Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network

Vulnerability Assessment of Chemical Facilities to Intentional Attacks based on Bayesian Network

REVISED VERSION – September 2017

Francesca ARGENTI[1], Gabriele LANDUCCI[2],
Genserik RENIERS[3,4], Valerio COZZANI[1,*]

(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 1, 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)-051-2090240; fax (+39)-051-2090247
e-mail: valerio.cozzani@unibo.it

Submitted for publication in:

RELIABILITY ENGINEERING & SYSTEM SAFETY

ABSTRACT

Chemical facilities may be targets of deliberate acts of interference triggering major accidents (fires, explosion, toxic dispersions) in process and storage units. Standard methodologies for vulnerability assessment are based on qualitative or semi-quantitative tools, currently not tailored for this type of facilities and not accounting for the role of physical protection systems. In the present study, a quantitative approach to the probabilistic assessment of vulnerability to external attacks is presented, based on the application of a dedicated Bayesian Network (BN). BN allowed the representation of interactions among attack impact vectors and resistance of process units, which determine the final outcomes of an attack. A specific assessment of protection systems, based on experts' elicitation of performance data, allowed providing a knowledge support to the evaluation of probabilities. The application to an industrial case study allowed the assessment of the potentialities of the approach, which may support both the evaluation of the vulnerability of a given facility, and the performance assessment of the security physical protection system in place.

KEYWORDS

Security Risk; Physical Protection Systems; Vulnerability; Probabilistic Assessment; Bayesian Networks.

1. Introduction

Industrial facilities storing and processing relevant quantities of hazardous chemicals have an inherent hazard potential that may be exploited by malevolent agents, causing a major accident [1-3]. The attack perpetrated in France against the production site of a chemical company in June 2015 [4] demonstrated that this type of threat for industrial facilities located in western countries is credible. At the same time, it was shown that the security of industrial sites must be addressed, both from the legislative and the technical point of view, as an issue of the greatest urgency.

Actually, after the events of "9/11", the security of sites where relevant quantities of hazardous chemicals are stored or processed became a concern [5], and security risks started to be included in formal risk assessment [6]. According to the prescriptions of the Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 ("the CFATS Act of 2014") [7], the U.S. Department of Homeland Security (DHS) is required to analyze vulnerabilities and establish risk-based security performance standards for critical infrastructures, which include chemical facilities as one of the highest priority sectors; facility owners and operators are required to prepare a security vulnerability assessment and a facility security plan, identifying specific assets of concern.

The "European Programme for Critical Infrastructure Protection (EPCIP)" [8] promotes the prevention, preparedness and response to terrorist attacks involving installations of the energy (electricity, oil and gas) and the transport (road, rail, air, inland waterways and ocean and short-sea shipping and ports) sectors. On the other hand, European Seveso-III Directive [9] concerning major accident hazards focuses on safety-related issues and does not addresses the need for a security analysis or for security countermeasures in industrial installations that may be considered attractive or vulnerable targets of terrorist attacks. Hence, no detailed guidelines are yet available for the security of chemical and process plants in the EU.

In the last 15 years, the development of security risk assessment methodologies was promoted to guide and support industrial operators in assessing and managing security risks. Among others, it is worth recalling the security risk assessment methodologies proposed by American Petroleum Institute – API [10], American Institute of Chemical Engineering [11], Sandia National Laboratories [12] and U.S. National Institute of Justice [13]. These methodologies allow for a qualitative or a semi-quantitative (e.g. in the case of API methodology) assessment of security risk, while 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 [14]. However, as the credibility of the threat against chemical and process industry facilities increases, the assessment of security-related and terrorism-related risks should be dealt with using more systematic approaches at a quantitative level, in order to provide a metric of existing vulnerability and of the available level of protection with respect to external attack scenarios.

In this study, an approach based on probabilistic risk analysis, supported by Bayesian Networks (BN), was developed for the analysis of outsiders' threat against chemical facilities. The approach focuses on the vulnerability of high-consequence loss of physical assets within the facility, i.e. process and storage equipment that are critical in terms of potential of causing major accidents [11,13]. A dedicated approach was developed in order to include the contribution of physical security elements in the determination of vulnerability. The approach and the BN presented herein are aimed at supporting the analysis of existing installations by security managers and risk analysts, as they provide a quantitative tool to conduct scenario-based vulnerability assessment.

The paper is structured as follows: in Section 2, the background on security and vulnerability studies dedicated to the process industry is presented; in Section 3, the methodological approach and the Bayesian Network tool are described; in Section 4 a case study is presented, whose results are discussed in Section 5; Section 6 discusses potentialities and limitations of the present approach and in Section 7 conclusions are drawn.

2. State of the art

2.1 Literature dealing with security risks evaluation

Literature studies concerning security-related issues faced by the process industry were mostly devoted to the evaluation of the severity of impacts due to external attacks on process plants [15-17], to the analysis and characterization of terrorist threats [18], or were focused on the determination of process facilities attractiveness to potential malevolent adversaries [19,3].

Beside the characterization of attacks and the assessment of attack tactics, several literature studies were also devoted to the analysis of the defense strategy adopted in complex systems. According to the review carried out by Hausken and Levitin [20], defense measures are divided into separation of system elements, redundancy, protection, multilevel or multilayered defense, deployment of false targets and preventive strike.

Few contributions investigated the potential of deliberate attacks to trigger domino effects [15,17, 21,22], leading to extensive damages due to consequence escalation and to the involvement of multiple units.

The scientific Community was however divided in the selection of the most suitable approach to be adopted to address the assessment of the likelihood of security risks: in particular, several authors (e.g. see [23-25]) discussed if probabilistic risk analysis (PRA) or intelligent adversary methods would be preferable for counterterrorism risk management. An extended discussion on the strengths and drawbacks of the two approaches can be found in the Special Issue dedicated to “Advances in Terrorism Risk Analysis” of the Risk Analysis journal [26]. Among others, Garrick et al. [27] and Paté-Cornell and Guikema [28] used a PRA approach to assess quantitatively the risk posed by terrorist-initiated events. Apostolakis and Lemon [29] applied PRA in the analysis of the risk posed to different types of infrastructures at Massachusetts Institute of Technology University campus by malevolent attackers with limited capability (minor threat). In the latter case, the whole analysis is conditional to the presence of the threat. Hausken applied game theory [30] to assess the role of human behavior and conflicts in resource allocation for the defense, thus providing a quantitative tool to incorporate the defender’s perspective into PRA.

Concerning the assessment of attacks against sophisticated networks and complex systems and infrastructures, several examples of modeling approaches are available in the literature. Hausken [31] proposed an integrated method for the optimization of protection investments and resources for complex infrastructures considering one strategical defender protecting an entire system of multiple targets potentially affected by multiple strategic attackers. In the approach, operations research, reliability theory, and game theory are merged to support the optimization.

Chopra and Khanna [32] combined an empirical economic input–output model with graph theory based techniques for understanding interdependencies and resilience in the United States economic system due to interdependencies among critical infrastructures; in particular, a comparison among the effect of random failures and targeted attacks on key nodes of the critical infrastructures network was carried out, evidencing critical system vulnerabilities.

Wu et al. [33] developed an attack strength degradation model able to capture the interdependencies among infrastructures and to model cascading failures based on the application of graph theory. The problem of interdependency, with particular reference to transportation networks, was also addressed by Zhang et al. [34], that investigated overloads and cascading failures possibly leading to catastrophic events.

However, according to the literature survey and in light of the qualitative or semi-quantitative nature of existing security risk assessment methodologies [11,13], the need to develop a quantitative evaluation approach tailored to the chemical industry clearly emerges. For this purpose, a PRA approach was selected in the present study, since it allows to structure the analysis of external attack scenarios from the point of view of the system under attack, more easily accounting for the measures in place to protect it. Actually, as pointed out by Garrick et al. [27], in the case of external attacks to chemical industry or, more in general, to industrial facilities, the initiating events triggered by external threats are tied to the design and operations of the facility under attack, which are fixed and well defined, as well as the protection systems.

In order to illustrate the framework in which the present study set its basis, the security risk formulation is firstly presented to support the PRA approach considered (Section 2.2). Then, since the focus of the study is the vulnerability assessment of chemical facilities, the concept of vulnerability and some key definitions are briefly discussed (Section 2.3).

2.2 Security risk formulation

The necessary basis to support the quantitative assessment of vulnerability adopted in the present study is to define a sound scientific risk framework aimed at conceptualizing the relevant terms object of the present investigation. The commonly adopted risk framework in process safety domain defines risk as a combination of consequences and associated probabilities or associated uncertainties [35]. In this framework, probability is normally interpreted as a “frequentist probability”, thus interpreted as the fraction of time in which the event occurs and continuously repeats over time [36].

Differently, within security framework, e.g. dealing with the assessment of intentional acts of interference, risk is commonly defined as the triplet asset/value, threat and vulnerability [23,26], without any explicit reference to a probabilistic component.

However, in a recent study, Amundrud et al. [36] provided indications on how safety and security risk frameworks are compatible and traced a blue line in which also security risk may be defined through events-consequences and uncertainties. To express the uncertainties, it is recommended to use probability or interval probabilities, together with judgments of the strength of knowledge supporting the probabilities [37,38]. In the review provided by [39] it is indicated that a way to express the uncertainties is to refer to probability. Moreover, a necessary element needed to strengthen this kind of approach is the support of a strong knowledge judgement, which, however is not systematically adopted in security analyses and may constitute an element of novelty [38].

Based on the aforementioned considerations, the following expression is adopted to describe the risk in the present work:

$$R = (P(A), P(L|A), K) \qquad (1)$$

where R is the security risk, $P(A)$ represents the probability of having an event (A) that affects the asset or installation under analysis, $P(L|A)$ is the probability of having a specified loss (L) for a target category given the event A, and K is the knowledge dimension.

The risk expression reported in Eq. (1) relies on the adoption of probabilistic terms. In this work, the probability expresses the uncertainty that a given attack will occur and that a possible impact is achieved as a consequence. These uncertainties are specifically evaluated through the likelihood of a given threat being involved in the attack, the value of the target given a specific threat, that is the attractiveness, and the vulnerability of the asset with respect to that threat [40,41], which is represented by the term $P(L|A)$ in Eq. (1) and constitutes the focus of this work.

To quantify the mentioned uncertainties, a subjective probabilistic evaluation based on expert judgement is considered, thus showing the role of the knowledge dimension K in supporting the probabilistic assessment, as indicated in [39]. In particular, the present work relies on specific performance data of physical security countermeasures which are elicited from experts' consultation and are then adopted to quantify the vulnerability of chemical facilities with respect to the possible propagation of accidents induced by external attacks.

It is worth mentioning that the risk expression reported in Eq. (1) features a multi-dimensional nature, since losses of different categories may occur as a consequence of single attack. In particular, according to [42], human lives, economic values, or symbolic/influence values may characterize both the impact of consequences and the attractiveness associated with a given target. Besides, environmental contamination may also be relevant to the characterization of loss categories, as described in [43] for ecoterrorism concerns.

Therefore, although simplified, the above-discussed security risk formulation may capture the fundamental multi-dimensional nature of security risk and is considered in the development of this study to enhance the practical value and ease of use of obtained results in the direct application of existing security risk assessment methodologies.

2.3 The concept of vulnerability

Vulnerability is often considered as a global system property that expresses the extent of adverse effects caused by the occurrence of a specific hazardous event. This interpretation of vulnerability is thus closely related to the definition of risk. However, the difference is that in the case of vulnerability the identification and characterization of scenarios are conditioned upon the occurrence of a specific hazardous event or strain. This concept of vulnerability inspired early developed security vulnerability assessment methodologies [10-12], that, although referring to "vulnerability", were meant to evaluate risks associated to security events.

Johansson et al. [44] define vulnerability as the ability of a system to withstand strains and the effects of failures. Haimes [45] has a similar view as he defines vulnerability as the manifestation of any possible technical, organizational, cultural state which a system may feature and that may lead to harm or damage the system itself.

Several literature studies concerning infrastructure security were developed starting from this statement [46-48]. In particular, Haimes [45] pointed out that, in the perspective of infrastructure and industrial facilities protection, two major considerations need to be taken into account:

i. the ability to recover the desired values of the states of a system that has been attacked, within an acceptable time period and at an acceptable cost;
ii. the ability to reduce the effectiveness of the attack (and thus its probability of success) by other actions that may or may not necessarily change the state variables of the system. Such actions may include detection, prevention, protection, interdiction and containment, which also represent the design functions of security protection systems.

The first consideration is associated to system resilience [39], which may be enhanced, for example, by adding redundancy and robustness[1].

The second consideration is the focus of investigation in the present study: herein vulnerability has been intended as the proxy for the likelihood of external attack success in agreement with the risk formulation proposed in Eq. (1) and its evaluation has been conducted accordingly.

More specifically, a quantitative estimation of the likelihood of success of external attack scenarios was derived conducting a performance-based assessment of vulnerability, as recommended for facilities with high-consequence loss physical assets (see for example [50]). The quantitative assessment of the effectiveness of physical security systems (PPSs) currently adopted to protect process and storage facilities was carried out, as explained in Section 3.2.2. The adoption of the present method, based on the analysis of the PPS performance provided a metric for the available level of protection, supporting the identification of weak elements and security functions that need improvement in a given installation.

According to [51], the vulnerability assessment is commonly based either on an asset-based or on a scenario based approach. In the case of asset-based vulnerability assessment, a broad evaluation of assets and threats that impact on those assets is carried out without considering and analyzing the attack scenario(s). On the contrary, the scenario-based approach focuses on the attack in order to foresee by which means, methods, and tools targets may be affected, thus also identifying possible countermeasures. Therefore, in the present analysis, a scenario-based assessment was privileged since in line with the aim of directly supporting the managerial decision process and providing recommendations on the implementation and/or improvement of security protections [10].

3. Methods and tools

3.1 Bayesian networks: overview

In the present study, Bayesian Networks (BN) were adopted to support the probabilistic assessment of vulnerability through the likelihood analysis of attack scenarios, the evaluation of the overall effectiveness of preventive security systems and the analysis of the vulnerability of industrial equipment to impact vectors associated with the more common attack modes. With respect to possible alternative quantitative methods (for example, attack trees [27]) the present method takes advantage of BN capability to update prior marginal probabilities in real time as new information becomes available, and to capture non-causal influences. It is worth mentioning that BN were applied in a "standard" configuration, since the novelty of the present study relies in the ability to provide quantitative data and in introducing a systematic vulnerability approach.

BN represent all conditional dependencies (and independencies) among a system's variables by means of joint probability distributions [52-54]. BN are acyclic directed graphs in which the systems' random variables (components) are represented by nodes (conventionally, elliptical) while the direct probabilistic dependencies among the nodes are represented by directed arcs (causal dependencies, sequential order, etc.). The nodes with arcs directed from them are called parents while the ones with arcs directed into them are called children. The nodes with no parents are also called root nodes, whereas the nodes with no children are known as leaf nodes.

[1] A classic definition of resilience is given by Woods [49], which describes resilience as "the capability of recognizing, adapting to, and coping with the unexpected".

The position and orientation of arcs specify the independence assumptions that hold between the variables.

Considering the conditional dependencies of variables, BN represents the joint probability distribution P(U) of variables $U = \{G_1, \dots, G_n\}$, as:

$$P(U) = \prod_{i=1}^{n} P\big(G_i \big| Pa(G_i)\big) \quad (2)$$

where $Pa(G_i)$ is the parent set of variable G_i [55]. Accordingly, the probability of G_i is calculated as:

$$P(G_i) = \sum_{U \backslash G_i} P(U) \quad (3)$$

where the summation is taken over all the variables except G_i.

As highlighted by Charniak [54], BNs offer a convenient approach to a multitude of problems in which one wants to come to conclusions that are not warranted logically but, rather, probabilistically. BNs may be applied to forward as well as to backward reasoning through evidence propagation along the network and probability updating. Indeed, BNs take advantage of Bayes' theorem to update the prior probabilities of variables given new observations, called evidence E, rendering the updated or posterior probabilities [55]:

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \quad (4)$$

The most probable explanation in light of evidence made available on the actual state of intermediate or ultimate consequences, and the associated probability of occurrence, can also be computed given the BN structure and a full quantification of prior probabilities.

Due to its flexible structure and probabilistic reasoning engine, BN is a promising method for risk analysis of large and complex systems [56-58].

As pointed out by Khakzad et al. [59], the popularity of BN lies in the fact that it benefits from both qualitative modeling techniques (i.e. representation of independencies within the system of variables through network graphical structure) and quantitative modeling techniques based on the computation of every node's Conditional Probability Table (CPT). In this study, the software HUGIN Researcher 8.1 is used to support the BN quantification [60].

3.2 Probabilistic vulnerability assessment

The structure of the generic BN proposed to support probabilistic vulnerability assessment is shown in Fig. 1. The BN evaluates multiple aspects that contribute to determine facility vulnerability and enables to capture the evolution of security events, from emergence of the threat analyzed in terms of foreseen attack scenarios, through its development and the intervention of preventive security measures and systems, to attack effects in terms of process and storage equipment damage.

The structure of the BN in Fig. 1 has generalized validity at a qualitative level, since it incorporates nodes with generic states which consider the typical structure of PPS in chemical and process facilities. Conversely, the quantitative analysis of the network (i.e. the selection of the number nodes states and the quantification of conditional probability tables) has to be carried out considering the specific features of the industrial site under analysis and may involve the choice of including a reduced number of nodes or node states, as shown in Section 4 in the analysis of a demonstration case study. Moreover, specific indications are discussed in Section 6 in order to extend the present approach to complex installations.

3.2.1 Attack scenarios characterization

In order to conduct a scenario-based analysis, a schematization of the elements that allow for the characterization of an attack scenario was proposed: the target equipment selected as target, the attack mode selected by an adversary to cause damage and the path, and thus the sequence of actions, needed to damage the selected target through the selected attack mode are identified as key variables (corresponding to the nodes shown in white color in Fig. 1).

A node for each equipment item storing hazardous materials in the facility (E.I.1, E.I,2, etc.) was introduced to estimate the likelihood that a given equipment item is selected as target. The probability of an equipment item being selected as target was estimated starting from a simplified attractiveness assessment, based on equipment hazard potential, which on turn is related to the inventory of hazardous materials and the operative conditions of temperature and pressure, as suggested in [61].

The states of node "attack mode" (N1 in Fig. 1) were determined starting from the classification presented by Störfallkommission [62] and are described in Table 1. This classification was chosen since it was specifically derived for process and chemical facilities. Moreover the considered attack modes were verified against historical records derived from a query in the START database [63] with respect to attacks perpetrated against industrial facilities. For the sake of brevity, the outcomes of the analysis of the START database supporting the definition of attack modes categories reported in Table 1 is shown in Appendix A.

The assignment of the marginal probability of the attack occurring according to a specific attack mode is left to the analyst. This assignment should be based on the results of threat characterization studies that, on the basis intelligence information and threat history (if records are available for the specific geographic area or company), provide insights on adversaries' profiles and their presumed capability and weapons.

An attack vector (e.g. heat load, overpressure effects, projectile impact) and a success criterion were associated to each attack mode, as summarized in the third and fourth column of Table 1. For attack modes that involve the act of shooting or triggering fires and explosions, the final aim of damaging equipment is achieved if the physical effects caused by the attack have a sufficient strength to result, in absence of rapid intervention of protective countermeasures, in a loss of structural integrity and thus in a loss of containment from the equipment item itself. In case of heat load and overpressure effects, threshold values below which the possibility of loss of containment from different categories of impacted process and storage equipment is considered not credible are provided in literature studies concerning domino effect assessment [64].

In the case of attacks perpetrated with the aid of rather unsophisticated tools and without the use of weapons (i.e. deliberate misoperation, interference using simple and major aids), it was assumed that potential attackers "only" require to be in the proximity to the selected target for successful damage. Inherent resistance of targeted equipment items in this case is conservatively neglected in the estimation of attack success likelihood.

Table 1. States of the node “attack mode” in the BN shown in Fig. 1; n.a. = not applicable.

State	Description	Associated attack vector	Associated success criterion	Intrusion required
Deliberate misoperation	Deliberate acts involving simple operations without the use of instruments	n.a.	Target equipment location is reached	Yes
Interference using simple aids	Deliberate interference using tools and aids that are present on site	n.a.	Target equipment location is reached	Yes
Interference using major aids	Prepared destruction of installation parts by force using heavy tools	n.a.	Target equipment location is reached	Yes
Arson using incendiary devices	Incendiary attacks	Heat load	Target equipment is damaged due to external fire exposure	Yes
Use of explosives	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	Overpressure	Target equipment is damaged due to overpressure effects of explosion	Yes
Use of vehicle bomb	Use explosives to blow up tanks and pipelines or to blow up load-bearing structures to cause the collapse of tanks	Overpressure	Target equipment is damaged due to overpressure effects of explosion	No
Shooting 1	Interference at close distance, using different types of weapons	Projectile impact	Perforation and/or penetration of target equipment due to projectile impact	Yes
Shooting 2	Interference at distance, using different types of heavy weapons	Projectile impact	Perforation and/or penetration of target equipment due to projectile impact	Yes
Vehicle accident	Vehicle accident in the establishment aimed to release hazardous substances or damage/destroy important parts of the installation	Vehicle impact	Target equipment is damaged due to vehicle impact	Yes
Aircraft accident	Aircraft accident aimed to release hazardous substances or damage/destroy important parts of the installation	Aircraft impact	Target equipment is damaged due to aircraft impact	No

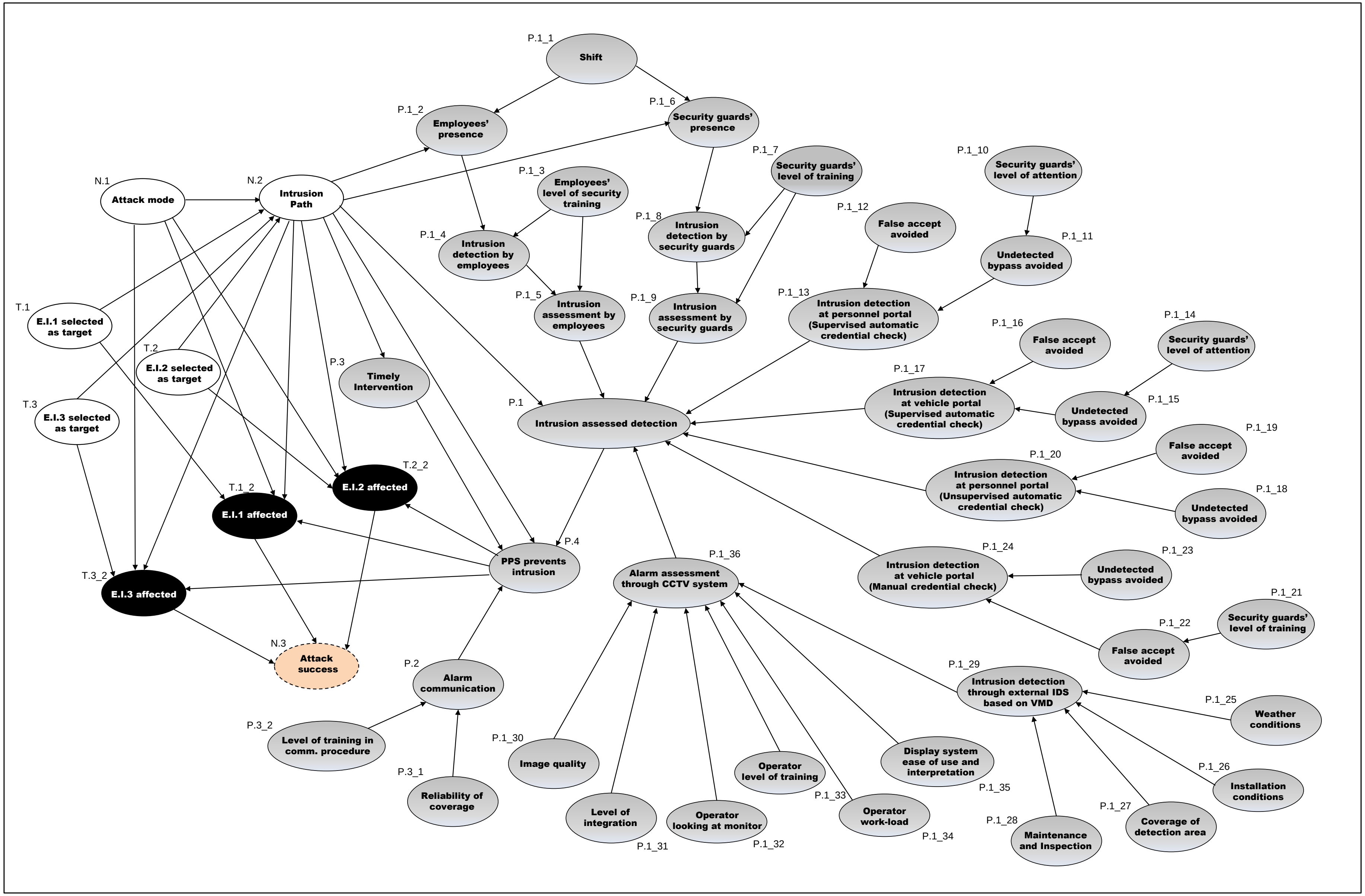
P.1_1
Shift
P.1_2
Employees' presence
P.1_6
Security guards' presence
P.1_7
Security guards' level of training
P.1_10
Security guards' level of attention
N.1
Attack mode
N.2
Intrusion Path
P.1_3
Employees' level of security training
P.1_8
Intrusion detection by security guards
P.1_12
False accept avoided
P.1_11
Undetected bypass avoided
P.1_4
Intrusion detection by employees
P.1_5
Intrusion assessment by employees
P.1_9
Intrusion assessment by security guards
P.1_13
Intrusion detection at personnel portal (Supervised automatic credential check)
T.1
E.I.1 selected as target
T.2
E.I.2 selected as target
T.3
E.I.3 selected as target
P.3
Timely Intervention
P.1_16
False accept avoided
P.1_14
Security guards' level of attention
P.1_17
Intrusion detection at vehicle portal (Supervised automatic credential check)
P.1_15
Undetected bypass avoided
P.1
Intrusion assessed detection
P.1_19
False accept avoided
P.1_20
Intrusion detection at personnel portal (Unsupervised automatic credential check)
P.1_18
Undetected bypass avoided
T.2_2
E.I.2 affected
T.1_2
E.I.1 affected
T.3_2
E.I.3 affected
P.4
PPS prevents intrusion
P.1_36
Alarm assessment through CCTV system
P.1_24
Intrusion detection at vehicle portal (Manual credential check)
P.1_23
Undetected bypass avoided
P.1_21
Security guards' level of training
P.1_22
False accept avoided
N.3
Attack success
P.2
Alarm communication
P.1_29
Intrusion detection through external IDS based on VMD
P.1_25
Weather conditions
P.3_2
Level of training in comm. procedure
P.3_1
Reliability of coverage
P.1_30
Image quality
P.1_31
Level of integration
P.1_32
Operator looking at monitor
P.1_33
Operator level of training
P.1_34
Operator work-load
P.1_35
Display system ease of use and interpretation
P.1_26
Installation conditions
P.1_27
Coverage of detection area
P.1_28
Maintenance and Inspection

Figure 1. Generic structure of Bayesian Network adopted for the probabilistic assessment of vulnerability to external attacks.

The node “Intrusion path” (N2 in Fig. 1) has *m+1* states. The number “*m*” and the specific paths to be accounted for should be selected by the analyst on the basis of site-specific and facility-specific considerations. This process consists in the identification of the foreseeable sequence of tasks that an attacker has to complete to guarantee the successful execution of a malevolent act attempt, and the associated physical location of the adversary inside site boundaries while performing these tasks. It represents the basis of the process known among physical security specialist as “path analysis” [14, 40] and requires a detailed knowledge of plant lay-out (e.g. potential target location within the site), access points and PPS elements location, which the authors assumed as fully available to security managers and plant managers. Clearly enough, only a sub-set of the *m* identified paths have a non-null conditional probability of being selected by the adversary given that a specific target equipment is selected as target (i.e. paths starting from outside the perimeter whose arrival point is the location of the specific target equipment).

The (*m+1)*-th state of “Intrusion path” node (see Fig. 1) corresponds to “no intrusion”. It has a conditional probability of occurrence equal to 1 given all attack modes that represent physical interference at a distance, i.e. interference actions that can be carried from outside the facility without requiring perimeter trespassing nor intrusion, for example shooting 2 or aircraft impact (see Table 1). The probabilistic values to populate the CPT of the “Intrusion path” node (see Fig. 1) are to be based on analyst judgement. Some guidelines and a sample evaluation are reported in the analysis of the case study (see Section 4).

3.2.2 Physical protection system effectiveness

The nodes shown in grey color in Fig. 1 constitute the BN portion dedicated to the analysis of the effectiveness of the physical protection system (PPS) that represents the preventive layer of physical security, and of its contribution in probabilistically determining the outcomes of an attack.

As it can be noticed from the network structure, the effectiveness of PPS is intended as an overall performance variable measured as the probability of successful PPS intervention, which is derived through a functional analysis of the PPS and modelled as dependent on adversary’s path. The Sandia effectiveness metric [50] was applied in the representation of “intrusion assessed detection”, “alarm communication” and “timely intervention” of response force as parent nodes of “PPS prevents intrusion” (see Fig. 1).

The necessary information for selecting modules and nodes to be represented were made available in a previous study [65]. In this study, the objective of carrying out the performance assessment of physical protection systems adopted to secure process industry is met through the conduction of an expert judgement exercise, which involved security managers of companies, security consultants, sites managers and safety managers having specific security expertise and responsibilities. It is worth mentioning that the expert elicitation of performance data may be a sound support to the present subjective probabilistic assessment based on knowledge judgment, that is a key element to strengthen the implementation of probabilistic assessment into security risk studies [38].

The elicitation of query variables selected in [65] was sufficient to quantify all network modules concerning PPS adopted herein; in fact, it concerned:

- the marginal probability of occurrence of the favorable state of each influencing factor;
- the conditional probability of successfully performing the primary security function, given that all identified influencing factors are in favorable state (this was considered as “baseline” to represent the best case in which the security function could be performed);

- the measure of impact, to be estimated as a multiplicative factor (ranging between 0 and 1), that each influencing factor has on the "baseline" conditional probability if it changes from the favorable to the unfavorable state.

For the sake of brevity, rules for quantifying the performance of PPS through the data gathered in [65] are summarized in detail in Appendix B.

3.2.3 Process equipment fragility models as attack targets

The nodes in black color in Fig. 1 were associated to the equipment items belonging to the facility and represent the uncertainty of each equipment item being damaged as a consequence of an attack. These nodes have binary states (namely "true" and "false"). In particular, "true" state of node "E.I.*j* affected*"* represents the condition of *j*-th equipment item being affected up to a point that a release of hazardous material is obtained. The damage condition can occur if and only if the *j*-th equipment item has been previously selected as a target (which means if node "E.I.*j* selected as target" is in "true" state) and the attack attempt has succeeded according to the previously defined success criteria, that are influenced by the attack mode (see Section 3.2.1 and Table 1).

The BN was quantified so that the successful execution of an attack attempt invariantly corresponds to "true" state of black nodes in Fig. 1. An auxiliary node named "attack success", having a CPT quantified as an OR-gate, was added to the network to represent in an aggregate form all possible variable states that lead to the undesired case, i.e. the success of a generic attack attempt.

Table 2 provides guidance on the rules and calculation models applied to quantify the conditional probabilities of a generic equipment item being damaged, given it has been selected as target and depending on the combination of states of remaining parent nodes (i.e. "attack mode", "PPS prevents intrusion").

It is worth remarking that for attack modes that require intrusion into site perimeter, the following simplifying assumptions was adopted: the successful preventive action of the PPS is sufficient for the attack attempt to be frustrated.

For attack attempts that involve the execution of misoperation or the direct assault of equipment (for example deliberate opening of valves, interference with objects retrieved on site, major interference to cause a breach in the tank by using sledgehammers or cutting torches etc.), it was conservatively assumed the tank residual resistance is negligible. Hence, the probability of target equipment being affected was conservatively set equal to 1 if the preventive action of PPS fails.

For what concerns the evaluation of the equipment damage probabilities when exposed to heat radiation (such as in the case of arson devices) and overpressure caused by explosions, fragility models based on probit equations were adopted. Probit models give the probability of the considered degree of equipment damage as a direct function of the intensity of physical effects associated to the impact vector of each attack mode, thus allowing a rather rapid assessment that gives probabilities as outputs and avoids the oversimplification of threshold approaches. Probit models were developed by in previous studies based on the application of physical modeling and analysis of equipment damage data for equipment exposed to fire heat radiation [66] and overpressure [67-69]. Appendix C reports more details on the probit models and on their development. The robustness of the adopted overpressure and fire fragility models was documented in the literature [70-73].

Table 2. Probabilistic assessment of equipment vulnerability to external attack modes.

Parent nodes' state		***Conditional probability of target equipment damage***	***Notes***
Attack mode	***PPS prevents intrusion***		
Deliberate misoperation	True	0	
	False	1	Conservative Assumption
Interference using simple aids	True	0	
	False	1	Conservative Assumption
Interference using major aids	True	0	
	False	1	Conservative Assumption
Arson using incendiary devices	True	0	
	False	Probit models, see Appendix C	Calculation
Use of explosives	True	0	
	False	Probit models, see Appendix C	Calculation
Shooting 1	True	0	
	False	1	Conservative Assumption
Shooting 2	True	1	Assumption
	False	1	Conservative Assumption
Vehicle accident	True	1	Conservative Assumption
	False	1	Conservative Assumption
Aircraft accident	True	1	Assumption
	False	1	Assumption

Finally, for what concern the remaining attack modes, despite relevant works were published to analyze the effects of shooting (see for example relevant reviews [74,75] and specific studies [76,77]) and vehicle or aircraft impact [78-80] on process equipment, the development of adequate fragility models for these impact vectors is still lacking. Therefore, the conservative assumption of adopting a unitary damage probability is considered for equipment items exposed to successful shooting attacks or to vehicle or aircraft impact, as summarized in Table 2. This choice introduces a simplification that certainly overestimates the possibility of process equipment being damaged, especially in the case of shooting attacks with small arms and vehicle impact, considering that process plant layout is designed so that process and storage equipment is located in restricted areas and set courses, physical obstacles and traffic circulation rules are adopted to limit incoming vehicles speed.

4. Definition of a case study

4.1 Description of the facility and physical security elements

In order to provide a sample application, the approach and BN developed in the present study were applied to the analysis of a case study concerning a chemical facility. Fig. 2 shows the lay-out considered, the physical protection systems and the adversary paths considered.

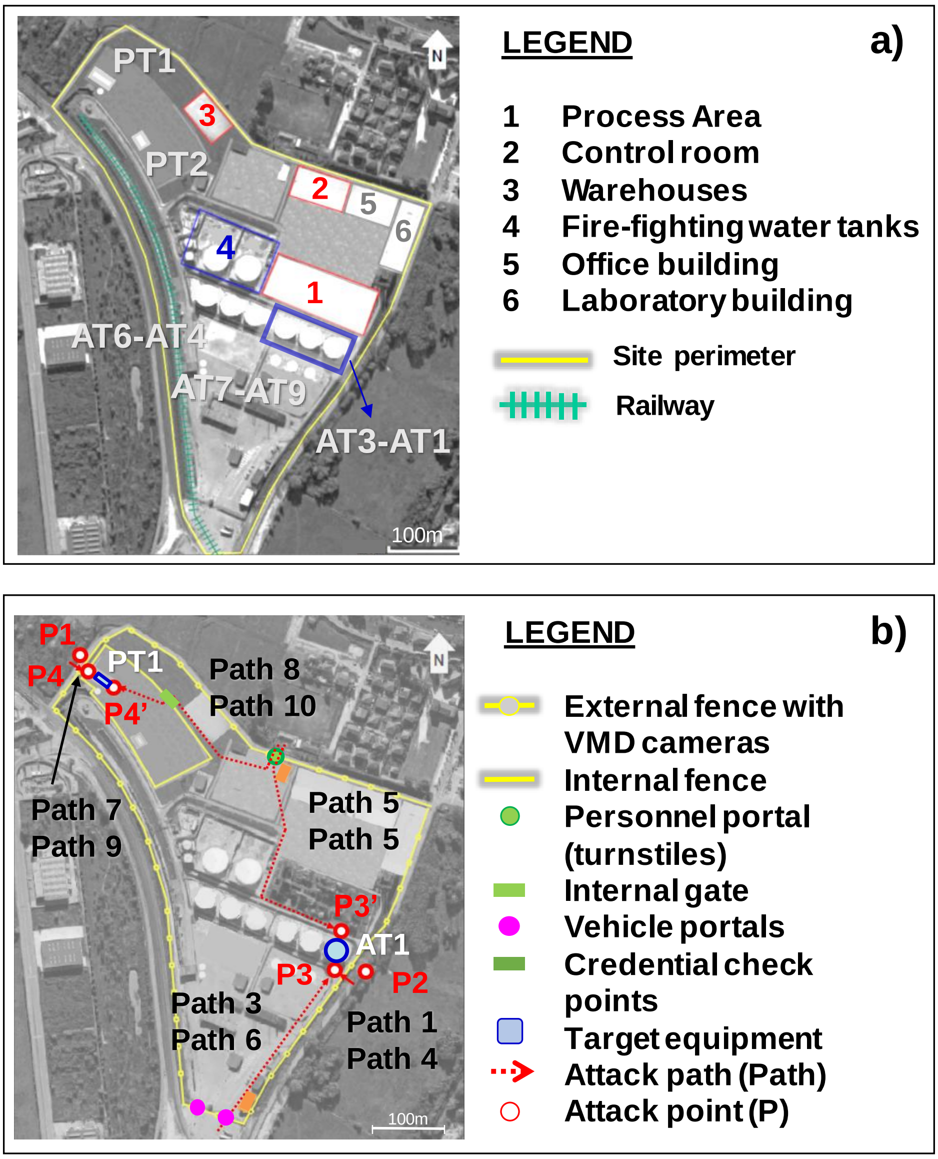

Figure 2. Chemical facility considered in the case study: a) facility layout; b) position of physical protection systems, attack positions (P) and adversary paths (Path) considered for attack scenarios listed in Table 5.

Table 3. Main features of the storage equipment considered in the case study. Vessel position and plant layout are shown in Fig. 2a.

Equipment ID	**Tank type**	**Diameter (m)**	**Height/ Length (m)**	**Stored substance**	**Inventory (ton)**	**Operating pressure (barg)**
AT1	Atmospheric	9	16.2	Wet solvent[a]	650	0.02
AT2	Atmospheric	9	16.2	Dry solvent[a]	650	0.02
AT3	Atmospheric	9	3.6	Paraffin oil	180	0.02
AT4 - AT5 - AT6	Atmospheric	9	3.6	Polymer emulsion	200	0.02
AT7 - AT8 - AT9	Atmospheric	6	5.4	Additives[b]	100	0.1
PT1	Pressurized	4	18	1,3 Butadiene	150	3.5
PT2	Pressurized	2.8	6	Waste hydrocarbon	35	1

[a] Hexane, nominal storage 1030 m^3
[b] Antioxidant, de-emulsifier, viscosity regulation

Table 4. Summary of PPS elements adopted in the facility considered for the case study. See Fig. 2b for the position of PPS elements.

ID	**Physical security element**	**Function**
PS01	Detection & assessment by employees working on site during day shifts	Intrusion Detection & Assessment
PS02	Detection & assessment by roving guards during night shift	Intrusion Detection & Assessment
PS03	Video Motion Detection cameras integrated to Closed Circuit Television (CCTV) along fence line[a]	Intrusion Detection & Assessment
PS04	Manual credential checks at vehicle portal	Intrusion Detection & Assessment
PS05	Supervised automatic credential check at personnel portal	Intrusion Detection & Assessment
PS06	Perimeter fence[b]	Delay
PS07	Internal fence[b]	Delay
PS08	Mesh gate with padlock	Delay
PS09	Dike wall	Delay
PS10	Radio communication of alarm	Communication & Response
PS11	External response force intervention	Communication & Response

[a] Camera images assessment is carried out by a security officer through monitors in the central control room
[b] Vinyl coated 1.8 mm x 40 mm mesh fence

The facility considered in the case-study is designed to produce polybutadiene from the polymerization of butadiene monomer. The synthesis process requires hexane as a solvent and the use of several additives. Hence, toxic and flammable substances are handled at the site. Fig. 2b displays the main physical protection system elements implemented to protect the site. Table 3 summarizes the main characteristics of the storage tanks considered in the vulnerability analysis. Table 4 summarizes the features of each element of the physical protection system. As shown in Fig. 2b, there are three access points to the site: the personnel and visitors entry portal to the North and two vehicle portals for railcars and tank cars entry. At personnel portal, access control is guaranteed through supervised automatic credentials (ID-badges) check. Two security guards are present at the

security post located close to the south portals during the opening hours (day shift, 16 hours a day) in order to oversee vehicle access and perform the manual check of driver and shipment credentials.
Although meant for illustrative purpose only, the case study is representative of industrial installations, since a realistic lay-out and set of physical security countermeasures was considered. However, numerical values and scenarios discussed are to be intended as illustrative and not concerning existing facilities.

4.2 Description of attack scenarios

For the sake of brevity, the site vulnerability analysis was carried out considering only two potential targets, namely the pressurized vessel PT1 and the atmospheric tank AT1, and a few significant attack scenarios which, however, represent typical attack modes based on past events. In particular, the analysis concerned intrusion attempts aimed at conducting deliberate misoperations or aimed at positioning improvised explosive devices (IEDs) in close proximity of storage tanks, as well as attacks with vehicle bombs from outside the facility perimeter. All categories of actions are intended to cause a massive release of the hazardous material present inside the target vessels considered. Several intrusion paths were accounted for. A summary of attack scenarios considered is shown in Table 5. Attack positions and adversary's paths are sketched in Fig. 2b.
In the case study presented herein, Ammonium Nitrate (AN) – Fuel Oil (i.e. ANFO) mixtures and Acetone Peroxide or Triacetone Triperoxide Peroxyacetone (TATP) mixtures were selected as reference explosives, since they are often adopted for terrorist attacks, suicide bombing, and other malicious uses [81-83]. A detailed description of ANFO and TATP characteristics in terms of TNT trinitrotoluene) equivalence, ideal detonation energy and other properties that affect explosive effects are reported elsewhere [22].

4.3 BN quantification input data

Fig. 3 illustrates the BN portion that was considered for case study analysis. As stated above, for the sake of brevity only the nodes associated to PT1 and AT1 were considered as potential targets according to the set of attack scenarios analyzed. The modules included in the representation of PPS were selected in light of the implemented physical security elements. In particular, Table 6 illustrates which PPS elements were regarded as performing the design preventive function along the analyzed attack paths. The conditional probability table of node *"Intrusion assessed detection"* was filled in accordingly.

Table 5. Summary of attack scenarios considered in the case study. ANFO: Ammonium Nitrate (AN) – Fuel Oil mixture; TATP: Triacetone Triperoxide Peroxyacetone mixtures; n.a. = not applicable. For path and attack position, refer to Fig. 2b.

ID	Target ID	Attack mode	Attack aim	Position	Attack path	Day/ Night	IED type	IED quantity (kg)
A	AT1	Explosive	Detonate truck bomb outside facility perimeter	P_1	No intrusion path	-	ANFO	1000
B	PT1	Explosive	Same as B	P_2	No intrusion path	-	ANFO	1000
C	AT1	Explosive	Detonate backpack bomb in close proximity to the target	P_3	Path 1	Day	TATP	15
D	AT1	Explosive	Same as C	P_3'	Path 2	Day	TATP	15
E	AT1	Explosive	Same as C	P_3	Path 3	Day	TATP	15
F	AT1	Explosive	Same as C	P_3	Path 1	Night	TATP	15
G	PT1	Explosive	Same as C	P_4'	Path 7	Day	TATP	15
H	PT1	Explosive	Same as C	P_4	Path 8	Day	TATP	15
I	PT1	Explosive	Same as C	P_4'	Path 7	Night	TATP	15
J	AT1	Deliberate misoperation	Open drain valve to cause massive release and ignite flammable liquid	P_3	Path 4	Day	n.a.	n.a.
K	AT1	Deliberate misoperation	Same as J	P_3'	Path 5	Day	n.a.	n.a.
L	AT1	Deliberate misoperation	Same as J	P_3	Path 6	Day	n.a.	n.a.
M	AT1	Deliberate misoperation	Same as J	P_3	Path 4	Night	n.a.	n.a.
N	PT1	Deliberate misoperation	Same as J	P_4'	Path 9	Day	n.a.	n.a.
O	PT1	Deliberate misoperation	Same as J	P_4	Path 10	Day	n.a.	n.a.
P	PT1	Deliberate misoperation	Same as J	P_4'	Path 9	Night	n.a.	n.a.

Table 6. PPS elements that perform the preventive function along the analyzed attack paths and during work shifts. PPS elements are described in Table 4.

Scenario ID	**Path &Shift**	**Physical security elements**										
		PS01	**PS02**	**PS03**	**PS04**	**PS05**	**PS06**	**PS07**	**PS08**	**PS09**	**PS10**	**PS11**
C	Path 1 Day	X		X			X			X	X	X
F	Path 1 Night		X	X			X			X	X	X
D	Path 2 Day	X				X				X	X	X
E	Path 3 Day	X			X					X	X	X
J	Path 4 Day	X		X			X			X	X	X
M	Path 4 Night		X	X			X			X	X	X
K	Path 5 Day	X				X				X	X	X
L	Path 6 Day	X			X					X	X	X
G	Path 7 Day	X		X			X	X		X	X	X
I	Path 7 Night		X	X			X	X		X	X	X
H	Path 8 Day	X				X			X	X	X	X
N	Path 9 Day	X		X			X	X		X	X	X
P	Path 9 Night		X	X			X	X		X	X	X
O	Path 10 Day	X				X			X	X	X	X

BN quantification was carried out adopting the following assumptions:

- The conditional probability of employees being present along the adversary's path to spot an intrusion is path dependent, hence the following values were assumed: 0.70 for paths crossing process, storage and building areas; 0.20 for paths crossing the loading area in the southern-most part of the site; 0.07 for relatively short paths at facility internal boundaries.
- An average value of marginal probability of security guards' presence equal to 0.05 was considered for all areas during night shift.
- The conditional probability of having a timely intervention of the response force given intrusion assessed detection was calculated for each analyzed path through the use of EASI (Estimate of Adversary Sequence Interruption) analysis (conducted according to the model presented in [40]). Table C.1 in Appendix D summarizes the calculated values.
- The normal distribution characterizing response force intervention time has a mean value of 5 minutes and a variance of 20%.
- For the sake of simplicity, the attack modes *"deliberate misoperation"* and *"use of explosives"* were set as equally probable.
- Similarly, the adversary paths identified as credible given attack mode and target equipment were assigned equal probabilities of being chosen.

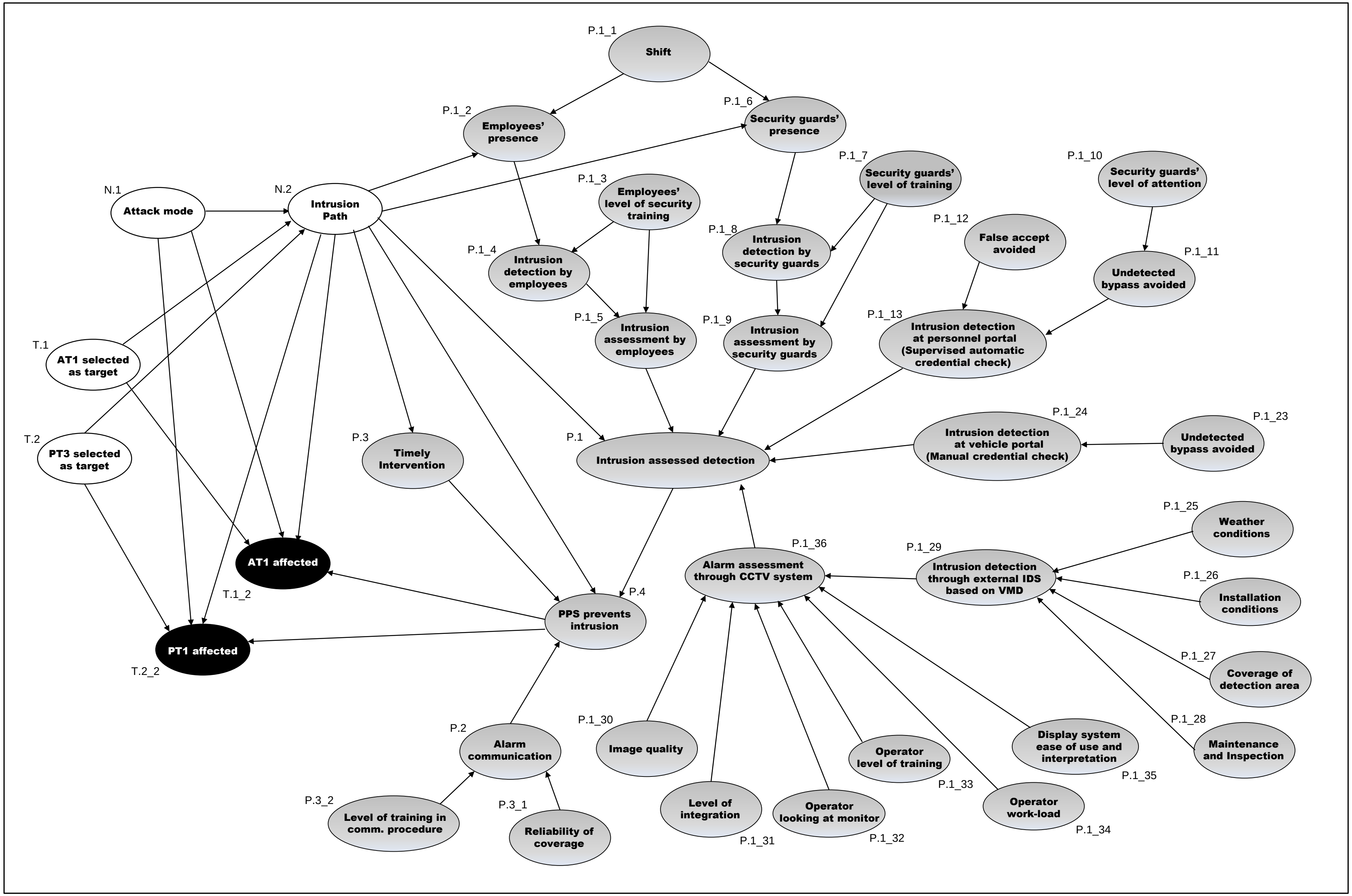
P.1_1
Shift
P.1_2
Employees' presence
P.1_6
Security guards' presence
P.1_7
Security guards' level of training
P.1_10
Security guards' level of attention
N.1
Attack mode
N.2
Intrusion Path
P.1_3
Employees' level of security training
P.1_8
Intrusion detection by security guards
P.1_12
False accept avoided
P.1_11
Undetected bypass avoided
P.1_4
Intrusion detection by employees
P.1_5
Intrusion assessment by employees
P.1_9
Intrusion assessment by security guards
P.1_13
Intrusion detection at personnel portal (Supervised automatic credential check)
T.1
AT1 selected as target
P.1_24
Intrusion detection at vehicle portal (Manual credential check)
P.1_23
Undetected bypass avoided
T.2
PT3 selected as target
P.3
Timely Intervention
P.1
Intrusion assessed detection
P.1_25
Weather conditions
P.1_36
Alarm assessment through CCTV system
P.1_29
Intrusion detection through external IDS based on VMD
AT1 affected
T.1_2
P.4
PPS prevents intrusion
P.1_26
Installation conditions
PT1 affected
T.2_2
P.1_27
Coverage of detection area
P.2
Alarm communication
P.1_30
Image quality
Display system ease of use and interpretation
P.1_35
P.1_28
Maintenance and Inspection
Operator level of training
P.1_33
P.3_2
Level of training in comm. procedure
P.3_1
Reliability of coverage
Level of integration
P.1_31
Operator looking at monitor
P.1_32
Operator work-load
P.1_34

Figure 3. Bayesian Network applied to the analysis of the case study.

This latter choice may be an acceptable first guess estimate, which neglects the representation of adversary's preference in favor of easier to accomplish actions or less detectable actions but is still functional to the path-specific calculation of PPS effectiveness.

The probability of attack success while targeting a specific equipment item was calculated to estimate the vulnerability of each equipment item. Moreover, scenario-based vulnerability assessment was carried out in order to calculate the probability of attack success for each scenario listed in Table 5.

In the analysis of attack scenarios based on the use of IEDs, the value of peak overpressure impacting on target was calculated as a function of the net equivalent charge of TNT and the distance from the explosion point, applying to the procedure of Landucci et al. [22] summarized in Appendix C. The results of these calculations are reported in Table 7 for attack scenarios involving the use of IEDs. The overpressure values obtained are input to the probit model for overpressure (see Appendix C and Table B.1) to obtain the conditional probability of damage due to IEDs, supporting CPTs quantification shown in Table 7.

Table 7. Conditional probability of target equipment damage given the attack scenarios involving the use of IED (p_s = peak static overpressure).

Scenario	IED	Quantity (kg)	TNT efficiency (η)	Target Equipment	Distance (m)	p_s (kPa)	Probit	Conditional damage Probability
A	ANFO[a]	1000	0.23	AT1	30	33.7	6.48	0.931
B	ANFO[a]	1000	0.23	PT1	26	43.3	3.78	0.112
C, D, E	TATP	15	0.61	AT1	2.5	1210	15.2	1.000
G, H, I	TATP	15	0.61	PT1	2.5	1210	18.2	1.000

[a] Commercial ammonium nitrate is considered to constitute the explosive, hence 50% wt. ammonium nitrate and 50% wt. inert dolomite [22].

5. Results

The computation of the BN provided in Fig. 3 allowed deriving the conditional probability of success for the set of attack scenarios considered in the case study. The probability values obtained are reported in the seventh column of Table 8 and represent a measure of scenario-specific vulnerability. Table 8 also reports the attack scenario specific values of conditional probability of the physical protection system successfully accomplishing its functions. Prior probabilities of the developed BN are reported in the first row for the sake of completeness.

As expected, for attack scenarios A and B, involving the use of truck bombs placed outside site perimeter, the conditional probability of success of all preventive security functions is null, since existing PPS elements are only positioned along the fence line and inside perimeter. Therefore, the probability of attack success coincides with the probability of target equipment damage due to explosion effects (which are the reference attack vector in these cases).

For attack scenarios involving a deliberate misoperation attempt (from J to P), the probability of attack success results equal to the conditional probability of PPS failure in its preventive function, since reaching close proximity to the selected target was conservatively assumed as a success criterion (see Table 1). In the case of attack scenarios C to I, the conditional probability of attack success is derived as the product of conditional probability of PPS failure and the conditional probability of target equipment being damaged by TATP explosion effects. The latter value is estimated as equal to 1 after the application of the overpressure fragility model (see Appendix C), as a consequence of the very short distance from the target (see Table 7) at which the IED explosion is triggered.

As far as PPS effectiveness is concerned, it is equal to 0 in 8 of the 14 attack scenarios analyzed involving intrusion in the site: in all cases, the PPS action is frustrated by the incapability to provide an adequate response action before adversary tasks along path 1, 4, 7 and 9 are completed (see Appendix D for input data). The conditional probability of PPS successfully preventing the remaining attack scenarios varies in the range 0.10 – 0.32.

BN computation was applied also to the calculation of target equipment vulnerability measures with more generalized validity, which are reported in Fig. 4.

Table 8. Case study results: attack scenario analysis. Prior probabilities of the developed BN are reported in *italic*.

Attack scenario ID	**Intrusion assessed detection (*"success"* state)**	**Timely Intervention (*"success"* state)**	**PPS prevents intrusion (*"success"* state)**	**AT1 affected (*"true"* state)**	**PT1 affected (*"true"* state)**	**Attack Success (*"true"* state)**
Priors	*0.0983*	*0.0220*	*0.0180*	*0.0759*	*0.0512*	*0.123*
A	0.000	0.000	0.000	0.931	0.000	0.931
B	0.000	0.000	0.000	0.000	0.112	0.112
C	0.494	0.000	0.000	1.000	0.000	1.000
D	0.953	0.172	0.141	0.859	0.000	0.859
E	0.974	0.121	0.101	0.899	0.000	0.899
F	0.483	0.000	0.000	1.00	0.000	1.00
G	0.494	0.000	0.000	0.000	1.00	1.00
H	0.953	0.178	0.146	0.000	0.854	0.854
I	0.483	0.000	0.000	0.000	1.00	1.00
J	0.494	0.000	0.000	1.00	0.000	1.00
K	0.953	0.391	0.320	0.680	0.000	0.680
L	0.974	0.358	0.300	0.700	0.000	0.700
M	0.483	0.000	0.000	1.00	0.000	1.00
N	0.494	0.000	0.000	0.000	1.00	1.00
O	0.953	0.395	0.324	0.000	0.676	0.676
P	0.483	0.000	0.000	0.000	1.00	1.00

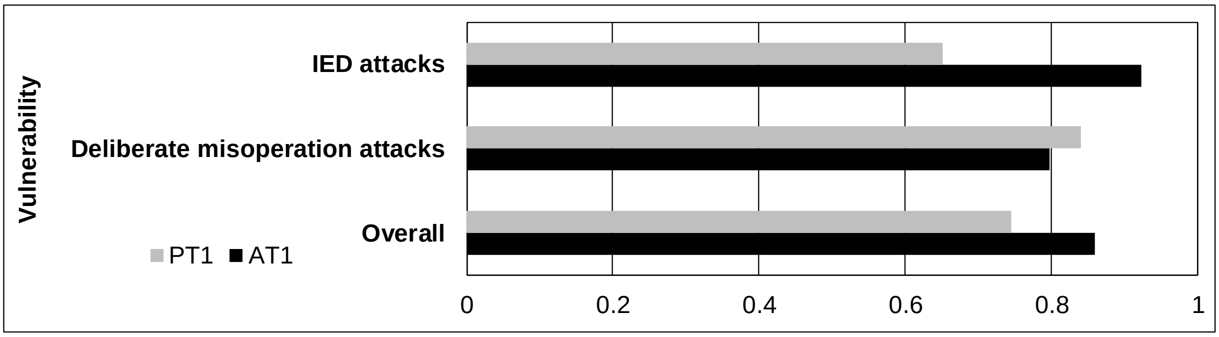

Figure 4. Summary of vulnerability assessment for the two target vessels considered (tanks PT1 and AT1).

6. Discussion

The results shown in Section 5 demonstrate the potentiality of the present approach in supporting quantitative security vulnerability studies in a dual perspective. A first issue is that, according to the vulnerability definition of Section 2.3, the assessment of attack success probability given a target equipment is considered a measure of equipment vulnerability and, at the same time, of the likelihood of attack success term for security risk assessment studies [10]. Therefore, this may support the identification of the most security-critical equipment items. In the demonstrative case study, the overall vulnerability of the atmospheric tank (AT1) is about 15% higher than that estimated for the pressurized tank (PT1), as shown in Fig. 4, due to the inherent higher structural fragility of AT1 vessel, but also due to the location and the different configuration of physical security elements.

Secondarily, the present analysis allows for the identification of the more critical attack scenarios and, eventually, the effectiveness of physical security systems in stopping the execution of an attack. In fact, in the demonstrative case study, protection against intentionally induced losses was shown to be not completely adequate, depending on the type of scenario. Improvements may be obtained if the "Defence in Depth" principle [84] is applied in the design of physical security elements, by deploying concentric rings of protection to defend critical targets, where each ring represents an independent defense that accomplishes or triggers the success of primary protection functions of assessed detection (which is often critical and not redundant), delay and response.

It is worth mentioning that in the case study, only two targets were considered for the quantification of the Bayesian network. However, the network shown in Fig. 1 may be extended to more complex configurations introducing all the relevant targets in a given facility and eventually extending the analysis even to complex interconnected facilities, such as chemical clusters [17]. In particular, for any further piece of equipment or asset included in the analysis, two nodes need to be added. One node represents the probability that a given i-th target is selected for the attack (i.e., T.i in Fig. 1), and one node expresses the likelihood that the i-th target is affected by the attack (node T.i_2 in Figure 1). However, the choice of adding further targets strongly affects the quantification of the network, with possible state explosion for nodes P.1 and P.4 (see Figure 1). Therefore, it is recommended to carry out a preliminary screening among the targets and assets in a given facility, in order to limit the computational efforts, such as the preliminary simplified attractiveness assessment carried out in the present study [61].

Despite the risk and mathematical framework supporting the quantification of the Bayesian network (see Eqs. (1)-(4)) features a general validity, the present method shall be considered tailored to chemical facilities and to industrial sites featuring the risk of major accidents [9]. In fact, the PPS architecture based on the three functions "detect-delay-respond" is common to other sectors, but the performance data were specifically gathered and reflect the PPS "typicals" in the present industrial sector [65]. Moreover, equipment vulnerability models for the determination of equipment failure probability are specifically related to process and storage units and need to be modified in case of extension to other industrial sectors and assets.

Therefore, through the present method, a step ahead can be made in the concrete determination of the existing level of chemical and process facilities protection against external malevolent attacks and in the identification of weak elements. These objectives cannot be achieved by the compliance-based assessment of security countermeasures nor by a qualitative assessment of physical security systems seen as a whole, which are as yet proposed in the majority of security risk assessment methods.

However, it should be remarked that for the analyzed case study, the joint probability of the node attack success being "true"[2] cannot constitute a representative measure of the overall vulnerability of the facility. Indeed, obtaining such a measure would have required the inclusion in the BN structure of nodes representing every equipment item and the analysis of all credible paths leading to them, as well as of all attack modes. Hence, in accordance with other general risk assessment procedures [23], the completeness of analysis in terms of evaluation of all relevant attack scenarios (i.e. attack modes, potential target equipment and attack paths) is a key issue.

Despite the potential value of the results obtained in the perspective of security management in chemical facilities, it is worth to mention that the present approach features some limitations, mainly due to the simplified assumptions adopted and to the extensive use of expert judgement to quantify BN conditional probability tables. The main simplifying assumptions adopted concern: i) the description of attack scenarios through a schematization according to which the selection of target equipment and attack mode are seen as independent, which is however compatible to the level of detail that characterizes an analysis carried out according to existing security risk assessment methodologies; ii) the binary nature assumed for factors that influence the performance of PPS, which needed to be introduced in order to avoid the explosion of BN states; iii) the straightforward evaluation of the probability of target equipment damage in case of attack vectors for which vulnerability models are not available yet, which is however an assumption on the safe side (see Section 3.2.3).

The use of expert judgement to CPTs quantification is justifiable in light of the complex non-physically explainable nature of the considered dependencies and of the lack of reliable quantitative data in the technical literature concerning PPS performance. It should also be noted that, according to the presented analysis, PPS plays its preventive role only in the case of external attack scenarios that involve intrusion. However, this is not a limitation of the method, but a system limitation, since almost all chemical and process industry sites adopt measures to avoid intrusion while these installations result more vulnerable (especially as far as the preventive physical security layer is concerned) with respect to attack scenarios characterized by a higher criminal energy: for example, attacks that use remotely controlled or long distance heavy weapons or other technologically sophisticated tools (e.g. rocket-propelled grenades, drones, etc.) or that involve the use of considerable quantities of explosives outside the perimeter fence in order to damage plant facilities, as addressed in the case study.

7. Conclusions

In the present study, a quantitative approach for the evaluation of the vulnerability of industrial installations with respect to external acts of interference was presented. The approach is based on the application of Bayesian networks to evaluate the vulnerability and is specifically dedicated to chemical and process facilities.

The present study relies on the structured implementation of knowledge support in the evaluation of subjective probability in the vulnerability assessment, which constitutes an element of novelty in security studies dedicated to the chemical and process industry. In particular, a specific expert elicitation process was applied to express uncertainties related to the performance of physical security

[2] The node is in the "true" state if at least one of the two targets (AT1 and PT1) is successfully damaged after the attack

countermeasures [65]; moreover, equipment fragility models were adopted to derive a sound probabilistic evaluation of attack success associated with equipment failure.

The application to an industrial case study demonstrated the practical and informative implications of the method, providing risk analysts, safety and security managers with a useful support i) to address the identification of the more critical target equipment, ii) to evidence possible weaknesses in the protection system, and iii) to drive the technical response measures and investments to reduce the facility vulnerability. The method application is a benchmark to experiment possible alternative security countermeasures or the to test the upgrade in existing security protections.

Future developments of the approach are related to the inclusion in the present method of consequences and impact of the identified escalation scenarios, and to the likelihood of attack, in order to support the integration into conventional process safety risk studies [85], obtaining a holistic determination of safety and security related risk in chemical facilities.

References

[1] Cozzani V, Krausmann E, Reniers G. Other Causes of Escalation. In: Cozzani V, Reniers G, editors. Domino Effects in the Process Industries: Modelling, Prevention and Managing, Amsterdam, the Netherlands: Elsevier; 2013, p. 154-174.

[2] Landucci G, Tugnoli A, Spadoni G, Cozzani V. LNG Regasification Terminals: Assessment of Accidents due to External Acts of Interference, In: Proc of 11th Int Probab Saf Assess Manag Conference and Annl Eur Saf and Reliability Conference 2012; 4373-4382.

[3] Argenti F, Landucci G, Spadoni G, Cozzani V. The assessment of process plant attractiveness related to terrorist attack. Saf Sci 2015; 77C:169-181.

[4] 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).

[5] Baybutt P, Reddy V. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homel Def J; 2003;2:1.

[6] Bajpai S, Gupta JP. Site security for Chemical Process Industry. J Loss Prevention Process Ind 2005;18(4–6), 301–309.

[7] Office of the Law Revision Counsel of the United States House of Representatives. Chemical Facility Anti-terrorism Standards. United States Code, Title 6, Chapter 1, Subchapter XVI. http://uscode.house.gov/view.xhtml?path=/prelim@title6/chapter1/subchapter16&edition=prelim

[8] European Commission. 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 of Eur Union 2008; L345: 75–82.

[9] European Commission, 2012. Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC Text with EEA relevance. Off J Eur Union 2012; L197: 1-37.

[10] American Petroleum Institute (API). ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry. New York: American Petroleum Institute; 2013.

[11] American Institute of Chemical Engineers, Center of Chemical Process Safety (AIChE-CCPS). Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. New York: American Institute of Chemical Engineers, Center of Chemical Process Safety; 2003.

[12] Jaeger CD. Chemical facility vulnerability assessment project. J Hazard Mater 2003;104: 207–213.

[13] U.S. Department of Justice. A Method to Assess the Vulnerability of U.S. Chemical Facilities. Report NCJ 195171. Washington: Office of Justice Programs; 2002.

[14] Norman TL. Risk Analysis and Security Countermeasure Selection. Boca Raton: CRC Press; 2010.

[15] Reniers G, Dullaert W, Audenaert A, Ale BJM, Soudan K. Managing domino effect-related security of industrial areas. J Loss Prev Process Ind 2008; 21(3): 336-343.

[16] Reniers G, Sörensen K, Khan F, Amyotte P. Resilience of chemical industrial areas through attenuation-based security. Reliability Eng Syst Saf 2014; 131:94-101.

[17] Reniers G, Audenaert A. Preparing for major terroristic attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Saf and Environ Prot 2014; 92(6): 583-589.

[18] Keeney GL, von Winterfeldt D. Identifying and Structuring the Objectives of Terrorists Risk Anal 2010; 30(12):1803-1816.

[19] Sabatini M, Zanelli S, Ganapini S, Bonvicini S, Cozzani V. Ranking the attractiveness of industrial plants to external acts of interference. (2009) Proc Joint ESREL and SRA - Eur Conf 2009; 2: 1199-1205.

[20] Hausken K, Levitin G. Review of Systems Defense and Attack Models. Int J Performability Eng 2012;8:355–66.

[21] Salzano E, Antonioni G, Landucci G, Cozzani V. Domino effects related to explosions in the framework of land use planning. Chem Eng Trans 2013; 31: 787–792. http://doi.org/10.3303/CET1331132

[22] Landucci G, Reniers G, Cozzani V, Salzano E. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliability Eng Syst Saf 2015;143:53–62.

[23] Cox LA. Some Limitations of “Risk = Threat × Vulnerability × Consequence” for Risk Analysis of Terrorist Attacks. Risk Anal 2010;28(6):1749-.61

[24] Ezell BC, Bennett SP, von Winterfeldt D, Sokolowski J, Collins AJ. Probabilistic Risk Analysis and Terrorism Risk. Risk Anal, 2010; 30(4):575-89.

[25] Parnell GS, Smith CM, Moxley FI. Intelligent Adversary Risk Analysis: A Bioterrorism Risk Management Model. Risk Analysis 2010; 30 (1): 32-48.

[26] Greenberg MR, Cox LA. Introduction to Special Issue: Advances in terrorism risk analysis. Risk Anal 2010.

[27] Garrick BJ, Hall JE, Kilger M, McDonald JC, O’Toole T, Probst PS et al. Confronting the risks of terrorism: making the right decisions. Reliability Eng Syst Saf 2004;86:129–76.

[28] Paté-Cornell ME, Guikema S. Probabilistic modelling of terrorist threats: a system analysis approach to setting priorities among countermeasures. Military Operations Res 2002; 7:5-20.

[29] Apostolakis GE, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Anal 2005; 25(2): 361-76.

[30] Hausken K. Probabilistic Risk Analysis and Game Theory. Risk Anal 2002;22:17–27.

[31] Hausken K. Protecting complex infrastructures against multiple strategic attackers. Int J Syst Sci 2011;42:11–29.

[32] Chopra SS, Khanna V. Interconnectedness and interdependencies of critical infrastructures in the US economy: Implications for resilience. Phys A Stat Mech Its Appl 2015;436:865–77.

[33] Wu B, Tang A, Wu J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. Reliab Eng Syst Saf 2016;147:1–8.

[34] Zhang P, Cheng B, Zhao Z, Li D, Lu G, Wang Y, et al. The robustness of interdependent transportation networks under targeted attack. EPL (Europhysics Lett) 2013;103:68005p1-p5.

[35] Crowl DA, Louvar JF. Chemical process safety – Fundamentals with applications. 2nd ed. New Jersey: Prentice Hall PTR; 2002.

[36] Amundrud Ø, Aven T, Flage R. How the definition of security risk can be made compatible with safety definitions. Proc IMechE Part O J Risk Reliab 2017;231:286–94.

[37] Jore SH and Egeli A. Risk management methodology for protecting against malicious acts – are probabilities adequate means for describing terrorism and other security risks? In: Podofillini L, Sudret B, Stojadinovic B, et al. (eds) Safety and reliability of complex engineered systems (Proceedings of the 2014 European safety and reliability conference, Wroclaw, Poland, 14–18 September 2014). Boca Raton, FL: CRC Press, 2014, pp.807–815.

[38] Aven T. Probabilities and background knowledge as a tool to reflect uncertainties in relation to intentional acts. Reliab Eng Syst Saf 2013;119:229–34..

[39] Kriaa S, Pietre-cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Saf 2015;139:156–78.

[40] Garcia ML. The Design and Evaluation of Physical Protection Systems. Burlington: Elsevier Butterworth-Heinemann; 2008.

[41] Aven T. A unified framework for risk and vulnerability analysis covering both safety and security**.** Reliability Eng Syst Saf 2007;92(6):745–54.

[42] Hausken K. A cost–benefit analysis of terrorist attacks. Def Peace Econ 2016:1–19. doi:10.1080/10242694.2016.1158440

[43] Villa V, Reniers GLL, Paltrinieri N, Cozzani V. Development of an economic model for the allocation of preventive security measures against environmental and ecological terrorism in chemical facilities. Process Saf Environ Prot 2017;109:311–39.

[44] Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems. Reliability Eng Syst Saf 2013;120:27–38.

[45] Haymes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Anal 2006;26(2):293–6.

[46] Setola R, De Porcellinis S, Sforna M. Critical infrastructure dependency assessment using the input–output inoperability model. Int J Critical Infrastructure Protection 2009; 2(4): 170-8.

[47] Marrone S, Nardone R, Tedesco A, D'Amore P, Vittorini V, Setola R, De Cillis F, Mazzocca N. Vulnerability modeling and analysis for critical infrastructure protection applications. Int J Critical Infrastructure Protection 2013; 6(3-4): 217-27.

[48] Levitin G, Gertsbakh I, Shpungin Y.Evaluating the damage associated with intentional network disintegration. Reliability Eng Syst Saf 2011; 96(4):433-9.

[49] Woods D. Essential characteristics of resilience. In: Leveson N, E. Hollnagel E, Woods D, editors, Resilience engineering: concepts and precepts. Aldershot: Ashgate; 2006, p. 21–34.

[50] Garcia ML. Vulnerability Assessment of Physical Protection Systems. Burlington: Elsevier Butterworth-Heinemann; 2006.

[51] Vellani K. Strategic Security Management: A Risk Assessment Guide for Decision Makers. Oxford (UK): Butterwoth-Heinemann; 2006

[52] Pearl J. 1988. Probabilistic Reasoning in Intelligent Systems. Morgan Kaufmann, San Francisco, CA.

[53] Neapolitan R. 2003. Learning Bayesian Networks. Prentice Hall, Inc., Upper Saddle River, NJ, USA.

[54] Charniak E. Bayesian networks without tears. Artificial Intell Mag 1991; 12(4): 50-63.

[55] Jensen FV, Nielsen TD. Bayesian networks and decision graphs. 2nd ed. New York: Springer; 2007.

[56] Abimbola M, Khan F, Khakzad N, Butt S. Safety and risk analysis of managed pressure drilling operation using Bayesian network. Saf Sci 2015;76:133–44.

[56] Baksh A-A, Khan F, Gadag V, Ferdous R. Network based approach for predictive accident modelling. Saf Sci 2015;80:274–87.

[58] Khakzad N, Khan F, Amyotte P. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Saf Sci 2013;57:108–17. doi:10.1016/j.ssci.2013.01.022.

[59] Khakzad N, Khan F, Amyotte P, Cozzani V. Domino Effect Analysis Using Bayesian Networks. Risk Anal 2013; 33(2): 292–306.

[60] Andersen, S. 1989. HUGIN—A shell for building Bayesian belief universes for expert systems. In Proc of the 11th Int Jt Conference on Artificial Intelli. Menlo Park, California: Int Jt Conferences on Artificial Intell; 1989, p. 1080–5.

[61] Argenti F, Landucci G, Reniers G, 2016, Probabilistic vulnerability assessment of chemical clusters subjected to external acts of interference. Chem Eng Trans 2016; 48: 691-696. DOI:10.3303/CET1648116

[62] Störfallkommission (SFK). SFK – GS – 38, Report of the German Hazardous Incident Commission. Baden: Störfallkommission; 2002.

[63] START database, www.start.umd.edu/gtd, last accessed on 10th June 2017

[64] Cozzani V, Tugnoli A, Bonvicini S, Salzano E. Threshold-Based Approach. In: Cozzani V, Reniers G, editors. Domino Effects in the Process Industries: Modelling, Prevention and Managing. Amsterdam (NL): Elsevier; 2013, p. 12-29.

[65] Argenti F, Landucci G, Cozzani V, Reniers G. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Saf Sci 2017;94:181–96.

[66] Landucci G, Cozzani V, Birk M. Heat Radiation Effects. In: Cozzani V, Reniers G, editors. Domino Effects in the Process Industries: Modelling, Prevention and Managing. Amsterdam, The Netherlands: Elsevier; 2013, p. 70–115.

[67] Cozzani V, Salzano E. The quantitative assessment of domino effects caused by overpressure: Part I. Probit models. J Hazard Mater 2004; 107(3): 67–80.

[68] Salzano E, Cozzani V. The analysis of domino accidents triggered by vapor cloud explosions. Reliability Eng Syst Saf 2005; 90(2-3): 271–284.

[69] Salzano E, Hoorelbeke P, Khan F, Amyotte P. Overpressure Effects. In: Cozzani V, Reniers G, editors. Domino Effects in the Process Industries: Modelling, Prevention and Managing. Amsterdam, The Netherlands: Elsevier; 2013, p. 43–69.

[70] Antonioni G, Spadoni G, Cozzani V. Application of domino effect quantitative risk assessment to an extended industrial area. J Loss Prevention in Process Ind 2009; 22(5): 614–624.
[71] Cozzani V, Antonioni G, Khakzad N, Khan F, Taveau J, Reniers G. (2013). Quantitative Assessment of Risk Caused by Domino Accidents. In: Cozzani V, Reniers G, editors. Domino Effects in the Process Industries: Modelling, Prevention and Managing. Amsterdam, The Netherlands: Elsevier; 2013, p. 208-228.
[72] Cozzani V, Antonioni G, Landucci G, Tugnoli A, Bonvicini S, Spadoni G. Quantitative assessment of domino and NaTech scenarios in complex industrial areas. J Loss Prevention in Process Ind 2014; 28: 10–22.
[73] Baybutt P. The treatment of domino effects in process hazard analysis. Process Saf Prog 2015; 34(3): 220–227.
[74] Corbett GG, Reid SR, Johnson W. Impact loading of plates and shells by free-flying projectiles: a review. Int J Impact Eng 1996; 18(2):141-230.
[75] Goldsmith W. Review: Non-ideal projectile impact on targets. Int J Impact Eng 1999;22:95-395.
[76] Borg JP, Cogar JR, Tredways S, Yagla J, Zwiener M. Damage resulting from high speed projectile in liquid filled metal tanks. In: Computational methods and experimental measurements 2001; X: 889–902. Wassex Institute of Technologies Press.
[77] Lecysyn N, Dandrieux A, Heymes F, Slangen P, Munier L, Lapebie E et al. Preliminary study of ballistic impact on an industrial tank: projectile velocity decay. J Loss Prevention in the Process Ind 2008;21:627-34.
[78] Hu B, Li G, Sun J. Numerical investigation of K4-rating shallow footing fixed anti-ram bollard system subjected to vehicle impact. Int J Impact Eng 2014; 63:72-87.
[79] Sharma H, Hurlebaus S, Gardoni P. Performance-based evaluation of reinforced concrete columns subject to vehicle impact. Int J Impact Eng 2012; 43:52-62.
[80] Schneider P, Buchar F, Zápeca. Short Communication: Structural response to thin steel shell structures due to aircraft impact. J Loss Prev in Process Ind 1999; 12: 325–9.
[81] Price MA, Ghee AH. Modeling for detonation and energy release from peroxides and non-ideal improvised explosives. Cent Eur J Energ Mater 2009;6:239–54.
[66] Buczkowski D, Zygmunt B. Detonation properties of mixtures of ammonium nitrate based fertilizers and fuels. Cent Eur J Energ Mater 2011;8:99–106.
[82] Department of Homeland Security. IED attack factsheet: improvised explosive devices ⟨http://www.dhs.gov/ied-attack-fact-sheet⟩ (accessed 29.10.14).
[83] International Atomic Energy Agency (IAEA). Defence in Depth in Nuclear Safety. Vienna: IAEA; 1996.
[85] Uijt de Haag PAM, Ale BJM. Guidelines for quantitative risk assessment (Purple Book). The Hague (NL): Committee for the Prevention of Disasters; 1999.
[86] Bounds WL. Design of blast resistant buildings in petrochemical facilities. Reston, VA, USA: ASCE Publications; 1997.

APPENDIX A

The attack modes classified in [62] and reported in Table 1 were chosen since they are specific to the chemical sector. In order to strengthen the present selection of attack modes, a query in the START database [63] was carried out. The START database classifies more than 150,000 terrorist attacks occurred in the period 1970-2014.

Firstly, a list of possible targets and target installations was obtained from the database; the results are summarized in the following:

- Abortion Related
- Airports and Aircraft
- Business
- Educational Institution
- Food or Water Supply
- Government (Diplomatic)
- Government (General)
- Journalists & Media
- Maritime
- Military
- NGO
- Police
- Private Citizens & Property
- Religious Figures/Institutions Telecommunication
- Terrorists/Non-state Militia
- Tourists
- Transportation
- Utilities
- Violent Political Party
- Other or uknown

Then, the following attacks were obtained for the pertinent categories associated with the present study (chemical facilities or "process plants were not explicitly covered):

- Food and Water supply: 302 attacks
- Transportation: 957 attacks

Hence, a significant number of events (more than 1200) was collected in order to determine information about the attack modes. Based on the database query, the following modes were identified:

- Explosives/Bombs/Dynamite
- Explosives/Bombs/Dynamite, Firearms
- Incendiary
- Armed Assault
- Chemical (that is introduction of chemical agents into the process)

Then, a more generic query was carried out in the database by setting attack type = "Infrastructure Attack". In this case, more than 10000 records were obtained, considering that also political parties, privates or non-state militia may be as well affected. In this case, the following attack modes were obtained:

- Explosives/Bombs/Dynamite
- Firearms
- Incendiary
- Unarmed Assault
- Sabotage equipment

Therefore, it may be concluded that the attack modes selected in the present work are compatible with the START query and even more detailed, since associated with a particular category of targets, e.g. chemical facilities.

APPENDIX B

The present appendix discusses the quantification of the nodes related to physical protection systems effectiveness. In order to quantify the BN nodes, conditional probability tables characterization was carried out calculating probability of success in performing the design security function according to Eq.(B.1):

$$P = P_0 \prod_{h=1}^{Q} (X_h r_h) \tag{B.1}$$

where Q 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 (i.e. given that most favorable conditions to success are present), r_h is the measure of the unfavorable impact on the baseline conditional probability P_0 from changing the state of the h-th influencing factor from the favorable state to the unfavorable state and assuming all other influencing factors are still in the favorable state, and $X_h=1$ if the h-th influencing factor is in its unfavorable state, while $X_h=1/r_h$ if the h-th influencing factor is in its favorable state.

The numerical values to be applied in the CPTs quantification for the different modules are selected as the aggregate performance data derived from expert consultation: more specifically, the median value of the probabilistic estimates gathered for each query variable is applied.

An example of the quantification procedure is given in Table B.1 for the node “Alarm communication” (node P.2 in Fig. 1); the reader is referred to [65] for further details.

A direct dependency on adversary path has been taken into account for the security functions of assessed detection of an intrusion attempt and of timely intervention of the response force, as well as for overall PPS effectiveness.

The successful assessed detection at system level is possible if successful assessed detection occurs at least at one of the Rings of Protection (RoPs) implementing security barriers suitable to perform the detection function that are crossed by adversary’s path. Therefore, the CPT of the node “Assessed detection” (node P.1 in Fig. 1) is populated as if it represents an OR-gate among the nodes representing assessed detection at the different RoPs but accounting for path analysis results. It is equivalent to calculate the probability of having a successful assessed detection as per Eq.(B.2) ($P_{sx,m}$), when the m-th path is considered:

$$P_{sx,m} = 1 - \prod_{l=1}^{N_l} (1 - \alpha_{l,m} P_{sx,l}) \tag{B.2}$$

where $P_{sx,l}$ is the probability of successful assessed detection at the l-th RoP; $\alpha_{l.m}$=1 if the l-th RoP is crossed by the m-th path and $\alpha_{l.m}$=0 otherwise.

Table B.1: Example of data and method applied to CPT quantification for node P.2 in Fig. 1.

INPUT DATA as provided in [65]

Node ID	***Node***	***Query variable ID***	***Query variable***	***Median of elicited values***
P3_1	Reliability of coverage	MP_{3_1}	Marginal probability of having a reliable coverage of all the facility area	0.99
P3_2	Security guards' level of training in communication procedures	MP_{3_2}	Marginal probability of the security guards having a high level of training in communication procedures	0.90
P3	Communication to/ among response force	CP_3	Conditional probability of having an effective communication to response force, given that all influencing factors are in favorable state (given high reliability of coverage and high level of training in communication procedures)	0.95
P3_1	Reliability of coverage	r_{3_1}	Measure of negative impact on the probability of having an effective communication to response force from changing the reliability of coverage to the unfavorable state and assuming security guards' level of training in communication procedures remain in a favorable state	0.10
P3_2	Security guards' level of training in communication procedures	r_{3_2}	Measure of negative impact on the probability of having an effective communication to response force from changing the security guards' level of training in communication procedures to the unfavorable state and assuming reliability of coverage remain in a favorable state	0.50

Calculations to fill in Conditional Probability Table of node P3

Level of training	High		Low	
Reliability of coverage	High	Low	High	Low
Success	CP_3	$CP_3 \cdot r_{3\_1}$	$CP_3 \cdot r_{3\_2}$	$CP_3 \cdot r_{3\_1} \cdot r_{3\_2}$
Failure	$1- CP_3$	$1- CP_3 \cdot r_{3\_1}$	$1- CP_3 \cdot r_{3\_2}$	$1- CP_3 \cdot r_{3\_1} \cdot r_{3\_2}$

Conditional Probability Table of node P3: Communication to/ among response force

Level of training	High		Low	
Reliability of coverage	High	Low	High	Low
Success	*0.95*	*0.475*	*0.095*	*0.0475*
Failure	*0.05*	*0.525*	*0.905*	*0.9525*

The probability of having a timely intervention by the response force depends on the response force intervention time and on the cumulative delay accumulated by the adversary to overcome existing delay barriers, which varies depending on path. Eq.(B.3) was used to calculate the probability of timely intervention along the m-th path, (P_{T_m}) as suggested in [40]:

$$P_{T_m} = \frac{1}{\sqrt{2\pi(\sigma_{RTF}^2+\sigma_D^2)}}\int_0^{T_m} \exp\left(-\frac{T_m^2}{\sqrt{2\pi(\sigma_{RTF}^2+\sigma_D^2)}}\right)dT_m \;\; ; \; T_m = \sum_m T_{Di,m} - RFT \qquad \text{(B.3)}$$

where $T_{Di,m}$ is the penetration time for i-th delay barrier present along m-th path; RFT is the response force time. Normal distribution of time parameters is assumed. Data on the mean and variance of the normal distribution of delay times associated to barriers can be retrieved from [40]; while the mean value of response force intervention time is supposed to be known and a variance of 30% can be considered as a first estimate [40].

Clearly enough, for the “no intrusion” state of the path node, the conditional probability of accomplishing any of the security functions is equal to 0.

APPENDIX C

As mentioned in Section 3.2.3 and Table 2, the evaluation of the equipment damage probabilities when exposed to heat radiation (such as in the case of arson devices) and overpressure caused by explosions is carried out through the application of fragility models based on probit equations. Probit models give the probability of having the considered degree of damage to attacked equipment item as a direct function of the intensity of physical effects associated to the impact vector of each attack mode. Probit models were developed by Cozzani and coworkers in previous works [66-69] and are summarized in Table C.1.

Table C.1. Models for damage probability considered in the present study for escalation due to radiation and overpressure (Y: probit value; ttf: time to failure, s; I: radiation intensity on the target equipment, kW/m^2; V: equipment volume, m^3; p$_s$: peak static overpressure on the target, kPa).

Impact vector	Target equipment	Damage probability models	Reference
Steady fire (e.g. from arson device)	atmospheric	Y = 9.25 – 1.847·ln(ttf/60) ln(ttf) = -1.13·ln(I) – 2.667·10^{-5} V + 9.877	[66]
	pressurized	Y = 9.25 – 1.847·ln(ttf/60) ln(ttf) = -1.29·ln(I) + 10.97 V$^{0.026}$	
Overpressure caused by explosives	atmospheric	Y = -18.96 + 2.44 ln(p$_s$)	[67-69]
	pressurized	Y = -42.44 + 4.33 ln(p$_s$)	
	elongated (toxic)	Y = -28.07 + 3.16 ln(p$_s$)	
	elongated (flammable)	Y = -28.07 + 3.16 ln(p$_s$)	
	auxiliary (toxic)	Y = -17.79 + 2.18 ln(p$_s$)	
	auxiliary (flammable)	damage probability below cut-off	

The overpressure caused by improves explosive devices (IED) explosions was evaluated on the basis of TNT efficiency values evaluated in [22] adapting the following literature correlation [86]:

$$p_s = \frac{W_{TNT}^{1/3}}{r} + 4.4\frac{W_{TNT}^{2/3}}{r^2} + 14.0\frac{W_{TNT}}{r^3} \qquad \text{(C.1)}$$

where p_s (bar) is the peak overpressure, r (m) is the distance from the center of the explosion and W_{TNT} is the equivalent mass of TNT expressed in kg, calculated accordingly to the following expression for a given amount of home-made explosive:

$$W_{TNT} = \eta \times f \times W_{exp} \tag{C.2}$$

where W_{exp} is the overall amount of home-made explosive including additives (expressed in kg), η is the TNT efficiency, and *f* is the actual mass fraction of the explosive material, which is introduced in order to consider the possible presence of inert materials in home-made explosives. In the case study, TATP has a unitary mass fraction, while for ANFO f = 0.5 due to the presence of dolomite in the commercial ammonium nitrate.

APPENDIX D

Table D.1 shows the conditional probability of having a timely intervention of the response force given intrusion assessed detection calculated for each analyzed path through the use of EASI analysis [40].

Table D.1. Conditional probability of timely interruption of adversary sequence of actions for the considered paths and attack scenarios; n.a. = not applicable. For attach scenario ID see Table 5.

Path	Adversary tasks sequence	Probability of timely interruption (P_T)	Attack scenario ID
No Intrusion path	n.a.	0	A, B
Path 1	Walk 12 m; Cut external fence with pliers; Walk 10m; Climb over dike; Trigger explosion trough IED	0	C, F
Path 2	Use counterfeit badge to pass through supervised automatic credential check at personnel portal; Walk 280 m; Climb over dike; Trigger explosion trough IED	0.172	D
Path 3	Bypass manual credential check at vehicle portal; Walk 240 m; Climb over dike; Trigger explosion trough IED	0.121	E
Path 4	Walk 12 meters; Climb over external fence; Walk 10 m; Climb over dike; Open drain valve at tank bottom	0	J, M
ìPath 5	Use counterfeit badge to pass through supervised automatic credential check at personnel portal; Walk 280 m; Climb over dike; Open drain valve at tank bottom	0.391	K
Path 6	Bypass manual credential check at vehicle portal; Walk 240 m; Climb over dike; Open drain valve at tank bottom	0.358	L
Path 7	Walk 5 meters; Cut external fence with pliers; Walk 5 m; Cut internal fence with pliers; Climb over dike; Trigger explosion trough IED	0	G, I
Path 8	Use counterfeit badge to pass through supervised automatic credential check at personnel portal; Walk 190 m; Use manual bolt cutter to open locked internal gate; Walk 70 m; Climb over dike; Set in place IED	0.178	H
Path 9	Walk 5 m; Climb over external fence; Walk 5 m; Climb over internal fence; Climb over dike; Open drain valve	0	N, P
Path 10	Use counterfeit badge to pass through supervised automatic credential check at personnel portal; Walk 190 m; Use manual bolt cutter to open locked internal gate; Walk 70 m; Climb over dike; Open drain valve	0.395	O