CHEMICAL ENGINEERING TRANSACTIONS

VOL. 53, 2016

A publication of AIDIC

The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Valerio Cozzani, Eddy De Rademaeker, Davide Manca
Copyright © 2016, AIDIC Servizi S.r.l.,
ISBN 978-88-95608-44-0; **ISSN** 2283-9216

DOI: 10.3303/CET1653018

Application of Cost-Benefit Analysis for the Selection of Process-Industry Related Security Measures

Valeria Villa*[a], Genserik L.L. Reniers[b], Valerio Cozzani[a]

[a]LISES – DICAM, Alma Mater Studiorum – Università di Bologna, via Terracini 28, 40131 Bologna, Italy
[b]Safety and Security Science Group, TPM Faculty, Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands
valeria.villa4@unibo.it

In the last few years, several accidental events have highlighted the importance of major manmade hazards, either accidental or deliberate by nature, within chemical and process facilities. Moreover, many plants are located in unstable geo-political areas, where the risk of major accidents triggered by external factors, such as terroristic attacks or sabotages, is not negligible. Hence, intentional risks should be investigated by proper risk assessments, included in the risk picture and reduced by applying adequate security measures. Because of the increased attention for security issues, optimal selection of security measures, by developing and applying economic analyses, may become more important to reduce plants vulnerability towards intentional malevolent acts, as terroristic attacks and sabotages. Despite economic models, such as cost-benefit analysis for supporting the decision-making process, have proved to be fundamental in many respects with regards to safety, for instance no specific applications of cost-benefit analysis are available in the security domain, within the chemical and process industry context. In this paper, the role of the fundamental terms of cost-benefit analysis within the specific framework of process-industry security is discussed, focusing on the estimation of the threat probability, the assessment of physical security systems costs and performances and the evaluation of the costs of the losses derived from either perspective or retrospective accidental scenarios.

Furthermore, a cost-benefit analysis was applied to an illustrative case study, based on a hypothetical sabotage to a storage tank in a process facility, leading to a major accident. The aim of the case study is to prove that the application of cost-benefit analysis provides an economic aid or criterion for selecting additional security measures in a process plant. Starting from a credible sequence of adversary's actions, the uncertainties related to the threat probability have been accounted and realistic security measures in place have been considered, determining the baseline physical security system performance. Therefore, three pertinent security upgrades have been proposed; for each of them the performances improvement and realistic total costs have been calculated; the losses derived from an expected accidental scenario have been estimated. Then, cost-benefit analysis has been applied proving that it allows defining a rational allocation of security measures. Therefore, we conclude that cost-benefit analysis may offer a relevant support in security risk analysis and its related decision-making process, within the chemical and process industry domain.

1. Introduction

Nowadays the necessity to tackle security threats in chemical and process facilities and hazardous material transportation routes is a relevant matter worldwide, as demonstrated by two security related accidents happened in France in 2015, regarding respectively an attack to a gas production facility (BBC News, 2015) and a sabotage of two oil-derivatives storage tanks (Le Guernigou and Revilla, 2015). Despite the growing attention toward security issues in the chemical and process industry, at European Union level only a general Directive on how to prevent, prepare and respond to terroristic attacks toward critical infrastructures was issued (The Council of the European Union, 2008). No detailed guidelines for security management of chemical enterprises currently exists. According to Reniers et al. (2015), security can be defined as the condition of being protected against the potential danger or loss that can result from the deliberate, malicious, and unlawful acts of others, and security risks assume threats, vulnerabilities and consequences as main components. Security risk assessment within process plants is a systematic approach to collect and organize information regarding the site-specific assets (i.e., people, properties, infrastructures, reputation and information) that need to be protected, the threats that may be posed against those assets, and the likelihood and consequences of malevolent attacks against them (CCPS, 2003). The result of a security risk assessment is a number of consequent actions planning and tracking on the threats tackled by the analysis. Reniers et al. (2015) suggested a unified framework for safety and security risk assessment and related decision-making, considering as key different element between the two domains the risk source that in the safety domain can be considered random, while in the security domain it is the result of a specific intent.

In the past decades, cost-benefit analysis and the specific features of its application to the process safety domain were explored, both for fixed installations (Gavious et al., 2009), and hazardous materials transportation (Paltrinieri et al., 2012). Ongoing research within the process industry addresses economic assessment for safety decision-making in the context of occupational accidents (Reniers and Brijs, 2014a) and major accidents prevention (Reniers and Brijs, 2014b). Economic models for supporting security measures selection, such as cost-benefit analyses, have been applied successfully to other domains (e.g., aviation (Stewart and Mueller, 2013)). Despite the potential of security cost-benefit analysis in establishing competitive business advantage (Reniers, 2014) the mentioned method has not been applied yet for the choice of process-industry related security measures. In the present study, the fundamentals of cost-benefit analysis within process-industry related security framework have been discussed and later an application to an illustrative case study has been presented.

2. Cost-benefit analysis for the selection of security measures in the process industry domain

The general layout of cost-benefit analysis within process-industry related security framework is showed in Figure 1. The economic model includes five main terms: (1) Likelihood of the attack; (2) Effectiveness assessment; (3) Cost assessment; (4) Benefit assessment and (5) Cost-benefit analysis. 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 pertinent hypothetical scenarios. Therefore, it enables the comparison among different security upgrades and guides the choice of those that are economically feasible by means of its outputs (i.e., a set of cost-benefit indicators). The ultimate aim of the analysis is allowing a more rational selection of security measures and supporting the decision-making process, within the context of process industries.

2.1 Likelihood of the attack

The threat probability, or likelihood of the attack (P(T)), expresses the probability of an individual or a group to attack a 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, due to the uncertainties and lack of information on this term, a deterministic approach toward the estimation of the threat probability can be applied: it implies to consider the probability of the attack equal to one. Alternatively, a range of values from 0 to 1 can be accounted in purpose to avoid over-conservative assumption and to obtain a broader set of economic indicators.

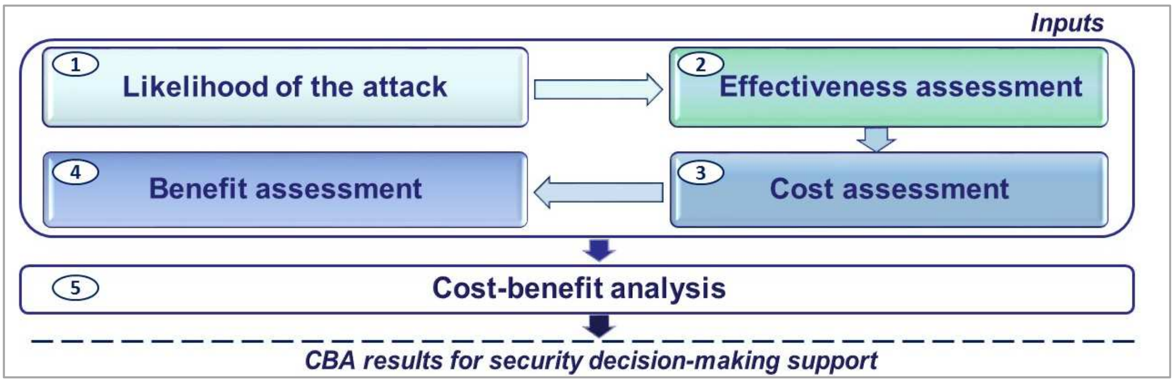

Figure 1: General layout of cost-benefit analysis for process-industry related security measures.

2.2 Effectiveness assessment

Effectiveness assessment is aimed at evaluating the baseline physical protection system performance by site-specific analysis, proposing security upgrades and determining the reduction in risk due to each security measure. A Physical Protection System (PPS) 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, 2007). The principal indicator for the performance of a PPS is its effectiveness, varying from 0 to 1, which expresses the conditional probability of an attacker's path of actions being stopped. Effectiveness assessment should take into account the complex configuration of detection, delay and response function that compose the PPS (Garcia, 2007). Following the assumption of adding one security device at time, risk reduction due to the introduction of a generic security measure i in the existing Physical Protection System can be computed as:

$$\Delta R_i = \eta_{PPS,new\ i} - \eta_{PPS,old}\ \forall i \in \{1,\ldots,n\}, n \in Z \tag{1}$$

Where $\eta_{\mathrm{PPS,new\ i}}$ expresses the probability of attacker's path of actions being stopped in presence of each additional (i.e., "new") security measure i among the possible n security measures. It expresses the upgraded PPS effectiveness. On the other hand, $\eta_{\mathrm{PPS,old}}$ represents the probability of attacker's path of actions being stopped before the addition of a security measure; it has been indicated as baseline PPS effectiveness. Both the terms can be determined by means of a pertinent path-level effectiveness model. EASI model (i.e., Estimate of Adversary Sequence Interruption), developed by Sandia Laboratories (Garcia, 2007), calculates the probability of interruption referred to a sequence of adversary actions aimed at theft or sabotage and it has been applied in the present study.

2.3 Cost assessment

Cost assessment is aimed at evaluating the costs for each risk-reducing security measure i ($\mathrm{C_{Security,i}}$). Cost assessment for a security device should include direct economic costs of applying a security device and indirect costs associated with its use. The Overall annual costs due to the implementation of one generic security measure ($\mathrm{C_{Security,i}}$) can be computed as the sum of six contributions, for each security measure, according to the fundamentals of cost-benefit analysis (Campbell and Brown, 2003) and to a previous study referred to the safety domain for the process industry (Reniers and Brjis, 2014b):

$$C_{Security,i} = \left(C_{INITIAL,OV} + C_{INSTALL,OV} + C_{OPERATION,OV} + C_{MIS,OV} + C_{OR,OV} + C_{SPEC,OV}\right)_i\ \forall\ i \in \{1,\ldots,n\}, n \in Z \tag{2}$$

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

2.4 Benefit assessment

Benefit assessment consists on the definition of the costs derived from a hypothetical accidental scenario. The losses derived from a successful attack 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 infrastructure. Indeed, the losses depend on the selection of the accidental scenario. An expected scenario, which considers the average benefits, weighted by probabilities of occurrence, of different possible outcomes can be considered. 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 Defence, 2000). Similarly to what have been done for cost classification, also benefit categories within the security domain have been developed in analogy with a similar study referred to the safety domain for the chemical and process industry (Reniers and Brjis, 2014b), by outlining nine benefit categories. The Overall benefits derived from a generic accidental scenario ($\mathrm{C_{Loss,j}}$) can be computed as the sum of the nine mentioned contributions, for each scenario j considered in the analysis:

$$C_{Loss,j} = \left(B_{SUPC,OV} + B_{DAMAGE,OV} + B_{LEGAL,OV} + B_{INS,OV} + B_{H\&E,OV} + B_{INTV,OV} + B_{REPT,OV} + B_{OTH,OV} + B_{SPEC,OV}\right)_j\ \forall j \in \{1,\ldots,m\}, m \in Z \tag{3}$$

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

2.5 Cost-benefit analysis

The core of cost-benefit analysis is the calculation of the Net Benefit, or Net Present Value, for each security measure. The calculation allows defining the single security measures i that are economically feasible with reference to a scenario j. Therefore, the expression of Net Benefit proposed by Stewart and Mueller (2013) has been modified with reference to every security measure i and each scenario j:

$$\begin{cases} Net\ Benefit_{ij} = P(T) \cdot C_{Loss,j} \cdot \Delta R_i - C_{Security,i} \\ \qquad \forall i \in \{1, \dots, n\}, n \in Z \\ \qquad \forall j \in \{1, \dots, m\}, m \in Z \end{cases} \tag{4}$$

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. It should be noted that, in order to compare benefits and costs occurring at different points in time, it is necessary to introduce an appropriate discount rate. Therefore, the implementation of a single security measure i is acceptable, with reference to scenario j, if:

$$Net\ Benefit_{ij} \geq 0 \tag{5}$$

Else, it should be rejected. The calculation of Net Benefit$_{ij}$ represents the output of cost-benefit analysis; the analysis should be repeated for each security measure i and for each scenario j.

2.6 Limitations of Cost-benefit analysis

The Cost-benefit analysis presented here in is an empirical model; indeed, it shows some limitations. For instance, it is necessary to retrieve detailed information on the costs of security measures, and the quantification of all the losses derived from a major accident may raise some ethical biases (i.e., monetization of human lives and injuries). Indeed, whenever cost-benefit analysis is applied, it is important to present the analysis in a fully transparent manner, specifying the assumptions made and discussing the uncertainties arisen, for example regarding the likelihood of the attack and definition of scenarios. On the other hand, the application of stricter mathematical models within its main five terms (e.g., game theory for the estimation of the probability of attack success), might over-complicate the analysis, leading at the same time to relevant uncertainties (e.g., adversary tactics in perspective analysis may be very difficultly predicted). Therefore, the application of the present empirical model may be preferred in an industrial and/or regulatory context, because of its understandable constituents and outputs.

3. Application of cost-benefit analysis to an illustrative case study

3.1 Definition of the case study

Cost-benefit analysis was applied to an illustrative case study, inspired by a real incident that took place in summer 2015 in France, consisting in the sabotage of storage tanks in a process facility (Le Guernigou and Revilla, 2015). In the case study, the sabotage of one storage tank containing naphtha has been considered. The tank farm, to which the target belongs, includes 8 atmospheric storage tanks containing naphtha, with a volume of 40,000 m^3 each. The adversary was supposed to carry out the sabotage by foot, starting from cutting the perimeter fence, then running 200 m up to external tank protected area, opening a security door with camera on it, running for 200 m up to the target and placing explosives and detonators on it, in purpose to trigger a major accident. The identification of key protection elements and key distances is necessary to calculate the baseline physical protection system effectiveness. A range of values regarding the likelihood of the attack has been accounted (i.e., 0.01; 0.20; 0.50; 0.75; 1).

Table 1: Effectiveness and cost calculations for three security upgrades

Upgrade ID	Description	Risk reduction	Cost (€)	Prevalent cost category ID and percentage
A	Additional detection sensors at perimeter level	0.3182	$2.509 \cdot 10^4$	Overall installation costs; 41.88 %
B	Additional delay element at target level (i.e., concrete wall with security door)	0.0865	$3.079 \cdot 10^4$	Overall installation costs; 81.54 %
C	Relocation of guards in a closer dispatch	0.4257	$5.734 \cdot 10^4$	Overall installation costs; 68.79 %

Table 2: Scenario definition and expected benefits calculation

Scenario ID	Descriptive word	Description	Probability of occurrence	Overall benefits (€)	Prevalent benefit category ID and percentage
T1	Catastrophic accident	2 fatalities and 8 injuries. Damage and production loss greater than 750,000 €.	$1.000 \cdot 10^{-5}$	$1.843 \cdot 10^{7}$	Human and environmental benefits; 81.75 %
T2	Critical accident	No fatalities and 6 injuries. Damage and production loss between 75,000 € and 750,000 €.	$2.000 \cdot 10^{-1}$	$8.295 \cdot 10^{5}$	Human and environmental benefits; 64.51 %
T3	Marginal accident	A single injury. Damage and production loss between 7,500 € and 75,000 €.	$7.500 \cdot 10^{-1}$	$1.021 \cdot 10^{5}$	Legal benefits; 38.98 %
T4	Negligible accident	No injuries. Damage and production loss below 7,500 €.	$4.999 \cdot 10^{-2}$	$1.936 \cdot 10^{4}$	Legal benefits; 44.61 %

3.2 Effectiveness and cost calculations

The baseline performance of PPS has been evaluated according to EASI model and the results highlighted a rather low value of baseline PPS effectiveness (i.e., 0.1759). Therefore, three security upgrades have been proposed, according to technical references (Garcia, 2007): (A) adding fence sensors as perimeter detection system; (B) adding a delay element by building a concrete wall with security door at sabotage target level; (C) reducing response force time by building a closer guard dispatch. The upgraded value of PPS effectiveness, and therefore the risk reduction index (i.e., ΔR_i) have been calculated for each of the proposed security measures (Table 1).

Cost calculations have been realized for each of the three PPS upgrades proposed in the case study, according to the six main categories mentioned in Section 2.3. Realistic information have been retrieved from vendors' websites. The cost calculations, reported in Table 1, showed that the order of magnitude of the Overall costs is the same one for all the security upgrades. Nevertheless, despite costs distributions are slightly different, according to the security function, installation costs are the prevalent ones for all the three security upgrades.

3.3 Benefit calculations

In the present study, an expected scenario has been considered. Expected benefits are the losses derived from a hypothetical scenario, which considers the average benefits, weighted by probabilities of occurrence, of four possible outcomes, as described in Section 2.4. Illustrative probabilities were defined for each category of scenario and listed in Table 2, together with a description of the losses for each scenario. The Overall expected benefits are $2.436 \cdot 10^{5}$ €. Benefits distribution depends on the scenario selection (Table 2): for catastrophic and critical accidents, the costs due to casualties and injuries are prevailing, while for marginal and negligible accidents, the prevailing losses are related to legal issues and assets damages.

4. Results and discussion

The results of the assessment of the case study consist in cost-benefit analysis results, which are the values of actualized Net benefits, for three PPS upgrades with reference to the expected scenario. Overall costs for each security measure and Overall expected benefits have been made comparable by applying appropriate discount rates (i.e., 3.5 % and 1.5 % respectively (HSE, 2015)) over a 10 year time-span. The latter is a conventional number of operational years for a security measure. Considering several values for the likelihood of the attack, the values of Net Benefit, also named Net Present Value (NPV), have been calculated for each of the three PPS upgrades, according to the expected losses, by applying Eq(4). The values have been compared with respect to the acceptability criteria, expressed by Eq(5). The final results of cost-benefit analysis, reported in Figure 2, prove the coherency of the model, highlighting that the feasibility of all the security upgrades is dependent on the value assumed for the likelihood of the attack. Indeed, all the three upgrades are feasible under the assumption of likelihood of the attack unitary, even if the values of Net Benefit are higher for Upgrades A and C than for Upgrade B. Nevertheless, the results of cost-benefit analysis for different values of the likelihood of the attack show that Upgrade A is feasible even for low values of the likelihood of the attack (i.e., 0.2), while Upgrade C is not. Therefore, the possible suggestion derived from the economic indicators may be to adopt security upgrade A, due to its feasibility even with low probabilities of the attack and to its high Net Benefit under deterministic assumption.

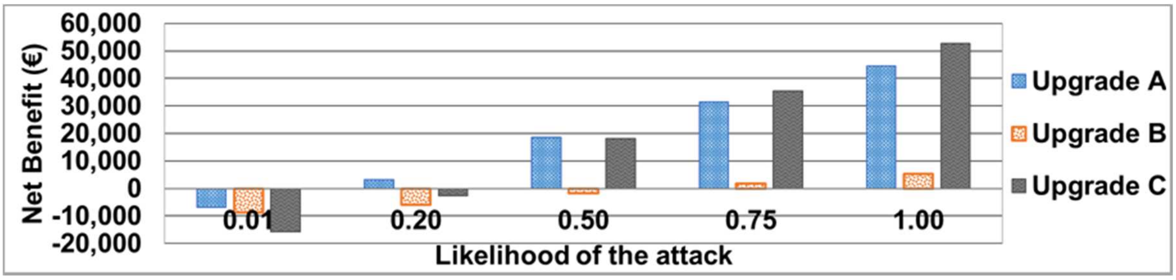

Figure 2: Results of cost-benefit analysis for three security upgrades, with reference to different values of the likelihood of the attack and to an expected scenario.

5. Conclusions

The current contribution has been aimed at discussing the specificities of cost-benefit analysis within the framework of process-industry security and therefore at applying the mentioned economic analysis to an original case study, regarding a sabotage to a storage tank farm. Indeed, the application of cost-benefit analysis provides site-specific answers to security analysts, because it allows evaluating the performance of physical security measures present on-site and proposing several pertinent security upgrades. Indeed, the results of the case study made clear that cost-benefit analysis provides useful insights on the profitable security measures to be adopted in a process facility, by means of its outputs, which are a set of economic security-related indicators. Therefore, cost-benefit analysis outputs provide a sound support to managers and regulators within the decision-making process, and its application may eventually contribute to the reduction of process plants vulnerability toward intentional malevolent acts.

Reference

BBC News, 2015, France attack: as it happened <www.bbc.com/news> accessed 10.03.2016

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

CCPS, 2003, Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites, AIChE, New York, USA.

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

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

HSE, 2015, Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions <www.orr.gov.uk> accessed 10.03.2016

Le Guernigou, Y., Revilla, F., 2015, Criminal intent seen in petrochemical fire on French Bastille Day <www.uk.reuters.com> accessed 10.03.2016

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

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

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

Reniers, G.L.L., 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, 779-788, DOI: 10.1016/j.psep.2014.02.003

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

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

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

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