This item is the archived peer-reviewed author-version of:

A study on the performance assessment of anti-terrorism physical protection systems in chemical plants

Reference:

Argenti Francesca, Landucci Gabriele, Cozzani Valerio, Reniers Genserik.- A study on the performance assessment of anti-terrorism physical protection systems in chemical plants
Safety science - ISSN 0925-7535 - 94(2017), p. 181-196
Full text (Publisher's DOI): <https://doi.org/10.1016/J.SSCI.2016.11.022>
To cite this reference: <https://hdl.handle.net/10067/1415960151162165141>

A study on the performance assessment of anti-terrorism physical protection systems in chemical plants

***Francesca ARGENTI¹, Gabriele LANDUCCI²,
Valerio COZZANI¹, Genserik RENIERS^{3,4}***

*(1) LISES - Dipartimento di Ingegneria Civile, Chimica, Ambientale e dei Materiali,
Alma Mater Studiorum - Università di Bologna, via Terracini n.28, 40131 Bologna, Italy*

*(2) Dipartimento di Ingegneria Civile e Industriale, Università di Pisa, Largo Lucio Lazzarino,
56126, Pisa, Italy*

(3) Safety Science Group, TU Delft, Jaffalaan 5, Delft, The Netherlands

*(4) Engineering Management Department, Research Groups ARGoSS and ANT/OR, University of
Antwerp, Prinsstraat 13, 2000 Antwerp, Belgium*

(*) Author to whom correspondence should be addressed.

tel. (+39)-347-1786523; fax (+39)-051-2090247

e-mail: francesca.argenti@unibo.it

Submitted for publication in:

SAFETY SCIENCE

SPECIAL ISSUE: Editors' Corner 2015

Abstract

The threats originating from deliberate attacks against process and chemical sites where relevant quantities of hazardous substances are stored or processed is a credible one, as confirmed by the attacks carried out in France in the summer of 2015. Although such chemical sites implement multiple layers of protection to address safety-related accidents, they often get behind with providing adequate attention and resources to the protection of assets against external adversaries or, in other words, terrorist threats. The lack of a consolidated practice in the risk-informed implementation of security countermeasures goes hand in hand with the existence of very few rigorous approaches to the effectiveness assessment of security systems, and in particular of physical protection systems (PPSs). The present study addresses the issue of quantitatively assessing the effectiveness of physical security systems adopted to protect process and storage facilities, recognized as high-consequence loss physical assets. To this purpose, the security functions of PPSs were analyzed to guide the selection of performance parameters. Experts from the industry were involved to identify variables and influencing factors relevant to the successful accomplishment of security functions. Experience-based judgments on performance, to be expressed in terms of probabilistic estimates, were also obtained. An insight into the belief that experts hold on the probability of PPSs effectively preventing the success of an external attack and in the identification of critical elements was obtained. The application of the results to the quantitative assessment of the contribution of security controls in reducing vulnerability was also addressed.

Keywords

Physical Security; Process Industry; External terrorist attack; Physical protection system performance assessment

Highlights

- A quantitative assessment of physical security system performance was carried out
- A probabilistic approach to performance assessment was adopted
- Existing effectiveness metrics and expert judgement were combined
- Security experts from the industry were involved to obtain quantitative estimates
- The probability of successful action of security barriers was assessed

1. Introduction

Industrial facilities where relevant quantities of hazardous chemicals are stored or processed may be possible targets of malicious acts of interference and terroristic attacks. Such installations may constitute an attractive target from terrorists' perspective due to the inherent hazard potential that may be exploited to cause a major accident (Argenti et al., 2015), but also due to their economic and strategic importance as critical infrastructures holding systemic interrelationships and interdependencies with many of the relevant sectors of economic activity (European Commission, 2008).

Only after the 9/11 attacks in New York City, the security of sites where relevant quantities of hazardous chemicals are stored or processed became a matter of concern (Baybutt and Reddy, 2003) and thus started to be included in formal risk assessment (Bajpai and Gupta, 2005). The concern raised dramatically in Europe in 2015, following the attacks perpetrated in France against a production site of a chemical company and an oil refinery (ARIA Database, 2015).

Actually, these events showed that industry must address with the greatest urgency the security of such facilities. Objective, performance-based methods need to be applied to verify the adequateness of the resources dedicated to the protection of process and storage sites against external attacks.

Operators of the chemical and process industry may find guidance the assessment and management of security issues in the legislation and in technical standards. In particular, several methodologies to perform a systematic Security Risk Assessment, through characterization of the main components of security risks (namely Threat, Attractiveness, Vulnerability and Consequences), were proposed (e.g. see the methods developed by American Petroleum Institute (American Petroleum Institute, 2013), American Institute of Chemical Engineering (Center for Chemical Process Safety, 2003) and Sandia National Laboratories (Jaeger, 2003)). In addition, principles and guidelines to support the preparation of a facility Security Plan were made available.

The vast majority of these methodologies was developed in USA as a result of the cooperation between the government and industry (often through sector-specific institutions). However, they are now used worldwide and were adopted in the original or in slightly modified versions as corporate standards by several international companies.

These methodologies, although allowing a rather systematic analysis of security risks, lead to a qualitative or, at most, a semi-quantitative assessment (e.g. in the case of API methodology). However, provided that required data are available, in facility vulnerability assessment it would be useful to conduct the analysis of external attack scenarios at a quantitative level. This would allow providing an objective measure of the available level of protection and obtaining a sufficient resolution to identify weak elements and security functions that need improvement. Previous literature study concerning security risks faced by the process industry were devoted to the evaluation of the severity of impacts due to external attacks on process plants (Störfallkommission, 2002; Nolan, 2008; Reniers and Audenaert, 2014) or to the analysis and characterization of the terroristic threat (Keeney and von Winterfeldt, 2010). Bajpai and Gupta proposed semi-quantitative methodologies for application to the Oil&Gas (Bajpai and Gupta, 2007a) and chemical sector (Bajpai and Gupta, 2007b) based on the use of risk factor calculation tables. More recently, Argenti et al. (2015) proposed a semi-quantitative methodology for the attractiveness assessment of chemical facilities. Other contributions investigated the potential of deliberate attacks to trigger domino effects (Reniers et al., 2008; Reniers and Audenaert, 2014; Cozzani et al., 2009; Landucci

et al., 2015), leading to extensive damages due to consequence escalation and to the involvement of multiple units. These studies highlight the importance of an appropriate security management of chemical and process facilities which starts from the adequate selection of security countermeasures with respect to the security functions that have to be guaranteed to protect against credible threats.

In the specific field of Physical Security, the study by (Nunes-Vaz et al., 2011) shed light on the concepts of security functions, security layers and security barriers to be adopted with reference to physical protection systems, thus clarifying the concept of layered security (security-in-depth) and its implications in terms of resource allocation objectives. The more rigorous framework to security-in-depth and the related principles were then applied to provide practical guidance for the design of physical security in complex infrastructures (Nunes-Vaz and Lord, 2014).

Although methodologies and tools are available for the development of security risk assessments and security plans to be implemented at industrial facilities, no specific guidelines on the selection and on the performance assessment of security countermeasures have been established to date. Only general guidance for security risk mitigation and lists of possible solutions in terms of security countermeasures depending on the existing security alert level are provided in the literature (e.g. see Norman (2010)). However, the merits of effectiveness of security countermeasures and the estimation of the effects of their use are not systematically addressed in guidance documents and previous studies concerning process industry installations.

Despite it is generally agreed that a performance-based approach to vulnerability assessment (VA) should be preferred rather than a compliance-based (or feature criteria) approach, and despite quantitative techniques to performance-based VA are recommended for facilities with high-consequence loss physical assets (Garcia, 2006), very few rigorous approaches to the effectiveness evaluation of security systems, particularly physical protection systems (PPSs), were proposed to date. Nonetheless, the urgent concern of securing chemical and process facilities from deliberate external attacks results in an evident need of establishing sound criteria to evaluate measures already in place and, thus, the level of protection provided.

The present contribution addresses the quantitative assessment of the effectiveness of Physical Security Systems (PPSs) currently adopted to protect process and storage facilities, recognized as high-consequence loss physical assets. The study was focused on the analysis of outsiders' attacks, often involving intrusion attempts, that aim to cause direct damage to process and storage equipment, leading to loss of containment, and thus, to the release of hazardous substances that may result in a major accident. More specifically, the analyzed PPS elements were those constituting the *prevention* layer, according to the definition by (Nunes-Vaz et al., 2011). The successful action of this layer requires the coordinated contribution from detection, assessment, alert, delay and response aimed at attack interruption (Nunes-Vaz et al., 2011). The identified security functions of PPSs were thus analyzed to select performance parameters.

Then, experts from the industry were involved to identify variables and influencing factors relevant to the successful accomplishment of the security functions. Expert consultation also allowed obtaining experience-based performance judgments, expressed in terms of probabilistic estimates, that were applied to the assessment of the probability of preventing a successful attack scenario.

Being limited to the experience base of experts who showed their willingness to cooperate in the study, the analysis carried out cannot be considered as fully exhaustive and comprehensive. It was however possible to identify the physical security "typicals" more frequently applied in the chemical and process industry, and to quantitatively characterize their performance in terms of

probability of success in performing the design security function. An extended set of quantitative expert judgment based data that take into account performance variations due to operative conditions was derived. The application of the results to the quantitative assessment of the contribution of security controls in reducing vulnerability was also addressed.

2. Physical protection of process facilities

2.1 The principles of physical protection against external deliberate attacks

In recent years, the definition of strategic objectives to enhance the security of the chemical and process industry was based on the perspective that considers security throughout its timeline from emergence of the threat, through the occurrence of a defined security event, to its effects and downstream consequences. Hence, each security countermeasure may act as a pre-event or as a post-event control and have a contribution to overall risk reduction, as formulated originally by Talbot and Jakeman (2009).

In their study aimed at establishing a more rigorous conceptual framework for physical security, (Nunes-Vaz et al., 2011) accounted for four independent security layers to manage the risk of a terrorist attack against a given facility: deter, prevent, protect and contain. Two of the layers (deter and prevent) target likelihood reduction and focus on stopping the event sequence. If deterrence fails, then prevention is intended to stop the progress of the attack. The other two layers focus on consequence management. Protection manages, and potentially eliminates, the consequences of the attack by putting controls in place prior to the occurrence of damage (Nunes-Vaz et al., 2011). The contain layer is a combination of incident response and consequence management capabilities and actions.

Layers require the coordination of one or more security functions, which synthesize the accomplishment of protection objectives. The layers and functions are implemented by security barriers: a security barrier (also security control or countermeasure) is a physical, procedural, technical, or other device that performs or contributes to one or more security functions. (Nunes-Vaz et al., 2011; Garcia, 2006; Garcia, 2008).

Other authors (Garcia, 2008; Norman, 2010) propose to formalize the effect of security countermeasures by a single parameter, expressing the notion that enhanced security reduces risk by reducing vulnerability. Vulnerability is considered as influencing only the likelihood of a successful attack and the role of security barriers is limited to provide deterrence and prevention, by reducing the attractiveness of the target or by making a successful attack harder to achieve. This view is implicitly accepted in the formulation of the security risk equations adopted in the majority of available SRA methodologies, as those proposed by API (American Petroleum Institute, 2013) and Sandia National Laboratories (Jaeger, 2003). The latter approach was adopted in the present study, with the willingness of maintaining a proactive attitude towards security, focusing efforts on the prevention of potential accidents resulting from attacks, or of attacks themselves, rather than on the mitigation of consequences.

Deterrence function is related to the implementation of measures that are perceived by the potential adversary as too difficult to defeat, which makes the facility an unattractive target and should convince the adversary not to attempt an attack (Nunes-Vaz et al., 2011; Garcia, 2008). Many authors (e.g., Norman, 2010) agreed that caution should be used while attempting to measure and rely on deterrence. Being dependent on adversaries' perceptions, the effectiveness of the deterrence layer is difficult to measure and deterrence may reveal to be useless against adversaries who choose

to attack anyway. Furthermore, to date, there is no statistically valid information to support the effectiveness of deterrents (Garcia, 20006), while the study by Sivarajasingam and Shepherd (1999) provided support elements to the standpoint of questionable effectiveness of deterrence.

Hence, in the present study the security layer represented by deterrence was not analyzed, leading to a conservative analysis, which should be considered as conditional to the assumption that there will be an attack by a given adversary.

In the following, the functions and components of the preventive layer of physical security are illustrated in details. This characterization sets the basis of the quantitative assessment of the overall effectiveness of the system, which in turn represents the aim of the present study.

2.2 Preventive physical security: functions and components

As outlined above, we consider the ultimate objective of a physical protection system (PPS) as to prevent the accomplishment of malevolent actions against assets: the protection function is accomplished by a combination of detection, alarm assessment, alarm communication, delay and response.

In Garcia (2008), the primary security functions of a preventive PPS are identified in detection, delay and response, defined as follows. Detection is the discovery of an adversary action through sensing adversary actions, alarm transmission and alarm assessment. Delay is the slowing down of adversary progress towards the target equipment. In order to contribute to the effectiveness of the PPS, delay must occur after detection otherwise it does not provide additional time to respond. The response function consists of the action taken by the response force to prevent the adversary from reaching and damaging the target.

It is worth clarifying that detection without assessment cannot be considered effective detection, as it does not allow to start an appropriate response action. Intrusion detection technologies, representing the sensing sub-system, and alarm assessment sub-system made up of alarm communication, display and control systems, constitute the building blocks of the detection function. Entry control and contraband detection are included in the detection function as well.

The delay function can be accomplished by different types of items positioned in the path of the adversary: such items include people, perimeter barriers, structural elements, locks, activated delays, deployable barriers and specialized delay elements adopted in high-security sites.

The response force action against an adversary, as intended herein, is immediate and is performed according to the general strategies of denial. A denial strategy can be seen as the best response when protecting critical assets where release of hazardous materials would cause many injuries, deaths or contamination, particularly for capable and determined adversaries. It may consist simply in adversary interruption or in adversary neutralization by means of a force-to-force engagement after interruption.

The direct measure of PPS effectiveness derives from the assessment of the effectiveness measures pertaining to the three functions of detection, delay and response (Garcia, 2008).

2.3 Measuring the performance of physical protection system

In the present study, the metrics for physical protection system effectiveness that was proposed the Sandia Vulnerability Assessment Model was adopted. The Sandia model was developed to address mission-critical military and nuclear facilities but is recommended for every severe consequence that could affect community welfare. It is also notable that Sandia model focuses primarily on terrorist threats rather than on economic crimes or petty criminal threat.

The current Section is devoted to briefly recall the performance variables that were considered in the assessment of a preventive physical protection system, for a more detailed discussion of the Sandia model, the reader is referred to (Garcia, 2006; Garcia, 2008).

The Sandia model makes use of the concept of “timely detection” to measure PPS overall effectiveness. The principle of timely detection states that system effectiveness is measured by the cumulative probability of the detection at the point where there is still enough time remaining for the response force to interrupt the adversary, which is called Probability of adversary interruption P_I and represent the layer effectiveness. Probability of interruption is assessed considering detection, alarm communication, delay and response time:

$$P_I = P_{AssD} \times P_C \times P_T \quad (1)$$

where P_{AssD} is the probability of successful assessed detection of a security breach; P_C is the probability of successful communication to and among response force and P_T is the probability of response force intervening on time to prevent attack success.

The evolution in time of the attack is captured by the overall variable that expresses the probability of timely intervention of the response force (P_T), calculated as function of the penetration time for delay barriers (T_{Di}) that are present along adversary's path towards the target and the response force time (RFT), as shown in Eq. (2) and Eq. (3). In both cases, normal distribution of time parameters are assumed.

$$P_T = \frac{1}{\sqrt{2\pi(\sigma_{RFT}^2 + \sigma_D^2)}} \int_0^T e^{-\frac{T^2}{2(\sigma_{RFT}^2 + \sigma_D^2)}} dT \quad \text{where} \quad (2)$$

$$T = \sum_{i=k+1}^m T_{Di} - RFT > 0 \quad (3)$$

According to a rigorous derivation, P_{AssD} has to be calculated as the cumulative probability of assessed detection along the adversary's path. If a single alarm communication, display and control system is in place at the facility under analysis, assuming that it has the same degree of integration with the sensor systems implemented at the different rings of protection and assuming that all sensor signals are transmitted to the same centralized control room, P_{AssD} can be calculated as

$$P_{AssD} = [1 - \prod_{i=1}^k (1 - P_{D_i})] \times P_{Ass} = P_D \times P_{Ass} \quad (4)$$

where P_{Ass} is the probability of successful alarm assessment and P_{Di} is the probability of detection by the sensor system present at the i -th ring of protection.

It's worth noting that all equations reported above, are to be applied in relation to a specific adversary's path. Pathway analysis consists in determining the ordered series of a potential adversary's actions and locate them on the corresponding areas and perimeters of the site under analysis. Indeed, the previous identification of credible adversary paths towards a potential target equipment item allows to identify which security controls may actually pose an obstacle to adversary progress as they are physically located along the path.

While applying Sandia effectiveness metrics to a quantitative analysis, which is of interest for the present study, the performance variables represent a probability. Such a quantitative assessment has to be supported by the use of reliable quantitative data. Some difficulties were encountered with

respect to this point since it was not possible to retrieve reliable data to quantify all probabilistic variables. The results of performance tests carried at Sandia National Laboratories to support the full-scale application of their vulnerability assessment methodology might provide some baseline for quantification. But, in fact, these data are gathered in Sandia National Laboratories internal reports and provides information at components level for a limited number of technologies finding common application in the military and nuclear sector; moreover, their applicability to industrial sectors, facilities and environments other than those set as test conditions is questionable.

Hence, the authors limited the use of Sandia metric to that of a guideline in the definition of performance variables and, whenever possible, in security controls performance quantification (this is the case for data on the normal distribution of penetration time for delay barriers, derived from field tests and available in (Garcia, 2006)). In fact, the authors resorted to expert consultation to seek quantitative performance estimates.

Section 3 provides the details on the methodological approach followed in this study, evidencing the scope, the objectives and the protocol of expert consultation aimed to the effectiveness assessment of physical protection systems.

3. Methodology

3.1 Overview

The assessment of the effectiveness of security barriers constituting PPSs adopted to secure process facilities was conducted according to a methodological approach that involved the steps illustrated in the flow diagram in Figure 1.

Since investigating the protection offered to high-consequence loss assets against high threat, a performance-based vulnerability assessment approach that privileges quantitative assessment was adopted.

From a methodological point of view, the first issue to be addressed was represented by the definition of a suitable metric for effectiveness assessment and the identification of performance variables that mirror the design functions of a physical protection system applied to prevent the success of malevolent external attacks (step 1 in Fig. 1). As anticipated, the metric developed by Sandia National Laboratories, and illustrated in Section 2.3, was selected as reference.

The investigation was conducted privileging the experience-based evaluation of physical security systems that are actually implemented in process industry facilities, which could hopefully result in practical implications rather than offer a speculative comparison of all available alternatives of security controls that may in theory be picked up to build a PPS. Hence, the involvement of experts from the industry was necessary at different stages of the study. Experts' cooperation concerned the qualitative characterization of security controls (step 2 in Fig. 1), the identification of relevant influencing factors on performance, and the quantitative performance assessment through the estimation of probabilistic variables. Details on the procedure used for experts' consultation are given in Section 3.2.

Influencing factors that have an impact on overall functional performance were at first identified according to a literature review on PPS design and evaluation (Garcia, 2008; Garcia, 2006; Norman, 2010). Then, the results of literature review were validated, and consequently expanded or simplified on the basis of expert judgement in order to establish a set of influencing factors of reference for each physical security barrier applied in industrial practice (step 3 in Fig. 1). In the characterization of influencing factors, only a favorable and an unfavorable state of the considered

variable (representing two mutually exclusive cases) were taken into consideration: the favorable and unfavorable state have to be intended as having a positive impact and a negative impact respectively on the effectiveness in performing the security function for which the security barrier was designed. Although simplified, this choice was made to guarantee consistency with the binary logic applied in the Sandia model and allowed to reduce the burden placed on experts during the performance quantification phase by reducing the number of operational conditions to be analyzed. The probabilistic performance assessment (step 4 in Fig. 1) was carried out starting from the elicitation of performance variables from each involved expert separately (step 4A in Fig. 1). A simplified approach to elicitation was adopted that allowed to limit the number of query variables, especially the number of conditional probabilities to be elicited, as thoroughly described in Section 3.3. Such a simplified approach was preferred also in light of the fact that the quantification may be quite long and demanding, also considering the relatively short time frame allotted for interviews. Single expert estimates were then combined through an equal weighting aggregation scheme in order to provide quantitative performance data in a form suitable for use in the Sandia vulnerability assessment method.

Figure 1: Flow diagram of the methodological approach adopted in the study (PPS = Physical Protection System)

3.2 Protocol for expert consultation

Considering the lack of applicable experimental data and available literature information on the effectiveness of security barriers and controls, the performance quantification study was translated into an expert judgement exercise.

Expert judgment is an approach for soliciting informed opinions from individuals with particular expertise. It is used to obtain a rapid assessment of the state of knowledge about a particular topic. Expert judgement has always played a large role in science and engineering, and it is increasingly recognized as a specific type of scientific data requiring specific methods to treat it.

As it can be seen in Table 1, six experts provided information on the effectiveness of PPS elements applied to secure different types of industrial sites. Although in general the largest possible number of experts should be used, the size of expert pool can be regarded as acceptable considering that Cooke and Goossens (Cooke and Goossens, 2000) identified four as the minimum satisfying number of experts taking part to a study.

The experts to be involved in the study were identified as security managers of companies, security managers of existing industrial sites, sites managers and safety managers having specific security expertise and responsibilities. This selection was made in line with the concept of expertise as intended by O'Hagan et al. (2006): expertise does not only involves having great knowledge of the subject matter, but also having the ability of organizing and using that knowledge.

In the study, only European experts were consulted, hence results should only be considered for Europe and may have limited validity in other countries.

Table 1: List of experts that cooperated and of industrial sites that were analyzed in the study

Expert ID	Position	Analyzed site type	Site Location	Site ID
E.1	Site Security Manager	Chemical Production Site	Europe	Site A
E.2	Company Security Manager	Petrochemical Production Sites (category within company-owned sites)	Europe	Site B
		Isolated large scale petroleum products depots (category within company-owned sites)	Europe	Site C
		Isolated small scale petroleum products depots (category within company-owned sites)	Europe	Site D
E.3	Security Consultant	LNG regasification terminal + shore base	Europe	Site E
E.4	Security Consultant	Chemical Production Site	Europe	Site F
E.5	Site Manager	Seveso plant	Europe	Site G
E.6	Safety Manager	Chemical Production Site	Europe	Site H

As far as the operational process for expert consultation is concerned, a preparation phase preceded the expert elicitation. Besides leading to the selection of experts, the preparation phase served the main objectives of:

- Identifying and listing all target variables to be assessed by experts. This task actually involved the identification, by each expert, of the PPS elements to be considered for the site

under analysis and the selection of the most important factors and variables that affect the performance of PPS functional elements.

- Identifying the query variables. This task was particularly important as it allowed to limit the number of variables left over for expert elicitation.
- Defining the elicitation format document, which specified the exact description of the questions, necessary explanations of each question and the format in which the assessments needed be provided by the experts.

Since the identifying of query variables required direct expert support, the consultation of each expert was actually conducted in three phases. The first, preliminary, phase was aimed to gain insights on what kind of physical security barriers and controls constitute the preventive security layer implemented at the industrial site familiar to the expert; during this phase, each expert was asked to fill in a standardized and comprehensive checklist. The second phase, corresponding to the first part of the interview in person, was devoted to the identification by each expert of the influencing factors or variables that may affect the success of PPS barriers in performing their function. Once these two phases had been completed, the expert elicitation of query variables could start. Elicitation of probabilistic performance variables was carried out according to a simplified approach and supported by the use of a pre-prepared questionnaire tailored on the results of the previous phases of consultation, as explained thoroughly in Section 3.3.

The expert interview process was conducted in accordance to the guidelines provided by Norman (2010). The interview began with the analyst explaining the purpose and the format of the interview and covering the necessary terms of confidentiality; few minutes were also devoted to collect information concerning the interviewee's professional background. Then, the interviewee was focused on the topic by explaining the rationale behind the functional representation of PPS, investigated for what concerns its preventive function with respect to an external attack. Some notions about the Sandia effectiveness metric were given too, to evidence that the coordinated contributions from several interdependent functions (detection, alarm assessment, alarm communication, delay and response) are required to the successful accomplishment of the preventive function.

Before starting the elicitation of query variables, it was explained to the interviewees, who may not be familiar with probability theory, that the probability estimates they were requested to provide were to be understood as subjective probabilities used to express subjective judgements given their background knowledge. In other words, the estimated probabilities have to be interpreted according to Lindley's definition (Lindley, 2006): the probability has to be understood in relation to an uncertainty standard (it is usually identified with the event of drawing a specific ball out from an urn) and the estimation should not being affected by value-judgements. The separation from uncertainty assessment and value-judgement was clearly explained at the beginning of elicitation process and maintained throughout.

During the interview, questions were asked following the prepared questionnaire, one at a time and providing a transition between major topics. Questions were worded clearly, using simple sentences and defining any special term involved in the question.

Following the interview, minutes were drafted summarizing all relevant information and reporting full details of the numerical results of the elicitation phase in the questionnaire template. The minutes of each individual interview were transmitted to the expert for review and approval.

The post-elicitation phase mainly regarded the combination of expert assessments. Herein, an equal weighting aggregation scheme was applied. The simplest weighting scheme was adopted due to the lack of literature data on physical protection systems that might be used as seed variables to determine experts' performance as subjective probability assessors to be translated into global calibration scores to support performance-based weighing of experts. The use of more sophisticated combination techniques (for example, weighed averaging models provided in the framework of the Classical Model (Cooke and Goossens, 2000)) was deemed not suitable as their application requires to ask experts to present their subjective cumulative distributions in terms of 5%, 50%, 95% quantiles, while in the present investigation, point estimates of probability were derived from expert judgement.

The protocol adopted to conduct the expert judgement exercise follows the Procedures Guide provided in (Cooke and Goossens, 2000) up to an extent that the authors deemed satisfactory considering the explorative nature of the present study, taking into account that the investigation does not concern variables and parameters apt to describe physical phenomena or technical systems but probabilities which are not observable quantities. Indeed, although the empirical control of the elicited variables is not guaranteed to date, the following principles that form the basis of a structured expert judgement method according to (Cooke and Goossens, 2000) were respected:

- Scrutability: all data and all processing tools are open to peer review and results must be reproducible by competent reviewers.
- Fairness: experts are not pre-judged.
- Neutrality : methods of elicitation and processing must not bias results.

3.3 Elicitation of probabilistic performance variables

During the elicitation of quantitative PPSs performance estimates, the security barriers that constitute a functional sub-systems were considered one by one, as separate modules. The term "PPS functional sub-system" is herein used to represent a security barrier made up of hardware elements, software elements and/or procedural elements implementing in itself one of the primary function of the preventive PPS. As already mentioned, the experts were asked to identify the most relevant performance influencing factors for each security barrier representing a functional sub-system. Influencing factors were attributed a binary nature, distinguishing only between a favorable and an unfavorable state of the considered variable: the favorable and unfavorable state were intended as having a positive impact and a negative impact respectively on the effectiveness in performing the design security function. This choice was made primarily to guarantee consistency with the binary logic applied in the Sandia model, but also for the sake of simplicity.

The quantification regarded the overall performance variables, as defined according to Sandia effectiveness metric, together with all identified variables and situational factors affecting the performance. In the majority of cases, the influencing factors identified by the experts were considered as independently affecting the successful accomplishment of a security function; when interdependencies needed to be included, they were evidenced and quantitatively characterized through the elicitation of conditional probabilities.

The selection of query variables pertaining to each module was based on the adoption of a simplified approach, which required the elicitation of:

- The marginal probability of occurrence of the favorable state of each influencing factor identified as relevant;

- The conditional probability of the security barrier successfully performing the design security function, given that all identified influencing factors were in favorable state (this was considered as “baseline” to represent the best case in which the functional sub-systems could operate);
- The measure of impact, to be estimated as a multiplicative factor, that each influencing factor has on the “baseline” conditional probability if it changes from the favorable to the unfavorable state.

For the sake of clarity, a sample extract from the questionnaire adopted as elicitation document is provided in Table 2. The example concerns the security function of alarm communication to the response force, performed through the radio communication system. In the specific case, the influencing factors considered are the reliability of coverage of the communication means and the security guards level of training in communication procedures.

Table 2: Example of questionnaire to be used for expert elicitation of quantitative performance data

<i>Factor</i>	<i>Parameters to be elicited</i>	<i>Question for the interview</i>
Reliability of coverage	1 marginal probability	What is the probability of having a reliable coverage of all the facility area (no black spots, continuity of communication, integrity of the communication mean)?
Security guards' level of training in communication procedures	1 marginal probability	What is the probability of the security guards having a HIGH level of training in communication procedures?
Communication to/ among response force	1 conditional probability	What is the probability of having an effective communication to response force, given that all influencing factors are in favorable state? (<i>HIGH reliability of coverage, HIGH level of training in communication procedures</i>)
Reliability of coverage	1 impact measure	What is the impact on the probability of having an effective communication to response force from changing this influencing factor to the unfavorable state and assuming all other influencing remain in a favorable state? (<i>In other words, given HIGH level of training in communication procedure but LOW reliability of coverage</i>)
Security guards' level of training in communication procedures	1 impact measure	What is the impact on the probability of having an effective communication to response force from changing this factor to the unfavorable state and assuming all other influencing factors remain in a favorable state? (<i>In other words, given HIGH reliability of coverage but LOW level of training in communication procedures</i>)

This selection of query variables is suitable to characterize the probability of success of each security barrier given all possible combinations of states of its influencing factors. In fact, the probability of success in performing the design security function is calculated according to Eq. (5):

$$P = P_0 \prod_{i=1}^N (X_i r_i) \quad (5)$$

where N is the number of factors and variables that (independently) affect the performance of the security barrier, P_0 is the baseline conditional probability representing the probability of the security barrier successfully performing its function given that all influencing factors are in the favorable

state (most favorable conditions to success are present), r_i is the measure of the unfavorable impact on the baseline conditional probability P_0 from changing the state of the i -th influencing factor from the favorable state to the unfavorable state and assuming all other influencing factors are still in the favorable state, and $X_i = 1$ if the i -th influencing factor is in its unfavorable state, while $X_i = \frac{1}{r_i}$ if the i -th influencing factor is in its favorable state.

The adoption of this simplified probability calculation method, although not representing a rigorous approach to conditional probabilities derivation and although being constrained by the definition of binary states for influencing factors, allowed the reduction of the number of conditional probabilities to be elicited (few conditional probabilities of first order representing the “baseline” conditional probability for each security barrier were required). Furthermore, this formulation has the main advantage of being easily interpretable by the experts called to provide subjective probabilities, as the influence that factors have on the baseline probability is multiplicative. A scale to translate from a verbal description to a measure of impact (shown in Table 3) was used during the interview to aid the expert in eliciting numerical values to capture impact factors, r_i , on baseline probabilities.

The use of point estimates probabilities rather than of probability distributions is preferred in order to ease the interpretation of the provided estimates and to speed up the elicitation process, also in light of the familiarity that most of the involved experts had with probabilistic assessments. The preference for a simplified approach was motivated by the relatively limited timeframe allotted to the interviews with experts and by the need to limit the number and complexity of probabilistic estimates to be queried, in order not to place a too high cognitive burden on experts that could impair the validity of the effort.

Table 3: Conversion of verbal impact classification to r_i impact factors in Eq. (5)

<i>Verbal description of impact</i>	<i>Value of impact factor r_i</i>
None	1
Small	0.75
Medium	0.5
Significant	0.25
Large	0.1

4. Results and discussion

4.1 Physical security “typicals”

As discussed above, prior to the individual interviews, experts were asked to fill in a checklist which asked to describe the security barriers implemented to prevent the success of deliberate attacks. Thus, the analysis of the answers allowed the identification of the more typical types of security barriers used in a representative set of European industrial sites where relevant quantities of hazardous substances are stored or processed.

Table 4 shows the results of this analysis. In the table, security barriers are listed according to their function. Each row corresponds to an independent module implementing in itself one of the functions of detection, alarm assessment, alarm communication. The table clearly shows that, in almost all cases, roving security guards and employees working on site are relied upon to perform the detection and assessment functions. At large production sites, External Intrusion Detection

System (IDS) based on Video Motion Detection (VMD) and alarm assessment through Closed Circuit Television (CCTV) are often adopted. However, only in few cases the complete coverage of site perimeter with VMD cameras is guaranteed. The response function consists invariably in the deployment of unarmed security guards executed with the support of reliable and redundant communication means. The most diverse solutions are implemented to entry control.

If the results are compared to those in Table 2, it should be noted that the physical protection barriers associated to Site B, Site C and Site D actually represent the physical protection system typically implemented in all sites belonging to a specific category of facilities owned by the same company. In other words, the company applies a specific set of physical security countermeasures on the basis of facility type and size. Therefore, a side remark of the expert interviewed is that the information gathered, even if limited to 3 sites, might actually be representative of a wider set of sites managed by the company interviewed.

As shown in Table 4, procedures to search for contraband material (e.g. explosives, weapons etc.) on people, on vehicles and into baggage are regularly applied at onshore sites where security clearance functions are to be guaranteed to avoid unauthorized access to the offshore unit. On the other hand, contraband detection measures and technologies are not commonly adopted at onshore process or storage facilities: only in a single case, manual search of vehicles entering the site is applied. However, vehicles to be inspected are selected on a random basis. In light of the limited application and of the heterogeneity of contraband detection practices, it was not possible to identify a set of influencing factors on which experts' agreement could be reached. The aggregation of performance data concerning security barriers devoted to the contraband detection function was therefore hindered and is not further discussed.

During the first part of the interviews, consultation was finalized to the identification of the influencing factors or variables that may affect the success of PPS barriers in performing their function. An agreed set of influencing factors for the security barriers representing a PPS functional sub-system was extracted from interviews, and is reported in Table 5. Only the factors that were recognized as relevant by all experts were included in the table.

Despite the fact that experts were interviewed individually, it is worth pointing out that a very good level of agreement was present in the identification of the most relevant factors directly determining and affecting the performance of security barriers, which considerably reduced the loss of information that could have affected the process of limiting the analysis to items on which consensus had been reached.

In the case of entry control systems based on credentials check or biometrics recognition, all experts agreed that the barrier performance could be characterized by assessing the probability associated to the events corresponding to a false accept by the system and to an undetected bypass. Thus, calculating the probability of the union of these two events, the probability of entry control system success could be derived. Query variables for the questionnaire were identified accordingly.

Table 4: Implemented security barriers per site

		Site A	Site B	Site C	Site D	Site E	Site F	Site G	Site H
Detection	External IDS based on VMD	X	X			X	X	X	
	Intrusion detection by roving guards		X	X		X		X	X
	Intrusion detection by employees		X	X		X	X	X	X
	Entry control, supervised automatic credentials check (people)	X	X	X					X
	Entry control, unsupervised automatic credentials check (people)	X				X	X		
	Entry control, manual credentials check (people)		X	X				X	
	Entry control, unsupervised automatic biometrics check (people)				X				X
	Entry control, supervised automatic credentials check (vehicles)		X	X			X		X
	Entry control, manual credentials check (vehicles)	X				X			
	Manual machine -aided contraband detection on people					X			
	Manual machine -aided contraband detection on baggage/ items					X			
	Manual contraband detection for vehicles						X		
Alarm Assessment	Alarm assessment through CCTV system	X	X			X	X	X	
	Alarm assessment by roving guards		X	X		X		X	X
	Alarm assessment by employees		X	X		X	X	X	X
Alarm communication	Communication to/among response force	X	X	X		X	X	X	X

Table 5: Identified security barriers and associated performance influencing factors

Security function	Security barriers	Relevant influencing factors	Favorable state	Unfavorable state
Detection	External IDS based on VMD	Weather conditions	Favorable	Unfavorable
		Installation conditions	Favorable	Unfavorable
		Coverage of detection area	Complete	Partial
		Maintenance and inspection	Sufficiently frequent	Not sufficiently frequent
	Intrusion detection by roving guards	Guards' presence	True	False
		Security guards' level of training	High	Low
	Intrusion detection by employees	Employees' presence	True	False
		Employees' level of security training	High	Low
	Entry control, supervised automatic credentials check (people)	Prevention of false accept	True	False
		Prevention of undetected bypass	True	False
		Security guards' level of attention	High	Low
	Entry control, unsupervised automatic credentials check (people)	Prevention of false accept	True	False
		Prevention of undetected bypass	True	False
	Entry control, manual credentials check (people)	Prevention of false accept	True	False
		Prevention of undetected bypass	True	False
		Security guards' level of training (affecting prevention of false accept)	High	Low
		Security guards' level of attention (affecting prevention of false accept and undetected bypass)	High	Low
		Security guards' workload (affecting guards' level of attention)	Low	High
	Entry control, unsupervised automatic biometrics check (people)	Prevention of false accept	True	False
		Prevention of undetected bypass	True	False
		Presence of anti-bypass sensors	True	False

Security function	Security barriers	Relevant influencing factors	Favorable state	Unfavorable state	
	Entry control, supervised automatic credentials check (vehicles)	(affecting the probability of undetected bypass)			
		Prevention of false accept	True	False	
		Prevention of undetected bypass	True	False	
		Presence of anti-bypass sensors (affecting the probability of undetected bypass)	True	False	
		Security guards' level of attention (affecting the probability of undetected bypass)	High	Low	
	Entry control, manual credentials check (vehicles)	Prevention of false accept	True	False	
		Prevention of undetected bypass	True	False	
		Security guards' level of training (affecting the probability of false accept)	High	Low	
	Alarm Assessment	Alarm assessment through CCTV system	Image quality	Sufficient	Insufficient
			Level of integration with detection system and recording function	High	Low
Operator looking at monitor			True	False	
Operator's level of training			High	Low	
Operator's workload			Low	High	
Display system ease of interpretation and use of the		High	Low		
Alarm assessment by roving guards		Security guards' level of training	High	Low	
Alarm assessment by employees		Employees' level of security training	High	Low	
Alarm communication	Communication to/among response force	Reliability of coverage	High	Low	
		Security guards' level of training in communication procedures	High	Low	

4.2 Probabilistic assessment of PPS

The quantitative probabilistic assessment of PPS performance regarded the items listed in Table 5. Each expert was asked to assess the performance of PPS on the basis of past operational experience acquired at the facility (or facilities) under his/her responsibility. Expert elicitation was conducted through the adoption of the simplified elicitation method described in Section 3.3 and with the support of a questionnaire specifically prepared.

A satisfying percentage of the questions (higher than 85%) received an answer, providing a quantitative estimate of performance. The level of completeness of expert elicitation results is shown in Fig. 2, where the percent of answered questions with respect to the identified set of query variables is represented for each security barrier. In 8 cases out of 13, the expert provided the required query variables to fully characterize security barriers' performance (100% answered questions).

It was in general relatively easy for the experts to provide quantitative estimates on the expected performance of security barriers involving the action of employees and guards. However, more difficulties were present in the assessment of the expected successful accomplishment of security functions based on hardware and software systems.

Figure 2: Percentage of answered questions during expert elicitation of query variables, grouped according to security barrier of reference.

For the sake of brevity, only the analysis of questionnaire results concerning the modules of detection by employees working on site and alarm assessment by employees working on site is described in detail. These modules were selected as in most of the facilities considered employees working on site are relied upon to perform the detection and assessment functions and considered as actively taking part to the protection of all considered industrial facilities (see Table 4). The results are illustrated in Figure 3, where expert estimates are presented in the aggregate form a box plot, to provide a synthetic visualization of the different judgements. As shown in Table 4, in the case of intrusion detection by employees working on site, the main influencing factors are employees presence and their level of security training. All experts agreed that if employees are not present at the location where intrusion occurs, there cannot be detection. The estimates of marginal probabilities of employees being present at the location where intrusion occurs shown in Fig. 3a were derived taking into account that intrusion may occur at any location of the site and considering the different number of employees present during day shift and night shift. When experts were asked to provide the marginal probability of employees having received a high level of security

training, which represent the favorable state, the estimates obtained spanned almost the entire range from 0 to 1. However, 4 estimates out of 6 were equal or higher than 0.85 resulting in a high median value (see Fig. 3b). As shown in Fig. 3c, there was a rather good agreement among the experts in the assessment of employees performance in detecting intruders or, more in general, any suspect person, activity or behavior. However, this agreement did not hold for the case of employees performance in assessing and thus reporting the detected anomaly (see Fig. 3d). The box plots in Fig. 3e and Fig. 3f show the measures of the unfavorable impact that a low level of security training of employees has on the detection and the assessment functions respectively according to the involved experts. Since referring to an unfavorable impact, a lower value of the multiplicative factor corresponds to a more significant impact, causing a higher reduction in the probability of successful detection or assessment. With the exception of an expert who judged the impact of the level of training as negligible in both cases (impact measure equal to 1), all the others agreed that the level of training is more important to the success of the assessment function rather than the detection function.

Figure 3: Performance estimates provided by expert with respect to the security function of detection and alarm assessment by employees working on site. a) Marginal probability of employees' presence; b) Marginal probability of employees having a high level of security training; c) Conditional probability of having effective detection given that all influencing factors are in favorable state; d) Measure of the unfavorable impact that a low level of security training has on the probability of effective detection; e) Conditional probability of having effective alarm assessment given that all influencing factors are in favorable state; f) Measure of the unfavorable impact that a low level of security training has on the probability of effective alarm assessment. MP: marginal probability; CP: conditional probability; IM: impact measure.

4.3 Combination of expert estimates

An equal weighting aggregation scheme was adopted to combine expert estimates of probabilities and impact measures, resulting in an uncalibrated combined estimate of query variables that was considered satisfactory in light of the explorative nature of the study. More specifically, the median value of the estimates provided by experts was selected as aggregated variable to quantify performance. Median value was preferred with respect to mean value as it is less affected by outliers within the set.

The obtained results are presented in full details in Appendix A. In particular, Table A-1 reports the median of the estimates provided for each query variable, together with the number of original expert estimates that formed the available set of data and the characteristics of data distribution. The level of expert agreement in the evaluation of query variables can be observed from the characteristics of the distribution of elicited values.

The use of more sophisticated combination techniques (i.e. performance-based weighting techniques) was avoided due to the lack of literature data on physical protection systems that could be used as seed variables to determine expert performance as subjective probability assessors and to support the calculation of global calibration scores to be translated into global weights. Moreover, the majority of performance-based weighting techniques were originally developed and are consequently more apt to combine cumulative probability distributions that describes the uncertainty on the value of variables.

4.4 Discussion

Although founded on a structured definition of physical security functions and barriers, the present study was extensively based on the use of expert judgement. Hence it has all the limitations of expert judgement studies and may not be immune from biases. More specifically, the results are to be intended as descriptive of the European geo-political context.

Considering the explorative nature of the study and the sensitivity of the information handled, the expert consultation was conducted according to a rather simplified, multi-stage approach aimed to identify the most relevant and less controversial aspects to be accounted for to obtain a quantitative performance assessment of preventive physical security systems.

Query variable elicitation was conducted starting from an easily interpretable formulation for the calculation of the probability of security barrier success in performing the primary function of detection, alarm assessment and alarm communication and required the derivation of point estimate probabilities rather than probability distributions. The selection of this approach was motivated by the basic familiarity that most of the involved experts had with probabilistic assessments and by relatively limited timeframe allotted to the interviews.

Nevertheless, the adopted expert elicitation method meets the requirement of scrutability, fairness and neutrality. Furthermore, the elicitation results featured a satisfactory level of completeness, which fell below 90% only in the case of hardware and software systems performance in implementing security functions, probably due to the relatively recent introduction of these system at industrial sites that limits to 3-4 years of operation the acquired operational experience.

The use of an equal weighting aggregation scheme to combine expert estimates of probabilities and impact measures was justified in light of the lack of adequate seed variables in the specialized literature.

The median values of conditional probability of success in performing the security functions of the preventive layer given all analyzed combinations of influencing factors states, obtained from expert elicitation, represent an extended set of quantitative expert judgment based data. However, among the results presented in Appendix A, aggregate performance estimates derived from the combination of less than 4 point data elicited from experts should be applied with caution.

These data can be applied to support the vulnerability assessment of physical protection systems implementing security barriers similar to those investigated herein and would allow to select the best performance estimates on the basis of the actual operative conditions.

Alternatively, the data associated to a given security barrier may be further aggregated to build, by collecting the values of the probability of success given all possible combinations of influencing factors states, the probability distribution that describes the entire range of variation of overall performance variable for that security barrier. Thus, the variations due to operative conditions would be captured through distributions of the probability of successful intrusion detection (P_D in Eq.(4)), the probability of successful alarm assessment (P_{Ass} in Eq.(4)), and the probability of alarm communication to response force (P_C in Eq.(1)). In this way, quantitative data are provided to complete the set of inputs required to the direct application of Sandia model, by using the equations presented in Section 2.3.

Besides providing quantitative data for the performance assessment of physical security barriers in terms of functional effectiveness according to the Sandia model, the present contribution allowed capturing relevant explanatory details on what can affect PPS effectiveness (through the identification of relevant influencing factors and the quantification of their negative impact). A more complete picture of the elements that more significantly contribute to weaken the performance with respect to a security function, thus reducing the effectiveness of the overall preventive security layer, was therefore provided. With respect to the latter issue, the results confirm, as observed also by (Nunes-Vaz et al., 2011), that security-in-depth relies not only on generating effective layers, but also on their coherent integration with maintenance, training and protocols.

5. Conclusions

The present study was aimed at the quantitative performance assessment of physical protection systems adopted to secure process and storage facilities of the process industry against external acts of interference, that is, terrorist attacks. Considering the lack of literature data to support quantitative performance assessment, the authors resorted to experts' consultation. Different expert judgements were aggregated, using an equal weighting scheme, to derive performance measures that reflect recent operational experience in securing chemical and petrochemical sites in Europe.

The results of expert interviews allowed to characterize the security barriers more frequently implemented to prevent the success of deliberate attacks. Moreover, it was possible to gain an

insight into the belief that experts hold on the probability of physical security systems effectively preventing the success of an external attack and an insight into the level of agreement reached in the identification of critical elements.

The adopted expert elicitation approach allowed to address the evaluation of PPS effectiveness with respect to its preventive function fully quantitatively, providing numerical values for the probabilistic variables required to support a vulnerability assessment conducted according to the Sandia model. Furthermore, a detailed quantitative characterization of the negative impact that inadequate operative conditions, maintenance practices and training etc. have on PPS functional effectiveness was also obtained.

The results of the present study were gathered to form an extended set of quantitative expert judgment based data that take into account performance variations due to operative conditions; this data set, and any further extension of its original version, may be very useful to support quantitative approaches to vulnerability assessment that focus on physical security elements.

6. Appendix A

This Appendix presents the results of the combination of experts' estimates of probabilities and impact measures adopted to characterize PPS performance.

An equal weighting aggregation scheme was adopted to combine expert estimates and the median value of the estimates was selected as aggregated variable of reference to quantify performance. Median value was preferred with respect to mean value as it is less affected by outliers within the set.

Table A.1 reports the median of the estimates provided for each query variable, together with the number of original expert estimates that formed the available set of data and the characteristics of data distribution.

The level of expert agreement in the evaluation of query variables can be observed from the distribution characteristics reported in the sixth column of Table A.1.

It is however suggested that, among the presented results, aggregate performance estimates derived from the combination of less than 4 point data elicited from experts (see the fifth column of Table A.1) should be applied with caution.

Table A.1: Performance data based on the combination of estimates provided by experts

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
External IDS based on VMD	Detection through external IDS based on VDM	CP of success given all influencing factors in favorable state (baseline)	0.965	4	Minimum = 0.85; 1 st Quartile = 0.925; 3 rd Quartile = 0.982; Maximum= 0.99.
	Weather conditions	MP of weather conditions being favorable to detection	0.85	2	Minimum = 0.85; 1 st Quartile = 0.85; 3 rd Quartile = 0.85; Maximum= 0.85.
	Weather conditions	IM on the baseline CP from changing the weather conditions to the unfavorable state	0.7	3	Minimum = 0.5; 1 st Quartile = 0.6; 3 rd Quartile = 0.85; Maximum = 1.
	Installation conditions	MP of installation conditions being favorable to detection	0.825	4	Minimum = 0.25; 1 st Quartile = 0.665; 3 rd Quartile = 0.885; Maximum = 0.99.
	Installation conditions	IM on the baseline CP from changing the installation conditions to the unfavorable state	0.01	3	Minimum = 0.01; 1 st Quartile = 0.01; 3 rd Quartile = 0.38; Maximum = 0.75.
	Coverage of detection area	MP of having a full coverage of site area/ site perimeter	0.85	3	Minimum = 0.7; 1 st Quartile = 0.775; 3 rd Quartile = 0.925; Maximum = 1.
	Coverage of detection area	IM on the baseline CP from changing the level of site area/perimeter coverage to the unfavorable state	0.105	2	Minimum = 0.01; 1 st Quartile = 0.057; 3 rd Quartile = 0.152; Maximum = 0.2.
	Maintenance and inspection	MP of carrying out adequate maintenance and inspection	0.875	4	Minimum = 0.8; 1 st Quartile = 0.837; 3 rd Quartile = 0.92;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
Intrusion detection by roving guards	Maintenance and inspection	IM on the baseline CP from changing the maintenance and inspection to the unfavorable state	0.2	3	Maximum = 0.98. Minimum = 0.1; 1 st Quartile = 0.15; 3 rd Quartile = 0.35; Maximum = 0.5.
	Intrusion detection by roving guards	CP of success given all influencing factors in favorable state (baseline)	0.8	5	Minimum = 0.5; 1 st Quartile = 0.75; 3 rd Quartile = 0.95; Maximum = 0.95.
	Guards' presence	MP of guards being present where intrusion occur	0.40	3	Minimum = 0.04; 1 st Quartile = 0.22; 3 rd Quartile = 0.408; Maximum = 0.416.
	Guards' presence	IM on the baseline CP from changing the guards' presence to the unfavorable state	0	5	Minimum = 0; 1 st Quartile = 0; 3 rd Quartile = 0; Maximum = 0.
	Security guards' level of training	MP of security guards' having a high level of training	0.85	5	Minimum = 0.35; 1 st Quartile = 0.70; 3 rd Quartile = 0.95; Maximum = 1.
	Security guards' level of training	IM on the baseline CP from changing the security guards' level of training to the unfavorable state	0.5	5	Minimum = 0.3; 1 st Quartile = 0.5; 3 rd Quartile = 0.75; Maximum = 1.
Intrusion detection by employees	Intrusion detection by employees	CP of success given all influencing factors in favorable state (baseline)	0.89	6	Minimum = 0.7; 1 st Quartile = 0.82; 3 rd Quartile = 0.9; Maximum = 0.9.
	Employees' presence	MP of employees being present where intrusion occur	0.767	6	Minimum = 0.381; 1 st Quartile = 0.520; 3 rd Quartile = 0.829;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
					Maximum= 1.
	Employees' presence	IM on the baseline CP from changing the employees' presence to the unfavorable state	0	6	Minimum = 0; 1 st Quartile = 0; 3 rd Quartile = 0; Maximum= 0.
	Employees' level of security training	MP of employees' having a high level of security training	0.92	6	Minimum = 0.1; 1 st Quartile = 0.438; 3 rd Quartile = 0.99; Maximum= 1.
	Employees' level of security training	IM on the baseline CP from changing the employees' level of security training to the unfavorable state	0.8	6	Minimum = 0.35; 1 st Quartile = 0.75; 3 rd Quartile = 0.916; Maximum= 1.
Entry control, supervised automatic credentials check (people)	Prevention of false accept	MP of having a false accept by the system	0.99	4	Minimum = 0.85; 1 st Quartile = 0.995; 3 rd Quartile = 0.99; Maximum= 0.99.
	Prevention of undetected bypass	CP of having an undetected bypass given a high level of attention of security guards	0.92	4	Minimum = 0.8; 1 st Quartile = 0.875; 3 rd Quartile = 0.99; Maximum= 0.99.
	Security guards' level of attention	MP of security guards' having a high level of attention	0.9	4	Minimum = 0.7; 1 st Quartile = 0.812; 3 rd Quartile = 0.95; Maximum= 0.95.
	Security guards' level of attention	IM from changing the presence of anti-bypass sensors to the unfavorable state	0.9	4	Minimum = 0.5; 1 st Quartile = 0.8; 3 rd Quartile = 0.9; Maximum= 0.9.
Entry control, unsupervised automatic credentials check	Prevention of false accept	MP of having a false accept by the system	0.99	3	Minimum = 0.9; 1 st Quartile = 0.945; 3 rd Quartile = 0.995;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
(people)					Maximum= 0.999.
	Prevention of undetected bypass	MP of having an undetected bypass	0.99	3	Minimum = 0.95; 1 st Quartile = 0.97; 3 rd Quartile = 0.99; Maximum= 0.99.
Entry control, manual credentials check (people)	Prevention of false accept	CP of preventing a false accept by the system given all influencing factors in favorable state (baseline)	0.8	1	n.a.
	Prevention of undetected bypass	MP of preventing an undetected bypass given all influencing factors in favorable state (baseline)	0.6	1	n.a.
	Security guards' level of training	MP of guards having a high level of training	0.95	3	Minimum = 0.95; 1 st Quartile = 0.95; 3 rd Quartile = 0.975; Maximum= 1.
	Security guards' level of training	IM on the probability of preventing a false accept from changing guards' level of training to the unfavorable state	0.2	1	n.a.
	Security guards' level of attention	CP of guards having a high level of attention during credentials check given a low workload	0.95	1	n.a.
	Security guards' level of attention	IM on the probability of preventing a false accept from changing guards' level of attention to the unfavorable state	0.25	1	n.a.
	Security guards' level of attention	IM on the probability of preventing an undetected bypass from changing guards' level of attention to the unfavorable state	0.51	1	n.a.
	Security guards' workload	MP of guards having a low workload	0.7	1	n.a.

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
Entry control, unsupervised automatic biometrics check (people)	Security guards' workload	IM on the probability of guards having a high level of attention during credentials check from changing the workload to the unfavorable state	0.4	3	Minimum = 0.4; 1 st Quartile = 0.4; 3 rd Quartile = 0.55; Maximum= 0.7.
	Prevention of false accept	MP of not having a false accept by the system	0.99	2	Minimum = 0.99; 1 st Quartile = 0.99; 3 rd Quartile = 0.99; Maximum= 0.99.
	Prevention of undetected bypass	CP of not having an undetected bypass given the presence of anti-bypass sensors	0.99	1	n.a.
	Presence of anti-bypass sensors	MP of anti-bypass sensors being in place	0.5	2	Minimum = 0; 1 st Quartile = 0.25; 3 rd Quartile = 0.75; Maximum= 1.
	Presence of anti-bypass sensors	IM on the probability of not having an undetected bypass from changing the presence of anti-bypass sensors to the unfavorable state	0.01	1	n.a.
Entry control, supervised automatic credentials check (vehicles)	Prevention of false accept	MP of having a false accept	0.99	4	Minimum = 0.85; 1 st Quartile = 0.955; 3 rd Quartile = 0.992; Maximum= 0.999.
	Prevention of undetected bypass	CP of having an undetected bypass given a high level of training of security guards	0.97	4	Minimum = 0.9; 1 st Quartile = 0.937; 3 rd Quartile = 0.99; Maximum= 0.99.
	Security guards' level of attention	MP of security guards' having a high level of training in credentials check	0.95	4	Minimum = 0.7; 1 st Quartile = 0.887; 3 rd Quartile = 0.95; Maximum= 0.95.
	Security guards' level of	IM on the probability of undetected	0.75	4	Minimum = 0.5;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
Entry control, manual credentials check (vehicles)	attention	from changing the level of attention to the unfavorable state			1 st Quartile = 0.575; 3 rd Quartile = 0.9; Maximum= 0.9.
	Prevention of undetected bypass	MP of having an undetected bypass	0.97	2	Minimum = 0.95; 1 st Quartile = 0.96; 3 rd Quartile = 0.98; Maximum= 0.99.
	Prevention of false accept	CP of having a false accept by the system given a high level of training of security guards	0.99	2	Minimum = 0.99; 1 st Quartile = 0.99; 3 rd Quartile = 0.99; Maximum= 0.99.
	Security guards' level of training	MP of security guards' having a high level of training in credentials check	0.6	2	Minimum = 0.35; 1 st Quartile = 0.475; 3 rd Quartile = 0.725; Maximum= 0.8.
	Security guards' level of training	IM on the probability of preventing false accept from changing the level of training to the unfavorable state	0.95	2	Minimum = 0.9; 1 st Quartile = 0.925; 3 rd Quartile = 0.975; Maximum= 1.
Alarm assessment through CCTV system	Alarm assessment through CCTV system	CP of success given all influencing factors in favorable state (baseline)	0.97	5	Minimum = 0.9; 1 st Quartile = 0.95; 3 rd Quartile = 0.99; Maximum= 0.99.
	Image quality	MP of having a sufficient image quality to assessment	0.795	2	Minimum = 0.6; 1 st Quartile = 0.697; 3 rd Quartile = 0.892; Maximum= 0.99.
	Image quality	IM on the baseline CP from changing image quality to the unfavorable state	0.4	5	Minimum = 0.001; 1 st Quartile = 0.01; 3 rd Quartile = 0.5; Maximum= 1.
	Level of integration with	MP of having a sufficient level of	0.9	3	Minimum = 0.85;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
	detection system and recording function	integration with detection system and recording function			1 st Quartile = 0.875; 3 rd Quartile = 0.925; Maximum= 0.95.
	Level of integration with detection system and recording function	IM on the baseline CP from changing the level of integration with detection system and recording function to the unfavorable state	0.1	3	Minimum = 0.01; 1 st Quartile = 0.05; 3 rd Quartile = 0.45; Maximum= 0.8.
	Operator looking at monitor	MP of the operator being looking at monitor when alarm occurs	1	5	Minimum = 0.27; 1 st Quartile = 1; 3 rd Quartile = 1; Maximum= 1.
	Operator looking at monitor	IM on the baseline CP of the operator not being looking at monitor when alarm occurs	0	5	Minimum = 0; 1 st Quartile = 0; 3 rd Quartile = 0; Maximum= 0.
	Operator's level of training	MP of operator having a high level of training	0.65	4	Minimum = 0.3; 1 st Quartile = 0.337; 3 rd Quartile = 0.95; Maximum= 0.95.
	Operator's level of training	IM on the baseline CP from changing the operator level of training to the unfavorable state	0.25	4	Minimum = 0.2; 1 st Quartile = 0.237; 3 rd Quartile = 0.387; Maximum= 0.8.
	Operator's workload	MP of operator having a low workload	0.825	4	Minimum = 0.6; 1 st Quartile = 0.75; 3 rd Quartile = 0.861; Maximum= 0.895.
	Operator's workload	IM on the baseline CP from changing the operator workload to the unfavorable state	0.575	4	Minimum = 0.25; 1 st Quartile = 0.437; 3 rd Quartile = 0.675; Maximum= 0.75.
	Display system ease of	MP of the display system being easy to	0.75	5	Minimum = 0.45;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
	interpretation and use of the	interpret and use	0.5	5	1 st Quartile = 0.5; 3 rd Quartile = 0.9; Maximum= 1.
	Display system ease of interpretation and use of the	IM on the baseline CP from changing the display system ease of use and interpretation to the unfavorable state			Minimum = 0.1; 1 st Quartile = 0.2; 3 rd Quartile = 0.5; Maximum= 0.75.
	Alarm assessment by roving guards	CP of success given all influencing factors in favorable state (baseline)			Minimum = 0.65; 1 st Quartile = 0.9; 3 rd Quartile = 0.9; Maximum= 0.99.
Alarm assessment by roving guards	Security guards' level of training	MP of security guards having a high level of training	0.85	5	Minimum = 0.35; 1 st Quartile = 0.70; 3 rd Quartile = 0.95; Maximum= 1.
	Security guards' level of training	IM on the baseline CP from changing the security guards' level of security training to the unfavorable state	0.55	5	Minimum = 0.5; 1 st Quartile = 0.5; 3 rd Quartile = 0.9; Maximum= 1.
Alarm assessment by employees	Alarm assessment by employees	CP of success given all influencing factors in favorable state (baseline)	0.875	6	Minimum = 0.2; 1 st Quartile = 0.812; 3 rd Quartile = 0.952; Maximum= 0.99.
	Employees' level of security training	MP of employees having a high level of security training	0.92	6	Minimum = 0.1; 1 st Quartile = 0.438; 3 rd Quartile = 0.99; Maximum= 1.
	Employees' level of security training	IM on the baseline CP from changing the employees' level of security training to the unfavorable state	0.5	6	Minimum = 0.1; 1 st Quartile = 0.2; 3 rd Quartile = 0.762; Maximum= 1.
Communication	Communication to response	CP of success given all influencing	0.95	7	Minimum = 0.85;

Security barriers	Factor	Query variable	Aggregate performance estimate (Median)	N. of expert estimates	Distribution Characteristics
to/among response force	force	factors in favorable state (baseline)			1 st Quartile = 0.9; 3 rd Quartile = 0.98; Maximum= 1.
	Reliability of coverage	MP of having a highly reliable coverage	0.99	7	Minimum = 0.75; 1 st Quartile = 0.97; 3 rd Quartile = 1; Maximum= 1.
	Reliability of coverage	IM on the baseline CP from changing the reliability of coverage to the unfavorable state	0.1	7	Minimum = 0.01; 1 st Quartile = 0.055; 3 rd Quartile = 0.125; Maximum= 0.75.
	Security guards' level of training in communication procedures	MP of security guards' having a high level of training in communication procedures	0.9	7	Minimum = 0.25; 1 st Quartile = 0.7; 3 rd Quartile = 0.9; Maximum= 1.
	Security guards' level of training in communication procedures	IM on the baseline CP from changing the level of training in communication procedures to the unfavorable state	0.5	7	Minimum = 0.1; 1 st Quartile = 0.175; 3 rd Quartile = 0.775; Maximum= 1.

MP = marginal probability; CP= conditional probability; IM= impact measure; n.a. = not applicable.

7. References

- Analyse, Recherche et Information sur les Accidents (ARIA), French ministry of ecology and sustainable development (<http://www.aria.developpement-durable.gouv.fr/>) (accessed December 2015).
- Argenti, F., Landucci, G., Spadoni, G., Cozzani, V., 2015. The assessment of process plant attractiveness related to terrorist attack. *Saf. Sci.* 77C, 169-181.
- European Commission, 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. *Off. J. Eur. Union* L345, 75–82.
- Bajpai, S., Gupta, J.P., 2005. Site security for Chemical Process Industry. *J. Loss. Prev. Process. Ind.* 18 (4–6), 301–309.
- Baybutt, P., Reddy, V., 2003. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. *Homeland Defence Journal* 2, 1.
- American Petroleum Institute (API), 2013. ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry. American Petroleum Institute, Washington, DC.
- American Petroleum Institute (API), 2003. API Recommended Practice 70 - Security for Offshore Oil and Natural Gas Operations. American Petroleum Institute, Washington, DC.
- Bajpai, S., Gupta, J.P., 2007a. Securing oil and gas infrastructure. *J. Petroleum Sci. Eng.* 55, 174-186.
- Bajpai, S., Gupta, J.P., 2007b. Terror proofing chemical process industries. *Process Safety and Environmental Protection*, Trans IChemE, Part B, 85 (B6), 559-565.
- Center for Chemical Process Safety (CCPS), 2003. Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. American Institute of Chemical Engineers, Center of Chemical Process Safety, New York, USA.
- Cooke, R. M., Goossens, L. J. H., 2000. Procedures guide for structured expert judgment. European Commission Project Report n. EUR 18820 En
- Cozzani, V., Tugnoli A., Salzano, E., 2009. The development of an inherent safety approach to the prevention of domino accidents. *Accid. Anal. and Prev.* 41, 1216–1227.
- Garcia, M. L., 2006. Vulnerability Assessment of Physical Protection Systems. Butterworth-Heinemann.
- Garcia, M.L., 2008. The Design and Evaluation of Physical Protection Systems. Butterworth-Heinemann.
- International Maritime Organization (IMO), 2004. The Ship and Port Facility Security Regulations. HMSO, London, UK.
- Jaeger, C. D., 2003. Chemical facility vulnerability assessment project. *J. of Hazard. Mater.* 104, 207–213.
- Keeney, G. L., von Winterfeldt, D., 2010. Identifying and Structuring the Objectives of Terrorists Risk Anal. 30 (12), 1803-1816.
- Landucci, G., Reniers, G., Cozzani, V., Salzano, E., 2015. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. *Rel. Eng. and Syst. Saf.* 143, 53–62.
- Lindley, D.V., 2006. Understanding uncertainty. Wiley, Hoboken, NJ.

- Nolan, D. P., 2008. Safety and security review for the process industries. Elsevier Inc., Amsterdam, The Netherlands.
- Norichica, T., Mitsutoshi S., 2014. A probabilistic extension of the EASI Model. *J. Physic. Secur.* 7 (2), 12-29.
- Norman, T.L., 2010. Risk Analysis and Security Countermeasure Selection, CRC Press, Boca Raton.
- Nunes-Vaz, R., Lord, S., Ciuk, J., 2011. A more rigorous framework for security-in-depth. *J. Appl. Secur. Res.* 6 (3), 372–393.
- Nunes-Vaz, R., Lord S., 2014. Designing physical security for complex infrastructures. *Int. J. of Crit. Infrastruct. Protection* 7, 178-192.
- O'Hagan, A., Buck, C. .E., Daneshkhak, A., Eiser, J.R., Garthwaite, P. H., Jenkinson, D. J., Oakley, J.E., Rakow, T., 2006. Uncertain Judgements: Eliciting Experts' Probabilities. John Wiley & Sons.
- Reniers, G., Dullaert, W., Audenaert, A., Ale, B.J.M., Soudan, K., 2008. Managing domino effect-related security of industrial areas. *J. Loss. Prev. Process. Ind.* 21 (3), 336-343.
- Reniers, G., Audenaert, A., 2014. Preparing for major terroristic attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. *Process Saf. And Environ. Protection* 92 (6), 583-589.
- Sivarajasingam, V., Shepherd, J. P., 1999. Effect of closed circuit television on urban violence. *J. Accid. and Emerg. Med.* 16 (4), 255-257.
- Störfallkommission (SFK), 2002. SFK – GS – 38, Report of the German Hazardous Incident Commission. Störfallkommission, Baden, Germany.
- Talbot, J., Jakeman, M., 2009. Security risk management body of knowledge. Hoboken, NJ: Wiley.