Cost-benefit management of intentional domino effects in chemical industrial areas

Cost-Benefit Management of Intentional Domino Effects in Chemical Industrial Areas

Chao Chen[a], Genserik Reniers[a, b, c*], Nima Khakzad[a]

[a] Safety and Security Science Group, Faculty of Technology, Policy and Management, TU Delft, Delft, The Netherlands
[b] Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), University Antwerp, Antwerp, Belgium
[c] CEDON, KULeuven, Campus Brussels, Brussels, Belgium

[*] Corresponding author:

Email: g.l.l.m.e.reniers@tudelft.nl

Phone: +31 15 27 83749

Address: Jaffalaan 5, Delft 2628 BX, The Netherlands.

Abstract

Chemical industrial areas comprising various hazardous installations may be attacked by adversaries, triggering possible intentional domino effects. Compared with accidental domino effects, intentional domino effects may be more difficult to prevent since intelligent and strategic adversaries can adapt their tactics according to protection measures. However, how and to what extent domino effects affect security management is ignored in previous studies. This study proposes a methodology to prevent and mitigate intentional domino effects taking into consideration economic issues in the decision-making process on safety and security resources. The methodology is divided into five parts: threat analysis, vulnerability analysis of installations w.r.t. intentional attacks, vulnerability analysis of installations subject to possible domino effects caused by the attacks, cost-benefit analysis and optimization. Net present value of benefits (*NPVB*) is employed and quantified in the cost-benefit analysis to determine whether a protection strategy (a combination of safety and security measures) is profitable, or not. Besides, an optimization algorithm called "PROTOPT" based on "maximin" strategy is developed to achieve the most profitable protection strategy. An illustrated case study shows that domino effects can not be ignored in security management since they may have a profound impact on adversaries' strategies.

Keywords:

Intentional domino effects; Vulnerability assessment; Cost-benefit analysis; Dynamic graphs; Safety and security measures; Optimization

1. Introduction

Domino effects or so-called knock-on events in the process and chemical industries have received increasing attention in scientific and technical literature since the 1990s (Bagster and Pitblado, 1991). Domino effects can be triggered by either unintentional (safety-related) events (e.g., mechanical failure, human error, and natural disasters) or intentional (security-related) events (e.g., terrorist attacks). Public concern pay attention to domino effects caused by intentional attacks (security-related domino effects) since Reniers et al. (2008) proposed to deal with intentional domino effects in chemical clusters. Adversaries may execute an attack with the purpose of

triggering domino effects, inducing catastrophic events or indirectly damaging installations. Besides, intentional attacks might result in unplanned domino effects due to the interaction between the target installation and the nearby installations (Chen et al., 2019). Compared with domino effects caused by unintentional events, intentional domino effects may induce more severe consequences due to simultaneous damage of installations induced by multiple target attacks. For example, three tanks in a French chemical plant were attacked via explosive devices in July 2015, inducing two simultaneous tank fires (one damaged tank failed to be ignited) (BBC News, 2015). An overview of the definitions and characteristics of accidental domino effects and intentional domino effects is given in Table 1.

Table 1 Comparison of the definitions and main characteristics between accidental domino effects and chemical technology (incomplete enumeration)

Types	Accidental domino effects	Intentional domino effects
Definition	Domino effects triggered by unintentional events	Domino effects triggered by intentional events
Positions of primary events	Usually occurring at installations	Any positions within chemical plants or outside the area nearby
Sources of hazards	Hazardous materials in chemical installations and hazardous materials form loading and unloading vehicles	Hazardous materials in chemical installations, and external hazardous materials carried by attackers such as explosive devices
Main escalation vectors	Heat radiation, fire impingement, overpressure, and fragments	Heat radiation, fire impingement, overpressure, and fragments
Simultaneous primary scenarios	Usually involving a single installation	Multiple installations can be involved due to multiple target attacks
Protection measures	Safety barriers	Security countermeasures and safety barriers

In order to prevent or mitigate accidental and intentional domino effects, Reniers and Soudan (2010) recommended to set up an institution, the so-called Multi-Plant Council (MPC), in order to stimulate the prevention cooperation in a chemical industrial cluster. Reniers and Audenaert (2014) proposed to reduce the potential consequences of intentional domino effects based on vulnerability analysis, providing a systematic method to intelligently protect chemical industrial areas against intentional attacks. Landucci et al. (2015b) assessed the vulnerability of industrial installations subject to attacks by homemade explosives. The results indicated that domino effects can be triggered by explosion attacks only in the case that homemade explosives are positioned inside the facility or near to hazardous installations outside the industrial area. Zhou and Reniers (2016) studied the emergency strategies to multiple simultaneous fires caused by intentional attacks. Hosseinnia et al. (2018) established an emergency response decision matrix to determine the

emergency level of each company tackling terrorist attacks with improvised devices in chemical clusters. Khakzad and Reniers (2018) applied graph theory and dynamic Bayesian network to identify critical units and proposed a strategy whereby some of the storage tanks are made empty to mitigate intentional domino effects.

The economic issues of risk play an indispensable role in the decision-making process with respect to safety and security management since companies usually face budget limitations. Economics reminds us that protection resources are always limited and the resources allocated to one target are not available for others (Birk, 2014; Paltrinieri et al., 2012; Poole, 2008). Although economic issues of risk may only be one part of risk management, it has a great impact on the effectiveness of a company's prevention policy as well as the company's profitability in the long term (Reniers and Van Erp, 2016). Economic models, therefore, are usually used to optimize the allocation of protection resources so as to maximize the protection effectiveness, such as the prevention investment decision model based on cost-benefit analysis (Reniers and Sorensen, 2013; Villa et al., 2017) and the domino mitigation model in view of cost-effective analysis (Janssens et al., 2015; Khakzad et al., 2018). Besides the application in resource allocation, economic models of terrorism provided new insights into the motivation and strategy behind terrorist events from economic perspectives by analyzing the costs and benefits of terrorism (Blomberg et al., 2004; Brück, 2007).

However, there is a research gap between economic models and intentional domino effects due to the complexity and uncertainty of domino effect evolution as well as the fact that there are intelligent and strategic adversaries. This study aims to develop a methodology to employ economic models for preventing and mitigating intentional domino effects in chemical industrial areas. First, the methodology with five steps is elaborated in Section 2. Second, we expound on threat analysis to obtain the likelihood and possible attack scenarios in Section 3. After introducing the vulnerability assessment of installations against direct attacks, a dynamic graph approach for assessing the vulnerability of installations subject to intentional domino effects is provided in Section 4. Next, a cost-benefit analysis on the basis of threat and vulnerability analysis is elaborated in Section 5. Moreover, an optimization algorithm is developed in Section 5 in order to achieve the optimal cost-benefit protection strategy within budget constraints. A case study is provided in Section 6 while conclusions drawn from this work are presented in Section 7.

2. Methodology

The aim of the methodology is to obtain the most profitable protection strategy for tackling intentional domino effects in the process and chemical industries. Fig. 1 shows the steps of the methodology. The methodology for preventing and mitigating intentional domino effects consists of five parts: threat analysis, vulnerability assessment of installations directly against intentional attacks, vulnerability assessment of installations subject to possible domino effects induced by attacks, and cost-benefit analysis. Threats can be defined as the intention and capability of a threat to undertake actions that would be detrimental to valued assets. (API, 2013) The first step aims to determine the threat probability (the likelihood of the threat) and possible attack scenarios caused

by the threat. In terms of intentional domino effects, installations may be damaged by direct attacks or consequent domino effects. Therefore, steps 2 & 3 deal with the vulnerability of installations directly to intentional attacks and consequent domino effects respectively. The performance of safety measures and security barriers is also considered in the vulnerability assessment step. According to the results of threat analysis and vulnerability assessment, a cost-benefit analysis is conducted in step 4 to determine whether an integrated protection strategy (a combination of safety and security measures) is profitable, or not. Afterwards, the cost-benefit protection strategy is obtained through an optimization algorithm in step 5. The five steps will be elaborated hereafter.

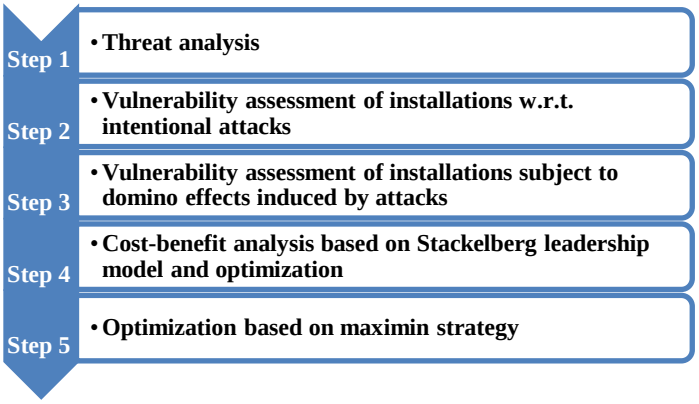


Fig.1 Procedures of the developed methodology.

3. Threat analysis

Threat analysis which provides the basic data (e.g., threat probabilities, possible attack scenarios) for vulnerability analysis, is needed to conduct an economic analysis for managing intentional domino effects. A threat can be regarded as an indication, a circumstance, or an event that possibly leads to losses of, or damage to, facilities (API, 2013). A large number of hazardous installations are mutually linked in terms of the hazard level they pose to each other due to possible domino effects. The first step of threat analysis is to collect information on possible threats, such as motivations, attack types, attack capability, and attack objectives. According to adversaries' motivations, domino effects caused by intentional attacks may be categorized into three types: (i) adversaries may execute an attack with the purpose of triggering domino effects, inducing catastrophic consequences; (ii) adversaries attack target installations resulting in unplanned domino effects; (iii) adversaries indirectly attack an object installation via domino effects. The objective of threat analysis for tackling intentional domino effects is, therefore, to identify possible scenarios caused by intentional attacks and to determine the threat probability.

Intentional attacks may result from internal adversaries, external adversaries or internal adversaries working in collusion with external adversaries. The adversaries encompass individuals, groups, organizations, or governments possibly executing these intentional events. So a threat analysis should consider as many adversaries as possible, such as intelligence services of host nations, or third-party nations, political and terrorist groups, criminals, rogue employees, cyber criminals, and

private interests (API, 2013). Besides, the capability and the resources of the attackers in terms of available information, instruments, and tools should be considered in the analysis. However, quantifying adversaries is a considerable challenge since it requires a multitude of data and knowledge, and modeling the motivations, intents, characteristics, capabilities, and tactics of adversaries (Baybutt, 2017; Paté-Cornell and Guikema, 2002). Expert judgment methods may be applied to determine the threat probability, P_T (the likelihood of the threat) based on available data and information. In this study, a five-level threat assessment method recommended by the American Petroleum Institution (API) is adopted, as shown in Table 2.

Table 2 SRA methodology for threat assessment, adapted from API (2013)

Threat level	Description
Very low	Indicates little or no credible evidence of capability or intent and no history of actual or planned threats against the asset or similar assets (e.g. "no expected attack in the life of the facility's operation").
Low	Indicates that there is a low threat against the asset or similar assets and that few known adversaries would pose a threat to the asset (e.g. "1 event or more is possible in the life of the facility's operation").
Medium	Indicates that there is a possible threat to the asset or similar assets based on the threat's desire to compromise similar assets, but no specific threat exists for the facility or asset (e.g. "1 event or more in 10 years of the facility's operation").
High	Indicates that a credible threat exists against the asset or similar assets based on knowledge of the threat's capability and intent to attack the asset or similar assets, and some indication exists of the threat specific to the company, facility, or asset (e.g. "1 event or more in 5 years of the facility's operation").
Very high	Indicates that a credible threat exists against the asset or similar assets; that the threat demonstrates the capability and intent to launch an attack; that the subject asset or similar assets are targeted or attacked on a frequently recurring basis; and that the frequency of an attack over the life of the asset is very high (e.g. "1 event/event per year").

In case of unacceptable high consequences caused by intentional domino effects or insufficient information and data available in order to implement the five-level threat assessment method, a conditional threat approach may be applied: assuming $P_T = 1$ (Mueller and Stewart, 2011; Villa et al., 2017). This conservative approach indicates that the potential consequences of possible intentional attacks are so severe that the threat likelihood assessment is not necessary. In that case, security management may focus on assessing the vulnerability of chemical installations, the potential consequences of intentional domino effects and the cost-benefit of protection measures.

4. Vulnerability assessment

Different from assessments of accidental domino effects, a vulnerability assessment for installations against intentional domino effects should consider (i) the vulnerability of installations against direct intentional attacks as well as (ii) the vulnerability of installations subject to possible domino effects caused by the attacks. To prevent and mitigate intentional domino effects, safety barriers and security measures may be integrated to reduce both the likelihood and consequences of these events.

4.1 Vulnerability assessment of installations against direct intentional attacks

The vulnerability of installations against direct intentional attacks can be regarded as any weakness that may be exploited by an attacker in order to gain access to direct targets and to successfully execute an attack (API, 2013). An intentional attack can be interrupted when the attack is detected and the guard communication to the response force is of success (Garcia, 2007). Therefore, the probability of a successful attack (P_S), indicating the likelihood that a target installation is directly damaged by the attack, can be expressed as follows:

$$P_S = P_T \cdot \left(1 - P_D \cdot P_C\right) \cdot P_E \tag{1}$$

where P_C is guard communication probability usually with a value of at least 0.95; P_D is detection probability; P_E is the probability that the attack is successfully executed. According to EASI model (Garcia, 2007), P_D depends on the attack path, detection measures along the path, and guard response time. If the needed time for an attacker to pass the segment between a detection position and the attack target is less than the guard response time, the detection measures should not be accounted for. In order to successfully interrupt intentional attacks, detection measures and delay measures should be arranged reasonably. Detection measures consist of fence sensors, door sensors, personnel, etc., and delay measures include fence fabric, door hardness, wall hardness, etc. To assess the damage probability of installations caused by direct attacks, it is required to quantify the detection probability of each detection measure and to calculate the delay time of each delay measures.

The factors that affect P_C include the training in the use of communication equipment, maintenance, dead sport in radio communication and the stress experienced during actual attacks (Garcia, 2007). The P_E depends on the capability and the resources of the attackers, which is relevant to available information, instruments, and tools. It was simplified as the product of the reliability of the available device (P_R) and the performance factor (P_P) of adversaries when using the device, as shown in Eq. (2). (Stewart and Mueller, 2012)

$$P_E = P_R \cdot P_A \tag{2}$$

With respect to explosion attacks launched by terrorist organizations, 4 types of explosive device complexity are defined (Table 3). The corresponding values of P_R and P_P are reported in Table 3.

Table 3 The values of P_R and P_P in terms of explosion attacks launched by terrorist organizations, adopted form (Stewart and Mueller, 2012; Villa et al., 2017).

Device complexity	Representative device	P_R	P_P
Simple	Pipe bomb	0.931	0.981
Medium	Mobile phone initiated VBIED*	0.920	0.980
Complex	Improvised mortar	0.910	0.905
No information available	Conservative assumption	1	1

*VBIED: Vehicle Borne Improvised Explosive Device

According to the above analysis, the possible primary hazardous scenarios initiating domino effects can be identified via cause-consequence analysis methods, such as what–if analysis and fault tree analysis (Chen and Reniers, 2018; Reniers et al., 2005). The primary hazardous scenario (H) can be expressed as a conditional probability of successful attacks, $P(H \mid S)$. Thus the probability of primary scenarios caused by intentional attacks is represented by Eq. (3).

$$P_H = P_S \cdot P(H \mid S) \tag{3}$$

The probability of primary hazardous scenarios (P_H) is deemed to be a prior probability to obtain the vulnerability of installations exposed to possible intentional domino effects in the considered chemical industrial area.

4.2 Vulnerability assessment of installations subject to domino effects

The main objective of vulnerability assessment for intentional domino effects is to determine the conditional damage probability of installations subject to possible domino effects caused by intentional attacks. A dynamic graph approach (Chen et al., 2019) is introduced to assess the vulnerability of installations exposed to possible intentional domino effects.

A chemical industrial area consists of various hazardous installations situated next to each. An intentional attack to one or more than one hazardous installation may trigger a chain of hazardous events, resulting in more severe consequences than that of the primary attack. These hazardous events may occur simultaneously or sequentially, so the evolution of domino effects may be a time-dependent or dynamic process. Therefore, a dynamic tool is more suitable for modeling the evolution of domino effects and to assess the vulnerability of installations subject to domino effects.

Dynamic graphs provide a mathematical tool for studying time-dependent interconnections among elements of a complex system. A dynamic graph model consists of a set of vertices (nodes), a set of edges (arcs), interconnection rules between each element, and the graph updating rules. Dynamic

graphs can be divided into two categories: undirected graphs and directed graphs. Directed graphs comprise ordered pairs of vertices where the edges between each pair of vertices have a direction associated with them. Dynamic graphs can be weighted when there are weights associated with nodes or edges. The weights may be real numbers, complex numbers, integers, etc (Bondy and Murty, 1976; Casteigts et al., 2012; Harary and Gupta, 1997). Graph updating is an operation that adds or removes nodes or edges, or changes weights of nodes and edges. Between each update, the graph can be regarded as a static graph. So a dynamic graph can be viewed as a discrete sequence of static graphs where each graph can be studied using static graph theory (Bondy and Murty, 1976; Casteigts et al., 2012; Harary and Gupta, 1997) .

A Domino Vulnerability Graph (DVG) is therefore defined as a directed dynamic graph, denoting installations' vulnerability w.r.t. domino effects caused by intentional events, as follows:

$$DVG = (I, E, f, q) \tag{4}$$

where I denotes a set of nodes denoting installations in a chemical industrial area. E represents a set of directed edges to model heat radiations among installations. f represents a group of node weights indicating the vulnerability or harmfulness of installations, including the state of installations, heat radiation, the residual time to failure, etc. q is an adjacent matrix denoting heat radiations among installations. An element q_{ij} of the matrix represents the heat radiation from a tail node i (an installation inducing the heat radiation) to a head node j (an installation received the heat radiation).

A DVG can be regarded as a chain of static graphs. The initial graph arises when a primary scenario caused by intentional attacks occurs. The DVG will update when a new installation catches fire or a fire extinguishes and ends when there is no escalation. The time to failure (*ttf*) is used to identify new fire while the time to burn out (*ttb*) is employed to determine the extinguished fire (Chen et al., 2018; Khakzad, 2015; Landucci et al., 2009). Several safety barriers are used to prevent or mitigate domino effects by delaying the *ttf*, such as water deluge systems and fireproof coatings. In general, water deluge systems can reduce 45% of the heat radiation while a 10 mm of fireproof coating is able to delay the *ttf* by at least 70 min (Landucci et al., 2015a). Fig. 2 is an illustrated DVG consisting of three static graphs.

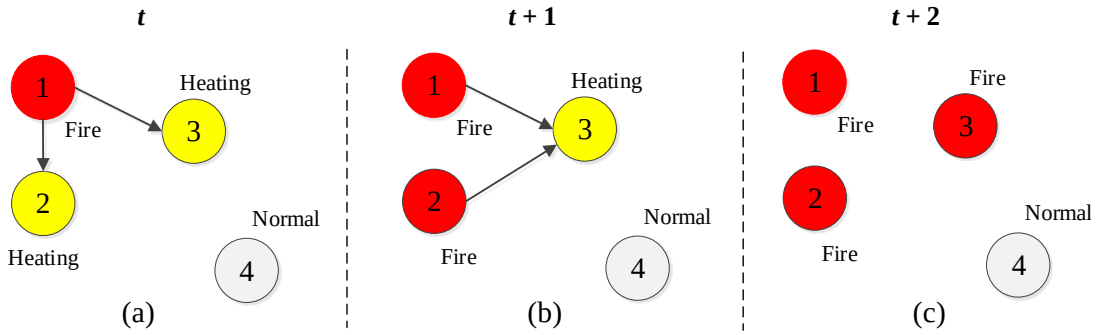


Fig. 2 A DVG with 4 tanks.

The DVG consists of three static graphs. The domino evolution starts at time *t* where a primary fire scenario is caused by an intentional attack to Tank 1 and it may continue until there is no escalation vector at time $t + 2$. Finally, 3 tanks are on fire while one tank survives. In other words, the domino effect can not escalate to tank 4. Besides, if any primary fire at tank 4 is not able to initiate domino effects, The chemical industrial area shown in Fig.2 can be divided into two domino islands[1] (Reniers and Audenaert, 2008) in terms of fire-induced domino effects. Taking into consideration the uncertainty of emergency response actions such as firefighting, the vulnerability of installations subject to possible intentional domino effects can be quickly obtained based on the graph updating principle of Minimum Evolution Time (MET)[2]. (Chen et al., 2018)

5. Cost-benefit analysis

5.1 Cost analysis

In order to be able to implement a protection strategy (a number of safety barriers and security measures) or to update existing protection systems, cost analysis of a protection strategy is indispensable since companies are always confronted with budget limitations. In this section, the various costs related to a protection strategy that a company may decide to implement are considered. The protection costs consist of investments that occur at present time such as initial costs and installation costs, and also the costs that occur throughout the remaining lifetime of the facility (Reniers and Brijs, 2014). In other words, cost analysis for a protection measure should include direct economic costs of applying the safety or security measures and indirect costs associated with their use. Eight cost categories of protection measures are listed in Table 4 for safety barriers (Reniers and Van Erp, 2016) and security measures.

Table 4 Categories of protection costs (Reniers and Van Erp, 2016; Villa et al., 2017).

Cost category	Subcategories
Initiation	Investigation, selection and design material, training, changing guidelines and informing
Installation	Production loss, start-up, equipment, installation team
Operation	Utilities consumption and labor Utilities
Maintenance	Material, maintenance team, production loss, start-up
Inspection	Inspection team
Logistics and transport	Transport and loading/unloading of hazardous materials, storage of hazardous materials, drafting control lists, relative documents
Contractor	Contractor selection, training
Other	Office furniture, insurance, and stationery items

[1] A chemical industrial area can be divided into one or more than one domino islands where where no domino effects can occur in between.

[2] The graph updating principle of MET considers the time interval between two updates as the minimum *ttf*s of tanks.

The present value of costs (PVC^n_j) caused by the implementation of the j-th safety or security measure in a protection strategy n is the sum of the initiation costs, installation cost, and the discounted present value of other six cost types, as follows:

$$PVC^n_j = C^n_{j,\text{ini}} + C^n_{j,\text{ins}} + \frac{(1+r)^y - 1}{r(1+r)^y}\left(C^n_{j,\text{ope}} + C^n_{j,\text{mai}} + C^n_{j,\text{ins}} + C^n_{j,\text{log}} + C^n_{j,\text{con}} + C^n_{j,\text{oth}}\right) \quad (5)$$

where $C^n_{j,\text{ini}}$ represents the initial costs of measure j, $C^n_{j,\text{ins}}$ concerns the installation costs of measure j, $C^n_{m,\text{ope}}$ equals the annual operation costs of measure j, $C^n_{j,\text{mai}}$ concerns the annual maintenance costs of measure j, $C^n_{j,\text{ins}}$ represents the annual inspection costs of measure m, $C^n_{j,\text{log}}$ equals the annual logistics and transport costs of measure m, $C^n_{j,\text{con}}$ equals the annual contractor costs of measure j, $C^n_{j,\text{oth}}$ represents the annual other costs of measure m, r is the discount rate, y is the minimum value of the number of years that the protection measure will operate and the remaining lifespan of the facility. For more information for the cost calculation of subcategories listed in Table 4, readers are kindly referred to Reniers and Van Erp (2016).

In terms of integrated protection strategy n, there may be multiple safety or security measures, so the total annual present value of costs due to the use of an integrated protection strategy can be expressed as follows:

$$PVC^n = \sum_{j=1}^{M} PVC^n_j \quad (6)$$

where PVC^n is the present value of cost with respect to protection strategy n, M is the total number of (safety and security) measures taken to prevent or mitigate intentional domino effects.

5.2 The overall expected loss of intentional domino effects

To analyze the overall expected loss, both the direct damage caused by intentional attacks and the damage resulting from subsequent domino effects should be considered. There may be multiple attack scenarios since the intelligent and strategic adversary may adapt to changing circumstances in terms of protection measures. Considering K attack scenarios may be present in a chemical industrial area, the overall expected losses caused by the k-th (k = 1, 2, 3, …, K) attack scenario under a protection strategy n can be simplified as the sum product of the installations' damage probabilities and their loss:

$$OL^k = \sum_{i=1}^{I} {}^{k}P_{D,i} \cdot L^k_i \quad (7)$$

$$P_{D,j}{}^{k} = \begin{cases} P^k_{DA,j} & (\text{installation } j \text{ is the direct target of attack scenario } k) \\ P^k_{DD,j} & (\text{installation } j \text{ is not direct target of attack scenario } k) \end{cases} \quad (8)$$

where $P^k_{D,i}$ is the damage probability of installation i in attack scenario k, $P^k_{DA,i}$ is the damage probability of direct target installation i in attack scenario k, representing the installation's vulnerability to direct attacks. $P^k_{DA,j}$ is the damage probability of non-target installation i in attack scenario k, representing the installation's vulnerability exposed to possible domino effects caused by the attack. Finally, L_j is the loss caused by damage to installation i.

The assessment of losses caused by intentional attacks should take into account economic loss, casualties, as well as any other influences such as psychological and political effects (Stewart and Mueller, 2011). Both the direct losses that are immediately visible and tangible and the indirect losses that are intangible and invisible are important to analyze avoided losses. (Jallon et al., 2011; Reniers and Van Erp, 2016) The direct avoided losses consist of these avoided losses caused by damage to installations, products, and equipment, medical expenses, paying fines and insurance premium rise while the indirect avoided losses include capacity losses, production schemes, recruitment and wage costs. (Gavious et al., 2009) The quantification of indirect losses is more difficult since they consist of hidden or invisible components, usually resulting in underestimation of the avoided losses. (Jallon et al., 2011) One simple method to estimate the indirect losses is using an indirect to direct loss ratio based on the assessment results of direct losses. The ratio varies in academic literature and this makes it induce difficult for users to choose a suitable ratio. For example, a widely used loss ratio of 4 is proposed based on an analysis of 7500 accidents while a range of 1 to 20 has been proposed on different industrial sectors and methods used. (Dorman, 2000) In the present study, we adopt the loss assessment method proposed by Reniers and Brijs (2014) to account for the losses of major accidents in chemical industrial areas and to address the losses related to intentional attacks, including reputation, symbolic, psychological and political effects. (Reniers and Van Erp, 2016) Therefore, the total loss caused by the damage of an installation i in scenario k can be estimated as a sum of eleven contributions, as follows:

$$L^k_i = L^k_{sup,i} + L^k_{dam,i} + L^k_{leg,i} + L^k_{ins,i} + L^k_{hum,i} + L^k_{env,i} + L^k_{per,i} + L^k_{med,i} + L^k_{int,i} + L^k_{inv,i} + L^k_{\mathrm{sec},i} \quad (9)$$

where $L^k_{sup,i}$ is the supply chain loss, $L^k_{dam,i}$ is the damage loss, $L^k_{leg,i}$ is the legal loss, $L^k_{ins,i}$ is the insurance loss, $L^k_{hum,i}$ is the human loss, $L^k_{env,i}$ is the environmental loss, $L^k_{per,i}$ is the personnel loss, $L^k_{med,i}$ is the medical loss, $L^k_{int,i}$ is the intervention loss, $L^k_{rep,i}$ is the reputation loss, $L^k_{inv,i}$ is the accident investigation and clean up loss, $L^k_{sec,i}$ is the security-related loss which is different from accidental losses. The avoided loss of each category can be calculated as the sum of the subcategories presented in Table 5.

Table 5 Categories of protection costs, adapted from (Reniers and Van Erp, 2016).

Cost category	Subcategories
Supply chain	Production, start-up, schedule
Damage	Damage to own material/property, other companies' material/property, surrounding living areas, public material/property
Legal	Fines, interim lawyers, specialized lawyers, internal research team, experts at hearings, legislation, permit, and license
Insurance	Insurance premium
Human	Compensation victims, injured employees, recruitment,
Environmental	Environmental damage and clean-up
Personnel	Productivity of personnel, training of new or temporary employees, wages
Medical	Medical treatment at location, medical treatment in hospitals and revalidation, using medical equipment and devices, medical transport
Intervention	The service from fire department, police department or ambulance
Investigation	Accident investigation
Security	Reputational, symbolic, psychological and political effects

5.3 Net benefits analysis

The benefits of an integrated protection strategy can be estimated by expressing the difference between expected losses of intentional domino accidents without and with the implementation of safety or security measure. In order to calculate the benefits of a protection strategy, a baseline ($k = 0$) should be defined. The baseline can be the strategy without any safety or security measures, or the initial strategy before protection upgrade. In that case, the benefits of a protection strategy n for a special attack scenario k can be defined as follows:

$$B^{n,k} = OL^{0,k} - OL^{n,k} \tag{10}$$

where $B^{n,k}$ is the benefit of protection strategy n for a special attack scenario k, $OL^{0,k}$ is the expected loss caused by attack scenario k under the protection of baseline strategy 0, $OL^{n,k}$ is the expected loss caused by attack scenario k under the protection of strategy n. Different from natural or accidental threats, adversaries with bad intention may adapt to the changing circumstances caused by a protection strategy to maximize their malevolent inspired benefits. According to the Stackelberg leadership model (Kroshl et al., 2015; Pita et al., 2009), the defender can be considered as the 'leader' (on the first step moves, taking the prior decision on protection) while the attacker is viewed as the 'follower' who knows the protection strategy before launching an attack. A

reasonable assumption is that the attacker is a benefit maximizer aiming to maximize the damage. In terms of a protection strategy *n*, the attacker would adapt to the protection by selecting an attack scenario *k* maximizing $OL^{n,k}$. In other words, the benefit of a protection strategy *n* should be represented by the attack scenario which causes the minimal expected benefit:

$$B^n = \min_k B^{n,k} \tag{11}$$

where B^n is the expected benefit of protection strategy *n*. In that case, the net present value of benefits (*NPVB*) of protection strategy *n* ($NPVB^n$) can be defined as the difference of the protection benefit and the protection cost of strategy *n*, as follows:

$$NPVB^n = \frac{(1+r)^y - 1}{r(1+r)^y} B^n - PVC^n \tag{12}$$

A protection strategy *n* is usually recommended if the annual net benefit exceeds a threshold (e.g., $NPVB > 0$), otherwise, it is considered to be not cost-effective or inefficient. (Reniers and Van Erp, 2016; Stewart and Mueller, 2013) Given $NPVB = 0$, the minimal threat probability (P^*) or risk reduction ($\triangle R$) needed for a special protection strategy *n* to be cost-benefit can be obtained by 'break-even' analysis. (Stewart and Mueller, 2014) Therefore, the *NPVB* can be regarded as a robust index for decision-making on protection strategies, addressing the intelligent and strategic actions of adversaries and the uncertainty in domino effect evolution.

5.4 Optimization

According to the cost-benefit analysis a protection strategy is recommended if the so-called net present value of benefits (*NPVB*) is greater than a threshold. However, companies usually face budget limitations and are expected to maximize the *NPVB* when it comes to decision-making on protection investments. This section thus aims to find out the most profitable protection strategy under budget limitations.

The allocation of safety or security resources in chemical industrial areas can be tackled according to the so-called "Knapsack problem", well-known in the field of Operations Research. (Reniers and Sorensen, 2013; Villa et al., 2017) In terms of intentional domino effects, a chemical industrial area with large quantities of hazardous installations may be regarded as an interdependent system. A non-linear optimization model can be obtained as follows:

$$\begin{cases} \max\limits_n NPVB^n \\ C_n \le C_{\text{Budget}} \\ n = 1, 2, \ldots, N \end{cases} \tag{13}$$

Eq. (13) indicates that *NPVB* of possible protection strategies should be maximized within the

constraint of available protection budget C_{Budget}. The monetary cost of a protection strategy n should then obviously not exceed C_{Budget}.

To simplify the problem, a robust optimization based on "maximin" strategy called "PROTOPT" for PROTection OPTimization, is proposed to sequentially allocate safety and security measures, maximizing a chemical plant's worst-case payoff (i.e., maximizing the minimum *NPVB*). The algorithm is shown in Fig. 3.

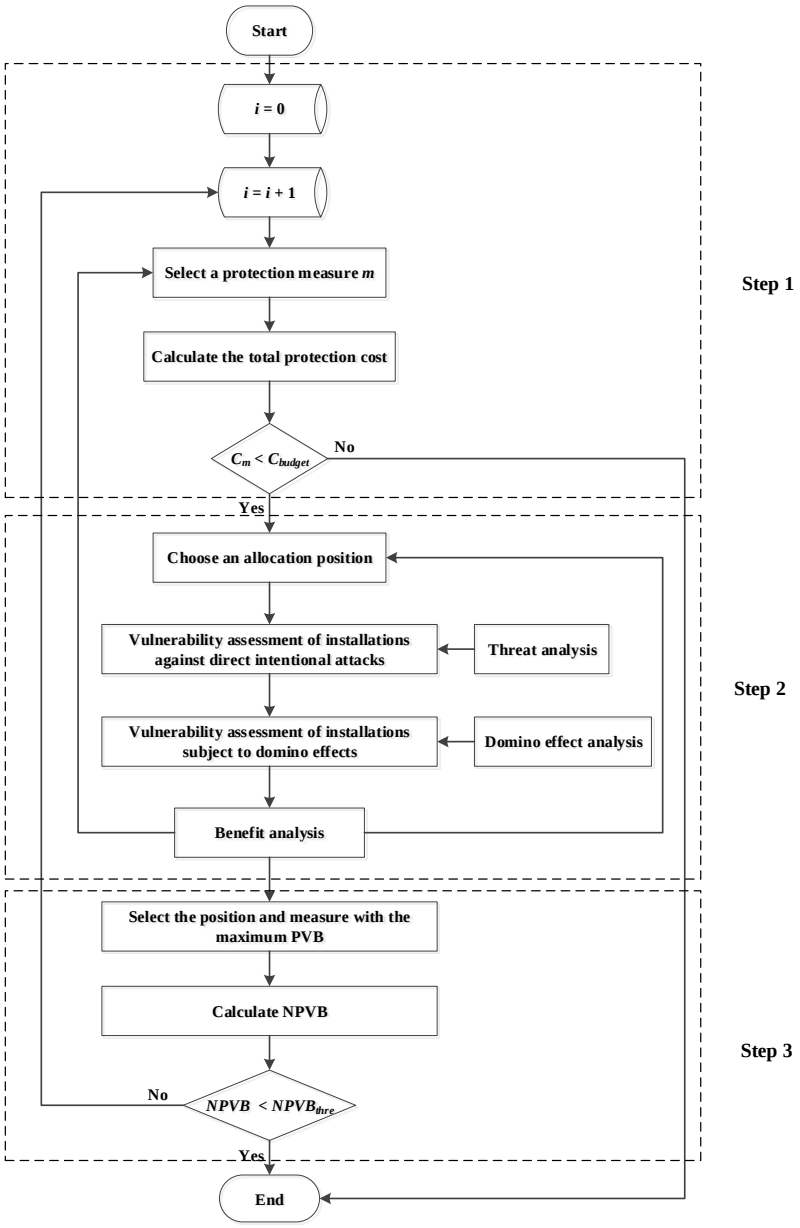


Fig. 3 The "PROTOPT" algorithm for cost-benefit optimization based on maximin strategy to achieve an optimal protection strategy.

As shown in Fig.3, the PROTOPT algorithm consists of three steps: cost analysis, benefit analysis and optimization. The algorithm will end when the *NPVB* is lower than the threshold of *NPVB* ($NPVB_{thre}$). The *NPVB* can be considered to be zero, which means that only profitable protection strategies should be recommended. Besides, $NPVB_{thre}$ can be calculated using a Disproportionate Factor (DF) which is a threshold value to determine whether the protection measure is grossly disproportional or not. (Talarico and Reniers, 2016) Applying this optimization algorithm, we can not only obtain the optimal protection strategy under an available protection budget but also obtain a recommended protection cost and relevant protection strategy to maximize the protection *NPVB* when there is no budget restriction.

6. An illustrative example

6.1 Case study

To demonstrate the application of the proposed methodology in tackling intentional domino effects using safety barriers and security measures, consider a petrochemical plant in Berre L'Etang, France, as shown in Fig. 4. The chemical industrial area was attacked in 2015, resulting in two tank fires, environmental pollution, yet no casualties. (BBC News, 2015)

Fig. 4 The layout of a chemical storage plant.

The petrochemical plant considered in this case covers an area of around 720,000 m², consisting of 32 gasoline storage tanks (T1-T34) and 6 dismissed tanks (T35-T40). The characteristics of the three types of gasoline storage tanks (small, middle and large tanks) considered in Fig. 4 are summarized in Table 6.

Table 6 Characteristics of petrochemical storage tanks

Tank	Type	Dimension $D \times H$ (m)	Chemical substance	Nominal Volume (m^3)	Chemical content (m^3)	Symbol
T1-T15	Atmospheric	42×7.2	Gasoline	9975	8000	Small
T16-T30	Atmospheric	48×7.2	Gasoline	11966	10000	Middle
T30-T34	Atmospheric	60×5.4	Gasoline	15268	13000	Large

These tanks are surrounded by tank dikes and each dike contains one or two tanks. To detect any abnormal events of tanks, cameras are installed in the dikes (E1~E19 as shown in Fig. 4), considering a detection probability of 0.9 for each camera. The west side of the plant concern other chemical facilities and loading and unloading zones are located in the North part of the plant. The curve marked in white in Fig. 4 is the simple wired perimeter fence on the eastern and northern boundaries of the plant.

6.2 Results and discussion

6.2.1 The threat to the chemical plant

According to the procedures of the methodology, we should firstly analyze possible threats. Since the chemical plant was maliciously attacked in 2015, consider an external adversary with the purpose of sabotaging tanks (setting fires), trying to maximize the company's loss. Besides, the threat level is regarded as high and the threat likelihood P_T is equal to 0.2 according to Table 2. The possible adversary may cut the simple wired fence at a special site (I1~I9), run into one tank dike (E1-E20) and attack one tank or two tanks sequentially in the dike. As a result, the possible 48 attack scenarios considered in this case study are shown in Fig.5. As shown in Fig.5, there are 34 attack scenarios with a single target and 14 attack scenario with two targets.

6.2.2 The Vulnerability of tanks against intentional attacks

The second step is to carry out a vulnerability assessment of installations against direct attacks. According to the procedures and paths of the possible attack scenarios presented in Fig. 5, the needed time to get through each path section for different attack scenarios can be calculated. A standard running speed of 3 m/s is assumed during the attack process of adversaries without any load (Villa et al., 2017). Since the adversaries may take some weapons or equipment, speed reduction factors of 0.5 and 0.75 are given to attacks with weapons to two targets and a single target respectively. In that case, the mean delay time during running in each path section of different

attacks can be obtained. A mean delayed time of 10 s is assumed to cut the fence and the mean delayed time to get to the dike (due to the height of the wall) is considered as 30 s.

The detection probability of cameras after entering a tank dike is equal to 0.9. The probability of response communication is 0.95 and the mean response force time equals 5 min. To deal with the uncertainty of delay-related time and response-related time, a standard deviation of 30% of the mean value is assumed according to the conservative assumption based on the normal distribution. (Garcia, 2007) Both ($P(H|S)$) and (P_E) are equal to 1. In that case, a single target attack scenario may result in one tank fire or no tank fire while a multiple-target attack can result in one tank fire, two tank fires or no tank fire. The likelihoods of possible primary hazardous scenarios caused by these attacks are listed in Table. 7.

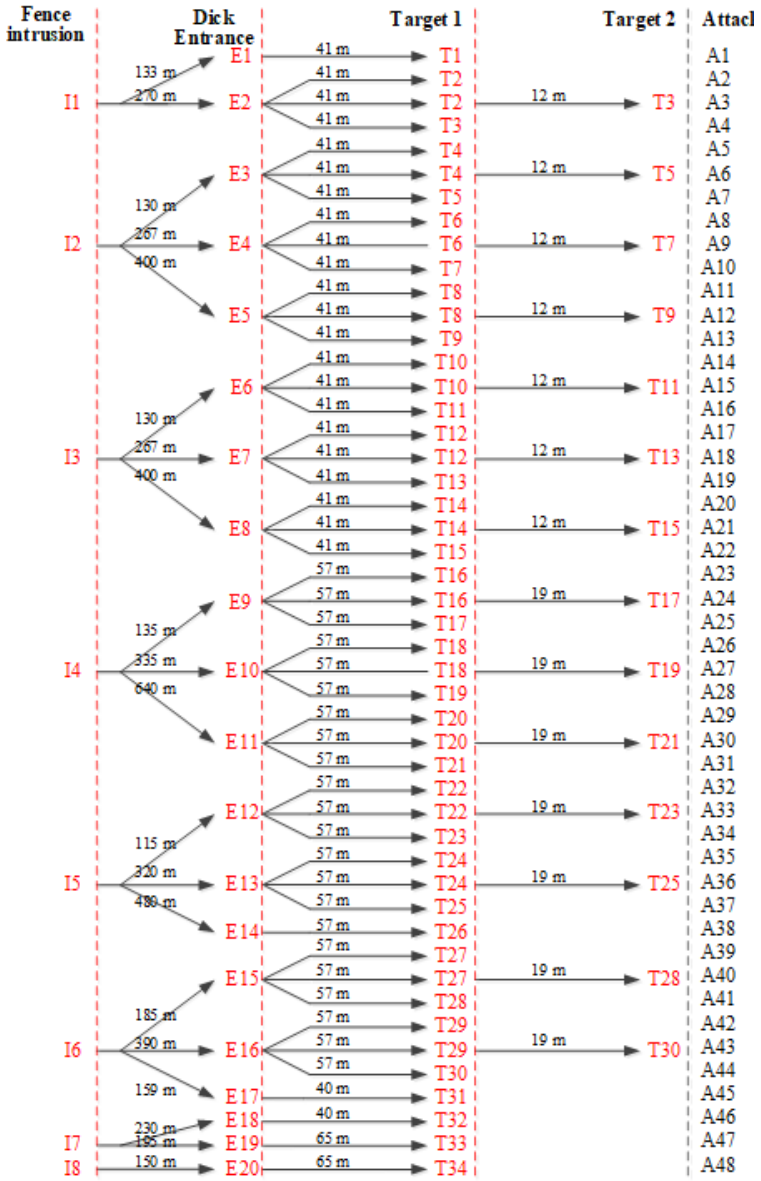


Fig. 5 The possible attack scenarios considered in this case study.

Table 7 Primary hazardous scenarios caused by different attack scenarios

Attacks	Hazardous scenarios	Conditional probability	Attacks	Hazardous scenarios	Conditional probability
A1	T1 on fire	0.959	A24	T16 & T17 on fire	0.624
A2	T2 on fire	0.959	A25	T17 on fire	0.953
A3	T2 on fire	0.295	A26	T18 on fire	0.953
	T2 & T3 on fire	0.669	A27	T18 on fire	0.333
A4	T3 on fire	0.959		T18 & T19 on fire	0.624
A5	T4 on fire	0.959	A28	T19 on fire	0.953
A6	T4 on fire	0.295	A29	T20 on fire	0.953
	T4 & T5 on fire	0.669	A30	T20 on fire	0.333
A7	T5 on fire	0.959		T20 & T21 on fire	0.624
A8	T6 on fire	0.959	A31	T21 on fire	0.953
A9	T6 on fire	0.295	A32	T22 on fire	0.953
	T6 & T7 on fire	0.669	A33	T22 on fire	0.333
A10	T7 on fire	0.959		T22 & T23 on fire	0.624
A11	T8 on fire	0.959	A34	T23 on fire	0.953
A12	T8 on fire	0.295	A35	T24 on fire	0.953
	T8 & T9 on fire	0.669	A36	T24 on fire	0.333
A13	T9 on fire	0.959		T24 & T25 on fire	0.624
A14	T10 on fire	0.959	A37	T25 on fire	0.953
A15	T10 on fire	0.295	A38	T26 on fire	0.953
	T10 & T11 on fire	0.669	A39	T27 on fire	0.953
A16	T11 on fire	0.959	A40	T27 on fire	0.333
A17	T12 on fire	0.959		T27 & T28 on fire	0.624
A18	T12 on fire	0.295	A41	T28 on fire	0.953
	T12 & T13 on fire	0.669	A42	T29 on fire	0.953
A19	T13 on fire	0.959	A43	T29 on fire	0.333
A20	T14 on fire	0.959		T29 & T30 on fire	0.624
A21	T14 on fire	0.295	A44	T30 on fire	0.953
	T14 & T15 on fire	0.669	A45	T31 on fire	0.959
A22	T15 on fire	0.959	A46	T32 on fire	0.959
A23	T16 on fire	0.953	A47	T33 on fire	0.949
A24	T16 on fire	0.333	A48	T44 on fire	0.949

As shown in Table 7, single-target attacks would result in one primary hazardous scenario while two-target attacks may result in two scenarios: the fire at the first target and the fires at both targets. Although the path distances between different single attacks are different, the tank fire probabilities caused by these attacks are the same or have small differences since the distance difference before reaching the detection measures (i.e., cameras) is meaningless according to Garcia (2007) For example, the tank fire probabilities of attack 1 and attack 2 are identical although the path of attack 2 is longer than the path of attack 1 (as shown in Fig.5). Besides, the probabilities of primary

hazardous scenarios are quite high which indicate that the effectiveness of the baseline security system is poor. The cameras should be installed near the start point of attacks so as to provide enough time for response communication and response force actions.

6.2.3 The results of domino effect analysis

The identical probabilities do not mean that the expected consequences of different attacks are not different because each tank may have a different potential to initiate domino effects. This is why the vulnerability of installations to possible domino effects caused by these primary hazardous scenarios should be assessed. According to the vulnerability assessment method presented in Section 4.2, we firstly obtain the potential heat radiation q_{ij} between each pair of tanks if tank i is on fire, as shown in the Appendix (Table A1). The potential evolution path, evolution time and installation damage probability due to domino effects caused by different primary hazardous scenarios can be obtained using the dynamic graph model. The analysis shows that T26, T33, and T34 can not initiate domino effects if they are attacked. In addition, the chemical industrial area can be divided into five domino islands where any primary hazardous event within the area can not escalate outside the area, as shown in Fig. 6.

Fig. 6 Five domino islands within the chemical plant.

A domino island can be analyzed independently since no escalation vector links with installations outside the area. The domino effect risk decreases with increasing the number of domino islands. The installation damage sequences caused by 48 possible primary hazardous scenarios are listed in Appendix (Table A2). The results of the domino effect analysis demonstrate that the attack on tanks in island 1 can lead to a more severe disaster (the damage of 24 tanks).

6.2.4 Protection strategies

The results of threat analysis and vulnerability assessment show that the plant is susceptible to intentional attacks, and the attack may lead to catastrophic consequences due to possible domino effects. As a result, additional safety and security measures might be proposed to protect the plant against intentional attacks. Assuming the protection budget is €2.5M, six protection upgrades are proposed, including three security strategy (PS1-PS3), one safety strategy (PS4), and two integrated protection strategies (PS5, PS6), as follows:

PS1) install fence sensors on the perimeter;

PS2) updating the perimeter delay measure by building a concrete reinforced external wall;

PS3) reducing response force time by building an additional guard dispatch;

PS4) applying fireproof coating on all storage tanks;

PS5) adding fence sensors on the perimeter and building an additional guard dispatch;

PS6) adding fence sensors on the perimeter and applying fireproof coating on critical tanks.

6.2.5 Cost analysis (Step 1 of the PROTOPT algorithm)

The cost calculation for each of the six protection strategies proposed in the previous section is carried out according to the cost categories and cost calculation method described in Section 5.1. The remaining lifespan of all the protection measures *y* is considered as 10 years and the discount factor for cost calculation is 0.035 (HSE, 2016). The conversion rate from USD to EUR is 0.888 based on the real exchange rate (wisselkoers, 2019). Fence sensor units used in PS1 are installed every 10m along the 5750 m perimeter (Villa et al., 2017). The concrete reinforced wall proposed in PS2 is 2.65 m high, 0.098m thick and 5750 m long. The initial costs of a concrete reinforced wall consist of concrete cost, forms cost, and reinforced steel costs, the costs of labor and equipment used in construction are considered in installation costs while the operation costs are ignored (Craftsman, 2018). The costs of PS3 are mainly from a new building and additional guards. To calculate the operation costs caused by additional guards, the average salary of €23/h and 8760 working hours/year are adopted (Explorer, 2019). A 10 mm fireproof coating is recommended in PS4 for all the tanks to make sure a delayed failure time of 70 min is present (Khakzad et al., 2018; Paltrinieri et al., 2012). The sum of initial costs and installation costs of the fireproof coating is €24/mm/m^2. The final proposal only applies fireproof coating on the top six critical tanks (T6, T7, T11, T12, T23, T24) based on the vulnerability of the tanks subject to domino effects. More cost details are shown in appendix (Table A3). The final cost calculation results are represented as the present value of costs (PVC) in Table 8.

Table 8 Cost calculation results

Protection strategies	Description	Performance	*PVC* (€)
PS1	575 fence sensors along 5750 m perimeter	Detection probability at the perimeter is 0.9	4.7×10^5
PS2	A concrete reinforced external wall (2.65m × 0.098m ×5750 m)	Delayed time at the perimeter is 180s	2.9×10^5
PS3	A new building with several guards near the chemical plant	Response time is reduced to 150s	1.8×10^6
PS4	10 mm fireproof coating for each storage tank with a	Delayed time of tank damage is 70min.	1.1×10^6
PS5	PS1+PS3	PS1+PS3	2.3×10^6
PS6	PS1+PS4	PS1+PS3	$\leqslant 2.5\times10^6$

As shown in Table 8, PS2 and PS4 should be excluded since the PVCs of building a concrete reinforced external wall and fireproof coating of all the tanks exceed the protection budget. The rest of the protection strategies should furtherly be assessed via a benefit analysis.

7.2.6 Benefit analysis of protection strategies (Step 2 of the PROTOPT algorithm)

The overall expected losses should be evaluated according to adversaries' attack strategies, protection strategies and the vulnerability of installations. Different from the consequence assessment of general security events, the loss assessment of intentional domino effects is a rather complex task since many scenarios with multiple contemporary events may take place. To simplify the calculation, a catastrophic case scenario where all the tanks are damaged with 30 fatalities and 3000 injuries is defined. (Reniers and Van Erp, 2016) Besides, assuming that the different categories of costs are proportional to the damage of the tanks, the losses of different domino scenarios can be obtained according to the catastrophic case scenario.

The supply chain losses are estimated by considering the storage profit, i.e., €0.58/(barrel · month) (Reuters, 2015). The supply chain losses caused by tank damage are considered to be the storage profit of the tank per year. In the calculation of damage losses, both the tank damage and the loss of gasoline in the tank are taken into consideration. Considering the loss of €711 k, €800 k and €933 k for the small-, middle- and large-sized tanks respectively, (Matches, 2014) the loss of gasoline can be represented by the product of the volume and the price of gasoline €1.45/L (GlobalPetrolPrices, 2019). The fines-related costs in legal losses are considered as €251.3 K if all tanks are damaged, referring to a previous accident in France (Reniers and Van Erp, 2016).

In order to calculate the costs of human life, the value of a statistic life (VSL) of €5.8 M (Birk, 2014) and the value of a statistical injury of €31 K (Kuhn and Ruf, 2013) are adopted for case study.

The insurance costs of €5 M, reputation costs of €384 M and intervention costs of €30 K for the worst case scenario are retrieved from a previous study (AFP, 2012). The environment costs, personnel costs, medical costs, investigation and clean-up costs are also estimated based on the above figures. As a result, the losses of the catastrophic case scenario and the expected losses related to the attacks are obtained, as displayed in Table 9.

Table 9 The losses of the worst case scenario and the expected losses from other possible attacks

Cost category	Losses related to the worst case scenario (€/year)	The expected losses from other possible attacks (€/year)
Supply chain	1.2×10^{6}	7.6×10^{5}
Damage	5.9×10^{8}	3.3×10^{6}
Legal	2.5×10^{5}	1.4×10^{4}
Insurance	5.0×10^{6}	2.8×10^{5}
Human	2.7×10^{8}	1.5×10^{7}
Environmental	1.2×10^{8}	6.6×10^{6}
Personnel	2.3×10^{5}	1.3×10^{4}
Medical	5.3×10^{7}	3.0×10^{6}
Intervention	3.0×10^{4}	1.7×10^{3}
Investigation	5.4×10^{6}	3.0×10^{5}
Security	3.8×10^{8}	2.1×10^{7}
In total	1.4×10^{9}	8.0×10^{7}

The expected attack scenario concerns a multiple-objective attack on T6 and T7, maximizing the losses of the plants. Therefore, the expected losses can be regarded as a baseline loss for decision-making on protection strategies. Table 10 lists the predicted attack scenarios and the corresponding benefits of each protection strategy.

Table 10 The net present value of benefits (*NPVB*) of each proposal protection strategy over a 10-year time-span.

Protection strategies	Attack scenarios	PVB (€)	NPVB (€)
PS1	S9: T6 & T7	3.2×10^{8}	3.2×10^{8}
PS2	S9: T6 & T7	0	-2.9×10^{6}
PS3	S9: T6 & T7	2.9×10^{8}	2.9×10^{8}
PS4	S24: T16 & T17	5.5×10^{8}	5.4×10^{8}
PS5	S9: T6 & T7	5.3×10^{8}	5.3×10^{8}
PS6	S45: T31	4.4×10^{8}	4.4×10^{8}

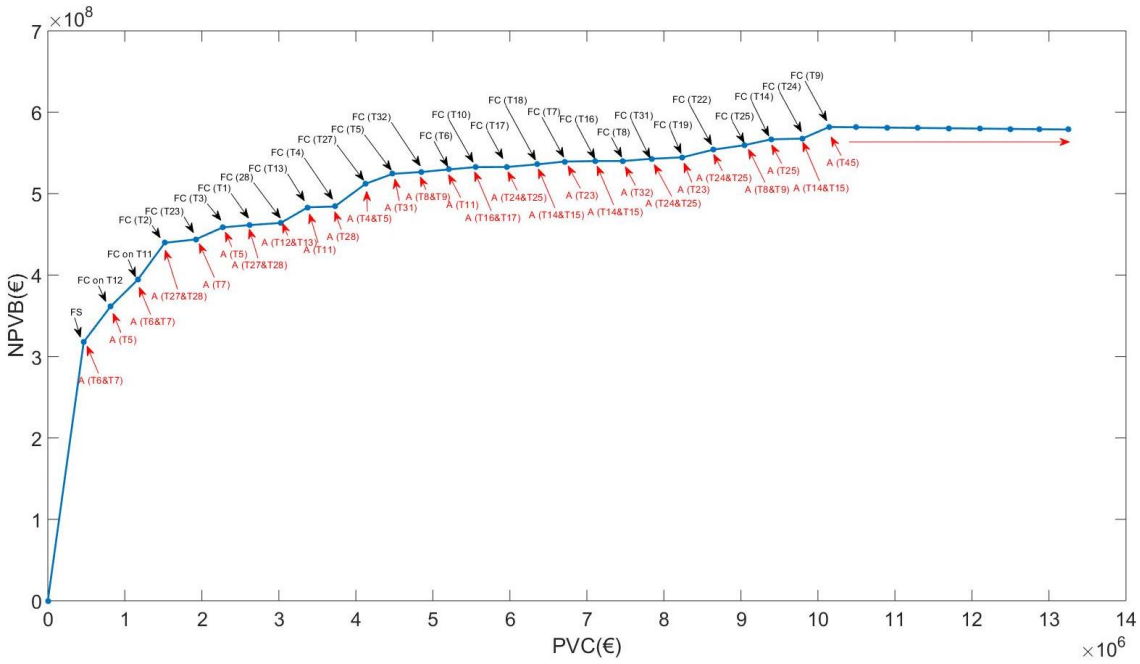
As shown in Table 10, all the proposals are recommended except PS2 (*NPVB*<0). PS4 has the largest hypothetical benefit but its cost exceeds the protection budget. The results of domino effect analysis using dynamic graphs demonstrate that domino effects are impossible due to the use of fireproof coatings on all the tanks. In other words, the expected loss with the baseline security system will be €14 M per year rather than €80 M per/year if we do not consider domino effects. Besides, the attack strategy will be S9 but not S24. Therefore, neglecting domino effects in security management may underestimate the loss of attacks and lead to unreasonable allocation of protection measures, resulting in large losses. Domino effect analysis is inevitable in chemical security management.

6.2.7 Optimization (Step 3 of the PROTOPT algorithm)

Both the results of cost analysis (Table 10) and benefit analysis (Table 12) show that PS2 is not advisable since *NPVB*<0 and *PVC*> C_{Budget}. Although PS2 is much more expensive than the other proposals, it has no effect on the chemical plant's security. Domino effect analysis demonstrates that PS4 can effectively prevent the escalation of all 48 primary scenarios while the cost of PS4 is much higher than the available budget of €2.5 M. As a result, PS2 and PS4 can not be recommended. Installing a fence sensor (PS1) can provide a faster response force, largely reducing the likelihood of successful attacks. Since it is a border security strategy, the attacker's strategy can be assumed to be unchanged. PS3 also reduces the likelihood of success of all 48 attacks by shortening the needed time for response. Therefore, the combination of PS1 and PS3 becomes the optimal cost-benefit strategy under the available budget of €2.5 M.

Besides PS5, PS6 is a cost-benefit strategy combining a detection measure and a safety barrier. To reduce the cost of fireproof coatings, only part of the tanks, those more vulnerable to domino effects, can be protected. The optimization algorithm proposed in Section 5 is used to obtain the number and position of the tanks where the fireproof coating should be installed. Fig. 7 shows the optimization results of PS6 based on a maximin strategy. The adversary's attack strategies vary with increasing the present value of costs (*PVC*). First, *NPVB* increases from 0 to € 318 M due to the installation of fence sensors on the plant perimeter. Next, fireproof coatings are sequentially installed on T12, T11, T2, T23, and T3. As a result, *NPVB* furtherly increases by € 141M while PVC increases to € 2.27 M. If more tanks are protected using fireproof coatings, *PVC* will excess the protection budget of 2.5M and the increase ratio of *NPVB* decreases gradually. After applying fireproof coatings on T9, the likelihood of domino effects becomes impossible and further investment in the fireproof coating will be unprofitable. These results demonstrate that the investment in protection measures follows the law of diminishing returns[3]. (Anderson and Mittal, 2000)

[3] In economics, diminishing returns indicates the decrease in marginal output (impact) from increasing one unit of input factor, while the amounts of all other input factors stay constant.



*The blue curve shows the *NPVB* (net present value of benefits) with increasing of *PVC* (present value of costs). The black text arrows denote the new protection measures while the red text arrows represent attack scenarios corresponding to different protection investments (FS: fence sensor; FC: fireproof coating; A: attack).

Fig. 7 The optimization results of PS6.

This case study shows that we can obtain the most cost-effective protection strategy applying the developed EPID. However, various chemical plants are located in different places and face different threats. As a result, the likelihood of threats is different for each chemical plant, which may have an important impact on the profitability of protection investments. Taking PS5 as an example, Fig. 8 shows the NPVB values with different threat probabilities.

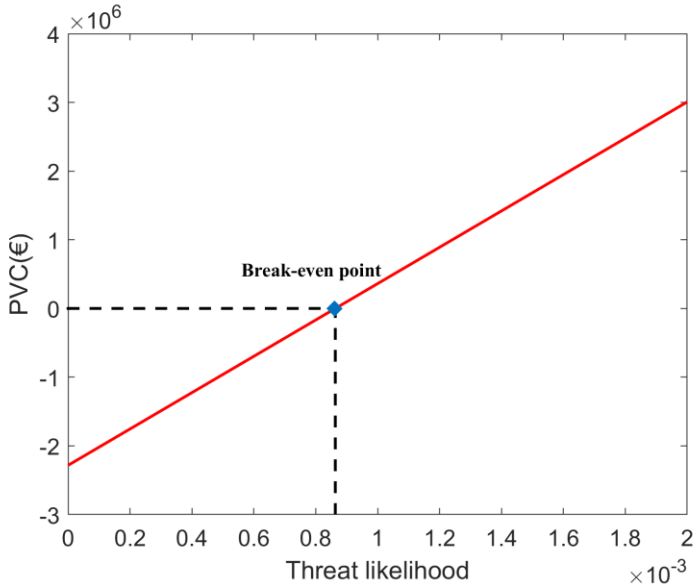


Fig. 8 *NPVB* values with different threat probabilities

Fig.8 indicates that *NPVB* is proportional to the threat likelihood. The threat probability at the break-even point (P^*) is 0. 86×10^{-3}, which means that the protection is profitable only when the threat likelihood $P_T > 0.86\times10^{-3}$. However, the results do not mean that the protection is not recommended when $P_T < 0.86\times10^{-3}$. In that case, cost-benefit indicators or disproportion factor analysis may be used to facilitate the decision making on the prevention of intentional domino effects.

7. Conclusions

The effectiveness of prevention strategy policies has a great impact on a company's profitability in the long term. This study therefore established a methodology for cost-benefit management of intentional domino effects in chemical industrial areas. The methodology considered hazardous installations' vulnerabilities to intentional attacks and subsequent possible domino effects. According to the Stackelberg leadership model, the defender was considered as the "leader" while the attacker was viewed as the "follower" who knows the protection strategy before launching an attack. As a result, the net present value of benefits (*NPVB*) is obtained to identify recommended protection strategies. Finally, an optimization algorithm (PROTOPT) based on the "maximin" strategy was developed to obtain the optimal protection strategy.

The results obtained from the application of the methodology to a case study demonstrated that domino effects have a great impact on the payoffs and strategies of adversaries, and should therefore not be neglected in chemical security management; multiple kinds of protection measures are recommended in chemical industrial areas since they follow the law of diminishing returns. The likelihood of threats plays a critical role in a protection strategy's profitability, so the optimal protection strategy varies from a chemical industrial area to the other.

In brief, the optimal protection strategy (including the types, quantities and position of protection measures) can be obtained using the developed methodology and PROTOPT algorithm, addressing the technical and financial issues in safety and security resources. However, further research is required to integrate intentional and accidental domino effects to improve safety and security management in chemical industrial areas.

References

AFP, 2012. Total Subsidiary Ex-boss Jailed for Deadly French Blast.
Anderson, E.W., Mittal, V., 2000. Strengthening the satisfaction-profit chain. Journal of Service research 3, 107-120.
API, 2013. ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry. American Petroleum Institute.
Bagster, D.F., Pitblado, R.M., 1991. The Estimation of Domino Incident Frequencies—An Approach. Process Safety & Environmental Protection 69, 195-199.

Baybutt, P., 2017. Issues for security risk assessment in the process industries. Journal of Loss Prevention in the Process Industries 49, 509-518.
BBC News, 2015. France explosions: Devices found near Berre-L'Etang plant.
Birk, A.M., 2014. Cost-effective application of thermal protection on LPG road transport tanks for risk reduction due to hot BLEVE incidents. Risk Anal 34, 1139-1148.
Blomberg, S.B., Hess, G.D., Weerapana, A., 2004. An economic model of terrorism. Conflict Management and Peace Science 21, 17-28.
Bondy, J.A., Murty, U.S.R., 1976. Graph theory with applications. Citeseer.
Brück, T., 2007. The economic analysis of terrorism. Routledge.
Casteigts, A., Flocchini, P., Quattrociocchi, W., Santoro, N., 2012. Time-varying graphs and dynamic networks. International Journal of Parallel, Emergent and Distributed Systems 27, 387-408.
Chen, C., Reniers, G., 2018. Risk Assessment of Processes and Products in Industrial Biotechnology, Adv Biochem Eng Biotechnol.
Chen, C., Reniers, G., Khakzad, N., 2019. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach. Reliability Engineering and System Safety.
Chen, C., Reniers, G., Zhang, L., 2018. An innovative methodology for quickly modeling the spatial-temporal evolution of domino accidents triggered by fire. Journal of Loss Prevention in the Process Industries 54, 312-324.
Craftsman, 2018. 2018 National Concrete and Masonry Estimator, 2018 ed. Craftsman.
Dorman, P., 2000. The economics of safety, health, and well-being at work: an overview. ILO Geneva.
Explorer, S., 2019. Average Salary in France 2019, February 2016 ed.
Garcia, M.L., 2007. Design and evaluation of physical protection systems. Elsevier.
Gavious, A., Mizrahi, S., Shani, Y., Minchuk, Y., 2009. The costs of industrial accidents for the organization: developing methods and tools for evaluation and cost–benefit analysis of investment in safety. Journal of Loss Prevention in the Process Industries 22, 434-438.
GlobalPetrolPrices, 2019. France Gasoline prices, liter.
Harary, F., Gupta, G., 1997. Dynamic graph models. Mathematical and Computer Modelling 25, 79-87.
Hosseinnia, B., Khakzad, N., Reniers, G., 2018. An emergency response decision matrix against terrorist attacks with improvised device in chemical clusters. International Journal of Safety and Security Engineering 8, 187-199.
HSE, 2016. Internal guidance on cost benefit analysis (CBA) in support of safety-related investment decisions, February 2016 ed.
Jallon, R., Imbeau, D., de Marcellis-Warin, N., 2011. Development of an indirect-cost calculation model suitable for workplace use. J Safety Res 42, 149-164.
Janssens, J., Talarico, L., Reniers, G., Sörensen, K., 2015. A decision model to allocate protective safety barriers and mitigate domino effects. Reliability Engineering & System Safety 143, 44-52.
Khakzad, N., 2015. Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. Reliability Engineering & System Safety 138, 263-272.
Khakzad, N., Landucci, G., Cozzani, V., Reniers, G., Pasman, H., 2018. Cost-effective fire protection of chemical plants against domino effects. Reliability Engineering & System Safety 169, 412-421.

Khakzad, N., Reniers, G., 2018. Low-capacity utilization of process plants: A cost-robust approach to tackle man-made domino effects. Reliability Engineering & System Safety.
Kroshl, W.M., Sarkani, S., Mazzuchi, T.A., 2015. Efficient Allocation of Resources for Defense of Spatially Distributed Networks Using Agent-Based Simulation. Risk Anal 35, 1690-1705.
Kuhn, A., Ruf, O., 2013. The Value of a Statistical Injury: New Evidence from the Swiss Labor Market. Swiss Journal of Economics and Statistics (SJES) 149, 57-86.
Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015a. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliability Engineering & System Safety 143, 30-43.
Landucci, G., Gubinelli, G., Antonioni, G., Cozzani, V., 2009. The assessment of the damage probability of storage tanks in domino events triggered by fire. Accid Anal Prev 41, 1206-1215.
Landucci, G., Reniers, G., Cozzani, V., Salzano, E., 2015b. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliability Engineering & System Safety 143, 53-62.
Matches, 2014. Tank Cost Estimate.
Mueller, J., Stewart, M.G., 2011. Terror, security, and money: Balancing the risks, benefits, and costs of homeland security. Oxford University Press.
Paltrinieri, N., Bonvicini, S., Spadoni, G., Cozzani, V., 2012. Cost-benefit analysis of passive fire protections in road LPG transportation. Risk Anal 32, 200-219; discussion 220-203.
Paté-Cornell, E., Guikema, S., 2002. Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. Military Operations Research 7, 5-23.
Pita, J., Jain, M., Ordóñez, F., Tambe, M., Kraus, S., Magori-Cohen, R., 2009. Effective solutions for real-world stackelberg games: When agents must deal with human uncertainties, Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems-Volume 1. International Foundation for Autonomous Agents and Multiagent Systems, pp. 369-376.
Poole, R.W., 2008. Toward risk-based aviation security policy. OECD/ITF Joint Transport Research Centre Discussion Paper.
Reniers, G., Brijs, T., 2014. Major accident management in the process industry: An expert tool called CESMA for intelligent allocation of prevention investments. Process Safety and Environmental Protection 92, 779-788.
Reniers, G., Dullaert, W., Audenaert, A., Ale, B.J., Soudan, K., 2008. Managing domino effect-related security of industrial areas. Journal of Loss Prevention in the Process Industries 21, 336-343.
Reniers, G., Soudan, K., 2010. A game-theoretical approach for reciprocal security-related prevention investment decisions. Reliability Engineering & System Safety 95, 1-9.
Reniers, G.L., Sorensen, K., 2013. An approach for optimal allocation of safety resources: using the knapsack problem to take aggregated cost-efficient preventive measures. Risk Anal 33, 2056-2067.
Reniers, G.L., Van Erp, H.N., 2016. Operational safety economics: a practical approach focused on the chemical and process industries. John Wiley & Sons.

Reniers, G.L.L., Audenaert, A., 2008. Preventing intentional disasters by investigating the security of chemical industrial areas. Disaster Advances 1, 14-19.
Reniers, G.L.L., Audenaert, A., 2014. Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Safety and Environmental Protection 92, 583-589.
Reniers, G.L.L., Dullaert, W., Ale, B.J.M., Soudan, K., 2005. Developing an external domino accident prevention framework: Hazwim. Journal of Loss Prevention in the Process Industries 18, 127-138.
Reuters, 2015. CORRECTED-COLUMN-Oil storage business is booming: Kemp.
Stewart, M.G., Mueller, J., 2011. Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. Journal of Homeland Security and Emergency Management 8.
Stewart, M.G., Mueller, J., 2012. Terror, security, and money: balancing the risks, benefits, and costs of critical infrastructure protection, pp. 513-533.
Stewart, M.G., Mueller, J., 2013. Terrorism risks and cost-benefit analysis of aviation security. Risk Anal 33, 893-908.
Stewart, M.G., Mueller, J., 2014. A risk and cost–benefit analysis of police counter-terrorism operations at Australian airports. Journal of Policing, Intelligence and Counter Terrorism 9, 98-116.
Talarico, L., Reniers, G., 2016. Risk-informed decision making of safety investments by using the disproportion factor. Process Safety and Environmental Protection 100, 117-130.
Villa, V., Reniers, G.L.L., Paltrinieri, N., Cozzani, V., 2017. Development of an economic model for counter terrorism measures in the process-industry. Journal of Loss Prevention in the Process Industries 49, 437-460.
wisselkoers, 2019. Exchange rate.
Zhou, J., Reniers, G., 2016. Petri-net based simulation analysis for emergency response to multiple simultaneous large-scale fires. Journal of Loss Prevention in the Process Industries 40, 554-562.

Appendix

Table A1 The Heat Radiation q_{ij} between each pair of tanks in kW/m^2. Values lower than 10 kW/m2 are excluded (-).

Tank	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
1	-	14.2	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
2	14.2	-	27.9	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
3	-	27.9	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
4	-	-	-	-	27.9	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
5	11.4	-	-	27.9	-	14.2	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
6	-	11.4	-	-	14.2	-	27.9	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7	-	-	11.4	-	-	27.9	-	14.2	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	14.2	-	27.9	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	27.9	-	-	-	-	-	-	11.4	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
10	-	-	-	11.4	-	-	-	-	-	-	27.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
11	-	-	-	-	11.4	-	-	-	-	27.9	-	14.2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	11.4	-	-	-	-	14.2	-	27.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
13	-	-	-	-	-	-	11.4	-	-	-	-	27.9	-	14.2	-	-	-	-	-	10.0	-	-	-	-	-	-	-	-	-	-	-	-	-	-
14	-	-	-	-	-	-	-	11.4	-	-	-	-	14.2	-	27.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15	-	-	-	-	-	-	-	-	11.4	-	-	-	-	27.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
17	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
18	-	-	-	-	-	-	-	-	-	10.9	11.6	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
19	-	-	-	-	-	-	-	-	-	-	10.9	10.3	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
20	-	-	-	-	-	-	-	-	-	-	-	-	10	10.3	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-	-
21	-	-	-	-	-	-	-	-	-	-	-	-	-	10.9	10.9	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-	-	-
22	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-
23	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-	-	-
24	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-
25	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-	-	-	-
26	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
27	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-
28	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-	-	-
29	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-
30	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	25.9	-	-	-	-	-
31	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	11	-	-	-	-	10.5	-	-
32	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	10.5	-	-	-
33	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
34	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Table A2 The evolution path of domino effects caused by different primary hazardous scenarios.

Primary scenarios	Domino evolution path																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
T1 on fire	T1	T2	T5	T3	T6	T4	T7	T11	T12	T8	T10	T13	T14	T9	T15	T19	T18	T20	T21	T24	T21	T26	T29	T30
T2 on fire	T2	T3	T1	T6	T7	T5	T4	T8	T12	T13	T11	T9	T14	T10	T15	T19	T20	T18	T21	T24	T25	T26	T29	T30
T3 on fire	T3	T2	T7	T6	T1	T5	T8	T4	T12	T13	T11	T9	T14	T10	T15	T19	T20	T18	T21	T24	T25	T26	T29	T30
T4 on fire	T4	T5	T1	T11	T6	T10	T12	T7	T2	T13	T3	T19	T18	T8	T14	T9	T15	T20	T21	T24	T25	T26	T29	T30
T5 on fire	T5	T4	T6	T1	T11	T10	T7	T12	T2	T3	T13	T8	T19	T18	T14	T9	T15	T20	T21	T24	T25	T26	T29	T30
T6 on fire	T6	T7	T5	T2	T12	T3	T13	T8	T1	T11	T4	T14	T9	T10	T15	T19	T20	T18	T21	T24	T25	T26	T29	T30
T7 on fire	T7	T6	T8	T3	T13	T2	T12	T5	T9	T14	T1	T11	T15	T4	T10	T20	T21	T19	T18	T26	T25	T24	T29	T30
T8 on fire	T8	T9	T7	T14	T15	T13	T6	T12	T3	T2	T5	T21	T11	T20	T1	T4	T10	T19	T18	T26	T25	T24	T29	T30
T9 on fire	T9	T8	T15	T14	T7	T13	T6	T12	T3	T21	T20	T2	T5	T11	T1	T4	T10	T19	T18	T26	T25	T24	T29	T30
T10 on fire	T10	T11	T4	T5	T12	T18	T19	T6	T13	T7	T1	T2	T3	T14	T8	T24	T25	T20	T15	T9	T21	T26	T29	T30
T11 on fire	T11	T10	T12	T5	T4	T19	T18	T13	T6	T7	T1	T2	T14	T8	T3	T20	T15	T24	T25	T9	T21	T26	T29	T30
T12 on fire	T12	T13	T11	T6	T7	T14	T10	T5	T8	T4	T15	T20	T19	T2	T3	T9	T1	T18	T21	T24	T25	T26	T29	T30
T13 on fire	T13	T12	T14	T7	T6	T11	T20	T15	T8	T5	T9	T21	T10	T3	T2	T4	T19	T1	T18	T26	T25	T24	T29	T30
T14 on fire	T14	T15	T13	T8	T9	T7	T12	T21	T20	T6	T3	T11	T5	T2	T19	T4	T10	T1	T26	T18	T25	T24	T29	T30
T15 on fire	T15	T14	T9	T8	T13	T21	T7	T20	T12	T6	T3	T11	T5	T2	T19	T4	T1	T10	T26	T18	T25	T24	T29	T30
T16 on fire	T16	T17	T23	T22	T27	T28	T31	T32	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T17 on fire	T17	T16	T23	T22	T27	T28	T31	T32	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T18 on fire	T18	T11	T19	T10	T12	T13	T5	T4	T6	T7	T25	T24	T14	T1	T20	T8	T2	T3	T15	T9	T21	T29	T30	T26
T19 on fire	T19	T18	T11	T10	T12	T13	T25	T24	T5	T6	T4	T7	T14	T20	T8	T1	T2	T15	T3	T9	T21	T29	T30	T26
T20 on fire	T20	T21	T14	T13	T15	T12	T26	T8	T7	T9	T6	T11	T5	T3	T19	T2	T10	T4	T18	T1	T25	T24	T29	T30
T21 on fire	T21	T20	T14	T15	T13	T12	T26	T8	T9	T7	T6	T11	T5	T3	T19	T2	T10	T4	T18	T1	T25	T24	T29	T30
T22 on fire	T22	T23	T27	T28	T16	T17	T31	T32	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T23 on fire	T23	T22	T27	T28	T16	T17	T31	T32	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T24 on fire	T24	T25	T29	T30	T18	T19	T11	T10	T12	T13	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T9	T21	T26
T25 on fire	T25	T24	T29	T30	T18	T19	T11	T10	T12	T13	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T9	T21	T26
T26 on fire	T26	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T27 on fire	T27	T28	T31	T22	T23	T32	T16	T17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T28 on fire	T28	T27	T31	T22	T23	T32	T16	T17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T29 on fire	T29	T30	T24	T25	T18	T19	T11	T10	T12	T13	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T9	T21	T26

T30 on fire	T30	T29	T24	T25	T18	T19	T11	T10	T12	T13	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T9	T21	T26
T31 on fire	T31	T32	T27	T28	T22	T23	T16	T17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T32 on fire	T32	T31	T27	T28	T22	T23	T16	T17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T33 on fire	T33	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T34 on fire	T34	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T2&T3 on fire	T2	T3	T6	T7	T1	T5	T8	T4	T12	T13	T11	T9	T14	T10	T15	T19	T20	T18	T21	T24	T25	T26	T29	T30
T4&T5 on fire	T4	T5	T1	T11	T6	T10	T12	T7	T2	T3	T13	T19	T18	T8	T14	T9	T15	T20	T21	T24	T25	T26	T29	T30
T6&T7 on fire	T6	T7	T2	T3	T12	T5	T8	T13	T1	T11	T14	T4	T9	T15	T10	T20	T19	T21	T18	T26	T25	T24	T29	T30
T8&T9 on fire	T8	T9	T14	T15	T7	T13	T6	T12	T3	T21	T2	T20	T5	T11	T1	T4	T10	T19	T18	T26	T25	T24	T29	T30
T10&T11 on fire	T10	T11	T4	T12	T18	T19	T5	T13	T6	T7	T1	T2	T14	T3	T8	T24	T25	T20	T15	T9	T21	T26	T29	T30
T12&T13 on fire	T12	T13	T7	T14	T11	T6	T8	T5	T20	T15	T10	T9	T4	T3	T2	T19	T21	T1	T18	T26	T25	T24	T29	T30
T14&T15 on fire	T14	T15	T8	T9	T13	T21	T20	T7	T12	T6	T3	T11	T5	T2	T19	T4	T10	T26	T1	T18	T25	T24	T29	T30
T16&T17 on fire	T16	T17	T23	T22	T27	T28	T31	T32	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0	T0
T18&T19 on fire	T18	T19	T11	T10	T12	T13	T24	T25	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T29	T30	T9	T21	T26
T20&T21 on fire	T20	T21	T14	T15	T13	T26	T12	T8	T9	T7	T6	T11	T5	T3	T19	T2	T10	T4	T18	T1	T25	T24	T29	T30
T22&T23 on fire	T22	T23	T27	T28	T16	T17	T31	T32	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T24&T25 on fire	T24	T25	T29	T30	T18	T19	T11	T10	T12	T13	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T9	T21	T26
T27&T28 on fire	T27	T28	T31	T22	T23	T32	T16	T17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
T29&T30 on fire	T29	T30	T24	T25	T18	T19	T11	T10	T12	T13	T5	T4	T6	T7	T14	T20	T8	T1	T2	T3	T15	T9	T21	T26

Table A3 The costs of different protection strategies.

Cost categories	PS1	PS2	PS3	PS4	PS5	PS6
Initial costs (€)	118000	786220	52900	7371872	170900	1552009
Installation costs (€)	162000	1114463	39000		201000	
Annual operating costs (€/Year)	4170	0	201480	0	205650	4170
Annual maintenance costs (€/Year)	8400	57020	2757	221156	11157	46560
Annual inspection costs (€/Year)	5600	38014	1838	147437	7438	31040
Annual logistics and transport costs (€/Year)	2800	19007	919	73719	3719	15520
Annual other costs (€/Year)	1400	9503	460	36859	1860	7760
Present value of costs (€)	466042	2928151	1817208	11356951	2283250	2425673