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

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

[*] 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 parks are susceptible to domino effects triggered by intentional attacks. Previous research on security risk management in chemical and process industries 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 all installations. A consequence-based methodology including a Dynamic Vulnerability Assessment Graph (DVSG) 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 methodology can quickly assess the consequences and damage probabilities of all possible intentional attacks so as to mitigate the risk via evaluation and allocation of security measures and safety barriers.

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

1. Introduction

The chemical sector is identified as one of 16 critical infrastructures by the U.S. Department of Homeland Security (Reniers et al., 2017). A growing public concern raised the attention on chemical and process security after the terrorist attack in New York City on September 11, 2001 (Baybutt, 2002, 2003; Bier et al., 2005; Lee et al., 2010; Reniers et al., 2008). In 2004, the American Petroleum Institute (API) published a recommendation on security risk assessment for the petroleum and petrochemical industries (API/NPRA, 2004). 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 (API,

2013). 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).

$$R_S = f_S(T, V, C) \qquad (1)$$

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 (Baybutt, 2017; Paté-Cornell and Guikema, 2002). Vulnerability analysis requires a detailed understanding of the design and operation of installations and the threat information (Matteini et al., 2018; Moore et al., 2007; Staalduinen et al., 2016). Security measures can improve the capability of installations against attacks but also may change the attackers' strategies because of the intelligent character of the adversaries (Cox, 2009; Cox, 2008; Powell, 2007). Game theory has been suggested as a promising tool to analyze adversaries' strategies and optimize the defenders' response via optimal allocation of security resources (Liu et al., 2008; Reniers and Soudan, 2010; Rios and Insua, 2012; Tambe, 2011). Consequence analysis requires modeling the potential scenarios related to the attack, such as fires, explosions, and toxic material releases (Willis, 2007).

The above researches on security risk 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 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 (Abdolhamidzadeh et al., 2011; Cozzani et al., 2005; Darbra et al., 2010; Hemmatian et al., 2014; Khan and Abbasi, 1998, 2001) 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 a large amount of hazardous (e.g., flammable, explosive and toxic) substances. These hazardous installations situated next to each other may easily 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] (Reniers, 2010) should be considered in chemical security management.

Reniers et al. (2008) proposed integrating safety and security to prevent domino effects in chemical clusters. When eliminating terrorist groups and intentional attacks seems impossible, minimizing the potential consequences of intentional attacks can be considered as an effective approach to protect industrial plants against terrorist attacks (Reniers and Audenaert, 2014).

---

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

2

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) (Bagster and Pitblado, 1991; Necci et al., 2015; Reniers and Cozzani, 2013). Deliberate fires are more likely to lead to a more severe fire escalation because the possibility of several simultaneous primary fires at different locations exist (Chen et al., 2018). Installations involved in a domino effect are vulnerable at the beginning 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 all installations in chemical industrial parks should be considered due to possible domino effects caused by deliberate attacks. However, previous evolution models (Abdolhamidzadeh et al., 2010; Alileche et al., 2017; Kadri et al., 2013; Khakzad, 2015; Masum Jujuly et al., 2015) for domino effects may be too complex or time-consuming and not suitable for security analysis in chemical industrial parks with large numbers of installations.

The present study is aimed at establishing a consequence-based methodology 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 all installations that may be damaged by the spatial-temporal evolution of intentional attacks. The quantitative potential consequences of all 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.

The main steps of the methodology are outlined in Section 2. After presenting the foundations of dynamic graphs, the Dynamic Vulnerability Assessment Graph (DVAG) model is elaborated in Section 3. Case studies based on the methodology proposed in this study are presented in Section 4 to illustrate the methodology's application in a large chemical industrial park. Finally, the conclusions drawn from this work are presented in Section 5.

2. Methodology

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 methodology with a Dynamic Vulnerability Assessment Graph (DVAG) model is developed in the present study. The flow chart of the developed methodology is shown in Fig. 1. First,

all 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 all possible primary scenarios are identified. Step 3 conducts a vulnerability analysis using the DVAG model and obtains the damage possibilities of all installations. Finally, the potential consequences of all primary 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 be caused by intentional events.
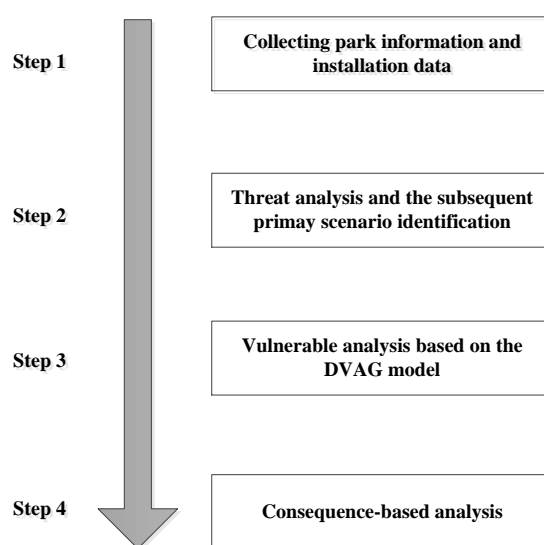

Fig. 1 Flow chart of the procedures developed for the consequence-based methodology.

2.1 Collecting park information and installation data

The first step of the methodology is to gather all the information and data needed to implement the consequence-based methodology 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 (API, 2013). 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 all possible primary scenarios caused by intentional events that may trigger domino effects. In this study, domino effects triggered by intentional events are categorized 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 an object 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 execute theses 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). 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 Commission, 2012). In chemical industrial parks, a vulnerability assessment should be conducted for all 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 all 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 all considered in the DVSG model based on dynamic graphs.

2.4 Consequence-based analysis

The consequence of intentional attacks in a chemical industrial park should include three aspects: economic loss, casualties, and environmental pollution. In this study, all possible damaged installations should be considered in the consequence analysis based on the vulnerability assessment results. Considering M intentional scenarios capable of triggering domino effects in a chemical park, the potential consequence caused by the m-th (m = 1, 2, 3, …, M) attack 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 m, in EUR; $CP_j^{\ m}$ is the conditional probability of installation j being damaged give an attack m; $L_j^{\ m}$ is the total consequence caused by the damage of installation j in attack m, in EUR; N is the number of installations in the park; $L_{j\_1}^{\ m}$ is the direct economic loss caused by installation j in attack m, in EUR; $L_{j\_2}^{\ m}$ is the loss of casualties caused by installation j in attack m, in EUR; $L_{j\_3}^{\ m}$ is the loss of environmental pollution caused by installation j in attack m, in EUR. The average potential consequence of all possible intentional attacks in a chemical industrial park, APC in EUR, is determined by Eq. (4). The average conditional probability of installation j being damaged of all possible intentional attacks, ACP_j, can be calculated according to Eq. (5).

$$APC = \frac{\sum_{j=1}^{m} PC^m}{m} \tag{4}$$

$$ACP_j = \frac{\sum_{m=1}^{M} CP_j^{\ m}}{m} \tag{5}$$

The average potential consequence (APC), and the average conditional probability of installations being damaged (ACP) are systematic indicators used to evaluate the overall effects of safety and security resources in a system (a chemical industrial area). Thus the likelihood difference of attacks is not considered in the two indicators.

3. Dynamic Vulnerability Assessment Graph (DVSG) 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 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: (Bondy and Murty, 1976; Casteigts et al., 2012; Harary and Gupta, 1997)

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 $\{v_i, v_j\}$ 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 (Harary and Gupta, 1997).

3.2 DVSG model

3.2.1 Definition

A Dynamic Vulnerability 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. The dynamic graph can be represented by Eq. (6).

$$G = (N, E, f, q) \tag{6}$$

(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. (7).

$$f = (S, Q, RTF, RTB, CPS, CP) \tag{7}$$

- 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.

Table 1 State description

State	Description	Marked color
Vulnerable	The installation is not physically damaged but it may receive heat radiations from other installations. The installation's temperature or internal pressure may increase in this state because of the received heat radiation.	Yellow
Harmful	The installation is on fire due to intentional events or the escalation from external installations. Installations in this state have a harmful impact on other installations receiving their heat radiations.	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

- 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. (8). The CPS can be decreased by taking security measures.

$$CPS = P(Success \,|\, Attack) \tag{8}$$

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. (9).

$$CP_i^m = CPS_i^m \tag{9}$$

(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. (10).

$$Q = \begin{bmatrix} 0 & q_{12} & \dots & q_{1n} \\ q_{21} & 0 & \dots & q_{2n} \\ \dots & \dots & 0 & \dots \\ q_{n1} & q_{n2} & \dots & 0 \end{bmatrix} \tag{10}$$

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. (11).

$$g = \begin{cases} 1 & \text{initial graph} \\ g+1 & \text{after a new update} \end{cases} \tag{11}$$

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. (12).

$$T^g = \begin{cases} 0 & g=1 \\ T^{g-1} + t^{g-1} & g>1 \end{cases} \tag{12}$$

- 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.

Fig. 2 State transition of installations

- Directed edge update

Directed edges connect installations in "harmful" states with all 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 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.

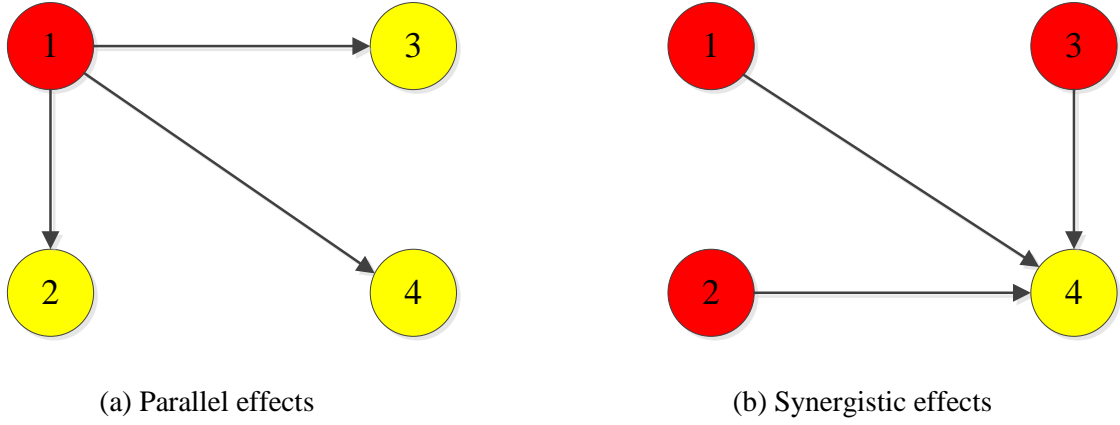(a) Parallel effects   (b) Synergistic effects

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

According to the synergistic effect model, the total heat radiation received by an installation j (Q_j) can be obtained, as shown in Eq. (13).

$$Q_j = \sum_{i=1}^{N} q_{ij} \tag{13}$$

The heat radiation received by each installation may vary over time due to new occurrences of harmful installations or dead installations. For update operations, all the potential heat radiation values between each pair of installations can be calculated by software such as ALOHA (ALOHA, 2016). In that case, an adjacency matrix of potential heat radiation (PQ) can be employed to represent all the potential heat radiation values, as shown in Eq. (14).

$$PQ = \begin{bmatrix} 0 & pq_{12} & \dots & pq_{1n} \\ pq_{21} & 0 & \dots & pq_{2n} \\ \dots & \dots & 0 & \dots \\ pq_{n1} & pq_{n2} & \dots & 0 \end{bmatrix} \tag{14}$$

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 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 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. (15).

$$q_{ij} = (1 - \eta \times \varphi) \times pq_{ij} \tag{15}$$

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 (Landucci et al., 2015).

- 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/m² (Cozzani et al., 2009)) at evolution time T_g, the *RTF* can be calculated by Eq. (16) (Landucci et al., 2009).

$$RTF_j^g = \frac{\exp\left(a \times V^b + c\ln(Q_j) + d\right)}{60} \tag{16}$$

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. So the RTF_j^g can be expressed as Eq. (17).

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

A conservative *TL* of 70 min (Landucci et al., 2015) 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* at the time T^{g+1} will be updated according to Eq. (18) (Chen et al., 2018).

$$RTF_j^{g+1} = \left(\frac{Q_j^{g+1}}{Q_j^g}\right)^c \cdot \left(RTF_j^g - t^g\right) \tag{18}$$

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

Table 2 The parameter value of *a*, *b*, *c,* and *d* adapted from Landucci et al. (2009).

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

(6) Residual time to burn out update

12

Assuming an installation i 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 obtained according to Eq. (19).

$$RTB_i^g = \frac{W_i}{v_i} \tag{19}$$

Where W_i is the mass of flammable substances in installation i, kg; v_i is the mass flow 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 $RTB_j^g > t^g$, 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. (20).

$$RTB_i^{g+1} = RTB_i^g - t^g \tag{20}$$

(7) Damage probability update

Emergency response is essential for eliminating possible escalation or mitigating the consequence of domino effects in the chemical industry (Zhou and Reniers, 2016). So the 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 (Landucci et al., 2009). 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. (21) (Chen et al., 2018).

$$\log ttc \sim N\left(u, \sigma^2\right) \tag{21}$$

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 (Chen et al., 2018). 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. (22). If installation j is the target of an attack m (i.e., $i = j$), the equation is equivalent to Eq. (9).

$$CP_j^m = CPS_i^m\left(1 - \text{LND}\left(T^g\right)\right) \tag{22}$$

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 all possible attacks. The flow diagram of the algorithm is reported in Fig. 4.
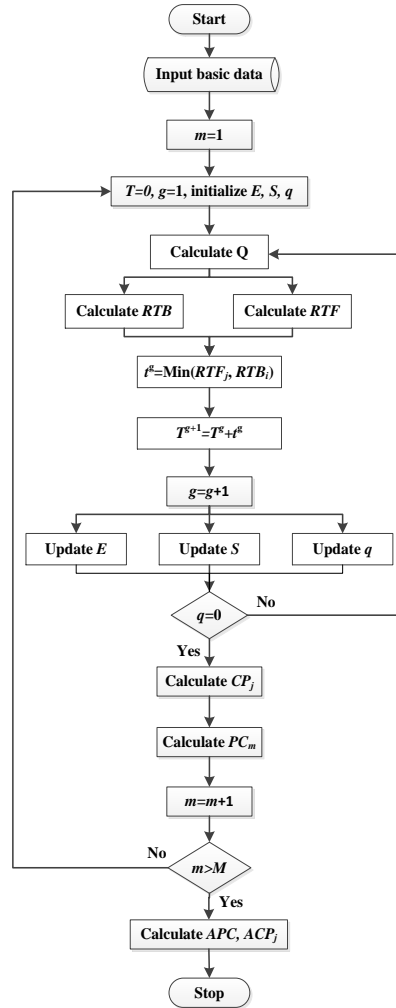

Fig. 4 Flow diagram of the algorithm for the DVAG model.

The algorithm is described and explained as follows. First, all basic data needed for performing the methodology 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 this 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 quantified 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 quickly using this algorithm. The 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 cases

Section 3 has elaborated the dynamic graph approach for vulnerability-consequence assessment of domino effects caused by intentional events and decision making on security measures and safety barriers. In this section, the developed methodology will be applied to two case studies.

4.1 Case 1: A single plant

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℃, wind blowing from the West with a speed of 1.5m/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., $\log ttc \sim \left(\mu, \sigma^2\right)$, the mean of *ttc* is equal to 10 min and the corresponding variance is equal to 2 min (Chen et al., 2018). Table 5 illustrates the identified primary scenarios caused by intentional events and the conditional probability of these primary scenarios given the intentional attack.
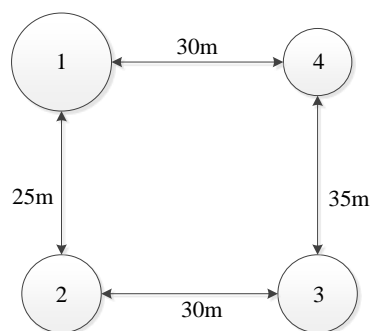

Fig. 5 Layout of an illustrative chemical storage plant (case 1)

Table 3 Features of chemical storage tanks

Tank	Type	Dimension	Chemical substance	Volume (m^3)	Chemical content (t)	Consequence (1,000 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

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

Using the consequence-based methodology proposed in this work, the failure time and failure probability of each tank following escalation caused by attacks are obtained, as shown in Table 6 and Table 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.

Table 6 The damage time of tanks (min).

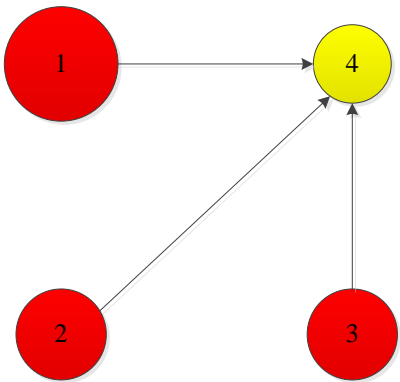| Tank	A1	A2	A3	A4
1	0	11.01	19.17	-
2	6.08	0	12.16	-
3	7.36	16.06	0	-
4	13.52	20.30	22.19	0

The evolution speed of primary scenario 1 is the fastest while that of the primary scenario 4 is the slowest. 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.
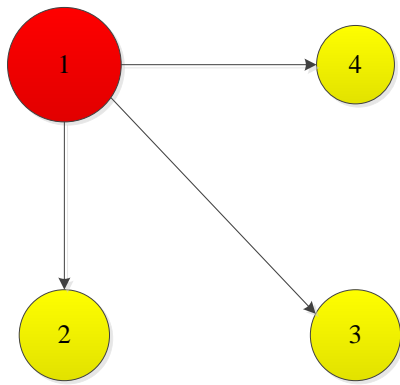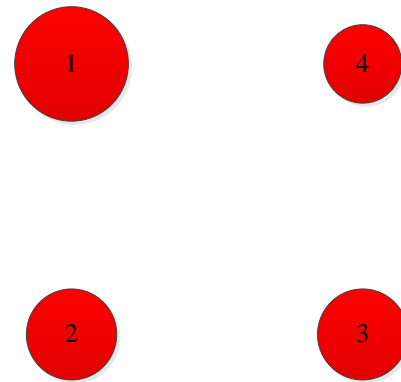
(a) Graph 1: $t = 0.00 \sim 6.08$ min
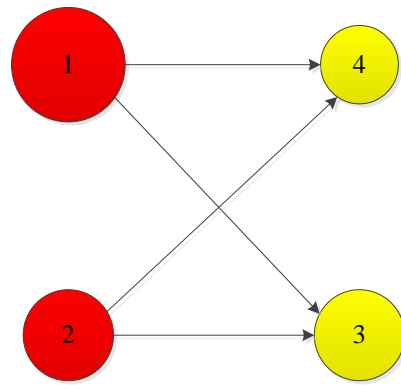
(b) Graph 2: $t = 6.08 \sim 7.36$ min

(c) Graph 3: $t = 7.36 \sim 11.25$ min

(d) Graph 4: $t = 13.52 \sim 247.42$ min

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

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

Table 8 shows the potential consequences of all attacks. The potential consequence of the attack on Tank 1 is much higher than that of other three attacks since the four tanks have a high probability to be damaged by the domino effects initiating 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*.

Table 8 The potential consequences of attacks

Primary scenario	A 1	A 2	A 3	A 4	Average
Potential consequence (1,000 EUR)	3092.5	1527.9	536.4	50.0	1301.7

Table 9 The potential consequences of attacks with additional protection measures

Additional measures	Potential consequence (1,000 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 (1,000 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%

In order to validate the methodology, the results are compared with the results of a static graph approach (Khakzad and Reniers, 2015). Employing the static graph methodology, the out-closeness metric reflects installations' potential contribution to the escalation of domino effect 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 15kW/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 methodology 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.
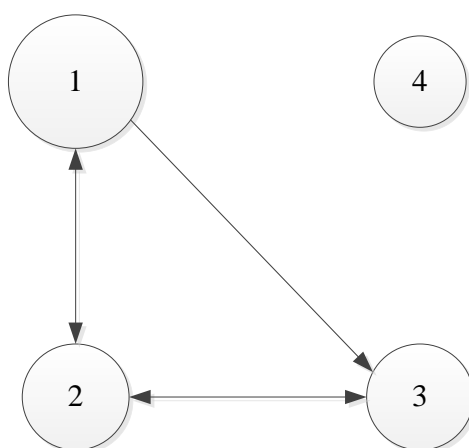

Fig.7 Static graph model of the chemical storage plant in case 1.

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

4.2 Case 2: A chemical cluster

A complex case is used to illustrate the application of the methodology to chemical industrial parks 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 successfully 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 5m/s and other parameters are the same as in Section 4.1.
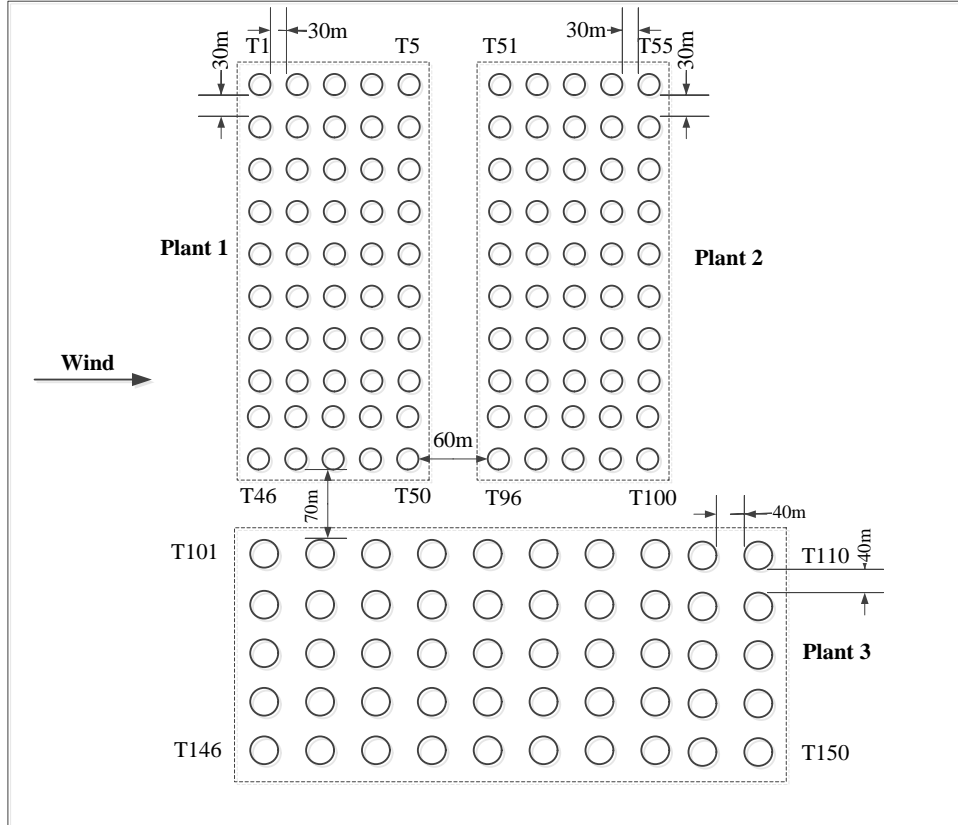

Fig. 8 The layout of three illustrative chemical storage plants within a chemical industrial park

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 (1,000 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

The potential consequences (*PC*) of the 150 attacks and the average conditional probability of installations being damaged (*ACP*) are quickly 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 escalation capability of the attacked installations while the *ACP* characters 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 in Plant 1 is 2.45×10^7 EUR (the attack at Tank 26), in Plant 2 it is 5.86×10^6 EUR (the attack at Tank 76), and in Plant 3 it is 1.92×10^7 EUR (the attack at 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 are 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 to reduce the *ACP*. For example, the average potential consequence 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).
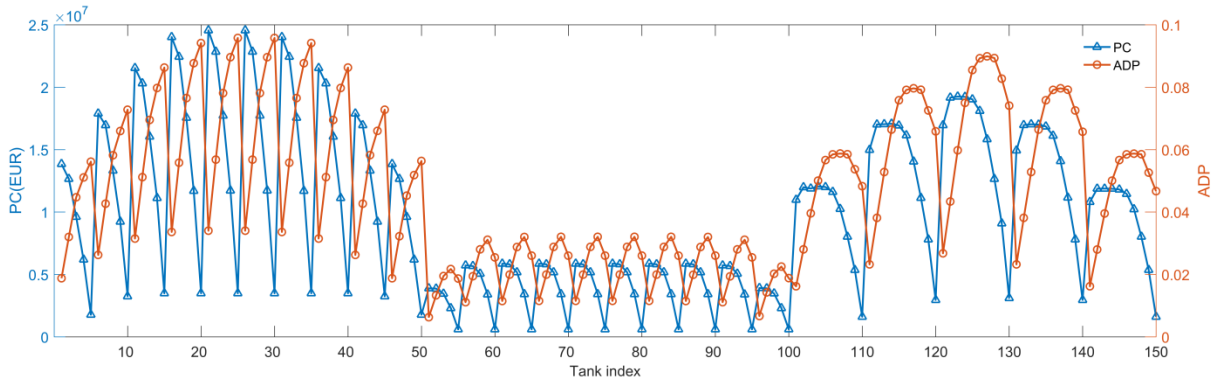
Fig. 9 The potential consequence (*PC*) and the average conditional probability (*ACP*) of each attack

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 the maximum probability of 0.13, and that in Plant 3 is 26.5 min with the 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.
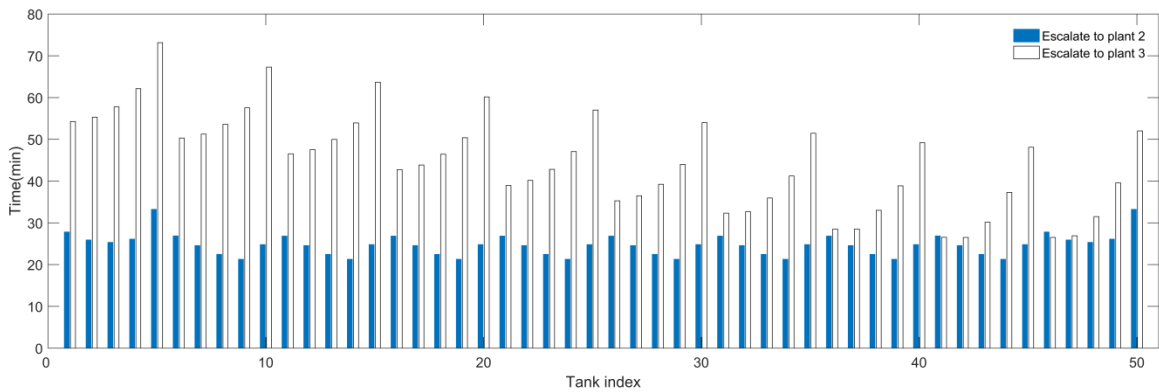

Fig. 10 The required time of external domino effects given an attack to one of the tanks in Plant 1.

5. Discussion

The case studies in section 4 indicate that our methodology can quickly obtain the quantitative results of consequences caused by intentional attacks in chemical industrial areas, considering all 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 the 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 and potential consequence 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 quickly 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 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). It should be remarked that this *PC*-based allocation rule is mainly suitable for the case that security information is limited or can't be easily obtained; otherwise, the adversaries' strategies may be considered.
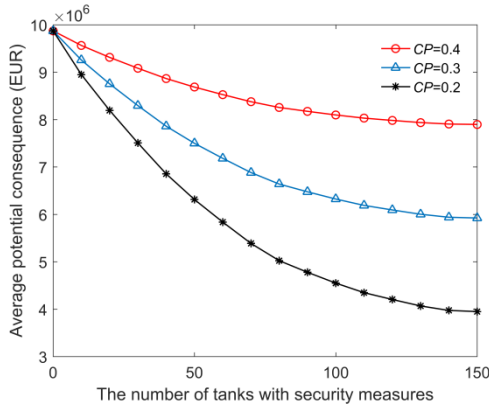
(a) Security measure allocation
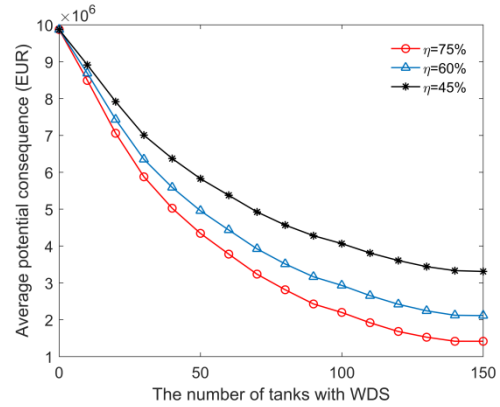
(b) WDS allocation

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

The *PC*-based allocation can also be applied to the allocation of safety barriers as shown in Fig.11(b). The *APC* decreases with 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. (15) 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 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.
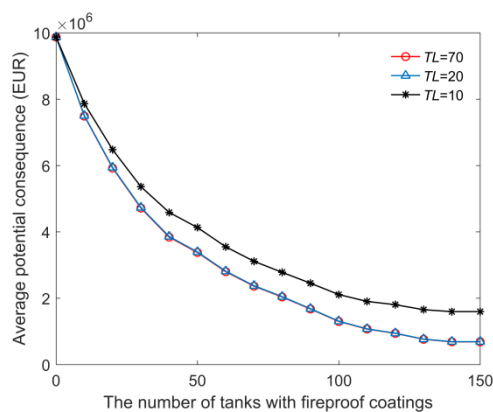
(a) fireproof coatings
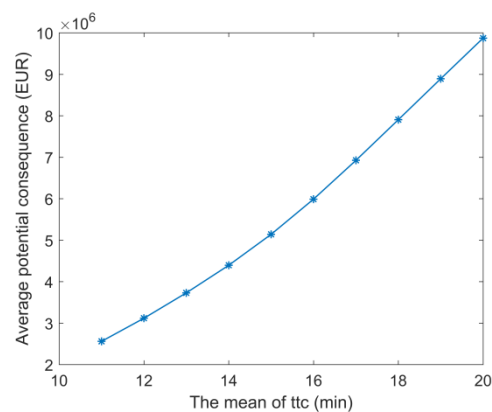
(b) Emergency response time

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

24

As mentioned above, the methodology 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 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 methodology 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 quantitative consequences of all 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.

Resource allocation recommendations for reducing the potential consequences of attacks may be proposed based on potential consequence-related indicators via two case studies, as follows: (i) Security measures and safety barriers should be allocated to installations with high potential consequences (*PC*), (i) 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 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 the advent of emergency response.

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.

References

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D., Abbasi, S.A., 2010. A new method for assessing domino effect in chemical process industry. J Hazard Mater 182, 416-426.

Abdolhamidzadeh, B., Abbasi, T., Rashtchian, D., Abbasi, S.A., 2011. Domino effect in process-industry accidents – An inventory of past events and identification of some patterns. Journal of Loss Prevention in the Process Industries 24, 575-593.

Alileche, N., Olivier, D., Estel, L., Cozzani, V., 2017. Analysis of domino effect in the process industry using the event tree method. Safety Science 97, 10-19.

ALOHA, 2016. US Environmental Protection Agency, National Oceanic and Atmospheric Administration, ALOHA, Version 5.4.7.

API, 2013. ANSI/API Standard 780 – Security risk assessment methodology for the petroleum and petrochemical industry. American Petroleum Institute.

API/NPRA, 2004. Recommended practice for security vulnerability assessment for petroleum and petrochemical facilities. 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., 2002. Assessing risks from threats to process plants: Threat and vulnerability analysis. Process Safety Progress 21, 269-275.

Baybutt, P., 2003. Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defence Journal 2.

Baybutt, P., 2017. Issues for security risk assessment in the process industries. Journal of Loss Prevention in the Process Industries 49, 509-518.

Bier, V.M., Nagaraj, A., Abhichandani, V., 2005. Protection of simple series and parallel systems with components of different values. Reliability Engineering & System Safety 87, 315-323.

Bondy, J.A., Murty, U.S.R., 1976. Graph theory with applications. Citeseer.

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., 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.

Cox, J.L.A., 2009. Game Theory and Risk Analysis. Risk analysis 29, 1062-1068.

Cox, L.A., Jr., 2008. Some limitations of "Risk = Threat x Vulnerability x Consequence" for risk analysis of terrorist attacks. Risk Anal 28, 1749-1761.

Cozzani, V., Gubinelli, G., Antonioni, G., Spadoni, G., Zanelli, S., 2005. The assessment of risk caused by domino effect in quantitative area risk analysis. J Hazard Mater 127, 14-30.

Cozzani, V., Tugnoli, A., Salzano, E., 2009. The development of an inherent safety approach to the prevention of domino accidents. Accid Anal Prev 41, 1216-1227.

Darbra, R.M., Palacios, A., Casal, J., 2010. Domino effect in chemical accidents: main features and accident sequences. J Hazard Mater 183, 565-573.

EU Commission, 2012. staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), Retrieved from. European Commission, Brussels.

Harary, F., Gupta, G., 1997. Dynamic graph models. Mathematical and Computer Modelling 25, 79-87.

Hemmatian, B., Abdolhamidzadeh, B., Darbra, R.M., Casal, J., 2014. The significance of domino effect in chemical accidents. Journal of Loss Prevention in the Process Industries 29, 30-38.

Kadri, F., Châtelet, E., Chen, G., 2013. Method for quantitative assessment of the domino effect in industrial sites. Process Safety and Environmental Protection 91, 452-462.

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., Reniers, G., 2015. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliability Engineering & System Safety 143, 63-73.

Khan, F.I., Abbasi, S., 1998. Models for domino effect analysis in chemical process industries. Process Safety Progress 17, 107-123.

Khan, F.I., Abbasi, S., 2001. An assessment of the likelihood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. Journal of Loss Prevention in the Process Industries 14, 283-306.

Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015. 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.

Lee, Y., Kim, J., Kim, J., Kim, J., Moon, I., 2010. Development of a risk assessment program for chemical terrorism. Korean Journal of Chemical Engineering 27, 399-408.

Liu, D., Wang, X., Camp, J., 2008. Game-theoretic modeling and analysis of insider threats. International Journal of Critical Infrastructure Protection 1, 75-80.

Masum Jujuly, M., Rahman, A., Ahmed, S., Khan, F., 2015. LNG pool fire simulation for domino effect analysis. Reliability Engineering & System Safety 143, 19-29.

Matteini, A., Argenti, F., Salzano, E., Cozzani, V., 2018. A comparative analysis of security risk assessment methodologies for the chemical industry. Reliability Engineering & System Safety.

Moore, D.A., Fuller, B., Hazzan, M., Jones, J.W., 2007. Development of a security vulnerability assessment process for the RAMCAP chemical sector. Journal of hazardous materials 142, 689-694.

Necci, A., Cozzani, V., Spadoni, G., Khan, F., 2015. Assessment of domino effect: State of the art and research Needs. Reliability Engineering & System Safety 143, 3-18.

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.

Powell, R., 2007. Defending against terrorist attacks with limited resources. American Political Science Review 101, 527-541.

Reniers, G., 2010. An external domino effects investment approach to improve cross-plant safety within chemical clusters. J Hazard Mater 177, 167-174.

Reniers, G., Cozzani, V., 2013. Domino Effects in the Process Industries, Modeling, Prevention and Managing. Elsevier, Amsterdam, The Netherlands.

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., Khakzad, N., Gelder, P.V., 2017. Security Risk Assessment: In the Chemical and Process Industry. De Gruyter, Berlin.

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.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.

Rios, J., Insua, D.R., 2012. Adversarial risk analysis for counterterrorism modeling. Risk analysis 32, 894-915.

Staalduinen, M.A.v., Khan, F., Gadag, V., 2016. SVAPP methodology: A predictive security vulnerability assessment modeling method. Journal of Loss Prevention in the Process Industries 43, 397-413.

Tambe, M., 2011. Security and game theory: algorithms, deployed systems, lessons learned. Cambridge University Press.

Willis, H.H., 2007. Guiding resource allocations based on terrorism risk. Risk Anal 27, 597-606.

Zhou, J., Reniers, G., 2016. Petri-net based modeling and queuing analysis for resource-oriented cooperation of emergency response actions. Process Safety and Environmental Protection 102, 567-576.