Integrating safety and security resources to protect chemical industrial parks from man-made domino effects

A dynamic graph approach

Chen, Chao; Reniers, Genserik; Khakzad, Nima

DOI
10.1016/j.ress.2019.04.023

Publication date
2019

Document Version
Final published version

Published in
Reliability Engineering and System Safety

Reliability Engineering and System Safety 191 (2019) 106470

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: A dynamic graph approach

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

ARTICLE INFO

Keywords:
Security risk management
Domino effects
Security measures
Safety barriers
Dynamic graphs

ABSTRACT

Chemical industrial parks, being critical infrastructures, are susceptible to domino effects triggered by intentional attacks. Previous research on security risk management has mainly focused on using security measures to prevent intentional attacks, neglecting the effects of safety barriers. Safety barriers are able to reduce the potential consequences and decrease the attractiveness of chemical industrial parks to terrorists who aim to maximize the damage. From a systematic perspective, the potential consequence of intentional attacks is defined as the expected loss which is the sum-product of damage probability and consequence of installations. A consequence-based method including a Dynamic Vulnerability Assessment Graph (DVAG) model is proposed to integrate safety and security resources for reducing the risk of intentional attacks. The DVAG model is developed based on dynamic graphs, considering the effects of security measures, safety barriers, and emergency response. This method can assess the consequences and damage probabilities of possible intentional attacks so as to mitigate the risk via evaluation and allocation of security measures and safety barriers with fast computation speed.

1. Introduction

Critical infrastructures are sensitive to disruptions that may lead to cascading failures since they are complex, interdependent, and ubiquitous [7,15]. Even a minor disruption can trigger a chain of events and cause performance degradation of infrastructure systems, resulting in substantial consequences [14]. The protection of critical infrastructures from system collapses with cascading effects is significant and challenging in counter-terrorism [25]. Hausken and Levitin [30] divided infrastructure systems into eight categories: single element, series systems, parallel systems, series-parallel systems, networks, multiple elements, interdependent systems, and other types of systems. Hausken and Levitin [29] used minmax strategy to allocate defensive resources in complex multi-state systems. Mirzasoleiman et al. [43] investigated the cascaded failures in weighted networks to assess the networks' robustness against cascaded failures. Chen et al. [18] studied the influence of coupling effect on the cascading failures in interdependent networks under targeted attacks and found that cascading failure mechanisms are different with various coupling preferences. Wu et al. [60] proposed an attack strength degradation model to analyze the cascading failures caused by terrorist attacks in interdependent infrastructures, considering physical and geographical interdependencies.

The chemical sector is identified as one of 16 critical infrastructures by the U.S. Department of Homeland Security [51]. A growing public concern raised the attention on chemical and process security after the terrorist attack in New York City on September 11, 2001 [9,10,12,39,50]. In 2004, the American Petroleum Institute (API) published a recommendation on security risk assessment for the petroleum and petrochemical industries [6]. The recommendation provides a systematic security risk assessment (SRA) method based on threat, vulnerability and consequence analysis. In 2013, the SRA method was improved by expanding functional utility without changing the basic methodology [5]. Security risk (R_s) is regarded as a function of threat (T), vulnerability (V) and consequence (C) in the SRA method, as shown in Eq. (1).

$$R_S = f_S(T, V, C) \tag{1}$$

Threat analysis, especially for quantification of the threat, is a considerable challenge since it requires a multitude of data and knowledge, and modeling the motivations, intents, characteristics, capabilities, and tactics of adversaries [11,46]. Vulnerability analysis requires a detailed understanding of the design and operation of installations and the threat information [42,44,55]. Security measures can improve the capability of installations against attacks but also may change the attackers' strategies because of the intelligent character of

* Corresponding author at: Jaffalaan 5, Delft 2628 BX, the Netherlands.
E-mail addresses: g.l.l.m.e.reniers@tudelft.nl, genserik.reniers@ua.ac.be (G. Reniers).

https://doi.org/10.1016/j.ress.2019.04.023
Received 10 August 2018; Received in revised form 8 November 2018; Accepted 17 April 2019
Available online 18 April 2019
0951-8320/

the adversaries [21,22,47]. Game theory has been suggested as a promising tool to analyze adversaries' strategies and optimize the defenders' response via optimal allocation of security resources [40,52,54,56,58]. Consequence analysis requires modeling the potential scenarios related to the attack, such as fires, explosions, and toxic material releases [59].

The above researches on security risk in the process and chemical industries mainly focus on threat and vulnerability analysis for the purpose of preventing possible intentional attacks or reducing the likelihood of these attacks. Little attention has been paid to reduce consequences since consequence analysis in the security domain has many similarities with that in the safety domain. But consequence analysis has important impacts on the attractiveness of chemical parks and thus affects adversaries' strategies. Besides, consequence analysis becomes more complicated and significant when domino effects [2,19,23,31,35,36] are likely to be triggered by intentional attacks. Different from other critical infrastructures, chemical industrial parks with hundreds and even thousands of installations are more vulnerable to domino effects due to storing or processing large amounts of hazardous (e.g., flammable, explosive and toxic) substances. As a result, these hazardous installations situated next to each other in a chemical industrial area can be regarded as one large interdependent system which may be exploited by terrorists to trigger domino effects. In that case, the consequences are more severe than that of the primary attack event. Therefore, Both internal domino effects and external domino effects[1] [48] should be considered in chemical security management.

Reniers et al. [50] proposed integrating safety and security to prevent domino effects in chemical clusters. Hausken et al. [28] applied game theory and contest success functions to study the defensive strategy based on effectiveness analysis taking into account both natural disasters and terrorism, neglecting the effect of safety resources on the consequences of security events. When eliminating terrorist groups and intentional attacks seems impossible, minimizing the potential consequences of intentional attacks can be considered as an effective approach for protecting chemical industrial plants against terrorist attacks [53].

However, minimizing the potential consequences is challenging, not only due to the interactions among different installations but also because the evolution of domino effects is a dynamic process. In a complex evolution, a lower order accident scenario may contribute to the damage of multiple installations (parallel effects), and a higher order accident scenario may be caused by multiple installations (synergistic effects) [8,45,49]. Deliberate fires are more likely to lead to a more severe escalation because the possibility of several simultaneous primary fires at different locations exist [17]. Installations involved in a domino effect are vulnerable at the starting of the evolution. As time goes by, the exposed installation's vulnerability increases due to temperature/pressure build-up, and may become harmful to other installations if damaged. Therefore, the vulnerability of installations in chemical industrial parks should be considered due to possible domino effects caused by deliberate attacks. However, previous evolution models such as the Monte Carlo-based methods [1,32], the Bayesian network [33,61], the CFD-based simulation [41], and the event tree method [3], for domino effects may be too complex or time-consuming and not suitable for security management in chemical industrial parks with large numbers of installations.

The present study is therefore aimed at establishing a usable consequence-based method for the allocation of safety and security resources in chemical industrial parks. A chemical industrial area with a large number of installations that may be directly or indirectly (domino effects) damaged by intentional attacks is deemed as a system. Security measures and safety barriers are integrated into a Dynamic Vulnerability Assessment Graph (DVAG) model for vulnerability assessment of installations that may be damaged by the spatial-temporal evolution of intentional attacks. The quantitative potential consequences of possible intentional attacks can be quickly obtained via the developed algorithm. Therefore, the effect of safety measures or safety barriers on potential consequences can be quantified, facilitating the decision making on the allocation of safety and security resources based on the principle of minimizing the potential consequence. Moreover, this work can be used to optimize the allocation of safety and security resources since it provides a fast computational method to assess the consequences of domino effects.

The main steps of the method are outlined in Section 2. After presenting the foundations of dynamic graphs, the Dynamic Vulnerability Assessment Graph (DVAG) model is elaborated in Section 3. Two illustrative examples based on the method proposed in this study are presented in Section 4. Finally, the conclusions drawn from this work are presented in Section 5.

2. Method

To reduce the potential consequences caused by intentional attacks and to provide support for the allocation of safety and security resources in chemical industrial parks, a consequence-based assessment method with a Dynamic Vulnerability Assessment Graph (DVAG) model is developed in the present study. The flow chart of the developed method is shown in Fig. 1. First, necessary information and data are collected, including the layout of a chemical industrial park, installations' information, data on hazardous materials, etc. In the following step, threats that may induce domino effects are analyzed and possible primary scenarios are identified. Step 3 conducts a vulnerability analysis using the DVAG model and obtains the damage possibilities of installations. Finally, the potential consequences of attack scenarios are analyzed and the relative consequence ranking is obtained, supporting the decision-making of defensive resources. The accident evolution involved in the present study is based on the escalation vector of heat radiation, but the framework can be extended to other types of escalations which might eventually be caused by intentional events.

2.1. Collecting park information and installation data

The first step of the method is to gather the information and data needed to implement the consequence-based method in chemical parks. Collecting this information can be divided into two parts: gathering (i) security-related information and (ii) domino effect related data. The security part collects the information of possible threats, such as motivations, attack types, attack capability, and attack objectives [5]. The domino effect related data can be summarized as follows:

(1) Park information: a layout of the park with installation's position and the distance between adjacent installations, the environmental information including temperature, wind, humidity, and the distribution of employees in the park.
(2) Installation data: physical parameters (types, functions, shapes, sizes, etc.), hazardous materials in installations (types, quantities, and states), and economic parameters of installations.
(3) Measures to reduce potential consequences: security measures (e.g., patrolling), passive barriers (e.g., fireproof coating), active barriers (e.g., water delivery systems), and emergency response.

2.2. Threat analysis and primary scenario identification

The objective of this step is to identify possible primary scenarios caused by intentional events that may trigger domino effects. In this study, domino effects triggered by intentional events are categorized

[1] External domino effects denote one or more escalation events outside the boundaries of the plant where the domino effect originates. Internal domino effects occur within a single plant while external domino effects involve multiple plants.

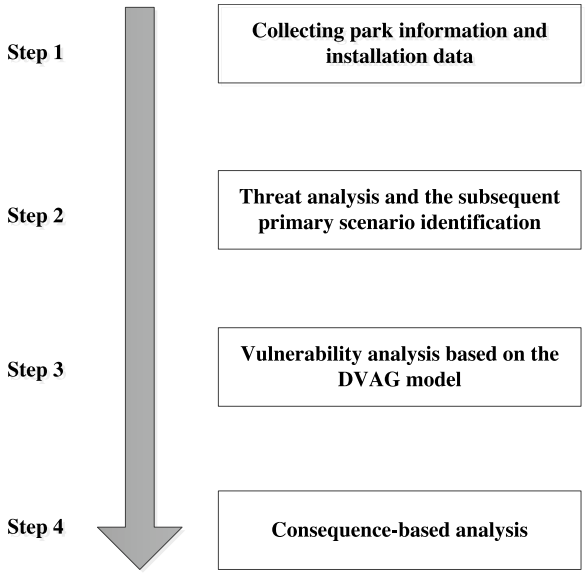


Fig. 1. Flow chart of the procedures developed for the consequence-based method.

into three types according to adversaries' motivations, as follows:

(1) Adversaries execute an attack with the purpose of triggering domino effects, inducing catastrophic accidents.
(2) Adversaries attack target installations resulting in unplanned domino effects.
(3) Adversaries indirectly attack a target installation via domino effects.

These intentional attacks may come from internal threats, external threats or internal threats working in collusion with external threats. The threat encompasses individuals, groups, organizations, or governments that may execute these intentional events. So threat analysis should consider as many threats 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. After threat analysis, the possible primary scenarios initiating domino effects can be obtained via cause-consequence analysis methods, such as what-if analysis and fault tree analysis. The risk analysis only serves to identify primary scenarios.

2.3. Vulnerability analysis

Previous vulnerability assessment methods for critical infrastructures mainly focus on target installations directly attacked by adversaries (API, 2013; EU [24]). In chemical industrial parks, a vulnerability assessment should be conducted for installations that may be involved in the attack due to possible domino effects. Thus, this step is aimed at assessing all installations' vulnerabilities and to obtain the damage probability of installations given different attacks. The vulnerability analysis is carried out using the Dynamic Vulnerability Assessment Graph (DVAG) model illustrated in Section 3. The spatial-temporal evolution, security measures, and safety barriers are considered in the DVAG model based on dynamic graphs.

2.4. Consequence-based analysis

Hausken [27] developed a cost-benefit analysis of terrorist attacks, considering economic value, human value, and influence value in benefit analysis. It is rather difficult to estimate the influence value associated with symbolic, political, and economic prestige, etc. For the process and chemical industries, environmental pollution should be addressed since large quantities of hazardous substances are usually present in industrial areas (API, 2013). Consequently, in terms of the consequences of intentional attacks in a chemical industrial park, this study considers three types of losses: economic loss, casualties, and environmental pollution. Possible damaged installations should be considered in the consequence analysis based on the vulnerability assessment results. Considering M attack scenarios capable of triggering domino effects in a chemical park, the potential consequence caused by the mth ($m = 1, 2, 3, \ldots, M$) attack scenario can be obtained by Eqs. (2) and (3).

$$PC^m = \sum_{j=1}^{N} CP_j^m \cdot L_j^m \tag{2}$$

$$L_j^m = L_{j\_1}^m + L_{j\_2}^m + L_{j\_3}^m \tag{3}$$

where PC^m is the potential consequence of attack scenario m, in EUR; CP_j^m is the conditional probability of installation j being damaged give an attack scenario m; L_j^m is the total consequence caused by the damage of installation j in attack scenario m, in EUR; N is the number of installations (possible targets) in the chemical industrial park, $M \le 2^N - 1$ (due to possible attack scenario with multiple targets); $L_{j\_1}^m$ is the direct economic loss caused by installation j in attack scenario m, in EUR; $L_{j\_2}^m$ is the loss of casualties caused by installation j in attack scenario m, in EUR; $L_{j\_3}^m$ is the loss of environmental pollution caused by installation j in attack scenario m, in EUR. The maximum potential consequence of possible attack scenarios in a chemical industrial park, MPC in EUR, is given in Eq. (4), while the average potential consequence of possible intentional attack scenarios (APC) is determined by Eq. (5). The average conditional probability of installation j being damaged by possible intentional attacks, ACP_j, can be calculated according to Eq. (6).

$$MPC = \max PC^m \tag{4}$$

$$APC = \frac{\sum_{j=1}^{m} PC^m}{m} \tag{5}$$

$$ACP_j = \frac{\sum_{m=1}^{M} CP_j^m}{m} \tag{6}$$

The maximum potential consequence (MPC) is a basic index for resource allocation to prevent man-made domino effects since rational attackers usually launch an attack with the objective of maximizing the potential consequence. The average potential consequence (APC), and the average conditional probability of installations being damaged (ACP) are systematic indicators used to examine the overall performance and robustness of safety and security resources in a chemical industrial area. Thus the likelihood difference of attacks is not considered in the two indicators.

3. Dynamic vulnerability assessment graph (DVAG) model

3.1. Fundamentals of dynamic graphs

Graph theory provides a mathematical approach for studying interconnections among elements in natural and manmade systems. Initially, interactions of elements were limited to binary relations denoted by vertices of the graph. Subsequently, functions were associated with graphs that assign a real number to each edge of a graph for quantifying the relationship between any pair of elements in a given system. So a classic graph consists of a set of vertices (nodes) and a set of edges (arcs) with the assumption that the structure of the graph is static.

However, the graphs may change over time in many applications, such as in computer programming languages and in artificial

Table 1
State description.

State	Description	Marked color
Vulnerable	The installation is not physically damaged but it may receive heat radiation from other installations. The installation's temperature or internal pressure may increase in this state.	Yellow
Harmful	The installation is on fire due to intentional events or due to escalation from other installations. Installations in this state have a harmful impact on other installations receiving their heat radiation.	Red
Dead	The fire on the installation is extinguished due to the burning out of flammable substances or emergency response actions. All edges connected to the node will be removed if the installation's state transfers from "harmful" to "dead".	Gray

intelligence. Dynamic graph models were systematically proposed in the 1990s to solve these practical dynamic applications. And the corresponding algorithms have been improved to study the dynamic graphs, such as Shortest Path algorithms. A dynamic graph, similar to the structure of static graphs, can be an undirected graph, a directed graph or a weighted graph (network). The three different structures of dynamic graphs are briefly described as follows. [13,16,26]

- An undirected graph is a pair $G = (V, E)$, where $V = \{V_1, V_2, V_3, \ldots, V_n\}$ is a set of vertices, and E is a set of edges. Each edge is an unordered pair where v_i and $v_j \in$V.
- A directed graph is a pair $G = (V, A)$, where V is again a set of vertices, and A is a set of arcs. Each arc is an ordered pair (v_i, v_j), $i \neq j$.

There are three kinds of weighted graphs (networks): a node-weighted graph, an edge-weighted graph, and a full weighted graph. A full weighted graph $G = (V, E, f, g)$, $f: V \rightarrow N_V$, $g: E \rightarrow N_E$, where N_V (N_E) is some numbered system, assigning a value or a weight of a node. The weights may be real numbers, complex numbers, integers, elements of some group, etc.

A dynamic graph G is updated when one or more than one of the following four entities change: V (a set of nodes), E (a set of edges), f (map vertices to numbers), and g (map edges to numbers). The dynamic graph can be divided into four basic categories according to the variation of different entities.

- A node-dynamic graph: the set V changes over time and the nodes may be added or removed. When a node is removed, the related edges are also eliminated.
- An edge-dynamic graph: the set E changes over time and the edges may be added or removed.
- A node weighted dynamic graph: the function f changes over time and the weights on the nodes update.
- An edge weighted dynamic graph: the function g changes over time and the weights on the edge also update.

Any combination of the above basic types can occur in real applications. An update on a graph is an operation that adds or removes nodes or edges, or changes in 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 and each graph can be studied by using the developed knowledge of static graph theory. Dynamic graph models may vary with different applications and the related algorithms can be developed according to the update rules of the dynamic graph [26].

3.2. Dynamic vulnerability assessment graph

3.2.1. Definition

A Dynamic Vulnerability Assessment Graph (DVAG) is defined as a dynamic graph indicating installations' vulnerability features in the evolution process of domino effects caused by intentional events. The dynamic graph starts when there is a primary fire scenario caused by intentional events and ends when the evolution is over. For illustration purpose, only the fire scenario is considered in the model, but it can be extended to other scenarios such as explosions and even the scenario changes between fire and explosion. The dynamic graph can be represented by Eq. (7).

$$G = (N,\ E,\ f,\ q) \tag{7}$$

(1) N is a set of nodes denoting installations in a chemical industrial park. The number of nodes (N) will not change in the entire evolution process.
(2) E is a set of directed edges from installations causing heat radiations to installations receiving the heat radiations. If there is an edge from node i to node j, node i is often called tail while node j is called head ($i \neq j$).
(3) f is a group of node weights (indicators) indicating the vulnerability or harmfulness of installations, as shown in Eq. (8).

$$f = (S,\ Q,\ RTF,\ RTB, CPS, CP) \tag{8}$$

- S is a set of states denoting the role of installations in a domino evolution. According to installations' vulnerable or harmful attributes in the evolution of domino effects, three states are defined: "vulnerable", "harmful" and "dead". The description of these states is shown in Table 1. For the sake of clear representation, an installation in the "vulnerable" state is marked as yellow, in the "harmful" state it is marked as red, and in the "dead" state it is marked as gray in the dynamic graph.
- Q is a weight of nodes denoting the total heat radiation received by installations, in kW/m^2. Installations in the "vulnerable" state receive heat radiations from installations in "harmful" state ($Q \geq 0$). The Q is equal to zero if an installation is in the "harmful" state or the "dead" state.
- RTF is a weight of nodes representing the residual time to failure (RTF) of installations, in min. The installation is assumed to be damaged when RTF is equal to zero.
- RTB is a weight of nodes denoting the residual time to burn out (RTB) of installations, in min. The fire on an installation is regarded to be extinguished when RTB is equal to zero.
- CPS is a set of conditional probabilities of installations being successfully attacked given a direct attack. It denotes the vulnerability of installations against direct attacks, as shown in Eq. (9). The CPS can be decreased by taking security measures.

$$CPS = P(Success|Attack) \tag{9}$$

If an installation i is the direct target of a possible attack m, the conditional probability of the installation being damaged is equal to the conditional probability of the installation being successfully attacked, as shown in Eq. (10).

$$CP_i^m = CPS_i^m \tag{10}$$

(4) q is the weight of directed edges which represent heat radiations from tail installations to head installations, kW/m^2. The q can be expressed by an adjacent matrix (a square matrix of dimension $N \times N$), as shown in Eq. (11).

$$Q = \begin{bmatrix} 0 & q_{12} & \cdots & q_{1n} \\ q_{21} & 0 & \cdots & q_{2n} \\ \cdots & \cdots & 0 & \cdots \\ q_{n1} & q_{n2} & \cdots & 0 \end{bmatrix} \tag{11}$$

where q_{ij} is the heat radiation from installation i to installation j. q_{ij} is equal to zero if there is no directed edge from installation i to installation j or i is equal to j. In the adjacency matrix, the row i indicates the harmfulness of installation i for other installations, and the column j characters the vulnerability of installation j.

3.2.2. Graph update

- Time update

A Dynamic Vulnerability Assessment Graph (DVAG) can be regarded as a chain of static graphs. The initial graph (graph 1) arises when a primary scenario caused by intentional events occurs. A new static graph will occur if an update operation is executed. The graph index (g) is also updated according to Eq. (12).

$$g = \begin{cases} 1 & \text{initial graph} \\ g+1 & \text{after a new update} \end{cases} \tag{12}$$

The period of time between two update operations is called "graph time" (t) in min. The total evolution time at the beginning of graph g (T^g, in min) can be obtained using Eq. (13).

$$T^g = \begin{cases} 0 & g = 1 \\ T^{g-1} + t^{g-1} & g > 1 \end{cases} \tag{13}$$

- State update

There are two update types among the three states, as shown in Fig. 2. In the initial graph, the attacked installation is in the "harmful" state and other installations are in the "vulnerable" state. An installation's state will be updated from "vulnerable" to "harmful" if it is damaged by escalation from external installations. Besides, an installation in a "harmful" state will be updated to a "dead" state if the fire on the installation is extinguished. Finally, the update will end when there is no escalation under the following conditions: (i) no installation in the "vulnerable" state; (ii) no installation in the "harmful" state.

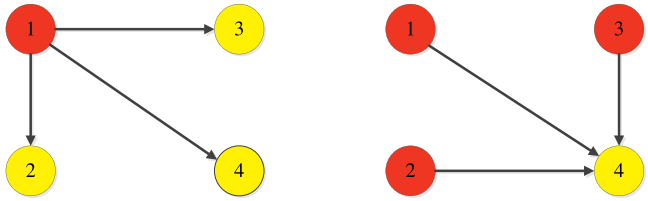
- Directed edge update

Directed edges connect installations in "harmful" states with installations in "vulnerable" states. Thus the directed edges should be added when any installation's state is updated. All directed edges from other installations to an installation in a "vulnerable" state will be deleted and the directed edges from the installation to other installations will be added when the installation's state transfers to "harmful". The directed edges from an installation to other installations will be deleted when the installation's state transfers to "dead".

- Heat radiation update

Installations with a "vulnerable" state in a domino evolution process may receive heat radiation from multiple installations with "harmful" states; this is known as "synergistic effects". Conversely, an installation in the "harmful" state may pose heat radiation on multiple installations

Fig. 2. State transition of installations.



(a) Parallel effects (b) Synergistic effects

Fig. 3. Graph models of the spatial evolution of domino effects.

being in "vulnerable" states; this is known as "parallel effects". Fig. 3a shows the graph model of a parallel effect while Fig. 3b shows a synergistic effect as a graph.

According to the synergistic effect, the total heat radiation received by an installation j in "vulnerable state" (Q_j) should be the sum of heat radiations received from other installations in "harmful" states, as shown in Eq. (14).

$$Q_j = \sum_{i=1}^{N} q_{ij} \tag{14}$$

The heat radiation received by each installation may vary over time due to new occurrences of harmful installations or dead installations. For update operations, the potential heat radiation values between each pair of installations can be calculated by software such as ALOHA [4]. In that case, an adjacency matrix of potential heat radiation (PQ) can be employed to represent the potential heat radiation values, as shown in Eq. (15).

$$PQ = \begin{bmatrix} 0 & pq_{12} & \cdots & pq_{1n} \\ pq_{21} & 0 & \cdots & pq_{2n} \\ \cdots & \cdots & 0 & \cdots \\ pq_{n1} & pq_{n2} & \cdots & 0 \end{bmatrix} \tag{15}$$

The heat radiation caused by installations in the "vulnerable" state can be reduced by active barriers such as water deluge systems (WDS). The WDS mitigates fire exposure by protection of the target, keeping a water film on exposed surfaces to absorb radiant heat and to cool the steelwork, thus reducing the heat radiation received by installations in a "vulnerable" state. In this study, WDS is used as an example of an active barrier in the evolution of domino effects. So the q_{ij} can be obtained using a radiation reduction factor (φ) and an effectiveness parameter (η) when the installation i is on fire and WDS are present in chemical industrial parks, as shown in Eq. (16).

$$q_{ij} = (1 - \eta \times \varphi) \times pq_{ij} \tag{16}$$

where pq_{ij} is the potential heat radiation caused by installation i on installation j, in kW/m^2; η is an effectiveness parameter of active protection systems; φ is the radiation reduction factor. If the active protection system is available, parameter values are assumed as follows: $\varphi = 60\%$, $\eta = 75\%$; otherwise, both parameters are equal to zero [37].

- Residual time to failure update

The RTF of installations may vary with time in the spatial-temporal evolution because of superimposed effects. Besides, passive protection systems also have great impacts on the RTF, such as fireproof coatings. Considering an installation j begins receiving effective heat radiation ($Q_j > 15$ kW/m^2 [20]) at evolution time T_g, the RTF can be calculated by Eq. (17) [38].

$$RTF_j^g = \frac{\exp(a \times V^b + c \ln(Q_j) + d)}{60} \tag{17}$$

where RTF_j^g is the residual time to failure of installation j at T^g, in min; a, b, c, and d are constants as presented in Table 2. In case of the presence of fireproof coatings, a time lapse (TL), should be considered

Table 2
The parameter value of *a, b, c,* and *d* adapted from Landucci et al. [38].

Installation	*a*	*b*	*c*	*d*
Atmospheric tank	-2.67×10^{-5}	1	−1.13	9.9
Pressurized tank	8.845	0.032	−0.95	0

since the failure time of installations is delayed due to the existing of fireproof coatings. As a result, the *TL* should be added to Eq. (17), as shown in Eq. (18).

$$RTF_j^g = \frac{\exp(a \times V^b + c\ln(Q_j) + d)}{60} + TL \tag{18}$$

A conservative *TL* of 70 min [37] is used in the present study if the fireproof coating is available; otherwise, the *TL* should be zero.

If $RTF_j^g > t^g$, the installation *j* will not be physically damaged at T^{g+1} and the residual time to failure of installation j in the "vulnerable" state at the time T^{g+1} will be updated according to superimposed effects: the heat radiation in different stages received by an installation should be superimposed in order to determine the residual time to failure at the time of T^{g+1}, as shown in Eq. (19) [17].

$$RTF_j^{g+1} = \left(\frac{Q_j^{g+1}}{Q_j^g}\right)^c \cdot (RTF_j^g - t^g) \tag{19}$$

The RTF_j^g is regarded as infinite when the installation *j* is in the "harmful" state or the "dead" state.

- Residual time to burn out update

Assuming an installation *i* is on fire at the evolution time of T^g, the residual time to burn out of installation *i* at the time of T^g can be represented by the ratio of flammable substance mass to the burning rate, shown in Eq. (20).

$$RTB_i^g = \frac{W_i}{v_i} \tag{20}$$

where W_i is the mass of flammable substances in installation *i*, kg; v_i is the burning rate of flammable substances in installation *i*, kg/min; RTB_i^g is the time to burn out of installation *i* at the evolution time of T^g.

If $RTB_i^g > t^g$, the installation *i* will continue to be on fire at T^{g+1} and the residual time to burning out of installation *i* at T^{g+1} will be updated according to Eq. (21).

$$RTB_i^{g+1} = RTB_i^g - t^g \tag{21}$$

- Damage probability update

Emergency response is essential for eliminating possible escalation or mitigating the consequence of domino effects in the chemical industry [57]. So emergency response should be considered in the vulnerability assessment of plant installations. However, the evaluation of emergency response is rather complex due to the uncertainties related to human factors in the performance of emergency response tasks. For simplification reasons, we assume that the domino effect evolution will be controlled when the emergency mitigation actions are started [38]. Taking into account the uncertainty of emergency response, a cumulative log-normal distribution (LND) function is used to model the time required to control domino effects (*ttc*), as shown in Eq. (22) [17].

$$\log ttc \sim N(u, \sigma^2) \tag{22}$$

where *u* is the mean of log *ttc* or expectation of the distribution; σ is the standard deviation of log *ttc* and σ^2 is the variance. These parameters can be obtained using Maximum Likelihood Estimation (MLE) based on the results of expert judgment, emergency exercises or simulations [17]. Therefore, if an installation *j* is supposedly damaged at T^g with a certain probability during the evolution of an intentional attack *m*, the conditional probability of installation *j* being damaged (CP_j) can be obtained by using Eq. (23). If installation *j* is the target of an attack *m* (i.e., $i = j$), the equation is equivalent to Eq. (10).

$$CP_j^m = CPS_i^m(1 - \mathrm{LND}(T^g)) \tag{23}$$

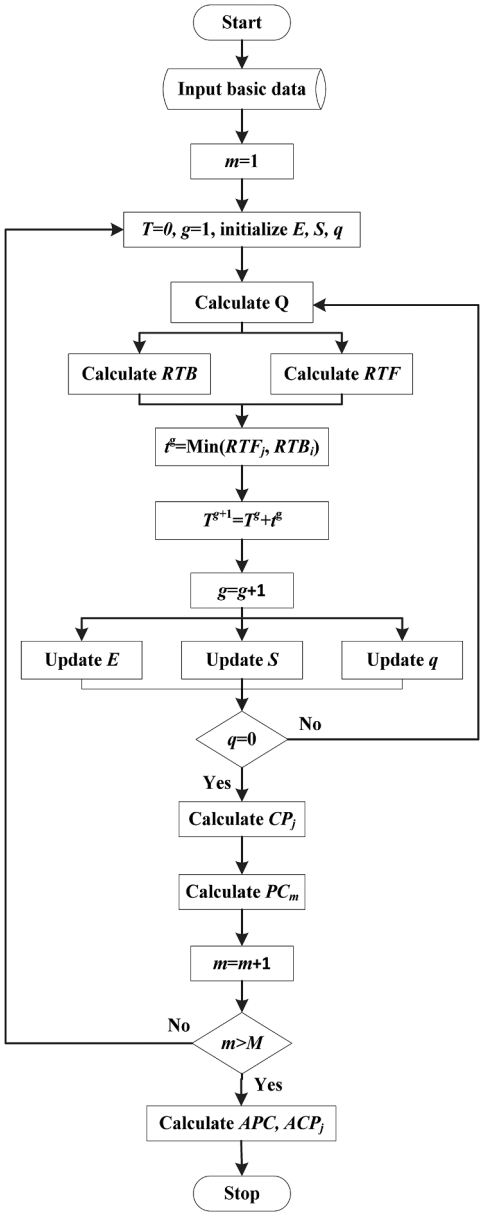


Fig. 4. Flow diagram of the algorithm for the DVAG model.

3.3. Algorithm

The Dynamic vulnerability Assessment graph (DVAG) model is established in Section 3.2, considering the effects of security measures, safety barriers of active protection measures, passive protection measures, and emergency response. This section describes the algorithm based on the DVAG model to obtain the quantitative potential consequence of possible attacks. The flow diagram of the algorithm is reported in Fig. 4.

The algorithm is described and explained as follows. First, basic data needed for performing the method is inputted, including park and plant information, potential heat radiations and primary scenarios,

safety and security measures, etc. Second, the parameters (*E, S, q*) of the DVAG model are initialized after selecting a primary scenario. The initial DVAG is updated at T^{g+1} when T^{g+1} is equal to the minimum of RTF_j and RTB_i. The parameters of *E, S, q* are calculated again after updating. If *q* is equal to zero, the graph update will stop and the damage probability of each installation is calculated. Another primary scenario will be selected after obtaining the consequence of the considered primary scenario. Otherwise, the update will proceed. The steps will continue until all the primary scenarios caused by intentional attacks are evaluated ($m > M$).

The potential consequence including induced domino effects of a security-related scenario, the installations' damage probabilities, and the graph time of each primary scenario are obtained using this algorithm. Decision-making on the allocation of safety and security resources can also be achieved considering different safety barriers and security measures in the potential consequence analysis.

4. Illustrative examples

In Section 3, the dynamic graph approach for vulnerability-consequence assessment of domino effects caused by intentional events was elaborated and explained. Decision making on security measures and safety barriers using this approach was expounded. In this section, illustrative examples aiming at interpreting the procedures and validation of the proposed method are given. Besides, the method is applied to a chemical cluster to show the method's advantages for such implementation situation.

4.1. Example 1: a single plant

According to the method proposed in Section 2, we firstly should collect the park information and installation data of the chemical plant, as follows. Fig. 5 shows the schematic of an illustrative single chemical plant with four storage tanks. The features of these tanks are summarized in Table 3. The weather condition is assumed as follows: ambient temperature of 20°C, wind blowing from the West with a speed of 1.5 m/s, relative humidity of 50%, and the stability class D. The heat radiation caused by pool fire and the burning rate of each tank are calculated through the ALOHA software. The heat radiation caused by tank *i* on tank *j* (i.e., q_{ij}) and the time to burn out (*ttb*) of each tank is shown in Table 4. Assuming a log-normal distribution of the time to control effectively (*ttc*), i.e., log*ttc* ~ (μ, σ^2), the mean of *ttc* is equal to 10 min and the corresponding variance is equal to 2 min [17].

The second step is to analyze possible threats and identify the corresponding primary scenarios. Table 5 illustrates the primary scenarios caused by possible intentional events and the conditional probability of these primary scenarios given the intentional attack.

The Dynamic Vulnerability Assessment Graph (DVAG) model proposed in Section 3 is used to assess the vulnerability of the tanks in the chemical plant. In this step, the failure time and failure probability of each tank following escalation caused by attacks are obtained, as shown in Tables 6 and 7. Taking primary scenario 1 as an example, Tank 1 is on fire caused by a direct intentional attack at $T = 0$ min (Fig. 6(a)). The heat radiation emitted from Tank 1 can cause a credible damage to Tank 2, resulting in a fire at Tank 2 at $T = 6.08$ min. After catching fire, the state of Tank 2 transfers from "vulnerable" to "harmful", inducing a synergistic effect on Tank 3 and Tank 4, as shown in Fig. 6(b). Consequently, Tank 3 is on fire at $T = 7.36$ min (Fig. 6(c)) due to a superimposed effect of stage 1 and stage 2. Tank 4 is the last one to catch fire. The damaged time of each tank in different primary scenarios is shown in Table 6. The evolution speed of primary scenario 1 is the fastest while that of the primary scenario 4 is the slowest.

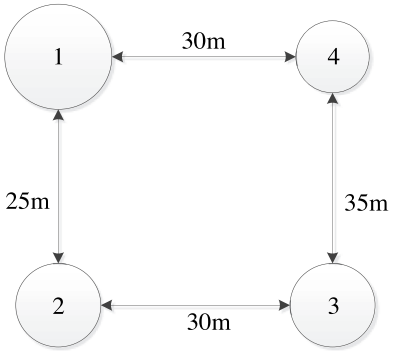


Fig. 5. Layout of an illustrative chemical storage plant (example 1).

Table 7 presents the damage probability of each Tank in different primary scenarios. It indicates that the domino effect caused by the attack on Tank 1 may be inevitable due to the fastest evolution. Tank 2 with the highest average conditional probability of being damaged (*ACP*) is more susceptible to domino effects caused by other tanks.

Finally, the performance of safety and security resources are analyzed based on the consequence assessment proposed in Section 2.4. Table 8 shows the potential consequences of all attacks. The potential consequence of the attack on Tank 1 is much higher than that of the other three attacks since the four tanks have a high probability to be damaged by the domino effects initiated at Tank 1, i.e., emergency response is unlikely to effectively control the escalation. The security measures' effect on Tank 4 is limited since the attack on Tank 4 cannot induce domino effects.

Table 9 lists several protection measures and the corresponding potential consequences. In this case, the fireproof coating can eliminate the possible domino effects because the potential consequence of each attack is equal to the potential loss of the attached tank. Four cases are considered to investigate the most effective allocation of passive barriers, as shown in Table 10. Obviously, the passive barriers should be allocated to Tank 2 which has the highest *ACP*.

In order to validate the method, the results are compared with the results of a static graph approach [34]. Employing the static graph methodology, the out-closeness metric reflects installations' potential contribution to the escalation of domino effects while the in-closeness metric represents the vulnerability of installations to get damaged during domino effects. The static graph model of the chemical storage plant is shown in Fig. 7 (threshold value is also equal to 15 kW/m^2).

The results of two graph metrics (out-closeness and in-closeness) of the four tanks are illustrated in Table 11. It indicates that the method proposed in this study is valid since the ranking of units based on their out-closeness is the same as their ranking based on their *PA* (Table 8); likewise, the ranking of units based on their in-closeness is also identical to their ranking based on their respective *ACP* (Table 7). The dynamic graph approach, in addition, seems to be able to grasp the dynamic evolution of domino effects compared to the static graph which seems to provide merely a snapshot of the whole process at once.

4.2. Example 2: a chemical cluster

A complex example is used to illustrate the application of the method to a chemical industrial park with a large number of installations. Fig. 8 shows the layout of an area including three chemical storage plants. The plant information and tank data are shown in Table 12. All the tanks (150 in total) may be potentially attacked with the same conditional probability of successful attack (*CPS*) of 0.5. Assuming the mean of *ttc* (μ) is equal to 20 min and the corresponding variance (σ) is equal to 5 min. The wind speed is 5 m/s and other parameters are the same as in Section 4.1.

The potential consequences (*PC*) of the 150 attack scenarios and the average conditional probability of installations being damaged (*ACP*) are obtained via the algorithm presented in Section 3.3, as shown in Fig. 9. The total computational time is 4.1 s using a personal computer (Intel (R) Core (TM) i5 CPU, 4GB RAM). The *PC* represents the

Table 3
Features of chemical storage tanks.

Tank	Type	Dimension	Chemical substance	Volume (m^3)	Chemical content (t)	Consequence (1000 EUR)
1	Atmospheric	30 × 10	Benzene	6000	4000	2900
2	Atmospheric	20 × 10	Acetone	2500	2000	2400
3	Atmospheric	20 × 10	Toluene	2500	1500	900
4	Atmospheric	10 × 6.5	Toluene	500	200	100

Table 4
The Heat Radiation q_{ij} between each pair of tanks and the time to burn out (*ttb*) of tanks.

Tank *i, j*	q_{ij} (kW/m^2)				*ttb* (min)
	1	2	3	4	
1	–	32.5	25.1	12.9	1666.7
2	17.7	–	13.2	4.1	1369.9
3	8.7	17.6	–	13.8	980.4
4	10.1	3.5	8.3	–	233.9

escalation capability of the attacked installations while the *ACP* characterizes the vulnerability of installations. Thus installations are more likely to initiate or propagate domino effects if their rankings of *PC* are higher than that of *ACP*. Alternatively, installations with higher rankings of *ACP* than that of *PC* exhibit a high probability of being damaged by domino effects occurring in the area. The maximum potential consequence (*MPC*) in Plant 1 is 2.45×10^7 EUR (an attack on Tank 26), in Plant 2 it is 5.86×10^6 EUR (an attack on Tank 76), and in Plant 3 it is 1.92×10^7 EUR (an attack on Tank 123). The potential consequences of attacks in Plant 2 are obviously smaller than those in Plant 1 and Plant 3 since the wind blows from west to east (i.e., the tank is more likely to be damaged by the heat radiation caused by the tank in the west), and the heat radiation caused by tanks in Plant 3 is greater than in Plant 2, as shown in Table. 4.

Security measures (e.g., patrols, fences, CCTV systems) for reducing the conditional probability of installations being successfully attacked (*CPS*) or active barriers (i.e., water delivery systems) for absorbing heat radiation can be allocated to these tanks with high *PC* to reduce the *MPC* of the chemical industrial area. In that case, the *APC* decreases from 9.87×10^6 EUR to 6.44×10^6 EUR by decreasing the *CPS* (from 0.5 to 0.3) using security measures in Plant 1 and Plant 3. The red curve in Fig. 9 shows the *ACP* of each tank. The tanks located in the east have a higher *ACP* than those located in the west due to the effect of the wind. The maximum *ACP* in Plant 1 is 0.0575 (Tank 30), in Plant 2 it is 0.0192 (Tank 74), and in Plant 3 it is 0.0539 (Tank 127).

These tanks with high *ACP* should be allocated more passive barriers protecting these installations against fires. For instance, the average potential consequence is reduced by 38.9% by allocating fireproof coatings on the top 20 tanks (the ranking of *ACP* in descending order).

Fig. 10 shows the required time of external domino effects if a tank in Plant 1 is attacked. The minimum time required for initiating external domino effects in Plant 2 is 21.3 min with a maximum probability of 0.13, and that in Plant 3 is 26.5 min with a maximum conditional probability of 0.0024. The attacks in Plant 3 can also induce external domino effects in Plant 1 and Plant 2, and the maximum conditional probabilities are 0.21 and 0.23 separately. However, the external domino effects caused by attacks in Plant 2 may be impossible and Plant 3 is thus more likely to suffer from external domino effects since it is located downwind. The external domino effects can be eliminated by improving emergency response capabilities. For example, the maximum probability of external domino effects in Plant 3 triggered by Plant 1 will decrease to 2.19×10^{-4} if the emergency response time is shortened to 10 min.

Table 6
The damage time of tanks (min).

Tank	A1	A2	A3	A4
1	0	11.01	19.17	–
2	6.08	0	12.16	–
3	7.36	16.06	0	–
4	13.52	20.30	22.19	0

Table 7
The conditional probability of installations being damaged (*CP*).

Tank	A1	A2	A3	A4	Average
1	0.50	0.11	6.71×10^{-7}	0	0.15
2	0.50	0.50	0.04	0	0.26
3	0.49	1.48×10^{-4}	0.50	0	0.25
4	6.70×10^{-3}	8.52×10^{-8}	2.45×10^{-9}	0.5000	0.13

5. Discussion

The illustrative examples in Section 4 indicate that our method can quickly obtain quantitative results of consequences caused by intentional attacks in large chemical industrial areas, considering installations that may be damaged in the spatial-temporal evolution of domino effects. This section discusses the effects of safety and security resources on potential consequences (*PC*) of attacks, thus supporting the decision-making of resource allocation.

Security measures can prevent the occurrence of the primary scenarios while safety barriers are able to weaken the evolution of domino effects; thus these limited resources should be properly allocated so as to decrease the attractiveness by decreeing the maximum potential consequence (*MPC*) and the average potential consequences (*APC*) of the entire park area (which we consider as a system). Fig. 11(a) shows the effect of security measures on average potential consequences (*APC*) in case 2. The *APC* decreases rapidly and then slows down as the number of tanks with allocated security resources increases. Taking the blue curve with triangles as an example, the *APC* decreases by 24.0% if the top 50 tanks (the ranking of *PC* in descending order) are allocated

Table 5
Possible primary scenarios caused by attacks.

Attacks	Primary scenario	*CPS* without security measures	*CPS* with security measures
A1	Pool fire at Tank 1	0.5	0.3
A2	Pool fire at Tank 2	0.5	0.3
A3	Pool fire at Tank 3	0.5	0.3
A4	Pool fire at Tank 4	0.5	0.3

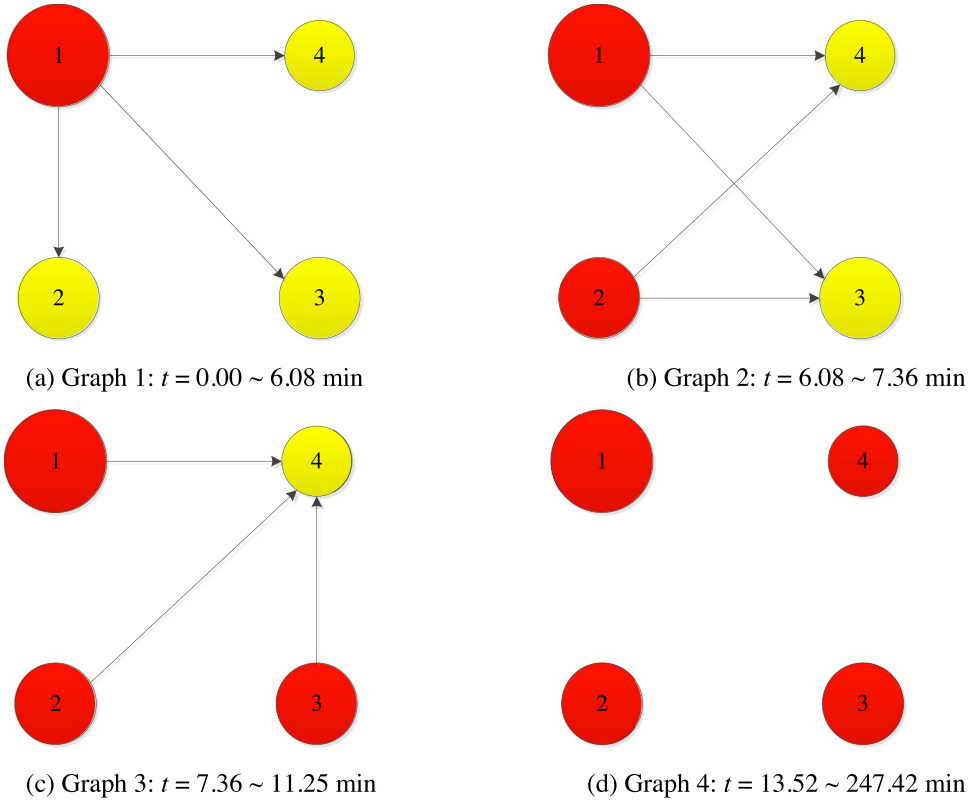


Fig. 6. The Dynamic Vulnerability Assessment Graph (DVAG) of the attack on Tank 1.

Table 8
The potential consequences of attacks.

Primary scenario	A 1	A 2	A 3	A 4	Average
Potential consequence (1000 EUR)	3092.5	1527.9	536.4	50.0	1301.7

security measures. However, the *APC* only decreases by 4.0% if these security resources are allocated to the last 50 tanks. Besides, different security measures have different effects on the conditional probability of installations being successfully attacked (*CPS*). The *APC* decreases with increasing the security investment in each tank (the *CPS* is inversely proportional to the security investment).

The *PC*-based allocation can also be applied to the allocation of safety barriers as shown in Fig.11(b). The *APC* decreases with

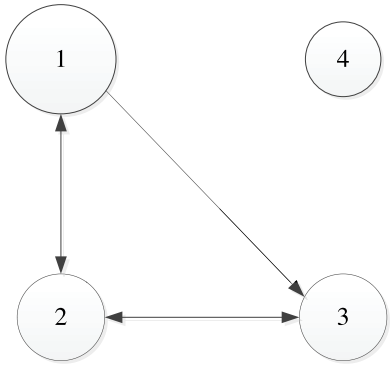


Fig. 7. Static graph model of the chemical storage plant in example 1.

Table 9
The potential consequences of attacks with additional protection measures.

Additional measures	Potential consequence (1000 EUR) A 1	A 2	A 3	A 4	Average	Decrease (%)
Security measures on Tank 1	1855.5	1527.9	536.4	50.0	992.5	23.8%
Security measures on Tank 4	1855.5	1527.9	536.4	30.0	1305.0	0.5%
WDS on all tanks	1450.0	1200.0	450.0	50.0	787.5	39.3%
Fireproof coatings on all tanks	1450	1200	450	50.0	787.5	39.3%
Shortening the mean of *ttc* to 8 min	2858.9	1241.0	458.0	50.0	1152.6	11.5%

Table 10
The potential consequences of each primary scenario with additional fireproof coatings.

Additional measures	Potential consequence (1000 EUR) A 1	A 2	A 3	A 4	Average	Decrease (%)
Fireproof coating on Tank 1	3092.5	1200.0	536.4	50.0	1219.7	6.3%
Fireproof coating on Tank 2	1863.0	1527.9	450.0	50.0	972.7	25.3%
Fireproof coating on Tank 3	2649.7	1527.7	536.4	50.0	1191.0	8.5%
Fireproof coating on Tank 4	3091.8	1527.9	536.4	50.0	1301.5	0.01%

Table 11
The results of graph metrics for the graph shown in Fig.7.

Tank	Out-closeness	In-closeness
1	0.42	0.17
2	0.19	0.34
3	0.17	0.22
4	0	0

increasing the number of tanks equipped with WDS. The *APC* decreases from 9.87 × 10^6 EUR to 4.95 × 10^6 by allocating security measures to the top 50 tanks while it only decreases to 8.76 × 10^6 EUR if we allocate these resources to the last 50 tanks. Combining Eq. (16) and Fig. 11(b), it can be concluded that improving effectiveness or radiation reduction factor of WDS is also an effective way to reduce the *APC*.

Passive safety barriers such as fireproof coatings can reduce the physical effects caused by the fire on the target installations. The case analysis in Section 4.1 states that the ranking of *ACP* in descending

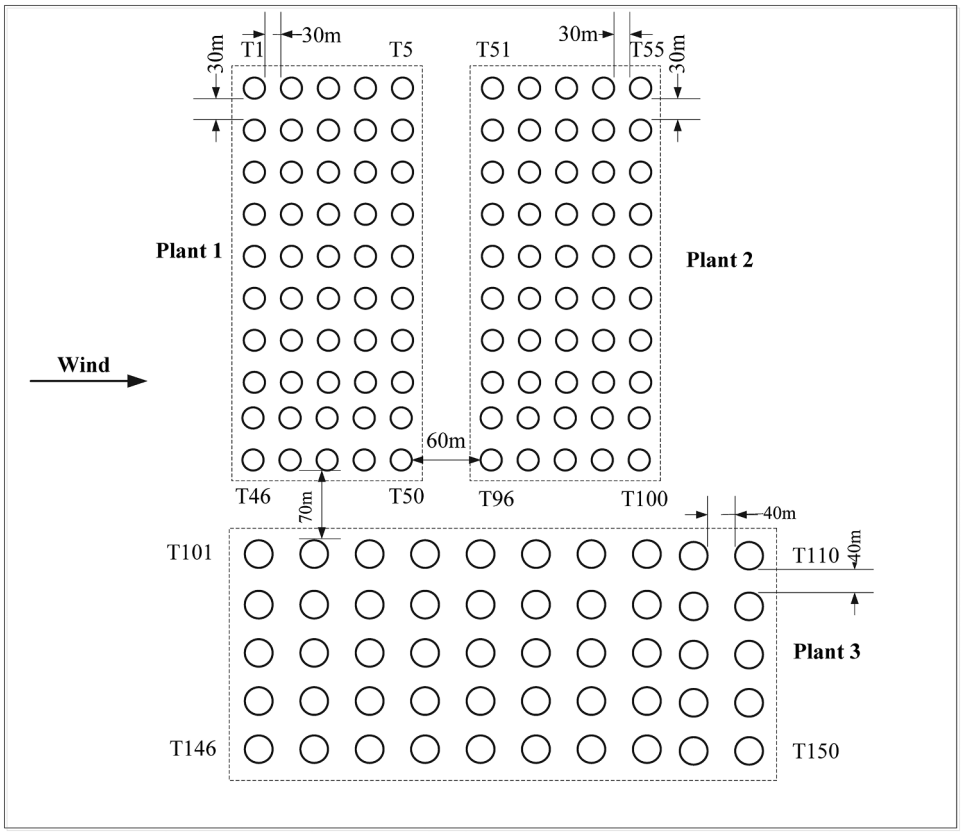


Fig. 8. The layout of three illustrative chemical storage plants within a chemical industrial park.

Table 12
Tank features in each plant.

Plant	Tank number	Tank Type	Chemical substance	The volume of each tank (m^3)	The chemical content of each tank (t)	*ttb* of each tank (min)	The consequence of each tank (1000 EUR)
1	50	Atmospheric	Toluene	2500	2500	1634	1500
2	50	Atmospheric	Acetone	2500	1000	685	1200
3	50	Atmospheric	Benzene	6000	2000	833	1400

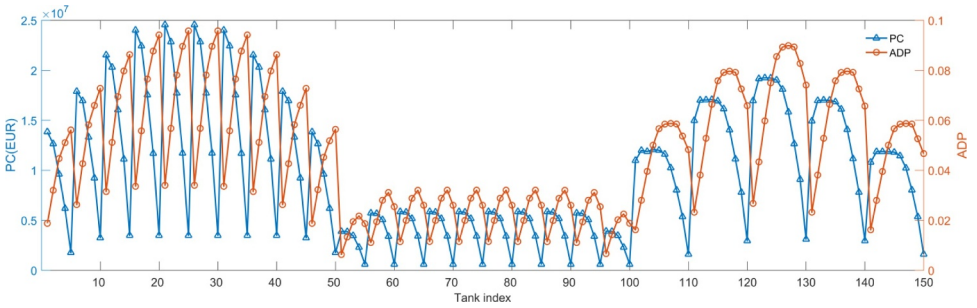


Fig. 9. The potential consequence (*PC*) and the average conditional probability (*ACP*) of each attack.

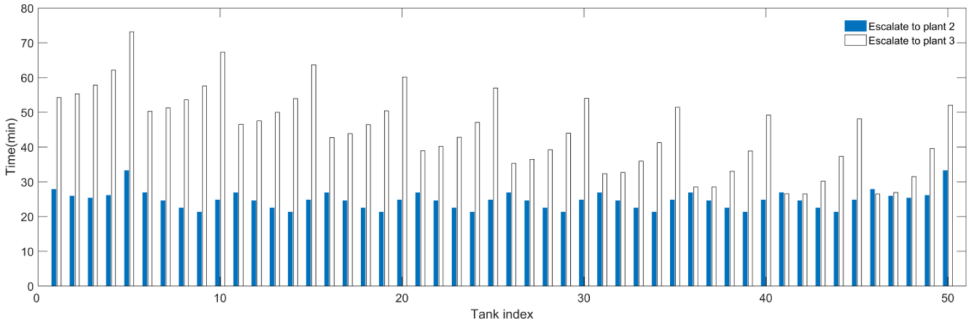


Fig. 10. The required time of external domino effects given an attack on one of the tanks in Plant 1.

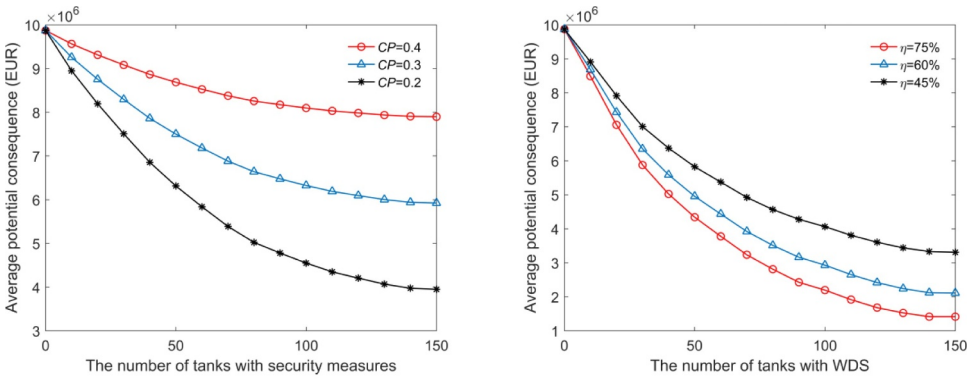


Fig. 11. The *PC*-based allocation for (a) security measures and (b) water deluge systems (WDS).

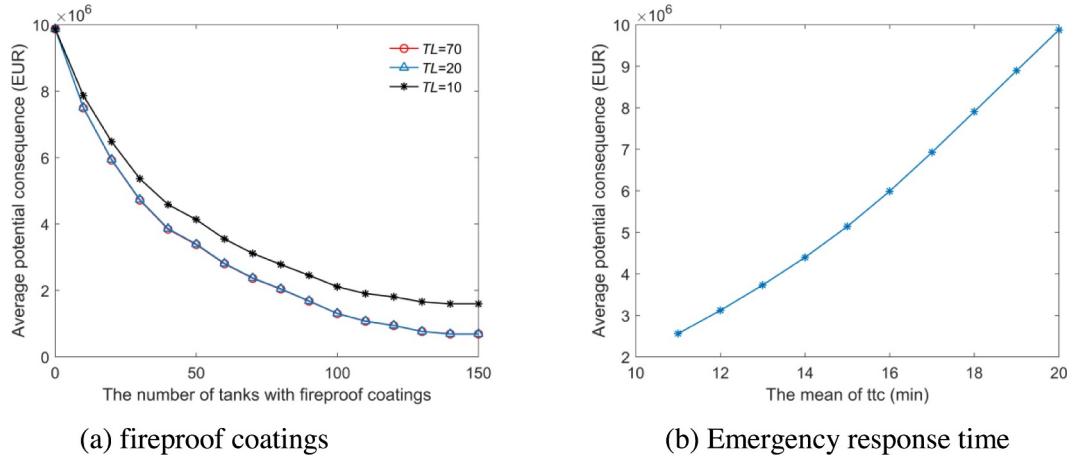


Fig. 12. The effects of (a) fireproof coatings and (b) emergency response time on the average potential consequence (*APC*) of attacks.

order can be used for the allocation of passive barriers. Fig. 12(a) shows the results of fireproof coating allocations. It indicates that the allocation based on *ACP* is also suitable for large chemical industrial parks, i.e., the reduction rate of *APC* decrease with increasing the number of fireproofed tanks.

Besides, we also investigate the effects of the time lapse (*TL*) of fireproof coatings on the *APC*. The *APC* decreases rapidly with increasing *TL* when *TL* is less than the mean of emergency response time (*u*) but it barely changes with the increase of *TL* when *TL* is greater than *u*. It manifests that passive barriers can provide enough time for the advent of emergency response when the *TL* is greater than *u*. Fig. 12b shows that the emergency response time has a great impact on the *APC* . More calculations indicate that all the 150 tanks may be damaged if the emergency response is not available since the passive and active barriers only extend the time to failure (*ttf*) of installations but can't eliminate the escalation.

For instance, fireproof coatings will be of no effect after 70 min while the minimal time to burn out (*ttf*) of installations is 685 min. Therefore, safety and security resources should be integrated and the allocation optimization of integrated safety barriers and security measures based on cost-effective analysis is another open issue in this domain.

As mentioned above, the method proposed in this study can be used to support decision-making for safety and security resources in large chemical industrial parks. It is a primary work for integrating safety and security resources to prevent man-made domino effects, considering the potential overall loss of a chemical industrial park. The DVAG model proposed in the study may be extended to model other escalation

vectors besides heat radiation, such as overpressure and fragments caused by explosions. The consequence-based approach may be improved by considering attack types, attack likelihood, and multi-targets. Besides, advanced decision-making and optimization tools (e.g., game theory and genetic algorithms) may be used based on the dynamic graph approach to better protect chemical industrial parks from catastrophic events.

6. Conclusions

In the present study, a consequence-based method for the allocation of security measures and safety barriers in chemical industrial areas based on dynamic graphs was developed. From a systematic aspect, the potential consequences consist of the possible losses of the target installations and the losses of other installations that may be damaged due to domino effects. The Dynamic Vulnerability Assessment Graph (DVAG) model based on dynamic graphs proposed in this paper is able to model the spatial-temporal feature of domino effects, considering the effects of security measures and safety barriers. The damage probability of installations and the consequences of possible attacks in a chemical industrial park can be quickly obtained using the developed approach, significantly facilitating the decision making on the allocation of safety and security resources. Therefore, this method can be applied to realistic chemical clusters with a large number of installations.

Resource allocation recommendations for reducing the potential consequences of attacks may be proposed based on potential consequence-related indicators and using two case studies, as follows: (i) security measures and active safety barriers should be allocated to installations with high potential consequences (*PC*), (ii) the ranking of *ACP* (average conditional probability of installations being damaged) is recommended for the allocation of passive safety barriers, (iii) the time lapse (*TL*) of fireproof coatings should be greater than the mean of *ttc*, (iv) external fire-induced domino effects are more likely to occur at the downwind area of chemical industrial parks, and (v) shortening emergency response time is an effective way to eliminate the possible escalations of attacks, and using active and passive barriers can provide more time for emergency response actions.

The present work is a preliminary work for integrating security and safety resources to protect chemical industrial parks from domino effects. The allocation optimization of safety barriers and security measures based on cost-effectiveness analysis and adversaries' strategies is a subject of future study.

Acknowledgments

This work is supported by the Chinese Scholarship Council (Grant No: 201708510111). We also appreciate those who assisted us with observations, the anonymous reviewers, and the editor for their constructive comments and suggestions.

References

[1] Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi SA. A new method for assessing domino effect in chemical process industry. J Hazard Mater 2010;182:416–26.
[2] Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi SA. Domino effect in process-industry accidents – An inventory of past events and identification of some patterns. J Loss Prev Process Ind 2011;24:575–93.
[3] Alileche N, Olivier D, Estel L, Cozzani V. Analysis of domino effect in the process industry using the event tree method. Saf Sci 2017;97:10–9.
[4] ALOHA. US environmental protection agency. National Oceanic and Atmospheric Administration, ALOHA; 2016. Version 5.4.7.
[5] AP. ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry. Am Petrol Instit 2013.
[6] API/NPRA. Recommended practice for security vulnerability assessment for petroleum and petrochemical facilities. Am Petrol Instit 2004.
[7] Apostolakis GE, Lemon DM. A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Anal 2005;25:361–76.
[8] Bagster DF, Pitblado RM. The estimation of domino incident frequencies—an approach. Process Saf Environ Protect 1991;69:195–9.
[9] Baybutt P. Assessing risks from threats to process plants: threat and vulnerability analysis. Process Saf Prog 2002;21:269–75.
[10] Baybutt P. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defence J 2003;2.
[11] Baybutt P. Issues for security risk assessment in the process industries. J Loss Prev Process Ind 2017;49:509–18.
[12] Bier VM, Nagaraj A, Abhichandani V. Protection of simple series and parallel systems with components of different values. Reliab Eng Syst Saf 2005;87:315–23.
[13] Bondy JA, Murty USR. Graph theory with applications 1976.
[14] Brown G, Carlyle M, Salmerón J, Wood K. Defending critical infrastructure. Interfaces 2006;36:530–44.
[15] Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S. Catastrophic cascade of failures in interdependent networks. Nature 2010;464:1025–8.
[16] Casteigts A, Flocchini P, Quattrociocchi W, Santoro N. Time-varying graphs and dynamic networks. Int J Parallel Emergent Distrib Syst 2012;27:387–408.
[17] Chen C, Reniers G, Zhang L. An innovative methodology for quickly modeling the spatial-temporal evolution of domino accidents triggered by fire. J Loss Prev Process Ind 2018;54:312–24.
[18] Chen Z, Du W-B, Cao X-B, Zhou X-L. Cascading failure of interdependent networks with different coupling preference under targeted attack. Chaos, Solitons Fract 2015;80:7–12.
[19] Cozzani V, Gubinelli G, Antonioni G, Spadoni G, Zanelli S. The assessment of risk caused by domino effect in quantitative area risk analysis. J Hazard Mater 2005;127:14–30.
[20] Cozzani V, Tugnoli A, Salzano E. The development of an inherent safety approach to the prevention of domino accidents. Accid Anal Prev 2009;41:1216–27.
[21] Cox JLA. Game Theory and Risk Analysis. Risk Anal 2009;29:1062–8.
[22] Cox Jr. LA. Some limitations of "Risk = Threat x Vulnerability x Consequence" for risk analysis of terrorist attacks. Risk Anal 2008;28:1749–61.
[23] Darbra RM, Palacios A, Casal J. Domino effect in chemical accidents: main features and accident sequences. J Hazard Mater 2010;183:565–73.
[24] Commission EU. staff working document on the review of the european programme for critical infrastructure protection (EPCIP),. Brussels: European Commission; 2012. Retrieved from.
[25] Garrick BJ, Hall JE, Kilger M, McDonald JC, O'Toole T, Probst PS, Parker ER, Rosenthal R, Trivelpiece AW, Van Arsdale LA. Confronting the risks of terrorism: making the right decisions. Reliab Eng Syst Saf 2004;86:129–76.
[26] Harary F, Gupta G. Dynamic graph models. Math Comput Modell 1997;25:79–87.
[27] Hausken K. A cost–benefit analysis of terrorist attacks. Defence Peace Econ 2018;29:111–29.
[28] Hausken K, Bier VM, Zhuang J. Defending against terrorism, natural disaster, and all hazards. Game theoretic risk analysis of security threats. Springer; 2009. p. 65–97.
[29] Hausken K, Levitin G. Minmax defense strategy for complex multi-state systems. Reliab Eng Syst Saf 2009;94:577–87.
[30] Hausken K, Levitin G. Review of systems defense and attack models. Int J Perform Eng 2012;8:355–66.
[31] Hemmatian B, Abdolhamidzadeh B, Darbra RM, Casal J. The significance of domino effect in chemical accidents. J Loss Prev Process Ind 2014;29:30–8.
[32] Kadri F, Châtelet E, Chen G. Method for quantitative assessment of the domino effect in industrial sites. Process Saf Environ Prot 2013;91:452–62.
[33] Khakzad N. Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. Reliab Eng Syst Saf 2015;138:263–72.
[34] Khakzad N, Reniers G. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliab Eng Syst Saf 2015;143:63–73.
[35] Khan FI, Abbasi S. Models for domino effect analysis in chemical process industries. Process Saf Prog 1998;17:107–23.
[36] Khan FI, Abbasi S. An assessment of the likelihood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. J Loss Prev Process Ind 2001;14:283–306.
[37] Landucci G, Argenti F, Tugnoli A, Cozzani V. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab Eng Syst Saf 2015;143:30–43.
[38] 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.
[39] Lee Y, Kim J, Kim J, Kim J, Moon I. Development of a risk assessment program for chemical terrorism. Korean J Chem Eng 2010;27:399–408.
[40] Liu D, Wang X, Camp J. Game-theoretic modeling and analysis of insider threats. Int J Crit Infrastruct Prot 2008;1:75–80.
[41] Masum Jujuly M, Rahman A, Ahmed S, Khan F. LNG pool fire simulation for domino effect analysis. Reliab Eng Syst Saf 2015;143:19–29.
[42] Matteini A, Argenti F, Salzano E, Cozzani V. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliability Engineering & System Safety; 2018.
[43] Mirzasoleiman B, Babaei M, Jalili M, Safari M. Cascaded failures in weighted networks. Phys Rev E Stat Nonlin Soft Matter Phys 2011;84:046114.
[44] Moore DA, Fuller B, Hazzan M, Jones JW. Development of a security vulnerability assessment process for the RAMCAP chemical sector. J Hazard Mater 2007;142:689–94.
[45] Necci A, Cozzani V, Spadoni G, Khan F. Assessment of domino effect: state of the art and research Needs. Reliab Eng Syst Saf 2015;143:3–18.
[46] Paté-Cornell E, Guikema S. Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Military Oper Res 2002;7:5–23.
[47] Powell R. Defending against terrorist attacks with limited resources. Am Polit Sci

Rev 2007;101:527–41.
[48] Reniers G. An external domino effects investment approach to improve cross-plant safety within chemical clusters. J Hazard Mater 2010;177:167–74.
[49] Reniers G, Cozzani V. Domino Effects in the Process Industries, Modeling. Prevention and managing. Amsterdam, The Netherlands: Elsevier; 2013.
[50] Reniers G, Dullaert W, Audenaert A, Ale BJ, Soudan K. Managing domino effect-related security of industrial areas. J Loss Prev Process Ind 2008;21:336–43.
[51] Reniers G, Khakzad N, Gelder PV. Security risk assessment. Chemical and Process Industry. De Gruyter; 2017.
[52] Reniers G, Soudan K. A game-theoretical approach for reciprocal security-related prevention investment decisions. Reliab Eng Syst Saf 2010;95:1–9.
[53] Reniers GLL, Audenaert A. Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures w.r.t. domino effects. Process Saf Environ Prot 2014;92:583–9.
[54] Rios J, Insua DR. Adversarial risk analysis for counterterrorism modeling. Risk Anal 2012;32:894–915.
[55] Staalduinen MAv, Khan F, Gadag V. SVAPP methodology: a predictive security vulnerability assessment modeling method. J Loss Prev Process Ind 2016;43:397–413.
[56] Zhang L, Reniers G. A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. Risk Anal 2016;36:2285–97.
[57] Zhou J, Reniers G. Petri-net based modeling and queuing analysis for resource-oriented cooperation of emergency response actions. Process Saf Environ Prot 2016;102:567–76.
[58] Tambe M. Security and game theory: algorithms, deployed systems, lessons learned. Cambridge University Press; 2011.
[59] Willis HH. Guiding resource allocations based on terrorism risk. Risk Anal 2007;27:597–606.
[60] Wu B, Tang A, Wu J. Modeling cascading failures in interdependent infrastructures under terrorist attacks. Reliab Eng Syst Saf 2016;147:1–8.
[61] Yang Y, Chen G, Chen P. The probability prediction method of domino effect triggered by lightning in chemical tank farm. Process Saf Environ Prot 2018;116:106–14.