Development of fragility models for process equipment affected by physical security attacks

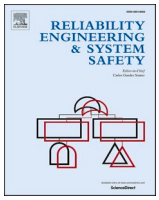
Marroni, G; Casini, L.; Bartolucci, A; Kuipers, S.; Casson Moreno, V; Landucci, G.

Reliability Engineering and System Safety 243 (2024) 109880

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress



Development of fragility models for process equipment affected by physical security attacks

Giulia Marroni [a], Leonardo Casini [a], Andrea Bartolucci [b], Sanneke Kuipers [b], Valeria Casson Moreno [a], Gabriele Landucci [a,*]

[a] Department of Civil and Industrial Engineering – University of Pisa, Largo Lucio Lazzarino n.2, 56126 Pisa, Italy
[b] Institute of Security and Global Affairs, Faculty of Governance and Global Affairs, Leiden University, Wijnhaven, Turfmarkt 99, 2511 DP, Den Haag, the Netherlands

ARTICLE INFO

Keywords:
Security Vulnerability Assessment
Bayesian Networks
Fragility models
Major accident hazard
Security management
Physical Protection System

ABSTRACT

The vulnerability of chemical and process facilities toward physical security attacks depends on the equipment resistance against such attacks and on the performance of Physical Protection Systems (PPS) in place. To enhance the protection against intentional attacks, the development of quantitative vulnerability metrics is essential, nevertheless current standard approaches only offer qualitative or semi-quantitative evaluations. The aim of the present work is to develop a quantitative methodology for the assessment of chemical and process facilities vulnerability towards external acts of interference. The proposed methodology is based both on the evaluation of equipment structural integrity in response to different types of specific impact vectors characterizing intentional attacks and on the quantitative performance assessment of related PPS. In particular, specific fragility models were developed for impact vectors associated with improvised explosive devices, firearms, and incendiary weapons. The novel fragility models were implemented in a comprehensive security vulnerability assessment (SVA) based on Bayesian Networks, in which the contribution of PPS performance was also considered. A case study was defined and analyzed to exemplify the application of the proposed approach. The results obtained allowed for the identification of the most critical security-related escalation scenarios and thus for an improved quantitative SVA.

1. Introduction

Security science is a relatively new field that has expanded considerably since the terroristic attacks in New York on September 11th, 2001. The process industry is not unrelated to security matters. Actually, chemical facilities, where relevant quantities of hazardous chemicals are stored or processed, may become possible targets of acts of interference and terroristic attacks [1]. Security concerns for chemical facilities revolve around both physical and cyber-attacks, as demonstrated by available analyses of intentional attacks occurred in recent years [2,3]. Besides, global affairs show that the risk of attacks at industrial infrastructures and chemical facilities is ubiquitous as part of violent conflicts in highly industrialized regions.

There have been a number of global and regional measures to address security issues. The CBRN (chemical, biological, radiological and nuclear) Risk Mitigation and Security Governance Programme was launched by the United Nations Crime and Justice Research Institute in 2004 to promote the co-operation and co-ordination between countries, international and regional organizations [4]. The government of the United States merged several federal organizations under the Department of Homeland Security in 2002 to create a comprehensive strategy against terrorism [5]. The Chemical Facility Anti-Terrorism Standards (CFATS) was established in 2007 and it is the first regulatory program that specifically focuses on the security of chemical facilities storing hazardous substances in the US [6]. In Europe, the directive 2018/114/EC was established as a result of the "European Programme for Critical Infrastructure Protection" (EPCIP) [7] and regulates the prevention, protection and response to terroristic attacks involving the energy and transport sector; the regulation EC No 725/2004 [8] enhances the security of international ports and shipping facilities. However, the European Seveso Directive III [9] concerning major accidents hazard for industrial installation does not address the need for a security-related analysis or countermeasures.

Nonetheless, security standards such as the API/ANSI Std 780 [10], the CCPS guidelines for the evaluation of security vulnerabilities and security vulnerability analysis (SVA) [11], the Sandia model for the vulnerability of physical protection systems (VAM-CF) [12] can provide

* Corresponding author.
E-mail address: gabriele.landucci@unipi.its (G. Landucci).

https://doi.org/10.1016/j.ress.2023.109880
Received 8 April 2022; Received in revised form 16 October 2023; Accepted 9 December 2023
Available online 17 December 2023

Acronyms

Acronym	Description
BN	Bayesian Network
IED	Improvised Explosive Device
PPS	Physical Protection System
QRA	Quantitative Risk Assessment
SVA	Security Vulnerability Assessment

Symbols and Units

$(dv/dx)_0$	(m/s)/m, Bullet muzzle retardation
A	-, Attractiveness
a	m, Distance between a generic target and explosive
AE	-, Absolute error
BHN	MPa, Brinell Hardness (Maximum, Minimum, Mean values)
C	-, Consequences
c	m^3, Equipment capacity
COD	-, Coefficient of determination
D_p	-, Perforation dose
D_{th}	s, Thermal dose
F	-, Parameter indicating how an unfavorable state affects the security barrier performance
f	-, Safety factor
H_d	m, Dike height
I	kW/m^2, Heat radiation intensity
J	-, Number of factors affecting the physical protection systems
k_1	-, First probit coefficient
k_2	-, Second probit coefficient
L_{eff}	m, Dike effective length
L_{jet}	m, Length of the flamethrower flame
M	-, Number of barriers on the adversary path
m	g, Bullet mass
m_{IED}	kg, Improvised Explosive Device mass
$m_{TNT,eq}$	kg, Equivalent TNT mass
n	-, Drag coefficient exponent
$N_{fail}(t)$	Number of equipment failed at a generic time t
N_{tot}	Total number of equipment
p	Pa, Pressure mitigated by dike
$P(E)$	-, Probability of a generic evidence E
$P(U)$	-, Joint probability distribution of a generic set U
P_0	-, Probability of physical protection system success in full favorable state
$Pa(G)$	-, Parent set variable of a generic variable G
P_C	-, Probability of communication from and to emergency response team
PCC	-, Pearson correlation coefficient
P_D	-, Probability of successful detection
P_{data}	-, Probability obtained using the reference study
$P_{fail}(t)$	-, Probability of equipment failure at generic time t
P_I	-, Probability of adversary interruption
P_{PPS}	-, Probability of success of a single physical protection system
P_{regr}	-, Probability obtained using the bullet perforation probit model
P_T	-, Probability of timely intervention of emergency response team
R_S	-, Security risk
R	m, Generic distance
r	$m/kg^{1/3}$, Scaled length of generic distance R
R_{de} (r_{de})	m, Distance (scaled distance) between dike and explosive
R_{dt} (r_{dt})	m, Distance (scaled distance) between dike and target
RE	-, Relative error
R_{et} (r_{et})	m, Distance (scaled distance) between explosive and target
s	mm, Plate thickness
SEP_{max}	kW/m^2, Maximum surface emissive power of the flamethrower flame
S_s	mm, Plate thickness required to avoid perforation
T	-, Threat
t^*	s, Time difference between adversary intrusion time and emergency response team time
t_d	s, Delay caused by a barrier
t_{ERT}	s, Emergency response team time
t_{exp}	s, Time of exposure to the flamethrower flame
t_{max}	s, Maximum flamethrower operating time
t_P	s, Adversary intrusion time
ttf	s, Equipment time to failure
t_w	s, Time to walk the path
V	-, Vulnerability
v	m/s, Bullet velocity
v_0	m/s, Bullet muzzle velocity
X	-, Parameter indicating the favorable state of a factor
x	m, Bullet position
x_0	m, Bullet initial position
Y	-, Probit variable
Y_t	GPa, Target flow stress
α	-, Coefficient for time to failure evaluation
ΔP	Pa, Peak static overpressure
ΔP_m	Pa, Mitigated static overpressure peak
ΔP_{nm}	Pa, Non-mitigated static overpressure peak
η	-, TNT efficiency
σ_{ERT}	s, Variance of the emergency response team time
σ_P	s, Variance of the adversary intrusion time
Ψ	-, Explosive mass fraction

guidance to analysts and plant managers. Matteini et al. [13] made an extensive analysis and determined that all the cited above methodologies have a common background and structure, yet also differ in important ways. While API and the VAM-CF follow a scenario-based approach, the CCPS guidelines suggest both a scenario-based and an asset-based approach. Although API Std 780 has the most straightforward application, the VAM-CF has a higher potential for a complete analysis since it also includes cyber-security risks.

However, the aforementioned standards only offer a semi-quantitative evaluation of vulnerability and security risk, meaning that numerical values are assigned, but they represent approximate results instead of exact or absolute ones [14] Moreover, as observed by Cox [15], previous approaches to security are linear: they do not take into consideration the interdependencies of each factor affecting the security risk.

Quantitative techniques in the framework of risk assessment provide a realistic numerical estimate [14], and can guide analysts in identifying weaknesses of process facilities, thus overcoming the limitations of semi-quantitative techniques. Recent studies addressed this aspect developing quantitative Security Vulnerability Assessment (SVA) methods dedicated to both critical infrastructures [16,17] and chemical installations [18–22]. Given the necessity to combine different types of information and the need to take into account mutual interactions between parameters, these studies adopted advanced probabilistic models, such as Bayesian Networks (BN), but only focused on the evaluation of the Physical Protection Systems (PPS) in place and, more in general, on the evaluation of security countermeasures performance in securing facilities against external attacks. However, the comprehensive

assessment of vulnerability in the framework of chemical and process installations also entails the evaluation of equipment resistance in terms of damage probability in case of successful attack.

Equipment vulnerability or fragility models are used to assess the probability of damage given a specified physical impact vector [18]. Recent works developed novel vulnerability models for equipment exposed to simultaneous fires and explosions based on evaluation of the total stress on the equipment shell [23,24]. Other works studied different ways to model consequences of domino effects and the interactions among different equipment [25–29]. However, to the best of the Authors' knowledge, fragility models tailored to the specific needs of assessing the impact of security attacks and suitable for quantitative security analyses are still lacking.

The aim of the present work is to develop a quantitative methodology for SVA implementing a comprehensive set of equipment fragility models for the assessment of physical attack scenarios, i.e., intentional attacks that need a physical intrusion and/or physical weapons to cause damage to a target. With respect to existing literature, fragility models were developed for impact vectors associated with improvised explosive devices, firearms, and incendiary weapons, and they were integrated for the first time into a comprehensive SVA. The idea behind this work was to build a quite simple approach for the assessment of damage probabilities that could provide robust and conservative results to be implemented into a security assessment. Indeed, the physical models associated with the attack vectors were simplified, as the final focus of the work was to obtain correlations for damage probability for different security scenarios, rather than describing the detailed mechanical behaviour of the process item. The developed models feature a simplified evaluation of the dose of physical effect. In this way, the models can be implemented in quantitative SVA without requiring input parameters that may be difficult to retrieve.

The SVA of the present work was based on a probabilistic model based on BN in order to provide an accurate estimate of vulnerability for security scenarios in the specific framework of chemical and process facilities, where also the performance of the PPS in place was considered. In fact, BN allow for the full characterization of the vulnerability of a given asset as they can include a great number of factors, their interdependencies, and allow for the continuous update once new evidence enters the network. Thus, BN are an appropriate tool for SVA, which has been already widely used to analyze process facilities [1,27,30–33].

To demonstrate the soundness of the developed BN and the contribution of equipment fragility evaluation, a sensitivity analysis has been conducted assessing the variation of vulnerability by modifying significant parameters of the fragility models developed. In order to test the potentialities of the present approach, an industrial case study was analyzed. The results identified the critical elements of a security attack to specific targets, highlighting the role of security countermeasures and equipment fragility. Thus, the tools and methods presented in the work could be exploited by plant managers to prioritize the resources available for security investments and to identify weaknesses in the analyzed installations.

2. Theoretical background on vulnerability assessment

2.1. Key concepts: vulnerability and security vulnerability assessment (SVA)

Aven [34] defines vulnerability as a fault or weakness that reduces or limits a system's ability to withstand a threat or to resume a new stable condition. Johansson et al. [35] include endogenous risks, stating that vulnerability is the inability of a system to withstand strains and the effects of failure. Haimes [36] goes one step further and describes vulnerability as the manifestation of the inherent states of the system that can be exploited to adversely affect that system. This last definition is more appropriate for a security framework, given that it includes the possibility of an external threat exploiting endogenous weaknesses.

Two major considerations need to be accounted for when referring to security of industrial infrastructures and chemical installations: 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 actions such as detection, prevention, protection, interdiction, and containment, which are functions implemented by security barriers [36].

Therefore, the vulnerability of a chemical and process facility is defined in this work as any property of the system that can be exploited to perform a successful attack. This definition is in agreement with the risk formulation proposed by API/ANSI Std 780 [10]:

$$R_S = T{\cdot}A{\cdot}V{\cdot}C \tag{1}$$

in which security risk (R_S) is intended as the likelihood that a threat (T) will consider attractive a specific asset (A) and will successfully commit an act against it, taking advantage of its vulnerability (V) to cause a given set of consequences (C), as per Eq. (1).

Vulnerability is, therefore, a key concept for the management of countermeasures in security science. SVA may be considered a useful managerial tool to support informed decision making to enhance security of an installation/site [37]. The identification of elements that could represent a weakness for the installation is a necessity when conducting a quantitative SVA [10,38]. To this purpose the performance of the security barriers should be firstly considered. An SVA should therefore include a systematic evaluation of the PPS components effectiveness, with the aim of providing an evaluation of the overall security system [12]. Such an evaluation also allows for the identification of critical PPS functions that may need improvement, as well as additional measures to be implemented. More details on PPS performance are provided in Section 2.2. Secondly, the structural resistance of targets to specific impact vectors characterizing security attacks should be quantified, and this has never been taken into consideration before in SVA framework. In this perspective, vulnerability assumes the meaning of fragility and fragility models are used to quantitatively assess the physical damage to targets (see Section 2.3).

2.2. PPS performance and reference data

This section outlines the theoretical background to mathematically model and quantify the performance of PPS to be implemented in the Bayesian Network to carry out the SVA.

A PPS integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage, or malicious attacks [38]. According to Garcia [38], PPS can be characterized according to four functions:

- Detection: it includes intrusion detection and the consequent alarm assessment. First, a sensor detects an intrusion and triggers the alarm; the information detected is reported and shown to the security staff which evaluates its credibility;
- Delay: this element aims at slowing down the adversary's progress towards the target through the introduction of barriers in order to provide additional time to respond;
- Response: it is the adversary interruption and threat neutralization.
- Deterrence: it decreases the facility attractiveness and convinces the adversary not to attempt an attack

The deterrence function is too difficult to measure, given that it relies on the perception of the threat and is therefore not a reliable source for adversary interruption [38]. For this reason, it is not considered in this study, which means that conservatively no action can be taken to prevent the attack.

It is important to point out that the PPS functions are highly

dependent on the path chosen by the threat to perform the attack, as it is hereby shown.

Quantitative metrics for physical protection systems effectiveness proposed by Sandia SVA Model were adopted in this study to evaluate the performance of PPS [12]. All the three functions (detection, delay, and response) shall be performed in sequence and within a time lapse that is shorter than the time required by the adversary to complete their task.

The probability of interruption P_I is expressed as:

$$P_I = P_D \cdot P_C \cdot P_T \tag{2}$$

where P_D is the probability of successful detection, P_C is the probability of communication to and among the emergency response team, and P_T is the probability of timely intervention from the emergency response team.

This work follows a previous approach from Argenti et al. [39] who developed a methodology that offers quantitative data of PPS performance. Experts from the industry were involved to determine variables and influencing factors of security functions. The probability of success of each element of the PPS is defined as:

$$P_{PPS} = P_0 \cdot \prod_{i=1}^{J} X_i \cdot F_i \tag{3}$$

where J is the number of factors that independently affect the performance of the security barrier, P_0 is the conditional probability of the security barrier successfully performing its function if all factors are in the favorable state, F_i is a parameter that measures how a factor in an unfavorable state affects the performance of the security barrier, and $X_i = 1$ if the i-th factor is in the unfavorable state, or $X_i = 1/F_i$ if the factor is in the favorable state. By means of expert elicitation, Argenti et al. [39] gathered specific data both the baseline probability P_0 and impact factors F_i for different types of security barriers and PPS elements.

P_D can be quantified using the methodology described above. Namely, to obtain P_D given a certain path, at least one of the security barriers must detect the intrusion, which means considering an OR operator among the different detection barriers. P_C can be as well assessed using Eq. (3). Instead, P_T expresses the probability of evolution in time of the attack. The mean adversary intrusion time (t_P) is calculated taking into consideration the time to walk (t_w) and the delay caused by the barriers and operations to carry out ($t_{d,i}$) on their path:

$$t_P = t_w + \sum_{i=1}^{M} t_{d,i} \tag{4}$$

where M is the number of delaying barriers encountered by the adversary on the attack path (e.g., fences, perimetral walls) and operations to be carried out to reach the target and complete the attack (for instance placing and detonating an explosive device). Garcia [12] reports numerical data on running speeds and delay times for different barriers, along with additional information on their statistical distribution: for example, the time needed to cut a fence using pliers is on average 120s, with a standard deviation of 49.2s.

Assuming a normal distribution for both t_P and emergency response team time (t_{ERT}), P_T is calculated as:

$$P_T = \frac{1}{\sqrt{2\pi \cdot (\sigma_{ERT}^2 + \sigma_P^2)}} \cdot \int_0^{\infty} e^{\frac{-(t-t*)^2}{2\left(\sigma_{ERT}^2 + \sigma_P^2\right)}} \cdot dt \tag{5}$$

where σ_P^2 and σ_{RFT}^2 are the variance of t_P and t_{ERT} respectively, and t^* is the difference between t_P and t_{ERT}.

It must be noted that all equations above must be applied to a specific adversary path. It is important to check beforehand the possible barriers for each possible path the adversary might choose.

2.3. State of the art on fragility models for equipment

Since the '90s, the concept of fragility model and, more specifically, of fragility curves has been adopted in the field of risk analysis. According to Singhal, fragility describes the probability of exceeding a certain level of damage to an infrastructure given a specific impact vector [40]. This approach has been adopted for the study of the behavior of different types of structures to earthquakes [41–45] as well as other extreme natural hazards [45–50].

The definition from Singhal [40] is hence adopted in this study by generalizing the damage cause to physical effects associated to security scenarios. In this framework, vulnerability assumes the connotation of fragility, in order to evaluate the resistance of a target to a given amount of physical effect.

An effective approach to model the probability distribution of damage is to utilize simplified relationships, such as the probit regression, which is a non-linear regression method typically used for dichotomous outcome variables [55]. In the present study, the variable is the damage of the equipment, and the possible outcomes are the mutually exclusive statuses called "damaged" and "not damaged".

Probit models have found extensive application in safety risk assessment studies to evaluate health damages on humans [56] and to study domino effect propagation among process facilities [57]. The ease of application and the widespread use in the framework of quantitative safety studies make probit models an appropriate form of fragility models to be developed for security scenarios.

In the following, a brief review of equipment fragility models is provided in order to show the limitations in their implementation in the framework of quantitative security analyses and quantitative risk assessment (QRA) studies devoted to chemical and process facilities. Table 1 reports a summary of the main literature approaches.

Engineering systems typically exhibit complex nonlinear behaviors [58] and methodologies have been proposed in the literature to account for statistical uncertainties, inaccurate model forms and/or missing variables [59,60]. In the framework of QRA, however, simplified vulnerability models like the ones in Table 1 are usually adopted, as they require a limited number of input parameters. The use of simplified models reduce the calculation time for security escalation assessment, since QRA procedures involve the analysis of a high number of accidental scenarios even after an initial screening. Clearly enough, the better the fragility model is, the more accurate the QRA results are. Nevertheless, to the aim of a practical use of QRA by industrial practitioners, simplification is needed to reduce time and costs of the analysis, given that the results obtainable by a certain approach have to be conservative.

2.3.1. Equipment fragility models for damage caused by fragments

Fragments typically originate from storage or process vessels as a consequence of a catastrophic rupture [57]. The projection of fragments can be divided into three main phases: fragment generation, ejection and impact. Tugnoli et al. [61] provided an extensive review for both descriptive and probabilistic models of each phase. In the framework of security, fragment projection is not a direct attack mode that attackers would exploit. It might become relevant when taking into consideration the domino effect of a successful intentional attack; however, this scenario is outside the scope of this study. Nevertheless, bullets can be seen as a type of fragment ejected from a firearm impacting a target by puncturing. The models available to describe the behavior of fragments generated by the catastrophic failure of process equipment are not suitable for bullets given the difference in the characteristic length with respect to conventional fragments. Still, the perforation of a shell of a process equipment by means of a bullet could cause a leak, leading to the loss of containment of potentially hazardous chemicals. However, no fragility model has been yet integrated into a framework for SVA for process plants considering the role of PPSs. A recent work [62] reviewed perforation models for different types of bullets and investigated their

Table 1
Summary of fragility models based on probit relationships available in literature for relevant impact vectors. Y: probit variable, ttf: time to failure (s), I: radiation intensity (kW/m^2), c: equipment volume (m^3); α coefficient depending on equipment type; ΔP: static overpressure peak (Pa).

Model ID	Reference	Impact vector	Target equipment	Damage probability model
1	[51]	Heat radiation from single source	Atmospheric tanks	$Y = 9.25 - 1.85 \cdot \ln(ttf/60)\ln(ttf) = -1.13 \cdot \ln(I) - 2.67 \cdot 10^{-5} \cdot c + 9.9$
			Pressurized vessels	$Y = 9.25 - 1.85 \cdot \ln(ttf/60)\ln(ttf) = -0.95 \cdot \ln(I) + 8.845 \cdot c^{0.032}$
2	[52]	Heat radiation from multiple fires	Atmospheric, pressurized equipment	$Y = 9.25 - 1.85 \cdot \ln(ttf/60) ttf \propto I^{\alpha}$ See [52] for more details
3	[53]	Overpressure	Atmospheric tanks	$Y = -18.96 + 2.44 \cdot \ln(\Delta P)$
			Pressurized vessels	$Y = -42.44 + 4.33 \cdot \ln(\Delta P)$
			Elongated equipment	$Y = -28.07 + 3.16 \cdot \ln(\Delta P)$
			Small equipment	$Y = -17.79 + 2.18 \cdot \ln(\Delta P)$
4	[54]	Overpressure	Atmospheric tanks	$Y = -9.36 + 1.43 \cdot \ln(\Delta P)$
			Pressurized vessels	$Y = -14.44 + 1.82 \cdot \ln(\Delta P)$
			Elongated equipment	$Y = -12.22 + 1.65 \cdot \ln(\Delta P)$
			Small equipment	$Y = -12.42 + 1.64 \cdot \ln(\Delta P)$

accuracy by comparison with experimental data, build a repository of perforations models. The models adopted in this study are present in the review [62] and their compatibility was therefore confirmed. Still, the review [62] revealed that other models might be suitable to develop a fragility model for different types of bullets. In this sense, the framework developed in this work can be still used even with the application of other perforation models.

2.3.2. Equipment fragility models for damage caused by fires

The assessment of probability of failure of equipment induced by fires is of primary importance when dealing with the assessment of domino effect scenarios [57]. Landucci et al. [51] developed a fragility model based on the detailed simulation of vessel behavior to fire, carried out through a lumped model. The lumped model is based on the "thermal nodes" approach [63], based on the subdivision of the system under analysis in a limited number of nodes. In each node, the solution of heat and material balances allows for the evaluation of wall temperature and internal pressure. The failure of the equipment takes place when the equivalent stress reaches the maximum allowable stress. The lumped model offers a simplified approach for the evaluation of the time to failure (*ttf*) of equipment, which in turn, is adopted in the fragility model shown in Table 1 (Model 1) for atmospheric and pressurized equipment.

More recently, Zhou et al. [52] defined a methodology to evaluate the *ttf* of equipment exposed to multiple fires, taking into account the time at which the different secondary fires start or are extinguished. The thermal dose was therefore changed, while the same probit equation as in Landucci et al. [51] has been adopted (see Model 2 in Table 1).

In the context of security-related scenarios, an incendiary weapon could be used to concentrate a high heat load on a restricted portion of the surface of a chemical equipment. This might significantly alter the physical properties of the construction material, leading to material damage and equipment failure. However, to the best of the Authors' knowledge, incendiary weapons have never been considered as a source of heat radiation in the development of fragility models.

2.3.3. Equipment fragility models for damage caused by overpressure

Explosions triggered by external acts of interference may cause extensive damage to process facilities. Relevant overpressure impact may be caused by the detonation of military explosives (such as trinitrotoluene, TNT) or Improvised Explosive Devices (IED in the following) [37]. The probability of failure of equipment due to overpressure has been studied by several authors as shown in Table 1. Miura et al. [64] developed a methodology to account for the role of dikes in the mitigation of overpressure effects. Landucci et al. [65]developed a specific methodology to study the effect of IED using a TNT-equivalent charge of explosive.

Although the approaches mentioned above are quite consolidated in literature, their integration to support the probabilistic assessment of security-related scenarios was never undertaken to the best of Authors' knowledge.

3. Methodology and tools

3.1. Overview

Fig. 1 shows the steps of the methodology proposed in this study to support the security vulnerability assessment using improved fragility models.

The first step of the methodology (Step 1 in Fig. 1) consists in the identification of physical attack vectors relevant for process facilities. For this purpose, past accident data gathered by Casson Moreno et al. [2] were adopted. Out of a total of 300 collected events, 26 events had enough details to allow Casson Moreno and coworkers to analyze the dynamics of the attacks; the most exploited weapons were explosives (11 out of 26 events), firearms (6 out of 26 events) and incendiary devices (5 out of 26 events) [2]. 10 out of 11 attacks with explosives were able to breach inside the facility; 3 out of 5 arson attacks reached warehouses and tank farm, while only a single attack reached the actual processing part of the facility; finally, 5 out of 6 attackers with firearms were able to reach the process plant [2]. This analysis highlights the damage potential of attacks carried out using these weapons. Thus, this study focused on explosives, firearms, incendiary weapons, and fragility models tailored for the specific case of security assessment.

In Step 2, fragility models for the identified attack vectors have been developed. For firearms and incendiary devices (Steps 2.1 and 2.2 in Fig. 1, respectively), the dose of physical effect has been identified deriving probit relationships. To evaluate the mitigated impact of explosives, conventional approaches have been integrated in Step 2.3 of Fig. 1.

The fragility models developed have been used in combination with PPS performance in Step 3 to evaluate the vulnerability of targets and the overall likelihood of attack success. Bayesian Networks (BN) have been exploited as a probabilistic assessment tool to cope with the integration of fragility models and the performance of PPS.

Step 4 is the application of the BN approach to a demonstrational case study. Step 4.1 consists of a baseline vulnerability assessment, in which the vulnerability obtained with the improved fragility models is compared against the vulnerability obtained using conventional approaches. Lastly, a sensitivity analysis is performed in Step 4.2 to investigate the changes in vulnerability with key input parameters.

3.2. BN implementation

BN are adopted in this work to conduct a scenario-based probabilistic vulnerability assessment. BN are graphical methods of reasoning under uncertainty using probabilities; they consist of the following elements [66]: i) a set of variables, called nodes, and ii) a set of directed edges, called arcs, between the variables. Nodes with arcs directed from them are called parents, while nodes with arcs directed to them are called children; the presence of parent and children nodes means that nodes together with arcs form an acyclic directed graph. In other words, it is

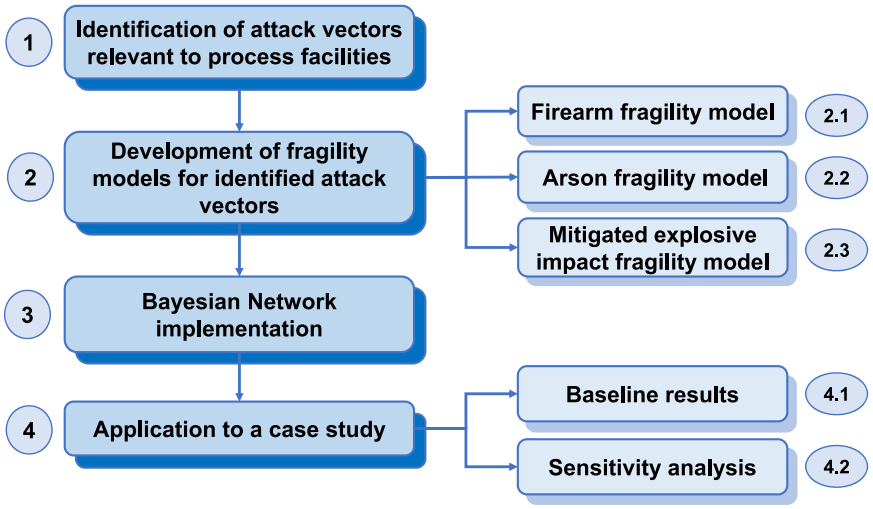


Fig. 1. Flowchart of the methodology for vulnerability assessment developed in the present work

impossible to follow the arcs and form a closed loop.

Given a set of $U = \{G_1, G_2 \ldots G_n\}$ variables, BN specifies a unique joint probability distribution $P(U)$, given by the product of all conditional probabilities of each parent node, as in Eq.6):

$$P(U) = \prod_{i=1}^{n} P(G_i|Pa(G_i)) \tag{6}$$

where $Pa(G_i)$ is the parent set of variable G_i.

One advantage of BN is the possibility to include a wide amount of data and complex inter-dependencies into the analysis; moreover, BN make use of Bayes' Theorem to update the probability of children nodes once new evidence E is available for parent nodes, as shown in Eq. 7:

$$P(U|E) = \frac{P(U \cap E)}{P(E)} = \frac{P(E|U) \cdot P(U)}{P(E)} \tag{7}$$

This property is convenient in a security framework because the network can be updated in real time once new evidence is shown, e.g., an attack path or the use of a given weapon.

In this study, the software GeNIe Modeler by Bayesfusion, LLC [67] has been used to quantify the BN. Each variable of the network is assumed to be described by discrete states. Thus, the so-called chance nodes have been used on GeNIe Modeler to quantify the variables involved in SVA. Chance nodes are quantified by filling a conditional probability table, in which the probability in each discrete state is assigned depending on the state of the parent nodes.

Fig. 2 shows the structure of the BN developed for the present study, highlighting the specific nodes and novel aspects of the present analysis. An example of the full BN model developed is shown in Section 5.3 for the analysis of a specific case study. Compared to previous works [18] dealing with SVA based on BN, the BN developed in this work includes additional connections among nodes with the aim of better capturing the aspects related to a possible intrusion in a chemical facility. For instance, this work considers that the attack mode causes additional delay on the attacker, e.g., the time needed to operate an incendiary weapon. Moreover, the same intrusion point and path can be followed for different attack modes. These assumptions add another degree of complexity to the BN. In fact, the conditional probability table for timely intervention of PPS (N3.1) needs to be quantified taking into consideration the attack mode as well, as shown in Fig. 2 with the dashed line between N1.1 and N3.1.

Another key aspect introduced in the BN is that the damage to assets that are not direct targets of the attack has been considered; referring to Fig. 2, if the targets T_1 and T_2 are reasonably near, then T_1 could be damaged even if T_2 is the primary target of the attack.

Node N1.1 specifies the attack mode and has been quantified assuming that all attack modes have the same probability of being chosen. Regarding the intrusion path (N1.2), all paths compatible with a single attack weapon and target have the same possibility of being chosen. Nodes N2.1 to N2.2 are related to the attractiveness of the targets and their quantification is based on the values suggested in API Std 780 [10].

To quantify the performance of PPS (Nodes 3.1 to 3.5), the approach described in Section 2.2 has been used. Numerical values have been retrieved from the reference work of Garcia [12] and Argenti et al. [39]. The probability of PPS effectively preventing an intrusion (N3.4) can only happen if all three functions (Intrusion Assessed Detection, Alarm Communication and Timely Intervention) happen in sequence.

As highlighted in Fig. 2, a crucial element of the BN is the implementation of the improved fragility models developed in the present study for escalation triggered by explosion, firearms and arson attack (see Section 4). However, in order to show the influence of fragility on overall vulnerability, the results have then been compared with conventional fragility models and assumptions implemented in previous studies dedicated to the assessment of the escalation of domino effect (see Section 2.3). In particular, the conventional approaches ignore the overpressure mitigation associated with the presence of bunds or dikes and consider the probability of firearms damage as unitary. The model from Landucci et al. [51] introduced in Section 2.3.1 (Model 1 in Table 1) has been used to evaluate the damage caused by heat radiation of incendiary devices.

Further details on the BN are introduced in Section 5 for the SVA of a specific case study.

4. Development of improved fragility models for security scenarios

Improved fragility models tailored to intentional attack modes to process equipment are presented in this section. Fragility models for bullet perforation, arson and mitigated explosive impact were investigated according to the methodology outlined in Section 3.1. The physical models associated with the attack vectors were simplified, but this is related to the fact that the final focus of the work was to obtain correlations for damage probability of different security scenarios, rather than describing the detailed mechanical behavior of the targeted process item. Thus, the use of the developed fragility models should be restricted to the framework of SVA and, more generally, of QRA, as they require a limited number of input parameters. This simplification is necessary for the practical use of SVA by industrial practitioners, to reduce time and costs of the analysis, as the results obtainable by a certain approach has

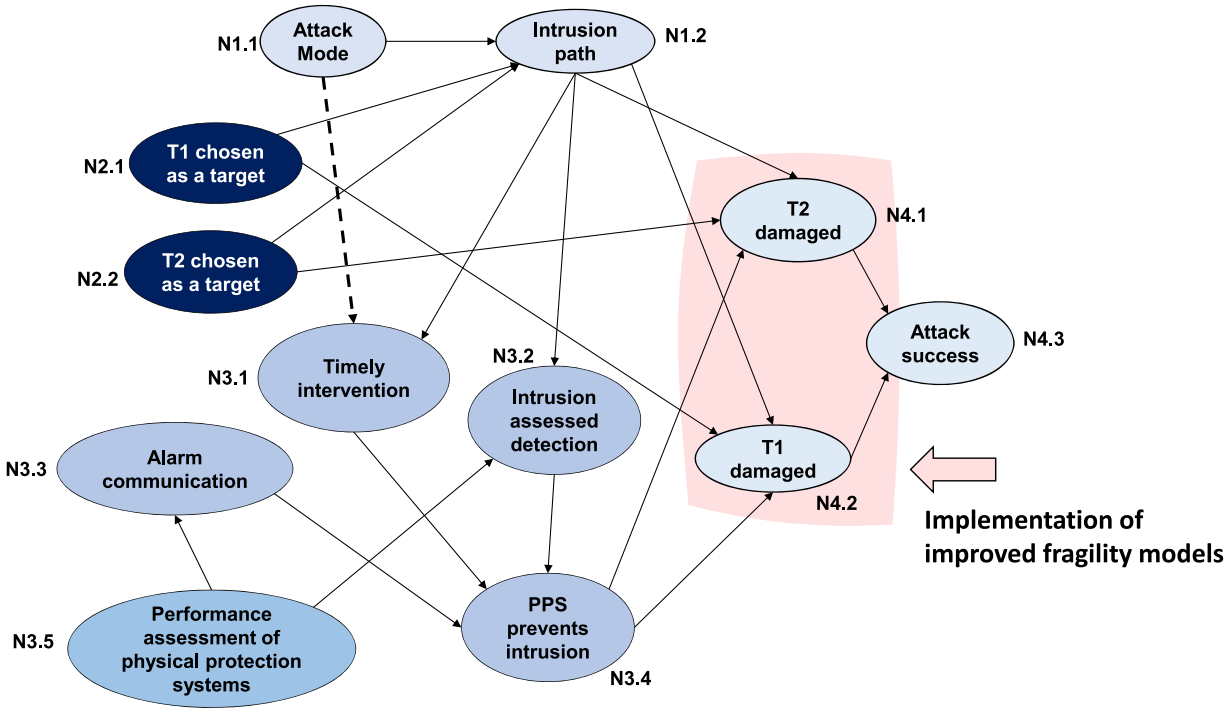


Fig. 2. Structure of the BN developed in the present study for the vulnerability assessment; two targets (T_1 and T_2) are considered for the sake of exemplification. The dashed line shows the dependency of timely intervention on the attack mode.

to be conservative.

It is also worth mentioning that the methodological framework introduced in the present work is open. Indeed, depending on the scope of the assessment and risk management [68], the implemented fragility models can be modified (e.g., depending on the firearm used [62]), integrated with other attack modes or completely changed if a higher level of precision for the prediction of the final damage to a target is required.

4.1. Fragility model for bullet perforation

The procedure developed in this study to determine the probability of damage from firearms is based on two stages. The first stage consists in the evaluation of the velocity of the bullet when impacting the target. The approach followed in this study to quantify the velocity of a bullet was proposed by the U.S. Army Research Laboratories [69]. This approach combines a simplified expression of Newton's second law with Mayevski's expression for the drag coefficient [70]. The resulting equations offer a simple expression to calculate the horizontal trajectory of the bullet, as shown in Eq. (8) and Eq. (9):

$$v = v_0 \cdot \left(1 + n \cdot \left(\frac{dv}{dx}\right)_0 \cdot \frac{(x - x_0)}{v_0}\right)^{\frac{1}{n}};\ n \neq 0 \tag{8}$$

$$v = v_0 \cdot \exp\left(\left(\frac{dv}{dx}\right)_0 \cdot \frac{(x - x_0)}{v_0}\right);\ n = 0 \tag{9}$$

where x is the position (m), x_0 is the initial position (m), v is the velocity (m/s) in the position x, v_0 is the muzzle velocity (m/s), $(dv/dx)_0$ is the muzzle retardation ((m/s)/m); n is a non-dimensional exponent and it comes from Mayevski's expression of the drag coefficient, which is proportional to a power of the velocity [70].

Three reference bullet types have been chosen in the present work. Table 2 summarizes the relevant characteristics of the reference bullets, which are typically used in assault rifles. The first reference bullet is an intermediate cartridge, the 7.62 × 39 mm (namely, B1), commonly employed for assault rifles such as the AK-47 [71]. The other two bullets, the 7.62 × 51 NATO (namely, B2) and the 7.62 × 54R (namely, B3), have a larger caliber, and are employed for sniper rifles, which allow a long firing distance and high accuracy [72].

The parameter v_0 in Table 2 have been evaluated for each reference bullet by averaging the typical values associated with commercial bullet types provided by several manufacturers [74–79]. The parameters n and $(dv/dx)_0$ have been obtained for the three reference cartridges based on the data available in literature [73] for standard bullet types with a similar mass (namely, m, see Table 2).

The second stage of the procedure consists of defining the probabilistic model based on probit regression for bullet perforation. Stewart et al. [80] conducted field tests of 7.62 × 51 mm AP (armor piercing) ammunition fired into mild steel targets. The resulting data have then been processed by Stewart et al. [80] by means of a Monte Carlo probabilistic analysis to estimate the probability of intrusion given different velocities, target thicknesses and plate material. The study considered a range of target thickness values (i.e., 10 to 32 mm) comparable to storage tanks of industrial facilities. Moreover, the plates adopted in the

Table 2
Relevant characteristic of the bullets considered in this study elaborated from manufacturers data and literature [73]. The thickness required to avoid perforation of each reference steel (S_s) is calculated according to the procedure described in Section S.1 of the Supplementary Material, whereas reference steel properties are reported in Table 3.

ID	Reference cartridge	m [g]	v_0 [m/s]	N [-]	$(dv/dx)_0$ [(m/s)/m]	S_s (Grade 250 Mpa)	S_s (Grade 350 Mpa)
B1	7.62 × 51 NATO	9.23	840.00	0.519	-0.8003	38.98	33.98
B2	7.62 × 39	8.02	740.00	0.485	-1.1747	27.93	24.47
B3	7.62 × 54R	11.19	780.00	0.493	-0.6518	39.27	34.27

study were made of steels that are compatible with the ones of atmospheric [81] and pressure vessels [82]. In particular, Grade 250 MPa and Grade 350 MPa steel plates have been considered and their relevant physical properties are shown in Table 3.

Lastly, the ammunition used in the field tests is typical of assault rifles, which are compatible with the reference bullets chosen in the first step of the procedure (see Table 2). An armor piercing bullet has been used in the reference study of Stewart et al. [80], thus obtaining conservative results. For these reasons, the data gathered in [80] constitute a significant basis to develop the fragility model.

In order to obtain a probit regression of the failure data, a dose associated with the impact of the bullet on the target needs to be defined. In this specific case, the damage is associated with the perforation of the bullet into a steel target and a reference value to measure the severity of impact is the thickness required to avoid perforation, S_s. Therefore, the dose (D_p) was defined by comparing the actual thickness of the plate (namely, s) against the value of S_s, as follows:

$$D_p = \frac{f \cdot S_s}{s} \tag{10}$$

where s and S_s are expressed in mm, and f (= 0.9 according to [80]) is a safety factor.

Several approaches are available in literature to support the evaluation of S_s. The Supplementary Material (see Section S.1) summarizes the most widely applied, which were compared in order to determine the more suitable relationship to deal with thickness values and geometrical features of typical chemical and process equipment. The Supplementary Material also shows the estimated values of S_s for the bullets and materials considered in the present study (see Table 2 and Table 3, respectively). The correlation selected to calculate S_s in the present study was derived by the study of Rosenberg and Dekel [83], obtaining the S_s values shown in Table 2.

Based on the D_p values calculated according to Eq. (10), the probit regression was obtained for each bullet velocity, based on the data obtained in [80] for Grade 250 MPa and 350 MPa steel. The first and second probit coefficients (k_1 and k_2) were estimated through the interpolation of the values obtained for the range 700-850 m/s. Fig 3a shows the probit curve obtained for Grade 250 MPa steel plates, while Fig 3b shows the probit curve for Grade 350 MPa steel plates.

The so obtained probit relationships for Grade 250 MPa steel and 350 MPa steel are respectively shown in Eq. (11) and (12):

$$Y = k_1 + k_2 \cdot \ln(D_p) = 5.25 + 9.53 \cdot \ln(D_p) \tag{11}$$

$$Y = k_1 + k_2 \cdot \ln(D_p) = 5.42 + 13.70 \cdot \ln(D_p) \tag{12}$$

An error analysis was carried out in order to verify the accuracy of the probit model developed. The results proved that the model developed for Grade 250 MPa steel has an absolute error lower than ±0.05 and a percentual error around ±5%; whereas for the case of Grade 350 MPa steel the absolute error is lower than ±0.05 and the percentual error is approximately ±10%. Hence, the fragility model developed predicts the probability of perforation with an acceptable error for both materials, see Appendix A.

Table 3
Properties of reference steels in this study from [80]; BHN is Brine Hardness and Y_t is the target flow stress.

Property	Grade 350 Mpa	Grade 250 Mpa
BHN_{max} [MPa]	180.00	160.00
BHN_{min} [MPa]	140.00	110.00
BHN_{mean} [MPa]	160.00	135.00
Y_t [Gpa]	0.63	0.53

4.2. Fragility model for arson

There are different types of incendiary devices, such as flamethrowers or incendiary bombs. Only flamethrower damage has been taken into consideration in this study, although incendiary bombs such as Molotov are easy to build and carry. However, the latter generate small pool fires (~1 m diameter) [84] that could only damage small connections and gaskets. Thus, these incendiary devices were not considered in the present study. Instead, weapons able to generate a high amount of heat radiation in a localized part of the target, such as flamethrowers, were modelled.

The methodology to obtain a fragility model for arson is as follows:

1. Model the ejected flame;
2. Simulation of the heat radiation damage;
3. Regression of the data to obtain a probit relationship.

Firstly, the flame ejected by a flamethrower is to be modeled. To build an accurate model, it is important to understand how such a weapon is built and operated. Military flamethrowers use gasoline/kerosene mixtures, and are composed of different chambers, some containing the fuel and some containing a pressurized inert gas, which is used to eject the fuel out [85]. On the other hand, commercial flamethrowers use LPG (Liquefied Petroleum Gas) [86] and are mostly used for land-management tasks [87]. Both types have an ejection pipe and an ignition source, which is necessary to ignite the fuel.

Based on the previous considerations, the fire ejected by a flamethrower was schematized as a jet fire. A high uncertainty lies on the performance of such a weapon, so the flamethrower has been modelled according to a worst-case scenario, as detailed in the Appendix B, in which the features of the considered flame are reported. In particular, a maximum operating time was estimated (t_{max} = 110s) based on the conservative assumptions documented in Appendix B.

The second stage is aimed at evaluating the damage caused by jet fire impingement on different equipment items. The impact of the jet has been evaluated by determining the time to failure *ttf* of both atmospheric and pressurized equipment featuring the typical geometries adopted in chemical and process facilities. An extended dataset of equipment features was used for the simulations, as reported in the Supplementary Material (section S.2).

To study the behavior of a vessel partially impinged in a jet fire, the lumped model developed by Landucci and coworkers [51] was adopted with specific settings detailed in the Supplementary Material (section S.2). The model was applied to generate an extended failure dataset for fired vessels. It is worth mentioning that the model was validated against experimental data and the so obtained dataset may be considered reliable [51].

Concentrating the heat load on the surface containing the liquid does not cause relevant damage, as the liquid absorbs all the heat due to its high heat capacity. This was verified in several experimental works dealing with pressurized vessels exposed to fire [88]. Moreover, previous studies demonstrated that the vapor space is the most critical point in the exposure to heat radiation, as it holds the highest stress [89]. Therefore, the most effective way to cause a rupture is concentrating the flame on the top vapor space. For this reason, the chosen filling level in each simulation was set to a minimum credible value of 20%. The chosen filling substance is benzene for atmospheric vessels and pressurized liquefied propane for pressure vessels. The maximum exposure time has been set to t_{max}, i.e., the maximum flamethrower emptying time, given the uncertainty on the maximum operating time of the flamethrower. Moreover, the tanks were considered unprotected by safety barriers (i.e., pressure safety valves, fireproofing, firefighting, etc.). This is reasonable, given the limited time duration of the jet fire impact.

After determining the *ttf* of each tank included in the dataset, the exposure time has been divided in 10s intervals. For each interval, the

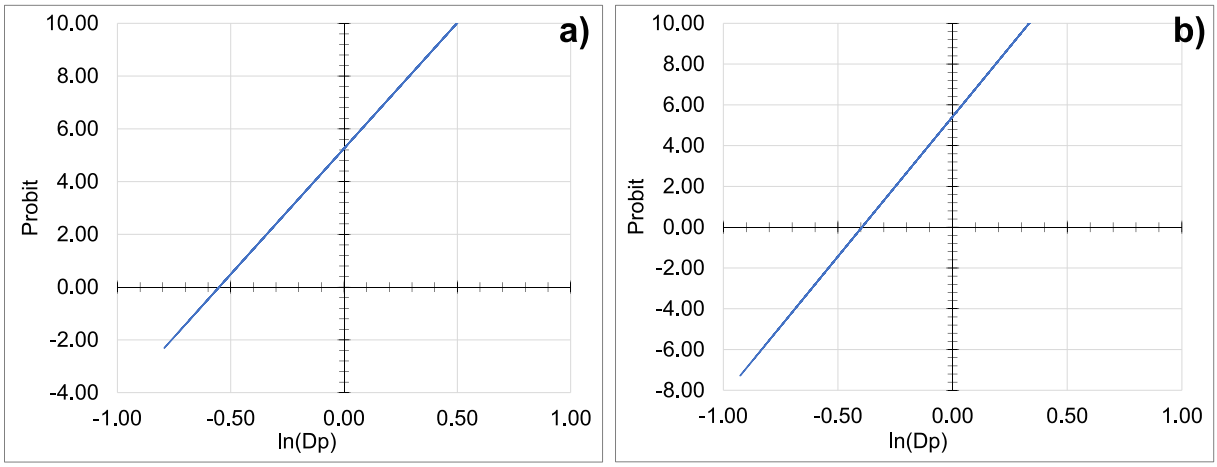


Fig. 3. Plots for evaluation of probit regression coefficients: a) Probit curve for Grade 250 MPa steel; b) Probit curve for Grade 350 MPa.

probability of failure $P_{fail}(t)$ at the exposure time t_{exp} has been computed as follows:

$$P_{fail}\left(t_{exp}\right) = \frac{N_{fail}\left(t_{exp}\right)}{N_{tot}} \tag{13}$$

where $N_{fail}(t_{exp})$ is the number of vessels that failed in a time equal or lower than t_{exp}, and N_{tot} is the total number of vessels simulated.

In this way, a distribution of probability is obtained from the initial time of fire exposure up to t_{max} (=110 s). In order to derive a simplified probit relationship, the chosen thermal dose D_{th} is the exposure time, thus:

$$D_{th} = t_{exp} \tag{14}$$

Next, the probability data were converted into probit (see Section 2.3), obtaining the distributions represented in Fig. 4a for atmospheric tanks and in Fig. 4b for pressure vessels (see the black dots in Fig. 4) with respect to the considered dose. In both panels of Fig. 4, a probit correlation fits the data over a threshold value, that is 20s for atmospheric tanks (see the dashed line in Fig. 4a) and 60s for pressure vessels (see the dashed line in Fig. 4b). A higher threshold for pressure vessels is reasonable, given the higher shell thickness value and robustness of this equipment type. The probit regression is obtained with the application of the Ordinary Least Square method to the data above the threshold considering $ln(t_{exp})$ as the independent variable. Table 4 shows the obtained probit models for atmospheric and pressure vessels.

The significance of the probit models developed can be assessed through the evaluation of the regression coefficients shown in Table 4. The *PCC* lies between -1 and 1 and a higher value signifies that a linear relation represents the sets of data well [90]. In this study, both models shown in Table 4 have a high value of *PCC* meaning that there is significative relation between the probit variable Y and $ln(t_{exp})$. Also, the *COD* [90] shows values close to unity for both correlations, thus confirming the validity of the present approach.

4.3. Fragility model for mitigated explosive impact

To evaluate the damage caused by IEDs, four different approaches have been combined. The methodology used to evaluate the probability of damaged caused by mitigated explosive impact is as follows:

1. Evaluation of equivalent TNT mass $m_{TNT,eq}$;
2. Calculation of dike relevant parameters to determine whether the mitigating effect is in place;
3. Evaluation of overpressure;
4. Probability of damage calculation.

The equivalent TNT mass $m_{TNT,eq}$ can be evaluated using the actual IED mass m_{IED} (g) and account for the actual mass fraction Ψ of the explosive and the TNT efficiency η [65], as follows:

$$m_{TNT,eq} = \Psi \cdot \eta \cdot m_{IED} \tag{15}$$

Two IED often adopted in previous attacks [18] have been considered in this study. In particular, Ammonium Nitrate – Fuel Oil (ANFO) and Triacetone Triperoxide Peroxyacetone (TATP). Data were derived from a previous study [65] and are summarized in Table 5.

Then, the presence of a dike is considered as a possible source of explosion mitigation. To calculate the reduction of overpressure, the approach from Miura et al. [64] can be used. Fig. 5 shows the geometrical parameters to be considered. The approach is based on the assumption that the mitigating effect only happens in a portion of space after the dike itself, which is named effective length, L_{eff}. If the target is within L_{eff}, then the wall significantly mitigates the overpressure, otherwise, the mitigation effect is considered negligible.

In order to apply the approach to different equivalent TNT masses, each geometrical parameter shown in Fig. 5 needs to be re-scaled through the Hopkinson-Cranz relationship [91], as follows:

$$r = \frac{R}{m_{TNT,eq}^{1/3}} \tag{16}$$

where r is the scaled length (m/kg$^{1/3}$) of the actual geometrical parameter R displayed in Fig. 5 (m).

The effective length l_{eff} (kg/m$^{1/3}$) can now be evaluated based on the re-scaled parameters as follows [64]:

$$l_{eff} = (0.765 \cdot r_{de} - 0.366) \cdot h_d + 0.9 \tag{17}$$

Meaning that, with reference to Fig. 5, the mitigating effect exists only if the actual distance between the target and the dike R_{dt} is lower than L_{eff}.

Then the overpressure generated by the explosive at a certain distance is calculated using the correlation proposed by Bounds et al. [92]:

$$\Delta P = 10^5 \cdot \left(\frac{m_{TNT,eq}^{\frac{1}{3}}}{a} + 4.4 \cdot \frac{m_{TNT,eq}^{\frac{2}{3}}}{a^2} + 14.0 \cdot \frac{m_{TNT,eq}}{a^3} \right) \tag{18}$$

where a is the distance (m) and ΔP is the overpressure (Pa). If the mitigating effect exists, then overpressure in case of mitigation (ΔP_m) can be evaluated using the following equation:

$$\Delta P_m = \Delta P\left(R_{de} + L_{eff}\right) + p \tag{19}$$

where $\Delta P(R_{de} + L_{eff})$ is the overpressure evaluated at a distance ($R_{de} + L_{eff}$) with Eq. (18), while p in Pa is derived by the study from Miura et al.

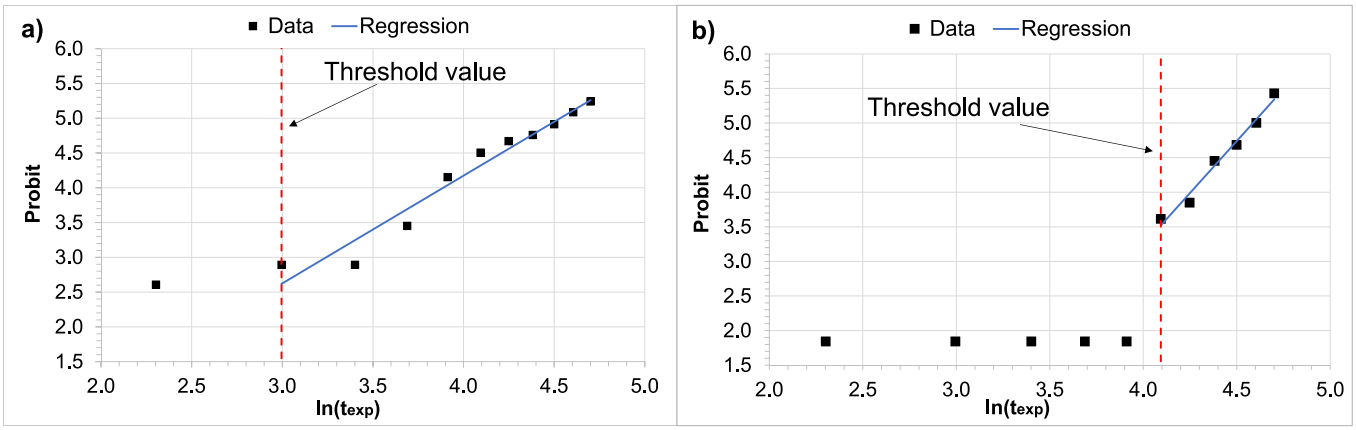


Fig. 4. a) Simulation failure data and probit regression for atmospheric tanks; b) Simulation failure data and probit regression for pressure vessels; t_{exp} is the time of exposure to the flame.

Table 4
Probit model and regression coefficient for attack with an incendiary device; Y is the probit variable, t_{exp} is the exposure time.

	Atmospheric Tanks	Pressure Vessels
Probit model	$Y = -2.02 + 1.55 \cdot \ln(t_{exp})$	$Y = -8.80 + 3.01 \cdot \ln(t_{exp})$.
Pearson correlation coefficient (PPC)	0.97	0.99
Coefficient of determination (COD)	0.95	0.98

Table 5
Values of mass fraction Ψ and TNT efficiency η for IEDs used in this study, derived from [65].

IED Type	Ψ	η
ANFO	0.50	0.23
TATP	1.00	0.61

[64] using the scaled parameters as follows:

$$p = 3.187 \cdot 10^6 \cdot r_{de}^{-4.59} \cdot \exp\left(\left(-0.20 \cdot r_{de}^2 + 2.62 \cdot r_{de} - 8.33\right) \cdot h_d\right) \quad (20)$$

If the mitigated effect is not relevant, the overpressure (ΔP_{nm}) is obtained by using Eq. (18) where a becomes R_{et}, i.e., the distance between explosive and target (see Fig. 5).

The so-obtained overpressure can then be finally used to assess the probability of damage using existing fragility models. In particular, Model 3 in Table 1 [53] was adopted.

5. Application to a demonstration case study

5.1. Description of the facility and targets

The fragility models developed in Section 4 have been implemented in the BN probabilistic model described in Section 3.2 to support an industrial SVA case study. Fig. 6 shows the layout of the analyzed facility. The facility is surrounded by an external perimeter and has one main access gate (possible intrusion point #3) and two secondary ones (possible intrusion points #1 and #2). Both pedestrians and vehicles can access the facility from the main gate, while the secondary gates are for vehicles only. Additionally, the facility has a parking lot for employees (possible intrusion point number #4).

The figure also highlights the targets and relevant assets, as well as the selected intrusion paths. Four targets have been identified, consisting in two horizontal pressure vessels (P_1 and P_2 in Fig. 6) and two

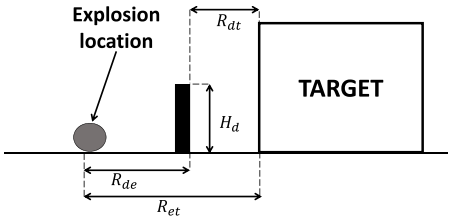


Fig. 5. Geometrical reference values for mitigated explosive impact.

atmospheric tanks (A_1 and A_2 in Fig. 6). The main features of the tanks are shown in Table 6. A_1 and A_2 store styrene and ethanol respectively and are located in proximity of the external perimeter. Tank A_2 is bounded by a 4m high dike. P_1 and P_2 store 1,3-butadiene and acrylonitrile respectively and are located near the process area and a warehouse. Table 6 reports the necessary information on the target equipment to carry out SVA.

5.2. Description of attack scenarios and PPS in place

The facility has a PPS system in place. The external perimeter is highlighted in yellow in Fig. 6 and is protected by a fence and by a video motion detection system connected to the Closed Circuit Television (CCTV). The main gate (red gate in Fig. 6) is surveilled: personnel is checked through automatic credentials checks, while vehicles and drivers undergo manual credentials check. The secondary gates (blue gates in Fig. 6) are instead unattended. The facility is also surveilled with CCTV both around the perimeter and inside. The parking lot is instead unsupervised. Employees are present on-site for 12 hours a day, while the facility is surveilled by security guards at night.

Table 7 summarizes the intrusion scenarios analyzed in this work, which were defined for illustrative purposes. It is worth mentioning that systematic procedures based on Adversary Path Analysis [10] may be also applied at this stage to determine all relevant intrusion paths [37]; however, their application is outside the scope of this study.

In scenarios a) and b) the attacker targets P_1. The chosen path is secluded, as the attacker moves along the external perimeter of the facility. In scenarios c) and d), the attacker targets P_2 and instead choses a path that directly crosses operation areas. Scenarios e) and f) feature the use of a high amount of ANFO, therefore the attacker enters the facility using a vehicle. To do so, they forge a counterfeit badge in order to pass the controls at the entry gate. In scenarios g) and h), the attacker instead enters the facility with a small amount of TATP by bypassing the automatic credentials check at the main gate. Scenario i) accounts for more targets at the same time (P_1, P_2, and A_1); indeed, the attack is carried out

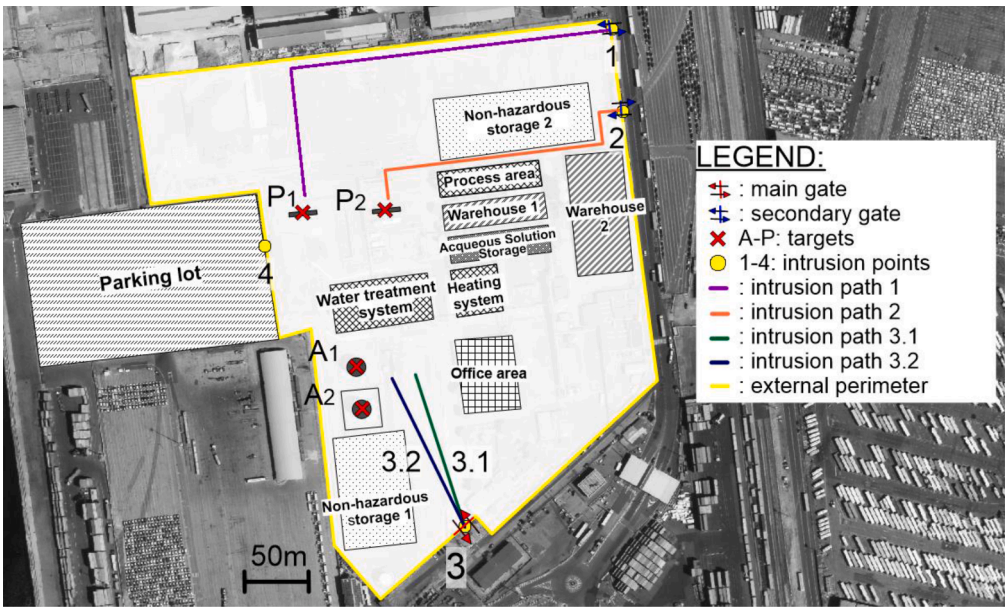


Fig. 6. Layout of the facility selected as a case study. Target features are reported in Table 6; attack scenarios are listed in Table 7. A: atmospheric storage tanks. P: pressurized tanks.

Table 6
Main features of the tanks considered as targets in the case study.

Name	Content	Type	Diameter [m]	Length or height [m]	Thickness [mm]	Construction material	Capacity [m^3]
P_1	1,3-butadiene	pressurized	8.0	20.0	24.0	Grade 250MPa	250
P_2	Acrylonitrile	pressurized	8.0	20.0	24.0	Grade 250MPa	250
A_1	Styrene	Atmospheric	12.0	9.0	9.2	Grade 250MPa	1000
A_2	Ethanol	Atmospheric	12.0	9.0	9.2	Grade 250MPa	1000

from the outside and the attacker uses a firearm, so they can target multiple equipment in the span of a few seconds.

The information on the paths and the PPSs related to each adversary task sequence are summarized in Table 7.

5.3. BN input data quantification

Fig. 7 shows the BN used for the assessment of the case study. First of all, to quantify the performance of PPS means to quantify how likely is for an intruder to come across someone (employees or security guards) along an intrusion path. From existing literature [39] we know that, during the day, the probability of coming across employees on a path crossing assets is 70 % (20% on paths crossing empty areas), whereas, during the night, the probability of coming across security guards is 5%. Therefore, we used Node N3.1 (called "Shift") to define a "day shift", referring to the probability of coming across employees only on a path versus a "night shift" to represents the probability of coming across security guards only. It has to be specified that the probability values associated to Node 3.1 can be changed in case of availability of case-specific data. In our case, we assigned values to Node 3.1 based on a conservative assumption: considering that the probability of coming across employees is higher compared to that of security guards, because of the higher number of employees with respect to security guards [18], we chose to set the node "Shift" to 50%-50% (i.e. 12 hours day-shift and 12 hours night-shift) rather than 33%-67% (i.e. 8 hours day-shift + 16 hours night shift).Then, as explained before, to quantify Nodes N3.2 and N3.6 related to personnel presence, values have been taken from literature [18]. N3.3, N3.4 and N3.5 to N3.32 can be quantified using the approach and data presented in Section 2.2. by using the quantitative data from Argenti et al. [39]. For the sake of exemplification, Node N3.8 related to the intrusion detection from security guards is considered. It depends on the presence of security guards (N3.6) and their level of training (N3.7); if security guards are absent, then the probability of detecting the intrusion is null. If the guards are present and have a high level of training, the probability of detecting the intrusion is 0.85. The impact factor associated to a low level of training is 0.5 [39], meaning that the probability of detecting the intrusion lowers to 0.40 in that case. N3.31 can be quantified considering the PPS in place for each intrusion path shown in Table 7: if at least one PPS present on the attack path works, then the intrusion is detected. To evaluate Node 3.34, the approach in Section 2.2 requires the quantification of the time needed by the intruder to complete attack. The following data have been considered for the analysis:

- The emergency response team comes from the main gate; then, 180s are needed for its preparation and their running speed is 4 m/s, which is the medium value reported in literature [12]. So, for instance, the emergency team needs on average 265s to reach P_1 in attack scenario a) and 213s to reach A_1 in scenario "e".
- The attacker needs 90s to jump the gate and 20s to place and detonate the explosive [12]. Its running speed on foot is 3.2 m/s, which is the lowest speed reported in literature [12]. A reduced velocity is considered not only to account for the weight of the weapons, but also because the attacker will not run at full speed in order to decrease the probability of being detected. If the attacked enters with a truck (Intrusion Path 3.1 in Table 7), they drive the truck at 30 km/h (approximately 8.3 m/s). For instance, the mean adversary intrusion time t_P for scenario e) is 125s. Using the values of t_{ERT} computed for scenario "e" and applying Eq. 5, the probability of Timely Intervention P_T for scenario "e" is 0.077.

The PPS system effectively prevents the intrusion only if all three

Table 7
Case study: description of the intrusion scenarios analyzed. For intrusion points and paths see Fig. 6; CCTV: Closed Circuit Television.

Intrusion Point	Intrusion Path	Target	Attack Mode	Adversary task sequence	PPS	Scenario ID
#1 (Secondary Gate)	1	P_1	15 kg TATP	Trespass the gate; walk 350 m to the target; place the explosive	CCTV; Intrusion assessment by employees; Intrusion assessment by security guards;	a)
			Arson for 60 s	Trespass the gate; walk 350 m to the target; use the weapon	CCTV; Intrusion assessment by employees; Intrusion assessment by security guards;	b)
#2 (Secondary Gate)	2	P_2	15 kg TATP	Trespass the gate; walk 250 m to the target; place the explosive	CCTV; Intrusion assessment by employees; Intrusion assessment by security guards;	c)
			Arson for 60 s	Trespass the gate; walk 250 m to the target; use the weapon	CCTV; Intrusion assessment by employees; Intrusion assessment by security guards;	d)
#3 (Main Gate)	3.1	A_1	1000 kg ANFO	Use counterfeit badge to pass manual credential check at vehicle gate;	CCTV; Intrusion detection at vehicle portal; Intrusion assessment by employees; Intrusion assessment by security guards;	e)
		A_2	1000 kg ANFO	drive 125 m to the target; detonate the explosive		f)
	3.2	A_1	15 kg TATP	Bypass automatic credentials check at personnel portal; walk 135 m to the target; place the explosive	CCTV; Intrusion detection at personnel portal; Intrusion assessment by employees; Intrusion assessment by security guards;	g)
		A_2	15 kg TATP			h)
#4 (Parking Lot)	4	P_1 P_2 A_1	Firearm; B2	Attack from outside the perimeter of the facility	CCTV	i)

identified actions happen; therefore, node 3.33 is in the positive state only if N3.31, N3.32, and N.3.29 are in the positive state.

Nodes N4 are representative of the target fragility. These nodes are quantified using fragility models introduced in Section 4. The input data for each attack mode can be retrieved from Fig. 6, Table 6, and Table 7 and are:

- Explosive attacks: explosive type and mass, target type, distance from target, dike geometrical parameters (if present); for instance, in scenario h) 15 kg of TATP (9.15 kg of equivalent TNT, according to Eq. (15)) are used to target A_2. Considering the mitigating effect of the dike and applying Eqs. (16) - (20), the overpressure on A_2 is 0.087 bar and the probability of A_2 failing is 0.03 using Model 3 in Table 1. If the effect of the dike is neglected, then the overpressure on A_2 can be calculated with Eq. (18) and is 0.11 bar, leading to a probability of damage of 0.11.
- Firearm attack: bullet type, distance from target, target construction material and shell thickness; for instance, in scenario i), P_1 is 40 m distant from the attack points; by applying Eq. (8) using the data in Table 2, a speed of around 700 m/s at impact with the tank is obtained. Using the models detailed in Section 4.1, T_s is 25.30 mm. Using Eq. 9, a probability of damage of 0.40 is obtained.
- Arson attack: target type, exposure time. For instance, the probability of damaging P_2 in scenario d) can be computed using the model for pressurized vessels in Table 4, which leads to a damage probability of 0.06.

Node 4.5 can be quantified considering that the attack is considered "successful" only if at least one equipment among A_1, A_2, P_1, and P_2 is damaged.

Finally, a sensitivity analysis has been performed on the BN by identifying the parameters whose variation could impact the attack success likelihood. A one-at-a-time sensitivity analysis has been conducted, meaning that vulnerability variation is assessed by individually varying each parameter [93]. Both the target-specific and overall vulnerability maximum range of variation have been identified.

More specifically, the sensitivity analysis involved the new fragility models developed, i.e., firearms model and arson model. This means that the targets interested by the sensitivity analysis are A_1, P_1 and P_2, since A_2 is only targeted by explosives.

The parameters included in the sensitivity analysis for firearms attack are the bullet type, the distance from the target and the target construction material. The bullet type has been varied among B1, B2 and B3 (see Table 2); the distance from the target has been varied in a $\pm$ 30% range. Finally, the construction material has been varied between Grade 250 MPa and Grade 350 MPa steel (see Table 3). The type of bullet and the distance influence the velocity of the bullet when impacting the target, while the target construction material directly influences the fragility curve, given the difference in physical properties.

The parameter included in the sensitivity analysis for arson attack is the exposure time, which has been varied in a $\pm$ 30% range of the baseline value shown in Table 7.

6. Results and discussion

6.1. Vulnerability assessment

The use of the BN shown in Fig. 7 allowed for the evaluation of PPS

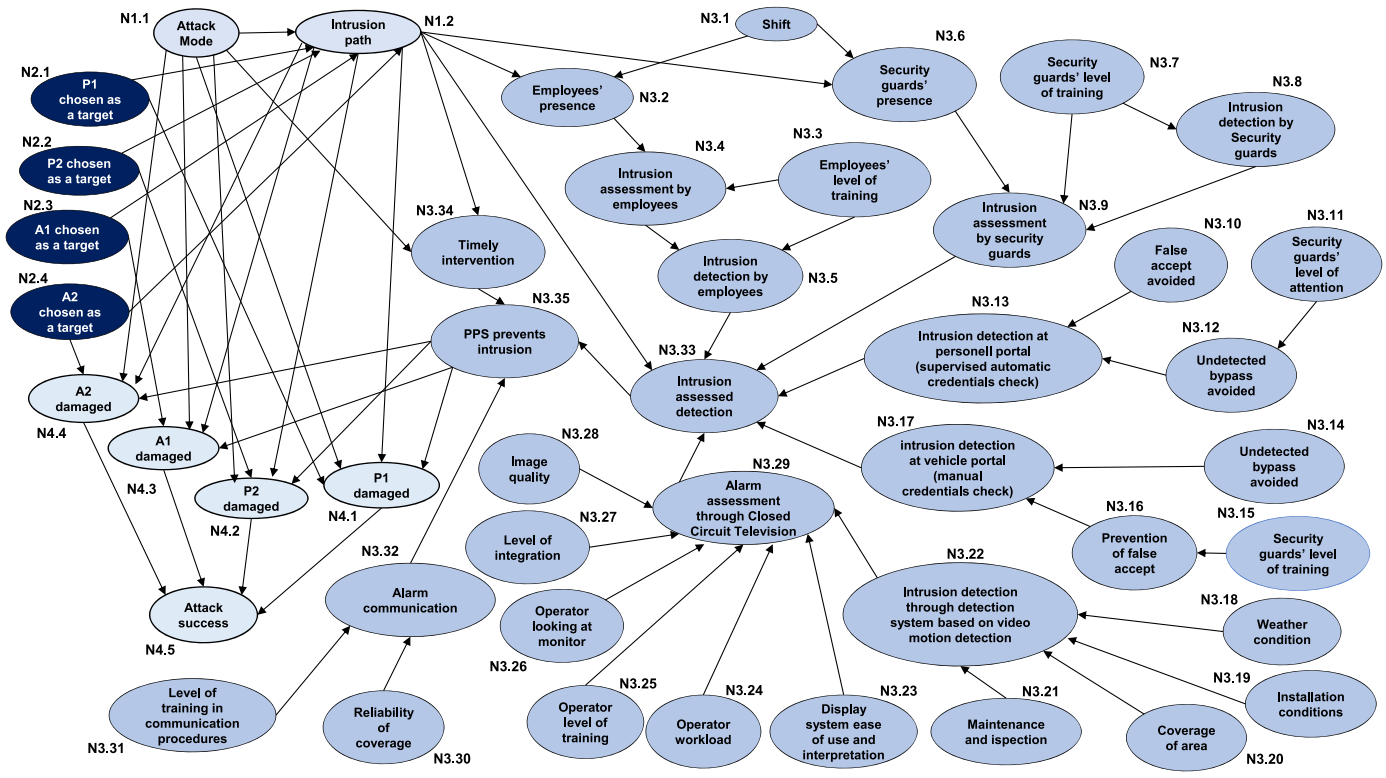


Fig. 7. Bayesian Network applied to the analysis of the case study.

performance and attack success likelihood for the case study. The so obtained results are summarized in Table 8, which shows the prior probabilities, i.e., the probability obtained without setting any evidence, as well as the probability when the attack scenarios in Table 7 are set. The calculations were obtained using GeNIe Modeler as stated in Section 3.2. To obtain the probabilities of the attack scenarios, GeNIe allows for all needed evidence to be set. For example, to evaluate the success of scenario "a", evidences were set on Nodes N1.1, N1.2 and N2.1, and the probability of attack success in Node 4.5 was calculated accordingly.

Part A of Table 8 is dedicated to the performance summary of the PPS in place. The prior scenario shows that PPS have a probability of neutralizing an attack lower than 0.10. Timely intervention and intrusion assessed detection, which are two of three functions of PPS, especially have a low performance; the maximum probability of intrusion assessed detection for the scenarios outlined in Table 7 is 0.61 (scenarios "g" and "h), while the maximum probability of timely intervention is lower than 0.50. This firstly means that PPS are not installed in critical locations and, if they are, their performance is not sufficiently high due to low quality of instrumentation or poor training of security personnel. Consequently, the conditional probability of PPS successfully preventing intrusion in each scenario is always lower than 0.20. The performance of PPS is, therefore, unsatisfactory. As these values were calculated based on average literature data, representative of industrial facilities performance, this evidences that more resources should be allocated to improve the security aspects of process facilities, in order to effectively raise the probability of interruption of an intentional attack.

Part B in Table 8 summarizes target specific vulnerability and the overall likelihood of attack success based on the implementation of the fragility models developed aimed at supporting the failure probability estimation in case of successful attack.

Scenarios involving the use of ANFO (scenario "e" and "f") yield the same probability values. This is due to two factors: firstly, the targets

Table 8
Case study results: scenario-based analysis; for attack scenarios see Table 7.

Event	State	Priors	Posterior probability for single attack scenario								
			a)	b)	c)	d)	e)	f)	g)	h)	i)
A. PPS performance											
Intrusion assessed detection	("success state")	0.40	0.43	0.43	0.54	0.54	0.61	0.61	0.61	0.61	0.37
Timely Intervention	("success state")	0.15	0.27	0.47	0.17	0.35	0.08	0.08	0.17	0.17	0.00
PPS prevents intrusion	("success state")	0.06	0.09	0.16	0.07	0.16	0.04	0.04	0.08	0.08	0.00
B. Vulnerability using advanced fragility models											
A_1 damaged	("success state")	0.18	0.00	0.00	0.00	0.00	0.68	0.68	0.32	0.32	1.00
A_2 damaged	("success state")	0.02	0.00	0.00	0.00	0.00	0.18	0.18	0.03	0.03	0.00
P_1 damaged	("success state")	0.11	0.33	0.06	0.00	0.00	0.00	0.00	0.00	0.00	0.40
P_2 damaged	("success state")	0.04	0.00	0.00	0.34	0.06	0.00	0.00	0.00	0.00	0.04
Attack success	("success state")	0.31	0.33	0.06	0.34	0.06	0.73	0.73	0.34	0.34	1.00
C. Vulnerability using the conservative approach											
A_1 damaged	("success state")	0.18	0.00	0.00	0.00	0.00	0.68	0.68	0.32	0.32	1.00
A_2 damaged	("success state")	0.07	0.00	0.00	0.00	0.00	0.51	0.51	0.10	0.10	0.00
P_1 damaged	("success state")	0.30	0.33	0.82	0.00	0.00	0.00	0.00	0.00	0.00	1.00
P_2 damaged	("success state")	0.30	0.00	0.00	0.34	0.83	0.00	0.00	0.00	0.00	1.00
Attack success	("success state")	0.61	0.33	0.82	0.34	0.83	0.83	0.83	0.38	0.38	1.00

have the same probability of being chosen because they are both atmospheric tanks. Secondarily, the intrusion path is the same, which means that both A_1 and A_2 will be damaged either way even if only one target is chosen by the attacker. The same consideration can be done for scenarios "g" and "h" involving the use of TATP. Scenarios "e" and "f" are critical from both a PPS standpoint and a fragility standpoint. In fact, the probability of PPS preventing the intrusion is one of the lowest among the cases analyzed (0.04) and the probability of damaging the targets is among the highest for A_1 (0.68) and the highest for A_2 (0.18).

Scenarios involving the use of TATP on atmospheric equipment (scenarios "g" and "h") are less critical compared to scenarios "e" and "f" involving ANFO. Firstly, the probability of timely intervention is higher given that the intruder has to walk instead of driving a truck. The probability of damaging A_1 and A_2 is also significantly lower; in fact, although TATP has a higher TNT equivalency ratio, the small quantity of TATP that can be carried in a backpack does not compensate for the amount of ANFO that can be hidden in a truck.

Attacks using firearms (scenario "i") are the most critical due to both PPS performance and equipment fragility. Even if an intrusion is assessed from PPS, the attack cannot be stopped because the attack is almost instantaneous, making it impossible for the emergency response team to act. Moreover, the probability of damaging the targets is among the highest of all cases. Atmospheric tanks are especially vulnerable, as shown by the unitary probability of successfully damaging A_1.

Scenario "b" and "d", which involve arson attack, have a probability of success lower than 0.1, meaning that arson is not a critical attack mode for pressure vessels. This is the result of both the performance of PPS and the resistance of the equipment. Scenarios "b" and "d" have the highest probability of timely intervention, since the incendiary weapon needs to be fired for 60s, which highly delays the attacker. Moreover, the high thickness of pressure equipment makes them less vulnerable to arson attacks.

Finally, Part C in Table 8 summarizes results for vulnerability assessment using a conservative approach, as explained in Section 3.2. Arson (scenarios "b" and "d") has a 90% lower credibility than what assumed by the conservative approach, as seen by comparing Part B and Part C of Table 8. This means that the conservative estimation was highly overestimating the impact of arson on pressure vessels. In scenarios "e" and "f", in which ANFO is used to damage atmospheric tanks, the vulnerability of target A_2 is reduced by 65%, leading to an overall reduction of over 10% in vulnerability. This shows that dikes can be effective in mitigating the effect of overpressure, even if they are not built with the specific purpose of being blast walls. The same reduction in vulnerability can also be noticed for attacks with TATP (scenario "g" and "h").

A more precise estimation can be obtained from the advanced fragility model for firearms. A reduction of attack success likelihood up to around 95% can be observed for pressure vessels in scenario "i". On the other hand, atmospheric tanks keep the same vulnerability due to the lower shell thickness values, which causes them to be very vulnerable targets for firearms.

6.2. Sensitivity Analysis

As outlined in Section 5.3, sensitivity analysis has been performed in order to assess the variability of vulnerability estimates by modifying relevant parameters. Fig. 8 summarizes the results and shows the comparison with vulnerability evaluated using the conservative approach (see Section 3.2).

The vulnerability associated with atmospheric tank A_1 is not significantly modified by the variation of parameters and is not reduced by improving the material properties (i.e., considering steel Grade 350 MPa). This confirms the critical vulnerability of atmospheric equipment towards attacks performed by using firearms.

On the other hand, the vulnerability estimated for pressure vessels P_1 and P_2 by means of the present approach is significantly lower compared to the one obtained by the conservative approach. Moreover, the baseline application of improved fragility models shows that P_2 has a 90% lower vulnerability compared to P_1. In fact, P_2 is located further from the shooting position (intrusion point 4 in Fig. 6) compared to P_1, which lowers the shooting success probability. This could not be observed by means of the conservative approach. The probability of damaging both P_1 and P_2 is significantly varied in the sensitivity analysis. However, the maximum values of successfully damaging P_1 and P_2 obtained by the sensitivity analysis are 30% lower than the conservative approach vulnerability.

The use of the fragility models developed leads to a baseline value of overall plant vulnerability that is approximately 50% lower than the one obtained by means of the conservative approach. The range of variation of overall plant vulnerability obtained from the sensitivity analysis is at most 25% and at the least -15%.

The relevant decrease of plant vulnerability shows that the use of improved fragility models can offer guidance to a more correct allocation of resources compared to using conservative approaches.

6.3. Discussion

The application analysis of the case study demonstrate that the present methodology is suitable for identifying critical security issues among chemical and facilities. In particular, the analysis evidenced a

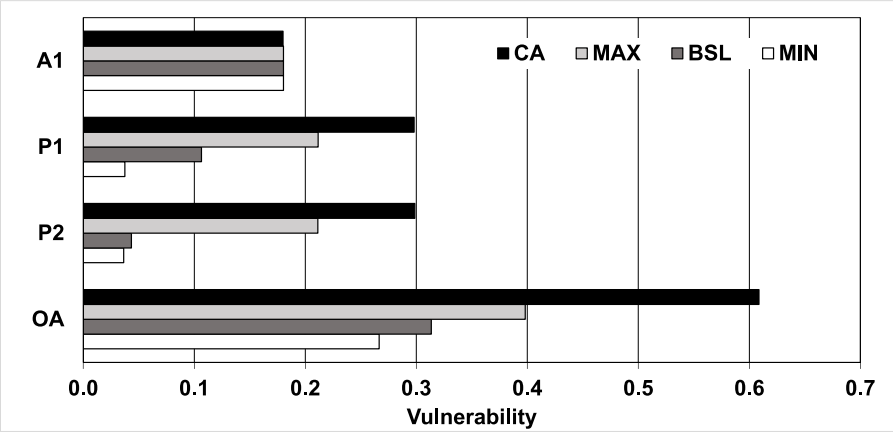


Fig. 8. Results of the sensitivity analysis: A_1, P_1 and P_2 are the vulnerabilities associated with each target at the correspondent ID, OA is the overall attack success probability, BSL is the baseline value of vulnerability obtained, MAX and MIX are respectively maximum and minimum value of vulnerability obtained, and CA is the vulnerability obtained using the conservative approach (see Section 3.2).

lack in PPS effectiveness, given that the maximum probability of effectively stop an intrusion is 0.16, as shown in Table 8. However, it must be noted that PPS effectiveness was quantified based on the outcomes of a study providing results of general validity [39]. The analysis could be improved by tailoring the PPS effectiveness directly on the facilities examined; in this way, more precise information on security measures could be obtained. In particular, the organization of a given site affects the personnel presence and its training level. For the present study, baseline values were assumed to quantify Nodes N3.2 and N3.6 (see Fig. 7) associated with detection by internal personnel, as explained in Section 5.3. Nevertheless, this methodology can be even extended to unmanned facilities, as the detection system can be customized, once a list of PPS available on-site is available. In order to determine the influence of nodes associated with personnel presence and training, the values of Node N3.2 and N3.6 were varied in a range of ±30%. The maximum obtained variation of overall vulnerability is around ±1%. This is due to the fact that the overall performance of PPS in preventing intrusion (Node N3.35 in Fig. 7) is mostly affected by the emergency response team (Node N3.34 in Fig. 7). Thus, any variation of nodes related to the performance of internal personnel does not significantly affect the overall vulnerability of the plant, as any change is shadowed by Node N3.34.

The proposed improved fragility models allowed for a more precise evaluation of vulnerability of a given process facility. To develop the fragility model, conservative assumptions on the physical model were made in order to reduce input parameters and simplify the expressions. The combined model for overpressure allowed to consider the mitigating effect from dikes, which are commonly installed in process facilities, but without the specific purpose of overpressure protection [56]. The probability of damaging A_2 decreased from 0.51 to 0.18 when considering the mitigation due to dikes (scenario "f"), making them also an effective security barrier. The model developed for firearms damage showed that atmospheric vessels are very vulnerable to this type of attack, given their relative low thickness. Indeed, scenario "i" showed that the probability of damage of A_1 remained 1.00 even when applying the new fragility model. Pressurized vessels are instead less vulnerable, due to the higher thickness of the shell. This can also be noticed in scenario "i": the probability of damaging P_1 reduced from 1.00 to 0.40 and the probability of damaging P_2 varied from 1.00 to 0.04 with the application of the firearm fragility model, showing the benefit of using it with respect to conventional fragility models for equipment exposed to fire. In this sense, additional models could be developed to account for the different types of firearms, bullet size and construction material of chemical equipment, as well as different attack devices. It is also important to note that attacks with firearms are also critical to prevent using PPS. As a matter of fact, these are sudden attacks and could happen far away from the plant external perimeter. To prevent such attacks, a study of the surrounding is necessary since the attacker could take advantage of height points, i.e., highways, to circumvent possible perimetral barriers. Indeed, using concrete perimetral fences might pose an obstacle for attackers, who would then need to climb the wall to be able to aim at the target. This would increase their chance to be identified. In this perspective, a dike might also serve not only as a safety barrier and a protection from explosives, but also as a barrier from potential shooters.

The application of the improved model for arson showed that pressure vessels are only slightly vulnerable to heat radiation from an incendiary device; scenario "b" showed how the damage probability decreases from 0.82 to 0.06 by using the improved fragility model. However, this scenario remains critical, because a catastrophic failure of a pressure vessel could cause very severe consequences [65].

Equipment damage is the starting point of a loss of containment, which can bring to the potential loss of human lives and assets. Therefore, a risk evaluation criterion that involves both this aspect is beneficial in decision making processes as well. Pasman and Rogers [94] showed that BN are a powerful tool for consequence assessment, once physical effects from the scenarios following loss of containments have been quantified. Moreover, Khakzad et al. [95] developed a methodology to include the evaluation of mitigation measures in the BN, e.g., fireproofing.

Future works need to integrate the economic and the human aspects of risk mentioned above, as well as the performance of safety barriers, in the perspective of risk-related decision-making processes. In this perspective, BN allow for the combination of different decision criteria, making them a suitable tool for integrated safety and security studies.

7. Conclusions

As the threat to intentional attacks to chemical facilities is on the rise and particularly prominent in a time when countries with high-developed chemical industries are the site of violent conflicts, proper quantitative tools for security risk analysis need to be defined.

This work focused on the improvement of fragility models that are used to quantitatively assess the vulnerability of chemical equipment, in terms of probability of damage. Fragility models have been developed based on probit regression, which is used in conventional safety risk analyses due to its simple application.

Fragility models for bullet perforation, arson and mitigated explosive impact have been developed. The developed models implement simplifying yet conservative assumptions, in order to minimize the input needed for the analysis. The fragility models developed have shown that atmospheric tanks are highly vulnerable to attack with firearms. The vulnerability of pressurized vessels is reduced up to 95% with respect to atmospheric vessels, due the higher thickness of the shell. However, pressurized vessels are more susceptible to arson attacks for high exposure times.

The use of advanced fragility models to a case study showed a 45% reduction of overall plant vulnerability compared to the use of a conservative approach, allowing for a more precise security analysis. Still, PPS performance was demonstrated to critically affect the vulnerability of process facilities, as the probability of PPS successfully preventing the attack is lower than 10%. These considerations highlight the need to improve the current security measures in chemical facilities. The developed models constitute one step further towards the harmonization of approaches used in operational safety and security, whose integration will be explored in future studies. The possibility to analyze each node and to implement risk assessment criteria make BN an adequate tool for vulnerability assessment. In conclusion, the evaluation of physical fragility with adequate but simplified fragility models is essential for SVA. Equipment fragility, coupled with PPS performance, can provide guidance for security managers and analysists in security investment by highlighting the most critical assets and barriers.

CRediT authorship contribution statement

Giulia Marroni: Writing – original draft, Visualization, Software, Formal analysis. **Leonardo Casini:** Visualization, Software. **Andrea Bartolucci:** Writing – review & editing. **Sanneke Kuipers:** Writing – review & editing, Project administration. **Valeria Casson Moreno:** Writing – review & editing, Validation, Methodology, Investigation, Formal analysis, Data curation. **Gabriele Landucci:** Writing – review & editing, Supervision, Resources, Project administration, Funding acquisition, Conceptualization.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This study was in part developed within the project LIFE20 ENV/IT/000436 – LIFE SECURDOMINO "Seveso sites: assessment of integrated safety-security hazards and risks and related domino effects" with the contribution of LIFE Program of the European Union.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.ress.2023.109880.

Appendix A –Fragility model for bullet perforation: error analysis

An error analysis was carried out in order to verify the accuracy of the probit model developed in Section 4.1. Absolute error *AE* and relative error *RE* have been defined as follows:

$$AE = P_{regr} - P_{data} \tag{A.1}$$

$$RE = \frac{P_{regr} - P_{data}}{P_{data}} \tag{A.2}$$

where P_{regr} is the probability obtained using the developed probit regression and P_{data} is the probability obtained by the reference study [80]. The parity plot reported in Fig. A.1 shows the comparison between P_{data} and P_{regr} and related *AE* and *ER*.

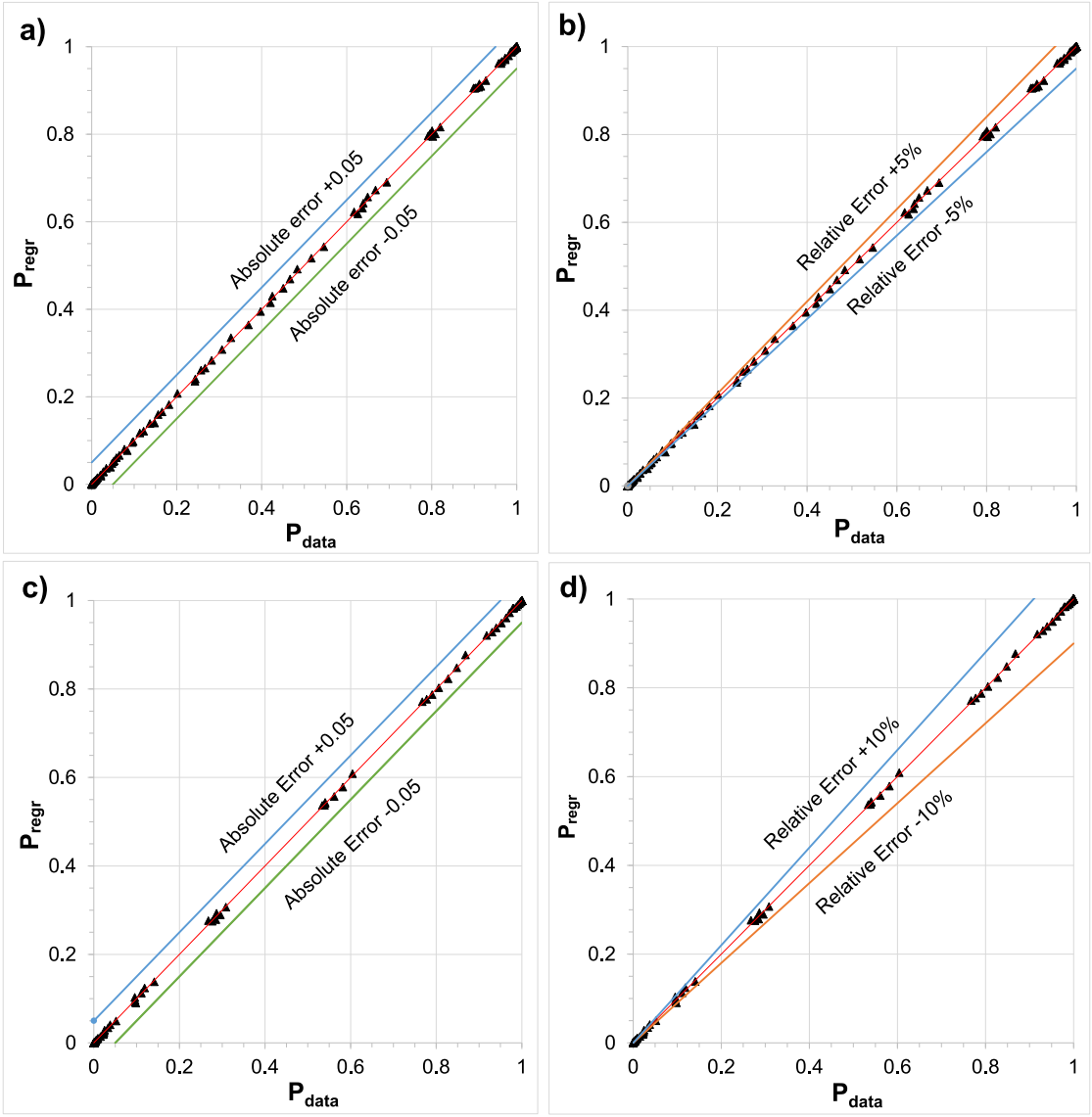


Fig. A.1. Error analysis of the probit regression developed in the present work for the firearm impact on process equipment; parity plots for: a) absolute error for Grade 250 MPa steel, b) relative error for Grade 250 MPa steel, c) absolute error for Grade 350 MPa steel (c), parity plot of relative error for Grade 350 MPa steel (d).

Appendix B – Flamethrower impact assessment

The aim of the present Appendix is to model the characteristics of a flamethrower in order to obtain the fragility model for arson. As stated in Section 4.2, a high uncertainty lies in the definition of typical parameters of a such a weapon. Extensive reviews of flamethrowers used in war context are available, however the models are dated and can have very different parameters [85].

Given that typically flamethrowers used for offense operate using gasoline/kerosene mixtures, simulations have been run in the software DNV GL Phast 8.2 [96] with different sets of chemicals, in order to obtain a worst case scenario of flame length, surface emissive power and emptying time to be used. A release from a 5mm hole of 50 L of pressurized flammable substance has been simulated.

Considering the typical composition of benzene and kerosene, two simulations were carried out: the first one used n-butane as key compound of the volatile fraction of gasoline. The second one used n-octane as key compound for the heavy fraction of gasoline. The results are gathered in Table B.1 and represent the worst value obtained from the two simulations for flame length, maximum emptying time t_{max} and maximum surface emissive power. These values have been used in Section 4.2 to study the behavior of vessels exposed to the flamethrower flame.

Table B.1
Worst-case characteristics of the flamethrower flame, from the simulation of a 5mm release of different flammable liquids; L_{jet} is the length of the flame, t_{max} is the maximum emptying time and SEP_{max} is the maximum surface emissive power.

Flamethrower characteristics	L_{jet} [m]	t_{max} [s]	SEP_{max} [kW/m^2]
	10	110	150

References

[1] van Staalduinen MA, Khan F, Gadag V, Reniers G. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliab Eng Syst Saf 2017;157:23–34. https://doi.org/10.1016/j.ress.2016.08.014.

[2] Casson Moreno V, Reniers G, Salzano E, Cozzani V. Analysis of physical and cyber security-related events in the chemical and process industry. Process Safety and Environmental Protection 2018;116:621–31. https://doi.org/10.1016/j.psep.2018.03.026.

[3] Iaiani M, Casson Moreno V, Reniers G, Tugnoli A, Cozzani V. Analysis of events involving the intentional release of hazardous substances from industrial facilities. Reliab Eng Syst Saf 2021;212:107593. https://doi.org/10.1016/j.ress.2021.107593.

[4] United Nations Interregional Crime and Justice Research Institute (UNICRI). CBRN Risk Mitigation and Security Governance Programme n.d. http://www.unicri.it/topics/cbrn (accessed February 28, 2022).

[5] U.S. Department of Homeland Security - About DHS n.d. https://www.dhs.gov/about-dhs (accessed February 28, 2022).

[6] Cybersecurity and Infrastructure Security Agency (CISA). Chemical Facility Anti-terrorism standards (CFATS) n.d. https://www.cisa.gov/chemical-facility-anti-terrorism-standards (accessed February 28, 2022).

[7] European Council. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union 2008;345:75–82. L.

[8] European Parliament and Council. Regulation (EC) No 725/2004 of the European Parliament and the Council of 31 March 2004 on enhancing ship and port facility security. Official Journal of the European Union 2004;129:6–91. L.

[9] European Commission. European Parliament and Council Directive 2012/18/EU of 4 July 2012 on control of major-accident hazards involving dangerous substances, amending and subsequently repealing council directive 96/82/EC. Official Journal of the European Communities 2012:1–37. L197.

[10] ANSI/API standard 780 - Security risk assessment methodology for the petroleum and petrochemical industries. Washington DC: American Petroleum Institute; 2013. American Petroleum Institute.

[11] Center for Chemical Process Safety. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. 2003.

[12] Garcia ML. Vulnerability Assessment of Physical Protection Systems. Burlington, MA: Butterworth-Heinemann; 2006.

[13] Matteini A, Argenti F, Salzano E, Cozzani V. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab Eng Syst Saf 2019;191:106083. https://doi.org/10.1016/j.ress.2018.03.001.

[14] Khan F, Rathnayaka S, Ahmed S. Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection 2015;98:116–47. https://doi.org/10.1016/j.psep.2015.07.005.

[15] Cox LA. Some limitations of "risk = threat x vulnerability x consequence" for risk analysis of terrorist attacks. Risk Analysis 2008;28:1749–61. https://doi.org/10.1111/j.1539-6924.2008.01142.x.

[16] Paté-Cornell E, Guikema S. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research 2002;7:5–23.

[17] Paté-Cornell E, Garber R, Guikema S, Kucik P, Bier VM, Azaiez MN. Games and risk analysis, three examples of single and alternate moves. Springer; 2009. https://doi.org/10.1007/978-0-387-87767-9. Game theoretic risk analysis of security threats.

[18] Argenti F, Landucci G, Reniers G, Cozzani V. Vulnerability assessment of chemical facilities to intentional attacks based on Bayesian Network. Reliab Eng Syst Saf 2018;169:515–30. https://doi.org/10.1016/j.ress.2017.09.023.

[19] Landucci G, Argenti F, Cozzani V, Reniers G. Assessment of attack likelihood to support security risk assessment studies for chemical facilities. Process Safety and Environmental Protection 2017;110:102–14. https://doi.org/10.1016/j.psep.2017.06.019.

[20] Misuri A, Khakzad N, Reniers G, Cozzani V. A Bayesian network methodology for optimal security management of critical infrastructures. Reliab Eng Syst Saf 2019;191. https://doi.org/10.1016/j.ress.2018.03.028.

[21] Feng Q, Cai H, Chen Z. Using game theory to optimize the allocation of defensive resources on a city scale to protect chemical facilities against multiple types of attackers. Reliab Eng Syst Saf 2019;191. https://doi.org/10.1016/j.ress.2017.07.003.

[22] Zhang Y, Weng WG. Bayesian network model for buried gas pipeline failure analysis caused by corrosion and external interference. Reliab Eng Syst Saf 2020;203. https://doi.org/10.1016/j.ress.2020.107089.

[23] Ding L, Khan F, Ji J. A novel vulnerability model considering synergistic effect of fire and overpressure in chemical processing facilities. Reliab Eng Syst Saf 2022;217. https://doi.org/10.1016/j.ress.2021.108081.

[24] Li X, Chen G, Amyotte P, Khan F, Alauddin M. Vulnerability assessment of storage tanks exposed to simultaneous fire and explosion hazards. Reliab Eng Syst Saf 2023;230:108960. https://doi.org/10.1016/j.ress.2022.108960.

[25] Chen C, Reniers G, Khakzad N. A dynamic multi-agent approach for modeling the evolution of multi-hazard accident scenarios in chemical plants. Reliab Eng Syst Saf 2021;207:107349. https://doi.org/10.1016/j.ress.2020.107349.

[26] Jiang D, Pan XH, Hua M, Mébarki A, Jiang JC. Assessment of tanks vulnerability and domino effect analysis in chemical storage plants. J Loss Prev Process Ind 2019;60:174–82. https://doi.org/10.1016/j.jlp.2019.04.016.

[27] George PG, Renjith VR. Bayesian estimation and consequence modelling of deliberately induced domino effects in process facilities. J Loss Prev Process Ind 2021;69:104340. https://doi.org/10.1016/j.jlp.2020.104340.

[28] Zeng T, Chen G, Yang Y, Chen P, Reniers G. Developing an advanced dynamic risk analysis method for fire-related domino effects. Process Safety and Environmental Protection 2020;134:149–60. https://doi.org/10.1016/j.psep.2019.11.029.

[29] Chen C, Khakzad N, Reniers G. Dynamic vulnerability assessment of process plants with respect to vapor cloud explosions. Reliab Eng Syst Saf 2020;200. https://doi.org/10.1016/j.ress.2020.106934.

[30] Mkrtchyan L, Straub U, Giachino M, Kocher T, Sansavini G. J Loss Prev Process Ind. J Loss Prev Process Ind, 74; 2022. https://doi.org/10.1016/J.JLP.2021.104673.

[31] Zhu R, Hu X, Bai Y, Li X. Risk analysis of terrorist attacks on LNG storage tanks at ports. Saf Sci 2021;137. https://doi.org/10.1016/J.SSCI.2021.105192.

[32] Dehkordi MK, Behnam B, Pirbalouti RG. Probabilistic fire risk analysis of process pipelines. J Loss Prev Process Ind 2022;80:104907. https://doi.org/10.1016/J.JLP.2022.104907.

[33] Tong Q, Gernay T. Resilience assessment of process industry facilities using dynamic Bayesian networks. Process Safety and Environmental Protection 2023;169:547–63. https://doi.org/10.1016/J.PSEP.2022.11.048.

[34] Aven T. A unified framework for risk and vulnerability analysis covering both safety and security. Reliab Eng Syst Saf 2007;92:745–54. https://doi.org/10.1016/j.ress.2006.03.008.

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

[36] Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis 2006;26:293–6. https://doi.org/10.1111/j.1539-6924.2006.00755.x.

[37] Landucci G, Khakzad N, Reniers G. Physical Security in the Process Industry, 148. Elsevier; 2020. https://doi.org/10.1016/C2017-0-00539-6.
[38] Garcia ML. The Design and Evaluation of Physical Protection Systems. 2nd ed. Burlington, MA: Butterworth-Heinemann; 2008.
[39] 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. https://doi.org/10.1016/j.ssci.2016.11.022.
[40] Singhal A, Kiremidjian AS. Method for Probabilistic Evaluation of Seismic Structural Damage. Journal of Structural Engineering 1996;122:1459–67. https://doi.org/10.1061/(ASCE)0733-9445(1996)122:12(1459).
[41] Lagomarsino S, Giovinazzi S. Macroseismic and mechanical models for the vulnerability and damage assessment of current buildings. Bulletin of Earthquake Engineering 2006;4:415–43. https://doi.org/10.1007/s10518-006-9024-z.
[42] Rota M, Penna A, Strobbia CL. Processing Italian damage data to derive typological fragility curves. Soil Dynamics and Earthquake Engineering 2008;28:933–47. https://doi.org/10.1016/j.soildyn.2007.10.010.
[43] Lanzano G, Salzano E, de Magistris FS, Fabbrocino G. Seismic vulnerability of natural gas pipelines. Reliab Eng Syst Saf 2013;117:73–80. https://doi.org/10.1016/J.RESS.2013.03.019.
[44] Argyroudis SA, Mitoulis SA. Vulnerability of bridges to individual and multiple hazards- floods and earthquakes. Reliab Eng Syst Saf 2021;210:107564. https://doi.org/10.1016/J.RESS.2021.107564.
[45] Zuluaga Mayorga S, Sánchez-Silva M, Ramírez Olivar OJ, Muñoz Giraldo F. Development of parametric fragility curves for storage tanks: A Natech approach. Reliab Eng Syst Saf 2019;189:1–10. https://doi.org/10.1016/j.ress.2019.04.008.
[46] Panteli M, Pickering C, Wilkinson S, Dawson R, Mancarella P. Power System Resilience to Extreme Weather: Fragility Modeling, Probabilistic Impact Assessment, and Adaptation Measures. IEEE Transactions on Power Systems 2017;32:3747–57. https://doi.org/10.1109/TPWRS.2016.2641463.
[47] Rossi L, Casson Moreno V, Landucci G. Vulnerability assessment of process pipelines affected by flood events. Reliab Eng Syst Saf 2022;219:108261. https://doi.org/10.1016/j.ress.2021.108261.
[48] Yang Y, Chen G, Reniers G. Vulnerability assessment of atmospheric storage tanks to floods based on logistic regression. Reliab Eng Syst Saf 2020;196. https://doi.org/10.1016/j.ress.2019.106721.
[49] Bernier C, Padgett JE. Fragility and risk assessment of aboveground storage tanks subjected to concurrent surge, wave, and wind loads. Reliab Eng Syst Saf 2019;191. https://doi.org/10.1016/j.ress.2019.106571.
[50] Muntasir Billah AHM, Shahria Alam M. Seismic fragility assessment of highway bridges: a state-of-the-art review. Structure and Infrastructure Engineering 2015;11:804–32. https://doi.org/10.1080/15732479.2014.912243.
[51] Landucci G, Gubinelli G, Antonioni G, Cozzani V. The assessment of the damage probability of storage tanks in domino events triggered by fire. Accid Anal Prev 2009;41:1206–15. https://doi.org/10.1016/j.aap.2008.05.006.
[52] Zhou J, Reniers G, Cozzani V. Improved probit models to assess equipment failure caused by domino effect accounting for dynamic and synergistic effects of multiple fires. Process Safety and Environmental Protection 2021;154:306–14. https://doi.org/10.1016/j.psep.2021.08.020.
[53] Cozzani V, Salzano E. The quantitative assessment of domino effects caused by overpressure: Part I. Probit models. J Hazard Mater 2004;107:67–80. https://doi.org/10.1016/j.jhazmat.2003.09.013.
[54] Mingguang Z, Juncheng J. An improved probit method for assessment of domino effect to chemical process equipment caused by overpressure. J Hazard Mater 2008;158:280–6. https://doi.org/10.1016/j.jhazmat.2008.01.076.
[55] Agresti A. An Introduction to Categorical Data Analysis. 3rd ed. John Wiley & Sons; 2018.
[56] Mannan S. Lees' Loss Prevention in the Process Industries. 3rd ed. Oxford, UK: Elsevier; 2005. https://doi.org/10.1016/B978-0-7506-7555-0.X5081-6.
[57] Cozzani V, Reniers G. Domino Effects in the Process Industries. Elsevier; 2013. https://doi.org/10.1016/C2011-0-00004-2.
[58] Tabandeh A, Asem P, Gardoni P. Physics-based probabilistic models: Integrating differential equations and observational data. Structural Safety 2020;87:101981. https://doi.org/10.1016/j.strusafe.2020.101981.
[59] Gardoni P, Der Kiureghian A, Mosalam KM. Probabilistic Capacity Models and Fragility Estimates for Reinforced Concrete Columns based on Experimental Observations. J Eng Mech 2002;128:1024–38. https://doi.org/10.1061/(ASCE)0733-9399(2002)128:10(1024).
[60] Gardoni P. Routledge Handbook of Sustainable and Resilient Infrastructure. 1st ed. Abingdon, Oxon ; New York, NY : Routledge, 2019. |: Routledge; 2018. https://doi.org/10.4324/9781315142074.
[61] Tugnoli A, Scarponi GE, Antonioni G, Cozzani V. Quantitative assessment of domino effect and escalation scenarios caused by fragment projection. Reliab Eng Syst Saf 2022;217:108059. https://doi.org/10.1016/j.ress.2021.108059.
[62] Iaiani M, Sorichetti R, Tugnoli A, Cozzani V. Projectile perforation models for the vulnerability assessment of atmospheric storage tanks. Process Safety and Environmental Protection 2022;161:231–46. https://doi.org/10.1016/j.psep.2022.03.025.
[63] Hottel HC, Sarofim AF. Radiative transfer. New York: McGraw-Hill; 1967.
[64] Miura H, Matsuo A, Tabuchi G. Numerical investigation for pressure mitigation effects of dike on blast wave. J Loss Prev Process Ind 2013;26:329–37. https://doi.org/10.1016/j.jlp.2011.05.013.
[65] Landucci G, Reniers G, Cozzani V, Salzano E. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliab Eng Syst Saf 2015;143:53–62. https://doi.org/10.1016/j.ress.2015.03.004.
[66] v Jensen F, TD Nielsen. Bayesian Networks and Decision Graphs. 2nd ed. New York, NY: Springer; 2007.
[67] GeNIe Modeler - BayesFusion, LLC 2022. https://www.bayesfusion.com/genie/(accessed February 28, 2022).
[68] International Organization for Standardization. ISO 31000:2018 Risk management - Guidelines 2018.
[69] Weinacht P, Cooper GR, Newell JF. Analytical Prediction of Trajectories for High-Velocity Direct-Fire Munitions. Aberdeen Proving Ground, MD 2005.
[70] Mayevski NV. Traité de balistique extérieure. Paris: Gauthier-Villars; 1872.
[71] Small Arms Survey. Research Note 2013;25:1–2. Military Assault Rifles.
[72] Small Arms Survey. Research Note 2014;38:1–2. Traditional Military Rifles.
[73] Weinacht P, Newill JF, Conroy PJ. Conceptual Design Approach for Small-Caliber Aeroballistics With Application to 5 . 56-mm Ammunition. Aberdeen Proving Ground 2005. MD.
[74] MagTech Ammunition. Homepage 2021. https://magtechammunition.com/(accessed December 10, 2021).
[75] Federal Ammunition. Homepage 2021. https://www.federalpremium.com/(accessed December 20, 2021).
[76] Remington. Homepage 2021 December 20, 2021. https://www.remington.com/(accessed.
[77] Sellier&Bellot. Homepage 2021. https://www.sellier-bellot.cz/en/(accessed December 20, 2021).
[78] Tula Ammo. Homepage 2021. http://tulammo.ru/en/(accessed December 20, 2021).
[79] Nammo. Homepage 2021. https://www.nammo.com/(accessed December 20, 2021).
[80] Stewart MG, Netherton MD. Statistical variability and fragility assessment of ballistic perforation of steel plates for 7.62 mm AP ammunition. Defence Technology 2020;16:503–13. https://doi.org/10.1016/j.dt.2019.10.013.
[81] Petroleum Institute American. API 650 Welded Steel Tanks for Oil Storage. Policy 2007;552.
[82] The American Society of Mechanical Engineers (ASME). New York, NY: The Americal Society of Mechanical Engineers; 2021. Boiler & Pressure Vessel Code.
[83] Rosenberg Z, Dekel E. Revisiting the perforation of ductile plates by sharp-nosed rigid projectiles. Int J Solids Struct 2010;47:3022–33. https://doi.org/10.1016/j.ijsolstr.2010.07.003.
[84] Kolaitis DI. An experimental investigation of improvised incendiary devices used in urban riots: The "Molotov cocktail. In: Fire Safety Science - Proceedings of the Second International Symposium; 2015.
[85] McNab C. The Flamethrower. Oxford: Osprey Publishing; 2015.
[86] Favarato LF, Souza JL, Guarçoni RC, Bahiense DV. Flamethrower Application Time in Weed Control. Planta Daninha 2016;34:327–32. https://doi.org/10.1590/S0100-83582016340200014.
[87] Kayll AJ. Use of Fire in Land Management. Fire and Ecosystems 1974:483–511. https://doi.org/10.1016/b978-0-12-424255-5.50019-5.
[88] Bradley I, Scarponi GE, Otremba F, Birk AM. An overview of test standards and regulations relevant to the fire testing of pressure vessels. Process Safety and Environmental Protection 2021;145:150–6. https://doi.org/10.1016/j.psep.2020.07.047.
[89] Landucci G, Molag M, Reinders J, Cozzani V. Experimental and analytical investigation of thermal coating effectiveness for 3 m3 LPG tanks engulfed by fire. J Hazard Mater 2009;161. https://doi.org/10.1016/j.jhazmat.2008.04.097.
[90] Shevlyakov GL, Oja H. Robust Correlation: Theory and Applications. John Wiley & Sons; 2016.
[91] Baker WE, Westine PS, Dodge FT. Similarity Methods in Engineering Dynamics: Theory and Practice of Scale Modeling. 1st ed. Amsterdam: Elsevier; 1991.
[92] Task Committee on Blast-Resistant Design of the Petrochemical Committee of the Energy Division of ASCE. Design of Blast-Resistant Buildings in Petrochemical Facilities. Reston, VA. 1997.
[93] Saltelli A, Ratto M, Andres T, Campolongo F, Cariboni J, Gatelli D, et al. Global Sensitivity Analysis. The Primer. Chichester, UK: John Wiley & Sons, Ltd; 2007. https://doi.org/10.1002/9780470725184.
[94] Pasman H, Rogers W. Bayesian networks make LOPA more effective, QRA more transparent and flexible, and thus safety more definable! J Loss Prev Process Ind 2013;26:434–42. https://doi.org/10.1016/j.jlp.2012.07.016.
[95] Khakzad N, Landucci G, Cozzani V, Reniers G, Pasman H. Cost-effective fire protection of chemical plants against domino effects. Reliab Eng Syst Saf 2018;169:412–21. https://doi.org/10.1016/j.ress.2017.09.007.
[96] DNV. DNV PHAST Homepage n.d. https://www.dnv.com/software/services/phast/index.html (accessed February 28, 2022).