Received: 9 September 2022 | Revised: 28 December 2022 | Accepted: 10 January 2023

DOI: 10.1002/prs.12443

PROCESS SAFETY PROGRESS

ORIGINAL ARTICLE

Reducing the risk of intentional domino effects in process plants: A risk-based minimax strategy

Nima Khakzad

School of Occupational and Public Health, Ryerson University, Toronto, Canada

Correspondence
Nima Khakzad, School of Occupational and Public Health, Ryerson University, Toronto, Canada
Email: nima.khakzad@ryerson.ca

Funding information
Natural Sciences and Engineering Research Council of Canada, Grant/Award Number: RGPIN/03051-2021

Abstract

Compared with safety assessment, security risk assessment in chemical and process plants is more challenging. On top of uncertain environmental and operational parameters and interdependent failures, which are common in the safety risk assessment of complex systems and infrastructures, there are other uncertain parameters such as the likelihood of attack scenarios and attackers' expected outcomes. As such, the application of probabilistic risk assessment (PRA) techniques, which have long been applied to safety risk assessment and management, to security risk management may result in nonoptimal or suboptimal decisions. In the present study, we will demonstrate how a combination of PRA and game theory may outperform PRA and lead to a more cost-effective allocation of security measures. For this purpose, the outcome of a dynamic Bayesian network—as a PRA technique—is used as input to the minimax strategy—as a game theoretic strategy—for security risk management of a tank terminal under attacks with a homemade bomb. The proposed risk-based minimax strategy alleviates the need for estimation of attack likelihoods or attacker payoffs, which would have otherwise been too challenging to estimate if the analyst solely depended on a PRA technique.

KEYWORDS
decision-making under uncertainty, domino effect, game theory, IED attack, minimax strategy

1 | INTRODUCTION

Protecting critical infrastructures and hazardous facilities (nuclear facilities, chemical and process plants, etc.) against terrorist attacks has gained much attention since the September 11 terrorist attacks in the United States. Assessing and managing the risk of terrorist attacks is a multifaceted task that demands the analysis of potential targets, possible attack modes, credible attack scenarios, and the availability of mitigation alternatives. Factors such as the dynamic nature of terrorism risk, the countless number of possible attack scenarios, the contingent nature of the threats, and the limited resources available to eliminate all risks have led to the prioritization of the targets to protect and the defensive resources to allocate.[1] In this regard, risk scoring methodologies and probabilistic risk assessment (PRA) have been playing a key role in prioritizing antiterrorism measures.[2] Likewise, parallels between safety and security risks have been investigated, with discussions about safety risk assessment concepts that can essentially be modified and applied to the security risk assessment of hazardous facilities.[3]

In a report by the U.S. Government Accounting Office,[4] the need for "a comprehensive risk management process" for effective allocation of antiterrorism resources was pointed out, which in turn has resulted in a number of risk-based scoring methodologies for the allocation of defensive resources.[1,5–8] In such methodologies, the security risk (R) is defined as:

$$R = T \times V \times C, \quad (1)$$

where R is the security risk, T is the threat score (or likelihood), V is the vulnerability score, and C is the consequences. However, the application of PRA and, particularly the estimation of the risk of terrorist attacks using Equation (1), has been criticized by some researchers,[9–13] including Cox,[10] who claims that Equation (1) does not account for dependencies among the risk components and may result in an overestimation or underestimation of the risk. Khakzad et al.[14] used the analytic network process to demonstrate that linear scoring of the risk components (i.e., T, V, and C) may result in a different, and not necessarily accurate, prioritization of the threats and targets than those obtained from a nonlinear scoring approach capable of considering the mutual dependencies.

There have been attempts to take into account the dependencies in this regard, such as using a Bayesian network[15] or estimating the threat (T) as a function of target vulnerability (V) and attractiveness, both of which are estimated by defenders from the attackers' viewpoint.[7]

In the majority of such efforts, however, the defenders' uncertainty about the attackers' goals, asset valuation (attractiveness), and intention has been modeled based on simplifying assumptions or probability distributions that cannot seem to be easily verified. Cox[10] also debates that estimating and presenting the threat (T) and vulnerability (V) simply as numbers cannot seem to account for an intelligent attacker's ability to dynamically replan and carry out the attack in face of defensive measures.

Aside from the simplistic nature of Equation (1), prioritization of defensive resources based on the results of PRA can be quite self-defeating as it may make the defenders' resource allocation more predictable to attackers. For instance, a defender may rank order M facilities (targets) based on their respective risk scores, and decide to protect N facilities ($N < M$) depending on his available resources. This will leave an informed attacker (informed in the sense that the attacker would know that the defender would have followed a risk-based approach) with $K = M - N$ undefended facilities; the expected damage of attack to these could be even more than to the protected facilities.[10]

Cox[11] further demonstrated the inefficacy of risk scoring methodologies, among others, in reflecting the role of secrecy and deception in reducing the risk of attacks or the influence of risk externalities[16] (e.g., protecting one target can increase the attractiveness of other targets), making them even less effective in some cases compared with a random allocation of defensive resources. According to Bier,[16] negative externalities can be exploited by defenders to manipulate the attackers' choice, drawing their attention to less valuable targets or to well-secured and more valuable targets, only to find out their attack would cost more than it is worth.

Cox[10] recommends decision trees, optimization techniques, and game theory models as more viable alternatives to PRA as they help the defender optimize the allocation of resources to minimize the maximum damage (or expected damage) resulting from the "best response" of attackers. Best response models, in their simplest form, can be formulated as two-level optimization problems in which the defender calculates the attacker's best response to various allocations of resources (the attacker's best response would maximize the net expected reward of the attacker) and chooses the allocation that would minimize the damage.[7,10,12,17,18]

Integration of PRA and game theory can effectively overcome the drawbacks of risk scoring approaches in both system safety management[19] and security management.[12] In the context of security risk, PRA can be used to calculate the expected payoffs of uncertain consequences of paired defender–attacker strategies, while game theory can be used to optimize the defenders' decisions (allocation of defensive resources) with regard to the attackers' best response.[12]

In simultaneous or one-stage defender–attacker games, the defender acts first, trying to minimize the maximum damage that the attacker can make via the best response to the defender's decision. Such games, also known as minimax strategies, are typically formulated in the form of relatively simple two-level optimization problems that do not require sophisticated game theoretic concepts.[12]

In a two-level optimization problem, the defender must allocate defensive resources to a collection of targets that might potentially be attacked. The defenders usually do not know the attackers' preferences, while the attackers may observe the defenders' resource allocation or know the defenders' valuation of the assets (a game of incomplete information), leading to a sequential game. On the other hand, if the defenders manage to conceal defensive allocations, the optimization problem would turn into a simultaneous game. Nevertheless, defenders will generally be better off in a sequential game than in a simultaneous game.[16] As a result, a simultaneous game can be considered the worst-case scenario, resulting in the most conservative allocation of resources from the defenders' viewpoint.

The present study aims to illustrate the efficacy of the risk-based minimax strategy in reducing the risk of impending terrorist attacks on chemical and process facilities. Section 2 recapitulates the basics of minimax strategy; Section 3 demonstrates the application of risk-based minimax strategy on an illustrative tank farm and shows how relying merely on the results of PRA may lead to suboptimal decisions; and Section 4 is devoted to the discussions.

2 | MINIMAX STRATEGY

Game theory is a branch of applied mathematics for modeling situations of competitive cooperation or conflict of interest among a number of players (decision-makers) where usually one player gains at the expense of other player(s). A game consists of a set of players, a set of actions (moves) for each player, and a payoff (utility) function for each player. Games can be classified as simultaneous or sequential. In a simultaneous game (e.g., rock–paper–scissors), each player chooses their own action (makes a decision) without the knowledge of their opponents. On the other hand, in a sequential game (e.g., chess), the second player, when making their move, has some information about the first player's move.[20]

Classification of games as simultaneous or sequential is more about the availability of information to the players at the time of decision-making than the temporal sequence of decisions (moves). Simultaneous games, which are the scope of the present study, can be presented in

TABLE 1 A defender–attacker game in the normal form as a two-player bimatrix

	Attack A	Attack B
Defend A	a1, a2	b1, b2
Defend B	c1, c2	d1, d2

TABLE 2 The simplified defender–attacker game with a focus on defender's payoff

	Attack A	Attack B
Defend A	a1	b1
Defend B	c1	d1

their normal form as a payoff table (or bimatrix) for two players. It is worth noting that a game, whether simultaneous or sequential, can alternatively be presented in extended form as a game tree. Table 1 presents a case with two assets, A and B, while the defender's resources would only allow for defending one or the other. According to the payoffs in Table 1, for instance, if the defender decides to defend asset A whereas the attacker attacks asset B, the defender and attacker would end up, respectively, with b1 and b2 as the payoffs.

If the attacker or the defender knew beforehand what move their opponent would make (e.g., if the attacker knew which target would have been secured by the defender, or similarly, if the defender knew which target would be attacked), the game would change from simultaneous (a game with incomplete knowledge) to sequential (a game with perfect information). With the defender's knowledge of the attacker's move, the move with the highest payoff for the defender given the attacker's move is thus the one with the best response for the defender. To find the defender's best response, the defender does not need to know the attacker's payoff since the focus is on the defender's highest payoff. As a result, the payoff table can be simplified to the one presented in Table 2.

As can be noted in Table 2, although the best response strategy alleviates the defender's uncertainty about the attacker's payoff, it still suffers from uncertainty about the attacker's move based on which of the best responses should be identified. Without knowing the attacker's move ahead of time, and to avoid the uncertainty that comes with anticipating the attacker's move, the defender can allocate defensive resources to minimize his losses. An attacker's payoff may be multifaceted, including but not limited to, causing fatalities and property losses, distributing propaganda, and so forth. However, when it comes to chemical and process facilities, the defender (the facility owner, for instance) may justifiably presume that the attacker's payoff would be proportionate (not equal) to the defender's loss (mostly, property losses). This presumption, even if not realistic, would lead the defender to take actions to minimize his losses regardless of the attacker's payoffs.

For this purpose, the defender would look at the rows of Table 2 and in each row highlight the cell with the highest loss. The defender then selects the row with the lowest highlighted number, i.e., the lowest highest loss (Table 3). The defender's move corresponding to the selected row is called a minimax strategy,[21] ensuring that in the worst-case scenario (in the context of the attack scenario of interest), the defender's loss would not exceed the minimax value. Since in a minimax strategy the defender's focus is on reducing their potential losses regardless of the attacker's payoff, an a priori estimation of the attacker's payoff (or expected utility) would not be needed.

TABLE 3 Minimax strategy to find the defender's best response

	Attack A	Attack B	Minimax strategy
Defend A	a1	b1	$L_A = \max(a1, b1)$
Defend B	c1	d1	$L_B = \max(c1, d1)$

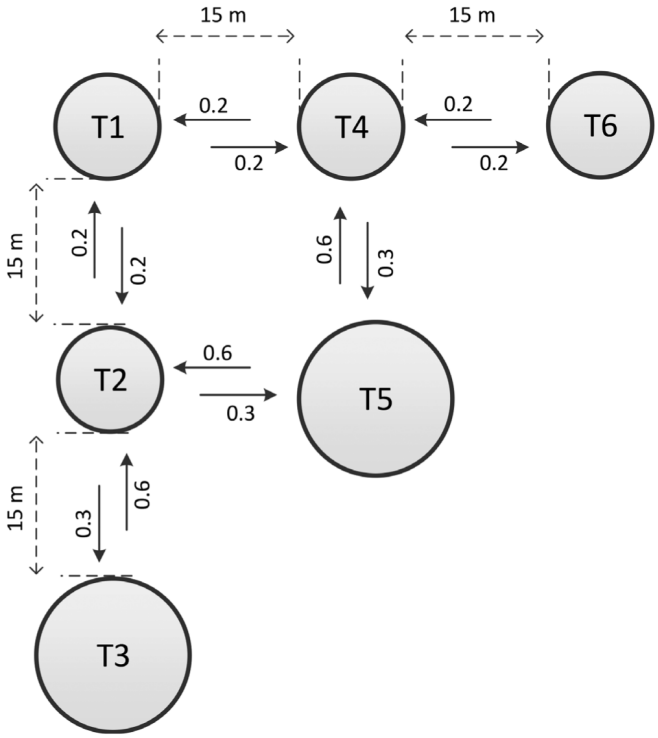

FIGURE 1 Layout of an oil terminal comprising six oil storage tanks. The arcs and their numbers denote, respectively, the direction and probability of fire propagation.

In Table 3, the loss attributed to any move made by the defender is equal to the maximum possible loss resulting from that move. For instance, the loss of "Defend A" is taken as $L_A = \max(a1, b1)$. As such, between "Defend A" and "Defend B", the defender selects the one attributed to the lowest loss, that is, $\min(L_A, L_B)$. In other words, by implementing the best response that the defender identifies via the minimax strategy, the maximum loss the defender would expect to incur $\overline{L_i}$ can be calculated as:

$$\overline{L_i} = \min_{x_i} \max_{x_j} L_i(x_i, x_j), \tag{2}$$

where i is the index of the defender, j is the index of the attacker, x_i is the decision made by the defender, x_j is the decision taken by the attacker, and L_i is the payoff the defender gets as a function of his and the attacker's decisions.

Threat description	Pipe bomb	Suitcase bomb	Compact sedan	Sedan
Explosive mass (kg TNT)	2.3	23	227	454

TABLE 4 Conventional IEDs and their explosive mass in terms of TNT equivalent[25]

This aspect of minimax strategy (i.e., getting rid of the need for calculation of attacker's payoff) is very important since the oversimplifications and thus the large uncertainties introduced to the calculation of the attacker's expected payoff could otherwise make a big difference in the allocation of defensive resources. Such oversimplification may arise, for instance, because the assumption that attackers will be expected value maximizers (maximizing the expected fatalities or property losses) might be too strong and inadequate if factors such as the attacker's motivation and required resources, cost of the attack, feasibility, and propaganda value are not taken into account.[7,16,22,23]

The minimax strategy seems to be a viable strategy to cope with imminent terrorist attacks to chemical and process facilities when time is not sufficient to acquire the information required to predict the attacker's payoffs.

3 | IED ATTACK RISK REDUCTION

3.1 | An illustrative example

For illustrative purposes, the layout of an oil terminal is depicted in Figure 1, which consists of six oil storage tanks of two different sizes: The large tanks, T3 and T5, and the smaller tanks, T1, T2, T4, and T6. Based on a thorough consequence analysis, the probability of fire propagation from a burning tank to an adjacent tank can be calculated using dose–effect relationships[24] given the dimensions of the adjacent tank and the amount of heat radiation it would receive. Figure 1 shows illustrative fire propagation probabilities, assuming the completion of a detailed consequence analysis, which is beyond the scope of the present study. In Figure 1, for instance, if T1 is on fire, the probability of T2 catching fire is 0.2, and vice versa.

Further assume that based on a threat assessment by law enforcement and intelligence services while considering a recent attack to a similar oil terminal in the vicinity, an attack with pipe bombs to the tank terminal with the aim of causing fire and property damage has been identified as the potential attack scenario. A simple semi-qualitative method for threat identification and ranking can be found in FEMA 452.[25]

The extent of damage caused by an improvised explosive device (IED) such as pipe bombs depends on the amount and the type of explosive materials, their construction, and the stand-off distance between the center of detonation and the target vessel. More information on the components, main ingredients, chemical reactions, and strength of IEDs can be found in Wilkinson et al.[26] and Landucci et al.[27] Table 4 presents a number of conventional IEDs and their explosive capacity (TNT equivalent mass) based on the maximum explosive materials that could be carried or delivered.[25]

In order to evaluate the impact of IEDs on process vessels, the overpressure generated by the IED's detonation should be calculated, for instance, using TNT equivalent mode[28]:

$$P = \frac{M_{TNT}^{\frac{1}{3}}}{r} + 4.4\,\frac{M_{TNT}^{\frac{2}{3}}}{r^2} + 14.0\,\frac{M_{TNT}}{r^3}, \tag{3}$$

where P (bar) is the peak overpressure, r (m) is the distance measured from the center of gravity of the explosion to the target vessel, and M_{TNT} (kg) is the equivalent mass of trinitrotoluene (TNT) determined for an IED as in Table 4. Having the amount of overpressure at a target vessel and the threshold values in Table 5,[29] it is then possible to determine whether the impact of a blast wave on the target vessel would be detrimental enough to result in a loss of containment. Such loss of containment can reasonably be assumed to result in a fire or explosion, particularly due to the heat generated by the detonation of the IED, which in turn can trigger secondary fires and explosions, initiating a domino effect in the facility.[30]

Considering the explosive mass of a pipe bomb (2.3 kg, as in Table 4) and the least amount of overpressure required to cause damage to an atmospheric storage tank (0.22 bar, as in Table 5), Equation (3) can be used to find the maximum distance of $r_{max} = 11$ m from the detonation center of a pipe bomb within which a storage tank can be damaged. Knowing the damage radius of 11 m and the rim-to-rim distance of 15 m between the adjacent tanks as in Figure 1, a pipe bomb placed roughly in the middle of two adjacent tanks can cause damage and ignite both of the tanks.

3.2 | Risk-based minimax strategy

The IED attack to the tank terminal is depicted in Figure 1 and the possibility of fire propagation in the form of a domino effect can be modeled using a dynamic Bayesian network (DBN) approach,[31] given that the attack would cause fire to the targeted tanks. In this regard, the tanks are represented as the nodes of the DBN while the escalation probabilities depicted in Figure 1 are used to fill in the conditional probability tables.

Figure 2 displays the developed DBN where tanks T2 and T5 have been attacked with the pipe bomb and are burning. This assumption has been realized in the model by instantiating the conditional probability tables of T2 and T5 to P(T = fire) = 1.0. If the analyst doubts that the IED attack would result in fire at T2 or T5, the instantiated probability could take any number below 1.0 to reflect the analyst's uncertainty. Implementing the DBN in GeNIe software, the probability of fire spread to the other tanks can be obtained. Table 6 lists such probabilities resulting from the IED attacks to each possible

piar of adjacent tanks, where the attacked tanks have been denoted by a unity probability.

The expected loss of each IED attack scenario can be estimated using the loss associated with the damage to each storage tank. Assume that given an IED attack, the defender would incur a cost of 3 units for damage to a large tank and a cost of 1.5 units for damage to a smaller tank, if the tanks are full (a full storage tank is filled to 0.85 of its capacity). Having these costs, a concurrent IED attack to T2 and T5 would result in the largest damage (see the last row of Table 6), and can be taken as the most credible attack scenario from a purely PRA perspective (we will later demonstrate how relying solely on the results of PRA could lead to choosing a different and not necessarily an efficient mitigating strategy).

TABLE 5 Overpressure threshold values to assess the impact of blast wave on process vessels[29]

Target vessel	Atmospheric	Pressurized (toxic materials)	Pressurized (flammable materials)
Blast wave (bar)	0.22	0.2	0.31

In the context of inherent safety, reducing the inventory of hazardous substances in chemical and process plants has been proposed as an effective way to limit the effect of not only accidental[32] but also intentional events.[33]

In the present study, emptying the storage tanks is chosen as a safety measure for reducing the risk of an imminent IED attack, which cannot be prevented but could be mitigated.[33] This safety measure can be categorized as the "minimization" and/or "limitation of effects" principles in the context of inherent safety. In this regard, it is assumed that the tank terminal cannot afford to keep more than one large tank or two smaller tanks empty, for instance, due to adverse impacts on the supply chain or loss of revenue. Keeping a large storage tank and a smaller storage tank empty would cost the terminal 0.5 and 0.3 units, respectively. Accordingly, attack to an empty tank would cost 2 units and 1 units, respectively, for a large tank and a smaller tank. The costs incurred because of IED attack or keeping

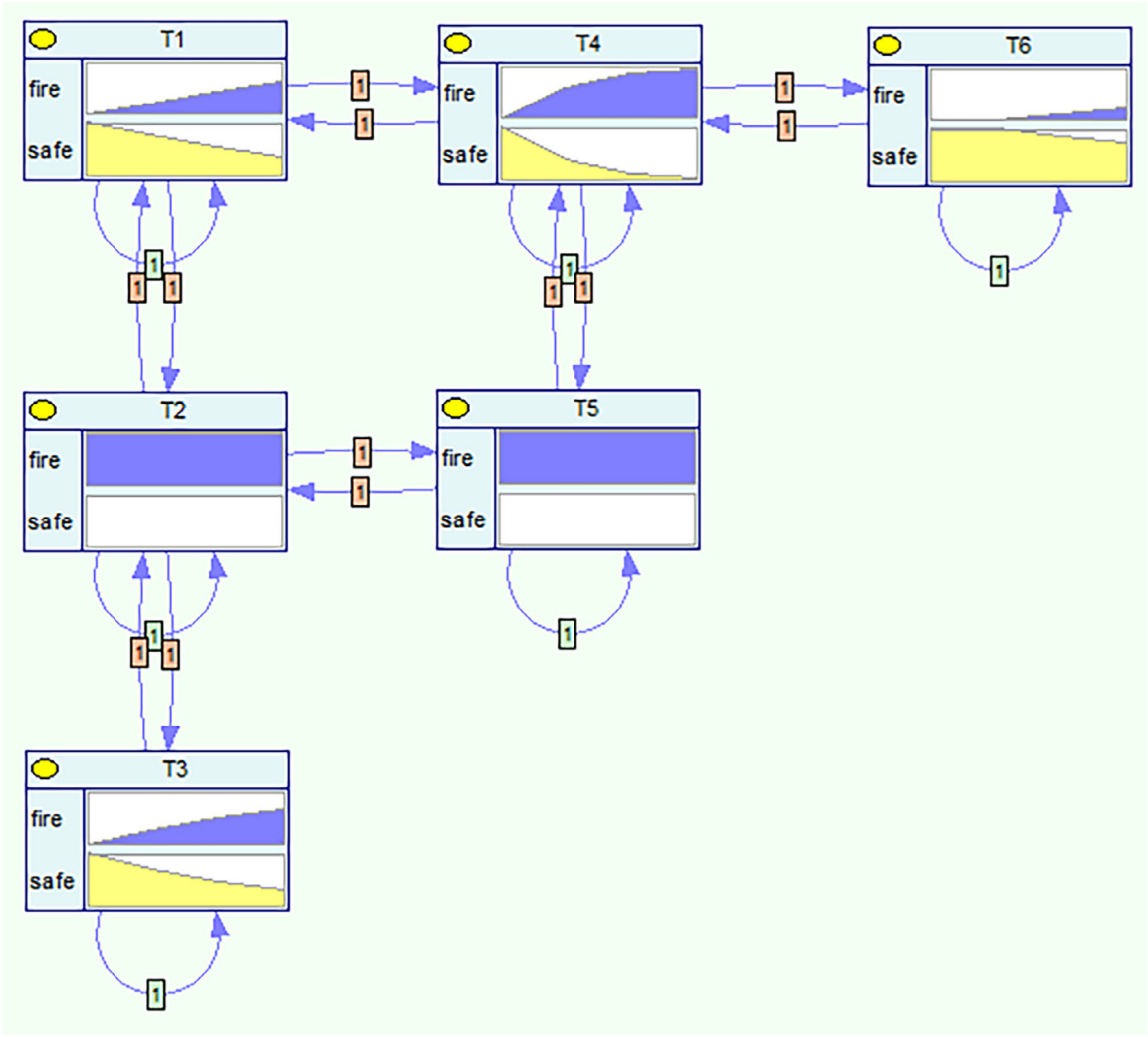

FIGURE 2 DBN for modeling the domino effect triggered by IED attack to T2 and T5. For the graphs presented inside each node, the abscissa and ordinate denote, respectively, time and probability.

empty are listed in Table 7. As can be noted from the numbers in Table 7, the attack to a full or empty tank does not seem to make a significant difference in terms of cost: For instance, attack to a full large tank would cause a damage of 3 units to the defender, while the same attack to an empty large tank would cause a damage of 2.5 units (the cost of the tank, 2, plus the cost of loss of revenue, 0.5). However, attack to an empty tank is expected to limit the damage to the target tank only, which prevents greater damage caused by potential domino effects.

The DBN developed in Figure 2 can be used to calculate the expected loss the defender would incur by defending tank Ti (keeping them empty) while tank Tj might get attacked, bearing in mind that (i) the defender cannot afford defending more than one large tank or two smaller tanks and (ii) the attacker would not be able to attack more than two adjacent tanks. For the sake of exemplification, consider a case where the defender decides to "Defend T1" and the attacker "Attack T1 and T2". We have chosen this simple defend–attack scenario because the corresponding domino effect can readily be modeled as a simple BN with no need for the DBN, as illustrated in Figure 3.

As can be seen in Figure 3, tank T1, because of being empty, does not contribute to the domino effect though it has been damaged due to the IED attack. Having a simple sequence of fires starting from T2, the probability of damage directly due to the IED attack (T1 and T2) or indirectly due to fire propagation inside the tank terminal (T3–T6) can be calculated as: $P(T1) = P(T2) = 1.0$; $P(T3) = P(T5) = 0.3$; $P(T4) = 0.3 \times 0.6 = 0.18$; $P(T6) = 0.3 \times 0.6 \times 0.2 = 0.036$. Having the damage probability P(Ti) and the cost C(Ti) of each tank, the corresponding expected loss L(Ti) can be calculated as $L(Ti) = P(Ti) \times C(Ti)$.

For the defend–attack scenario under consideration, this would result in: $L(T1) = 1.0 \times (1 + 0.3) = 1.3$, consisting of the cost of keeping empty (0.3) and the cost of damage due to IED attack (1); $L(T2) = 1.0 \times 1.5 = 1.5$; $L(T3) = L(T5) = 0.3 \times 3 = 0.9$; $L(T4) = 0.18 \times 1.5 = 0.27$; $L(T6) = 0.036 \times 1.5 = 0.054$. As a result, the total expected loss would be the sum of individual expected losses as $1.3 + 1.5 + 0.9 + 0.9 + 0.27 + 0.054 = 4.92$, shown as the first value in the payoff table in Table 8 (denoted with a bold number). Having the expected loss of each defend–attack scenario in Table 8, the maximum expected loss resulting from each "Defend" decision can be identified, as listed in the last column of the table. Making a comparison among the maximum expected losses, the minimum–maximum expected loss is attributed to the defensive decision, "Defend T2 and T4". In other words, considering all the possible attack scenarios in Table 8, by keeping T2 and T4 empty, the maximum expected loss would not exceed 5.20 units.

TABLE 6 Domino effect probabilities for given IED attack to each pair of adjacent tanks in Figure 1: Attack to T2 and T5 is associated with the maximum expected loss (denoted in bold numbers)

T1	**1**	**0.51**	**0.62**	**0.51**	**0.62**	**1**
T2	1	1	0.94	0.44	**1**	0.68
T3	0.66	1	0.38	0.06	0.66	0.19
T4	0.68	0.44	1	1	0.94	1
T5	0.71	0.66	1	0.66	**1**	0.71
T6	0.13	0.04	0.49	1	0.27	0.49
Expected loss	8.31	7.97	8.72	6.60	**9.22**	7.43

3.3 | Discussion

3.3.1 | Security risk management based on PRA

As previously discussed, prioritizing the defensive resources merely based upon a pure PRA, if not combined with decision-making and optimization techniques, would not necessarily result in identifying the most effective risk management strategies.[10] To show the aforementioned inefficacy of PRA, two cases will be investigated: Case 1 and Case 2.

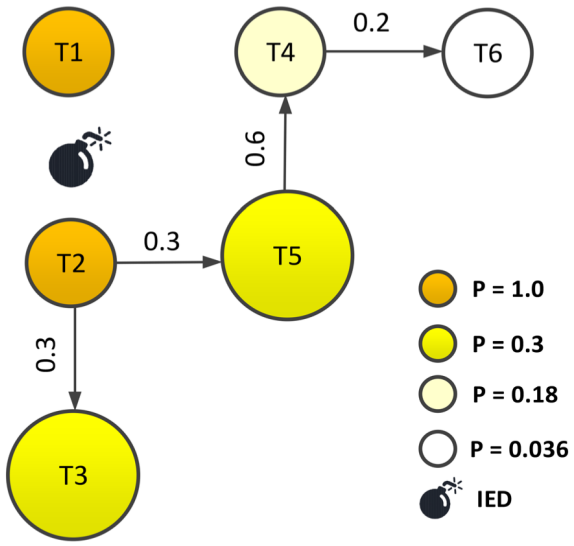

FIGURE 3 Probability of fire propagation due to IED attack to T1 and T2. Since T1 is empty of flammable substances, it will get damaged but cannot contribute to the domino effect (i.e., no direct arc from T1 to T4)

TABLE 7 Cost associated with attacking to or keeping a storage tank empty (from defender's viewpoint)

	Cost		
	Attack to a full tank	**Attack to an empty tank**	**Keep a tank empty**
Large tank	3	2	0.5
Smaller tank	1.5	1	0.3

TABLE 8 Payoff table for identifying the optimal decision using minimax strategy

	Attack →						Decision strategies	
Defend ↓	T1 and T2	T2 and T3	T1 and T4	T2 and T5	T4 and T5	T4 and T6	Minimax, Max. loss	Bayes–Laplace, Avg. loss
T1	**4.92**	7.03	4.43	6.98	6.74	4.83	7.03	5.82
T2	3.34	4.30	4.84	4.96	6.02	4.71	6.02	4.70
T3	5.66	5.63	5.55	7.16	6.05	5.15	7.16	5.87
T4	5.44	6.26	3.46	6.62	5.92	2.80	6.62	5.08
T5	5.44	5.98	4.96	5.27	4.70	4.51	5.98	5.14
T6	5.83	6.37	5.38	7.20	6.94	4.51	7.20	6.04
T1 and T2	2.60	4.60	4.30	5.80	6.20	4.88	6.20	4.73
T1 and T4	5.13	6.43	2.60	6.98	6.16	3.10	6.98	5.07
T1 and T6	5.22	6.53	4.63	7.32	7.04	4.65	7.32	5.90
T2 and T4	3.30	4.60	3.30	5.20	5.20	3.10	**5.20**	**4.12**
T2 and T6	3.62	4.60	5.06	5.80	6.22	4.50	6.22	4.97
T4 and T6	5.76	6.50	3.76	6.92	6.22	2.60	6.92	5.29

Case 1

Assume that the defender would choose to make their decision based on the outcomes of risk assessment where the IED attack to T2 and T5 would result in the highest risk of damage (see the expected losses in the last row of Table 6). Taking "Attack to T2 and T5" as the most likely attack scenario due to its maximum expected loss, the defender would choose "Defend T2" as the most cost-beneficial decision attributed to a minimum expected loss of 4.96 units (i.e., the value resulting from the intersection of "Defend T2" and "Attack T2 and T5" in Table 8).

An attacker who suspects that the defender would base their decision merely on the results of risk assessment would choose to launch the second riskier attack scenario (the one attributed to 8.72 as the second highest expected loss in Table 6), that is, "Attack T4 and T5". In such a case, the defender would end up with a loss of 6.02 units (i.e., the value resulting from the intersection of "Defend T2" and "Attack T4 and T5" in Table 8), which is higher than a loss of 5.20 resulting from a risk-based minimax strategy.

Case 2

One may also argue that strategies such as minimax are more suitable for decision-making under ignorance, that is, when a decision maker has no idea about the likelihood of "the states of nature",[21] which in our case are attack scenarios. In this regard, a PRA advocate may see it more appropriate to assign likelihoods to the attack scenarios proportional to their relative expected loss.[9] According to the expected losses of attack scenarios in Table 6, for instance, the likelihood of "Attack T1 and T2" can be calculated as P(Attack T1 and T2) = 8.31/(8.31 + 7.97 + 8.72 + 6.6 + 9.22 + 7.43) = 0.17. Assuming such likelihoods for the attack scenarios, the payoff table in Table 8 may be used for decision-making under risk. In decision-making under risk, the decision with the lowest expected loss can be chosen as the best defense strategy. The expected loss and standard deviation of defensive decisions are presented in Table 9. Considering only the expected losses, "Defend T2 and T4" may be selected due to having resulted in the lowest mean loss.

In decision-making under risk, between two decision alternatives with more or less the same mean values, the one with a lower standard deviation should be chosen as the desired alternative.[21] For this purpose, the Microsoft Excel® Data Analysis toolpak was used to conduct ANOVA (Analysis of Variance) between the two closest decision alternatives, that is, "Defend T2 and T4" and "Defend T2", to see if there was a significant difference between them in terms of resultant loss (to see if the slightly higher standard deviation of the former decision could have neutralized its slightly lower mean value, thus making the latter decision a better choice.) In ANOVA, the null hypothesis assumes that the mean values of two groups of data are identical whereas the alternative hypothesis assumes the opposite. If the null hypothesis is rejected, the alternative hypothesis would be accepted. The result of the ANOVA test with a significant level of $\alpha = 0.05$ did not provide enough evidence to reject the null hypothesis, indicating that the two decision alternatives do not result in substantially different losses. Accordingly, a PRA advocate may equally choose either decision alternative.

Nevertheless, it should be noted that if "Defend T2" is chosen, the defender may end up with 3.34 and 6.02 units of damage in the best and worst attack scenarios, respectively, while given "Defend T2 and T4", he may end up with 3.10 and 5.20 units of damage, in the best and worst attack scenarios, respectively. As can be seen in the case of "Defend T2 and T4", the lower and upper bounds of damage are still lower than the lower and upper bounds of damage of "Defend T2", indicating the former is a better option.

3.3.2 | How about other game theory strategies?

Minimax strategy is not the only game theoretic strategy for decision-making under uncertainty that can alleviate the need for estimating attack likelihoods and attack payoffs—two parameters with the highest uncertainty when it comes to security risk assessment.

TABLE 9 Identifying the optimal decision via decision-making under risk (mean loss)

Defend ↓	Attack scenarios (the numbers in the brackets present attack likelihoods)						Decision strategy	
	T1 and T2 (0.17)	T2 and T3 (0.17)	T1 and T4 (0.15)	T2 and T5 (0.19)	T4 and T5 (0.18)	T4 and T6 (0.14)	Mean loss	Standard deviation
T1	4.92	7.03	4.43	6.98	6.74	4.83	5.90	1.10
T2	3.34	4.30	4.84	4.96	6.02	4.71	4.71	0.82
T3	5.66	5.63	5.55	7.16	6.05	5.15	5.93	0.65
T4	5.44	6.26	3.46	6.62	5.92	2.80	5.22	1.39
T5	5.44	5.98	4.96	5.27	4.70	4.51	5.16	0.48
T6	5.83	6.37	5.38	7.20	6.94	4.51	6.13	0.90
T1 and T2	2.60	4.60	4.30	5.80	6.20	4.88	4.77	1.19
T1 and T4	5.13	6.43	2.60	6.98	6.16	3.10	5.22	1.63
T1 and T6	5.22	6.53	4.63	7.32	7.04	4.65	6.00	1.10
T2 and T4	3.30	4.60	3.30	5.20	5.20	3.10	4.19	0.91
T2 and T6	3.62	4.60	5.06	5.80	6.22	4.50	5.01	0.88
T4 and T6	5.76	6.50	3.76	6.92	6.22	2.60	5.45	1.51

While a minimax strategy implies a pessimistic (or conservative) defender (decision maker) who wishes to minimize the losses if the worst-case attack scenario (the attack scenario with the largest loss) takes place, a minimin strategy may be used by an optimistic defender who wishes for the best-case attack scenario (the attack scenario with the least loss). Bayes–Laplace strategy, on the other hand, may refer to a defender who considers a broader range of attack scenarios, including both worst-case and best-case scenarios, while giving equal weight to the scenarios. Between the minimin and Bayes–Laplace strategies, the former may sound too optimistic (if not ignorant) and likely to result in nonoptimal decisions for the defender. The Bayes–Laplace strategy, however, still makes sense as it implies a decision maker who is neither as conservative as a minimax decision maker nor as optimistic as a minimin decision maker.

To make a comparison between a defender who employs the minimax strategy and one who employs the Bayes–Laplace strategy, the results of the Bayes–Laplace strategy are also shown in the last column of Table 8. To apply the Bayes–Laplace strategy, the average value of the payoffs for a given decision is taken as the representative payoff of the decision. For instance, under the Bayes–Laplace strategy, the representative payoff for the decision "Defend T1" can be calculated as $(4.92 + 7.03 + 4.43 + 6.98 + 6.74 + 4.83)/6 = 5.82$, meaning that if this decision is taken, the average payoff would be 5.82 units. Having the average payoff of each decision, the decision with the lowest payoff can then be selected as the optimal decision. Given the average payoffs in the last column of Table 8, the decision "Defend T2 and T4" can be selected as the optimal decision under the Bayes–Laplace strategy, which is interestingly the same result as the one under the minimax strategy. Although both strategies point to the same optimal decision, the decision as to which strategy to use still depends on the decision maker's (the security manager's) expectation of the attack's severity and whether they want to be prepared for the worst-case attack scenario (the minimax strategy) or a range of attack scenarios (the Bayes–Laplace strategy).

However, it is worth noting that the average losses used in the Bayes–Laplace strategy for decision-making (e.g., those presented in the last column of Table 8), similar to any expected value, are the average losses the decision maker could expect if the entire range of the attack scenarios theoretically occur for each decision alternative, which obviously may not be realistic or feasible over the lifetime of a process plant. That being said, if the results obtained from the applications of the Bayes–Laplace and minimax strategies were different, the result of the minimax strategy would be more realistic and effective in security risk management of intentional domino effects under not only physical attacks[33] but cyberattacks.[34]

4 | CONCLUSIONS

PRA has long been used as an effective tool for prioritizing critical assets and allocating safety measures in a cost-effective way. However, if not combined with decision-making techniques, the use of PRA to achieve the same goals in the domain of security risk management has been criticized for diverting resources away from the most critical assets (i.e., resulting in suboptimal or nonoptimal decisions).

In the present study, we demonstrated, via a hypothetical tank terminal, that relying solely on PRA would likely lead to a suboptimal (if not nonoptimal) allocation of safety and security measures. We also illustrated that the combination of PRA and the minimax strategy (a simultaneous game theory strategy under imperfect information) could readily outperform PRA, resulting in a more effective allocation of resources. In this regard, PRA can be used to estimate the defender's expected loss for potential attack scenarios. Considering the expected losses as the defender's payoff, the minimax strategy can then be used to identify the best response of the defender without the need to know or estimate the attack likelihoods or the attacker's payoffs. This largely alleviates one of the main challenges faced in security risk management, namely, the lack of reliable and

accurate information about the likelihood of attack scenarios and the attackers' payoffs.

ACKNOWLEDGMENTS

The financial support provided by the Natural Sciences and Engineering Research Council of Canada (NSERC) via a Discovery Grant (Grant No: RGPIN/03051-2021) is appreciated. The BN models in this paper were created with the GeNIe Modeler, which is freely available for academic research and teaching from BayesFusion, LLC, https://www.bayesfusion.com.[35]

DATA AVAILABILITY STATEMENT

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

ORCID

Nima Khakzad https://orcid.org/0000-0002-3899-6830

REFERENCES

1. Dillon RL, Liebe RM, Bestafka T. Risk-based decision making for terrorism applications. *Risk Anal*. 2009;29(3):321-335.
2. Landucci G, Khakzad N, Reniers G. *Physical Security in the Process Industry: Theory with Applications*. Elsevier; 2020.
3. Reniers G, Landucci G, Khakzad N. What safety models and principles can be adapted and used in security science? *J Loss Prevent Proc Indust*. 2020;64:104068.
4. Government Accounting Office. Combating Terrorism: Actions Needed to Guide Services Antiterrorism Efforts at Installations. Washington, DC: Government Accounting Office Report GAO 03-14, November, 2002.
5. CCPS (Center for Chemical Process Safety). 2003. Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites. American Institute of Chemical Engineers, New York, Wiley; ISBN-13: 978-0816908776.
6. *American Society of Mechanical Engineers (ASME) Innovative Technologies Institute, all-Hazards Risk and Resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus (SM) Approach*. American Society of Mechanical Engineers; 2009.
7. Bier VM, Haphuriwat N, Menoyo J, Zimmerman R, Culpen AM. Optimal resource allocation for defense of targets based on differing measures of attractiveness. *Risk Anal*. 2008;28(3):763-770.
8. API (American Petroleum Institute). 2012. API RP-780: Security risk assessment methodology for the petroleum and petrochemical industries.
9. McGill WL, Ayyub B, Kaminskiy M. Risk analysis for critical asset protection. *Risk Anal*. 2007;27(5):1265-1281.
10. Cox LA. Some limitations of "risk = threat × vulnerability × consequence" for risk analysis of terrorist attacks. *Risk Anal*. 2008;28(6):1749-1761.
11. Cox LA. Improving risk-based decision making for terrorism applications. *Risk Anal*. 2009;29(3):336-341.
12. Cox LA. Game theory and risk analysis. *Risk Anal*. 2009;29(8):1062-1068.
13. Brown GG, Cox LA. How probabilistic risk assessment can mislead terrorism risk analysts. *Risk Anal*. 2011;31(2):196-204.
14. Khakzad N, Reniers G, van Gelder P. A multi-criteria decision making approach to security assessment of hazardous facilities. *J Loss Prevent Proc Indust*. 2017;48:234-243.
15. Pate-Cornell ME, Guikema S. Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. *Milit Operat Res*. 2002;7(4):5-23.
16. Bier VM. Choosing what to protect. *Risk Anal*. 2007;27(3):607-620.
17. Brown GG, Carlyle WM, Salmeron J, Wood K. Defending critical infrastructure. *Interfaces*. 2006;36(6):530-544.
18. Rios J, Rios ID. Adversarial risk analysis for counterterrorism modeling. *Risk Anal*. 2012;32(5):894-915.
19. Hausken K. Probabilistic risk analysis and game theory. *Risk Anal*. 2002;22(1):17-27.
20. Bonanno G. 2018. Game theory. Volume 1: basic concepts. 2nd edition. CreateSpace Independent Publishing Platform, ISBN-13: 978-1983604638.
21. Churchill G, Whalen T. Decisions under uncertainty. In: Kacprzyk J, Krawczak M, Zadrozny S, eds. *Issues in Information Technology*. EXIT; 2002:201-224.
22. Ridinger G, John RS, McBride M, Scurich N. Attacker deterrence and perceived risk in a Stackelberg security game. *Risk Anal*. 2016;36(8):1666-1681.
23. Bhashyam SS, Montibeller G. In the opponent's shoes: increasing the behavioral validity of attackers' judgments in counterterrorism models. *Risk Anal*. 2016;36(4):666-680.
24. Landucci G, Gubinelli G, Antonioni G, Cozzani V. The assessment of the damage probability of storage tanks in domino events. *Accident Anal Prevent*. 2009;41:1206-1215.
25. FEMA 452. Risk Assessment: A how-to Guide to Mitigate Potential Terrorist Attacks against Buildings. 2005. The Federal Emergency Management Agency (FEMA). Available online from: https://www.fema.gov/fema-452-risk-assessment-how-guide-mitigate-potential-terrorist-attacks-against-buildings. Last checked on 6-26-2019.
26. Wilkinson A, Bevan J, Biddle I. *Improvised Explosive Devices (IED): an Introduction*. Small Arms Survey; 2008, Chapter 14:136-144.
27. Landucci G, Reniers G, Cozzani V, Salzano E. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. *Reliab Eng Syst Safety*. 2015;143:53-62.
28. Bounds WL. *Design of Blast Resistant Buildings in Petrochemical Facilities*. ASCE Publications; 1997.
29. Cozzani V, Gubinelli G, Salzano E. Escalation thresholds in the assessment of domino accidental events. *J Hazard Mater*. 2006;129:1-21.
30. Salzano E, Landucci G, Khakzad N, Reniers G, Cozzani V. Vulnerability assessment of chemical plants to intentional acts. In: Cozzani V, Reniers G, eds. *Dynamic Risk Assessment and Management of Domino Effects and Cascading Events in the Process Industry*. Elsevier; 2021:175-192, ISBN 9780081028384. doi:10.1016/B978-0-08-102838-4.00012-2
31. Khakzad N. Application of dynamic Bayesian network to risk analysis of domino effects in chemical infrastructures. *Reliab Eng Syst Safety*. 2015;138:263-272.
32. Amyotte P, Goraya A, Hendershot D, Khan F. Incorporation of inherent safety principles in process safety management. *Proc Safety Prog*. 2007;26(4):333-346.
33. Khakzad N, Reniers G. Low-capacity utilization of process plants: a cost-robust approach to tackle man-made domino effects. *Reliab Eng Syst Safety*. 2019;191:106114.
34. Arief R, Khakzad N, Pieters W. Mitigating cyberattack related domino effects in process plants via ICS segmentation. *J Inform Sec Appl*. 2020;51:102450.
35. GeNIe 4.0 Academic Installer. (2022). Available online from: https://download.bayesfusion.com/files.html?category=Academia.

How to cite this article: Khakzad N. Reducing the risk of intentional domino effects in process plants: A risk-based minimax strategy. *Process Saf Prog*. 2023;42(2):281-289. doi:10.1002/prs.12443