Economic model for tackling intentional domino effects in a chemical facility

Chen, Chao; Reniers, Genserik

DOI
10.1016/B978-0-08-102838-4.00005-5

Publication date
2021

Document Version
Final published version

Published in
Dynamic Risk Assessment and Management of Domino Effects and Cascading Events in the Process Industry

Citation (APA)
Chen, C., & Reniers, G. (2021). Economic model for tackling intentional domino effects in a chemical facility. In *Dynamic Risk Assessment and Management of Domino Effects and Cascading Events in the Process Industry* (pp. 193-222). Elsevier. https://doi.org/10.1016/B978-0-08-102838-4.00005-5

CHAPTER NINE

Economic model for tackling intentional domino effects in a chemical facility

Chao Chen[1], **Genserik Reniers**[1,2,3]
[1]Safety and Security Science Group, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, the Netherlands
[2]Faculty of Applied Economics, Antwerp Research Group on Safety and Security (ARGoSS), University Antwerp, Antwerp, Belgium
[3]CEDON, KULeuven, Campus Brussels, Brussels, Belgium

Contents

Dynamic Risk Assessment and Management of Domino Effects and Cascading Events in the Process Industry. ISBN: 978-0-08-102838-4
https://doi.org/10.1016/B978-0-08-102838-4.00005-5

9.1 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; Bier et al., 2005; Reniers et al., 2008). Different from other critical infrastructures, chemical industrial facilities 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 be exploited by terrorists to trigger domino effects. In that case, the consequences are more severe than that of the primary attack event. Compared with accidental domino effects, intentional domino effects may induce severer consequences since simultaneous damages of installations are more likely to be induced by multiple target attacks. For example, three tanks in a French chemical plant were attacked via explosive devices in July 2015, inducing two simultaneous tank fires (BBC News, 2015). Besides, tackling intentional domino effects has to face intelligent and strategic adversaries besides the uncertainty (or randomness) and complexity in the evolution of domino effects. An overview of the definitions and characteristics of accidental domino effects and intentional domino effects is given in Table 9.1.

Economics reminds us that protection resources are always limited and the resources allocated to one target are not available for others (Poole, 2008). Economic analysis can facilitate the investment in prevention and may avoid loss costs, increasing profitability and to be a business strategy leading to long-term profitability and to sustainable and intrinsically healthy organizations (Reniers and Van Erp, 2016). Economic models therefore are usually used to optimize the allocation of protection resources so as to maximize the protection effectiveness, such as the prevention investment decision model based on cost—benefit analysis (CBA) (Reniers and Sorensen, 2013b; Villa et al., 2017) and the domino mitigation model in

Table 9.1 Comparison of the definitions and main characteristics between accidental domino effects and chemical technology (incomplete enumeration).

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

view of cost-effectiveness analysis (Janssens et al., 2015). Besides the application in resource allocation, economic models of terrorism can provide insights into the motivation and strategy behind terrorists from economic perspectives (Blomberg et al., 2004; Brück, 2007; Hausken, 2018).

Although economic issues of risk may only be one part of risk management, it has a great impact on the effectiveness of a company's prevention policy as well as the company's profitability in the long term (Reniers and Van Erp, 2016). Moreover, economic analysis may be more important when it comes to security management since an attack's costs and benefits are an unavoidable issue for terrorists as well, affecting the attacker's strategies and the likelihood of successful attacks. However, using economic models to tackle intentional domino effects is not an easy work. It is challenging to estimate the overall losses caused by domino effects in chemical industrial areas due to the complexity and uncertainty in the escalation evolution. In addition, it is difficult to assign a monetary value to certain aspects of symbolic, political, and economic prestige caused by intentional events.

In light of this, this chapter aims to prevent or mitigate intentional domino effects in chemical industrial facilities by using economic models, addressing economic issues in the decision-making process and making the protection to be more profitable. First, we introduce economic foundations that may be used to tackle intentional domino effects. Second, we expound on threat analysis and vulnerability assessment in order to obtain the threat probability, possible attack scenarios, and the success probability of attacks. Besides the vulnerability assessment of installations directly against attacks, a dynamic graph approach is presented in Section 9.4 to assess the vulnerability of installations subject to intentional domino effects. A CBA on the basis of threat and vulnerability analysis is elaborated in Section 9.5. Section 9.6 develops a cost-effectiveness analysis to achieve the most cost-effective protection strategy within budget constraints. Finally, conclusions drawn from this work are presented in Section 9.7.

9.2 Economic foundations

In economics, microeconomics focuses on the decision-making of individual economic units from an economic and rational viewpoint (Reniers and Van Erp, 2016). This section thus introduces some widely used microeconomic tools that may be implemented in risk management of intentional domino effects, including CBA, cost-effectiveness analysis, Stackelberg leadership, and the law of diminishing returns.

9.2.1 Cost–benefit analysis

A CBA is a systematic and analytical evaluation process of comparing benefits and costs in the same units, usually money. Although the CBA cannot demonstrate whether one safety or security investment is intrinsically better than another, a CBA allows decision-makers to improve their decisions by adding appropriate information on costs and benefits to certain prevention or mitigation investment decisions. An investment is recommended when the total net present value (NPV) of all cash flows is positive, and an investment is usually rejected when the NPV is negative. Therefore the NPV can be an indicator for assessing investment strategies (Quah and Haldane, 2007; Reniers and Van Erp, 2016).

9.2.2 Cost-effectiveness analysis

Cost-effectiveness analysis is to work out the best allocation strategy in available strategies, to maximize the quantity or quality of safety or security. Different from a CBA, the approach gives an idea of whether an investment is "affordable" or not rather than an optimal investment. A cost-effectiveness analysis does not strictly require the monetization of benefits, but always needs to compute cost-effectiveness ratios (CERs) and use these ratios to select strategies that are most effective (Reniers and Van Erp, 2016).

9.2.3 Stackelberg leadership

The Stackelberg leadership model (Von Stackelberg, 1934) is one of the most widely used economic models for analyzing firms' behavior in a competitive environment. It studies the strategic situation in which firms sequentially choose their outputs in a market. The follower may know the leader's strategy, and the leader should consider the possible strategies of the follower for decision-making. Thus the Stackelberg leadership model may be a reasonable tool for tackling strategic adversaries (Kroshl et al., 2015; Pita et al., 2009). In other words, the defender is regarded as the leader while the attacker is considered to be the follower. The model also can be used to explore whether the defender can increase the investment to prevent security-related domino effects by forming a monopoly.

9.2.4 The law of diminishing returns

In economics, marginal utility is the satisfaction consumer gains from consuming one more unit of a good or service. Similar to any goods or services, the marginal safety or security utility can be regarded as the satisfaction obtained from one unit of additional special protection measures (Reniers and Van Erp, 2016). The marginal safety utility of a certain type of safety measures decreases with increasing more of this type of measures. From a viewpoint of producers, diminishing returns indicates the decrease in marginal output (impact) from increasing one unit of input (Anderson and Mittal, 2000). Safety resources also follow the law of diminishing returns: the marginal return in safety benefits of a safety measure decreases when furtherly increasing the number of the measure (Fuller and Vassie, 2004). In other words, an additional investment in a safety or security measure becomes less cost-effective than the preceding investment. Therefore the law of diminishing returns can facilitate the optimization of resource allocation and investment decision-making (Meyer and Reniers, 2016).

9.3 Threat analysis and vulnerability assessment

Threat analysis and vulnerability assessment which provide the basic data (e.g., threat probabilities, possible attack scenarios and damage probabilities of installations) for economic models, are needed to conduct an economic analysis for managing intentional domino effects. Different from assessments of accidental domino effects, a vulnerability assessment for installations against intentional domino effects should consider (i) the vulnerability of installations against direct intentional attacks as well as (ii) the vulnerability of installations subject to possible domino effects caused by the attacks. To prevent and mitigate intentional domino effects, safety barriers, and security measures may be integrated to reduce both the likelihood and consequences of these events.

9.3.1 Threat analysis

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

Intentional attacks may result from internal adversaries, external adversaries, or internal adversaries working in collusion with external adversaries. The adversaries encompass individuals, groups, organizations, or governments possibly executing these intentional events. So a threat analysis should consider as many adversaries as possible, such as intelligence services of host nations, or third-party nations, political and terrorist groups, criminals, rogue employees, cyber criminals, and private interests (API, 2013). Besides, the capability and the resources of the attackers in terms of available information, instruments, and tools should be considered in the analysis. However, quantifying adversaries is a considerable challenge since it requires a multitude of

Table 9.2 SRA methodology for threat assessment.

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 is possible in the life of the facility's operation").
Medium	Indicates that there is a possible threat to the asset or similar assets based on the threat's desire to compromise similar assets, but no specific threat exists for the facility or asset (e.g., "≥ 1 event 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 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").

Adapted from API, 2013. ANSI/API Standard 780 – Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry. American Petroleum Institute.

data and knowledge, and modeling the motivations, intents, characteristics, capabilities, and tactics of adversaries (Baybutt, 2017; Paté-Cornell and Guikema, 2002). Expert judgment methods may be applied to determine the threat probability, P_T (the likelihood of the threat) based on available data and information. For example, a five-level threat assessment method is adopted by American Petroleum Institution (API) in Security Risk Analysis (SRA) methodology, as shown in Table 9.2.

In case of unacceptable high consequences caused by intentional domino effects or insufficient information and data available in order to implement the five-level threat assessment method, a conditional threat approach may be applied: assuming $P_T = 1$ (Mueller and Stewart, 2011; Villa et al., 2017). This conservative approach indicates that the potential consequences (Chen et al., 2019) of possible intentional attacks are so severe that the threat likelihood assessment is not necessary. In that case, security management may focus on assessing the vulnerability of chemical installations, the potential consequences of intentional domino effects, and the cost–benefit of protection measures.

9.3.2 Vulnerability assessment

Vulnerability analysis for installations in chemical industrial areas shall be divided into two parts: the vulnerability of installations against direct intentional attacks and the vulnerability assessment of installations subject to possible domino effects caused by the attacks. The former can be regarded as any weakness that may be exploited by an attacker in order to gain access to direct targets and to successfully execute an attack (API, 2013). An intentional attack can be interrupted when the attack is detected and the guard communication to the response force is successful (Garcia, 2007). Therefore, the success probability of attacks (P_S) indicating the likelihood that the direct target installation is damaged by the attack can be expressed as follows:

$$P_S = P_T \cdot (1 - P_D \cdot P_C) \cdot P_E \tag{9.1}$$

where P_D represents the detection probability. According to the EASI model (Garcia, 2007), the P_D depends on the attack path, detection measures along the path, and guard response time. If the needed time for an attacker to pass the segment between a detection position and the attack target is less than the guard response time, the detection measures should not be considered. In order to successfully interrupt intentional attacks, detection measures and delay measures should be arranged reasonably. Detection measures consist of, for instance, fence sensors, door sensors, personnel, while delay measures include fence fabric, door hardness, wall hardness, etc. To assess the direct attack success probability of installations, the detection probability of each detection measure needs to be quantified and the delay time of each delay measure should be calculated as well.

P_C is the guard communication probability usually with a value of at least 0.95. The factors that affect P_C include the training in the use of communication equipment, maintenance, dead spot in radio communication, and the stress experienced during actual attacks (Garcia, 2007). P_E is the probability that the attack is successfully executed. The P_E depends on the capability, the available resources, information, instruments, and tools of the attackers. It can be expressed as the product of the reliability of the available device (P_R) and the performance factor (P_P) of adversaries in the use of the device, as shown in Eq. (9.2) (Stewart and Mueller, 2012).

$$P_E = P_R \cdot P_A \tag{9.2}$$

Table 9.3 The values of P_R and P_P in terms of explosion attacks launched by terrorist organizations.

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

VBIED, vehicle-borne improvised explosive device.
Adopted form Stewart, M.G., Mueller, J., 2012. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Critical Infrastructure Protection, pp. 513—533; Villa, V., Reniers, G.L.L., Paltrinieri, N., Cozzani, V., 2017. Development of an economic model for counter terrorism measures in the process-industry. Journal of Loss Prevention in the Process Industries 49, 437—460).

In terms of explosion attacks launched by terrorist organizations, three types of explosive devices and a conservative assumption in case of lacking assessment information are defined: simple, medium, complex, and conservative assumption. The corresponding values of P_R and P_P are reported in Table 9.3.

Besides, a conditional damage probability, $P(D|S)$, is employed to express the vulnerability of installations subject to possible domino effects caused by intentional attacks. The $P(D|S)$ is equal to 1 if the installation is the direct attack target. In that case, the damage probability of installations (P_{DD}) can be obtained, as follows:

$$P_{DD} = P_S \cdot P(D|S) \tag{9.3}$$

A dynamic graph approach will be presented in Section 9.4 to model the evolution of intentional domino effects, estimating the conditional probability of $P(D|S)$.

9.4 Domino effect analysis

In this section, a dynamic vulnerability assessment graph (DVAG) model is introduced to assess the vulnerability of installations exposed to possible domino effects caused by intentional attacks. The DVAG model is based on dynamic graphs, which provides a mathematical approach for studying interconnections among installations and temporal dependences during the spatial-temporal evolution of domino effects.

9.4.1 Definition

A 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 hazardous scenario caused by intentional events and ends when the evolution is over. For illustrative purposes, only the fire scenario is considered in the model, but it can be extended to other scenarios such as explosions. The dynamic graph can be represented by Eq. (9.4).

$$G = (I, \quad E, \quad f, \quad q) \tag{9.4}$$

(1) I is a set of nodes denoting installations in a chemical industrial area. The number of nodes (I) 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. (9.5).

$$f = (S, \quad Q, \quad RTF, \quad RTB) \tag{9.5}$$

- 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 9.4. For the sake of clear representation, an installation in the "vulnerable" state is marked as yellow, in the "harmful" state it is marked as red, and in the "dead" state it is marked as gray in the dynamic graph.
- Q is a weight of nodes denoting the total heat radiation received by installations. 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. 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. The fire on an installation is regarded to be extinguished when RTB is equal to zero.

Table 9.4 State description.

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

(4) q is the weight of directed edges which represent heat radiations from tail installations to head installations. The q can be expressed by an adjacent matrix (a square matrix of dimension $N \times N$), as shown in Eq. (9.6).

$$Q = \begin{bmatrix} 0 & q_{12} & \cdots & q_{1n} \\ q_{21} & 0 & \cdots & q_{2n} \\ \cdots & \cdots & 0 & \cdots \\ q_{n1} & q_{n2} & \cdots & 0 \end{bmatrix} \tag{9.6}$$

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.

9.4.2 Graph update

9.4.2.1 Time update

A 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. (9.7).

$$g = \begin{cases} 1 & \text{initial graph} \\ g+1 & \text{graph after a new update} \end{cases} \tag{9.7}$$

The period of time between two update operations is called "graph time" (t). The total evolution time at the starting of graph g (T^g) can be obtained using Eq. (9.8).

$$T^g = \begin{cases} 0 & g = 1 \\ T^{g-1} + t^{g-1} & g > 1 \end{cases} \tag{9.8}$$

9.4.2.2 State update

There are two update types among the three states, as shown in Fig. 9.1. 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.

9.4.2.3 Directed edge update

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

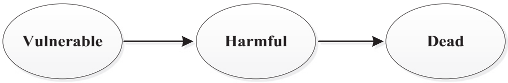


Figure 9.1 State transition of installations. *Adapted from Chen, C., Reniers, G., & Khakzad, N. (2019). Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach.* Reliability engineering & system safety, 191, *106470. https://doi.org/10.1016/j.ress.2019.04.023.*

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."

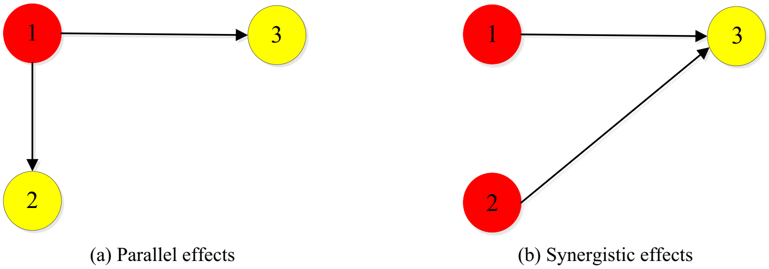
9.4.2.4 Heat radiation update

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 impose heat radiation on multiple installations being in "vulnerable" states; this is known as "parallel effects." Fig. 9.2A shows the graph model of a parallel effect, while Fig. 9.2B shows a synergistic effect as a graph.

According to the synergistic effect, the total heat radiation received by an installation j in a "vulnerable state" (Q_j) should be the sum of heat radiations received from other installations in "harmful" states, as shown in Eq. (9.9).

$$Q_j = \sum_{i=1}^{N} q_{ij} \tag{9.9}$$

The heat radiation received by each installation may vary over time due to new occurrences of harmful installations or dead installations. For update operations, the potential heat radiation values between each pair of installations can be calculated by software such as ALOHA (2016). In that case, an adjacency matrix of potential heat radiation (PQ) can be employed to represent the potential heat radiation values, as shown in Eq. (9.10).



(a) Parallel effects

(b) Synergistic effects

Figure 9.2 The harmful effects caused by heat radiation in a spatial evolution of domino effects: (A) parallel effects and (B) synergistic effects.

$$PQ = \begin{bmatrix} 0 & pq_{12} & \dots & pq_{1n} \\ pq_{21} & 0 & \dots & pq_{2n} \\ \dots & \dots & 0 & \dots \\ pq_{n1} & pq_{n2} & \dots & 0 \end{bmatrix} \tag{9.10}$$

The heat radiation caused by installations in the "vulnerable" state can be reduced by active barriers such as water deluge systems (WDSs). The WDS mitigates fire exposure by the protection of the target, keeping a water film on exposed surfaces to absorb radiant heat and to cool the steelwork, thus reducing the heat radiation received by installations in a "vulnerable" state. In this study, WDS is used as an example of an active barrier in the evolution of domino effects. So the q_{ij} can be obtained using a radiation reduction factor (φ) and an effectiveness parameter (η) when the installation i is on fire and WDSs are present in chemical industrial parks, as shown in Eq. (9.11).

$$q_{ij} = (1 - \eta \times \varphi) \times pq_{ij} \tag{9.11}$$

where pq_{ij} is the potential heat radiation caused by installation i on installation j; 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).

9.4.2.5 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 ($Q_j > 15\ \text{kW/m}^2$ (Cozzani et al., 2009)) at evolution time T^g, the RTF can be calculated by Eq. (9.12) (Landucci et al., 2009).

$$RTF_j^g = \frac{\exp\left(a \times V^b + c \ln\left(Q_j\right) + d\right)}{60} \tag{9.12}$$

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 9.5. In case of the presence of fireproof coatings, a time lapse (TL) should be considered since the failure time of installations is delayed due to the existing of fireproof coatings. As a result, the TL should be added to Eq. (9.12), as shown in Eq. (9.13).

Table 9.5 The parameter values of *a*, *b*, *c*, and *d*.

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

Adapted from Landucci, G., Gubinelli, G., Antonioni, G., Cozzani, V., 2009. The assessment of the damage probability of storage tanks in domino events triggered by fire. Accident Analysis & Prevention 41, 1206–1215.

$$RTF_j^g = \frac{\exp\left(a \times V^b + c\ln\left(Q_j\right) + d\right)}{60} + TL \tag{9.13}$$

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 in the "vulnerable" state at the time T^{g+1} will be updated according to superimposed effects: The heat radiation in different stages received by an installation should be superimposed in order to determine the residual time to failure at the time of T^{g+1}, as shown in Eq. (9.14) (Chen et al., 2018b).

$$RTF_j^{g+1} = \left(\frac{Q_j^{g+1}}{Q_j^g}\right)^c \cdot \left(RTF_j^g - t^g\right) \tag{9.14}$$

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

9.4.2.6 Residual time to burn out update

Assuming an installation i is on fire at the evolution time of T^g, the residual time to burn out of installation i at the time of T^g can be represented by the ratio of flammable substance mass to the burning rate, as shown in Eq. (9.15) (Chen et al., 2018b).

$$RTB_i^g = \frac{W_i}{v_i} \tag{9.15}$$

where W_i is the mass of flammable substances in installation i, kg; v_i is the burning rate of flammable substances in installation i; 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. (9.16).

$$RTB_i^{g+1} = RTB_i^g - t^g \tag{9.16}$$

9.4.2.7 Damage probability update

Emergency response in the chemical industry is essential to protect installations, the public, and workers' health and safety, to reduce the environmental impacts, and the recovery time of normal operations (Hosseinnia et al., 2018). Besides, it has an important impact on eliminating possible escalation or mitigating the consequence of domino effects in the chemical industry (Zhou and Reniers, 2016). So emergency response should be considered in the vulnerability assessment of plant installations. However, the evaluation of emergency response is rather complex due to the uncertainties related to human factors in the performance of emergency response tasks. The emergency response also influences the development of the accident and has important impacts on the occurring of domino effects (Zhou and Reniers, 2017). For performing a static risk assessment, the uncertainty of emergency response time is considered to obtain the "probit model" parameters (Landucci et al., 2009). 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. (9.17) (Chen et al., 2018b).

$$\log ttc \sim N\left(u, \sigma^2\right) \tag{9.17}$$

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., 2018b). Therefore, if an installation j is supposedly damaged at T^g with a certain probability during the evolution of intentional domino effects, the conditional probability of installation j being damaged $P(D|S)$ can be obtained by using Eq. (9.18).

$$P(D|S)_j = P(H|S)(1 - \mathrm{LND}(T^g)) \tag{9.18}$$

The likelihood of a primary hazardous scenario is expressed as a conditional probability of a successful attack, $P(H|S)$. $P(H|S)$ is deemed to be a prior probability to obtain the vulnerability of installations exposed to possible intentional domino effects in a chemical industrial area. On the basis of a threat and vulnerability analysis in Section 9.3, the possible primary scenarios initiating domino effects can be identified via consequence assessment methods (Chen and Reniers, 2018; Reniers et al., 2005).

9.4.3 Algorithm

The algorithm of the DVAG model based on the principle of minimum evolution time (MET) (Chen et al., 2018b) to obtain the damage probability of nontarget installations is elaborated in this section. The evolution principle indicates that an evolution enters into the next stage when any installation's state transfers to "harmful" or "dead." Finally, the domino effect evolution will end when $Q = 0$. Fig. 9.3 shows the flow diagram of the algorithm.

The algorithm is described and explained as follows. First, basic data needed for performing the method is inputted, including park and plant

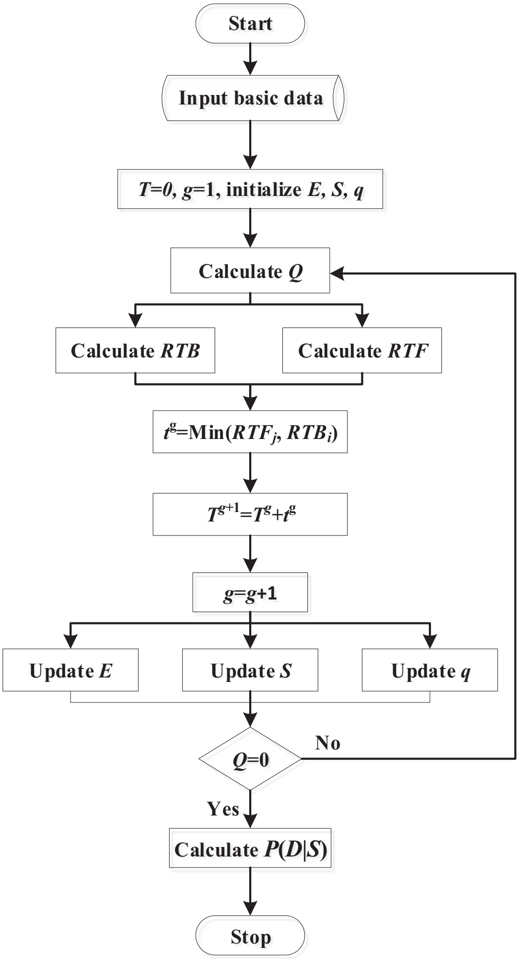


Figure 9.3 Flow diagram of the algorithm of the DVAG model (Chen et al., 2018b).

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 value 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 end and the damage probability of each installation is calculated. Besides the installations' damage probabilities, the damage time and evolution sequence are obtained using this algorithm.

9.5 Cost–benefit analysis

9.5.1 Cost analysis

To implement an integrated protection strategy (a combination of safety barriers and security measures) or to update existing protection systems, an economic analysis is recommendable in industrial practice since companies are always confronted with budget limitations (Reniers and Sörensen, 2013a). In this section, the various costs related to a protection strategy that a company may decide to implement are illustrated. The prevention and protection costs consist of investments that occur at present such as initial costs, installation costs, and the costs that occur throughout the whole remaining lifetime of the facility (Reniers and Brijs, 2014). In other words, a cost analysis for a prevention or a protection measure should include direct economic costs of applying the safety or security measures and indirect costs associated with their use. Eight categories of costs adopted from the classification of safety barriers (Reniers and Van Erp, 2016) and security measures (Villa et al., 2017) are listed in Table 9.6. The initial costs and installation costs don't need to be discounted to present values while the operation, maintenance, inspection, logistics, as well as transport and contractor costs which occur throughout the lifetime cycle of the facility should be discounted to present values.

The present value of costs caused by the implementation of one safety or security measure (C_m) is the sum of the initiation costs, installation costs, and the present value of six other cost types, as follows:

$$C_m = C_{m,\text{ini}} + C_{m,\text{ins}} + \frac{(1+r)^{\gamma}-1}{r(1+r)^{\gamma}}\big(C_{m,\text{ope}} + C_{m,\text{mai}} + C_{m,\text{ins}} + C_{m,\log} + C_{m,\text{con}} + C_{m,\text{oth}}\big) \tag{9.19}$$

Table 9.6 Categories of prevention and protection costs.

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

Adopted from Reniers, G.L., Van Erp, H.N., 2016. Operational Safety Economics: A Practical Approach Focused on the Chemical and Process Industries. John Wiley & Sons.

where $C_{m,\text{ ini}}$ is the initiation cost of measure m, $C_{m,\text{ ins}}$ is the installation cost of measure m, $C_{m,\text{ ope}}$ is the annual operation cost of measure m, $C_{m,\text{ mai}}$ is the annual maintenance cost of measure m, $C_{m,\text{ ins}}$ is the annual inspection costs of measure m, $C_{m,\text{ log}}$ is the annual logistics and transport cost of measure m, $C_{m,\text{ con}}$ is the annual contractor cost of measure m, $C_{m,\text{ oth}}$ are other annual costs of measure m, r is the discount rate, γ is the minimum value of the number of years that the protection measure can operate and the remaining lifespan of the facility. In case of more information for the cost calculation of subcategories listed in Table 9.6, readers are referred to Reniers and Van Erp (2016).

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

$$C^n = \sum_{m=1}^{M} C_m/\gamma \tag{9.20}$$

where C^n is the annual present costs of protection strategy n, M is the total number of (safety and security) measures taken in the strategy to prevent or mitigate intentional domino effects.

9.5.2 The overall losses of intentional domino effects

Possible intentionally damaged installations in chemical industrial areas should be considered in the analysis of avoiding costs or hypothetical benefits. Threat analysis, vulnerability assessment of installations toward intentional attacks, and exposure of installations to potential domino effects should be considered in this regard. Besides, multiple attack scenarios may be identified in threat analysis since the intelligent and strategic adversary will adapt to changing circumstances which are possible due to protection measures. Considering K attack scenarios capable of triggering domino effects in a chemical industrial area being identified in a threat analysis, the overall losses caused by the k-th ($k = 1, 2, 3, \ldots, K$) attack scenario under a protection strategy n ($OL^{n,k}$) can be simplified as the sum product of installations' conditional damage probabilities and the losses caused by the damage of the installations, as follows:

$$OL^{n,k} = \sum_{i=1}^{I} P(D|S)_i^{n,k} \cdot L_i \tag{9.21}$$

where $P(D|S)_i^{n,\,k}$ is the conditional damage probability of installation i under the protection of strategy n in attack scenario k. L_i is the loss caused by the damage of installation i, which is assumed to be independent with attack scenarios and protection strategies.

The loss assessment of intentional attacks should take into account economic losses, casualties, as well as any or all other influences such as psychological and political effects (Stewart and Mueller, 2011). Similar to the accidental loss analysis, both the direct losses that are immediately visible and tangible and the indirect losses that are intangible and invisible are of significance for the hypothetical benefit analysis w.r.t. intentional domino effects (Jallon et al., 2011; Reniers and Van Erp, 2016). The direct losses consist of the losses caused by damage to installations, products, and equipment, medical expenses, paying fines, and an insurance premium's rise while the indirect losses include capacity losses, production scheme problem losses, recruitment, and wage costs (Gavious et al., 2009). The quantification of indirect losses is more difficult since they are hidden or invisible components, usually resulting in underestimation (Jallon et al., 2011). One simple method to estimate the indirect losses is using a ratio of indirect to direct loss based on the assessment results of direct losses. The ratio varies in literature to another, inducing difficulties for users to choose a suitable value. For example, a widely used ratio of 4 is proposed based on an analysis of 7500 accidents while that of a range of 1–20 depending on different industrial sectors and methods used was found (Dorman, 2000). In this chapter, we adopt the loss assessment method proposed by Reniers and Brijs (2014) to account for parts of the losses similar to major accidents in chemical industrial areas (Reniers and Van Erp, 2016). Besides, a special category of loss is developed to address the losses related to intentional attacks, such as psychological and political effects. Therefore, the total losses caused by the damage of an installation *j* can be estimated as a sum of 12 contributions, as follows:

$$\begin{aligned} L_i = L_{i,sup} + L_{i,dam} + L_{i,leg} + L_{i,ins} + L_{i,hum} + L_{i,env} \\ + L_{i,per} + L_{i,med} + L_{i,int} + L_{i,rep} + L_{i,inv} + L_{i,sec} \end{aligned} \tag{9.22}$$

where $L_{i,sup}$ is the supply chain loss, $L_{i,dam}$ is the damage loss, $L_{i,leg}$ is the legal loss, $L_{i,ins}$ is the insurance loss, $L_{i,hum}$, is the human loss, $L_{i,env}$ is the environmental loss, $L_{i,per}$ is the personnel loss, $L_{i,med}$ is the medical loss, $L_{i,int}$ is the intervention loss, $L_{i,rep}$ is the reputation loss, $L_{i,inv}$ is the accident investigation and clean-up loss, $L_{i,\mathrm{sec}}$ is the security-related loss which is different from accidental losses, such as the losses caused by psychological and political effects. The loss of each category can be calculated by adding up the subcategories presented in Table 9.7.

Table 9.7 Categories of accident costs.

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

Adapted from Reniers, G.L., Van Erp, H.N., 2016. Operational Safety Economics: A Practical Approach Focused on the Chemical and Process Industries. John Wiley & Sons.

9.5.3 Net benefit analysis

The benefit of an integrated protection strategy is estimated as the difference of expected overall loss regarding intentional domino accidents without and with the implementation of safety and security measures. The expected overall loss is defined as the product of the success probability of attacks and the overall loss of intentional domino effects. In order to calculate the benefits of a protection strategy, a baseline ($n = 0$) should be defined. The baseline can be the strategy without any safety or security measure, or the initial strategy before a protection upgrade. In that case, the benefits of a protection strategy n for a special attack scenario k can be defined, as follows:

$$B^{n,k} = P_S^{0,k} OL^{0,k} - P_S^{n,k} OL^{n,k} \tag{9.23}$$

where $B^{n,k}$ is the hypothetical benefit of protection strategy n against a special attack scenario k, $OL^{0,k}$ is the overall loss of baseline protection strategy 0, $P_S^{0,k}$ is the success probability of attack scenario k under the baseline protection strategy, $P_S^{n,k}$ is the success probability of attack scenario k under the protection of baseline strategy. Different from natural or accidental threats, adversaries may adapt to the changing circumstances caused by a protection strategy to maximize their hypothetical benefits. According to the Stackelberg leadership model (Von Stackelberg, 1934), the defender can be considered as the leader while the attacker is viewed as the follower who knows the protection strategy before launching an attack. A reasonable assumption is that the attacker is a benefit maximizer aiming to maximize the damage. Therefore, the benefit of a protection strategy n should be represented by the attack scenario which causes the minimal protection benefit:

$$B^n = \min_k B^{n,k} \tag{9.24}$$

where B^n is the hypothetical benefit of a protection strategy n. In that case, the net present value given a protection strategy n (NPV^n) can be expressed as the difference of the total protection benefit and the total protection cost of strategy n in y years, as follows:

$$NPV^n = y(B^n - C^n) \tag{9.25}$$

A protection strategy n is usually recommended if the NPV exceeds zero ($NPV > 0$), otherwise, it is considered to be not cost-effective or inefficient (Reniers and Van Erp, 2016; Stewart and Mueller, 2013). The NPV is able to provide decision-making as regards protection strategies, addressing intelligent and strategic adversaries and the uncertainty in domino effect evolution. Besides, combining threat analysis and vulnerability assessment mentioned in Sections 9.3 and 9.4, a minimal threat probability (P_T^*) or risk reduction ($\triangle R$) needed for a special protection strategy n to be cost-effective can be obtained by "break-even" analysis (Stewart and Mueller, 2014). The "break-even" analysis indicates that the effectiveness of a protection strategy depends on the threat level that the chemical facility is confronted with.

9.5.4 Disproportion factor analysis

An intentional domino effect with catastrophic damage may be considered to be a low-frequency high-consequence event. In that case, the CBA based on *NPV* might not be satisfaction for decision-making on domino effect management in which the hypothetical benefits of protection strategies are usually less than the costs. To take this into account, a disproportion factor (DF) or so-called gross disproportion factor that can also be used to deal with type II[1] accidents is introduced in this section.

The ratio of the costs to the benefits is defined as the proportion factor (*PF*). The *PF* of a protection strategy n can be represented as:

$$PF^n = \frac{C^n}{B^n} \tag{9.26}$$

A *DF* is a threshold to determine whether the protection measure is grossly disproportionate or not. A protection investment is "reasonably practicable" when its costs are proportionate to the benefits ($PF < DF$). In the case of $PF \geq DF$, a further risk reduction would be too costly compared with the extra benefit gained from the protection measure. The *DF* reflects a bias in favor of safety and/or security over costs if it is higher than 1. Goose (2006) stated that the *DF* is usually less than 10 and should never be greater than 30. Theoretically, the *DF* increases with an increasing risk level and it should be infinite when the risk level reaches the intolerable region, meaning that the risk must be reduced no matter the costs (Talarico and Reniers, 2016).

A calculation method involving three factors to estimate the value of *DF* was proposed by Goose (2006). The factors are referred to "how bad," "how

[1] Three types of accidents can be discerned in terms of uncertainties: accidents where a lot of historical data are available (type I), accidents where little or extremely few historical data are available (type II), and accidents where no historical data are available (type III).

risky," and "how variable," and they are probably dependent on each other. Data or information needed for determining the three factors can be derived from an *FN* curve. For information on *FN* curve, the reader is referred to Reniers and Van Erp (2016).

The "how bad" factor depends upon the average number of fatalities per event, and can be calculated, as follows:

$$\text{How bad} = \log_{10}(N_{av}) \tag{9.27}$$

$$N_{av} = \frac{EV}{\sum FR} \tag{9.28}$$

where *EV* is the average number of deaths expected per year, $\sum FR$ is the sum of failure rates of all events per year, N_{av} is the average number of fatalities per event, represented by the ratio of N_{av} to $\sum FR$.

The "how risky" factor represents the effects of *EV* on the *DF*:

$$\text{How risky} = \log_{10}\left(10^5 \times EV\right) \tag{9.29}$$

The "how variable" factor depends on the ratio of the maximum potential fatalities for a single event ($N_{\max}$) to the average number of fatalities per event (N_{av}):

$$\text{How variable} = \log_{10}\left(\frac{N_{\max}}{N_{av}}\right) \tag{9.30}$$

The *DF* can then be calculated by adding 3 (dimensionless) to the product of the three "how" factors:

$$DF = \log_{10}(N_{av}) \times \log_{10}\left(10^5 \times EV\right) \times \log_{10}\left(\frac{N_{\max}}{N_{av}}\right) + 3 \tag{9.31}$$

For more information, see Reniers and Van Erp (2016) or Achille et al. (2017).

9.6 Cost-effectiveness analysis

The CBA in Section 9.5 stated that a protection strategy is recommended if the so-called *NPV* is greater than zero or the costs are proportionate to the benefits. However, companies usually face budget limitations and are expected to maximize their profits when it comes to decision-making on protection investments. This section thus aims to find out the most profitable protection strategy with budget limitations using cost-effectiveness analysis.

9.6.1 Deterministic cost-effectiveness analysis

The optimized allocation of safety or security resources in chemical industrial areas is simplified by using "Knapsack problem" approach, well known in the field of Operations Research (Reniers and Sorensen, 2013b; Villa et al., 2017). In terms of intentional domino effects, a chemical industrial area with large quantities of hazardous installations may be regarded as an interdependence system. Following the analysis in the previous sections, simulation-based optimization methods (Nguyen et al., 2014) may be employed to achieve the optimal integrated protection strategy for tackling intentional domino effects:

$$\begin{cases} \max\limits_{n} ANB^{n}(PS_{n}) \\ C_{n} \leq C_{\text{Budget}} \\ n\in\{1,2,3,\ldots,N\}, N\in Z \end{cases} \tag{9.32}$$

Eq. (9.32) indicates that the annual net benefit (*ANB*) from the possible protection strategies should be maximized within the constraint of the protection budget (C_{Budget}). The monetary cost of a protection strategy *n* from *N* possible combinations of safety and security measures should not exceed C_{Budget}. There may be thousands or even millions of protection strategies in a large chemical industrial area with a limited budget. It is unreasonable to assess the *ANB* of all protection strategies by an exhaustive method. In order to obtain the optimal protection strategy, advanced evolutionary algorithms such as genetic algorithm may be used to solve the optimization model, determining the optimal investment to maximize the protection benefits.

9.6.2 Proportion factor–based cost-effectiveness analysis

As elaborated in Section 9.5.4, the *PF* and *DF* can be determined and implemented to help understand a protection strategy's financial impact and thus determine whether the strategy is recommended or not. Therefore, the optimal protection strategy can be regarded as the protection strategy with the minimal value of *PF*, as follows:

$$\begin{cases} \min\limits_{n} PF^{0,n}(PS_{n}) \\ C_{n} \leq C_{\text{Budget}} \\ n\in\{1,2,3,\ldots,N\}, N\in Z \end{cases} \tag{9.33}$$

9.6.3 Marginal hypothetical benefit analysis

Various security measures and safety barriers with different functions can be used to tackle intentional domino effects in a chemical facility. For example, installing detection measures allows increasing the detection probability (P_D) and thus decreasing the probability of a successful attack. Assuming the detection likelihood of single detection equipment ($P_{d,e}$) is mutually independent, the detection probability can be calculated, as shown in Eq. (9.35).

$$P_D = 1 - \prod_{e=1}^{e=E} \left(1 - P_{d,e}\right) \tag{9.34}$$

where e is the index of detection measure and E is the number of detection measures installed on an attack path. Combining Eq. (9.35) with the CBA in Section 9.5 and keeping other parameters constant, the cost—return (hypothetical benefit) curve for the investment of detection measures can be obtained, as shown in Fig. 9.4.

Fig. 9.4 demonstrates that the investment in detection measures follows the law of diminishing marginal returns: increasing additional measures or equipment results in smaller increases in protection benefits. In that case, when the investment in detection measures reaches a certain amount, further increasing the number of detection measures will become less and less cost-effective. The law of diminishing marginal returns is also suitable

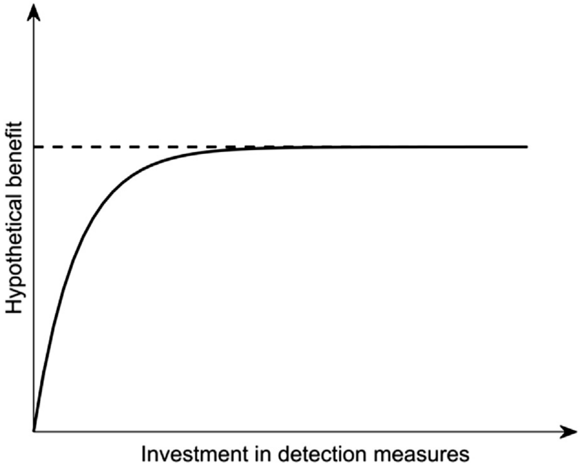


Figure 9.4 The protection benefit of investment in detection measures. *Adapted from Chen, C., Reniers, G., 2019. An economic framework for management of intentional domino effects in chemical industrial areas. Chemical Engineering Transactions 75.*

for the investment in safety barriers such as fireproof coatings and water delivery systems (Chen et al., 2019). The benefits obtained from an investment in fireproof coatings or water delivery systems decrease with increasing the number of tanks with these safety barriers. Thus, to be more efficient for tackling intentional domino effects, different types of protection measures should be taken, such as detection measures, communication measures, active barriers, passive barriers, etc. In other words, the total protection budget available should be allocated to a wide range of protection measures: safety-related measures and security-related measures.

According to the law of diminishing marginal returns, we can obtain a curve of diminishing marginal rate of return of each type of protection measures. Then a mathematical function for each curve of diminishing marginal rate needs to be determined via a numerical fitting. The type of function form of such curves is given, as follows:

$$y = \frac{ux}{x+v} \tag{9.35}$$

The parameters of u and v are constants and depend on the exact shape of a curve. The parameter u represents the maximal value that the curve is approximating. The parameter v indicates how fast the curve is approximating the maximum value, displaying the level of efficiency of the measures (Reniers and Van Erp, 2016). Therefore, the optimization objective function and the restriction for calculating the most cost-effective protection strategy can be expressed:

$$\begin{cases} \max \sum\limits_{w=1}^{w=W} \dfrac{u_w x_w}{x_w + v_w} \\ x_1 + x_2 + x_3 + \ldots + x_w = C_{\text{Budget}} \end{cases} \tag{9.36}$$

where w represents a type of protection measure and the total number of types is W. To obtain the solution, the Lagrange method can be implemented (Hoy et al., 2011).

$$L = \sum_{w=1}^{w=W} \frac{u_w x_w}{x_w + v_w} - \lambda \left(C_{\text{Budget}} - \sum_{w=1}^{w=W} x_w \right) \tag{9.37}$$

Carrying out all the first-order partial derivatives for Eq. (9.37), the optimization problem can be transferred to solve an equation set with $W+1$ equations. In this way, we can obtain the optimal investment allocation for each type of protection measure under the restriction of budget limitations.

9.7 Conclusions

Although quantifying the costs and benefits of safety and security measures with respect to intentional domino effects is rather challenging, it is a necessary work w.r.t. the effectiveness of a company's prevention and protection policy as well as the company's long-term profitability. In this chapter, the role of economic models in tackling intentional domino effects has been explored. An economic approach is therefore developed to mitigate and prevent intentional domino accidents that might cause significant financial losses and casualties. This approach considers hazardous installations' vulnerability against direct intentional attacks and the vulnerability of installations subject to possible intentional domino effects. Safety barriers and security measures are integrated as protection strategies. The CBA proposed in this approach is able to obtain the *NPV* and *DF* which is used to identify profitable strategies. A protection strategy is recommended when the *NPV* is greater than zero or the *PF* is less than the corresponding *DF*. The optimal protection strategy, under the restriction of budget limitations, is obtained by using a mathematically formulated and quantifiable cost-effectiveness analysis. In summary, the results obtained by employing an economic approach can support decision-making on protection strategies.

References

Achille, J., Ponnet, K., Reniers, G., 2017. Calculation of an adjusted Disproportion Factor (DF*) which takes the societal acceptability of risks into account. Safety Science 94, 171–180.

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

Anderson, E.W., Mittal, V., 2000. Strengthening the satisfaction-profit chain. Journal of Service Research 3, 107–120.

API, 2013. ANSI/API Standard 780 – Security Risk Assessment Methodology for the Petroleum and Petrochemical Industry. American Petroleum Institute.

Baybutt, P., 2002. Assessing risks from threats to process plants: threat and vulnerability analysis. Process Safety Progress 21, 269–275.

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

BBC News, 2015. France Explosions: Devices Found Near Berre-L'Etang Plant.

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.

Blomberg, S.B., Hess, G.D., Weerapana, A., 2004. An economic model of terrorism. Conflict Management and Peace Science 21, 17–28.

Brück, T., 2007. The Economic Analysis of Terrorism. Routledge.

Chen, C., Reniers, G., 2018. Risk assessment of processes and products in industrial biotechnology. Advances in Biochemical Engineering. https://link.springer.com/chapter/10.1007/10_2018_74.

Chen, C., Reniers, G., Zhang, L., 2018b. 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.

Chen, C., Reniers, G., Khakzad, N., 2019. Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach. Reliability engineering & system safety 191, 106470. https://doi.org/10.1016/j.ress.2019.04.023.

Chen, C., Reniers, G., Khakzad, N., 2020. Cost-benefit management of intentional domino effects in chemical industrial areas. Chemical Engineering Transactions 134, 392—405. https://doi.org/10.1016/j.psep.2019.10.007. In this issue.

Cozzani, V., Tugnoli, A., Salzano, E., 2009. The development of an inherent safety approach to the prevention of domino accidents. Accident Analysis & Prevention 41, 1216—1227.

Dorman, P., 2000. The Economics of Safety, Health, and Well-Being at Work: An Overview. ILO, Geneva.

Fuller, C., Vassie, L.H., 2004. Health and Safety Management: Principles and Best Practice. Pearson Education.

Garcia, M.L., 2007. Design and Evaluation of Physical Protection Systems. Elsevier.

Gavious, A., Mizrahi, S., Shani, Y., Minchuk, Y., 2009. The costs of industrial accidents for the organization: developing methods and tools for evaluation and cost—benefit analysis of investment in safety. Journal of Loss Prevention in the Process Industries 22, 434—438.

Goose, M.H., 2006. Gross Disproportion, Step by Step—A Possible Approach to Evaluating Additional Measures at COMAH Sites.

Hausken, K., 2018. A cost—benefit analysis of terrorist attacks. Defence and Peace Economics 29, 111—129.

Hosseinnia, B., Khakzad, N., Reniers, G., 2018. An emergency response decision matrix against terrorist attacks with improvised device in chemical clusters. Safety Security Studies 1, 187—199.

Hoy, M., Livernois, J., McKenna, C., Rees, R., Stengos, T., 2011. Mathematics for Economics. MIT press.

Jallon, R., Imbeau, D., de Marcellis-Warin, N., 2011. Development of an indirect-cost calculation model suitable for workplace use. Journal of Safety Research 42, 149—164.

Janssens, J., Talarico, L., Reniers, G., Sörensen, K., 2015. A decision model to allocate protective safety barriers and mitigate domino effects. Reliability Engineering & System Safety 143, 44—52.

Kroshl, W.M., Sarkani, S., Mazzuchi, T.A., 2015. Efficient allocation of resources for defense of spatially distributed networks using agent-based simulation. Risk Analysis 35, 1690—1705.

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. Accident Analysis & Prevention 41, 1206—1215.

Meyer, T., Reniers, G., 2016. Engineering Risk Management. Walter de Gruyter GmbH & Co KG, Berlin.

Mueller, J., Stewart, M.G., 2011. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security. Oxford University Press.

Nguyen, A.-T., Reiter, S., Rigo, P., 2014. A review on simulation-based optimization methods applied to building performance analysis. Applied Energy 113, 1043—1058.

Paté-Cornell, E., Guikema, S., 2002. Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Military Operations Research 7, 5—23.

Pita, J., Jain, M., Ordóñez, F., Tambe, M., Kraus, S., Magori-Cohen, R., 2009. Effective solutions for real-world stackelberg games: when agents must deal with human uncertainties. In: Proceedings of the 8th International Conference on Autonomous Agents and Multiagent Systems, vol. 1. International Foundation for Autonomous Agents and Multiagent Systems, pp. 369—376.

Poole, R.W., 2008. Toward risk-based aviation security policy. In: OECD/ITF Joint Transport Research Centre Discussion Paper.

Quah, E., Haldane, J., 2007. Cost-benefit Analysis. Routledge.

Reniers, G., Brijs, T., 2014. Major accident management in the process industry: an expert tool called CESMA for intelligent allocation of prevention investments. Process Safety and Environmental Protection 92, 779—788.

Reniers, G., Dullaert, W., Audenaert, A., Ale, B.J., Soudan, K., 2008. Managing domino effect-related security of industrial areas. Journal of Loss Prevention in the Process Industries 21, 336—343.

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

Reniers, G., Sörensen, K., 2013a. Optimal allocation of safety and security resources. Chemical Engineering Transactions 31, 397—402.

Reniers, G.L., Sorensen, K., 2013b. An approach for optimal allocation of safety resources: using the knapsack problem to take aggregated cost-efficient preventive measures. Risk Analysis 33, 2056—2067.

Reniers, G.L., Van Erp, H.N., 2016. Operational Safety Economics: A Practical Approach Focused on the Chemical and Process Industries. John Wiley & Sons.

Reniers, G.L.L., Dullaert, W., Ale, B.J.M., Soudan, K., 2005. Developing an external domino accident prevention framework: Hazwim. Journal of Loss Prevention in the Process Industries 18, 127—138.

Stewart, M.G., Mueller, J., 2011. Cost-benefit analysis of advanced imaging technology full body scanners for airline passenger security screening. Journal of Homeland Security and Emergency Management 8.

Stewart, M.G., Mueller, J., 2012. Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Critical Infrastructure Protection, pp. 513—533.

Stewart, M.G., Mueller, J., 2013. Terrorism risks and cost-benefit analysis of aviation security. Risk Analysis 33, 893—908.

Stewart, M.G., Mueller, J., 2014. A risk and cost—benefit analysis of police counter-terrorism operations at Australian airports. Journal of Policing, Intelligence and Counter Terrorism 9, 98—116.

Talarico, L., Reniers, G., 2016. Risk-informed decision making of safety investments by using the disproportion factor. Process Safety and Environmental Protection 100, 117—130.

Villa, V., Reniers, G.L.L., Paltrinieri, N., Cozzani, V., 2017. Development of an economic model for counter terrorism measures in the process-industry. Journal of Loss Prevention in the Process Industries 49, 437—460.

Von Stackelberg, H., 1934. Marktform und gleichgewicht. Julius Springer.

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.

Zhou, J., Reniers, G., 2017. Analysis of emergency response actions for preventing fire-induced domino effects based on an approach of reversed fuzzy Petri-net. Journal of Loss Prevention in the Process Industries 47, 169—173.