent monetary value.

For the determination of Overall specific costs $(C_{SPEC,OV})$, specific cost subcategories were outlined for each class of security measures, according to their functions and features. As stated by Lee et al. (Lee et al., 2002) cost metrics are often site-specific because each organization has its own security policies and risk factors. Despite the fact that this cost category is open to eventual additional contributions, Overall specific costs were determined as:

$$C_{SPEC,OV} = C_{FP,i} + C_{SITE_{SP}} \quad (6)$$

Where $C_{FP,i}$ indicates Overall cost of a false-positive case and $C_{SITE_{SP}}$ site-specific costs. The false-positive rate refers to a situation in which the detection device identifies an object (person or thing) as a potential hazard, when it is not (Lin and Van Gulijk, 2015). This error turns into additional security procedures that cause inconvenience to employees, but it may also delay systems operation (i.e., due to re-inspection) and it may eventually turn into a money and person-hours waste and reduced employees confidence toward security systems. The formula proposed by Lin and Van Gulijk (Lin and Van Gulijk, 2015, 2014) was applied to calculate the cost of such events:

$$C_{FP,i} = C_{FA,i} \cdot P(FA)_i = C_{FA,i} \cdot P(alarm \mid no\ attack)_i \cdot \left(1 - P(T)_{ij}\right) \quad (7)$$

Where: $C_{FP,i}$ is the Overall cost of a false-positive case for an individual detection security measure i, $C_{FA,i}$ is the cost of a single false-positive case (e.g., cost derived from additional security procedures, as re-inspections and personnel delays), $P(FA)$ is the false-positive probability or false-alarm probability, $P(T)_{ij}$ is the likelihood of the attack, referred to a security measure i and to an accidental scenario j. Further information on this term is available in Section 2.6. $P(FA)_i$ is a function of the security device i and it expresses the probability of having the alarm without an actual threat $(P(FA)_i = P(alarm, no\ attack)_i)$. The right member of equation (7) has been determined by applying the probability chain rule to $P(FA)_i$, with $P(FA)_i = P(alarm \mid no\ attack)_i \cdot \left(1 - P(T)_{ij}\right)$. Further details on the formula might be retrieved from a deliverable of SURVEILLE European Project on surveillance devices (Lin and Van Gulijk, 2014). For the estimation of $C_{FA,i}$ and $P(alarm \mid no\ attack)_i$ values, standard values for a generic individual detection measure (Garcia, 2007), not related to the specific detection device that is implemented, can be applied within cost assessment, after adequate validation by a panel of experts, whenever device-specific information is not available.

Therefore, false-positive costs depend on the assumption regarding the likelihood of the attack. Assuming the likelihood of the attack equal to 1 (i.e., a possible value according to the deterministic approach) turns false-positive costs to zero. Indeed, it leads to the minimum specific costs value, and consequently to the minimum Overall costs for a generic security measure. Setting $P(T)_{ij} = 0$ leads to the maximum value of specific costs and consequently to the maximum value of Overall costs for a generic security measure.

Therefore, the overall costs for a generic security measure, corresponding to intermediate values of $P(T)_{ij}$, fall within these extremes. Further information on the likelihood of the attack is reported in Section 2.6.

Site-specific costs (C_{SITE_SP}) can be eventually added when available. An example of typical site-specific costs might be the cost related to modification of safety measures/procedures necessary to accomplish the company safety standards after the implementation of the security measure. Therefore, specific costs are represented by a range of values (i.e., solely for detection elements), determining consequently a range of values for Overall costs of a generic security measure. Nevertheless, in case of a narrow range of values for overall costs, meaning very low values of specific costs with respect to overall costs, this dependence may be neglected.

2.5 Module 3: Benefit assessment

Benefit assessment consists on the definition of the costs of an either prospective or retrospective accident scenario j among m possible ones. Therefore, benefit assessment requires the quantification of the losses (i.e., named also damages) derived from a successful terroristic attack or, generally, from a security-based accident $(C_{Loss,j})$. Benefit modelling was indicated as module 3 in the general ECO-SECURE layout (Figure 2). As reported by CCPS (CCPS - Center for Chemical Process Safety, 2003), a security risk assessment, as well as the related selection and implementation of security measures, requires a definition either of reference assets or of reference scenarios, leading respectively to an "asset-based approach" and to a "scenario-based approach". As stated by Reniers (Reniers, 2010), in the case of security risk assessment within the chemical and process industry, a scenario-based approach might be more familiar to experts of safety risk assessment, wherein scenario-thinking is widely applied to picture possible unwanted situations. Considering that the effects of accidental or intentional events are often comparable (Nolan, 2008), in the tentative selection of security scenarios those considered for safety thinking can be considered. In case of a retrospective analysis (i.e., posterior application based on a real security-based accident), the actual losses sustained in the attack, named realistic benefits, may be accounted. In case of a prospective analysis, if available, information should be gathered on previous accidents triggered by terroristic attacks on similar reference installations. An expected scenario, which considers the average hypothetical benefits, weighted by probabilities of occurrence, of different possible outcomes, can be indeed considered in the scenario selection phase with reference to prospective analysis (US Department of Defense, 2000). Otherwise, in case of no information available regarding scenario selection and prospective analysis, a "worst-case scenario" should be taken into account. In fact, adversaries (e.g., in case of environmental-terrorism or eco-terrorism) deliberately search for the best manner to execute their plans. This means that they are aiming to cause as much damage as possible, and therefore, certain scenarios that would be labelled as extremely unlikely in case of safety thinking, might actually be considered in case of security thinking (Reniers and Audenaert, 2014).

The losses derived from a successful attack include environmental damages, fatalities and other damages, both direct and indirect, which will accrue because of a successful attack, taking into account the value and vulnerability of people, environment and infrastructure. Generally, in a CBA approach, a monetary quantification of the losses is carried out, but also non-quantifiable damages (i.e., psychological and political effects) are mentioned (Stewart and Mueller, 2011). Quantification of direct tangible costs (e.g., replacement costs due to property damage) is quite straightforward. On the other hand monetizing intangible terms related to a terroristic attack (e.g., value of human lives loss after an attack, long-term environmental consequences, fear or social issues emerging after the attack, sufferance and victimization costs) is a very difficult task that has always arisen ethical concerns since its introduction (Hansson, 2007; Kelman, 1981). Among these, the most controversial issue is the assignment of a monetary figure on a person's life (Tappura et al., 2014). Despite detailed descriptions, which can be found elsewhere (Paltrinieri et al., 2012; Viscusi and Aldy, 2003), it should be clear that the monetary value is referred to as "Value of a Statistical Life" (i.e., VSL), avoiding any personal involvement. Indeed, also the monetary estimation of environmental damages may

raise ethical bias, as it reflects the subjective environmental attitude of the analyst (Spash, 1997). Furthermore, environmental and health consequences of a hazardous substance release, as demonstrated by the notorious Seveso accident in Italy (1976), may last over 40 years. Indeed, as stressed by Lin and Van Gulijk (Lin and Van Gulijk, 2015) the alternative of not recognizing these costs is probably even more arguable. For instance, an alternative approach to economic analysis with respect to ECO-SECURE, may require different studies for tangible assets and intangible damages (i.e., human losses) to solve the mentioned issue (Hansson, 2007).

The details concerning the loss categories of the present study have been reported in Appendix A.2. The categories and subcategories referred to the costs of each scenario were adapted from previous studies (Reniers and Brijs, 2014a; Villa et al., 2016), enhancing the focus on short-term and long-term environmental damages.
The Overall benefits indicate, within risk assessment domain (Reniers, 2010), the damages derived from a generic accidental scenario $(C_{Loss,j})$. Overall benefits can be computed as the sum of seven contributions, for each scenario j considered in the analysis:

$$C_{Loss,j} = \left(B_{SUPC,OV} + B_{DMG,OV} + B_{LGL\&INS,OV} + B_{H,OV} + B_{ENV,OV} + B_{REPT,OV} + B_{SPEC,OV}\right)_j$$
$$\forall j \in \{1,\dots,m\}, m \in Z \quad (8)$$

Where: $B_{SUPC,OV}$ is Overall supply chain benefits, $B_{DMG,OV}$ is Overall damage benefits, $B_{LGL\&INS,OV}$ is Overall legal and insurance benefits, $B_{H,OV}$ is Overall human benefits, $B_{ENV,OV}$ is Overall environmental benefits, $B_{REPT,OV}$ is Overall reputation benefits and $B_{SPEC,OV}$ is Overall specific benefits.

The expressions applicable to the calculation of each benefit category were developed accordingly to the fundamentals of CBA (Campbell and Brown, 2003) and are reported in Appendix A.2 (Table A4). In order to calculate each benefit category, the benefits pertaining to each subcategory identified in the mentioned table need to be added:

$$C_B = \sum_{i=1}^{n} C_{SB,i} \quad (9)$$

Where C_B is the benefit category of interest, and $C_{SB,i}$ is the i-th benefit subcategory identified in Table A4.

The expressions reported in Table A4 (Appendix A.2) allow the calculation of the single benefit terms for either a prospective or a retrospective accidental scenario. Grouping them in the seven mentioned benefits categories, the total losses due to a generic accidental scenario can be computed. All the benefits terms should be expressed in coherent monetary value. Although this category is open to eventual additional contributions, Overall specific benefits in ECO-SECURE have been determined as:

$$B_{SPEC,OV} = B_{SITE\_SP} + B_{IMM} \quad (10)$$

Specific benefits are mostly site-specific (B_{SITE_SP}) and should be considered in case of additional information available. If additional information is available, also other immaterial terms (B_{IMM}), such as the "cost of fear", psychological damages, social and political tensions might be added to the analysis.

2.6 Module 4: Likelihood of the attack

In Module 4, the threat likelihood to be considered in the economic analysis is determined. The threat likelihood $(P(T)_{ij})$, named also "likelihood of the attack" and "probability of the attack", expresses the probability of an individual or a group with adequate motivation and capability to attack a chemical and process facility, committing theft, sabotage or other malevolent acts that would result in loss of assets. Threat assessment is aimed at quantifying the actual or potential threat on a facility by means of statistical data treatment, based on expert elicitation, as well as on available intelligence, law enforcement and open source information. However, several authors (Garcia, 2007; Stewart and Mueller, 2013; Villa et al., 2016) stressed

the difficulty to get a significant estimate of this term. Therefore, in the presence of uncertainties and lack of information on this term, two approaches can be applied:

Module 4.1 Deterministic approach. In this case, a defined value of $P(T)_{ij}$ within the range [0,1] is assumed, and is considered an input of the economic analysis. As suggested by Garcia (Garcia, 2005), in case of unacceptably high consequences (i.e., major accidents with possibility of cascading effects, national security at stake), for both prospective and retrospective accidents, a conditional threat approach may be applied: it implies to consider $P(T)_{ij} = 1$. This assumption means that the consequences of a possible attack are so severe that the estimation of the threat probability is not required; therefore, it allows focusing on the role of security measures management.

Module 4.2 Break-even approach. According to this approach $P(T)_{ij}$, renamed ${P(T)_{ij}}^*$ and ${P(T)_{vj}}^*$, respectively for cost-benefit and cost-effectiveness analyses, is the output of the economic analyses and it represents the minimum threat probability required for the benefits of a specific scenario *j* to equal the costs of a security measure i (or a combination of security measures v); the threat probability is calculated in modules 5 and 6.

2.7 Module 5: Cost-Benefit analysis

In Module 5, the single security measures i that are economically feasible with reference to all the m scenarios are identified.

Before starting an economic analysis, it should be noted that the total benefits and the total costs occur at different points in time. Therefore, it is necessary to introduce a discount rate to convert all cash flows to present values of annuities. This process, named "actualization", is shown by the following formula (Campbell and Brown, 2003):

$$\begin{cases} \bar{C} = C \cdot \frac{((1+r)^z - 1)}{((1+r)^z \cdot r)}, r \neq 0 \\ \bar{C} = C, \ r = 0 \end{cases} \quad (11)$$

Where $\bar{C}$ is the actualized value of overall cost or benefit, C is the yearly overall cost or benefit, z is the number of years the security measure will be operating and r represents the discount rate, intended here as the real rate of interest.

2.7.1 Module 5.1. Cost-Benefit analysis with deterministic approach

When deterministic approach is applied, the Net Benefit for every security measure i and each scenario j is determined according to the following equation:

$$\begin{cases} Net\ Benefit_{ij} = P(T)_{ij} \cdot C_{Loss,j} \cdot \Delta R_i - C_{Security,i} \\ \forall i \in \{1, \dots, n\}, n \in Z \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (12)$$

Where $Net\ Benefit_{ij}$ indicates the Net benefit obtained by applying a security measure i, among n possibilities, with reference to a specific scenario j, among m scenarios considered in the analysis. Following the standard CBA terminology, the term $P(T)_{ij} \cdot C_{Loss,j} \cdot \Delta R_i$ indicates the overall positive cash flow obtained by the application of a security measure i, for a scenario j, whose occurrence will lead to the overall benefits indicated as $C_{Loss,j}$. The value of the latter term, including environmental damages, fatalities and other damages, both direct and indirect, derived from a successful attack, is calculated according to the categories reported in Section 2.5. $C_{Security,i}$ indicates the costs of providing the risk-reducing security measure i that is necessary to obtain the overall benefits.

According to a deterministic approach, the implementation of a single security measure i is acceptable, with reference to all the m scenarios if:

$$\begin{cases} Net\ Benefit_{ij} \geq 0 \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (13)$$

Else, it should be rejected. The calculation of $Net\ Benefit_{ij}$ represents the output of cost-benefit analysis submodule 5.1. The analysis should be repeated for each security measure i and for each scenario j, obtaining therefore n x m values of Net benefits. A single security measure should be accepted or rejected over all the m scenarios.

2.7.2 Module 5.2. Cost-Benefit analysis with break-even approach

This submodule calculates the break-even point, which is the probability of the attack $P(T)_{ij}{}^{*}$, corresponding to $Net\ Benefit_{ij} = 0$ for every security measure i and each scenario j, according to the following equation:

$$\begin{cases} P(T)_{ij}{}^{*} = \frac{C_{Security,i}}{C_{Loss,j} \cdot \Delta\eta_i} \\ \forall i \in \{1, \dots, n\}, n \in Z \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (14)$$

According to a break-even approach, the implementation of a single security measure i is acceptable, with reference to all the m scenarios, if:

$$\begin{cases} P(T)_{ij}{}^{*} \leq P(T)_{ij}{}' \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (15)$$

Where $P(T)_{ij}{}'$ is a threshold value for the likelihood of the attack, which can be derived from different sources, as intelligence data or generic accident data gathering, as well as expert elicitation. Else, the security measure should be rejected. The calculation of $P(T)_{ij}{}^{*}$ represents the output of cost-benefit analysis submodule 5.2. The analysis should be repeated for each security measure i and for each scenario j, obtaining therefore n x m values of $P(T)_{ij}{}^{*}$. A single security measure should be accepted or rejected over all the m scenarios. The application of a break-even approach offers a sensitivity analysis on the likelihood of the attack, directly included in the model.

2.8 Module 6: Cost-Effectiveness analysis

This module calculates the most profitable combination of security measures with reference to the scenarios. Often, security investments should be compared with budget limitations. In this situation, the economic evaluation method turns into a cost-effectiveness analysis.

2.8.1 Module 6.1. Deterministic Cost-Effectiveness analysis

According to the deterministic approach, the optimization problem to be solved, known as the "Knapsack problem" in the field of Operations Research, consists on finding the solution of the following system:

$$\begin{cases} \max\left(Net\ Benefit_{vj} \cdot x_v\right) \\ C_v \cdot x_v \leq C_{Budget,j}\ \forall j \in \{1, \dots, m\}, m \in Z \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1, \dots, w\}, w \in Z \end{cases} \quad (16)$$

The first equation of the system expresses the total Net benefit from the selected investments portfolio, which should be maximized, hence obtaining the $\max\left(Net\ Benefit_{vj} \cdot x_v\right)$, among all the possible w combinations of security measures, indicated by $v \in \{1, \dots, w\}, w \in Z$. Therefore the calculation should be applied for each combination of security measure v and for each scenario j, obtaining w x m values of Net benefits.

The second equation expresses the fact that the total cost of the selected measures, composing combination v, $(C_v \cdot x_v)$ should not exceed the security budget $\left(C_{Budget,j}\right)$. The same constraint allows discarding directly also single security measures not respecting the budget. The security budget $\left(C_{Budget,j}\right)$ is the total annual monetary amount defined by security managers that can be allocated on a combination of measures. The security budget is often scenario-dependent, as it can vary based on scenario severity. However, in case of unacceptably high losses (e.g., cascading events) security budget might represent a fixed value, which cannot be reduced. The third constraint $(x_v \in \{0,1\})$ implies that a measures combination is either fully taken or not taken at all. A number of assumptions are implicitly embedded in this formulation:

- Security investments cannot be partial: a measure is either adopted or not;
- The overall hypothetical benefit of all measures considered is the sum of the individual benefits;
- The overall cost of all security measures adopted (C_v) is the sum of the costs of the individual measures, composing a combination v, as expressed by the second equation;
- Each security measure can be implemented independently, without consequences for the other investments. This simplifying assumption was kept in the present formulation. However, it might be overcome in future studies by considering reduction cost factors due to the combined implementation of security measures.

The output of submodule 6.1 is the most profitable combination of security measures (v^*), within the constraint of the security budget, for each scenario j, according to deterministic approach. A ranking of all the combinations, in order of decreasing profitability, is provided. However, the top-three most profitable combinations are identified, as they might be the probable final security investments. Therefore, the combinations that are outlined are the most profitable ones, under the deterministic assumption of $P(T)_{ij}$ as a defined value within the range $[0,1]$. The results of cost-effectiveness analysis, according to the deterministic approach, may differ significantly among scenarios. The application of an original scoring system allows defining an economic indicator expressing overall cost-effectiveness analysis results, derived from multiple scenarios, according to the deterministic approach.

2.8.2 Module 6.2. Break-Even Cost-Effectiveness analysis

Following a break-even approach, the optimization problem consists on finding the solution of the following system:

$$\begin{cases} \min \left(P(T)_{vj}{}^* \cdot x_v\right) \\ C_v \cdot x_v \leq C_{Budget,j} \; \forall j \in \{1, \dots, m\}, m \in Z \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1, \dots, w\}, w \in Z \end{cases} \tag{17}$$

The first equation of the system (17) expresses the probability of the attack with the application of a selected investments portfolio, which should be minimized, hence obtaining $\min \left(P(T)_{vj}{}^* \cdot x_v\right)$, among all the possible w combinations of security measures, indicated by $v \in \{1, \dots, w\}, w \in Z$. Therefore the calculation should be applied for each combination of security measure v and for each scenario j, obtaining $w \times m$ values of $P(T)_{vj}{}^*$. The values of $P(T)_{vj}{}^*$ can be calculated according to equation (14), by replacing a single measure i with a combination v. The constraint expressed by equation (14), regarding $Net\ Benefit_{vj} = 0$ is embedded in the formulation of system (17).The second equation expresses the fact that the total cost of the selected measures $(C_v \cdot x_v)$, composing combination v, should not exceed the security budget $\left(C_{Budget,j}\right)$, which in turn is often scenario-dependent. The third constraint $(x_v \in \{0,1\})$ implies that a measure is either fully taken or not taken at all. The assumptions embedded in the formulation, the constraints and the notations are the same ones as those expressed with a deterministic cost-effectiveness analysis. The output of submodule 6.2 is the combination of security measures, v^*, with the lowest probability of the attack, within the constraint of the security budget, for each scenario j, according to a break-even approach. A ranking of

all the combinations, in order of decreasing profitability, is provided. However, the top-three most profitable combinations are identified, as they might be the probable final security investments. The combinations that are outlined are the most profitable ones with the assumption of $Net\ Benefit_{vj} = 0$.

The application of a break-even approach to cost-effectiveness analysis offers a sensitivity evaluation on the likelihood of the attack, directly included in the model. The results of cost-effectiveness analysis, according to the break-even approach, may differ significantly among scenarios. The application of an original scoring system allows defining an economic indicator expressing overall cost-effectiveness analysis results, derived from multiple scenarios according to the break-even approach.

2.8.3 Module 6.3. Overall Cost-Effectiveness Indicator

The outputs of submodule 6.1 and submodule 6.2 may offer significant support to security decision-making. However, the indications provided by deterministic and break-even cost-effectiveness analyses might be different and sometimes conflicting with respect to the same scenario (e.g., a combination might have a high ${P(T)_{vj}}^*$ and a high $Net\ Benefit_{vj}$). For this reason, it is not possible to compare directly cost-effectiveness analyses results obtained from the two approaches, because Net Benefits are monetary values, within the range $(-\infty, +\infty)$, whereas ${P(T)_{vj}}^*$ are adimensional values, ranging within $[0,1]$. Moreover, within the same approach to cost-effectiveness analysis, results might be very different among scenarios, as discussed in Sections 2.8.1 and 2.8.2. Consequently, security investments that are not profitable with respect to a marginal scenario, might become economically feasible with respect to a catastrophic scenario.

The introduction of specific scoring systems is a common approach to provide more understandable information to stakeholders (Argenti et al., 2015; Srivastava and Gupta, 2010). Assuming that $Net\ Benefit_{vj} = f(P(T)_{vj})$ is a linear function increasing monotonically in the range $[0,1]$ (i.e., under the assumptions expressed in the two economic analyses modules), it is possible to define two original economic indicators, named KPI_1 and KPI_2, expressing respectively the results of deterministic and break-even cost-effectiveness analysis, and eventually to combine them linearly. The combined application of the two indicators allows defining the function univocally. Therefore, the sensitivity analysis regarding the threat probability is included in the model. The use of multi-scenario criteria allows defining average economic performance of security measures combinations, weighted on all the scenarios m.

The first economic indicator (KPI_1) expresses the results of deterministic cost-effectiveness analysis. KPI_1 is defined according to equation (18), for each possible combination of security measures v and for all the scenarios m:

$$\begin{cases} \text{If } C_v \cdot x_v \leq C_{Budget,j}\ \forall j \in \{1,\dots,m\}, m \in Z \\ KPI_1 = \left(\sum_{j=1}^{m}\left(Net\ Benefit_{vj} \cdot x_v / \left(\max\left(Net\ Benefit_{v^*j}\right)\right)\right)/m\right) \cdot 10 \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1,\dots,w\}, w \in Z \\ j \in \{1,\dots,m\}, m \in Z \\ \text{Else } KPI_1 = 0 \end{cases} \quad (18)$$

Therefore, KPI_1, ranging between $[0,10]$, expresses the combined economic and technical performance of each combination of security measures, according to the deterministic approach. The value of the indicator is normalized with respect to the most cost-effective options v^* obtained from a deterministic approach for each scenario, which scores 10 and weighted on all the scenarios m. The higher the value of KPI_1, the better the overall performance of the combination. If the combination does not comply with the budget constraint for all the scenarios, the value of the indicator is 0.

The second economic indicator (KPI_2) expresses the results of break-even cost-effectiveness analysis. KPI_2 is defined according to equation (19), for each possible combination of security measures v and for all the scenarios m:

$$\begin{cases} \text{If } C_v \cdot x_v \le C_{Budget,j}\ \forall j \in \{1,\dots,m\}, m \in Z \\ KPI_2 = \left(\sum_{j=1}^{m}\left(1-\left(P(T)_{vj}{}^{*}\cdot x_v\right)/\left(1-\min\left(P(T)_{v^*j}{}^{*}\cdot x_v\right)\right)\right)/m\right)\cdot 10 \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1,\dots,w\}, w \in Z \\ j \in \{1,\dots,m\}, m \in Z \\ \text{Else } KPI_2 = 0 \end{cases} \quad (19)$$

Therefore, KPI_2, ranging between $[0,10]$, expresses again the combined economic and technical performance of a combination of security measures, according to the break-even approach. However, KPI_2 is normalized with respect to the most cost-effective option v^*obtained from a break-even approach for each scenario j, which scores 10 and weighted on all the scenarios m. Also in this case, if the combination does not respect the budget constraints for all the scenarios, the indicator value is zero.

An overall performance indicator is calculated from the combination of KPI_1 and KPI_2:

$$\begin{cases} \text{If } KPI_1 \ge \alpha \text{ and } KPI_2 \ge \beta \\ ECS = (KPI_1 + KPI_2)\cdot 0.5 \\ \text{Else } ECS = 0 \end{cases} \quad (20)$$

Where ECS is an overall cost-effectiveness indicator, again ranging between $[0, 10]$. Constants α and β are acceptability thresholds, having a value ranging between [0, 10], which may be introduced by the security analyst and discussed with management, to warrant that combinations considered in decision-making perform above some minimum threshold values, under both the deterministic and break-even approaches. A possible guideline for the selection of α and β values has been proposed in Table 3. From a general perspective, in case of security managers that tend to put the focus of the economic analysis on the profitability of measures regardless the likelihood of the attack (i.e., high values of Net Benefit under deterministic approach and consequently high values of KPI_1), it is suggested to adopt high or very high α values. On the contrary, in case of security managers that tend to put the focus of the economic analysis on having an acceptable measure even with very low likelihood of the attack (i.e., low break-even probability and consequently high KPI_2), it is suggested to adopt high or very high β values. Other α and β values fall within the two discussed extremes.

Table 3 Guideline on α and β acceptability thresholds for security analysts.

Qualitative description of acceptability thresholds	**α**		**β**	
	Range of values for α	**Requirement for α selection**	**Range of values for β**	**Requirement for β selection**
Very high	$(8, 10]$	Very high Net benefit accepted under deterministic approach by security management	$(8, 10]$	Very low break-even probability accepted by security management
High	$(6, 8]$	High Net benefit accepted under deterministic approach by security management	$(6, 8]$	Low break-even probability accepted by security management
Medium	$(4, 6]$	Medium Net benefit accepted under deterministic approach by security management	$(4, 6]$	Medium break-even probability accepted by security management
Low	$(2, 4]$	Low Net benefit accepted under deterministic approach by security management	$(2, 4]$	High break-even probability accepted by security management
Very low	$[0, 2]$	Very low Net benefit accepted under deterministic approach by security management	$[0, 2]$	Very high break-even probability accepted by security management

Therefore, the module provides a scoring system based on three indicators, all ranging within $[0,10]$: two intermediate economic indicators, expressing respectively deterministic and break-even cost-effectiveness

approaches, and an overall cost-effectiveness indicator. The scoring system provides the basis for a sound comparison of all possible security alternatives.

3 Case study

3.1 Definition of the case study

The ECO-SECURE model was applied to an illustrative case study, consisting in the terroristic sabotage of four storage tanks in a fuel storage facility, aimed at causing environmental damages by releasing water pollutants. The oil depot considered in the case study includes 37 storage tanks containing various liquid hydrocarbons, as diesel and heating oil. The accident scenario consisted of a sequential sabotage of four storage tanks, named after respectively Target 1, Target 2, Target 3 and Target 4, as shown in Figure 3. Target 1 and Target 2 are two heating oil tanks, containing in total 800,000 kg of product; while Target 3 and Target 4 are two diesel tanks, containing in total 1,800,000 kg of product. The distances among the targets have been reported in Table 4, Part B. The damages, as well as the plant layout, are freely adapted from a real security-based accident that took place during the night between 22nd and 23rd February 2010 in Villasanta, Monza-Brianza province, Italy (Alpas et al., 2011; Associated Press in Rome, 2010; EMARS - Major accidents reporting system, 2010; Winfield, 2010a). However, the case study is fictional and its aim is the validation and the further implementation of the model, addressing the selection and allocation of physical security measures against environmental and eco-terroristic attacks in a chemical facility. Therefore, the causes of the security-based accident here-in considered (i.e., an external environmental terroristic attack) are not related to the causes of the real accident (Berni, 2016; La Repubblica, 2016).

The starting point for the adversary was chosen in correspondence of a railway route just outside the border of the facility, at about 50 m distance from the first target. The adversary was supposed to carry out the sabotage action by foot. The sabotage sequence of actions consisted in opening a valve and switching on a pump in correspondence of each target, leading to the spill of the entire contents of the four tanks, for a total amount of 2,600,000 kg of hydrocarbon liquid products (ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010). The spill substance, from the pipes of the loading docks and the repayment of the product, overfilled the tanks of the oil-water separator tank coming indirectly from the sewage system inside the plant and directly passed to curb protection, likely due to saturation of the sewer system itself; part of the spill was also poured into the containment basins. Then, the spill was drained from the oil-water tank through the main valve, always kept open to allow the discharge of wastewater from a hydraulic barrier aimed at remediation, to the sewer outside the plant, which flows into the main collector. Indeed, the spill reached the treatment plant of the nearby city through the main sewer. Consequently, the spill has been poured into the nearby river and caused a significant pollution of river water and rive sides downstream of the filter for about 100 km, with involvement of a second river in the stretch downstream from the mouth of the first river. Contaminated waters of the second river affected the second river delta and the coastal area of the sea. In the actual event, the Lambro river (i.e., first river in the case study) and the Po river (i.e., second river in the case study) were polluted for about 350 km. The realistic damages, derived from the actual event, consisted in severe environmental losses to the ecosystem, requiring therefore emergency actions to contain pollution that lasted several days after the accident. Furthermore, intense monitoring and in-site and off-site remediation actions were required during the subsequent months. The company had to sustain legal costs due to prosecution, as well as the payment of fines. The accident resulted in no human losses but in severe damages to the environment, in economic damage to the company, and in collateral damages to surrounding activities and public infrastructures (e.g., the treatment plant was off for about one month) in the nearby densely populated area (EMARS - Major accidents reporting system, 2010).

The determination of PPS in place was carried out using available information and comparing the description of PPS usually present in chemical facilities (Reniers et al., 2015) with photos and maps of the layout of the reference installation, reported in Figure 3. The screening allowed the identification of key protection

elements and key distances, which are data necessary to calculate the baseline physical protection system effectiveness. Further information on the PPS in place are reported in Section 3.2.

Figure 3 Layout of the reference installation considered in the case study, with adversary starting point and path of actions, the latter indicated by the numbers. The ending point is target 4. Further information on adversary tasks is available in Table 4. The layout has been retrieved from Google Earth®.

The application was carried out in Excel® modelling environment, using 7 different datasheets, corresponding to ECO-SECURE modules, as explained in Section 2.1.

3.2 Development of adversary sequence diagram and effectiveness calculation

3.2.1 Definition of site-specific adversary sequence diagrams and calculation of the baseline system effectiveness

A possible critical site-specific adversary sequence path, in relation with physical protection elements present on the reference site, was defined and is described in Table 4, Part A and shown in Figure 3. The calculation of baseline system effectiveness was carried out according to the approach described in Section 2.2, with the aim to determine the probability of interruption $(P_I{}^*)$ of the critical adversary path. The solely detection elements present are cameras on the wall delimiting the two storage areas, with $P_{AD,9} = 0.9$. The probability of assessed detection $(P_{AD,i})$ expresses the likelihood of detecting an adversary within the zone covered by cameras or intrusion detection sensors. In addition, the location of detection elements was included in the analysis, according to the EASI model. For all delay elements with the exception of running times, specific data have been retrieved (Garcia, 2007) and reported in Table 4, Part A, jointly with all the data inherent to the detection function for the path considered in the case study. For the calculation of running times, the standard adversary velocity of $10\ ft/s = 3.048\ m/s$ has been assumed, considering a reduction factor due to additional weights carried by the adversary unitary (i.e., no additional weight carried by the adversary). Distances among delay elements were retrieved from the reference map and reported in Table 4, Part B. Standard deviation for the delay parameter of each security element and for the response force time parameter was assumed as $3/10$ of the mean value throughout the case study, according to the conservative assumption on data dispersion reported in the EASI model (Garcia, 2007). This assumption allows considering that guards will not always respond exactly after the same time, and that adversaries may take more or less time to penetrate barriers with respect to average values. Inputs for the calculation of response element have been reported in Table 4, Part C; for the probability of guard communication (P_C) a conventional value for industrial facilities was assumed (Garcia, 2007), with a response force time of 8 minutes, considering that security guards are not present on site during the night shift, with the exception of the facility caretaker. The critical probability of interruption $(P_I{}^*)$ has been calculated according to equation

(1) and its value is 0.0425. $P_I{}^*$will be considered in the development of the case study and represents the value of the baseline PPS effectiveness (i.e., $\eta_{PPS,old}$). The value was obtained by inserting in the EASI model datasheet (Garcia, 2007) the inputs listed in Table 4, according to the approach described in Section 2.2. Therefore, the calculation of baseline system effectiveness highlights security weaknesses, which may be tackled by the introduction of pertinent security upgrades. The baseline effectiveness calculations can be performed in other case studies, according to the same approach; however, the results are site-specific as they require data regarding distances on site and security measures in place. Therefore the value of baseline effectiveness obtained (i.e., 0.0425) cannot be extended beyond the current case study.

Table 4 Input for the calculation of baseline PPS effectiveness referred to the critical path. Part A) Adversary sequence and inputs for the calculation of detection and delay elements referred to the identified adversary path; Part B) Additional data for the calculation of running delay times; Part C) Inputs for the calculation of the response function. Standard deviation was assumed 3/10 of the mean value. Values retrieved from data repository (Garcia, 2007) and site-specific plant layout.

Part A) Adversary Sequence Diagrams and Inputs for Detection and Delay elements

ADVERSARY TASKS		*DETECTION*	*DELAY*	
Task number	***Task Description***	***Detection elements and assessed detection probabilities*** $P_{AD,i}$	***Delay elements***	***Mean delays*** $t_{D,i}$ ***(s)***
1	**Starting point**	-	-	-
2	**Climb external wall**	None	Height of the wall	10.0
3	**Run to first tank (Target 1)**	None	Running time	14.8
4	**Open first valve**	None	Time required to open first valve	30.0
5	**Activate first pump**	None	Time required to activate first pump	60.0
6	**Run to second tank (Target 2)**	None	Running time	16.4
7	**Open second valve**	None	Time required to open second valve	30.0
8	**Activate second pump**	None	Time required to activate second pump	60.0
9	**Run to third tank (Target 3)**	Camera on wall delimiting two areas ($P_{AD,9} = 0.9$)	Running time	26.9
10	**Open third valve**	None	Time required to open third valve	30.0
11	**Activate third pump**	None	Time required to activate third pump	60.0
12	**Run to fourth tank (Target 4)**	None	Running time	43.6
13	**Open fourth valve**	None	Time required to open fourth valve	30.0
14	**Activate fourth pump**	None	Time required to activate fourth pump	60.0
15	**Ending point**	-	-	-

Part B) Data for Calculation of running delay times

Description of the action	*Symbol*	*Value*	*Unit*	*Description of the action*	*Symbol*	*Value*	*Unit*
Adversary velocity during running	v	3.048	*m/s*	**Distance external wall/ target 1 (Task 3)**	d_3	45	*m*
Distance target 1/ target 2 (Task 6)	d_6	50	*m*	**Distance target 2/ target 3 (Task 9)**	d_9	82	*m*
Distance target 3/ target 4 (Task 12)	d_{12}	133	*m*	**Reduction factor due to additional weight carried by adversary**	φ	1	*Adim.*

Part C) Data for the calculation of Response function

Probability of guard communication P_C	0.95	*Mean Response Force Time* t_G *(s)*	480

3.2.2 Security upgrades identification and calculation of upgraded system effectiveness (ΔR_i)

Starting from the value of baseline PPS effectiveness $(\eta_{PPS,old} = 0.0425)$, six PPS upgrades have been proposed, according to technical references (Garcia, 2007; Reniers et al., 2015):

A) Adding surveillance cameras as perimeter detection system;

B) Construction or additional height to concrete-reinforced external perimeter wall as perimeter delay element;
C) Adding detection elements (i.e., surveillance cameras) at sabotage targets level;
D) Adding delay elements at sabotage targets level;
E) Adding alarm for unauthorized manual valve opening and cages to hinder unplanned switching on/off pumps at sabotage targets level;
F) Reducing response force time by building a closer and 24h active guard dispatch.

It should be noted that upgrades A and C refer to the detection function, upgrades B and D refer to the delay function, upgrade E refers to the combination of detection and delay functions and upgrade F refers to the response function. Moreover, upgrades A and B refer to the external perimeter of the facility, while upgrades C, D, E and F refer to the proximity to the sabotage targets. All the tanks of the storage facility have been considered possible targets.

Table 5 Effectiveness results for six different possible PPS upgrades. From the left to the right, in column order: Upgrade identity, description of the upgrade, Physical protection function modification, reference number of adversary sequence diagram modified tasks, modified inputs for the effectiveness calculations, upgraded PPS effectiveness ($\eta_{PPS,new\,i}$) and risk reduction (ΔR_i). (*) Reduction of response force time does not affect a single task. A data repository regarding modified inputs values for security upgrades is available in Garcia (Garcia, 2007).

Upgrade ID	*Description*	*PPS - function modification*	*N° of modified tasks*	*Modified inputs*	$\eta_{PPS,\,new\,i}$	ΔR_i
A	**Addition of cameras at external perimeter wall level**	Detection; exterior cameras	2	$P_{AD,2} = 0.9$	0.3904	**0.3479**
B	**Construction/ additional height to external concrete-reinforced perimeter wall (3m high)**	Delay; wall hardness	2	$t_{D,2} = 180\ s$	0.0425	**0**
C	**Addition of detection elements at sabotage targets (cameras on each tank)**	Detection; exterior cameras	3; 6; 9; 12	$P_{AD,3} = P_{AD,6} = P_{AD,12} = 0.9$ $P_{AD,9} = 0.99$ for existing cameras	0.3685	**0.3260**
D	**Addition of delay elements at sabotage targets**	Delay; additional wall with doors	3; 6; 9; 12	$t_{D,3} = t_{D,6} = t_{D,9} = t_{D,12} = 30\ s$ additional delay with running time	0.0783	**0.0358**
E	**Addition of alarms for unauthorized manual valves opening and cages for pumps at sabotage targets**	Detection (alarms); Delay (cages)	4; 7; 10; 13 5; 8; 11; 14	$P_{AD,4} = P_{AD,7} = P_{AD,10} = P_{AD,13} = 0.9$ for alarms $t_{D,5} = t_{D,8} = t_{D,11} = t_{D,14} = 30\ s$ for pumps cages	0.5215	**0.4790**
F	**Reduction of response force time (by creating a closer and 24h active guard dispatch)**	Response; relocation of guards closer to storage area	- (*)	$t_G = 240\ s$	0.5771	**0.5346**

The upgraded values of effectiveness, indicated as $\eta_{PPS,new\,i}$, for each of the six options have been calculated by inserting the modified input items, listed in Table 5 (i.e., third to last column), in the effectiveness model previously applied to calculate baseline PPS effectiveness (i.e., the EASI model), according to the approach presented in Section 2.3. The modified inputs regarding each security upgrade, with the exception of upgrade F, affect only specific tasks of the adversary sequence diagram; for all the remaining tasks, the values reported in Table 4 have been applied.

The results regarding upgraded effectiveness (i.e., $\eta_{PPS,new\,i}$) and effectiveness improvement index (i.e., ΔR_i, named also risk reduction), corresponding to each of these upgrades, have also been reported in Table 5. Risk reduction values have been obtained for each security upgrade according to equation (3), using the baseline effectiveness value (i.e., $\eta_{PPS,old} = 0.0425$) and the upgraded effectiveness value (i.e., $\eta_{PPS,new\,i}$).

The results in Table 5 clearly show that, from the effectiveness point of view, the best option is the reduction of response force time (upgrade F), followed by the application of alarms for valves and cages for pumps at sabotage targets level (upgrade E). On the other hand, the presence of additional delay elements, represented by options B and D, proved to be ineffective in increasing PPS effectiveness. The addition of detection elements (i.e, cameras), both at external and sabotage targets level, represented respectively by upgrade A and C, shows an intermediate performance in terms of risk reduction. However, even if upgrades F and E are the best ones from the effectiveness intermediate calculation, it does not mean automatically that they are the best options in the end of the application, due to additional terms that are still to be considered in the analysis (e.g., costs, benefits, budget threshold, etc.). The approach presented in Section 2.3., here applied, can be used analogously in other case studies. However, the results of effectiveness calculations are site-specific and accident-specific; consequently they cannot be generalized beyond the current case study.

3.3 Cost calculation for security upgrades

Cost calculations were carried out for each of the six PPS upgrades proposed in the case study, according to the six main categories and 22 subcategories presented in ECO-SECURE (Section 2.4), considering the time span of one year and the implementation of a single security upgrade. Details of the calculations are reported in Appendix A.1. Figure 4 summarizes the results obtained. The values of Overall costs belong to the same order of magnitude (i.e., 10^4 €) for all the security upgrades, with the exception of upgrade F that is one order of magnitude higher. The comparison among percentage compositions, also reported in Figure 4, shows that for detection and delay elements (i.e., upgrades A, B, C, D and E) installation costs are the prevailing ones. For upgrades regarding the detection function (i.e., upgrades A, C and E), initial costs and operational costs are also relevant items.

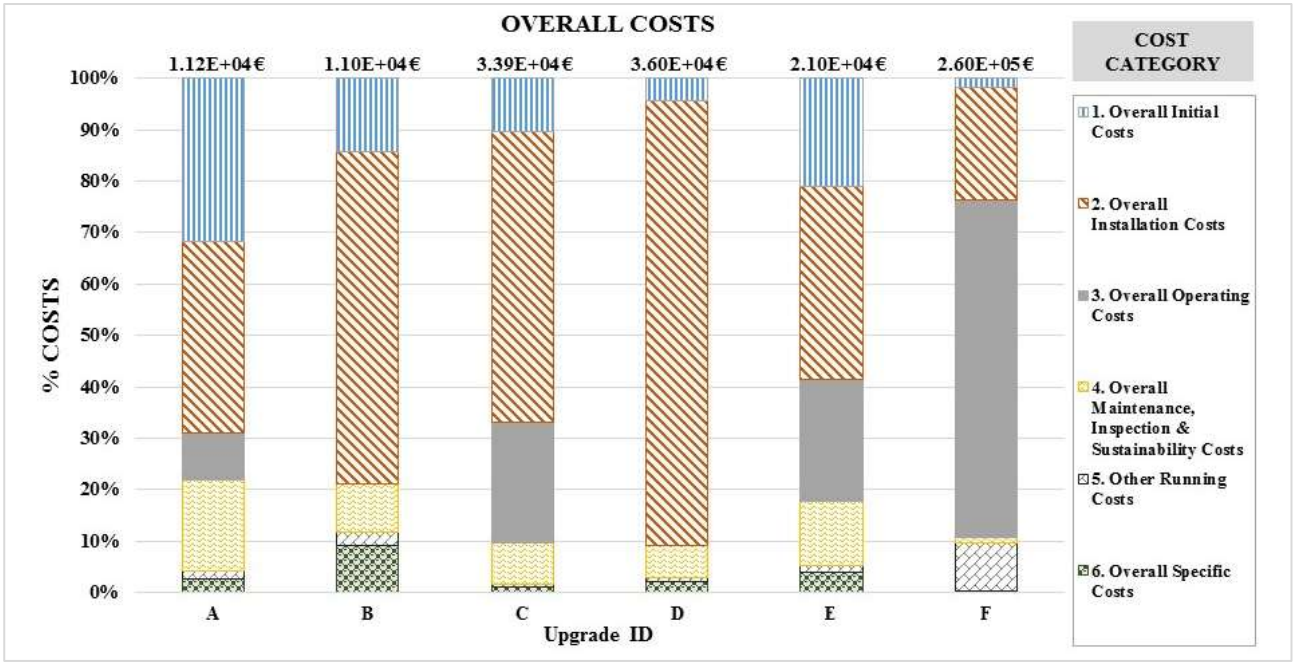


Figure 4 Percentage composition of Overall costs for each upgrade of the PPS, according to the six cost categories considered, under the assumption of $P(T)_{ij} = 1$. On x-axis, from the left to the right, the six PPS upgrades are represented: A) Adding surveillance cameras as perimeter detection system; B) Construction or additional height to concrete-reinforced external perimeter wall as perimeter delay element; C) Adding detection elements (i.e., surveillance cameras) at sabotage targets level; D) Adding delay elements at sabotage targets level; E) Adding alarms for unauthorized manual valves opening and cages to hinder unplanned switching on/off of pumps at sabotage targets level; F) Reducing response force time by building a closer and 24h active guard dispatch. Overall cost of each security upgrade is reported on the top of the corresponding column.

3.4 Benefit calculation for the actual scenario

The losses derived from a successful attack should include the environmental damages and other damages, both direct and indirect, which will accrue because of a successful attack, taking into account the value and

vulnerability of environment, people and infrastructures, as described in Section 2.5. Consequently, benefits calculations are dependent on the choice of an appropriate accidental scenario. In case of economic analyses based on a real event it is common practice to account the retrospective losses, named also realistic benefits, which indicate the actual losses sustained in the accident. Therefore, the realistic benefits were considered in the case study. These may not exactly reflect the actual ones, due to the limited amount of technical and site-specific information available. It was assumed that benefits are independent from the security measure that can be implemented.

The details of the calculations are reported in Appendix A.2; the results of benefit calculations are summarized in Figure 5. The overall benefits were estimated of $8.16 \cdot 10^7$ €, justifying therefore the definition of the accident as an "ecological disaster" (Winfield, 2010b). As shown in Figure 5, environmental benefits are strongly prevailing (i.e., about 47% of Overall benefits), with a particular relevance of the environmental remediation benefits subcategory. Moreover, reputational benefits and legal and insurance benefits are relevant (i.e., about 23% and 25% of Overall benefits respectively), due to the high media coverage give to the accident and to the legal procedures. The calculated benefit apportionment is typical of a major accident. Indeed, as stated in previous studies referred to the chemical industry domain (Gavious et al., 2009; Reniers and Brijs, 2014a), the value of indirect losses, which include for instance reputational losses, human and environmental losses, legal and insurance losses, is generally superior to direct losses. The gap tends to increase with the increasing severity of the accident (Gavious et al., 2009). Moreover, the comparison with a previous work, regarding the estimation of reputational losses derived from notorious accidents within the same domain (Kyaw and Paltrinieri, 2015), confirmed the gravity of reputational losses with respect to Overall benefits. In the present case study, damage benefits represent only 2% of Overall benefits derived from an environmental disaster. This low percentage value is confirmed by a previous application referred to a less severe accident scenario (Gavious et al., 2009) that estimated damage benefits around 10% of Overall benefits (i.e., $3{,}56 \cdot 10^5$ €).

The application of a possible global approach toward benefit calculations, including human and assets damages, has no relevance on the present case study, as human benefits value is zero, due to the absence of casualties and morbidities.

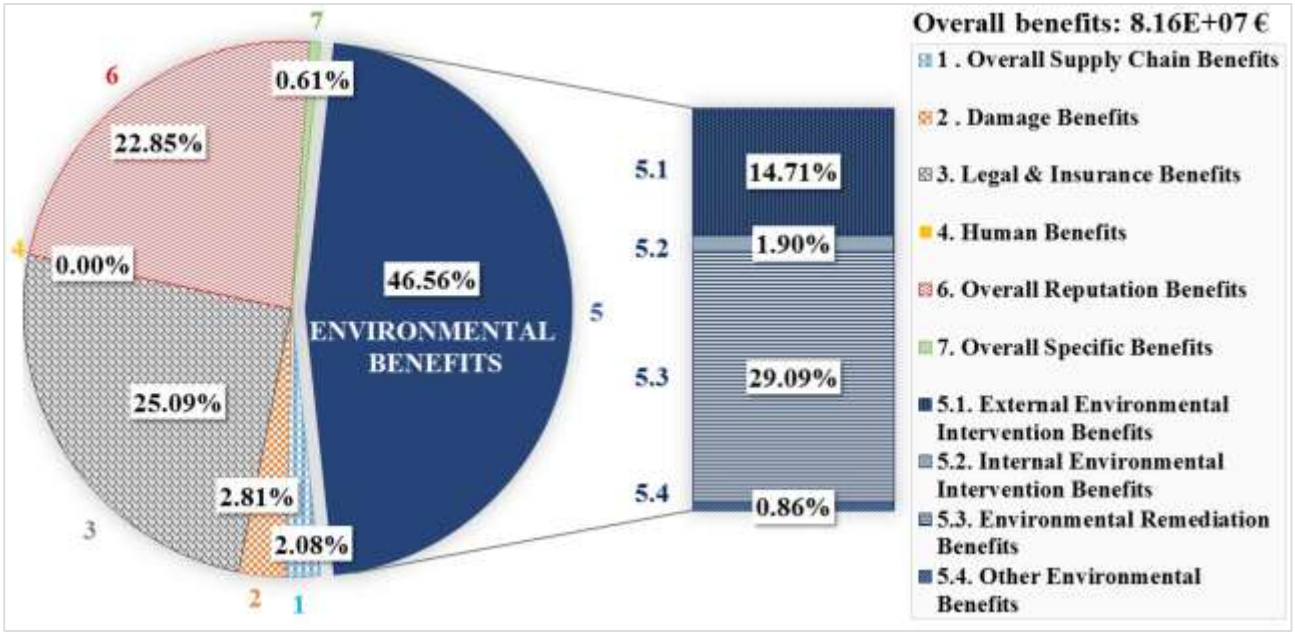


Figure 5 Percentage composition of Overall benefits for the actual scenario, according to seven benefits categories.

4 Results

The results of the assessment of the case study consist in cost-benefit analysis results, cost-effectiveness analysis results and final results based on the application of an original scoring system to cost-effectiveness analysis. Overall costs for each security measure and Overall benefits for each scenario have been made comparable by applying appropriate discount rates (i.e., 3.5% and 1.5% respectively (HSE - Health and Safety Executive, 2016)) over a 10 year time-span, according to equation (11). The latter is a conventional number of operational years for a security measure. With regards to the deterministic approach, the conservative conditional threat probability assumption of $P(T)_{ij} = 1$ has been taken (Garcia, 2007), because the scenario analysis is retrospective and refers to an environmental disaster.

Cost-benefit analysis results, reported in Table 6 for both the deterministic and break-even approaches, are coherent. Indeed, the security measures A, C, D, E and F may be applied according to the actual scenario. Therefore, the simple application of a conventional cost-benefit analysis does not offer precise indication on which single measure is the most useful with respect to the case study.

Table 6 Cost-benefit analysis results according to a deterministic and a break-even approach, in term of Net Benefits and $P(T)_{ij}^{*}$ respectively, for six different PPS upgrades with respect to the actual scenario.

PPS UPGRADE		DETERMINISTIC APPROACH		BREAK-EVEN APPROACH	
		Net Benefit	Upgrade economic feasibility	$P(T)_{ij}^{*}$	Upgrade economic feasibility
Upgrade ID	DESCRIPTION/UNIT	€	-	*adim.*	-
A	Addition of cameras at external perimeter wall level	1.89E+07	accept	1.75E-04	accept
B	Additional height to external perimeter wall (3m instead of 1.5m)	-3.14E+03	refuse	1.00E+00	refuse
C	Addition of a detection element at the sabotage targets (cameras on each tank)	1.77E+07	accept	5.53E-04	accept
D	Addition of a delay element at the sabotage targets (concrete wall + security door)	1.94E+06	accept	3.95E-04	accept
E	Putting alarms for unauthorized manual valves opening and cages for pumps at sabotage targets	2.60E+07	accept	2.35E-04	accept
F	Reduction of response force time (by creating a closer and 24h active guard dispatch)	2.90E+07	accept	2.56E-03	accept

Cost-effectiveness analysis was thus applied to determine the most profitable combination of security upgrades within the security budget constraint, according to a deterministic approach and a break-even approach. All the possible 63 combinations of PPS upgrades have been considered. Actualized Overall costs were calculated for each combination summing the Overall costs of each option and applying a 3.5% discount rate (HSE - Health and Safety Executive, 2016). Overall costs were then compared with the actualized security budget. Actualized security budget value considered is of 51.4 k€. The results, reported in Table 6, show that the most profitable combinations of security measures are different between deterministic and break-even approaches. Nevertheless, upgrades A (i.e., addition of cameras at external perimeter wall level) and/or upgrade E (i.e., installing alarms for unauthorized manual valves opening and cages for pumps at sabotage targets) are present within all the most profitable combinations, regardless the approach.

In order to allow a comparison of the results obtained from the two approaches, indicators KPI_1 and KPI_2, expressing deterministic and break-even cost-effectiveness analysis results, were calculated. The results for the most profitable combinations are reported in Table 7.

Table 7 Cost-effectiveness analysis results according to deterministic and break-even approaches. From the top to the bottom: first-most profitable combination, second-most profitable combination and third-most profitable combination.

COST-EFFECTIVENESS RANKING	*DETERMINISTIC APPROACH*				*BREAK-EVEN APPROACH*			
	Combination ID	*Net Benefit* (€)	*Total Cost of Combination* (€)	KPI_1	*Combination ID*	$P(T)_{vj}^{*}$ *(adim)*	*Total Cost of Combination* (€)	KPI_2
FIRST	**A+C+D+E**	**6.46E+07**	2.91E+04	10	**A**	**1.75E-04**	3.31E+03	10
SECOND	**A+B+C+D+E**	**6.46E+07**	3.23E+04	9.9995	**A+E**	**2.09E-04**	9.42E+03	9.9997
THIRD	**A+C+E**	**6.27E+07**	1.89E+04	9.7003	**E**	**2.35E-04**	6.11E+03	9.9994

Figure 6 shows the values calculated for the overall cost-effectiveness indicator, ECS, obtained combining KPI_1 and KPI_2, according to equation (20) and setting both the threshold values in the equation, α and β, equal to 3. All the combinations not complying with threshold values were not reported in Figure 6.

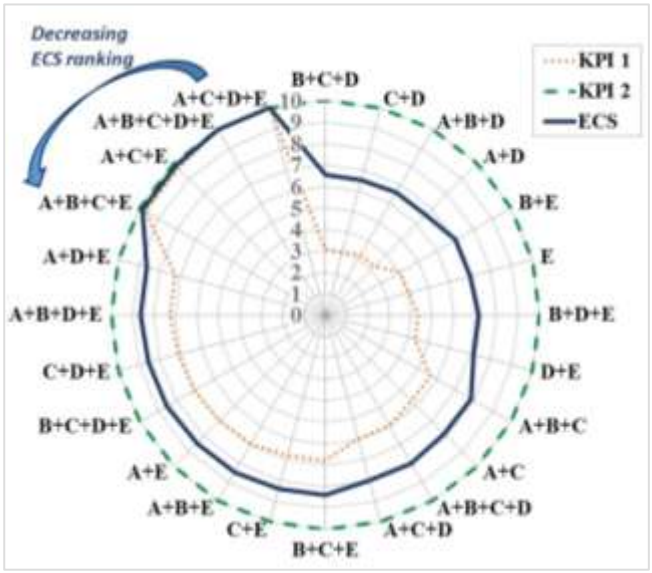


Figure 6 Values calculated for the deterministic performance indicators (KPI_1), break-even performance indicator (KPI_2) and overall cost-effectiveness indicator (ECS). Only combinations with threshold values α and β higher than 3 are reported.

As shown in the figure, the combinations with the highest values of ECS always include at least three measures. All the ten top combinations offer an integration of different security functions (i.e., detection, delay and response), providing therefore a more complete security protection. It should be noted that none of the combinations reported in Figure 6 include the security upgrade F, because its overall cost does not respect the security budget, even if its effectiveness improvement is the highest one.

5 Discussion

ECO-SECURE offers a complete framework for economic analysis, aimed at the selection and allocation of security measures w.r.t. environmental accidents, within the specific chemical industry context. Moreover, the model is relatively straightforward, enhancing its possibility to be applied in industrial practice. The application of ECO-SECURE to a case study suggested some answers to practical challenges that a security manager may face within a chemical facility.

The results obtained from the analysis of the case-study provided insights on three main issues:

(1) Advantages and limitations of input modules (modules from 0 to 3);
(2) Advantages and limitations of economic analysis modules (modules from 4 to 6);
(3) Possible further developments of the methodology.

Concerning point (1), input modules provide a complete evaluation with respect to costs and performances of security measures, as well as to losses, fostering the consequent accuracy of results. ECO-SECURE offers, according to modules from 0 to 2, site-specific answers to security analysts, because it allows evaluating the performance of physical security measures present on-site and comparing several security upgrades according to technical and economic criteria, as well as possible adversary paths dependent on the layout of the facility. As highlighted in ECO-SECURE application, the precise checklist provided for costs and benefits evaluation, in modules 2 and 3 respectively, may prevent omissions and inaccuracies. Moreover, regarding benefit assessment (i.e., module 3) ECO-SECURE may be applied both in predictive and in posterior analysis, as well as to different accident scenarios, in order to obtain scenario-specific economic indicators to be compared.

However, inputs modules show some limitations. As all economic analyses, the inputs may reflect the subjectivity of the analyst, concerning the monetization of intangible costs and benefits, whose inaccuracies may lead to misleading results. Moreover, although effectiveness assessment (i.e, module 1) is able to take into account uncertainties that may decrease the overall performance of the PPS (e.g., possible lag-time in detection by security guards), it offers just a simplified description of a possible real accident. Another possible limitation regarding inputs modules is the choice of an appropriate pool of security upgrades (i.e., module 1) and accidental scenarios (i.e., module 3) that is up to the security analysis, in particular whenever a prospective analysis should be performed. For this reason, whenever ECO-SECURE is applied, it is important to present the analysis in a fully transparent manner, specifying the assumptions made and discussing the uncertainties arisen from inputs modules.

Concerning economic analysis modules (issue 2, modules 4 to 6), three distinctive positive features of ECO-SECURE can be outlined. The method allows the combined use of both cost-benefit and cost-effectiveness analysis, adopts two complementary approaches to the likelihood of the attack (deterministic and break-even, see module 4), leading to an integrated specific scoring system.

The model allows performing economic analysis by means of both cost-benefit and cost-effectiveness analysis, according to module 5 and 6 respectively, offering as outputs a broad spectrum of economic analyses results, which can eventually support the security decision-making process. The application of solely cost-benefit analysis, according to module 5, might not provide significant screening criteria, in particular with reference to very severe environmental accidents. Costs of security measures are several orders of magnitude inferior to overall losses, resulting therefore in the feasibility of almost all the single security measures, as visible from the results of the case study reported in Section 4 (Table 6). Instead, cost-effectiveness analysis (i.e., module 6) may offer sound indications for the stakeholders to rationally select and allocate security measures, providing a range of economically profitable options that consider also security measures combinations within the budget constraints, as highlighted by the results of the case study reported in Section 4 (Table 7).

The combined application of deterministic and break-even approaches to cost-benefit and cost-effectiveness analysis offers a significant advantage within economic analyses, as it allows inserting directly the uncertainties related to the estimation of the likelihood of the attack in the model, avoiding the necessity to perform an additional sensitivity analysis on the results. The deterministic approach, provided in modules 5.1 and 6.1, offers to the security manager insight on the optimal revision of the physical protection system, within the constraint of the annual security budget, after a variation regarding the likelihood of the attack (e.g., due to socio-political changes, increased visibility of the target, etc.). Therefore, it defines the optimal allocation of security upgrades, as a trade-off of two relevant parameters: cost and effectiveness improvement index. The break-even approach, provided in modules 5.2 and 6.2, starting from a range of security options, allows defining the minimum likelihood of the attack that makes each option economically profitable, within the constraint of the annual security budget.

Nevertheless, it should be noted that all results of economic analyses may vary depending on the assumptions made by the security analysis on discount rates for costs and benefits. Moreover, cost-effectiveness analyses results may vary also depending on the threshold of the security budget, that is generally defined yearly by security management. For this reason, when applying the method, it is necessary to present assumptions introduced and uncertainties arisen transparently.

Another original feature of the model is the use of a specific scoring system (i.e., module 6.3), made necessary to compare the cost-effectiveness results obtained from the two approaches and to eventually combine them into an overall cost-effectiveness indicator (i.e., ECS). Eventual company-specific acceptance criteria and additional information should be considered. For instance, as visible from case study results in Section 4 (Figure 6), the application of the scoring system makes the model more understandable to decision-makers with non-technical backgrounds, because the final output of ECO-SECURE is constituted by solely one typology of indicator (i.e., ECS). Therefore, the application of an original scoring system allows to compare a limited pool of final combinations, and consequently to allocate the dedicated budget on security upgrades according to a rational criteria.

Concerning the possible further development of the methodology (issue 3), presently the methodology is limited to the selection and allocation of preventive security measures against environmental security-based accidents. This limitation is imposed by the specific features of such devices, and by the different intent of preventive measures with respect to mitigation measures (i.e., safety measures). Mitigation may consider both intentional and unintentional accidents and, as such, needs to incorporate a different analysis, including unintentional failure scenarios. Indeed, the tools required to carry out such analysis are different and address a specific legislation context. Nevertheless, in further research developments, the methodology will be extended to address post-accident mitigation, in purpose to compare the possible role of safety and security measures with respect to environmental accidents. The extended methodology will allow decision-maker to have an integrated view of safety and security deficits in a chemical installation and to allocate the budget on the most critical aspect (i.e., either on preventive or on mitigation measures).

The outputs of ECO-SECURE might be applied in risk-informed security decision-making at company level with different purposes: to increase the awareness of management towards environmental security issues by means of non-technical and rather user-friendly outputs, to tackle security vulnerability chemical facilities and to allocate the budget on profitable physical protection alternatives w.r.t. environmental accidents. Nevertheless, the general concepts of this economic model are applicable beyond the industrial security domain; for instance, to support security decision-making at social level against environmental damages (e.g., selection of security measures to prevent vandalism).

Eventually, ECO-SECURE application, as demonstrated by the case study, may be a systematic useful tool to cope with environmental-security based incidents in chemical facilities.

6 Conclusions

The model developed provides to security managers indications on the most profitable single security upgrades and combinations of them needed to prevent security-based accident scenarios. Results of deterministic analysis allow upgrading the physical protection system, according to possible variations in the likelihood of the attack. Break-even analysis provides the optimal allocation of the security budget, defined yearly by security management. The application of a specific scoring system allows comparing the two set of results, obtaining overall indicators. Thus, the method enables to define a more rational selection and allocation of physical security measures and its outputs provide a sound support to managers within the decision-making process. Its application may eventually contribute to the reduction of chemical plants vulnerability toward environmental and ecological terroristic attacks.

References

Ale, B.J.M., Hartford, D.N.D., Slater, D., 2015. ALARP and CBA all in the same game. Safety Science 76, 90–100. doi:10.1016/j.ssci.2015.02.012

Alibi, 2016. 3.0 Megapixel 100' IR IP Outdoor Bullet Security Camera - Technical and commercial datasheet [WWW Document]. Super Circuits Website. URL http://www.supercircuits.com/alibi-megapixel-day-night-ir-ip-outdoor-security-camera-ali-ipu3130r (accessed 11.15.16).

Alpas, H., Berkowicz, S.M., Ermakova, I., 2011. Environmental Security and Ecoterrorism, NATO Science for Peace and Security Series C: Environmental Security. Springer Netherlands, Dordrecht, The Netherlands. doi:10.1007/978-94-007-1235-5

Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of the attractiveness of process facilities to terrorist attacks. Safety Science 77, 169–181. doi:10.1016/j.ssci.2015.02.013

ARIA, 2015. Accident study findings on malicious acts perpetrated in industrial facilities [WWW Document]. The ARIA database. URL http://www.aria.developpement-durable.gouv.fr/wp-content/uploads/2015/10/2015-10_01_SY_accidentologie_Malveillance_PA_FINAL_EN.pdf (accessed 11.15.16).

ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010. Ecoscienza. Emergenze ambientali, dal petrolio i rischi e i danni più gravi (in Italian). Bullettin of Environmental Protection Agency - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna 100.

Associated Press in Rome, 2010. Environmental disaster warning as oil spill reaches the Po, Italy's biggest riverest river [WWW Document]. The Guardian. URL http://www.theguardian.com/world/2010/feb/24/oil-spill-po-italy-river (accessed 11.15.16).

Aven, T., 2007. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering & System Safety 92, 745–754. doi:10.1016/j.ress.2006.03.008

Bajpai, S., Gupta, J.P., 2007. Terror-Proofing Chemical Process Industries. Process Safety and Environmental Protection 85, 559–565. doi:10.1205/psep06046

Berni, F., 2016. Lombarda Petroli: le motivazioni della sentenza che ha ribaltato il processo (in Italian) [WWW Document]. Il Cittadino MB - Il Quotidiano Online di Monza e Brianza. URL http://www.ilcittadinomb.it/stories/Cronaca/lombarda-petroli-le-motivazioni-della-sentenza-che-ha-ribaltato-il-processo_1180628_11/ (accessed 11.15.16).

Berni, F., Rosa, R., 2015. Lambro, il disastro Lombarda Petroli. Dopo 5 anni la bonifica è cancellata (in Italian) [WWW Document]. Corriere della Sera. URL http://milano.corriere.it/notizie/cronaca/15_febbraio_23/lambro-disastro-lombarda-petroli-5-anni-bonifica-cancellata-23d229c4-bb52-11e4-aa19-1dc436785f83.shtml (accessed 11.15.16).

BMT, 2016. Average cost of construction in Australia - Technical and commercial datasheet [WWW Document]. BMT Website. URL http://www.bmtqs.com.au/construction-cost-table (accessed 11.15.16).

Campbell, H.F., Brown, R.P.C., 2003. Benefit-Cost Analysis: Financial and Economic Appraisal using Spreadsheets. Cambridge University Press, Cambridge, UK.

CCPS - Center for Chemical Process Safety, 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers (AIChE), New York, USA.

Cox, L.A., 2009. Improving risk-based decision making for terrorism applications. Risk Analysis 29, 336–341. doi:10.1111/j.1539-6924.2009.01206.x

Dillon, R.L., Liebe, R.M., Bestafka, T., 2009. Risk-Based Decision Making for Terrorism Applications. Risk Analysis 29, 321–335. doi:10.1111/j.1539-6924.2008.01196.x

EMARS - Major accidents reporting system, 2010. Release of liquid hydrocarbons from an oil depot in Villasanta (Monza province –Lombardia Region-Northern Italy) with environmental consequences in the rivers Po and Lambro [WWW Document]. URL https://emars.jrc.ec.europa.eu/fileadmin/eMARS_Site/PhpPages/ViewAccident/ViewAccidentPublic.php?accident_code=756 (accessed 11.15.16).

Etkin, D.S., 1999. Estimating Cleanup Costs for Oil Spills, in: International Oil Spill Conference Proceedings. Arlington, Massachusetts, U.S:, pp. 35–39. doi:10.7901/2169-3358-1999-1-35

Eurostat, 2016. Electric prices for industrial consumers, second half 2014 [WWW Document]. Eurostat - statistics explained Website. URL http://ec.europa.eu/eurostat/statistics-explained/index.php/File:Electricity_prices_for_industrial_consumers,_second_half_2014_([1])_(EUR_per_kWh)_YB15.png#file (accessed 11.15.16).

Franceschi, A., 2010. Che fine ha fatto l'emergenza petrolio nel fiume Lambro? (in Italian) [WWW Document]. Il Sole 24 Ore Website. URL http://www.ilsole24ore.com/art/SoleOnLine4/Italia/2010/05/intervista-responsabile-acque-wwf-fiume-lambro.shtml?uuid=79c5be10-579b-11df-b335-c4e158cb6808&DocRulesView=Libero&refresh_ce=1 (accessed 11.15.16).

Galvani, M., 2015. Monza - Processo Lombarda Petroli. La verità di Tagliabue: volevano sabotare la cessione dell'area

(in Italian) [WWW Document]. Il Giorno. URL http://www.infonodo.org/node/40075 (accessed 11.15.16).

Garcia, M.L., 2007. The Design and Evaluation of Physical Protection Systems, Second. ed. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Garcia, M.L., 2005. Vulnerability Assessment of Physical Protection Systems. Elsevier Butterworth-Heinemann, Burlington, MA, USA.

Gavious, A., Mizrahi, S., Shani, Y., Minchuk, Y., 2009. The costs of industrial accidents for the organization: Developing methods and tools for evaluation and cost-benefit analysis of investment in safety. Journal of Loss Prevention in the Process Industries 22, 434–438. doi:10.1016/j.jlp.2009.02.008

Get A Quote, 2016. Concrete wall and footing price estimation [WWW Document]. Get A Quote Website. URL http://www.get-a-quote.net/quickcalc/concrete.htm (accessed 11.15.16).

Goossens, G.J.H., 2012. The Big Oil Spill : The Market Value Consequences of the Deepwater Horizon Disaster. Tilburg School of Economics and Management, Tilburg, Belgium.

Grainger, 2016. Security doors and frames - Technical and commercial datasheet [WWW Document]. Grainger Website. URL http://www.grainger.com/category/security-doors/door-and-door-frames/security/ecatalog/N-b6c (accessed 11.15.16).

Hansson, S.O., 2007. Philosophical Problems in Cost–Benefit Analysis. Economics and Philosophy 23, 163. doi:10.1017/S0266267107001356

Hester, P.T., Adams, K.M., Mahadevan, S., 2010. Examining metrics and methods for determining critical facility system effectiveness. International Journal of Critical Infrastructures 6, 211. doi:10.1504/IJCIS.2010.033337

HSE - Health and Safety Executive, 2016. Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions [WWW Document]. URL http://orr.gov.uk/__data/assets/pdf_file/0018/18009/revised-safety-cba-guidance-05022016.pdf (accessed 11.15.16).

Janssens, J., Talarico, L., Reniers, G., Sörensen, K., 2015. A decision model to allocate protective safety barriers and mitigate domino effects. Reliability Engineering & System Safety 143, 44–52. doi:10.1016/j.ress.2015.05.022

Kelman, S., 1981. Cost-benefit analysis: an ethical critique. Across the board 18, 74–82.

Kyaw, K., Paltrinieri, N., 2015. The cost of reputational damage when a major accident occurs, in: Safety and Reliability of Complex Engineered Systems. Proceedings of the European Safety and Reliability Conference, ESREL 2015. Zurich, Switzerland, pp. 4537–4544.

La Repubblica, 2016. Milano, petrolio nel Lambro: condannato in appello il titolare della ditta che scaricò i silos (in Italian) [WWW Document]. La Repubblica Milano Website. URL http://milano.repubblica.it/cronaca/2016/04/04/news/milano_petrolio_nel_lambro-136917367/ (accessed 11.15.16).

Landucci, G., Reniers, G., Cozzani, V., Salzano, E., 2015. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliability Engineering & System Safety 143, 53–62. doi:10.1016/j.ress.2015.03.004

Lee, W., Fan, W., Miller, M., Stolfo, S., Zadok, E., 2002. Toward cost-sensitive modeling for intrusion detection and response. Journal of Computer Security 10, 5–22.

Lin, P.-H., Van Gulijk, C., 2015. Cost-benefit analysis of surveillance technologies, in: Safety and Reliability: Methodology and Applications - Proceedings of the European Safety and Reliability Conference, ESREL 2014. pp. 409–415.

Lin, P.-H., Van Gulijk, C., 2014. Surveille Deliverable 3.5.: Cost Model [WWW Document]. Surveille FP7 European Program. URL http://surveille.eui.eu/

Martinez, L.J., Lambert, J.H., 2012. Risk-benefit-cost prioritisation of independent protection layers for a liquefied natural gas terminal. International Journal of Critical Infrastructures 8, 306–325. doi:10.1504/IJCIS.2012.050106

Neilan, C., 2016. BP's share price falls to six-year low as energy giant reveals worse-than-expected $2.2bn fourth quarter loss on back of falling oil prices [WWW Document]. City A.M. URL http://www.cityam.com/233593/bp-to-cut-7000-jobs-as-it-suffers-22bn-q4-loss-on-back-of-falling-oil-prices (accessed 11.15.16).

Nolan, D.P., 2008. Safety and Security Review for the Process Industries, Second. ed. Elsevier, Amsterdam, The Netherlands.

Paltrinieri, N., Bonvicini, S., Spadoni, G., Cozzani, V., 2012. Cost-Benefit Analysis of Passive Fire Protections in Road LPG Transportation. Risk Analysis 32, 200–219. doi:10.1111/j.1539-6924.2011.01654.x

PayScale, 2016. Salary Comparison, Salary Survey, Search Wages [WWW Document]. PayScale - Human Capital Website. URL http://www.payscale.com/ (accessed 11.15.16).

Pecorella, G., 2011. Sessione Bicamerale d'inchesta del Parlamento italiano - Missione in Lombardia riguardante il sabotaggio della Lombardia Petroli (in Italian) [WWW Document]. URL http://www.camera.it/_bicamerali/leg16/rifiuti/missioni/17Lombardia/Rif_20110208 - 10 LombardaP.pdf (accessed 11.15.16).

Querzé, R., 2010. Scaricati altri veleni nel Lambro (in Italian) [WWW Document]. Corriere della Sera. URL http://milano.corriere.it/notizie/cronaca/10_febbraio_28/lambro-scaricati-altri-veleni-sciacalli-1602569139849.shtml (accessed 11.15.16).

Reniers, G.L.L., 2014. Safety and Security Decisions in times of Economic Crisis : Establishing a Competitive Advantage. Chemical Engineering Transactions 36, 1–6. doi:10.3303/CET1436001

Reniers, G.L.L., 2010. Multi-Plant Safety and Security Management in the Chemical and Process Industries, First Ed. ed. WILEY-VCH Verlag GmbH & Co. KGaA, Weinheim, Germany. doi:10.1002/9783527630356

Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Safety and Environmental Protection 92, 583–589. doi:10.1016/j.psep.2013.04.002

Reniers, G.L.L., Brijs, T., 2014a. Major accident management in the process industry: An expert tool called CESMA for intelligent allocation of prevention investments. Process Safety and Environmental Protection 92, 779–788. doi:10.1016/j.psep.2014.02.003

Reniers, G.L.L., Brijs, T., 2014b. An Overview of Cost-benefit Models / Tools for Investigating Occupational Accidents. Chemical Engineering Transactions 36, 43–48. doi:10.3303/CET1436008

Reniers, G.L.L., Sörensen, K., 2013. An Approach for Optimal Allocation of Safety Resources: Using the Knapsack Problem to Take Aggregated Cost-Efficient Preventive Measures. Risk Analysis 33, 2056–2067. doi:10.1111/risa.12036

Reniers, G.L.L., Van Erp, H.R.N., 2016. Operational Safety Economics: A Practical Approach focused on the Chemical and Process Industries. Wiley.

Reniers, G.L.L., Van Lerberghe, P., Van Gulijk, C., 2015. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Safety Progress 34, 72–83. doi:10.1002/prs.11683

Richardson Products & Cost Data On Line Inc., 2008. Richardson International Construction Factors Manual [WWW Document]. Richardson books. URL http://www.icoste.org/Book_Reviews/CFM-Info.pdf (accessed 11.15.16).

Shenzhen An Ying Technology Co. Ltd., 2016. Industrial alarm system - Technical and commercial datasheet [WWW Document]. Alibaba Website. URL http://www.alibaba.com/product-detail/GSM-Industrial-Alarm-Systems-Quad-Band_1460101510.html?spm=a2700.7724838.0.0.1fwpoJ (accessed 11.15.16).

Spash, C.L., 1997. Ethics and Environmental Attitudes With Implications for Economic Valuation. Journal of Environmental Management 50, 403–416. doi:10.1006/jema.1997.0017

Srivastava, A., Gupta, J.P., 2010. New methodologies for security risk assessment of oil and gas industry. Process Safety and Environmental Protection 88, 407–412. doi:10.1016/j.psep.2010.06.004

Stewart, M.G., Mueller, J., 2013. Terrorism Risks and Cost-Benefit Analysis of Aviation Security. Risk Analysis 33, 893–908. doi:10.1111/j.1539-6924.2012.01905.x

Stewart, M.G., Mueller, J., 2011. Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening. Journal of Homeland Security and Emergency Management 8, 1–24. doi:10.2202/1547-7355.1837

Stewart, M.G., Mueller, J., 2008. A risk and cost-benefit assessment of United States aviation security measures. Journal of Transportation Security 1, 143–159. doi:10.1007/s12198-008-0013-0

Tappura, S., Sievänen, M., Heikkilä, J., Jussila, A., Nenonen, N., 2014. A management accounting perspective on safety. Safety Science 71, 151–159. doi:10.1016/j.ssci.2014.01.011

Toronto Municipality, 2016. False alarms fees for the city of Toronto [WWW Document]. Toronto City Website. URL http://www.toronto.ca/311/knowledgebase/88/101000045888.html (accessed 11.15.16).

Totaro, S., 2014. Disastro ambientale nel Lambro, paga solo il custode: disastro compiuto contro ignoti (in Italian) [WWW Document]. Il Giorno. URL http://www.ilgiorno.it/monza-brianza/cronaca/lambro-sentenza-1.329538 (accessed 11.15.16).

US Department of Defense, 2000. Standard Practice for System Safety. MIL-STD-882D. Wright-Patterson AFB, Ohio, USA.

Villa, V., Reniers, G.L.L., Cozzani, V., 2016. Application of cost-benefit analysis for the selection of process-industry related security measures. Chemical Engineering Transactions 53, 103–108. doi:10.3303/CET1653018

Viscusi, W.K., Aldy, J.E., 2003. The Value of a Statistical Life: A critical review of market estimates thoughout the world. Journal of Risk and Uncertainty 27, 5–76. doi:10.1023/A:1025598106257

Winfield, N., 2010a. Italy's longest river at risk after sabotage at oil depot [WWW Document]. The Independent. URL http://www.independent.co.uk/news/world/europe/italys-longest-river-at-risk-after-sabotage-at-oil-depot-1909934.html (accessed 11.15.16).

Winfield, N., 2010b. Lambro River Oil Spill May Create "Ecological Disaster" In Italy [WWW Document]. The World Post. URL http://www.huffingtonpost.com/2010/02/24/lambro-river-oil-spill-ma_n_474642.html (accessed 11.15.16).

X-Rates, 2016. Currency Calculator (US Dollar, Euro) [WWW Document]. X-Rates Website. URL http://www.x-rates.com/calculator/ (accessed 11.15.16).

Appendix A. Costs and benefit calculations

A.1 Costs calculations

Cost calculations have been carried out for each of the six PPS upgrades proposed in the case study, according to the categories, subcategories and formula proposed in Table A1, displayed below. It should be noted that many subcategories consist of wages, so realistic annual salaries have been retrieved from a specific database (PayScale, 2016) and converted into hourly wages considering $1920\ hours/year$.

Table A1 Overview on Overall annual cost estimation for a generic security measure.

Cost modelling for a generic security measure				
Cost category	**Symbol**	**Cost subcategory**	**Symbol**	**Formula**
INITIAL COSTS	$C_{INITIAL,OV}$	**Investigation costs**	C_{INV}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Selection and design costs	$C_{S\&D}$	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Material costs	$C_{MAT,I}$	$\sum_{i=1}^{s} C_{M,i} \cdot N_{M,i}$
		Training costs (start-up/in service)	C_T	$\left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_{start-up} + \left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_{service}$
		Changing of guidelines and informing costs	$C_{G\&I}$	$\sum_{i=1}^{s} C_{G\&I,i} \cdot n_i$
INSTALLATION COSTS	$C_{INSTALL,OV}$	**Start-up costs**	C_{START}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Equipment costs (including P - purchase & R - rental costs, space requirement costs)	C_E	$\left(\sum_{i=1}^{s} C_{E,i} \cdot N_{E,i}\right)_P + \left(\sum_{i=1}^{s} C_{E,i} \cdot N_{E,i}\right)_R + \sum_{i=1}^{s} C_{Space,i} \cdot V_{E,i} \cdot N_{E,i}$
		Installing costs	$C_{INSTALL}$	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
OPERATING COSTS	$C_{OPERATION,OV}$	**Utilities costs**	$C_{U,OP}$	$\sum_{i=1}^{s} C_{M,i} \cdot N_{M,i}$
		Human resources operating costs	C_{HRO}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
MAINTENANCE, INSPECTION & SUSTAINABILITY COSTS	$C_{MIS,OV}$	**Material costs**	$C_{MAT,M}$	$\sum_{i=1}^{s} C_{M,i} \cdot N_{M,i}$
		Maintenance team costs (A- scheduled m. /B- unscheduled m.)	C_{MNT}	$\left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_A + \left(\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i\right)_B$
		Inspection team costs	C_{INSP}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		License and rental renewal	C_{LIC}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
OTHER RUNNING COSTS	$C_{OR,OV}$	**Office furniture costs**	C_{OF}	$C_{U,OF} \cdot A_{office}$
		Transport costs	C_T	-
		Additional communication costs	C_{COMM}	-
		Insurance costs	C_I	-
		Office utilities costs	C_{OU}	$C_{U,OU} \cdot A_{office}$
		Office supplies costs	C_{OS}	-
SPECIFIC COSTS	$C_{SPEC,OV}$	**False-positive case costs**	$C_{FP,i}$	$C_{FA,i} \cdot P(FA)_i$
		Site-specific costs	C_{SITE_SP}	-

Key			
Symbol	**Definition**	**Symbol**	**Definition**

A_{office}	*Total office area* (m^2)	C_{COMM}	*Cost of communication (e.g., post, phones, mails, etc.)* (€)
$C_{E,i}$	*Price for unit of equipment i* $\left(\frac{€}{unit}\right)$	$C_{FA,i}$	*Cost of a single false-positive case* (€)
$C_{G\&I,i}$	*Unit cost for changing of guidelines and informing* $\left(\frac{€}{unit}\right)$	C_I	*Cost of insurance* (€)
$C_{M,i}$	*Price for unit of material i* $\left(\frac{€}{unit}\right)$	C_{OS}	*Cost of office supplies* (€)

Table A1 (continued) Overview on Overall annual cost estimation for a generic security measure.

Key			
Symbol	**Definition**	**Symbol**	**Definition**
$C_{Space,i}$	*Space requirement cost for unit of equipment i* $\left(\frac{€}{unit \cdot m^3}\right)$	C_T	*Cost of transport* (€)
$C_{U,OF}$	*Cost of office furniture per unit area* $\left(\frac{€}{m^2}\right)$	$C_{U,OU}$	*Cost of office utilities per unit area* $\left(\frac{€}{m^2}\right)$
h_i	*Number of hours of category i* (h)	$N_{E,i}$	*Amount of units for equipment i (n° units)*
n_i	*Number of employees of category i (n° people)*	$N_{M,i}$	*Amount of units for material i (n° units)*
$P(FA)_i$	*False-alarm probability (adimensional)*	s	*Number of different materials (or equipment)*
t	*Number of employee categories*	$V_{E,i}$	*Volume of equipment i* (m^3)
w_i	*Hourly wage of category i* $\left(\frac{€}{h \cdot person}\right)$		

Several data regarding cost calculation have been retrieved in US dollars of year 2016. A conversion rate from US dollars to Euro of 0.9019 $€/U.S.A.$ \$ was assumed (X-Rates, 2016). Moreover, a location factor of 1.20 (Richardson Products & Cost Data On Line Inc., 2008) was applied in order to adjust US prices and salaries to those of Italy, the location of the case study. The use of location factor throughout the analysis allowed a site-specific cost calculation. In the estimation of wages, several professional profiles, which are typically involved in the selection, design, installation and maintenance of a security system in a chemical facility, were considered. According to their different job tasks, the following security-related jobs have been accounted for the calculation of appropriate cost subcategories: purchasing office staff and manager, security manager, security engineer, security guards and officers, training expert (i.e., security consultant), masons, installation and maintenance technicians.

In the calculation of initial costs for each security upgrade, wages for the job profiles involved, costs of auxiliary materials and publications of leaflets for internal use have been considered. In the calculation of Installation costs, with particular reference to equipment costs, specific information of market prices for each security upgrade have been retrieved from vendor websites and reported in Table A2.

In the calculation of operating costs, utility costs consist of the costs of annual electric power consumption, which are significant only for upgrades A, C and E. For the three mentioned upgrades the power has been calculated through the standard power law, retrieving data on intensity and voltage from products datasheets (Alibi, 2016; Shenzhen An Ying Technology Co. Ltd., 2016) and accounting the number of devices in place, which have been assumed to be working continuously all year long. The estimated annual electric power consumption has been $5.78 \cdot 10^2$ kWh for upgrade A, $3.89 \cdot 10^3$ kWh for upgrade C and $7.78 \cdot 10^3$ kWh for upgrade E. Considering an average industrial electric energy market price in Italy of 0.175 €/kWh (Eurostat, 2016), utilities costs have been finally calculated. Human resources operating costs have been calculated by considering the manpower, in terms of security officers and guards wages for each security upgrade, which is

not negligible for upgrade A, C and E. It should be noted that for security upgrades B and D, which are walls in different positions, this subcategory is equal to zero. For upgrade F, the hiring of four additional security guards, aiming to extend the security surveillance during the night shift, has been accounted. Therefore, operating costs, prevailing over other cost categories for upgrade F, consist of security guards annual wages, hiring and training costs.

In the calculation of Maintenance, inspection and sustainability costs, the following assumptions have been made for each security upgrade: material costs were estimated assuming an annual substitution rate for equipment and other materials in the range between 3% and 5%, 2 scheduled maintenances, 1 unscheduled maintenance and 2 scheduled inspections per year have been accounted. License and renewal costs appeared to be negligible for all the six upgrades.

Table A2 Data for the calculation of Equipment costs for six different PPS upgrades.

UPGRADE ID	***DATA FOR THE CALCULATION OF EQUIPMENT COSTS***			
	Description	***Unit***	***Value***	***Reference/Notes***
A	Number of surveillance cameras at perimeter level	$n°units$	11	8% of spare items not included
	Cost of an outdoor surveillance camera	$€/unit$	195.9	Vendor website (Alibi, 2016)
B	Length and height of the concrete wall, with footings	m	1382; 3	Layout of the facility
	Cost of the wall (according to these specifications)	€	3251.76	Vendor website (Get A Quote, 2016)
C	Number of cameras for each tank	$n°units/tank$	2	-
	Cost of an outdoor camera	$€/unit$	195.9	Vendor website (Alibi, 2016)
	Total number of cameras in place	$n°units$	74	8% of spare items not included
D	Number of tanks group	$n°units$	9	Layout of the facility
	Average length and height of the concrete wall around each unit	m	800; 3	Layout of the facility
	Cost of the wall for each unit (according to these specifications)	$€/unit$	1900	Vendor website (Get A Quote, 2016)
	Cost of security doors to be applied on each unit	$€/unit$	1082	Vendor website (Grainger, 2016)
E	Number of alarm per valve	$n°units/valve$	1	-
	Cost of an industrial alarm	$€/unit$	117.4	Vendor website (Shenzhen An Ying Technology Co. Ltd., 2016)
	Number of alarms	$n°units$	37	8% of spare items not included
	Number of cages per pump	$n°units/pump$	1	-
	Cost of a metallic cage for pump with lock	$€/unit$	18.4	-
	Number of pumps	$n°units$	37	-
F	Unit cost for the new building (standard warehouse with concrete floor and metal clad)	$€/m^2$	582.3	Vendor website (BMT, 2016)

	Area of the building	m^2	70	Layout of the facility

Other running costs have been calculated for each security upgrade; only for upgrade F this cost category has a significant role, provided that the construction of a new building for security guards requires additional office furniture and utilities.

In the calculation of Specific costs, the contribution offered by false-positive costs should be considered only for detection elements (i.e., upgrade A, C and E). For these upgrades, a single false-alarm cost has been assumed, based on expert judgement, $2.80 \cdot 10^3$ € (Toronto Municipality, 2016) and $P(alarm \mid no\ attack)_i = 0.143$ (Garcia, 2007). According to the considerations expressed in Section 2.4, false-positive costs depend on the assumption regarding the probability of the attack. Assuming the probability of the attack equal to one turns false-positive costs to zero, leading to the minimum value of specific costs value. Consequently, assuming the probability of the attack equal to zero, leads to the maximum value of specific costs. Site-specific costs, as revisions of safety measures and procedures, have been accounted in particular for delay elements, whose implementation might require a revision of emergency routes, as well as entrance doors and exit doors. Therefore, specific costs are represented by a range of values only for detection elements (i.e., upgrades A, C and E), in turn determining a range of values for Overall costs. Nevertheless, in case of a narrow range of values for overall costs, as in the case study, this dependence might be neglected.

For each of the six security upgrades, the main results obtained from cost calculations, according to the six cost categories of ECO-SECURE, as well as the Overall costs ($C_{Security,i}$) have been illustrated in Table A3.

Table A3 Calculation of Overall costs for six security upgrades, as the sum of six main categories: 1) Overall initial costs, 2) Overall installation costs, 3) Overall operating costs, 4) Overall maintenance, inspection & sustainability costs, 5) Other running costs, 6) Overall specific cost. For detection upgrades (i.e., upgrades A, C, E) Overall specific costs, and consequently Overall costs, depend on the assumption regarding the probability of the attack. Setting $P(T)_{ij} = 1$ leads to the minimum value of specific costs and consequently to the minimum value of Overall costs for a generic security measure. Setting $P(T)_{ij} = 0$ leads to the maximum value of specific costs and consequently to the maximum value of Overall costs for a generic security measure.

CALCULATION OF OVERALL COSTS ($C_{Security,i}$)			**UPGRADE A**	**UPGRADE B**	**UPGRADE C**	**UPGRADE D**	**UPGRADE E**	**UPGRADE F**
Symbol	***Description***	***Unit***	***Value***	***Value***	***Value***	***Value***	***Value***	***Value***
$C_{INITIAL,OV}$	***1. Overall initial costs***	**€**	3.53E+03	1.57E+03	3.53E+03	1.57E+03	4.41E+03	4.49E+03
$C_{INSTALL,OV}$	***2. Overall installation costs***	**€**	4.17E+03	7.10E+03	1.92E+04	3.11E+04	7.87E+03	5.71E+04
$C_{OPERATION,OV}$	***3. Overall operating costs***	**€**	1.01E+03	0	7.99E+03	0	5.01E+03	1.70E+05
$C_{MIS,OV}$	***4. Overall maintenance, inspection & sustainability costs***	**€**	1.98E+03	1.05E+03	2.69E+03	2.18E+03	2.62E+03	2.79E+03
$C_{OR,OV}$	***5. Other running costs***	**€**	1.80E+02	2.80E+02	1.80E+02	2.80E+02	2.80E+02	2.43E+04
$C_{SPEC,OV}$	***6. Overall specific costs***	**€**	3.00E+02 ÷ 7.00 E+02	1.00E+03	4.00E+02 ÷ 8.00 E+02	8.00E+02	8.00E+02 ÷ 1.20 E+03	1.00E+03
$C_{Security,\ i}$	***Overall costs***	**€**	**1.12E+04 ÷ 1.16E+04**	**1.10E+04**	**3.39E+04 ÷ 3.43E+04**	**3.60E+04**	**2.10E+04 ÷ 2.14E+04**	**2.60E+05**

A.2 Benefit calculations

Benefit calculations have been carried with respect to the actual scenario considered in the case study, according to the categories, subcategories and formula proposed in Table A4, displayed below.

Table A4 Overview on Overall annual benefits estimation for a generic accidental scenario, with focus on environmental benefits.

Benefit modelling for a generic scenario				
Benefit category	**Symbol**	**Benefit subcategory**	**Symbol**	**Expression**
SUPPLY CHAIN	$B_{SUPC,OV}$	**Production loss benefits**	B_{PL}	$Q \cdot t_{PS} \cdot Pr_U$

BENEFITS		**Start-up benefits**	B_{START}	$(Q - Q^*) \cdot t_D \cdot Pr_U$
		Schedule benefits	B_{SCH}	$(F_{canc} \cdot n_{canc}) + (F_d \cdot n_d \cdot d) + \left(n_{con} \cdot (C_{con} - C_{in\_h})\right)$
DAMAGE BENEFITS	$B_{DMG,OV}$	**Damage to own material/property**	$B_{D,OM\&P}$	$A + B + C$
		Damage to other companies material/property	$B_{D,OCM\&P}$	$D + E + F$
		Damage to surrounding living area	$B_{D,SA}$	G
		Damage to public material/property	$B_{D,PM\&P}$	$H + I + J$

Table A4 (continued) Overview on Overall benefits estimation for a generic accidental scenario, with focus on environmental benefits.

Benefit modelling for a generic scenario				
Benefit category	**Symbol**	**Benefit subcategory**	**Symbol**	**Expression**
LEGAL & INSURANCE BENEFITS	$B_{LGL\&INS,OV}$	**Fines-related benefits**	B_{FINES}	$K + L + M$
		Interim lawyers benefits	B_{ILAW}	$w_{SL} \cdot n_{SL} \cdot d_{SL} + w_{JL} \cdot n_{JL} \cdot d_{JL}$
		Specialized lawyer benefits	B_{SLAW}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Internal research team benefits	B_{IREST}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Expert at hearings benefits	B_{EH}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Legislation benefits	B_{LEG}	$S_B \cdot I_{SB}$
		Permit and license benefits	$B_{P\&LIC}$	$C_{CD} \cdot L_P$
		Insurance premium benefits	B_{INS}	$P_F \cdot I_{PF}$
HUMAN BENEFITS	$B_{H,OV}$	**Compensation victims benefits**	$B_{H,CF}$	$VSL \cdot n_F$
		Injured employees benefits	$B_{H,IE}$	$C_{LI} \cdot n_{LI} + C_{SI} \cdot n_{SI}$
		Recruit benefits	$B_{H,RECR}$	$\sum_{i=1}^{t} (C_{H,i} + C_{T,i}) \cdot n_i$
ENVIRONMENTAL BENEFITS	$B_{ENV,OV}$	**External intervention benefits (salaries related to emergency interventions / materials / post-accident monitoring / others)**	$B_{E,INTV}$	$\sum_{i=1}^{z} C_{S,i} + \sum_{i=1}^{s} C_{ME,i} \cdot N_{ME,i} + \sum_{i=1}^{v} C_{MONIT,i} \cdot N_{MONIT,i} + C_{OTH,INTV}$
		Internal intervention benefits (manager work-time benefits/ cleaning benefits)	$B_{I,INTV}$	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i + (w_c \cdot h_c \cdot n_c)$
		Environmental remediation benefits (short-term / long-term)	B_{REM}	$\left(\sum_{i=1}^{y} m_{SP,i} \cdot C_{SP,i}\right) + C_{REM,LT}$
		Other environmental benefits	$B_{OTH,ENV}$	-
REPUTATION BENEFITS	$B_{REPT,OV}$	**Share price benefits**	B_{SP}	$M_{REP} \cdot D_{REP}$
SPECIFIC BENEFITS	$B_{SPEC,OV}$	**Site-specific benefits**	B_{SITE_SP}	-
		Immaterial benefits	B_{IMM}	-

Key

Symbol	**Definition**	**Symbol**	**Definition**
A	*Damage to the company equipment and machines* (€)	B	*Damage to the company buildings and other infrastructures* (€)
C	*Damage to the company raw materials and finished goods* (€)	C_{CD}	*Cost due to facility close-down* (€)
C_{con}	*Cost per unit asked by the contractor* $\left(\frac{€}{unit}\right)$	$C_{H,i}$	*Hiring cost per employee of category i* $\left(\frac{€}{person}\right)$
C_{in_h}	*In-house cost per unit* $\left(\frac{€}{unit}\right)$	C_{LI}	*Cost of one light injured worker* $\left(\frac{€}{person}\right)$
$C_{ME,i}$	*Unit cost for material i applied during emergency intervention* $\left(\frac{€}{unit}\right)$	$C_{MONIT,i}$	*Unit cost of monitoring action type i* $\left(\frac{€}{unit}\right)$
$C_{OTH,INTV}$	*Other environmental costs* (€)	$C_{REM,LT}$	*Long-term remediation costs* (€)
C_{SI}	*Cost of one serious injured worker* $\left(\frac{€}{person}\right)$	$C_{S,i}$	*Intervention cost from organization/emergency*

			service i charged to the company (€)
$C_{SP,i}$	*Cost per unit of product i spilled* $\left(\frac{€}{kg}\right)$ *or* $\left(\frac{€}{m^3}\right)$	$C_{T,i}$	*Training cost per employee of category i* $\left(\frac{€}{person}\right)$
D	*Damage to other companies equipment and machines* (€)	d	*N° days of tardiness in the orders* $(n°days)$
d_{JL}	*Number of work days per junior lawyers* $(n°\ days)$	D_{REP}	*Expected drop in the share price* (%)
d_{SL}	*Number of work days per senior lawyers* $(n°\ days)$	E	*Damage to other companies buildings and other infrastructures* (€)
F	*Damage to other companies raw materials and finished goods* (€)	F_{canc}	*Fine for a cancelled order/contract* $\left(\frac{€}{contract}\right)$
F_d	*Fine for delays in deliveries per day* $\left(\frac{€}{delay \cdot day}\right)$	G	*Damage to surrounding living area* (€)
H	*Damage to public equipment and public machines* (€)	h_c	*Number of hours worked by a cleaning employee* (h)
h_i	*Number of hours of category i* (h)	I	*Damage to public buildings and other public infrastructure* (€)

Table A4 (continued) Overview on Overall benefits estimation for a generic accidental scenario, with focus on environmental benefits.

Key			
Symbol	**Definition**	**Symbol**	**Definition**
I_{PF}	*Expected increase of the premium* (%)	I_{SB}	*Increase of the security budget for the facility after major accident occurrence* (%)
J	*Damage to public materials and public goods* (€)	K	*Civil liability fines* (€)
L	*Criminal liability fines* (€)	L_P	*Likelihood of losing operating permit* (%)
M	*Administrative liability fines* (€)	M_{REP}	*Current total market value of the company* (€)
$m_{SP,i}$	*Amount of product i spilled* (kg) *or* (m^3)	n_c	*Number of cleaning employees (n° cleaning employees)*
n_{canc}	*N° of orders/contracts cancelled* $(n°contracts)$	n_{con}	*N° of units given by the contractor* $(n°units)$
n_d	*N° of orders with a delay* $(n°delay)$	n_F	*Number of fatalities* $(n°\ people)$
n_i	*Number of employees of category i (n° people)*	n_{JL}	*Number of junior lawyers* $(n°\ lawyers)$
n_{LI}	*Number of light injured workers* $(n°\ people)$	$N_{ME,i}$	*Amount of units of material i applied during emergency intervention (n° units)*
$N_{MONIT,i}$	*Number of monitoring actions type i (n° units)*	n_{SI}	*Number of serious injured workers* $(n°\ people)$
n_{SL}	*Number of senior lawyers* $(n°\ lawyers)$	P_F	*Current total premium cost of the facility* (€)
Pr_U	*Profit per unit sold* $\left(\frac{€}{unit}\right)$	Q	*Production rate of the factory* $\left(\frac{n°units}{h}\right)$
Q^*	*Production rate of the factory at the start of line reactivation* $\left(\frac{n°units}{h}\right)$	s	*Number of emergency materials applied during emergency intervention*
S_B	*Total security budget of the facility* (€)	t	*Number of employees categories*
t_D	*Duration of reduced production during reactivation* (h)	t_{PS}	*Duration of the stop in production* (h)
v	*Number of monitoring actions categories*	VSL	*Value of a statistical life* $\left(\frac{€}{person}\right)$
w_c	*Hourly wage of a cleaning employee* $\left(\frac{€}{h \cdot person}\right)$	w_i	*Hourly wage of category i* $\left(\frac{€}{h \cdot person}\right)$
w_{JL}	*Hourly wage of junior lawyers* $\left(\frac{€}{day \cdot lawyer}\right)$	w_{SL}	*Hourly wage of senior lawyers* $\left(\frac{€}{day \cdot lawyer}\right)$
y	*Number of products spilled*	z	*Number of organizations/emergency services involved*

In the calculation of Supply chain benefits, production losses and start-up losses have been neglected because the facility is an oil depot, not a production facility (e.g., a refinery). A flat rate for Schedule benefits has been retrieved (Galvani, 2015); details are available in Table A6.

In the calculation of Damage benefits, illustrative commercial equipment costs for the pumps damaged have been retrieved from vendors; details on the calculations are reported in Table A5. The values of damages to company infrastructures and surrounding living areas (e.g., canals, private properties) have been reported in Table A6. The estimation of damages to public infrastructures, as the water treatment system of the nearby city is presented in the same table. Regarding the evaluation of finished goods damages, average market prices have been assumed for both the products (i.e., diesel and heating oil); details on calculations are reported in Table A5.

In the calculation of Legal & insurance benefits and after, it should be noted that, as for costs calculations, many benefits subcategories consist of wages. The same data displayed in Appendix A.1, regarding the conversion rate from US dollars to € and the location factor have been applied. In the case of Legal & insurance benefits, the job profiles involved are junior lawyers and seniors lawyers, specialized lawyers, security manager, security engineer, security analyst and security consultant. Details on the data applied for the calculation of Legal & insurance benefit subcategories are available in Table A5. No human losses and injuries have been sustained in the actual accident; however, data regarding the calculation of Human benefits, as the value of a statistical life (VSL) and compensation costs for injuries might have been retrieved from previous studies (Paltrinieri et al., 2012; Viscusi and Aldy, 2003). Hiring benefits are inserted in Human benefits category as they refer to the costs that should be sustained by the company when an employee is hospitalized or dead after the accident to hire additional personnel in substitution. Therefore, no hiring benefits have been sustained in the actual accident. Data regarding their calculation may be retrieved from previous studies (Gavious et al., 2009; Reniers and Brijs, 2014a); it is suggested to consider hiring and training costs equivalent to a monthly salary each for the employee category.

In the calculation of Environmental benefits, flat rates for external and internal intervention costs have been reported in Table A6. Environmental remediation costs have been estimated according to the data reported in Table A5. A flat rate for other environmental damages to the surrounding ecosystem (i.e., plants and animals) is available in Table A6.

The data for the calculation of Reputation benefits are available in Table A5. The expected percentage drop of market price regarding a major oil spill has been assumed, with a value of 31% (Goossens, 2012). This data was confirmed in a long-term time perspective, which is the time span required for benefit calculations, by a recent study (Neilan, 2016). In the calculation of Specific benefits, collateral damages, due to voluntary spills in the river from nearby facilities subsequent to the major accident (Querzé, 2010), have been reported in Table A6.

Table A5 Data for the calculation of benefit subcategories with respect to the actual scenario.

BENEFIT CATEGORY	**BENEFIT SUBCATEGORY SYMBOL**	***DATA FOR THE CALCULATION OF BENEFIT SUBCATEGORIES***				
		Symbol	***Description***	***Unit***	***Value***	***Reference/Notes***
DAMAGE BENEFITS	$B_{D,OM\&P}$	A	*Damage to the company equipment and machines*	€	1.19E+04	Damage to 4 pumps; average unit cost for a pump assumed 2.98E+03 € from vendors and validated by expert judgement
		B	*Damage to the company buildings and other infrastructures*	€	5.00E+03	Limited damages to piping/surrounding infrastructures (EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement
		C	*Damage to the company raw materials and finished goods*	€	6.52E+05	Spill of diesel and heavy oil. Inventories of spilled diesel and heavy oil available in Section 3.1. Average market prices assumed for diesel and heavy oil (i.e., respectively 280 $€/m^3$ and 95 $€/m^3$)
LEGAL & INSURANCE BENEFITS	B_{ILAW}	K	*Civil liability fines*	€	6.89E+06	Civil liability fines as expressed by prosecutors (Totaro, 2014)
		M	*Administrative liability fines*	€	8.90E+05	Taxation on spilled products (Galvani, 2015)
	B_{LEG}	S_B	*Total security budget of the facility*	€	1.00E+04	Severe security deficiencies highlighted by accident report (EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement
		I_{SB}	*Increase of the security budget for the facility after accident occurrence*	%	17.00	Scenario dependent value, based on expert judgement, to reach usual budget values reported by (Reniers and Van Erp, 2016)
	$B_{P\&LIC}$	C_{CD}	*Cost due to facility close-down*	€	1.20E+08	Data retrieved from (Berni and Rosa, 2015)
		L_P	*Likelihood of losing operating permit* (%)	%	10.00	Likely closing-down of the facility after the accident (Berni and Rosa, 2015) – quantification based on expert judgement
	B_{INS}	P_F	*Current total premium cost of the facility*	€	5.00E+07	Premium based on possible value of the facility after partial sale, as declared by company owner (Pecorella, 2011)

		I_{PF}	*Expected increase of the premium*	%	1.00	Expert judgement
ENVIRONMENTAL BENEFITS	B_{REM}	$m_{SP,i}$	*Amount of product spilled* (kg) *or* (m^3)	kg	2.60E+06	Inventory of spilled hydrocarbons products available in Section 3.1
		$C_{SP,i}$	*Cost per unit of product i spilled* $\left(\frac{€}{kg}\right)$ *or* $\left(\frac{€}{m^3}\right)$	€	1.44	Unit remediation cost for liquid hydrocarbon spills retrieved from a previous study (Etkin, 1999), converted and actualized to $(€(2016))$
		$C_{REM,LT}$	*Long-term remediation costs*	€	2.00E+07	Long-term remediation costs for the site retrieved from (Berni and Rosa, 2015)
REPUTATION BENEFITS	B_{SP}	M_{REP}	*Current total market value of the company*	€	6.00E+07	Current total market price for the company based on (Pecorella, 2011)
		D_{REP}	*Expected drop in the share price*	%	31	Expected long-time percentage drop of market price regarding a major oil spill (Goossens, 2012)

The data reported in Table A5 and A6, applied for the calculation of benefit categories and subcategories, were retrieved from a collection of references and validated by a panel of security managers and academic security experts. Eventually, all the benefit numerical values have been determined accordingly to the pertinent categories and subcategories of the approach, allowing the calculation of the Overall benefits $(C_{Loss,j})$, for the actual scenario (Table A6). A discussion on losses apportionment is available in Section 3.4.

Table A6 Overall benefits results for realistic scenario. The calculation of Overall benefits has been carried out as the sum of seven main categories: (1) Overall supply chain benefits, (2) Overall damage benefits, (3) Overall legal & insurance benefits, (4) Overall human benefits, (5) Overall environmental benefits, (6) Overall reputation benefits, (7) Overall specific benefits. Intermediate calculations regarding benefit subcategories are reported, together with assumptions made.

CALCULATION OF OVERALL BENEFITS $(C_{Loss,j})$				
Symbol	***Category/ subcategory description***	***Unit***	***Value***	***Assumptions***
$B_{SUPC,OV}$	***1. Overall supply chain benefits***	**€**	**1.70E+06**	**See assumptions for subcategories**
B_{PL}	*Production loss benefits*	€	0	No stop in production, it is an oil depot
B_{START}	*Start-up benefits*	€	0	No start-up benefits, it is not a production facility
B_{SCH}	*Schedule benefits*	€	1.70E+06	Costumers refunding – flat rate retrieved from reference (Galvani, 2015)
$B_{DMG,OV}$	***2. Overall damage benefits***	**€**	**2.29E+06**	**See assumptions for subcategories**
$B_{D,OM\&P}$	*Damage to own material/property*	€	6.69E+05	Limited damages to equipment and machines – calculated according to data in Table A5; limited damages to piping/surrounding infrastructures – calculated according to data in Table A5; damage to finished goods (e.g., diesel and heavy oil) - calculated according to data in Table A5
$B_{D,OCM\&P}$	*Damage to other companies material/property*	€	2.00E+04	Very limited damages to other companies materials/properties (EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement, assuming 1.00E+04 € of damages each for 2 boundary facilities
$B_{D,SA}$	*Damage to surrounding living area*	€	1.00E+05	Damage to private properties/canals (ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010; EMARS - Major accidents reporting system, 2010) – quantification based on expert judgement, assuming 5.00E+03 € of damages for 20 householders in the surrounding densely inhabited area
$B_{D,PM\&P}$	*Damage to public material/property*	€	1.50E+06	Damages to the water treatment system of the nearby city (Pecorella, 2011)
$B_{LGL\&INS,OV}$	***3. Overall legal & insurance benefits***	**€**	**2.05E+07**	**See assumptions for subcategories**
B_{FINES}	*Fines-related benefits*	€	7.78E+06	Civil liability fines and taxation of spilled products – calculated according to data in Table A5; no criminal liability fines – based on expert judgement
B_{ILAW}	*Interim lawyers benefits*	€	1.31E+04	Senior and junior lawyers' wages – calculated according to (PayScale, 2016)
B_{SLAW}	*Specialized lawyer benefits*	€	6.28E+02	Specialized lawyers' wages – calculated according to (PayScale, 2016)
B_{IREST}	*Internal research team benefits*	€	2.91E+03	Security manager, security engineer and security analysts' wages – calculated according to (PayScale, 2016)
B_{EH}	*Expert at hearings benefits*	€	6.14E+02	Security consultant's wage – calculated according to (PayScale, 2016)
B_{LEG}	*Legislation benefits*	€	1.70E+05	Increase of security budget after the accident – calculated according to data in Table A5
$B_{P\&LIC}$	*Permit and license benefits*	€	1.20E+07	Calculated according to data in Table A5
B_{INS}	*Insurance premium benefits*	€	5.00E+05	Calculated according to data in Table A5
$B_{H,OV}$	***4. Overall human benefits***	**€**	**0**	**No human losses and injuries** (EMARS - Major accidents reporting system, 2010)**, no recruit benefits**
$B_{ENV,OV}$	***5. Overall environmental benefits***	**€**	**3.80E+07**	**See assumptions for subcategories**
$B_{E,INTV}$	*External intervention benefits*	€	1.20E+07	Overall external intervention benefits – flat rate retrieved from bulletin

	(salaries related to emergency interventions / materials / post-accident monitoring / others)			released by Italian environmental protection agency (ARPA - Agenzia Regionale Prevenzione Ambiente dell'Emilia-Romagna, 2010)
$B_{I,INTV}$	*Internal intervention benefits (manager work-time benefits/ cleaning benefits)*	€	1.55E+06	Overall internal intervention benefits – flat rate based on an interview to the company owner (Galvani, 2015)
B_{REM}	*Environmental remediation benefits (short-term / long-term)*	€	2.37E+07	Environmental remediation for hydrocarbons spill and cost of requalification project for the site – calculated according to data in Table A5
$B_{OTH,ENV}$	*Other environmental benefits*	€	7.00E+05	Damages to the ecosystem close to the river (Franceschi, 2010)
$\boldsymbol{B_{REPT,OV}}$	***6. Overall reputation benefits***	**€**	**1.86E+07**	**Expected long-term drop in market price - calculated according to data in Table A5**
$\boldsymbol{B_{SPEC,OV}}$	***7. Overall specific benefits***	**€**	**5.01E+05**	**See assumptions for subcategories**
B_{SITE_SP}	*Site-specific benefits*	€	5.00E+05	Collateral damages, due to voluntary spills in the river from nearby facilities subsequent to the major accident (Querzé, 2010) – quantification based on expert judgement, considering 1% of overall environmental benefits
B_{IMM}	*Immaterial benefits*	€	5.00E+02	Post-accident psychological meeting for employees (12 hours) – Salary of psychologist retrieved from (PayScale, 2016).
$\boldsymbol{C_{Loss,j}}$	***Overall benefits***	**€**	**8.16E+07**	-