Development of an Economic Model for Counter Terrorism Measures in the Process-Industry

Submitted for publication in: Journal of Loss Prevention in the Process Industries

Revised version

Abstract

In the last few years, several events have highlighted the risk of possible major accidents triggered by terrorist attacks within chemical and process facilities. Due to the increased attention for security issues, an optimal allocation of security measures, including related cost issues, becomes progressively more important. Despite the existence of economic models for supporting decision-making processes in general, for instance cost-benefit and cost-effectiveness analyses, no specific economic models are available in the domain of operational security (including counter-terrorism decision-making) to be applied within the chemical and process industry. In this study, a novel method for cost-benefit and cost-effectiveness analysis for the allocation of physical security measures was elaborated and tested using a case study. Starting from a site-specific analysis of the baseline physical security system performance, the model allows comparing and evaluating the costs of different security upgrades with the (hypothetical) benefits related to the avoided losses. The approach developed enables selecting economically feasible security measures, or a combination of such measures with a maximum net present value, within the budget constraints of a chemical plant.

Keywords

SECURITY COST-BENEFIT ANALYSIS; SECURITY COST-EFFECTIVENESS ANALYSIS; CHEMICAL INDUSTRY; PROCESS INDUSTRY; SECURITY DECISION-MAKING

1 Introduction

Many categories of critical infrastructures (Moteff, 2005) can be attractive targets for deliberate attacks, such as airports, power plants, road and maritime means of transportation. Chemical (and process) fixed installations were recognized several years ago by CCPS (CCPS - Center for Chemical Process Safety, 2003, 2008) (amongst others) as attractive targets for potential intentional malevolent acts, such as terroristic attacks and sabotage. Due to the high inventory of hazardous chemicals and possibly severe operating conditions, the potential consequences of these events, in terms of disruption of operations, destruction of property, injury and/or loss of life, are severe and include the possibility of cascading effects (Landucci, Reniers, Cozzani, & Salzano, 2015; Nolan, 2008). For instance, in 2015, two security-related accidents, possibly terroristic attacks, took place in France: an attack to a warehouse of explosive chemicals in a gas production factory on June 26th, 2015 (BBC News, 2015a) and the sabotage, with consequent explosions, of two storage tanks in an oil refinery on July 14th, 2015 (Le Guernigou & Revilla, 2015). Investigations, which are still underway, consider the intentional nature of both events and two suspects have been arrested, one for each of them; crime and terrorism are thus deemed as possible motivations (Associated Press, 2015; BBC News, 2015a; Pardini, 2016). These two security-based accidents are just the latest ones of a long series; as reported by the ARIA governmental agency, only in France, 850 malicious acts have been perpetrated within industrial facilities, mainly chemical industrial sites, in the period 1992-2015 (ARIA, 2015). Despite the growing attention towards counter-terrorism issues in the chemical and process industry, at a European Union level only a general Directive on how to prevent, prepare and respond to terrorist attacks related to critical infrastructures (The Council of the European Union, 2008) was issued. No detailed guidelines for security management of chemical enterprises currently exist. Instead, in the United States, following the 9/11 attack, a specific regulation named CFATS (i.e., Chemical Facility Anti-Terrorism Standards) has become effective since 2007, and applied to all the facilities classified by US Department of Homeland Security as “high-risk” (DHS - US Department of Homeland Security, 2007).

According to Reniers and Audenaert (Reniers & Audenaert, 2014), security can be defined as the state of being protected against potential danger or loss that can result from the deliberate, malicious, and unlawful acts of others. Security risks assume threats, vulnerabilities and consequences as main components. Security risk assessment within chemical plants is a systematic approach to collect and organize information regarding (Bajpai & Gupta, 2007; CCPS - Center for Chemical Process Safety, 2003; Reniers, Van Lerberghe, & Van Gulijk, 2015):

- Site-specific assets (i.e., people, properties, infrastructures, reputation and information) that need to be protected;
- Threats that may be posed against those assets;
- Probabilities and consequences of malevolent attacks against them.

The result of a security risk assessment is a number of consequent actions planning and tracking on the threats tackled by the analysis. Many authors (Aven, 2007; Reniers, 2014; Reniers & Audenaert, 2014) suggested a unified framework for safety and security risk assessment. Considering risk as the effect of uncertainties on objectives (ISO31000:2009, 2009), the key different element between the two domains is the risk source, that in the safety domain can be considered unintentional, while in the security domain it is the result of a specific intent. Security risk sources can be several: individuals, business competitors, intelligence organization, terrorists, and criminals. All may behave according to different motivations, varying from personal to political, religious, economic and business advantage. Moreover, for security-based events, as terroristic attacks, only qualitative probabilities of occurrence may be available (e.g., low, medium, high) (Broder & Tucker, 2012; Garcia, 2005), while quantitative probabilities and frequencies of safety related events are generally available on databases (TNO, 2005).

In the past decades, cost-benefit analyses and the specific features of its application to the safety domain were explored (Gavious, Mizrahi, Shani, & Minchuk, 2009; Martinez & Lambert, 2012; Paltrinieri, Bonvicini, Spadoni, & Cozzani, 2012). Ongoing research within the chemical industry addresses economic assessment for safety decision-making (Janssens, Talarico, Reniers, & Sörensen, 2015; Khakzad & Reniers, 2015; Reniers & Brijs, 2014a, 2014b). However, no economic model for the allocation of counter terrorism related measures to be used within the chemical industry has yet been developed.

In the present study, a novel model for cost-benefit and cost-effectiveness analysis of security measures was elaborated. It is named EM-PICTURES (Economic Model for Process-Industry related Counter Terrorism measURES) and is specifically aimed at chemical and process industries. The model, starting from the analysis of the baseline physical security system, allows proposing security upgrades and accounting both the performance improvement and the costs derived from their implementation. The model also includes the evaluation of benefits, considering avoided losses for different pertinent hypothetical scenarios. EM-PICTURES enables the comparison among different security upgrades and guides the choice of those that are economically feasible, as well as the determination of the combination that allows the maximum profit. 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 industries. In order to better understand the potentiality and results of the approach developed, EM-PICTURES was applied to an illustrative case study, based on a possible security-related event that took place in France.

2 Model description

2.1 General layout of the model

The EM-PICTURES general layout is shown in Fig. 1. The model includes six sub-modules. Modules from (1) to (4) include all the inputs, while modules (5) and (6) are dedicated to economic analysis:

1. Starting from available information on previous security issues, module (1) is aimed at defining $P(T)$, which represents the threat probability (e.g., the probability of attack) referred to a chemical installation. In this module also the vulnerability probabilities, expressing the conditional hazard and loss probabilities, are defined.
2. Module (2) is aimed at evaluating the overall effectiveness improvement ($\overline{\Delta\eta_i}$) achieved by implementing an additional security countermeasure i to the baseline Physical Protection System (i.e., PPS). It provides the degree to which the security measure foils, deters, disrupts or protects against a threat.
3. Module (3) is aimed at quantifying $C_{Security,i}$, which indicates the overall costs of a specific security measure i. This term includes direct and indirect economic costs of applying a security device.
4. Module (4) defines the overall losses or consequences of either perspective or retrospective accidental scenarios (i.e., $C_{Loss,j}$), expressed in monetary values, and indicated in the following section also as "overall benefits".
5. Module (5) allows defining, by means of cost-benefit analysis (i.e., CBA), the single security measures that are economically feasible for a specific reference scenario.
6. Module (6) provides, by means of cost-effectiveness analysis (i.e., CEA), the most profitable combination of security measures with reference to a specific scenario.

The output of the model is a set of cost-benefit and cost-effectiveness indicators that can support the security decision-making process. The content and procedures applied in the single modules will be explained in detail in the following.

2.2 Module 1: threat and vulnerabilities

Module (1) is aimed at defining the threat probability and vulnerability probabilities to be applied in the analysis. The threat probability ($P(T)$) 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 judgment, as well as on available intelligence, law enforcement and open source information. However, the probability of terroristic attacks on chemical installation is context-sensitive and therefore it may vary significantly over time, depending on social and political phenomena (European Commission, 2008). As stated by Stewart and Mueller (Stewart & Mueller, 2013), assessing the probability of terrorist acts is a challenging task, because terrorism is a phenomenon of multi-causal factors and terrorists deliberate effort to defy prediction. The complexity of terrorism combined with the unique attributes of individual groups makes it nearly impossible to capture the explanatory characteristics of the phenomenon in a single variable (i.e., the probability of the attack) (European Commission, 2008). However, in the present model a deterministic approach is applied to toward the estimation of threat probability. It implies to assume a defined value of $P(T)$ within the range $[0,1]$, which is considered an input of the economic analysis. A possible guidance in the choice of the threat probability, adapted from Stewart and Mueller (Stewart & Mueller, 2012) has been reported in Table 1.

As suggested by Garcia (Garcia, 2005), in case of unacceptably high consequences (i.e., possibility of cascading effects, national security at stake), a conditional threat approach may be applied: it implies to consider $P(T) = 1$. 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. As an alternative to the deterministic approach, following a break-even approach (Stewart & Mueller, 2012), the model can be applied in a reversed form, where the output of cost-benefit analysis is the minimum threat probability required for the benefits specific scenario j to equal the costs of a security measure i. Indeed, the threat probability is calculated after module (2), (3) and (4). Module (1) of EM-PICTURES is aimed at defining also the vulnerability probabilities, which are $P(H \mid T)$ and $P(L \mid H)$. $P(H \mid T)$ is the conditional probability of a hazard that indicates an initiating event leading to damage and loss of life, which can be expressed as follows (Stewart & Mueller, 2012):

$$P(H \mid T) = PSF \cdot R_{IED} \quad (1)$$

Where R_{IED} expresses the reliability of the device, which is often an improvised explosive device (i.e., IED) (Landucci et al., 2015); the Performance Shaping Factors (i.e., PSF) represents the performance of adversaries in the use of the device, depending on its complexity, on adversary skills and location. $P(H \mid T)$ guidance global data referred to terroristic organizations have been reported in Table 1; more detailed information regarding specific geographical areas and other typologies of adversaries (e.g., insurgent organization, criminals) can be found elsewhere (Stewart & Mueller, 2012).

$P(L \mid H)$ is the conditional probability of loss or consequences (e.g., having at least asset damages), given the occurrence of a hazard; guidance values have been reported in Table 1.

Threat severity	**Example of adversaries and malicious act**	$\boldsymbol{P(T)}$	$\boldsymbol{P(L \mid H)}$
Low	Individual stealing asset/ vandals	0.6	0.25
Medium	Organized criminals stealing assets/ weak sabotage action	0.3	0.80
High	Terrorists aimed at causing a major accident	0.1	1
Conditional threat	Terrorists aimed at causing cascading effects	1	1
$\boldsymbol{P(H \mid T)}$			
Reliability of Improvised Explosives Devices			
Device complexity	**Representative IED design**		$\boldsymbol{R_{IED}}$
Simple	Pipe bomb		0.931
Medium	Mobile phone initiated VBIED (Vehicle Borne Improvised Explosive Device)		0.920
Complex	Improvised mortar		0.910
Conservative assumption	No information available		1
Global Performance Shaping Factors			
Organizational culture	**Device complexity**		$\boldsymbol{PSF}$
Terrorist organization	Simple		0.981
	Medium		0.980
	Complex		0.905
	No information available		1

Table 1. Guidance values for the estimation of threat and vulnerability probabilities, retrieved from (Garcia, 2005; Stewart & Mueller, 2012).

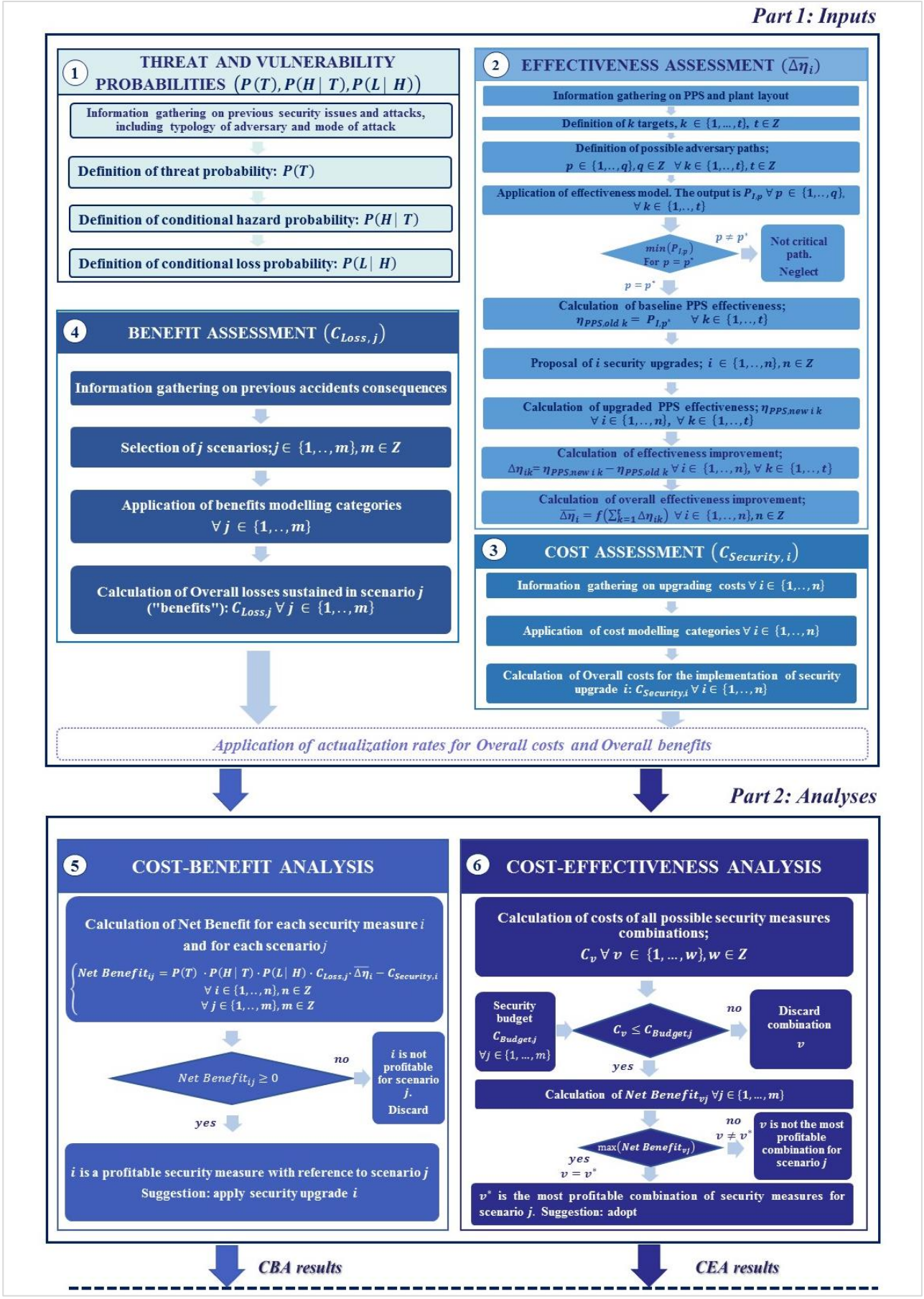

Fig. 1. General layout of EM-PICTURES. The model is composed by six sub-modules: (1) Threat and vulnerability probabilities, (2) Effectiveness assessment, (3) Cost assessment, (4) Benefit assessment, (5) Cost-benefit analysis and (6) Cost-effectiveness analysis.

2.3 Module 2: effectiveness assessment

Module (2) of EM-PICTURES is aimed at assessing the baseline physical protection system performance by site-specific analysis, proposing security upgrades and determining the overall effectiveness improvement due to each security measure i, $\overline{\Delta\eta_i}$.

Physical Protection Systems (i.e., PPS) have a crucial role in providing adequate security protection. A physical protection system is an integration of protection components and elements that can include people, procedures and equipment for the protection of assets or facilities against security threats, as theft, sabotage or other malevolent human attacks (Garcia, 2005, 2007). The selection, design and upgrade of PPS, often indicated as security barriers or security measures, require a methodological approach in which the objectives of the PPS are weighted against available resources and it eventually turns into a proposed design, that may be evaluated and subsequently further optimized in order to improve its performance (Garcia, 2007). Generally, the PPS design and implementation should address the systematic and integrated protection of assets in anticipation of adversary attacks rather than in reaction of attack occurrence. It should also achieve the protection objectives with respect to operational, safety, legal and economic constraints of the facility (CCPS - Center for Chemical Process Safety, 2003). However, the occurrence of an attack may offer the occasion to tackle the weakness of PPS and consequently upgrade the security measures present in the facility. The classification of PPS is generally carried out in three main categories accordingly to the function they serve and the elements that compose a security system (Garcia, 2005, 2007): detection of an adversary, delay of that adversary and response by security personnel. Indeed, for the system to be effective in protecting critical assets from theft or sabotage by a malevolent adversary, there must be notification of an attack (i.e., detection), then adversary progress must be slowed (i.e., delay), which will allow the response force time to interrupt or stop the adversary (i.e., response). The response force time indicates the time it takes for the response personnel, including proprietary guards, contractors and/or members of local law enforcement, to arrive at a location and establish interruption of the adversaries from progressing in their attack.

The principal indicator for the performance of a PPS is its effectiveness (η_{PPS}), which expresses the conditional probability of an attacker path of actions being foiled, deterred or disrupted. Effectiveness assessment should take into account the complex configuration of detection, delay and response function that compose the PPS (Garcia, 2005). For high-security systems (i.e. the ones considered for counter terrorism) the response is generally assumed to be immediate on-site, so the response force time is part of the PPS effectiveness (Garcia, 2007). Effectiveness assessment consists of a multidimensional decision problem. Its results can provide a sound basis not only to carry out cost-benefit and cost-effectiveness analyses, but also to reevaluate and update the design of protection systems over time, in order to keep it in the state of art and to accommodate the introduction of new processes, functions or assets within the facility. Following the assumption of adding one security device at time, effectiveness improvement due to the introduction of a generic security measure i in the existing Physical Protection System along a generic segment k can be computed as:

$$\Delta\eta_{ik} = \eta_{PPS,new\ ik} - \eta_{PPS,old\ k} \quad (2)$$
$$\forall\ i \in \{1, \dots, n\}, n \in Z$$
$$\forall\ k \in \{1, \dots, t\}, t \in Z$$

Where $\eta_{PPS,new\ ik}$ 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. k indicates a generic segment that connects either the starting point to the first target or two contiguous targets, among all possible segments, multiple of the number of possible targets (t). It expresses the upgraded PPS effectiveness. On the other hand, $\eta_{PPS,old\ k}$ represents the probability of attacker's path of actions being foiled, deterred or disrupted before the addition of a security measure along a segment k; it has been indicated as baseline PPS effectiveness for the segment k throughout the present study. Therefore, the determination of the effectiveness improvement along a segment k $(\Delta\eta_{ik})$ requires the evaluation of PPS effectiveness before and after the addition of a security measure i. $\Delta\eta_{ik}$ is sometimes named "risk reduction" (Stewart & Mueller, 2008, 2011, 2013); an explanation regarding the nomenclature is available in Section 2.6.

Both the terms, respectively $\eta_{PPS,old\,k}$ and $\eta_{PPS,new\,ik}$, $\forall\, i \in \{1,..,n\}, n \in Z$, can be determined by means of several models, whose detailed description can be found elsewhere (Garcia, 2007). EASI model has been applied throughout the present study. EASI (i.e., Estimate of Adversary Sequence Interruption) model, developed by Sandia Laboratories (Garcia, 2007), calculates the probability of interruption $(P_{I,p})$, referred to a sequence of adversary actions aimed at theft or sabotage. EASI is a path-level model, meaning that it can analyze PPS performance along one adversary path per time and it refers to a single target per time. Consequently, the preliminary step for its application is the selection of an adversary action sequence, by means of Adversary Sequence Diagrams, based on site-specific data and reasonable assumptions about the adversary. In case of multiple targets, the path should be divided into t segments, with t number of the targets, and effectiveness analysis should be repeated for each of them. In case of multiple paths possible between contiguous targets, effectiveness analysis should be repeated for each of them. EASI model requires the following input parameters: detection and communication probabilities (i.e., indicated respectively with $P_{D,i}$ and P_C), delay and response mean times (i.e., indicated respectively with t_i and t_G) and standard deviations for each security measure i. Details on the model can be found elsewhere (Garcia, 2005, 2007). In module (2) of EM-PICTURES neutralization probability is not accounted, following the stated assumption that in industrial facilities the use of lethal force against an adversary is unlikely (Garcia, 2007). Therefore, the baseline system effectiveness can be assessed, as follows:

$$\eta_{PPS,old\,k} = P_{I,p^*} = \min\left(P_{I,p}\right) \qquad with\ p = \{1, \dots, q\},\ q \in Z \qquad (3)$$
$$\forall k \in \{1, \dots, t\}, t \in Z$$

Where the path p^* with the lowest $P_{I,p}$ (i.e., P_{I,p^*}) among q possible ones, characterizes the baseline effectiveness of the protection systems along the segment k and it has been named critical path. The calculation should be repeated for each of the t segments.

In order to determine the effectiveness of upgrades, the EASI model was reapplied to the critical path p^* for each of the security upgrades i, obtaining $\eta_{PPS,new\,ik}, \forall i \in \{1,..,n\}, n \in Z$, and therefore the correspondent effectiveness improvement $(\Delta\eta_{ik})$, referred to each segment k. The calculation was reapplied to each of the k segments, in purpose to obtain the overall effectiveness improvement $(\overline{\Delta\eta_i})$, as follows:

$$\overline{\Delta\eta_i} = f\left(\sum_{k=1}^{t} \Delta\eta_{ik}\right) \qquad (4)$$
$$\forall i \in \{1, \dots, n\}, n \in Z$$

Where f is a function of adversary's mode of action.

In case of a sequential action (e.g., one attacker that sabotage a target and just after a second one), the overall effectiveness improvement for each security upgrade i can be expressed according to a "series model":

$$\overline{\Delta\eta_i} = \sum_{k=1}^{t} \Delta\eta_{ik} \qquad (5)$$
$$\forall i \in \{1, \dots, n\}, n \in Z$$

In case of a simultaneous action (e.g., two attackers that sabotage one target each in the same time), the overall effectiveness improvement for each security upgrade i can be expressed according to a "parallel model":

$$\overline{\Delta\eta_i} = 1/\left(\sum_{k=1}^{t} 1/\Delta\eta_{ik}\right) \qquad (6)$$

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

2.4 Module 3: cost assessment

Module (3) of EM-PICTURES provides the evaluation of costs for each risk-reducing security measure $\left(C_{Security,i}\right)$. Cost assessment for a security device should include direct economic costs of applying a security device and indirect costs associated with its use. Therefore, it may include general terms as purchase costs, personnel costs and running costs. On the other hands, also cost terms either specific for each category of PPS or site-specific might be highlighted. Six main categories for costs have been considered in EM-PICTURES. Among these, five have been developed in close analogy with a similar cost evaluation referred to safety measures for the chemical and process industry (e.g., the CESMA tool (Reniers & Brijs, 2014b)): initial costs, installation costs, operating

costs, maintenance costs, renamed in this context as maintenance, inspection and sustainability cost, other running costs, specific costs. The main difference sketched out in comparison with similar cost evaluations referred to safety measures (e.g., the CESMA tool (Reniers & Brijs, 2014b)) instead of to security measures is the absence of a "Production loss cost" term and the different meaning of its linked term "Start-up cost". Installation of security countermeasures usually does not interfere with the production rate of the process plant, determining the necessity to neglect this term from the analysis. However, in some situations an integration of safety and security measures have been realized, even if criticized by security experts (Garcia, 2007), allowing to extend the term "production loss cost" also to security countermeasures. On the other hand, maintenance cost category should incorporate also inspection and sustainability costs (e.g., renewing license and rental costs) and inspection costs, as a consequence it has been renamed "maintenance, inspection & sustainability 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 the limited influence on the total costs (Campbell & Brown, 2003). The last category has been named "specific costs" and it includes all the cost features that are peculiar of either a specific category of security measure or site-specific.

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

$$C_{Security,i} = \left(C_{INITIAL,OV} + C_{INSTALL,OV} + C_{OPERATION,OV} + C_{MIS,OV} + C_{OR,OV} + C_{SPEC,OV}\right)_i$$
$$\forall\, i \in \{1,\dots,n\}, n \in Z \quad (7)$$

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 (7) were developed accordingly to the fundamentals of CBA (Campbell & Brown, 2003) and reported in Appendix A (Table A.1). In order to calculate each cost category, the costs pertaining to each subcategory identified in Table A.1 need to be added:

$$C_C = \sum_{i=1}^{n} C_{SC,i} \quad (8)$$

Where C_C is the cost category of interest, and $C_{SC,i}$ is the i-th cost subcategory identified in Table A.1.

Table A.1 reports details on the calculation of the single cost terms for a generic security device. Grouping them in 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 costs term should be expressed in coherent monetary value (e.g., all of them should be expressed in €/2016).

For the determination for Overall specific costs $\left(C_{SPEC,OV}\right)$, specific costs subcategories should be outlined for each class of security measures, according to their functions and features. Nevertheless, CBA is always a trade-off among accuracy and simplicity and sometimes accounting too many cost terms, whose contributions are clear only to patent owners or vendor, turns into a reduction of the user-friendliness of the model. As stated by Lee et al. (Lee, Fan, Miller, Stolfo, & Zadok, 2002) cost metrics are often site-specific because each organization has its own security policies and risk factors. Despite this cost category is open to eventual additional contributions, in the present approach Overall specific costs have been determined as:

$$C_{SPEC,OV} = C_{FP} + C_{SITE\_SP} \quad (9)$$

Where C_{FP} indicates Overall cost of a false-positive case and C_{SITE_SP} site-specific costs.

False-positive rate, whose cost is expressed by C_{FP}, refers to a situation in which the device identifies an object (person or thing) as a potential hazard, when it is not (Lin & Van Gulijk, 2015). This error turns into additional security procedures that causes 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. In the model, the formula proposed by Lin and Van Gulijk (Lin & Van Gulijk, 2015), which estimates the costs derived from a false-positive case in a physical detection system has been applied:

$$C_{FP} = C_{FA} \cdot P(FA) = \ C_{FA} \cdot P(alarm \ | no \ attack) \cdot \big(1 - P(T)\big) \quad (10)$$

Where: C_{FP} Overall cost of a false-positive case, C_{FA} cost of a single false-positive case, $P(FA)$ false-positive probability or false-alarm probability. It is a function of the security device and it expresses the probability of having the alarm without an actual threat ($P(FA) = P(alarm, no \ attack)$). The right member of equation (10) has been determined by applying to $P(FA)$ the probability chain rule, with $P(alarm, no \ attack) = P(alarm \ | no \ attack) \cdot \big(1 - P(T)\big)$.

Site-specific costs $\big(C_{SITE\_SP}\big)$ can be eventually added in case additional information is 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 countermeasure.

2.5 Module 4: benefit assessment

Benefit assessment consists on the definition of the avoided costs of each accidental scenario j among m possible ones: these are the losses derived from a successful attack $\big(C_{Loss,j}\big)$. Benefit modelling was indicated as module (4) in the general EM-PICTURES layout (Fig. 1). 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 risk assessment for safety purposes, wherein scenario-thinking is widely applied to picture possible unwanted situations. Despite the accidental or intentional nature of the event, a scenario-based approach is aimed at quantifying the probability of occurrence of a given outcome, as well as its causal chain and its consequences in terms of production loss, human health loss, assets loss, and environmental loss (CCPS - Center for Chemical Process Safety, 2003). 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. For instance, the application of both expected and worst-case scenarios is considered common practice within economic analyses for safety purposes in the chemical industry domain (Reniers and Van Erp, 2016). Le Sage (Le Sage, 2013) stressed the importance of considering in the security field a wide range of fictional scenarios to identify to which extent the proposed security measures can mitigate the identified risks (or threats) and fit within their operational context. If available, information should be gathered on previous accidents triggered by terroristic attacks on similar reference installations. Indeed, an expected scenario, which considers the average benefits, weighted by probabilities of occurrence, of different possible outcomes can be considered in the scenario selection phase. In this contribution, a rating for consequence severity composed by four categories; for instance T1 (i.e., catastrophic accident), T2 (i.e., critical accident), T3 (i.e., marginal accident) and T4 (i.e., negligible accident), has been adapted from a previous study (US Department of Defense, 2000). The mentioned approach has been already applied to the economic analysis of safety prevention investments within the chemical industry (Reniers & Sörensen, 2013a). However, in the selection of security scenarios it should be highlighted that adversaries (e.g., terrorists) 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 & Audenaert, 2014). Therefore, also a "worst-case scenario", should be taken into account in security. For what concerns the definition of probability for each scenario, the model framework allows considering different values of $P(T)$ for different scenarios, if the security analyst deems it necessary.

The losses derived from a successful attack include the damages, both direct and indirect, which will accrue because of a successful attack, taking into account the value and vulnerability of people and infrastructure, reputational losses, legal expenses and costs connected to supply-chain interruption. Generally, in CBA approach, a monetary quantification of both direct and indirect losses is carried out, but also non-quantifiable damages (i.e., psychological and political effects) should be at least mentioned (Stewart & Mueller, 2011). Quantification of direct tangible costs (e.g., replacement costs due to property damage) is quite straightforward. Although the monetization of the value of human lives loss after an attack is a common practice in CBA (Cropper & Sahin, 2009; Viscusi & Aldy, 2003),

it has always arisen ethical concerns since its introduction (Kelman, 1981). Among these, the most controversial issue is the assignment of a monetary figure on a person's life (Ackerman & Heinzerling, 2002; Ale, Hartford, & Slater, 2015). Indeed, the definition of the "Value of a Statistical Life" (VSL) has been defined a "complicated situation" (Tappura, Sievänen, Heikkilä, Jussila, & Nenonen, 2014) and a "philosophical problem" (Hansson, 2007) within the cost-benefit analysis domain. As reported by Viscusi and Aldy (Viscusi & Aldy, 2003), the variability of VSL all over the world may give raise to ethical issue and criticism. However, as stressed by Lin and Gulijk (Lin & Van Gulijk, 2015) the alternative of not recognizing this cost is probably even more arguable.

The quantification of indirect losses has been carried out within the model, provided that they are often comparable or even superior to direct losses (Reniers & Brijs, 2014b). The indirect losses derived from a major accident include reputational losses, legal expenses, costs due to accident investigation, involving both internal and external personnel, costs related to supply-chain delays and bottlenecks at the start-up phase (Gavious et al., 2009).

Similarly to what have been done for cost classification, also benefit categories within the security domain have been developed in close analogy with a similar study referred to the safety domain for the chemical and process industry (e.g., the CESMA tool (Reniers & Brijs, 2014b)), by outlining 9 benefit categories. The Overall annual benefits (i.e., avoided losses) derived from a generic accidental scenario $\left(C_{Loss,j}\right)$ can be computed as the sum of the nine mentioned contributions, for each scenario j considered in the analysis:

$$C_{Loss,j} = \left(B_{SUPC,OV} + B_{DAMAGE,OV} + B_{LEGAL,OV} + B_{INS,OV} + B_{H\&E,OV} + B_{INTV,OV} + B_{REPT,OV} + B_{OTH,OV} + B_{SPEC,OV}\right)_j$$
$$\forall j \in \{1, \dots, m\}, m \in Z \quad (11)$$

Where: $B_{SUPC,OV}$ is Overall supply chain benefits, $B_{DAMAGE,OV}$ is Overall damage benefits, $B_{LEGAL,OV}$ is Overall legal benefits, $B_{INS,OV}$ is Overall insurance benefits, $B_{H\&E,OV}$ is Overall human and environmental benefits, $B_{INTV,OV}$ is Overall intervention benefits, $B_{REPT,OV}$ is Overall reputation benefits, $B_{OTH,OV}$ is Overall other benefits and $B_{SPEC,OV}$ is Overall specific benefits.

The expressions applicable to the calculation of each benefit category in equation (11) were developed accordingly to the fundamentals of CBA (Campbell & Brown, 2003) and reported in Appendix B.1 (Table B.1). In order to calculate each benefit category, the benefits pertaining to each subcategory identified in Table B.1 need to be added:

$$C_B = \sum_{i=1}^{n} C_{SB,i} \quad (12)$$

Where C_B is the benefit category of interest, and $C_{SB,i}$ is the i-th benefit subcategory identified in Table B.1.

The expressions reported in Table B.1 allow the calculation of the single benefit terms for an either perspective or retrospective accidental scenario. Grouping them in the nine mentioned benefit categories, the total losses due to a generic accidental scenario can be computed. All the benefits term should be expressed in coherent monetary value (e.g., all of them should be expressed in €/2016).

Despite this category is open to eventual additional contributions, Overall specific benefits in EM-PICTURES have been determined as:

$$B_{SPEC,OV} = B_{SITE\_SP} + B_{IMM} \quad (13)$$

Specific benefits are mostly site-specific $\left(B_{SITE\_SP}\right)$ and should be outlined in case of additional information available. If additional information is available, also other immaterial terms (B_{IMM}), as the ones referred to cost of fear, psychological damages, social and political tensions might be added to the analysis.

2.6 Module 5: cost-benefit analysis

Module (5) of EM-PICTURES is aimed at defining the single security measures i that are economically feasible with reference to a scenario j.

The core of EM-PICTURES is the calculation of the Net Benefit, or Net Present Value, for a security countermeasure, carried out in this module. The Net Benefit has the following general expression (Stewart & Mueller, 2008, 2011, 2012, 2013):

$$Net\ Benefit = E(C_b) + \sum_T \sum_H \sum_L P(T) \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss} \cdot \Delta\eta - C_{Security} \quad (14)$$

Where $E(C_b)$ indicates the expected benefit from the security countermeasure not directly related to mitigating security threats (e.g., increased personnel confidence, reduction in crime, etc.). Often the assumption of $E(C_b) \cong 0$ is introduced in order to obtain conservative results. $P(T)$ represents the threat probability (e.g., the probability of attack) referred to a critical infrastructure. $P(H \mid T)$ and $P(L \mid H)$ are the vulnerability probabilities, described in Section 2.2. C_{Loss} indicates the overall losses or consequences, expressed in monetary values, and indicated also as "overall benefits". $\Delta\eta$ represents the effectiveness improvement achieved by implementing the Security measure (or Physical Protection System, i.e. PPS). $C_{Security}$ indicates the overall costs of the specific security measures (or systems) required to attain the benefits. The summation refers to the number of possible Threats (T) scenarios, Hazard (H) levels and Losses (L).

With the assumptions of $E(C_b) = 0$, equation (14) can be rewritten (see also Stewart and Mueller (Stewart & Mueller, 2008, 2011, 2012, 2013, 2014)) for a single scenario j as:

$$Net\ Benefit_j = P(T) \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \Delta\eta - C_{Security} \quad (15)$$

The product of threat and vulnerability probability is sometimes indicated as a single term (i.e., P_A) (Stewart & Mueller, 2008, 2011, 2012), expressing the probability of a "successful" attack:

$$P_A = P(T) \cdot P(H \mid T) \cdot P(L \mid H) \quad (16)$$

It should be noted that, in order to compare total benefits and total costs occurring at different point in time, it is necessary to introduce a discount rate to convert all cash flows in the future to present values of annuities. The conversion process, often termed as "actualization", is shown by the following formula (Campbell & Brown, 2003):

$$C' = C \cdot \frac{((1+r)^z - 1)}{((1+r)^z \cdot r)} \quad (17)$$

Where 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.

Since the purpose of cost-benefit analysis is to support the security risk management and decision-making, often the security risk is made explicit:

$$R = P(T) \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \eta_{PPS} \quad (18)$$

According to equation (18), the reduction in risk achieved by implementing an additional security measure i with reference to the same scenario, depends only on the effectiveness improvement (i.e., $\overline{\Delta\eta_i}$). Indeed, it explains how sometimes the nomenclature for the two terms overlaps (Stewart & Mueller, 2008, 2011, 2013).

In the context of EM-PICTURES the simplified expression of Net Benefit (equation (15)), present in modules (5) and (6)) has been modified with reference to every Security measure i and each scenario j:

$$\begin{cases} Net\ Benefit_{ij} = P(T) \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \overline{\Delta\eta_i} - C_{Security,i} \\ \forall i \in \{1, \dots, n\}, n \in Z \\ \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \quad (19)$$

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 $P(T) \cdot P(H \mid T) \cdot P(L \mid H) \cdot C_{Loss,j} \cdot \overline{\Delta\eta_i}$ indicates the overall risk variation obtained by the application of security measure i for scenario j, while $C_{Security,i}$ indicates the costs of providing the risk-reducing

security measure i that is necessary to obtain the benefits. Equation (19) allows considering different values of the threat and vulnerability probabilities for different scenarios, if the security analyst deems it necessary.

The implementation of a single security measure i is acceptable, with reference to scenario j, if:

$$Net\ Benefit_{ij} \geq 0 \tag{20}$$

Else, it should be rejected. The calculation of $Net\ Benefit_{ij}$ represents the output of cost-benefit analysis module (module (5) in Fig. 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.

2.7 Module 6: cost-effectiveness analysis

Module (6) of EM-PICTURES is aimed at determining the most profitable combination of security measures with reference to a specific scenario. Often, security investments should be compared with budget limitations. In this situation, the economic evaluation method turns into a cost-effectiveness analysis. As suggested by Reniers and Sörensen (Reniers & Sörensen, 2013b), the optimization problem to be solved, known as "Knapsack problem" is analogous in its general formulation for security countermeasures to the one already applied in the safety domain, and it consists on finding the solution of the following system:

$$\begin{cases} \max\left(Net\ Benefit_{vj} \cdot x_v\right) \\ C_v \cdot x_v \leq C_{Budget,j}\ \forall j \in \{1, \dots, m\}, m \in Z \\ x_v \in \{0,1\}, x_v \in Z \\ v \in \{1, \dots, w\}, w \in Z \end{cases} \tag{21}$$

The first equation of the system expresses the total Net benefit from the selected investments portfolio, which should be maximized, that means 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 $(C_v \cdot x_v)$ should not exceed the security budget $\left(C_{Budget,j}\right)$, which in turn is scenario-dependent, as further explained in Section 2.5. The third constraint $(x_v \in \{0,1\})$ implies that a measure is either fully taken or not taken at all. A number of assumptions are implicitly embedded in this formulation: security investments cannot be partially taken:

- The overall hypothetical benefits of all measures selected is the sum of the individual benefits;
- The overall cost of all security measures taken is the sum of the costs of the individual measures;
- Each security measure can be implemented independently, without consequences for the other investments.

The output of module (6) is the most profitable combination of security measures (v^*), within the constraint of the security budget, for each scenario j.
Therefore, the output of EM-PICTURES is a set of indicators derived from economic analyses that can support the security decision-making process within the chemical and process industry domain. Several risk acceptance criteria may be considered in the analysis, depending on the type of risk to be quantified (such as safety, economic, environmental, social), the focus of the stakeholders and decision-makers and the quality of information available.

3 Case study

3.1 Case study definition

The proposed EM-PICTURES model was applied to an illustrative case study, inspired by a real incident that took place in summer 2015 in Berre l'Étang, France, consisting in the sequential sabotage of two storage tanks in a chemical facility (Associated Press, 2015; BBC News, 2015b; Le Guernigou & Revilla, 2015; Le Huffington Post, 2015; Pardini, 2016; RFI News, 2015). The analysis carried out focuses on the selection and management of the security measures, given the probability of the attack. Considering the analysis temporary posterior to the event and in purpose to maintain the focus on the role of security measures, the probability of the attack was assumed equal to one throughout the case study. Indeed, the assumption of $P(T) = 1$ was justified by guidance values reported in

Table 1. Due to the limited amount of information available, $P(H \mid T)$ and $P(L \mid H)$ have been assumed equal to 1, following the conservative assumptions reported in Table 1.

The tank farm considered in the case study includes 40 atmospheric storage tanks, but 6 of them are dismissed. The scope of introducing dismissed tanks in the illustrative case study is to give security analysts a practical answer on security strategies to be adopted on dismissed areas of the plant/dismissed equipment, located close to the possible targets, but not containing hazardous substances anymore. The tanks have two different sizes: 10 have a volume of $40000\ m^3$ and contain naphtha, while 30 have a volume of $10000\ m^3$ and contain gasoline. The accidental scenario considered consists of a sequential sabotage to two storage tanks, named after respectively "first sabotage target" and "second sabotage target" as shown in Fig. 2. "First target" is a $40000\ m^3$ naphtha tank, while "second target" is a gasoline tank. The distance between the two targets is $500\ m$. The starting point for the adversary was chosen in correspondence of a pedestrian route just outside the border of the facility (i.e., $300\ m$ from the first target). The adversary was supposed to carry out the sabotage action by foot, placing improvised explosives on the targets, as confirmed by recent investigations (Pardini, 2016). Electronic devices, compatible with detonators, were found in proximity of the targets (BBC News, 2015b). The realistic damages, derived from the actual event, consisted on fire, environmental damage, but no casualties. The two tanks involved in the accident were completely destroyed, as well as their content. It was assumed that during emergency intervention, which lasts 13 hours, refinery activities were not shut down, but production rates were decreased. Moreover, additional consequences on public transportation (i.e., temporary highway closing-down) were derived from the actual event.

The determination of PPS in place was carried out comparing the description of PPS usually present in chemical facilities (Reniers et al., 2015) with photos and maps of the layout of a reference installation, reported in Fig. 2. 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 has been reported in Section 3.2.

Fig. 2. Layout of a reference installation considered in the case study, with adversary starting point, sabotage targets and critical adversary paths, divided into two segments. Segment n°1 connects the starting point with the first target. Segment n°2 connects the first target with the second target. The ending point is the second target.

3.2 Development of adversary sequence diagrams and effectiveness calculation

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

A possible site-specific adversary sequence path, in relation with physical protection elements present on the site, has been found. Two segments related to the two sabotage targets have been identified: "Segment n°1" connects the starting point with the first target; "Segment n°2" connects the first target with the second one. The details have been reported in Table 2, Part A and Fig. 2.

The calculation of baseline system effectiveness was carried out accordingly to Section 2.3, with the aim to determine the probability of interruption (P_{I,p^*}), for the critical paths of the two segments. The detection elements present in both the segments are cameras on doors, at level of both the sabotage targets, whose $P_D = 0.9$. Also the location of detection elements has been included in the analysis, according to EASI model. For all delay elements with the exception of running times, specific data have been retrieved (Garcia, 2007) and reported in Table 2, Part A, joined with all the data inherent to the detection function, for both the paths 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 the weight of explosives and detonators. Distances among delay elements have been retrieved from the map and reported in Table 2, Part B. Inputs for the calculation of response element have been reported in Table 2, Part C.

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

ADVERSARY TASKS – CRITICAL PATH - SEGMENT N°1		***DETECTION***	***DELAY***	
Task n°	***Task Description***	***Detection elements***	***Delay elements***	***Mean delays (s)***
1	**Cut simple wired perimeter fence**	none	Fence fabric	10.0
2	**Run to first tank protected area**	none	Running time	65.6
3	**Open door**	camera on the door; $P_{D,3} = 0.9$	Height of the wall	30.0
4	**Run to first tank (target)**	none	Running time	131.2
5	**Sabotage first target**	none	Place explosives and detonators	120.0
ADVERSARY TASKS – CRITICAL PATH - SEGMENT N°2		***DETECTION***	***DELAY***	
Task n°	***Task Description***	***Detection elements***	***Delay elements***	***Mean delays (s)***
6	**Exit first target zone**	none	Running time	21.9
7	**Run to second tank protected area**	none	Running time	196.9
8	**Open door**	camera on the door; $P_{D,8} = 0.9$	Door hardness	30.0
9	**Reach second tank (target)**	none	Running time	91.9
10	**Sabotage second target**	none	Place explosives and detonators	120.0

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	ve	3.048	*m/s*	**Distance first wall/first target (Task 4 – segment n°1)**	d_2	200	*m*
Reduction velocity factor due to additional weight - a (before first sabotage – segment n°1)	φ_1	0.5	*adim.*	**Distance first target/exit first target zone (Task 6 – segment n°2)**	d_3	50	*m*
Reduction velocity factor due to additional weight - b (after first sabotage – segment n°2)	φ_2	0.75	*adim.*	**Distance exit first target zone/ second wall (Task 7 – segment n°2)**	d_4	450	*m*
Distance out/first wall (Task 2 – segment n°1)	d_1	100	*m*	**Distance second wall/second target (Task 9 – segment n°2)**	d_5	210	*m*

Part C) Data for the calculation of Response function

Probability of guard communication: P_C	0.95	***Mean Response Force Time: t_G (s)***	300

Table 2. Input for the calculation of baseline PPS effectiveness. From the top to the bottom: Part A) Adversary sequence and inputs for the calculation of detection and delay elements for critical segment n°1 and critical segment n°2; Part B) Additional data for the calculation of running delay times for both the segments; Part C) Inputs for the calculation of the response function, valid for both the segments.

The EASI model, applied for the calculation of the effectiveness, takes into account uncertainties regarding each task (e.g., presence of a lag time in the detection) by applying probability distribution. According to the conservative assumption on data dispersion of the model (Garcia, 2007), standard deviation for each security element has been assumed as $3/10$ of the mean value throughout the case study. This assumption allows considering uncertainties, as guards that will not always respond exactly after the same time and adversary that may take more or less time to penetrate barriers with respect to average values. The critical probabilities of interruption (P_{I,p^*}) are respectively 0.27 for segment n°1 and 0.16 for segment n°2; these values represent the baseline PPS effectiveness for the two segments (i.e., $\eta_{PPS,old\ k}$) that will be considered in the following developments of the case study.

3.2.2 Proposal of five security upgrades and calculation of upgraded system effectiveness ($\overline{\Delta\eta_i}$)

Starting from the values of baseline PPS effectiveness for the two segments ($\eta_{PPS,old\ 1} = 0.27$ and $\eta_{PPS,old\ 2} = 0.16$), five PPS upgrades have been proposed, according to technical references (Garcia, 2007; Reniers et al., 2015):

A) Adding fence sensors as perimeter detection system
B) Adding a perimeter delay element by building a concrete-reinforced external wall
C) Adding detection elements (i.e., cameras) at sabotage targets level
D) Adding delay elements at sabotage targets level
E) Reducing response force time by building a closer 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 and upgrade E refers to the response function. Moreover, upgrades A and B refer to external perimeter of the facility, and consequently only to segment n°1, while C, D and E refer to the proximity of the storage tank farm and consequently belong both to segment n°1 and segment n°2.

Upgrade ID	***Description***	***PPS function modification***	***N° of modified tasks (segment n°1)***	***N° of modified tasks (segment n°2)***	***Modified inputs***	$\Delta\eta_{i,1}$	$\Delta\eta_{i,2}$	$\overline{\Delta\eta_i}$
A	**External infrared fence sensors as perimeter detection system (at fence level)**	Detection; infrared fence sensors	1	none	$P_{D,1} = 0.9$	0.3541	0	**0.3541**
B	**Construction of an external reinforced concrete wall (instead of the fence)**	Delay; wall hardness	1	none	$t_1 = 180\ s$	0	0	**0**
C	**Addition of detection elements at sabotage targets**	Detection; exterior cameras	5	10	$P_{D,5} = P_{D,10} = 0.9$ $(for\ both\ the\ targets)$	0.0027	0.0027	**0.0054**
D	**Addition of delay elements at sabotage targets**	Delay; additional wall with doors	5	10	$t_5 = t_{10}$ $150\ s$	0.0945	0.0836	**0.1781**
E	**Reduction of response force time (by creating a closer guard dispatch)**	Response; relocation of guards closer to storage area	- (*)	- (*)	$t_G = 180\ s$	0.1961	0.1535	**0.3496**

Table 3. Effectiveness results for five 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 modified tasks for segment n°1 and segment n°2, effectiveness improvement for segment n°1 ($\Delta\eta_{i,1}$)and segment n°2 ($\Delta\eta_{i,2}$) and overall effectiveness improvement ($\overline{\Delta\eta_i}$). (*) Reduction of response force time does not affect a single task.

The upgraded values of effectiveness, indicated as $\eta_{PPS,new\ i\ 1}$ and $\eta_{PPS,new\ i\ 2}$, for each of the five options have been calculated by inserting in the effectiveness model for the two segments (i.e., the same model previously applied to calculate baseline PPS effectiveness) the modified inputs listed in Table 3. The results regarding upgraded effectiveness index (i.e., $\Delta\eta_{i,1}$ and $\Delta\eta_{i,2}$) and overall effectiveness improvement for a sequential action (i.e., $\overline{\Delta\eta_i}$), correspondent to each of these upgrades have been reported indeed in the same table.

The results, reported in Table 3, clearly show that, from the effectiveness point of view, two options belonging to different security functions are the best ones: the addiction of detection elements at external fence level (upgrade A) and guard relocation (upgrade E). Neverthless, the presence of additional delay elements at fence level, represented by upgrade B, and the addition of detection elements at sabotage targets proved to be uneffective in increasing PPS effectiveness. Additional delay at targets level, indicated with upgrade D, appeared as an

intermediate option in terms of effectiveness improvement. However, even if upgrades A 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.). Furthermore, the results of effectiveness assessment 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 five PPS upgrades proposed in the case study, according to six main categories and 22 subcategories presented in EM-PICTURES (see Section 2.4 and Appendix A.2), considering the time span of one year and the implementation of a single security upgrade.

For each of the five security upgrades, the details of cost calculations have been illustrated in Appendix A.2. The results of costs calculation are summarized in Fig. 3. Despite the values of Overall costs ($C_{Security,i}$) belong to the same order of magnitude (i.e., 10^4 €) for all the security upgrades, the same consideration does not apply to the percentage composition of each cost category, as it is visible in Fig. 3.

The comparison among percentage compositions (Fig. 3), obtained for each security measure by using the respective Overall cost as reference, shows that for detection elements (i.e., upgrades A and C) Installation costs are the prevailing ones, followed by relevant Initial costs and Operational costs. For delay elements (i.e., upgrades B and D) Installation costs are predominant, but Operating costs are negligible. For response element (i.e., upgrade E) Installation costs are the prevailing ones, followed by Other running costs; the latter ones are almost negligible for all the other security upgrades. Eventually, Maintenance, inspection and sustainability costs are around 5% of the Overall costs for all the five security upgrades considered in the case study.

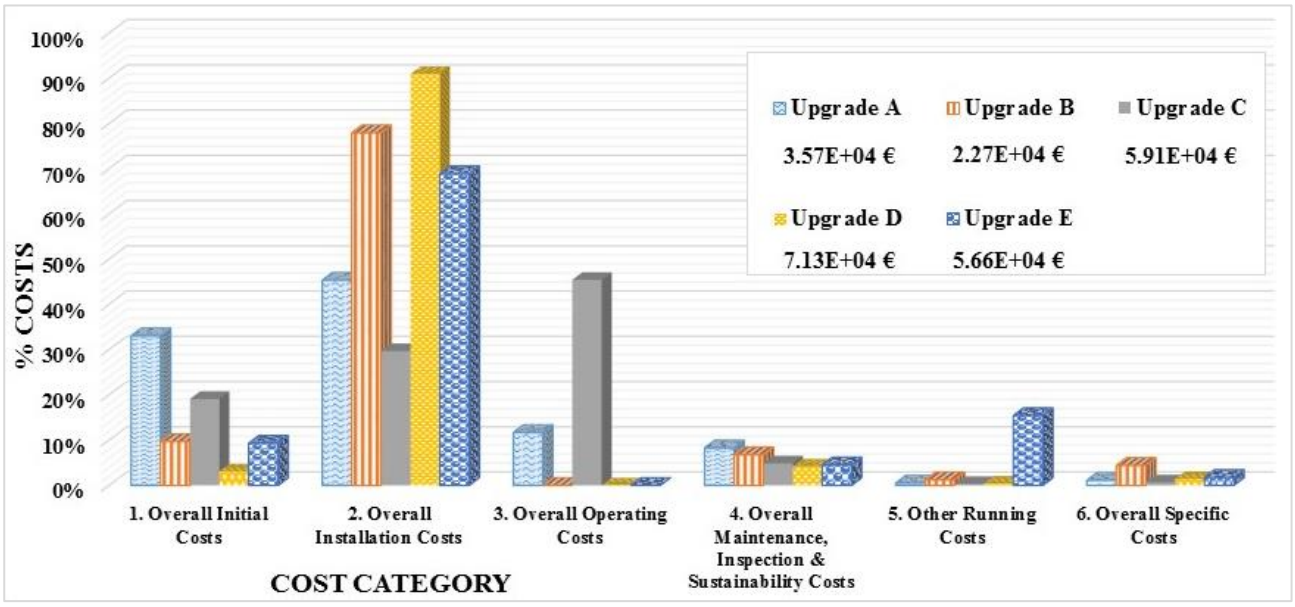

Fig. 3. Percentage composition of Overall costs for each upgrade of the PPS, according to six main cost categories. For each cost category, from the left to the right: A) Adding fence sensors as perimeter detection system, B) Adding a perimeter delay element by building a concrete-reinforced external wall, C) Adding detection elements at sabotage targets level, D) Adding delay elements at sabotage targets level, E) Reducing response force time by relocating guards closer to the targets. Overall cost of each security upgrade is reported in the box on the right.

3.4 Benefit calculation for different scenarios

The losses derived from a successful attack should include the 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 and infrastructures, as described in Section 2.5. Consequently, benefits calculation is dependent on the choice of an appropriate accidental scenario. In the present case study, three possible scenarios have been analyzed for benefit calculation, with the purpose to illustrate the potentiality of EM-PICTURES: realistic scenario, worst-case scenario and expected scenario. Realistic benefits indicates the actual losses sustained in the attack. The realistic benefits considered may not exactly reflect the actual ones, due to the limited amount of technical information available. On

the other hand, worst-case benefits are the consequences sustained in the worst-case scenario that is a domino accident in the tank farm, with several casualties and injuries and severe damage and production loss. Indeed, expected benefits are the benefits derived from a hypothetical scenario, which considers the average benefits, weighted by probabilities of occurrence, of four possible outcomes, as described in Section 2.5. Illustrative probabilities were defined for each category of scenario, together with a detailed description of all the scenarios analyzed in the case study, in Appendix B.2 (Table B.2). It was assumed that, for each scenario considered, benefits are independent from the security countermeasure that can be implemented. The details regarding benefits calculations are reported in Appendix B.2.

The results of benefits calculations are summarized in Fig. 4; the values of Overall benefits belong to the same order of magnitude (i.e., 10^5 €) for realistic scenario and expected scenario, while the Overall benefits referred to worst-case scenario are three orders of magnitude higher.

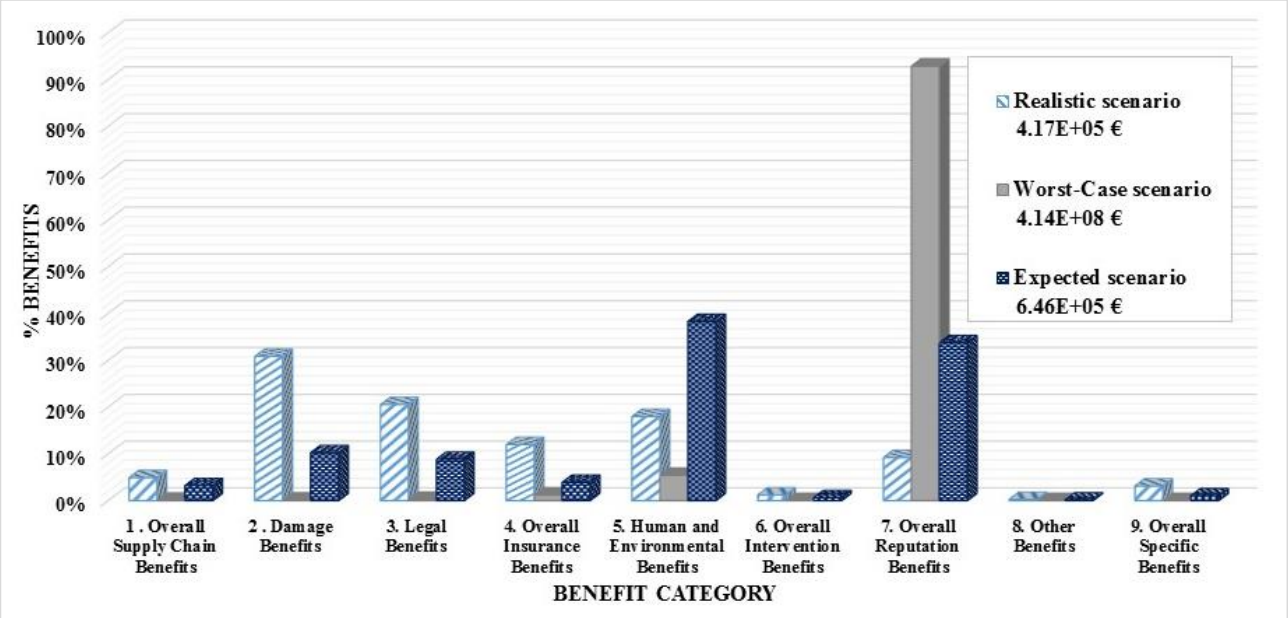

Fig. 4. Percentage composition of Overall benefits for three different scenarios. For each benefit category, from the left to the right: realistic scenario, worst-case scenario and expected scenario. Overall benefits are reported in the box on the right for each scenario.

The comparison among percentage compositions, obtained for each scenario by using the respective Overall benefits as reference and reported in Fig. 4, shows that, from a general point of view, Human and environmental benefits, Overall reputational benefits, Overall damage benefits, Overall insurance benefits are the most relevant categories. Both for worst-case scenario and for expected scenario Human and environmental benefits are relevant, due to the high monetary value attributed to injuries and casualties, in comparison with damages to assets; however, especially in worst-case scenario, the reputation loss is prevailing. On the other hand, for realistic scenario, benefits distribution among categories is the most uniform one, but Overall damage benefits are slightly prevailing, due to the relevant damages to company assets and to the absence of human losses.

4 Results and discussion

4.1 Results of case study

The results of the assessment of the case study consist in cost-benefit and cost-effectiveness analyses results. The first are the values of actualized Net benefits, for five PPS upgrades and for three scenarios. The latter are the most profitable combinations of security upgrades for each scenario, within the constraint of the security budget.

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 (17). The latter is a conventional number of operational years for a security measure. Certain costs (e.g., initial and installation costs) occurs only in the present and thus do not have

to be actualized, whereas other costs (e.g., operating costs, maintenance, inspection and sustainability costs, other running costs) refer to the whole remaining lifetime of the facility and therefore they should be discounted to the present. The benefit categories should be all actualized, as they represent positive cash flows, occurring throughout the remaining lifetime of the facility. The actualized values of Overall Benefits are respectively $2.70 \cdot 10^5$ € for realistic scenario, $2.76 \cdot 10^8$ € for worst-case scenario and $4.31 \cdot 10^5$ € for expected scenario. Considering the threat and vulnerability probabilities unitary, the value of Net Benefit, also named Net Present Value (NPV), has been calculated for each of the five PPS upgrades, according to the three scenarios, by applying equation (19). The final results of cost-benefit analyses, reported in Table 4, prove the coherency of the model, highlighting that security upgrades A and E are economically feasible for all the scenarios considered. Upgrade D is acceptable only with reference to expected scenario and worst-case scenario; upgrade C is acceptable only with reference to worst-case scenario.

SECURITY UPGRADES		***NET BENEFITS***		
		REALISTIC SCENARIO	**WORST - CASE SCENARIO**	**EXPECTED SCENARIO**
Upgrade ID	**DESCRIPTION/UNIT**	€	€	€
A	**External infrared fence sensors as perimeter detection system (at fence level)**	**6.80E+04**	**9.76E+07**	**1.22E+05**
B	**Construction of an external reinforced concrete wall (instead. of the fence)**	**-2.21E+04**	**-2.21E+04**	**-2.21E+04**
C	**Addition of detection elements (i.e., cameras) at sabotage targets**	**-4.69E+04**	**1.44E+06**	**-4.60E+04**
D	**Addition of delay elements at sabotage targets**	**-2.06E+04**	**4.90E+07**	**6.59E+03**
E	**Reduction of response force time (by creating a closer guard dispatch)**	**4.86E+04**	**9.63E+07**	**1.02E+05**

Table 4. Cost-benefit analysis results, in term of Net Benefits, for five different PPS upgrades and three possible scenarios.

Cost-effectiveness analysis has been applied in order to determine the most profitable combination of security upgrades within the security budget constraint for each scenario. For each scenario, all the possible 30 combinations of PPS upgrades have been considered, starting from each single security measure, to couples, triplets, quartets and eventually group of five. Actualized Overall costs have been calculated for each combination by applying a 3.5% discount rate to the pertinent cost categories of each option taken and by summing the actualized costs (HSE - Health and Safety Executive, 2016), then Overall costs have been compared with the actualized security budget. It should be noted that the security budget is different among the three scenarios, due to different percentage increases of security budget after the accident, depending on consequence severity. For each scenario, only the combinations respecting the budget criteria have been selected and their Net Benefits have been calculated and compared, according to equation (21). The actualized values of Overall benefits applied in the calculation have been the ones reported in this section.

SCENARIO REFERENCE	***FIRST COST-EFFECTIVE COMBINATION***			***SECOND COST-EFFECTIVE COMBINATION***			***Security Budget***
	Combination ID	***Net Benefit*** (€)	***Total Cost of Combination*** (€)	***Combination ID***	***Net Benefit*** (€)	***Total Cost of Combination*** (€)	***Value*** (€)
REALISTIC	**A+E**	**1.17E+05**	7.90 E+04	**A+B+E**	**9.46E+04**	1.01E+05	**1.20E+05**
WORST - CASE	**A+C+E**	**1.95E+08**	1.27 E+05	**A+E**	**1.94E+08**	7.90E+04	**1.44E+05**
EXPECTED	**A+E**	**2.24E+05**	7.90 E+04	**A+B+E**	**1.01E+05**	2.02E+05	**1.10E+05**

Table 5. Cost-effectiveness analysis results, regarding all possible combinations of security measures, for each of the three scenario. From the left to the right: first-most profitable combination, second-most profitable combination and security budget.

The results of cost-effectiveness analyses, reported in Table 5, show that the combination of security measures A and E (i.e., application of detection system at external fence level and relocation of security guards) is the one with the maximum Net Benefit for realistic and expected scenario. Nevertheless, the most profitable combination for worst-case scenario include, besides upgrades A and E, also upgrade C, which refers to additional detection system at sabotage targets. The second most profitable combination includes upgrades A and E for the three scenarios; indeed, for realistic and expected scenarios also the application of upgrade B (i.e., additional delay element at external level) is suggested. Fig. 5 shows the complete ranking of all possible combinations of security measures, according to cost-effectiveness analysis, for each of the three scenarios. The results show that several profitable combination offer an integration of different security functions (i.e., detection, delay and response), providing therefore a more complete security protection. Nevertheless, none of the combinations respecting the budget constraints includes more than three security upgrades. Moreover, in the top ten most profitable combinations for the three scenarios are often present security measures whose single performance increases are very limited, due to the relatively low costs of implementation (e.g., upgrade B).

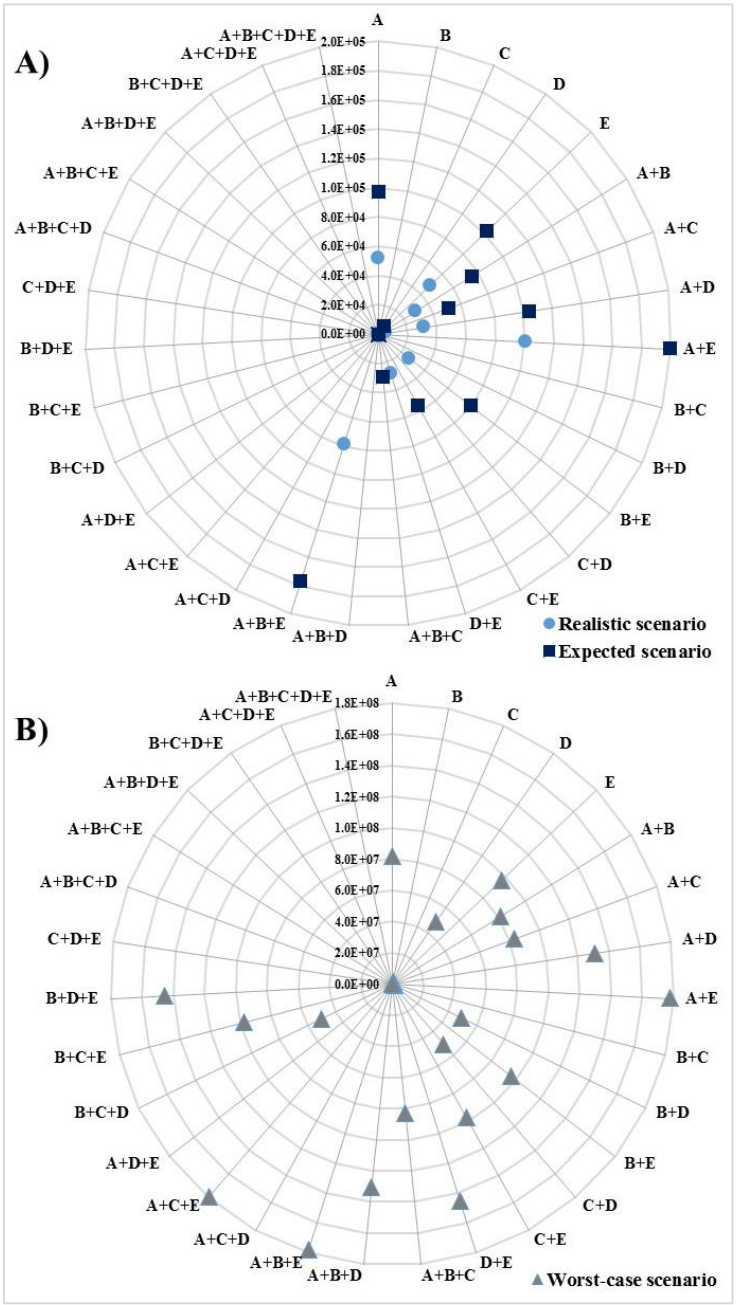

Fig. 5. Cost-effectiveness analysis results, showing the ranking in terms of Net Benefit respecting budget (expressed in €(2016)) for all possible combinations of security measures, with reference to the three scenarios: A) realistic scenario and expected scenario; B) worst-case scenario.

Therefore, the consistent results of cost-benefit and cost-effectiveness analyses highlight that upgrade A and upgrade E are the suggested security measures to be implemented together. This option offers improved detection at perimeter level and improved response of security guards. However, the implementation of a triplet of security upgrades (e.g., upgrades A+B+E), might be convenient with reference to a worst-case scenario. According to all these options, an integration of different security functions is carried out, providing therefore a more complete security protection, according to the OPER principle (Reniers et al., 2015). These results may offer sound indications for the stakeholders to rationally select and allocate security measures, providing a range of economically profitable options, which should be eventually compared with company-specific acceptance criteria and information.

4.2 Scenario analysis validation

The application of EM-PICTURES highlighted a significant similarity, in terms of benefit category results between realistic scenario and expected scenario (see Fig. 4). As explained in Section 3.4, the initial probabilities of occurrence for four different outcomes that compose expected benefits have been chosen arbitrarily, for illustrative purposes (Table B.2). Indeed, a validation of scenario analysis through the re-calculation of probabilities for four different outcomes has been carried out, imposing for each category, as well as for Overall values, the equality of expected benefits with realistic benefits, by means of Excel Solver®.

EXPECTED BENEFITS RECALCULATION RESULTS		***EXPECTED SCENARIO***		***RATIO*** $(C_{Loss,Expected} - C_{Loss,Realistic})/C_{Loss,Realistic}$	
		After scenario validation		***Before scenario validation***	***After scenario validation***
Symbol	***Description***	***Unit***	***Value***	***Value (%)***	***Value (%)***
$B_{SUPC,OV}$	***1 . Overall supply chain benefits***	€	2.04E+04	1.39%	0
$B_{DAMAGE,OV}$	***2 . Overall damage benefits***	€	6.59E+04	-48.55%	-48.74%
$B_{LEGAL,OV}$	***3. Overall legal benefits***	€	5.75E+04	-33.55%	-32.91%
$B_{INS,OV}$	***4. Overall insurance benefits***	€	2.27E+04	-49.45%	-54.54%
$B_{H\&E,OV}$	***5. Overall human and environmental benefits***	€	2.33E+05	229.67%	210.93%
$B_{INTV,OV}$	***6. Overall intervention benefits***	€	4.09E+03	-20.21%	-18.27%
$B_{REPT,OV}$	***7. Overall reputation benefits***	€	3.84E+04	468.00%	0
$B_{OTH,OV}$	***8. Other benefits***	€	8.22E+02	-23.24%	-22.32%
$B_{SPEC,OV}$	***9. Overall specific benefits***	€	6.60E+03	-48.91%	-49.21%
C_{Loss}	***Overall benefits***	€	**4.50E+05**	**54.85%**	**7.80%**
PROBABILITY OF OCCURENCE RECALCULATION RESULTS		**EXPECTED SCENARIO**		**RATIO** $(P_{after\ sv} - P_{before\ sv})/P_{before\ sv}$	
		After scenario validation			
Category	***Descriptive word***	***Value***		***Value (%)***	
T1	**Catastrophic accident**	**3.05E-05**		**-93.91%**	
T2	**Critical accident**	**3.91E-01**		**-2.35%**	
T3	**Marginal accident**	**6.09E-01**		**10.79%**	
T4	**Negligible accident**	**0**		**-100.00%**	

Table 6. Scenario validation (i.e., sv) results.

The comparison has been made among non-actualized benefit values, but it should be remarked that this element does not affect the comparison results, as long as the discount rate applied is the same. The results of probability revision, reported in Table 6, show that the severity of consequences in the real accident is between category T2 (critical accident) and category T3 (marginal accident), accordingly to the severity ranking considered in the case

study. Therefore, EM-PICTURES may be effectively applied also retrospectively, in purpose to validate the probability of occurrence for security-based accidental scenarios. The present application might be useful in the security domain, due to the lack of quantitative information regarding accidents occurrence in this domain.

4.3 Discussion

The application of EM-PICTURES to a case study made clear that the model provides a useful insight on the profitable security measures to be adopted in a chemical and process facility. The main advantages of the model are its completeness with respect to cost and performance of security measures, as well as to losses, and the consequent accuracy of the results. Moreover, the model is not over-complicated, therefore enhancing its possibility to be applied in industrial practice. Indeed, EM-PICTURES provides site-specific answers to security analysts, because it allows evaluating the performance of physical security measures present on-site and comparing several security upgrades, as well as possible adversary paths dependent on the layout of the facility. The cost assessment allows a precise definition of the most relevant cost terms due to the implementation of security measures, leaving at the same time enough space for the analyst to add specific costs. Moreover, the potentiality of EM-PICTURES both in predictive and in posterior analysis has been proved by its application to several possible accidental scenarios. Indeed, the benefit assessment allows a detailed description of the losses derived from either perspective or retrospective accidental scenarios. In particular, the retrospective application of EM-PICTURES (Section 4.2) may offer an additional tool to retrieve and validate quantitative information on security-based scenarios.

Nevertheless, as all cost-benefit analyses, the model needs to retrieve detailed information on the costs of security measures, and the monetization of all the losses derived from a major accident is not always free from complication. For instance, assigning monetary values to mortality and morbidity is a common practice in economic analyses, but it is still defined “a complicated situation” (Tappura et al., 2014), which might arise ethical concerns (Ale et al., 2015). On the other hand, following a precise checklist for costs and benefits evaluation, as the one presented in EM-PICTURES, may prevent omissions and inaccuracies. Moreover, also the assumptions regarding discount rates for overall costs and benefits might be affected by subjectivity of the analyst. Indeed, also the definition of adequate threat and vulnerability probabilities requires carefulness of the security analyst, as they depend on many variables. The deterministic approach here-in applied provide guidance for the choice of these values and it allows focusing on the role of security measures in the prevention of accidental scenarios. Also the effectiveness assessment present several uncertainties: the analysis is site-specific and accident-specific, as it depends on the possible adversary path of actions. Therefore, the results obtained from effectiveness assessment cannot be generalized beyond the specific application. Moreover, although the model is able to take into account possible additional terms that may affect the overall performance of the physical protection system (e.g., lag-time in detection by the security guards), it should be considered as a simplified representation of reality. Therefore, whenever EM-PICTURES is applied, it is important to present the analysis in a fully transparent manner, specifying the assumptions made and discussing the uncertainties arisen, in purpose to avoid misleading conclusions.

The distinctive feature of the model is the flexibility, given by its capability to perform both cost-benefit and cost-effectiveness analysis, offering as outputs a broad spectrum of economic analyses results, which can eventually support the security decision-making process. Indeed, the interpretation of the economic analyses results derived from EM-PICTURES is a crucial point. As showed in Section 4.1, the results obtained by cost-benefit and cost-effectiveness analyses are generally coherent; however, they show a strong dependency on the selection of pertinent security-based scenarios. For instance, security measures that are not feasible with reference to a marginal scenario might be appropriate with reference to a catastrophic scenario. This issue makes the selection of an appropriate pool of credible scenarios even more important. Moreover, the results of cost-effectiveness analysis depend on the threshold defined by security budget that is generally defined yearly by security management. Besides, the final results may suggest adopting combinations of security measures that include also one or more security measures singularly not profitable. In these situations, it is a management decision whether to revise the security expenditure, as well as to give priority either to cost-benefit or to cost-effectiveness analyses results. Indeed, a profitable combination of security measures may include one or more measures whose performances are not excellent, due to several factors standing between effectiveness assessment and final results (e.g., costs, budget threshold, selection

of scenarios, etc.). In these cases, the combinations of security measures belonging to more than one security function should be preferred, as they provide a more complete protection.

Therefore, the outputs of EM-PICTURES might be applied in risk-informed security decision-making both at company and at regulatory level, to increase the awareness of management or regulators toward security issues by means of non-technical and rather user-friendly outputs. At company level, possible solutions for the optimal selection and allocation of security prevention investments provided by EM-PICTURES may be discussed by the management and eventually weighted with respect to company specific acceptance criteria, site-specific issues and additional qualitative information available. At regulatory level, EM-PICTURES might be applied to tackle security vulnerable chemical facilities and to propose economically feasible physical protection alternatives, which allow meeting eventual legal requirements. However, the application of the model at company level seems to be more feasible in a short-term perspective, due to the actual lack of regulation at European Union level regarding security risk assessment and related decision-making within chemical and process facilities. Indeed, even if the framework is not over-complicated, its application requires an effort that should be avoided whenever the results are obvious from the outset, because in these situations it does not provide additional support to security decision-making.

5 Conclusions

A novel model for cost-benefit and cost-effectiveness analyses of process-industry related counter-terrorism measures was developed. The model, starting from the baseline physical protection system effectiveness of a process facility, allows evaluating and comparing the costs derived from the introduction of a security upgrade with the losses derived from either perspective or retrospective accidental events, named benefits, accounting also effectiveness improvement. Therefore, model application enables to define a more rational selection and allocation of process industry related physical security measures. EM-PICTURES, which is indeed the first quantitative model developed within the specific framework of security economic analysis for the chemical and process industry domain, allows obtaining a set of economic security-related indicators. Therefore, EM-PICTURES outputs provide a sound support to managers and regulators involved in the security decision-making process, and may eventually contribute to the reduction of chemical plants vulnerability towards intentional malevolent acts.

6 Nomenclature

Acronym	**Definition**
CBA	Cost-benefit analysis
CEA	Cost-effectiveness analysis
CFATS	Chemical Facility Anti-Terrorism Standards
EASI	Estimate of Adversary Sequence Interruption
EM-PICTURES	Economic Model for Process-Industry related Counter Terrorism measURES
IED	Improvised Explosive Device
NPV	Net Present Value; synonym: Net Benefit
PPS	Physical Protection Systems (i.e., system including all the physical security measures on site)
SV	Scenario validation
VBIED	Vehicle Borne Improvised Explosive Device

Symbol	**Definition**	**Unit**
$B_{DAMAGE,OV}$	Overall damage benefits; benefit category	€
$B_{H\&E,OV}$	Overall human and environmental benefits; benefit category	€
B_{IMM}	Immaterial benefits; benefit subcategory	€
$B_{INS,OV}$	Overall insurance benefits; benefit category	€
$B_{INTV,OV}$	Overall intervention benefits; benefit category	€
$B_{LEGAL,OV}$	Overall legal benefits; benefit category	€
$B_{OTH,OV}$	Overall other benefits; benefit category	€
$B_{REPT,OV}$	Overall reputation benefits; benefit category	€
B_{SITE_SP}	Site-specific benefits; benefit subcategory	€
$B_{SPEC,OV}$	Overall specific benefits; benefit category	€
$B_{SUPC,OV}$	Overall supply chain benefits; benefit category	€
C	Yearly overall cost or benefit	€
C'	Actualized value of overall cost or benefit	€
C_B	Generic nomenclature for benefit category	€
$C_{Budget,j}$	Security budget	€

Symbol	Definition	Unit
C_C	Generic nomenclature for cost category	€
C_{FA}	Cost of a single false-positive case	€
C_{FP}	Overall cost of a false-positive case; cost subcategory	€
$C_{INITIAL,OV}$	Overall initial costs; cost category	€
$C_{INSTALL,OV}$	Overall installation costs; cost category	€
$C_{Loss,j}$	Overall losses or consequences of either perspective or retrospective accidental scenario j expressed in monetary values; overall benefits. Reported elsewhere as C_{Loss}; see equation (14).	€
$C_{MIS,OV}$	Maintenance, inspection and sustainability costs; cost category	€
$C_{OPERATION,OV}$	Overall operating costs; cost category	€
$C_{OR,OV}$	Other running costs; cost category	€
$C_{SB,i}$	Generic nomenclature for benefit subcategory	€
$C_{SC,i}$	Generic nomenclature for cost subcategory	€
$C_{Security,i}$	Overall annual costs due to the implementation of one generic security measure i. Indicated elsewhere as $C_{Security}$; see equation (14).	€
C_{SITE_SP}	Site-specific costs; cost subcategory	€
$C_{SPEC,OV}$	Overall specific costs; cost category	€
C_v	Overall cost of a combination of security measures	€
d_i	Distance between delay elements along adversary's path	*m*
$E(C_b)$	Expected benefit from the security countermeasure not directly related to mitigating security threats (e.g., increased personnel confidence, reduction in crime, etc.)	€
f	Function expressing adversary's mode of action (e.g., series, parallel, etc.) in presence of multiple targets	*adim.*
H	Hazard levels	*adim.*
i	Security upgrade (i.e., additional single security measure)	*adim.*
j	Accidental scenario	*adim.*
k	Generic segment that connects either the starting point to the first target or two contiguous targets	*adim.*
L	Losses levels	*adim.*
m	Number of accidental scenarios accounted in the economic analysis	*adim.*
n	Number of security upgrades	*adim.*
$Net\ Benefit_{ij}$	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. Reported elsewhere as: $Net\ Benefit_j$, $Net\ Benefit$ (see equation (14) and (15)).	€
$Net\ Benefit_{vj}$	Net Benefit obtained by applying a combination of security measure v, among w possibilities, with reference to a specific scenario j, among m scenarios considered in the analysis.	€
p	Generic adversary's path of action for each segment k	*adim.*
p^*	Critical path that characterizes the baseline physical protection system performance	*adim.*
P_A	Product of threat and vulnerability probability; expressing the probability of a "successful" attack	*adim.*
$P(alarm \mid no\ attack)$	Conditional probability of having an alarm without a terroristic attack; see equation (10)	*adim.*
P_C	Probability of guard communication	*adim.*
P_D	Detection probability	*adim.*
$P(FA)$	False-positive probability; false-alarm probability; expressed as $P(alarm, no\ attack)$	*adim.*
$P(H \mid T)$	Conditional hazard probability	*adim.*
$P(L \mid H)$	Conditional loss probability	*adim.*
$P_{I,p}$	Probability of interruption of an adversary along a path p	*adim.*
P_{I,p^*}	Probability of adversary's interruption along the path p^* for a segment k; it equals the baseline physical protection system performance according to EASI model	*adim.*
$P(T)$	Threat probability/ probability of the attack to a chemical facility	*adim.*
PSF	Performance shaping factor	*adim.*
q	Number of path for each segment k	*adim.*
r	Discount rate	*adim.*
R	Security risk	€
R_{IED}	Reliability of improvised explosive device	*adim.*
t	Number of targets included in adversary's action	*adim.*
t_G	Mean response force time	*s*
t_i	Mean delay time	*s*
T	Threats scenarios	*adim.*
$T1$	Severity category included in an expected scenario indicating a catastrophic accident	*adim.*
$T2$	Severity category included in an expected scenario indicating a critical accident	*adim.*
$T3$	Severity category included in an expected scenario indicating a marginal accident	*adim.*
$T4$	Severity category included in an expected scenario indicating a negligible accident	*adim.*
v	Combination of security measures (including also single security upgrades)	*adim.*

Symbol	Definition	Unit
v^*	Most profitable combination of security measures derived from Cost-effectiveness analysis	*adim.*
ve	Adversary velocity during running	*m/s*
w	Number of security measures combinations	*adim.*
x_v	Subscript for Knapsack problem formulation (i.e., Cost-effectiveness analysis)	*adim.*
z	Number of years the security measure will be operating	*n° year*
$\overline{\Delta\eta_i}$	Overall effectiveness improvement (EM-PICTURES nomenclature); term indicated with no accent and subscript elsewhere	*adim.*
$\Delta\eta_{ik}$	Effectiveness improvement due to the introduction of a generic security measure i in the existing physical protection system along a generic segment k; named elsewhere as risk reduction. Reported elsewhere as $\Delta\eta$.	*adim.*
η_{PPS}	Physical protection system effectiveness (generic)	*adim.*
$\eta_{PPS,new\ ik}$	Upgraded physical protection system effectiveness, in presence of each additional (i.e., "new") security measure i along segment k	*adim.*
$\eta_{PPS,old\ k}$	Baseline physical protection system effectiveness, before the addition of a security measure along a segment k. Indicated elsewhere with η_{PPS}; see equation (18).	*adim.*
φ_k	Reduction velocity factor due to additional weight carried by the adversary for a segment k	*adim.*

7 References

Ackerman, F., & Heinzerling, L. (2002). Pricing the Priceless: Cost-Benefit Analysis of Environmental Protection. *University of Pennsylvania Law Review*, *150*(5), 1553. http://doi.org/10.2307/3312947

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

Alibi. (2016). 3.0 Megapixel 100' IR IP Outdoor Bullet Security Camera - Technical and commercial datasheet. Retrieved March 20, 2017, from http://www.supercircuits.com/alibi-megapixel-day-night-ir-ip-outdoor-security-camera-ali-ipu3130r

ARIA. (2015). Accident study findings on malicious acts perpetrated in industrial facilities. Retrieved March 20, 2017, from http://www.aria.developpement-durable.gouv.fr/wp-content/uploads/2015/10/2015-10_01_SY_accidentologie_Malveillance_PA_FINAL_EN.pdf

Associated Press. (2015). French minister says double plant blast was criminal act. Retrieved March 20, 2017, from http://bigstory.ap.org/article/1f9382f079764ac0a68b72d94bab4968/french-minister-says-double-plant-blast-was-criminal-act

Aven, T. (2007). A unified framework for risk and vulnerability analysis covering both safety and security. *Reliability Engineering & System Safety*, *92*(6), 745–754. http://doi.org/10.1016/j.ress.2006.03.008

Bajpai, S., & Gupta, J. P. (2007). Terror-Proofing Chemical Process Industries. *Process Safety and Environmental Protection*, *85*(6), 559–565. http://doi.org/10.1205/psep06046

BBC News. (2015a). France attack: as it happened. Retrieved March 20, 2017, from http://www.bbc.com/news/live/world-europe-33287095

BBC News. (2015b). France explosions: Devices found near Berre l'Étang plant. Retrieved March 20, 2017, from http://www.bbc.com/news/world-europe-33537345

BMT. (2016). Average cost of construction in Australia - Technical and commercial datasheet. Retrieved March 20, 2017, from http://www.bmtqs.com.au/construction-cost-table

Broder, J. F., & Tucker, E. (2012). *Risk analysis and the Security Survey* (Fourth Ed). Burlington, MA, USA: Elsevier Butterworth-Heinemann.

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

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

CCPS - Center for Chemical Process Safety. (2008). *Guidelines for Chemical Transportation Safety, Security, and Risk Management*. New York, USA: American Institute of Chemical Engineers (AIChE).

Cropper, M., & Sahin, S. (2009). Valuing mortality and morbidity in the context of disaster risks. *World Bank Policy Research Working Paper*, (February), 4832–4877. http://doi.org/10.2139/ssrn.1344717

DHS - US Department of Homeland Security. Chemical Facility Anti-Terrorism Standards (CFATS) - Risk-Based Performance Standards (RBPS) (2007). Washington, DC, USA.

Engineering ToolBox. (2017). Liquid densities. Retrieved March 20, 2017, from http://www.engineeringtoolbox.com/liquids-densities-d_743.html

European Commission. (2008). Sixth Framework Programme on Transnational Terrorism, Security and the Rule of Law, Deliverable 5, Workpackage 3, Concepts of Terrorism: Analysis of the Rise, Decline, Trends and Risk. *Transnational Terrorism, Security & the Rule of Law*.

Eurostat. (2016). Electric prices for industrial consumers, second half 2014. Retrieved March 20, 2017, from

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

Friedman, S. M. (2017). The inflation calculator. Retrieved March 20, 2017, from http://www.westegg.com/inflation/

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

Garcia, M. L. (2007). *The Design and Evaluation of Physical Protection Systems* (Second Ed). Burlington, MA, USA: Elsevier Butterworth-Heinemann.

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*(4), 434–438. http://doi.org/10.1016/j.jlp.2009.02.008

Get A Quote. (2016). Concrete wall and footing price estimation. Retrieved March 20, 2017, from http://www.get-a-quote.net/quickcalc/concrete.htm

Grainger. (2016). Security doors and frames - Technical and commercial datasheet. Retrieved March 20, 2017, from http://www.grainger.com/category/security-doors/door-and-door-frames/security/ecatalog/N-b6c

Hansson, S. O. (2007). Philosophical Problems in Cost–Benefit Analysis. *Economics and Philosophy*, *23*(2), 163. http://doi.org/10.1017/S0266267107001356

HSE - Health and Safety Executive. (2016). Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions. Retrieved March 20, 2017, from http://orr.gov.uk/__data/assets/pdf_file/0018/18009/revised-safety-cba-guidance-05022016.pdf

ISO31000:2009. Risk management - Principles and Guidelines (2009). Geneva, Switzerland.

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

Kelman, S. (1981). Cost-benefit analysis: an ethical critique. *Across the Board*, *18*(7), 74–82.

Khakzad, N., & Reniers, G. L. L. (2015). Cost-effective allocation of safety measures in chemical plants w.r.t land-use planning. *Safety Science*, 1–8. http://doi.org/10.1016/j.ssci.2015.10.010

Landucci, G., Reniers, G. L. L., 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. http://doi.org/10.1016/j.ress.2015.03.004

Le Guernigou, Y., & Revilla, F. (2015). Criminal intent seen in petrochemical fire on French Bastille Day. Retrieved March 20, 2017, from http://uk.reuters.com/article/2015/07/14/uk-france-fire-intent-idUKKCN0PO0S420150714

Le Huffington Post. (2015). Bouches-du-Rhône: incendie sur le site pétrochimique LyondellBasell à Berre-l'Étang. Retrieved March 20, 2017, from http://www.huffingtonpost.fr/2015/07/14/incendie-bouches-du-rhone-berre-letang-petrochimie-plan-orsec_n_7790400.htm

Le Sage, T. (2013). Scenario based risk assessment. Retrieved March 20, 2017, from www.jdibrief.com

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*(1), 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). Wroclaw, Poland.

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*(4), 306–325. http://doi.org/10.1504/IJCIS.2012.050106

Moteff, J. (2005). *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences*. *Science And Technology*. Washington, DC, USA.

Nolan, D. P. (2008). *Safety and Security Review for the Process Industries* (Second Ed). Amsterdam, The Netherlands: Elsevier.

OPEC. (2014). Annual Statistical Bulletin of Oil and Gas 2014 - World Output of Refined Petroleum Products by Country. Retrieved March 20, 2017, from http://www.opec.org/library/Annual Statistical Bulletin/interactive/current/FileZ/Main-Dateien/Section3.html

Paltrinieri, N., Bonvicini, S., Spadoni, G., & Cozzani, V. (2012). Cost-Benefit Analysis of Passive Fire Protections in Road LPG Transportation. *Risk Analysis*, *32*(2), 200–219. http://doi.org/10.1111/j.1539-6924.2011.01654.x

Pardini, S. (2016). Berre l'Etang - Feux à LyondellBasell un homme écroué. Retrieved March 20, 2017, from http://www.laprovence.com/article/faits-divers-justice/4000586/feux-a-lyondellbasell-un-homme-ecroue.html

PayScale. (2016). Salary Comparison, Salary Survey, Search Wages. Retrieved March 20, 2017, from http://www.payscale.com/

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

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

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*(6), 583–589. http://doi.org/10.1016/j.psep.2013.04.002

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

Reniers, G. L. L., & Brijs, T. (2014b). Major accident management in the process industry: An expert tool called CESMA for intelligent allocation of prevention investments. *Process Safety and Environmental Protection*, *92*(6), 779–788. http://doi.org/10.1016/j.psep.2014.02.003

Reniers, G. L. L., & Sörensen, K. (2013a). An Approach for Optimal Allocation of Safety Resources: Using the Knapsack Problem to Take Aggregated Cost-Efficient Preventive Measures. *Risk Analysis*, *33*(11), 2056–2067. http://doi.org/10.1111/risa.12036

Reniers, G. L. L., & Sörensen, K. (2013b). Optimal allocation of safety and security resources. *Chemical Engineering Transactions*, *31*, 397–402. http://doi.org/10.3303/CET1331067

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*(1), 72–83. http://doi.org/10.1002/prs.11683

RFI News. (2015). French chemical plant blaze may have been deliberate. Retrieved March 20, 2017, from http://www.english.rfi.fr/americas/20150714-french-chemical-plant-blaze-may-have-been-deliberate

Richardson Products & Cost Data On Line Inc. (2008). Richardson International Construction Factors Manual. Retrieved March 20, 2017, from http://www.icoste.org/Book_Reviews/CFM-Info.pdf

Shanghai Iven Pharmatech Engineering Co. Ltd. (2016). Fuel storage tank - Technical and commercial datasheet. Retrieved March 20, 2017, from http://www.alibaba.com/product-detail/fuel-storage-tank_60260194681.html?spm=a2700.7724838.14.5.WWRDh0&s=p

Shenzhen P&H Electronic Co. Ltd. (2016). Outdoor fence detector alarm sensor - Technical and commercial datasheet. Retrieved March 20, 2017, from http://www.alibaba.com/product-detail/outdoor-fence-detector-alarm-sensor_60249507350.html?spm=a2700.7724857.35.1.vKQFA2

Stewart, M. G., & Mueller, J. (2008). A risk and cost-benefit assessment of United States aviation security measures. *Journal of Transportation Security*, *1*(3), 143–159. http://doi.org/10.1007/s12198-008-0013-0

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), 1–24. http://doi.org/10.2202/1547-7355.1837

Stewart, M. G., & Mueller, J. (2012). Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Critical Infrastructure Protection. In *5th International Conference on Reliable Engineering Computing* (pp. 513–534). http://doi.org/10.1080/03071847.2012.714212

Stewart, M. G., & Mueller, J. (2013). Terrorism Risks and Cost-Benefit Analysis of Aviation Security. *Risk Analysis*, *33*(5), 893–908. http://doi.org/10.1111/j.1539-6924.2012.01905.x

Stewart, M. G., & Mueller, J. (2014). A risk and cost–benefit analysis of police counter-terrorism operations at Australian airports. *Journal of Policing, Intelligence and Counter Terrorism*, *9*(2), 98–116. http://doi.org/10.1080/18335330.2014.940816

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

The Council of the European Union. Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, 8 December Official Journal of the European Union 75–82 (2008).

TNO. (2005). *The "Purple book" – Guidelines for quantitative risk assessment, CPR 18 E. Publication Series on Dangerous Substances (PGS 3)*. The Hague, Netherlands: Commitee for the Prevention of Disasters.

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

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. http://doi.org/10.1023/A:1025598106257

Wang, D., & Kim, J. (2015). Asia Naphtha & LPG Report. Retrieved March 20, 2017, from http://www.opisnet.com/Images/ProductSamples/AsiaNaphtha-sample.pdf

X-Rates. (2016). Currency Calculator (US Dollar, Euro). Retrieved March 20, 2017, from http://www.x-rates.com/calculator/

Appendix A. Cost categories and calculations

A.1. Cost categories

The cost categories, subcategories and formula to assess the overall annual cost derived from the implementation of a security measure *i*, according to Module (3) of EM-PICTURES, have been reported in Table A.1. Further information on cost assessment is reported in Section 2.4.

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	$C_{OPERATION,O}$	**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}	$C_{FA} \cdot P(FA)$
		Site-specific costs	C_{SITE_SP}	-

Key			
Symbol	**Definition**	**Symbol**	**Definition**
A_{office}	*Total office area* (m^2)	$C_{E,i}$	*Price for unit of equipment i* $\left(\frac{€}{unit}\right)$
C_{COMM}	*Cost of communication (e.g., post, phones, mails, etc…)* (€)	C_{FA}	*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* (€)
$C_{Space,i}$	*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)*
$P(FA)$	*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* $\left(\frac{€}{h \cdot person}\right)$		

Table A.1. Overview on Overall annual cost estimation for a generic security measure.

A.2. Cost calculations

Cost calculations have been carried out for each of the five PPS upgrades proposed in the case study, according to the categories, subcategories and formula proposed in Table A.1. 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.

Indeed, several data regarding cost calculation have been retrieved in U.S.A. dollars of year 2016; the conversion rate from U.S.A. dollars to € has been assumed 0.8683 $€/U.S.A.$ \$ (X-Rates, 2016) throughout the case study. Moreover, a location factor of 1.13 (Richardson Products & Cost Data On Line Inc., 2008) was applied in order to adjust US prices and salaries to those of France. 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 process facility, have been 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 has been retrieved from vendor websites for each security upgrade and reported in Table A.2.

UPGRADE ID	***DATA FOR THE CALCULATION OF EQUIPMENT COSTS***			
	Description	***Unit***	***Value***	***Reference/Notes***
	Cost of a couple of fence sensors (i.e., unit cost)	$€/unit$	20	(Shenzhen P&H Electronic Co. Ltd, 2016)
	Total number of fence sensors in place	$n°units$	575	8% of spare items not included
B	Length and height of the concrete wall, with footings	m	5750; 3	Layout of the facility
	Cost of the wall (according to these specifications)	€	13530	(Get A Quote, 2016)
C	Number of cameras for each operative (*) and dismissed (**) tank	$n°units/tank$	2 (*); 1 (*)	-
	Cost of an outdoor camera	$€/unit$	178	(Alibi, 2016)
	Total number of cameras in place	$n°units$	74	8% of spare items not included
D	Number of couples of small tanks	$n°units\ type\ 1$	15	Layout of the facility
	Number of major tanks	$n°units\ type\ 2$	10	Layout of the facility
	Length and height of the concrete wall around unit type 1 (*) and unit type 2 (**)	m	600 (*); 650 (**); 3	Layout of the facility
	Cost of the wall for each unit (type 1 (*) and type 2 (**))	$€/unit$	1412 (*); 1530 (**)	(Get A Quote, 2016)
	Cost of security doors to be applied on each unit (both type 1 and type 2)	$€/unit$	1000	(Grainger, 2016)
E	Unit cost for the new building (standard warehouse with concrete floor and metal clad)	$€/m^2$	548	(BMT, 2016)
	Area of the building	m^2	50	Layout of the facility

Table A.2. Data for the calculation of Equipment costs for five different PPS upgrades.

In the calculation of Operating costs, Utility costs consist of the costs of annual electric power consumption, which are significant only for upgrades A and C. For both the upgrades the power has been calculated through the standard power law, retrieving data on intensity and voltage from products datasheets (Alibi, 2016; Shenzhen P&H Electronic Co. Ltd, 2016) and accounting the number of devices in place, which have been assumed to be working continuously all the yearlong. The estimated annual electric power consumption has been $9.07 \cdot 10^3 kWh$ for upgrade A and $3.89 \cdot 10^3 kWh$ for upgrade C. Considering an average industrial electric energy market price in France of $0.095\ €/kWh$ (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 of the security countermeasures, which was not negligible for upgrade A and C. It should be noted that for security upgrades B and D, which are walls in different position, this subcategory is equal to zero. For upgrade E the guards have been just relocated, so no additional human resources operating costs have been accounted in comparison with the baseline situation.

In the calculation of Maintenance, inspection and sustainability costs the following assumptions have been applied for each security upgrade: material costs have been estimated by assuming an annual substitution rate for equipment and other materials in the range between 3% and 5%, 2 scheduled maintenances, 1 unscheduled maintenances and 2 scheduled inspections per year have been accounted. License and renewal costs appeared to be negligible for all the five upgrades. Other running costs have been calculated for each security upgrade; only for upgrade E 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 and C). For both these upgrades, despite a single false-alarm cost, according to expert judgement, is about $2.80 \cdot 10^3$ € and $P(alarm \mid no\ attack) = 0.143$ (Garcia, 2007), assuming the probability of the attack unitary turn false-positive costs to zero. Nevertheless, 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 and exit doors.

For each of the six security upgrades, the main results obtained from cost calculations, according to the six cost categories of EM-PICTURES, as well as the Overall costs ($C_{Security,i}$) have been illustrated in Table A.3.

CALCULATION OF OVERALL COSTS ($C_{Security,i}$)			**UPGRADE A**	**UPGRADE B**	**UPGRADE C**	**UPGRADE D**	**UPGRADE E**
Symbol	***Description***	***Unit***	***Value***	***Value***	***Value***	***Value***	***Value***
$C_{INITIAL,OV}$	***1. Overall initial costs***	€	1.18E+04	2.20E+03	1.13E+04	2.20E+03	5.29E+03
$C_{INSTALL,OV}$	***2. Overall installation costs***	€	1.62E+04	1.77E+04	1.76E+04	6.48E+04	3.90E+04
$C_{OPERATION,OV}$	***3. Overall operating costs***	€	4.17E+03	0	2.69E+04	0	0
$C_{MIS,OV}$	***4. Overall maintenance, inspection & sustainability costs***	€	2.95E+03	1.54E+03	2.86E+03	2.98E+03	2.57E+03
$C_{OR,OV}$	***5. Other running costs***	€	1.80E+02	2.80E+02	1.80E+02	2.80E+02	8.75E+03
$C_{SPEC,OV}$	***6. Overall specific costs***	€	4.00E+02	1.00E+03	4.00E+02	1.00E+03	1.00E+03
$C_{Security,\ i}$	***Overall costs***	€	**3.57E+04**	**2.27E+04**	**5.91E+04**	**7.13E+04**	**5.66E+04**

Table A.3. Calculation of Overall annual costs for five 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 costs.

Appendix B. Benefit categories and calculations

B.1. Benefit categories

The benefit categories, subcategories and formula to assess the overall annual benefits (i.e., avoided losses) derived from the occurrence of a generic accidental scenario *j*, according to Module (4) of EM-PICTURES, have been reported in Table B.1. Further information on benefit assessment is reported in Section 2.5.

Benefit modelling for a generic scenario				
Benefit category	**Symbol**	**Benefit subcategory**	**Symbol**	**Expression**
SUPPLY CHAIN BENEFITS	$B_{SUPC,OV}$	**Production loss benefits**	B_{PL}	$Q \cdot t_{PS} \cdot Pr_U$
		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	$B_{DAMAGE,OV}$	**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	$B_{D,PM\&P}$	$H + I + J$
LEGAL BENEFITS	$B_{LEGAL,OV}$	**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 BENEFITS	$B_{INS,OV}$	**Insurance premium benefits**	$B_{P,INS}$	$P_F \cdot I_{PF}$
HUMAN AND ENVIRONMENTAL BENEFITS	$B_{H\&E,OV}$	**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 damage benefits	B_E	$m_{SP} \cdot C_{SP}$
INTERVENTION BENEFITS	$B_{INTV,OV}$	**Intervention benefits**	-	$F_{INT} + P_{INT} + A_{INT} + S_{INT}$
REPUTATION BENEFITS	$B_{REPT,OV}$	**Share price benefits**	B_{SP}	$M_{REP} \cdot D_{REP}$
OTHER BENEFITS	$B_{OTH,OV}$	**Manager work-time benefits**	B_{MWT}	$\sum_{i=1}^{t} w_i \cdot h_i \cdot n_i$
		Cleaning benefits	B_{CLN}	$w_c \cdot h_c \cdot n_c$
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* (€)	A_{INT}	*Ambulance service costs charged to the company* (€)
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_{SI}	*Cost of one serious injured worker* $\left(\frac{€}{person}\right)$
C_{SP}	*Cost per unit of product 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* (€)

Table B.1. Overview on annual Overall benefits estimation for a generic accidental scenario.

Key			
Symbol	**Definition**	**Symbol**	**Definition**
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* $\left(\frac{€}{delay \cdot day}\right)$	F_{INT}	*Fire department costs charged to the company* (€)
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* (€)	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}	*Amount of product 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_{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* (€)	P_{INT}	*Police department costs charged to the company* (€)
P_P	*Probability of losing operating permit* (%)	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* (€)
S_{INT}	*Special units costs charged to the company* (€)	t	*Number of employees categories*
t_D	*Duration of reduced production during reactivation* (h)	t_{PS}	*Duration of the stop in production* (h)
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* $\left(\frac{€}{day \cdot lawyer}\right)$		

Table B.1. (continued). Overview on annual Overall benefits estimation for a generic accidental scenario.

B.2. Benefits calculations

Benefits calculations have been carried with respect to the three scenarios considered in the case study (i.e., realistic, worst-case and expected scenario), according to the categories, subcategories and formula proposed in Table B.1. The description of the three scenarios has been reported in Table B.2.

In the calculation of Supply chain benefits, a realistic production rate for the facility has been estimated by assuming $1/10$ of the overall national French oil derivatives production in 2013 that is $1.26 \cdot 10^6\ barrel/day$ (OPEC, 2014); for the conversion into mass flow rate a reference density for naphtha has been considered (Engineering ToolBox, 2017). The estimated production rate for the facility has been $4.17 \cdot 10^5\ kg/h$, with a profit per unit sold that is the market price equal to $4.08 \cdot 10^{-4}$€ (Wang & Kim, 2015). For Schedule benefits, the fine for a cancelled contract has been assumed, based on expert judgment, $1.00 \cdot 10^5\ €/contract$ and the fine for delay in deliveries per day, $1.00 \cdot 10^4\ €/(delay \cdot day)$.

SCENARIO ID / BENEFITS	REALISTIC	WORST-CASE	EXPECTED			
			T1 **Catastrophic accident**	**T2** **Critical accident**	**T3** **Marginal accident**	**T4** **Negligible accident**
			Probability of occurrence (P(T))			
			5.00E-04	4.00E-01	5.55E-01	4.95E-02
	Description					
1. Overall supply chain benefits	No stop in production; 20% activity slowed for 13 hours (emergency intervention time); fines for delays in deliveries	Stop in production for 24 hours; 0% production rate at reactivation; 48 hours start-up; fines for delays in deliveries and 2 orders cancelled	Stop in production for few hours; delays in the supply chain	Production slowed for few hours; delays in the supply chain	Negligible	
2. Overall damage benefits	Two tanks completely destroyed, damage to piping	6 tanks destroyed with content; severe damage to piping; severe damages to other company's and public properties; severe damage to surrounding living areas	Two tanks completely destroyed and other assets damages.	Two tanks damaged (20%) ; minor other assets damages	Minor damages to 2 tanks (3%)	
3. Overall legal benefits	Civil liability fine for pollution; lawyers' wages; 50% increase of the Security budget; very improbable closing down (10^{-5}%)	Civil liability fine for pollution; lawyers' wages; 80% increase of the Security budget; possible closing down (10%)	Fines; salaries; 50% increase of Security budget	Fines; salaries; 30% increase of Security budget	Fines; salaries; 8% increase of Security budget	
4. Overall insurance benefits	0.1% premium increase	10% premium increase	0.1% premium increase.	10^{-2}% premium increase	10^{-3}% premium increase	
5. Overall human and environmental benefits	No casualties and injuries; content of the two tanks burnt	3 casualties; 4 serious injuries and 8 light injuries; several new recruitments; content of the six tanks burnt; severe environmental damages	2 serious injuries; 4 light injuries; environmental damages	1 light injury; marginal environmental damages	Negligible	
6. Overall intervention benefits	Significant emergency intervention	Massive Emergency intervention, with special units	Critical	Marginal	Negligible	
7. Overall reputation benefits	10^{-4}% expected drop in the share-price	1% expected drop in the share-price	10^{-4}% share price drop	$5 \cdot 10^{-5}$% share price drop	10^{-5}% sh are price drop	
8. Other benefits	Manager work-time benefits and cleaning benefits	Significant manager work-time benefits and cleaning benefits	Critical	Marginal	Negligible	
9. Overall specific benefits	Airport and traffic delays; limited immaterial consequences	Severe airport and traffic delays; relevant immaterial consequences	Critical	Marginal	Negligible	

Table B.2. Description of the scenarios applied in the case study for benefit assessment: realistic scenario, worst-case scenario and expected scenario. Realistic benefits indicate the actual losses sustained in the terroristic attack. Expected benefits have been calculated as the average of four possible outcomes weighted by respective probabilities of occurrence. Worst-case and T1 benefits are coincident. Vulnerability probabilities are considered unitary.

In the calculation of Damage benefits, illustrative commercial equipment costs for storage tanks have retrieved from vendors (Shanghai Iven Pharmatech Engineering Co. Ltd, 2016): a commercial value of $8.00 \cdot 10^4$ € for 40000 m^3

tank and of $3.00 \cdot 10^4$ € for $10000\ m^3$ tank has been assumed throughout the case study; for the estimation of finished goods damages the same market price has been assumed for both the products (i.e., naphtha and petrol).

In the calculation of Legal benefits and after, it should be noted that, as for costs calculations, many benefits subcategories consist of wages; the expression for converting annual salaries into hourly wages applied has been the same one reported in Appendix A.2. Moreover, also the same values regarding conversion rate from U.S.A. dollars to € and location factor have been applied (Appendix A.2). In the case of Legal benefits, the job profiles involved are junior lawyers and seniors lawyers, specialized lawyers, security manager, security engineer, security analyst and security consultant. The total security budget prior to the accident has been assumed, based on expert judgment, $8.00 \cdot 10^4$ €, but the percentage increase of the security budget after the accident is different for the three scenarios considered, depending on consequences severity.

In the calculation of Insurance benefits, the value of the current total premium cost of the facility has been considered, based on expert judgment, $5.00 \cdot 10^7$€, while the percentage increase of the premium due to the accident is scenario dependent. In the calculation of Human benefits, the value of a statistical life (VSL) has been retrieved from a previous study (Viscusi & Aldy, 2003) and converted from $U.S.A.\$(2000)$ into €(2016) by the application of appropriate conversion rate (X-Rates, 2016) and inflation rate (Friedman, 2017); the final VSL is $7.07 \cdot 10^6$€. Following the same reference and approach, the monetary values for a light and a serious injury are respectively $1.41 \cdot 10^4$ € and $2.06 \cdot 10^5$ €.

In the calculation of Intervention benefits, a different flat rate has been assumed for the three scenarios. In the calculation of Reputation benefits, a current total market price for the company of $3.84 \cdot 10^{10}$€ has been accounted, but the expected percentage drop is scenario dependent. In the calculation of Other benefits, wages for security manager and cleaning employees have been accounted, while in the estimation of Specific benefits, transportation delays costs and psychological counselling for accident witnesses have been considered.

Eventually, all the benefit numerical values have been determined accordingly to the pertinent 9 categories of EM-PICTURES, up to Overall benefits $(C_{Loss,j})$, for each of the three scenarios considered (Table B.3).

CALCULATION OF OVERALL BENEFITS $(C_{Loss,j})$			**REALISTIC SCENARIO**	**WORST - CASE SCENARIO**	**EXPECTED SCENARIO**
Symbol	***Description***	***Unit***	***Value***	***Value***	***Value***
$B_{SUPC,OV}$	***1 . Overall supply chain benefits***	**€**	2.04E+04	3.87E+05	2.07E+04
$B_{DAMAGE,OV}$	***2. Overall damage benefits***	**€**	1.29E+05	5.23E+05	6.61E+04
$B_{LEGAL,OV}$	***3. Overall legal benefits***	**€**	8.56E+04	1.18E+06	5.69E+04
$B_{INS,OV}$	***4. Overall insurance benefits***	**€**	5.00E+04	5.00E+06	2.53E+04
$B_{H\&E,OV}$	***5. Overall human and environmental benefits***	**€**	7.50E+04	2.24E+07	2.47E+05
$B_{INTV,OV}$	***6. Overall intervention benefits***	**€**	5.00E+03	3.00E+04	3.99E+03
$B_{REPT,OV}$	***7. Overall reputation benefits***	**€**	3.84E+04	3.84E+08	2.18E+05
$B_{OTH,OV}$	***8. Other benefits***	**€**	1.06E+03	9.94E+03	8.12E+02
$B_{SPEC,OV}$	***9. Overall specific benefits***	**€**	1.30E+04	5.50E+04	6.64E+03
$C_{Loss,\ j}$	***Overall benefits***	**€**	**4.17E+05**	**4.14E+08**	**6.46E+05**

Table B.3. Overall annual benefits results for different scenarios: realistic benefits, worst-case benefits and expected benefits. The calculation of Overall benefits has been carried out as the sum of nine main categories: (1) Overall supply chain benefits, (2) Overall damage benefits, (3) Overall legal benefits, (4) Overall insurance benefits, (5) Overall human and environmental benefits, (6) Overall intervention benefits, (7) Overall reputation benefits, (8) Other benefits, (9) Overall specific benefits.