Integrated Safety and Security Management to Tackle Domino Effects

Chen, Chao; Reniers, Genserik; Yang, Ming

DOI
10.1007/978-3-030-88911-1_5

Publication date
2022

Document Version
Final published version

Published in
Integrating Safety and Security Management to Protect Chemical Industrial Areas from Domino Effects

Chapter 5
Integrated Safety and Security Management to Tackle Domino Effects

5.1 Introduction

A series of risk assessment methods for domino effects in the chemical industry are introduced in Chaps. 2, 3 and 4. These methods can model both unintentional domino effects and intentional domino effects.[1] To prevent and mitigate domino effects, domino effect management methods should be developed based on the results delivered by domino effect risk assessments. Previous work on domino effect management mainly focused on safety barriers management and land-use planning to prevent domino effects. Landucci et al. [3] explored the role of safety barriers in managing domino effects. Janssens et al. [4] developed an optimization method to allocate protective safety barriers and mitigate domino effects in chemical plants. Ghasemi and Nourai [5] optimized the spacing of storage tanks in land use planning for minimizing domino effect risks. Khakzad and Reniers [6] established a cost-effectiveness approach for the allocation of safety measures in chemical plants for land-use planning. These attempts on domino effect management aim to prevent and mitigate domino effects induced by unintentional events. However, the consequences of intentional domino effects may be more severe due to for instance simultaneous attacks on multiple chemical installations.

Besides safety barriers, security measures may also be used to prevent possible multiple primary scenarios. Process security in the chemical industry is a relatively new domain compared to process safety. The U.S. Department of Homeland Security identified the chemical sector as one of 16 critical infrastructures vulnerable to intentional attacks [7]. An increasing public concern raised the attention on process security after the terrorist attack in New York City on September 11, 2001 [8–12]. In 2003, the Center for Chemical Process Safety (CCPS) issued guidelines for analyzing and managing the security vulnerabilities of chemical industrial areas. The guidelines provide useful tools to industrial companies that deal with hazardous materials for

[1] This chapter is mainly based on two publications: Chen et al. [1] and Chen [2].

C. Chen et al., *Integrating Safety and Security Management to Protect Chemical Industrial Areas from Domino Effects*, Springer Series in Reliability Engineering,
https://doi.org/10.1007/978-3-030-88911-1_5

assessing and managing their risks caused by terrorists. A comprehensive approach was developed to integrate process security management and process safety management strategies. However, possible domino effects triggered by (unintentional or) intentional events were ignored in this document [13].

In 2004, the American Petroleum Institute (API) published a recommendation on security risk assessment for the petroleum and petrochemical industries [14]. This document provides a systematic security risk assessment (SRA) method based on threat, vulnerability, and consequence analysis. In 2013, the SRA method was revised by expanding functional utility [15]. According to the SRA method, the security risk is a function of threat, vulnerability, and consequence. Threat analysis is a considerable challenge since it requires a multitude of data and knowledge and modeling the motivations, intents, characteristics, capabilities, and tactics of adversaries [16, 17]. Vulnerability analysis requires a detailed understanding of the design and operation of installations and the threat information [18–20]. Security measures can improve the capability of installations against attacks but may change the attackers' strategies because of the intelligent character of the adversaries [21–23]. Consequently, Game theory was recognized as a promising tool for analyzing adversaries' strategies and optimizing the defenders' response via optimal allocation of security resources [24–27].

In terms of intentional domino effects, Reniers and Audenaert [28] proposed using safety barriers to mitigate the potential consequences of intentional attacks. However, the escalation caused by intentional events may be very difficult to prevent due to possible acceleration induced by synergistic effects. Consequently, integrating safety and security management may be a viable approach to deal with intentional and unintentional domino effects. However, there is a research gap to integrate safety and security management to prevent and mitigate domino effects in chemical industrial areas. This chapter, therefore, provides a framework to this end.

5.2 Safety and Security Management Principles

5.2.1 Inherent Safety and Security

In light of the severe consequences of the Flixborough disaster in 1974 and the Bhopal disaster in 1984, Kletz [29] proposed the concept of inherent safety or inherently Safer design (ISD) to make chemical plants safer. Unlike traditional plant designs that try to reduce the risk by adding protective equipment and following safety procedures, inherent safety aims to remove or reduce the hazards from the start, hence, by design. In terms of security, inherent safety also leads to the removal or reduction of threats. If hazards or threats are removed, no undesired events are possible and thus no subsequent domino effects are possible. Inherent security should thereby also reduce the attractiveness of assets belonging to chemical plants and therefore also remove or reduce threats. Kletz and Amyotte [30] proposed 10 inherent safety principles:

- **Intensification or minimization**: Reduction of the number and amount of hazardous materials in a chemical plant.
- **Substitution**: Substitution of a hazardous material by a safer one; For instance, a chemical plant can use a non-flammable material to replace a flammable material.
- **Attenuation**: attenuation of hazardous effects by using a hazardous material under safer conditions such as low temperature and low pressure.
- **Limitation of effects**: limitation of hazardous effects by changing designs (e.g., unit segregation design), operations, or reaction conditions.
- **Simplicity**: Simplicity of equipment, process, operations for reducing opportunities for errors and equipment failure.
- **Avoiding domino effects**: avoiding the escalation of major accidents by increasing layout spacing, providing firebreaks between sections, etc.
- **Making incorrect assembly impossible**: chemical plants should be designed to avoid incorrect assembly. For instance, a compressor valve should be designed to avoid incorrect assembly of inlet and exit valves.
- **Making status clear**: avoiding complicated equipment and overloading information and marking important information.
- **Tolerance of misuse**: tolerance of poor installation or operation without failure. For example, expansion loops are more tolerant of poor installation than bellows in the pipework.
- **Ease of control**: control by using physical principles rather than adding control equipment and avoidance of hands-on control [31].

The above principles are guidelines for an inherent safety (and security) design from a safety perspective. Some unique principles for inherent security are proposed in this book, as follows:

- **Reduction of attractiveness**: reduction of the assets that are attractive for adversaries;
- **Hidden attractive assets**: attractive assets should be located in hidden places or covered by other materials to make them difficult to be found.
- **Making the access of attractive assets difficult**: Attractive assets should be designed to be difficult to assess. For example, the control center is located far from the entrances.
- **Least privilege**: Each attractive asset or part of the digital system is designed with the privileges needed for its function to avoid multiple losses of assets or the failure of the whole digital system.

With the application of inherent safety and security design principles, it is expected to achieve fewer hazards, threats, fewer additional safety and security measures, fewer people to be exposed to hazardous effects, and fewer attractive assets to be exposed to threats.

5.2.2 *Layers/Rings of Protection*

CCPS [32] defined an independent protection layer (IPL) as a device, system, or action that can prevent a scenario from proceeding to undesired consequences, independent of the initiating event and other protection layers for the scenario. The concept of rings of protection (RoP) in the security domain defines a protection system as a series of independent protection rings [13]. It is similar to the layers of protection (LOP) used in chemical process plants for safety barrier management [33]. The concept of "Layers of Protection" is usually used for safety barrier management in chemical process plants [13] and the "Rings of Protection" for security are derived from this concept. A layer of protection analysis (LOPA) is a simple risk assessment method used for judging whether there are sufficient protection layers to control the risk of an undesired event.

Protection layers are independent of each other and not influenced by the likelihood or consequences of the initiating event [32]. The performance of a protection layer depends on the availability and effectiveness of safety barriers associated with the layer. Availability denotes the probability of failure on demand (PFD) of the safety barriers, while effectiveness is the probability that the safety barrier can prevent the scenario if it is successfully activated. Since no layer is perfectly effective, a scenario may require more than one protection layer depending on the process complexity and potential severity of a consequence [32]. For example, a pressure relief valve, a fire sprinkler system, a fireproofing coating, and a firefighting team may be simultaneously used for preventing fire escalation and failure of hazardous material vessels, as shown in Fig. 5.1. Each safety barrier in Fig. 5.1 is an independent protection layer. The escalation risk decrease with the increase of protection layers. If the protection layers are sufficient to prevent the escalation, no additional protection layers are needed. Otherwise, more protection layers should be implemented.

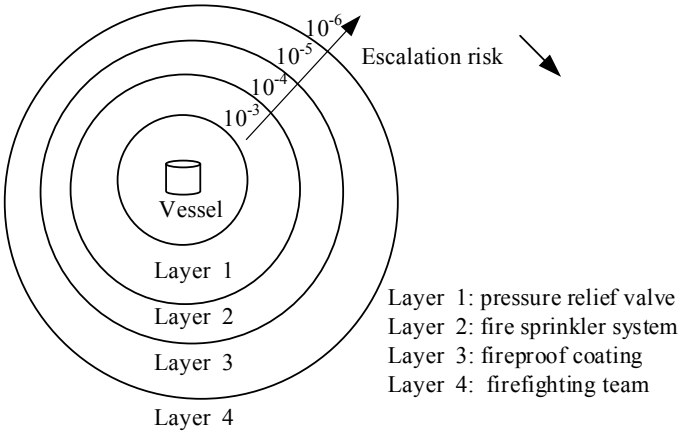

Fig. 5.1 Layers of protection: an illustrative example

If the risk tolerance criterion for domino effects is determined in a chemical plant, appropriate protection layers should be used to decrease the escalation risk below the tolerance criterion. Besides, the escalation risk can also be reduced by improving the availability and effectiveness of safety barriers in each layer.

In terms of security, the concept of "Rings of Protection" is also known as "Layered Defenses" and is based on the "Defense in Depth" principle [34]. Each defense layer consists of any device, system, or action that is capable of preventing the success of an attack. Appropriate defense layers need to be implemented in a chemical plant to protect critical assets. In terms of domino effects, critical installations may be defined as any hazardous facility with a high probability of initiating or propagating domino effects. If the current security risk is higher than the tolerance criteria, additional protection layers may be needed as attack prevention or mitigation measures. In chemical plants, security barriers such as a locked door and a fence can be considered to be preventive rings, while safety barriers such as a fire sprinkler that can prevent possible escalation caused by attacks may be regarded as mitigation rings.

According to the theory of protection rings, the most critical or vulnerable assets (e.g., the control room and hazardous material storage tanks) should be put into the center of concentric levels. In that case, an attack has to penetrate many defense rings, such as a fence, a locked exterior door, an alert receptionist, an elevator with key-controlled floor buttons, and a locked door [13]. It should be remarked that the defense against external attacks is less difficult than that against attacks within the company because internal attackers can easily bypass or penetrate part of the rings [35]. Unlike protection layers of safety barriers, the effectiveness of a protection ring constituting security measures is influenced by adversaries. If adversaries have the protection information of a chemical plant, they may use available means to lower the availability of protection rings. These means may for instance include using explosions to induce the failure of protection devices, releasing toxic gases to incapacitate all inhabitants of the control room, or bypass defense layers. As a result, defense rings should be robust, and the details of protection information may not be open to the public.

5.3 Integrated Safety and Security Management

5.3.1 Motivations for Integrating Safety and Security

According to the analysis in Sect. 5.2, both safety management and security management can be achieved by the inherent safety and security principles and the layers/rings of protection. In other words, both safety and security can be integrated into the design stage and operation stage in light of the intentional and unintentional threats associated with chemical plants. Safety barriers for preventing domino effects in process industries are generally divided into three categories: (i) active protection systems, (ii) passive protection systems, and (iii) emergency measures

[33, 36]. Previous researches on the management of domino effects mainly focus on accidental domino effects. Landucci et al. [37] developed a fault tree methodology to quantify the performance of safety barriers in fire-induced domino effects. Janssens et al. [4] developed an optimization model to allocate safety barriers for the sake of maximizing the *ttf* of chemical installations. Khakzad et al. [38] proposed a DBN approach for the performance assessment of fire protection systems during domino effects, taking into account the dynamic failure process of fireproofing coatings. Khakzad et al. [39] also developed an approach based on a limited memory influence diagram (LIMID) to multi-attribute decision analysis of safety measures. Advanced tools such as Petri-net and event sequence diagrams were applied to assess emergency response actions during fire-induced domino effects [40, 41].

A few attempts to manage intentional domino effects are based on securing critical installations or reducing potential consequences using safety barriers, ignoring the integration of safety barriers and security measures. Figure 5.2 shows the dependencies in the decision-making on safety and security resources, assuming the possibility of domino effects occurring after the allocation.

Safety barriers can prevent or mitigate accidental domino effects and also may have an impact on intentional domino effect scenarios. For instance, safety barriers may reduce the potential consequences of intentional events and decrease the attractiveness of chemical industrial areas. In terms of cross-plant areas, safety and security resources allocated in one chemical plant may lead to benefit of plants nearby due to the mitigation of possible external domino effects while it may also relatively increase the security risk of nearby plants because of the change of attractiveness. Therefore, safety and security resources should be integrated to prevent or mitigate

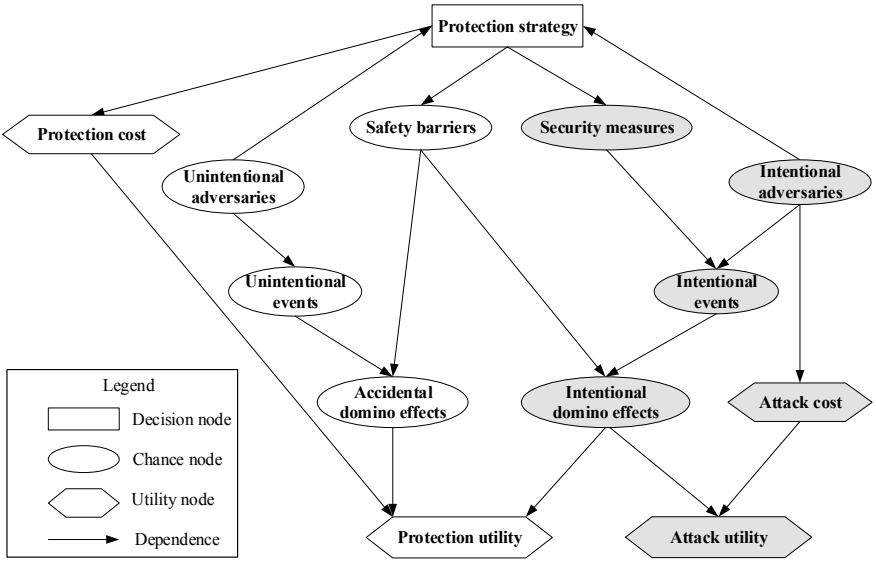

Fig. 5.2 The diagram for the allocation of safety and security resources

all possible domino effects caused by safety or security accident scenarios. In this book, "integrated safety and security measures" are called protection measures.

5.3.2 *Classification of Protection Measures*

In light of possible intentional and accidental domino effects, both safety and security measures may be used in domino effect management. A new classification of protection measures (safety or security measures) for preventing and mitigating domino effects in chemical industrial areas is proposed, as shown in Fig. 5.3.

According to their functions, protection measures are divided into three categories: detection measures, delay barriers, and emergency response actions. The three types of protection measures will be explained and elaborated below.

(1) **Detection measures**

Detection measures are used to detect intentional and unintentional abnormal events such as accidental releases and adversary actions and take the necessary actions to deal with them. The detection function consists of three sub-functions: (i) sensing, seeing, and discovering the problems (sensor), (ii) evaluating, assessing, and thinking about a solution for the problem (logic solution), and (iii) doing, acting, and carrying acts to solve the problem (actuator). A detection for an abnormal event is successful only when the functions are all there correctly executed. As a result, the detection performance depends on the probability that detection sensors or persons successfully

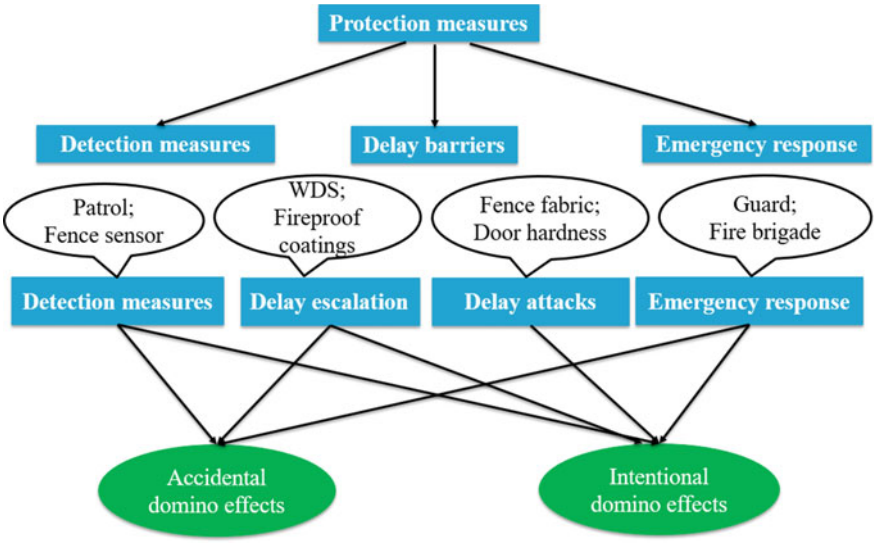

Fig. 5.3 Classification of add-on protection measures related to domino effect management

discover abnormal events, the probability that the alarm related to the events is successfully communicated, the probability that the alarm is successfully assessed and acted upon, and the time needed for the entire detection process (detection time) is adequate. An additional detection performance indicator is the nuisance alarm rate. A nuisance alarm is any alarm that is not caused by abnormal events. In an ideal detection system, the detection probability would be 1, and the nuisance alarm rate would be zero. However, in a chemical plant, all sensors interact with their environment, and they may be disturbed by other disturbances in their detection zones, such as vegetation, wildlife, and weather conditions. In a chemical plant, a typical detection system may consist of exterior and interior intrusion sensors, video alarm assessment, entry control, and alarm communication systems. Video alarm assessment is always conducted by closed-circuit television (CCTV) camera coverage of each sensor sector. An entry control system allows authorized personnel and material to get into and out of facilities while detecting and possibly prevent the access of unauthorized movements. Alarm communication aims to transport an alarm and information to a center and possibly present and assess the information [34, 42].

(2) **Delay barriers**

Delay barriers may be divided into two categories: delay attack measures and delay escalation measures. Delay attack measures are barriers that can increase the time in which an adversary needs to carry out an action, and such measures can thus delay the implementation of an attack. An adequate protection system first requires that the detection system successfully discovers the abnormal event. In that case, response force (e.g., guards, police) can prevent the attack when the alarm is correctly assessed and delivered to the response force. However, the start of an effective response force needs time. If the time is larger than the time required for completing the adversary attack, the response force would be ineffective, and the attack can not be prevented. As a result, after an adversary action is detected, delay measures are employed to delay the implementation of the attack until an adequate response force is available. Therefore, the response force can successfully interrupt the adversary attack before the attack goal is achieved only when the adversary is detected. The response force is available (active) before the attack is implemented [1, 42]. Delay escalation barriers are barriers to delaying the escalation of major accidents, such as fireproof coatings and water delivery systems. For example, fireproof coatings can block heat radiation transfer from the installation on fire to nearby installations exposed to the fire, increasing the time to failure (ttf) of the exposed installations [43, 44].

(3) **Emergency response**

Response force refers to any response personnel and measures involved in response to intentional attacks or hazardous scenarios in a chemical plant. As a result, emergency response in a chemical plant is essential to protect installations, the public, workers, and the environment. The response force may be on-site and offsite, including security guards, police, medical emergency teams, the fire brigade, etc. Guards and police may

be regarded as a preventive response that may prevent the completion of an attack if the attack is successfully detected. And if the delay measures provide enough time for the start of the response force. Medical emergency teams and fire brigades are used to mitigate the consequences of attacks. Protection of different targets may require response plans and the performance of response force depends on the threat types. For example, it is almost impossible to use security guards to prevent drone attacks. This is one reason why the drone attack on the Abqaiq oil plant in 2019 led to a 50% reduction in Abqaiq's oil production and a nearly 15% increase in the crude oil price [45]. Therefore, inherent safety and security, besides the add-on protection measures, is very important, and different chemical plants may also need additional protection strategies, and an effective protection strategy requires a reasonable arrangement of detection, delay, and response measures [1, 34, 42].

5.4 An Integrated Approach to Manage Domino Effects

This section develops an integrated management framework for preventing and mitigating intentional and unintentional domino effects. The procedures of the developed approach are shown in Fig. 5.4.

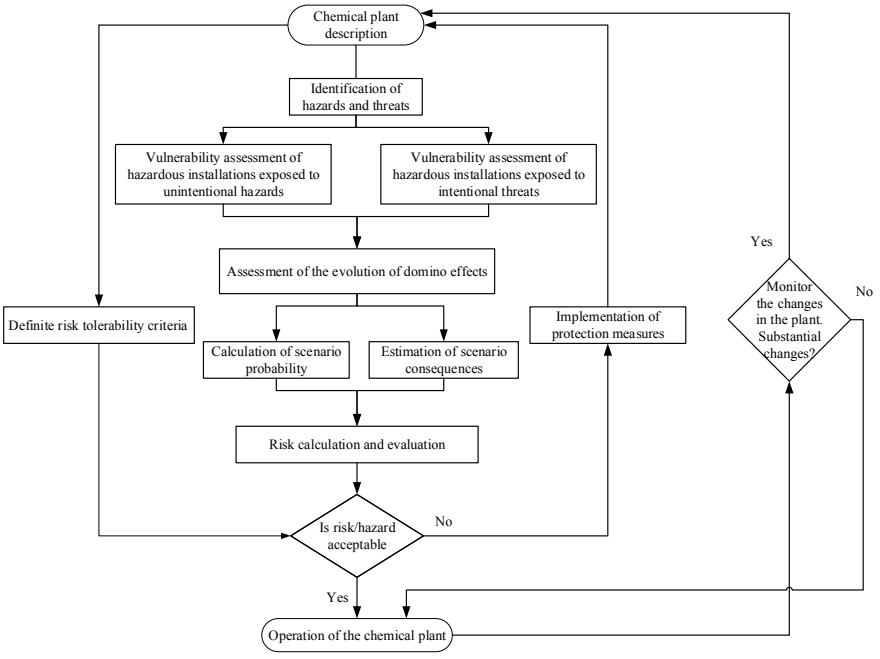

Fig. 5.4 Integrated management framework for domino effects

First, we need to collect all the data and information of a chemical plant related to risk assessment and management. Based on this information and data, possible intentional threats and hazards should be identified for the basis of vulnerability analysis. In this framework, vulnerability assessment should consider (i) the vulnerability of installations directly against threats and hazards and (ii) the vulnerability of installations subject to possible domino effects caused by intentional and unintentional events. Next, a consequence analysis should be conducted to obtain the possible consequences of domino effects. Furtherly, the domino effect risk is calculated and evaluated to judge whether risk reduction is needed by comparing it against the risk tolerability criteria. If the risk is higher than the criteria, risk reduction strategies (add-on safety and security measures) should be formulated.

5.4.1 Chemical Plant Description

In the first step, necessary data and information associated with the scope of the study need to be collected. The foremost necessary information and data are as follows:

- Plant information: The location of the chemical plant, the social, political, and economic environment around the chemical plant, nearby chemical plants or other critical infrastructures, products, etc.
- Layout information: Asset positions, distances between different installations, physical links between various installations, etc.
- Asset information: numbers, types, shapes, sizes, value, functions, materials, etc.
- Hazardous material information: types, quality, locations, hazardous characteristics, states (e.g., phase state, pressure, and temperature).
- Protection measures information: detection measures, delay measures, internal emergency response, and external emergency response.
- Meteorological data: temperature, wind direction, speed, humidity, etc.

5.4.2 Threat and Hazard Analysis

In terms of domino effects, this step needs to answer the question: what can induce primary scenarios? Since domino effects can be caused by intentional attacks and unintentional events, the step of threat and hazard analysis should identify both hazards and intentional threats (that is, the intentional issues of hazards), providing information and data for carrying out a vulnerability analysis.

Hazard identification in a chemical plant is to identify unintentional possible unwanted events leading to losses for people, property losses, and environmental damages, obtaining the weaknesses in the design and operation that could lead to hazardous material releases, fires, or explosions [46]. These hazards are always caused by the presence of hazardous materials or the processing conditions and hence, they belong to the field of “process safety”. The characteristics of hazards can be

flammability, combustibility, toxicity, corrosivity, radioactivity, etc. The processing conditions refer to hazardous physical conditions such as high temperature, high pressure, vibration, and liquid hammering and the strike [46]. These unintentional threats can be analyzed by widely used hazard identification methods such as the Hazard and Operability Study (HAZOP) method and the checklist method.

An intentional threat may be regarded as an indication, a circumstance, or an event that can lead to deliberate damage to humans, property and the environment, etc. [15]. Intentional threat analysis should identify possible threats and the attractiveness of installations to these threats. Intentional threat identification needs to collect information and data on potential threats, such as threat types, motivations, and weapons. The types of adversaries in chemical plants include terrorists, criminals, violent activities, deranged individuals, and disgruntled employees [13]. The motivations of threats may be the willingness to die, maximizing damage and casualties, inflicting psychological terror on the employees and public, and demonstrating the inability of the host company or country for instance [13]. Adversaries may take simple physical actions (e.g., opening valves, cutting electricity cables, and distorting production parameters), use simple arms (e.g., handguns, knives, and explosives), and exploit advanced weapons (missiles, drones, and nuclear weapons) to increase the likelihood of a successful attack and expand the consequences [13]. Adversaries may be internal adversaries, external adversaries, or internal adversaries working in cooperation with external adversaries, and they may be individuals or from groups, organizations, or governments. Threat analysis should consider as many adversaries as possible, such as intelligence services of host nations or third-party nations, political and terrorist groups, criminals, rogue employees, cybercriminals, and private interests [15]. Based on the information and data of adversaries, we can estimate the probability of threats, as shown in Table 5.1.

According to the identified threats, the attractiveness of assets to each threat should be determined to obtain the possibility of attack scenarios. The attractiveness of an asset may change with different threats. Consequently, the Expert should assess the attractiveness of each asset to each threat from the perspective of adversaries. According to various threats, one or more following factors [15] may be considered: (i) potential for mass casualties/fatalities; (ii) extensive property damage; (iii) proximity to national assets or landmarks; (iv) possible disruption or damage to critical infrastructure; (v) disruption of the national, regional, or local economy; (vi) ease of access to target; (vii) media attention or possible interest of the media; (viii) company reputation and brand exposure; (ix) vulnerability of installations exposed to attacks; (x) Potential for triggering domino effects. The potential for triggering domino effects is the main difference in attractiveness assessment between the chemical industry and other sectors without escalation effects. The domino effect potential assessment is a simple assessment of domino effects, and simple domino effect models are recommended, such as graph metrics [47]. According to graph theory, closeness metrics measure the centrality of a node in a network [48]. The out-closeness metric can reflect 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 [43]. The installation with a high out-closeness value has a

Table 5.1 SRA methodology for threat assessment (*Note* Adapted from API [15])

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

high potential to start domino effects, while the installation with a high in-closeness value is likely to be damaged by domino effects caused by other installations. Let's assume that adversaries expect to trigger a domino effect to induce severe consequences or indirectly damage installations with high in-closeness values. In that case, the installations with a high out-closeness value may be the targets.

Based on the above attractiveness analysis, the attractiveness of an asset to a threat represented by the likelihood that an installation is attacked by a threat can be determined based on the attractiveness levels shown in Table 5.2.

Table 5.2 Attractiveness evaluation table (API [15])

Attractiveness level	Likelihood L_A	Description
Very low	$0.0 \leq L_A < 0.2$	The threat would have little to no level of interest in the asset
Low	$0.2 \leq L_A < 0.4$	The threat would have some degree of interest in the asset, but it is not likely to be of interest compared to other assets
Medium	$0.4 \leq L_A < 0.6$	The threat would have a moderate degree of interest in the asset relative to other assets
High	$0.6 \leq L_A < 0.8$	The threat would have a high degree of interest in the asset relative to other assets
Very high	$0.8 \leq L_A \leq 1$	The threat would have a very high degree of interest in the asset, and it is a preferred choice relative to other assets

5.4.3 Vulnerability Assessment of Installations Against Direct and Threats

In this step, the vulnerability assessment aims to identify possible primary scenarios that may trigger domino effects and thus determine the probability of the primary scenarios caused by threats or hazards. The widely used risk assessment methods such as fault tree, event tree, and Bayesian network may be used to analyze possible primary scenarios caused by hazards and threats. In terms of the vulnerability of installations exposed to intentional attacks, it can be any weakness that may be exploited by an attacker to gain access to direct targets and to successfully execute an attack [15]. Before identifying primary scenarios caused by intentional attacks, we need to assess the likelihood that an attack is successfully carried out. In this chapter, the EASI model [42] is recommended to obtain the conditional probability that an attack is successfully carried out. According to the model, the likelihood depends on three parameters:

(1) The conditional probability that detected information is communicated to the emergency force. It depends on the training in communication equipment, maintenance, dead spot in radio communication, and the stress experienced during actual attacks [42].
(2) The conditional probability that an attack is detected on time. It depends on the attack path, detection measures along the path, and emergency response time. If the needed time for an attacker to pass the path between the detection position and the attack target is larger than the emergency response time, the attack is assumed to be interrupted. Otherwise, the attacker would reach the location of the target. To improve the likelihood of interrupting intentional attacks, the time the attacker is detected should be as early as possible. Besides, multiple detection measures may be implemented to increase the detection probability. Furthermore, delay measures may be used to delay the time that the attacker reaches the target and thus provide more time for the response of emergency force.
(3) The conditional probability that the attack is successfully executed when the adversary gets access to the target. It is determined by the performance that the attacker correctly uses the weapon and the reliability of the weapon [49].

5.4.4 Assessment of the Evolution of Domino Effects

Based on the vulnerability assessment method illustrated in Sect. 5.4.2, we can obtain all the primary scenarios that may induce domino effects. These primary scenarios can be intentional or unintentional. Besides, multiple failures may be present in one primary scenario. According to the primary scenarios, the graph-based models presented in Chaps. 2, 3 and 4 can be selected to analyze the possible subsequent domino effects and to calculate the failure probability of installations and the death

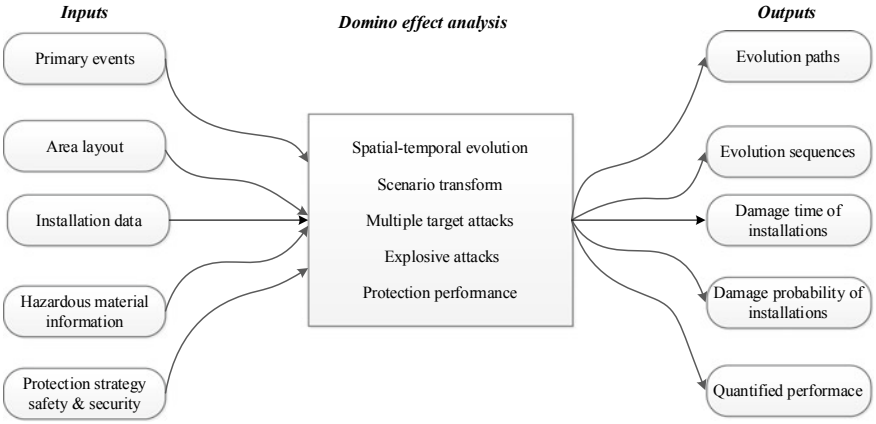

Fig. 5.5 The framework for domino effect analysis

probability of humans. The inputs and outputs of the domino effect analysis are shown in Fig. 5.5.

5.4.5 Consequence Analysis

Domino effects may result in many consequences, such as fatalities, economic losses, and environmental damage. Based on the consequence analysis method proposed by API [15], five categories of consequences are considered: (i) fatalities and injuries, (ii) property damage, (iii) environmental impacts, (iv) business interruption, (v) damage to reputation or negative publicity.

Loss of human life

Humans are vulnerable to toxic gas, heat radiation, overpressure, and fragments. Since the probability of humans dying from fragments is much lower than dying from the other harmful effects, we focus on the latter effects. In this chapter, therefore, the probit models for human vulnerability developed by TNO [50] are recommended to obtain the death probability caused by hazardous effects. For example, the acute intoxication of humans caused by a toxic gas is a function of the harmful effects of the toxic gas, the toxic gas concentration, and the exposure time. In terms of the death caused by overpressure, the vulnerability of humans exposed to heat radiation is also a dynamic process and depends on the exposure time, and the received heat radiation. For the damage caused by heat radiation, the superimposed effects may be considered since the heat radiation received by humans may vary with the number of hazardous installations being on fire during the spatial–temporal evolution of hazards.

Property damage

The property damage caused by domino effects in a chemical plant should account for all possible damaged installations based on the results obtained from the vulnerability assessment and domino effect analysis. The property damage is always monetarized as the cost of lost property [51].

Business loss

The business loss is related to the operation interruption of the chemical plant caused by domino effects, and the interruption time can be used as an indicator of business loss [15].

Environmental damage

Besides the damage to humans, property, and business, environmental impacts are not neglected. Spills of hazardous materials may cause damage to the environment, indirectly affecting the population, plants, and animals by contaminating land, surface water, and groundwater [52]. A certain period of time is needed for the recovery of the environment. As a result, the damage to the environment may be assessed by the time needed to recover [15].

Reputation or negative publicity

The damage to reputation or negative publicity is challenging to evaluate. Some indirect indicators may be used to determine it, such as the degree of loss of reputation or business viability, the attention of regulatory agencies, and the report of media [15].

According to the above analysis, a consequence evaluation table can be obtained, as shown in Table 5.3.

For instance, the damage to two above-ground gasoline tanks in a decked area can lead to on-site injuries that are not widespread but only in the vicinity of the incident location (low); over €1 billion to €10 million loss in property damage (medium); minor environmental impacts to immediate incident site area only, less than 1 year to recover (low); Short-term (>2 weeks to 3 months) business interruption/expense (low); and a medium loss of reputation or business viability (medium). Since two types of consequences are in the medium level, the total consequence level is medium.

5.4.6 Risk Evaluation

To determine whether measures need to be taken to reduce domino effect risks, risk evaluation should be conducted based on the likelihood and consequence of domino effects. To make it more user-friendly, a risk matrix is recommended, as shown in Fig. 5.6. According to the risk attitude of decision-makers, the risk threshold

Table 5.3 Consequence evaluation table (API [15])

Consequence level	Description (already look at the worst-case parameters)
Very low	(i) Possibility of minor injury on-site; no fatalities or injuries anticipated off-site (ii) Up to €X loss in property damage (iii) No environmental impacts (iv) Very short-term (up to X weeks) business interruption/expense (v) Very low or no impact or loss of reputation or business viability; mentioned in the local press
Low	(i) On-site injuries that are not widespread but only in the vicinity of the incident location; no fatalities or injuries anticipated off-site (ii) €X to €X loss in property damage (iii) Minor environmental impacts to immediate incident site area only, less than X year(s) to recover (iv) Short-term (>X week to Y months) business interruption/expense (v) Low loss of reputation or business viability; query by the regulatory agency; significant local press coverage
Medium	(i) Possibility of widespread on-site serious injuries; no fatalities or injuries anticipated off-site (ii) Over €X to €X loss in property damage (iii) Environmental impact on-site and/or minor off-site impact, Y year(s) to recover (iv) Medium-term (Y to Z months) business interruption/expense (v) Medium loss of reputation or business viability; attention of regulatory agencies; national press coverage
High	(i) Possibility of X to Y on-site fatalities; the possibility of off-site injuries (ii) Over €X to €X loss in property damage (iii) Tremendous environmental impact on-site and/or large off-site impact, between Y and Z years to recover (iv) Long-term (X to Y years) business interruption/expense (v) High loss of reputation or business viability; prosecution by the regulator; extensive national press coverage
Very high	(i) Possibility of any off-site fatalities from large-scale toxic or flammable release; possibility of multiple on-site fatalities (ii) Over €X loss in property damage (iii) Major environmental impact on-site and/or off-site (e.g., large-scale toxic contamination of public waterway), more than XX years/poor chance of recovery (iv) Very long-term (>X years) business interruption/expense; large-scale disruption to the national economy, public or private operations; loss of critical data (v) Very high loss of reputation or business viability; international press coverage

* X, Y, Z, and XX are variables that users should determine

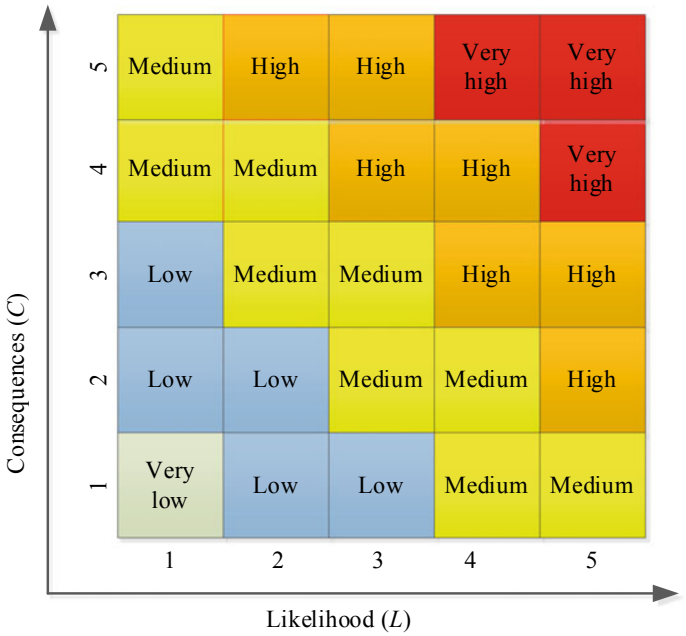

Fig. 5.6 Risk matrix for domino effect risk evaluation (to be filled in based on Tables 5.2 and 5.3)

may differ. If the obtained risk is lower than the threshold, the risk is acceptable; otherwise, add-on risk reduction measures may be taken to make the risk lower than the threshold.

5.4.7 Risk Treatment

Risk treatment is an essential step in the integrated management framework, focusing on selecting and implementing appropriate measures to deal with domino effect risk. The common-used risk treatment strategies include risk retention, risk avoidance, risk reduction, risk transfer [51]. One or more risk treatment strategies may be selected according to distinctive risk evaluation results and the preferences of decision-makers.

If the domino effect risk of a chemical plant is lower than the risk tolerability criteria, a risk retention strategy may be adopted. Based on the risk retention strategy, the chemical plant will accept the domino effect risk and be prepared if a domino effect occurs. If the domino effect risk of a chemical plant exceeds the tolerability threshold, the risk is unacceptable and risk treatment strategies such as risk avoidance, risk reduction, and risk transfer may be taken to make the risk lower than the threshold. The following risk treatment possibilities exist:

(1) **Risk avoidance**

In terms of domino effect risks, risk avoidance may refer to the inherent safety and security measures. For instance, using less hazardous or attractive materials and processes can reduce or eliminate hazards and threats and thus decreases the likelihood of primary scenarios. Besides, changing the design of plant layout (e.g., providing ample layout spacing) or operations (e.g., reducing the hazardous material unloading velocity) may limit the hazardous effects of escalation so as to lower the escalation potential. Other inherent safety and security measures are shown in Sect. 5.2.1.

(2) **Risk reduction**

Risk reduction can be needed and it is determined by additional protection measures, decision in ideally influenced by the performance of the used protection measures [44]. For example, we can install additional detection sensors to improve the detection probability of abnormal events (unintentional events and intentional events) and provide more time for the initiation of emergency response, thus decreasing the domino effect risk. Besides, delay measures such as fireproof coatings can be used to prevent fire-induced escalation, and fences may be used to delay intentional attacks originating from outside the chemical plant. Furthermore, emergency response forces may be improved to shorten the time needed to respond to an abnormal event and enhance the capability to control adversaries and accident scenarios. Besides the risk reduction performance of protection measures, the costs of protection measures may also be considered in the decision-making on risk protection strategies since there is always a budget for the investment of safety and security. After implementing protection measures, a risk assessment should be conducted again to check whether the reduced risk is satisfactory.

(3) **Risk transfer**

Risk transfer aims to shift the risk to another party. Insurance is a typical risk transfer measure in which a specified risk is transferred from a chemical plant to the insurer by purchasing insurances [53]. In that case, if a domino effect event occurs, the insurance company pays the cost. However, the risk is not reduced by the insurance. Usually, the company can only get an economic income from the insurance company to compensate for a name of different losses. In terms of security risk, risk transfer may occur without any intentional actions. For example, a chemical plant invests in protection measures to prevent intentional attacks while the nearby chemical plants in the chemical cluster do not take any protection measures. In that case, the adversary of the chemical cluster may aim to attack the chemical companies without protection measures, resulting in a risk transfer from the plant with protection measures to the plant without protection measures.

5.5 Conclusions

In this chapter, an integrated domino effect management framework is developed to tackle the possible domino effects caused by intentional threats or hazards. According to this framework, safety and security measures should be integrated to avoid possible overlaps. Besides, both intentional threats and unintentional hazards should be identified to prevent underestimating the domino effect risk. The vulnerability assessment is divided into two parts: the vulnerability of installations directly against hazards and attacks and the vulnerability of installations exposed to possible domino effects. Consequence analysis accounts for fatalities, property loss, environmental impacts, business loss, and reputation or negative publicity. Finally, the domino effect risk can be calculated and evaluated to determine whether the risk is acceptable. If the risk is unacceptable, additional protection measures should be taken until the risk is lower than the pre-defined risk tolerability criteria. Based on the framework, decision-making approaches such as cost-effectiveness analysis and cost–benefit analysis can be developed to obtain optimal protection strategies.

References

1. Chen C, Reniers G, Khakzad N (2020) Cost-benefit management of intentional domino effects in chemical industrial areas. Process Saf Environ Prot 134:392–405
2. Chen C (2021) A dynamic and integrated approach for modeling and managing domino-effects. Delft University of Technology
3. Landucci G, Argenti F, Spadoni G, Cozzani V (2016) Domino effect frequency assessment: the role of safety barriers. J Loss Prev Process Ind 44:706–717
4. Janssens J, Talarico L, Reniers G, Sörensen K (2015) A decision model to allocate protective safety barriers and mitigate domino effects. Reliab Eng Syst Saf 143:44–52
5. Ghasemi AM, Nourai F (2017) A framework for minimizing domino effect through optimum spacing of storage tanks to serve in land use planning risk assessments. Saf Sci 97:20–26
6. Khakzad N, Reniers G (2017) Cost-effective allocation of safety measures in chemical plants w.r.t land-use planning. Saf Sci 97:2–9
7. Reniers G, Khakzad N, Gelder PV (2017) Security risk assessment: in the chemical and process industry. De Gruyter, Berlin
8. Baybutt P (2002) Assessing risks from threats to process plants: threat and vulnerability analysis. Process Saf Prog 21(4):269–275
9. Baybutt P (2003) Strategies for protecting process plants against terrorism, sabotage and other criminal acts. Homeland Defence J 2(1)
10. Bier VM, Nagaraj A, Abhichandani V (2005) Protection of simple series and parallel systems with components of different values. Reliab Eng Syst Saf 87(3):315–323
11. Reniers G, Dullaert W, Audenaert A, Ale BJ, Soudan K (2008) Managing domino effect-related security of industrial areas. J Loss Prev Process Ind 21(3):336–343
12. Lee Y, Kim J, Kim J, Kim J, Moon I (2010) Development of a risk assessment program for chemical terrorism. Korean J Chem Eng 27(2):399–408
13. CCPS (2003) Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites. American Institute of Chemical Engineers
14. American Petroleum Institute (API) (2004) Recommended practice for security vulnerability assessment for petroleum and petrochemical facilities. American Petroleum Institute

15. API (2013) ANSI/API Standard 780—security risk assessment methodology for the petroleum and petrochemical industry. American Petroleum Institute
16. Baybutt P (2017) Issues for security risk assessment in the process industries. J Loss Prev Process Ind 49:509–518
17. Paté-Cornell E, Guikema S (2002) Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Mil Oper Res 7(4):5–23
18. Staalduinen MAv, Khan F, Gadag V (2016) SVAPP methodology: a predictive security vulnerability assessment modeling method. J Loss Prevent Process Indus 43:397–413
19. Moore DA, Fuller B, Hazzan M, Jones JW (2007) Development of a security vulnerability assessment process for the RAMCAP chemical sector. J Hazard Mater 142(3):689–694
20. Matteini A, Argenti F, Salzano E, Cozzani V (2018) A comparative analysis of security risk assessment methodologies for the chemical industry. Reliab Eng Syst Saf
21. Cox JLA (2009) Game theory and risk analysis. Risk Anal 29(8):1062–1068
22. Cox LA Jr (2008) Some limitations of "Risk = Threat x Vulnerability x Consequence" for risk analysis of terrorist attacks. Risk Anal 28(6):1749–1761
23. Powell R (2007) Defending against terrorist attacks with limited resources. Am Politi Sci Rev 101(3):527–541
24. Reniers G, Soudan K (2010) A game-theoretical approach for reciprocal security-related prevention investment decisions. Reliab Eng Syst Saf 95(1):1–9
25. Rios J, Insua DR (2012) Adversarial risk analysis for counterterrorism modeling. Risk Anal 32(5):894–915
26. Tambe M (2011) Security and game theory: algorithms, deployed systems, lessons learned. Cambridge University Press
27. Liu D, Wang X, Camp J (2008) Game-theoretic modeling and analysis of insider threats. Int J Crit Infrastruct Prot 1:75–80
28. Reniers GLL, Audenaert A (2014) Preparing for major terrorist attacks against chemical clusters: Intelligently planning protection measures w.r.t. domino effects. Process Saf Environ Protect 92(6):583–589
29. Kletz TA (2003) Inherently safer design—its scope and future. Process Saf Environ Prot 81(6):401–405
30. Kletz TA, Amyotte P (2010) Process plants: a handbook for inherently safer design. CRC Press
31. Khan FI, Amyotte PR (2003) How to make inherent safety practice a reality. Canad J Chem Eng 81(1):2–16
32. CCPS (2001) Layer of protection analysis: simplified process risk assessment. AIChE–CCPS, New York
33. CCPS (2011) Layer of protection analysis: simplified process risk assessment. American Institute of Chemical Engineers—Center of Chemical Process Safety, New York
34. Reniers G, Van Lerberghe P, Van Gulijk C (2015) Security risk assessment and protection in the chemical and process industry. Process Saf Prog 34(1):72–83
35. Reniers G, Landucci G, Khakzad N (2020) What safety models and principles can be adapted and used in security science? J Loss Prevent Process Indus 64
36. De Dianous V, Fievez C (2006) ARAMIS project: a more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. J Hazard Mater 130(3):220–233
37. Landucci G, Argenti F, Tugnoli A, Cozzani V (2015) Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab Eng Syst Saf 143:30–43
38. Khakzad N, Landucci G, Reniers G (2017) Application of dynamic Bayesian network to performance assessment of fire protection systems during domino effects. Reliab Eng Syst Saf 167:232–247
39. Khakzad N, Landucci G, Cozzani V, Reniers G, Pasman H (2018) Cost-effective fire protection of chemical plants against domino effects. Reliab Eng Syst Saf 169:412–421
40. Zhou J, Reniers G, Khakzad N (2016) Application of event sequence diagram to evaluate emergency response actions during fire-induced domino effects. Reliab Eng Syst Saf 150:202–209

41. Zhou J, Reniers G (2018) Petri-net based evaluation of emergency response actions for preventing domino effects triggered by fire. J Loss Prev Process Ind 51:94–101
42. Garcia ML (2007) Design and evaluation of physical protection systems. Elsevier
43. Chen C, Reniers G, Khakzad N (2019) Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach. Reliab Eng Syst Saf 191
44. Chen C, Reniers G, Khakzad N (2020) A thorough classification and discussion of approaches for modeling and managing domino effects in the process industries. Saf Sci 125
45. Chen C, Li C, Reniers G, Yang F (2021) Safety and security of oil and gas pipeline transportation: a systematic analysis of research trends and future needs using WoS. J Cleaner Product 279
46. CCPS (1992) Guidelines for hazard evaluation procedures, 2nd edn. American Institute of Chemical Engineers, New York
47. Khakzad N, Landucci G, Reniers G (2017) Application of graph theory to cost-effective fire protection of chemical plants during domino effects. Risk Anal 37(9):1652–1667
48. Freeman LC (1978) Centrality in social networks conceptual clarification 1(3):215–239
49. Stewart MG, Mueller J (2012) Terror, security, and money: balancing the risks, benefits, and costs of critical infrastructure protection, pp 513–533
50. Van Den Bosh C, Merx W, Jansen C, De Weger D, Reuzel P, Leeuwen D, Blom-Bruggerman J (1989) Methods for the calculation of possible damage (Green Book). Committee for the Prevention of Disasters, The Hague, NL
51. Reniers GL, Van Erp HN (2016) Operational safety economics: a practical approach focused on the chemical and process industries. Wiley
52. Bonvicini S, Antonioni G, Cozzani V (2018) Assessment of the risk related to environmental damage following major accidents in onshore pipelines. J Loss Prev Process Ind 56:505–516
53. Abrahamsen EB, Asche F (2010) The insurance market's influence on investments in safety measures. Saf Sci 48(10):1279–1285