Integrated Risk Management of Hazardous Processing Facilities

Guozheng Song,[a] Faisal Khan ,[a] and Ming Yang [b]

[a]Centre for Risk, Integrity and Safety Engineering (C-RISE), Faculty of Engineering and Applied Science, Memorial University of Newfoundland, St. John's, Newfoundland A1B 3X5, Canada; (for correspondence)
[b]Department of Chemical Engineering, School of Engineering, Nazarbayev University, Astana 010000, Kazakhstan

Published online 9 August 2018 in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/prs.11978

Processing facilities handling large amounts of hazardous substances are attractive targets for terrorists. Thus, these work sites are exposed not only to accidents but also to intentional threats. Some research has separately studied risk caused by either potential accidental events or terrorist acts. However, studies focusing on integrated risk assessment and management (dealing with both safety and security issues) are lacking. This paper proposes an approach to assess and manage integrated risks. This method is based on an influence diagram which incorporates safety and security-related factors into one framework. It considers the effects of management actions on both accidental and intentional risks. This method can help to detect hidden risk (i.e., the risk not recognized during design and operation stages) and ensure to reduce the real risk to an acceptable level by guiding the selection of management actions. The effectiveness of the proposed method is demonstrated using the overfilling risk management of an oil tank. © 2018 American Institute of Chemical Engineers Process Saf Prog 38: 42–51, 2019

Keywords: decision making; safety and security; influence diagram; multicriteria; hidden risk

INTRODUCTION

Terrorism is increasingly threatening the world, and attacks on process plants have repeatedly occurred in recent years [1]. In June 2015, a terrorist attacked a U.S.-owned chemical plant in France and caused an explosion in gas canisters, leaving one person dead and two injured [2]. Three weeks later, two explosions were caused by malicious acts at a petrochemical plant in southern France [3]. In 2016, an Algerian gas plant was hit by terrorists using rockets [4]. In the same year, suicide car bombers attacked Libya's main oil terminals (Es Sider oil export terminal), and an oil storage tank at Ras Lanuf was set on fire after a rocket hit [5]. In 2017, an attack was launched to blow up an Aramco fuel terminal in southern Saudi Arabia using a speedboat laden with explosives [6]. Process facilities are thus exposed to not only accidental but intentional risks as well, which raises challenges to risk management. The accidental and intentional risks are synergistic [7], influencing their causation and the effects of risk prevention measures, and thus affecting the decision making of risk management. In this paper, the term measure is used to represent a management action to minimize risk.

Some researchers have argued that it is not sufficient to address accidental hazards; integrated risks including accidental and intentional ones need to be studied to ascertain the real risks confronted by the process industry [7–10]. Compared to the work on separate assessment of either safety or security related risks [11,12], relatively limited work has been conducted using integrated risk assessment considering the dependency of safety and security [7]. Fovino et al. [13] incorporated intentional factors into traditional risk analysis by integrating attack trees into a pre-existent fault tree (FT). Their approach considered the dependency of intentional acts and accidental failures to obtain the integrated risk. Pietre-Cambacedes et al. [7] modeled the dependency of safety and security of critical systems using Boolean logic Driven Markov Processes. This model analyzed risk scenarios in a qualitative and quantitative form, combining safety and security aspects. As for integrated risk management, to the authors' knowledge, no specific decision model exists for integrated risks considering both safety and security aspects.

Previous works have studied the decision making for accidental risk. Yuan et al. [14] proposed a Bayesian network (BN)-based method to help allocate safety measures for dust explosions considering both available budget and acceptable residual risk. Sedki et al. [15] proposed an influence diagram (ID)-based approach to study the consequences of deviant actions of operators based on three parameters: benefit, cost, and deficit. This model enables managers to rank a set of actions through the utility calculation of each action pertaining to the criteria. However, these works only consider accidental risks, ignoring intentional ones. Thus, their selected management actions to minimize risk cannot solve the problem of hidden risks, which will be discussed in this paper. The hidden risk refers to that which managers do not recognize while conducting risk management. Aside from the works about safety-oriented concerns, some research has analyzed the measure decision for security issues. Villa et al. [16] proposed a method to conduct cost-benefit and cost-effectiveness analysis for the allocation of physical security measures. The approach helps to select economically feasible security measures with a maximum net present value considering the budget constraints of a chemical plant.

Stewart et al. [17] described risk-informed decision support for assessing the costs and benefits of counterterrorism protective measures for infrastructure. This research showed under what combination of risk reduction, threat probability, and fatality and damage costs, the counterterrorism protective measures would be cost-effective for infrastructures through three illustrative examples. However, these studies did not consider the influence of interaction of safety and security on risk reduction effects of measures. Thus, the efficiency of measures may be underestimated, negatively influencing the decision making for minimizing risk.

This paper proposes a risk-based measure decision method for integrated risk management. It discusses the process and principles of measure decision and clarifies the influence of the interaction of safety and security on decision making. This method includes the dependency of safety and security-related factors and visually shows how measures work to reduce integrated risks. By managing risks from an integrated perspective, the method avoids the underestimation of measures' effects. Furthermore, this method can detect the hidden risk to ensure that the real risk confronted by facilities is reduced to an acceptable level. The new point is that the proposed risk-based method can effectively manage integrated risks considering the dependency of safety and security.

This paper is organized as follows: background section presents the background of integrated risk, an influence diagram and the effects of measures. Method description section explains the risk-based decision-making method. A case study of overfilling of a gasoline tank is demonstrated in illustrative example section. Conclusions and future work section provides discussion and conclusions.

BACKGROUND

Integrated Risk

To facilitate the study of integrated risk, both safety-related events (i.e., accidents, incidents, mishaps, and near misses) and security-related events (i.e., terrorism, vandalism, and mischief) are called abnormal events. Safety-related events are called accidental abnormal events, while security-related events are called intentional abnormal events. The risk is defined as probability multiplied by consequences (losses) [8,18]. Following this definition, the integrated risk is the product of probability and consequence of an abnormal event. Integrated risk constitutes an accidental risk and intentional risk (see Figure 1). The basic difference between accidental and intentional risks is whether it includes harmful human intentions [19]. The accidental risk is caused by random failure (accidental abnormal events), while the intentional risk includes intentional acts (intentional abnormal events).

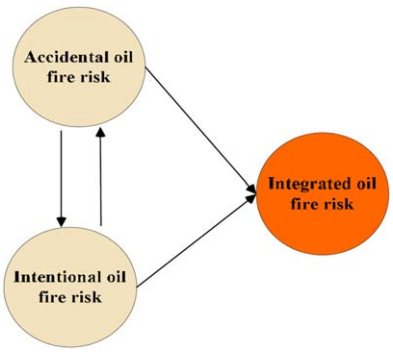

Figure 1. Integrated oil fire risk. [Color figure can be viewed at **wileyonlinelibrary.com**]

Oil fire is taken as an example to explain integrated risk. As shown in Figure 1, oil fire can occur in an accidental scenario where oil leaks due to corrosion and the leaked oil are accidentally ignited by the spark of electronic equipment; it can also occur in an intentional scenario where attackers destroy the tank to expose oil and ignite it using a lighter. The accidental scenario and intentional scenario can both lead to an oil fire. The product of probability and consequence of oil fire in both accidental and intentional scenarios is the integrated risk of an oil fire. Managing oil fire risk through an integrated perspective is necessary because accidental and intentional oil fires are dependent as shown in Figure 1, and thus a risk measure may have effects on both an accidental and intentional oil fire. For example, an effective fire suppression system can mitigate not only an accidental oil fire but also an intentional oil fire. The goal of this study is to demonstrate the advantage of integrated risk management considering the synergy of accidental and intentional abnormal events. To clearly demonstrate the function of the proposed method, some simplifications are made. The consequences (i.e., damage of abnormal events to facilities) are considered as fixed, and probabilities of abnormal events are considered as the only variable reflecting integrated risks. Thus, this study focuses on discussion about the management of occurrence probabilities of abnormal events.

Influence Diagram

An ID is a probabilistic graphical model used to help decide risk management measures under uncertainty, considering the utility (e.g., efficiency and cost) of measures. Compared to a risk assessment model like BN, besides chance nodes, ID (see Figure 2) contains two extra types of nodes—decision nodes and utility nodes [15]. Decision nodes represent the decision to apply or not to apply certain measures, while utility nodes represent the utility of decision alternatives or strategies. By analyzing the utility values of different decision alternatives, the measures reducing risks to an acceptable level are selected. Also, since the budget is limited in practice, the selected measures need to satisfy budget requirements, which can be analyzed by comparing utility values to the budget. The chance nodes, decision nodes, and utility nodes are linked using arcs. The arcs among chance nodes of an ID have the same properties as the arcs in a BN,

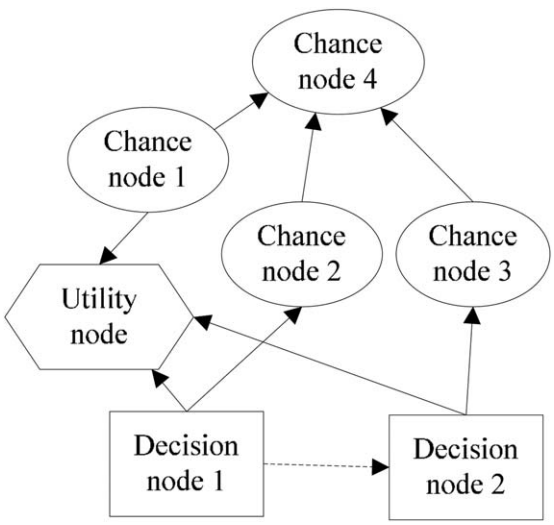

Figure 2. A general influence diagram.

representing that the linked chance nodes are dependent [20]. The arcs from decision nodes to chance nodes mean the decision of measures to be taken can change the occurrence probabilities of the linked chance variables. For example, safety training may reduce the occurrence probabilities of human error; thus, the decision node "safety training" needs to be linked to the chance node "human error." Their quantitative relationship is represented using a conditional probability table (CPT) in which the decision to "not provide safety training" corresponds to a high occurrence probability of human error (e.g., 0.45), while the decision to "provide safety training" corresponds to a smaller occurrence probability such as 0.1 [21,22]. In this way, the ID establishes a link between a decision and the causal factor. When the measure "provides safety training" is analyzed by a manager, the state of the decision node is set as "provide safety training." Then the ID is updated, and it obtains the updated risks after application of the measure. The arcs from chance nodes and decision nodes to utility nodes demonstrate that the utility values are influenced by the state combination of chance nodes and decision nodes. Their relationships are represented by conditional tables which show the utility values corresponding to different state combinations of chance nodes and decision nodes. When different measures are applied, the ID is updated to obtain new utility values based on which the measures are assessed and the decision is made. The dashed arcs among decision nodes represent the decision sequence of different measures [15,23]. The shapes of chance, decision and utility nodes in an ID are different. Chance nodes are oval, while decision nodes are rectangular [24]. The utility nodes are hexagons [15]. The values of chance nodes are probabilities, ranging from 0 to 1, while those of utility nodes do not have the range limitation. The decision nodes represent the proposed measures; thus, they only have two states, "application of the measure" or "no application of the measure" without numerical values. The ID including decision and utility nodes is an excellent tool for decision making. It can represent the dependency of safety and security-related factors and facilitate measure selection considering measures' effects on accidental and intentional risks.

Effects of Measures on Accidental and Intentional Risks

Safety and security are dependent, as shown in Figure 3; thus, the safety measures may influence security, while security measures influence safety. For example, the safety measure of a high-level alarm can also inform the high level

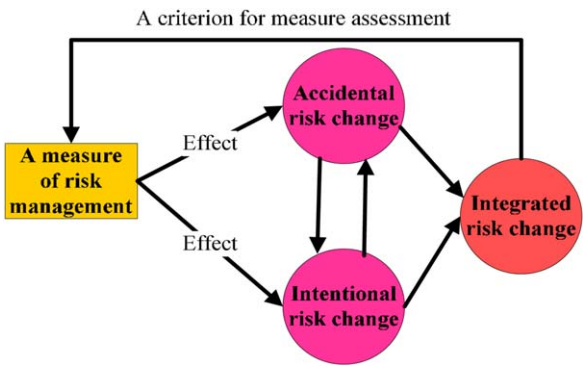

Figure 3. The effects of measures on accidental and intentional risks. [Color figure can be viewed at **wileyonlinelibrary.com**]

caused by intentional acts, and thus prevent the intentional damage. Personal Protective Equipment (PPE) can protect workers from abnormal events (e.g., toxic gas release) caused by both accidental and intentional causes. The security measure of unauthorized access control can not only prevent attackers but also reduce human-induced unintentional events (human error), since it can avoid accidents by preventing unauthorized or untrained personnel from entering specific workplaces. However, some measures may have conflicting effects on safety and security. The security measure "non-explosion-proof security surveillance facilities" may cause an accidental explosion of released flammable substances. The safety measure "warning signs for accidents" may provide attack thoughts for terrorists. Since measures have effects on both safety and security, the decision needs to be made from an integrated perspective. Figure 3 also demonstrates that integrated risk change reflects the efficiency of measures which serves as one of the criteria for measure assessment.

A real accident is analyzed to explain how risk management measures can influence safety and security. According to a CSB report [25], a toxic chemical release occurred during an unloading operation at the MGPI Processing, Inc. in Atchison, the United States in 2016. The driver of the cargo tank motor vehicle (CTMV) incorrectly connected the discharge hose of sulfuric acid to the unsecured fill line for the sodium hypochlorite bulk tank. This led to the inadvertent mixing of sulfuric acid and sodium hypochlorite, which caused a reaction in the sodium hypochlorite bulk tank. This reaction promoted the release of a cloud containing toxic chlorine gas and other compounds. Because of this gas release, over 140 individuals sought medical attention and six of them were hospitalized. In this toxic gas release, some measures influenced safety and security-related risks. The padlock on the cam lever dust cap that secures the fill line is designed to prevent unauthorized access. It can not only prevent human error (incorrect connection) as occurred in the MGPI accident, but can also prevent the damage caused by intentional acts. Thus, the measure "install padlock on the cam lever dust cap" can reduce both accidental and intentional risks. Another measure has opposite effects on accidental risk and intentional risk. To protect the respirators from theft and intentional damage, operators have a practice of locking respirators between shelves. Thus, in an emergency condition, operators would be unable to access their respirators, thereby worsening the severity of the injuries and becoming a source of potential fatality. The measure "locking respirators" benefits security to some degree, but it increases the safety-related risk. The accident occurred because the driver mistook the sulfuric acid's fill line for the sodium hypochlorite's. If the measure "add markers of the chemical at fill line connections" is applied, this error can be avoided. However, such markers may provide information for attackers to cause damage. Thus, the measure "add markers of the chemical at fill line connections" can reduce the accidental risk, but may increase the intentional risk. Another measure, "install additional monitoring and emergency shutdown devices," as applied by MGPI after the accident, can detect a release caused by either accidental or intentional events and shut down the operation to minimize the damage. Thus, this measure can reduce the accidental and intentional risks at the same time. Through the analysis of the MGPI toxic gas release incident, it is evident that a measure can simultaneously influence safety and security-related risks. Thus, a measure decision of risk management needs to consider the measure's effects on accidental and intentional risks. The effects of measures on integrated risk can be treated as a criterion for measure assessment and decision making.

METHOD DESCRIPTION

Methodology Framework

This ID-based risk management method is divided into two stages. As mentioned in integrated risk section, the consequences (i.e., damage of abnormal events to facilities) are considered as fixed, and then the integrated probability of abnormal events reflects integrated risk. Thus, this study focuses on discussion about the management of probabilities of abnormal events. The first stage is integrated probability assessment, while the second is measure decision. In the first stage, a BN was established for the assessment of an integrated probability of an abnormal event. If the probability is unacceptable, potential measures are proposed and an ID is established in stage two based on the BN of stage one. The rationality analysis of proposed measures is conducted first. Rationality of measures is explained in criteria of measure assessment section. Then the effects and costs of reasonable measures are assessed using the ID, based on which the decision is made. The methodology framework is shown in Figure 4.

Approach for Risk-based Measure Decision

Criteria of Measure Assessment

Three criteria are applied for measure decisions: rationality, risk reduction efficiency and cost.

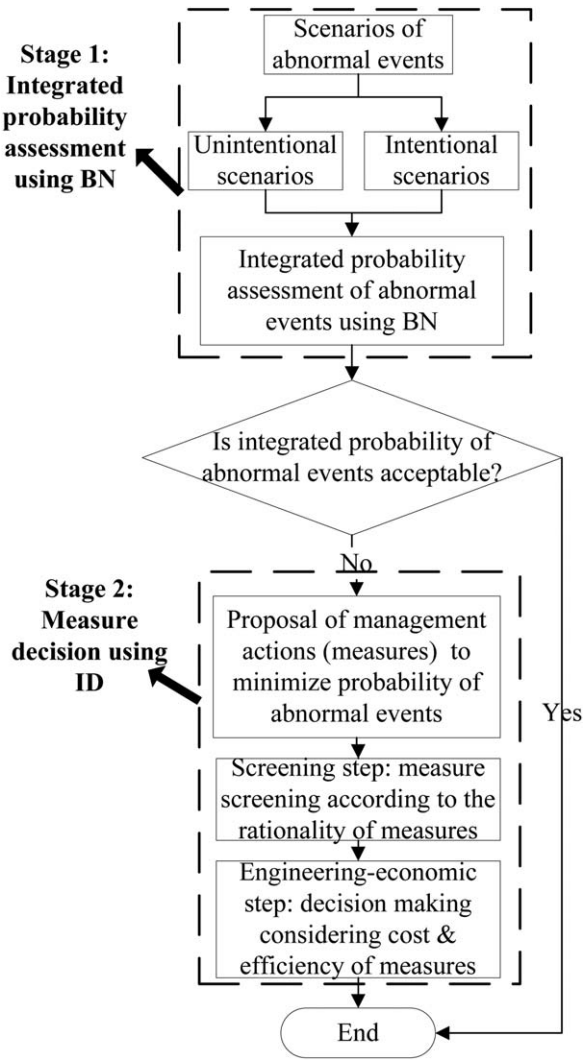

Figure 4. Methodology framework.

1. Rationality: Rationality of measures means that measures do not influence the normal operation of the process plant. For example, attackers may release oil through valves. If all valves are removed, it causes problems for the oil release by attackers, but the function of valves necessary for normal production is missing. Thus, this measure is not rational. To conserve assessment resources, such measures are discarded in the screening step of decision making.
2. Risk reduction efficiency: The goal of measures is to reduce risks. Thus, the selected measures (strategies) need to reduce risk to an acceptable range effectively.
3. Cost: Risk can be reduced with the increase of investment for risk management. In an extreme case, the process plant is protected by the security measures used to protect the military base and the security risk may be reduced to close to 0. However, those measures are too expensive to apply. Practically, risk management has the limitation of budget, and the cost of measures cannot exceed the budget allocation. The cost of measures should be a criterion of measure selection. Thus, when several measures (strategies) can reduce risks to an acceptable range, the economic ones are preferred.

Risk Assessment

BN is applied to assess the integrated probability of the abnormal event considering the dependency of safety and security, as shown in Figure 5a. First, an abnormal event (e.g., gas release or explosions) is defined, and then the accidental and intentional causal factors are identified. These causal factors and the abnormal event are represented using chance nodes in BN. According to the dependency among causal factors and abnormal events, these nodes are linked by arcs, and their quantitative relationship is represented using CPTs [20]. In this way, the dependency between safety and security is included (see the green arcs in Figure 5a), and the integrated probability of the abnormal event is obtained. If the calculated probability is higher than the accepted standard, risk management measures are requested.

Decision Making

1. Measure proposal

   Experts propose potential measures for integrated risk reduction based on the causal factors. The measures can be inherent, engineered, or procedural [14].
2. Measure assessment

   Decision nodes and utility nodes are added to the BN to obtain an ID (see Figure 5b). The decision nodes representing measures are linked to related chance nodes. Their effects on the linked chance nodes are represented using CPTs. Besides adding cost as a utility node, the node "abnormal event" changes from a chance node to a utility node, since the probability change of the abnormal event is a parameter for effect assessment of the measure. Thus, there are two utility nodes in the ID. To assess the cost of these measures, these decision nodes are also linked to the utility (cost) node. After establishing the ID, measures are assessed in two steps based on the criteria.

Screening step: Proposed measures are analyzed to see whether they influence normal operations. If a measure influences normal operations, it is not rational and needs to be discarded. The screening process makes the analysis of the next step clearer.

Engineering-economic step: This step includes the efficiency and cost assessment of measures. The decision nodes are set as "application" or "no application"; then the updated integrated probability of the abnormal event and costs of measures is obtained. The updated probability of the abnormal event and cost of measures is compared to the accepted

standard and budget to select management measures. If several measures (strategies) satisfy the requirement of risk reduction, the economical one is selected. The cost cannot exceed the budget designation.

This method uses a graphical model to clearly show how the measures reduce the integrated risks in a visual form. For example, the red arcs in Figure 5b represent how measure 2 reduces the integrated risk. Measure 2 works on the accidental causal factor 3 which contributes accidental and intentional abnormal events; thus, measure 2 can influence the occurrence probabilities of both accidental and intentional abnormal events. This visual form can assist experts to propose further measures, which are explained in illustrative example section. Furthermore, using CPTs, this model has a flexible form to represent the relationship between measures and causal factors. The relationships between measures and factors have two types. The first is that the measure eliminates causal factors [26], while the second improves the state of factors. For example, if the avoiding safety measure 2 [26] in Figure 5b eliminates the safety-related causal factor 3. The proposed model uses a CPT (see Table 1) to represent this relationship without a structural change of the model. Table 2 shows another relationship: the application of measure 1 reduces the occurrence probability of accidental causal factor 1 to a smaller value (0.05) instead of eliminating this causal factor.

ILLUSTRATIVE EXAMPLE

Overfilling of storage tanks is a potential hazard for offloading operations of gasoline. It can lead to fire and explosions, causing severe damage to the community and environment [27,28]. Thus, controlling the occurrence of overfilling to an acceptable level is very important for the safe offloading operation in an oil storage depot. An illustrative example of overfilling a gasoline storage tank is analyzed to demonstrate the function of the proposed method. This case study is analyzed based on a practical overflow accident which occurred at the Caribbean Petroleum Corporation facility [27]. In 2009, an overflow occurred in San Juan Bay when the Cape Bruny cargo ship was unloading more than 11.5 million gallons of gasoline to various tanks on site. Tank 409 started to overflow between the 11 p.m. and 12 a.m. check on October 22. The released gasoline formed a vapour and exploded, burning 17 of the 48 tanks. The CSB report [27] revealed the following causes for the overfilling. The level measure gauge and transmitter did not work; thus, operators could not obtain accurate tank levels. In this situation, operators incorrectly estimated the tank fill time due to lacking the ability to identify and incorporate the flow rate change in real time into tank fill time calculations. No independent alarm existed to inform operators about the high level of gasoline. Therefore, the operators failed to shut down or divert the flow before overfilling. After failing to shut down the flow manually, no automatic overfilling prevention system existed to prevent potential overfilling, rendering the occurrence of overfilling.

Overfilling Probability Assessment

As described in method description section, BN is applied to assess the occurrence probability of gasoline overfilling. This model not only considers the accidental factors identified based on the practical case [27], but also includes the security factors. For the intentional perspective, this case study considers a specific attack scenario where an outsider creeps into a storage farm without firearms and attempts to cause an overflow. To achieve this goal, attackers need to launch attacks, enter the storage farm, and successfully cause the overflow. Thus, lax entrance control and lax security inside the farm contribute to the intentionally caused overfilling. The identified root causal factors and their prior probabilities are shown in Table 3. These prior probabilities are decided through an informed estimation based on the available literature [29,30]. The storage farm has a much weaker

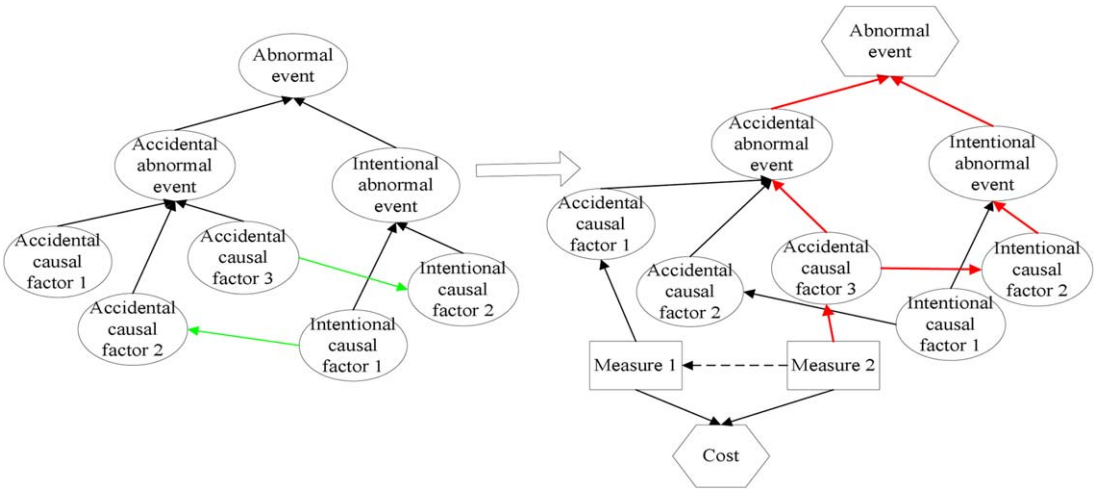

Figure 5. The establishment of ID based on BN. (a) BN for risk assessment (b) ID for risk management. [Color figure can be viewed at **wileyonlinelibrary.com**]

Table 1. CPT for accidental causal factor 3.

Measure 2	Application	No Application
Poor state of accidental causal factor 3	0	0.10
Good state of accidental causal factor 3	1	0.90

security level than chemical plants; thus, its probabilities of lax entrance control and lax security inside the farm are considered to be high. According to [27], since the plant does not have an independent high-level alarm and automatic overfilling prevention system, the prior probabilities of these two factors are 1.

After identifying causal factors and analyzing their relationships, the BN is established and shown in Figure 6. This model includes the dependency of safety and security-related factors (see the blue, green, and orange arcs). Specifically, when attackers attempt to cause overfilling, the automatic overfilling prevention system prevents their success by diverting the flow to another tank. Furthermore, when the level reaches a critical value, the independent high-level alarm can inform operators about the danger of overfilling. By this, the operators may detect the intentional acts and prevent the intentionally caused overfilling. Moreover, when attackers operate the valves to divert the flow to full tanks, the attackers' acts may be detected in time by operators in the control room by monitoring the abnormal level change. Thus, the three accidental factors, "failure of the automatic overfilling prevention system," "failure of the independent high-level alarm" and "not obtaining gasoline level" contribute not only to accidental overfilling but also to overfilling caused by attackers. By linking the three accidental causal factors to the security node "successfully cause overfilling" the dependency between safety and security is established in the model.

The occurrence probability of gasoline overfilling is calculated using the BN of Figure 6. As shown in row 2 and column 4 of Table 5, the occurrence probability of gasoline overflow is 1.48 E −2. In this case, the accepted standard for gasoline overflow is considered as 1.00 E −3. Then, it is observed that the occurrence probability of overfilling is unacceptable; thus, measures are needed to manage the risk of overflow.

Table 2. CPT for accidental causal factor 1.

Measure 1	Application	No Application
Poor state of accidental causal factor 1	0.05	0.10
Good state of accidental causal factor 1	0.95	0.90

Table 3. Root causal factors and prior probabilities [29, 30].

Root Causal Factors	Prior Probabilities
Malfunction of the level measure gauge	1.05 E−1
Failure of the transmitter	2.43 E−2
Incorrect estimation of the level	1.10 E−1
Failure of the independent high-level alarm	1.00
Failure of the automatic overfilling prevention system	1.00
Attack	1.00 E−1
Lax entrance control	3.00 E−1
Lax security inside the farm	2.50 E−1

Risk Management

Potential measures are proposed to reduce the overflow probability.

1. Removing all valves
   Attackers can operate valves to divert flow to full tanks, thereby causing overfilling. Thus, when removing all valves, a hazardous factor for intentional overfilling is eliminated.
2. Education for level estimation
   When the level measure gauge fails, workers need to estimate the gasoline level and calculate filling time. If the estimation is correct, the flow can be manually diverted before a tank is full. Therefore, educating operators to estimate levels correctly can help to avoid accidental overfilling.
3. Installation of an independent high-level alarm
   The independent high-level alarm can inform operators to stop or divert flow to avoid overfilling when a level reaches the critical value, even if the primary system of level measure fails.

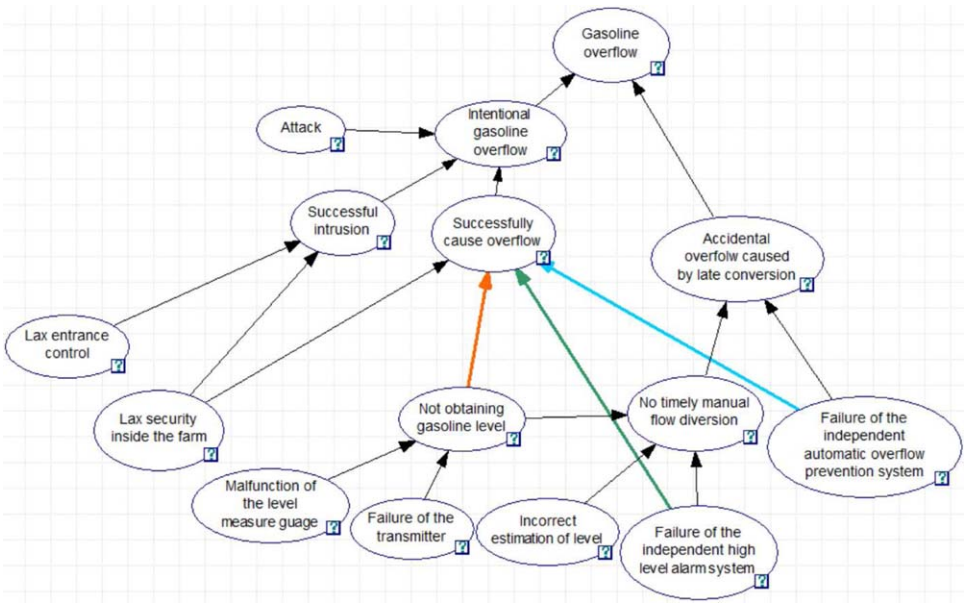

Figure 6. The BN for gasoline overflow assessment. [Color figure can be viewed at **wileyonlinelibrary.com**]

4. Installation of an automatic overfilling prevention system
   The automatic overfilling prevention system can automatically stop or divert the flow to another tank when the level is beyond the critical value to avoid overfilling.
5. Inspection and maintenance of level measure gauge
   The level measure gauge provides required level information for operators to divert the flow in time. As a procedural measure, "inspection and maintenance of level measure gauge" improves the operation of the level measure gauge, which helps to reduce the overfilling probability.

These measures are assessed based on the criteria (rationality, risk reduction efficiency, and cost) explained in method description section. First, the rationality of measures is analyzed. For the measure "removing all valves," if all valves are removed, operators cannot control the flow, negatively influencing the offloading operation. Thus, this measure is not rational in this case study, and it needs to be discarded. The remaining measures (education for level estimation, installation of an independent high-level alarm, installation of an automatic overfilling prevention system, and inspection and maintenance of level measure gauge) do not influence the required operations; thus, they are rational. The effects and cost of these reasonable measures are further analyzed to select the proper measures. After linking these reasonable measures with corresponding causal factors in Figure 6, the ID is obtained, as shown in Figure 7. It is worth noting that the chance node "gasoline overflow" of BN is converted to a utility node in the ID since the probability of gasoline overflow serves as an index for measure assessment. Besides the utility node "gasoline overflow," another utility node "cost" is added in the ID. Then CPTs of causal nodes influenced by measures are decided according to the related literature [29] and experts' opinion. Taking the CPT of failure of an independent high-level alarm as an example, its CPT is shown in Table 4. It shows that when the measure installation of an independent high-level alarm is applied, the probability of failure of the independent high-level alarm is reduced from 1 to 0.043 [29].

Table 4. The CPT for the failure of the independent high-level alarm [29].

Installation of an Independent high-level alarm	Application	No Application
Failure of an independent high-level alarm	0.043	1
Success of an independent high-level alarm	0.957	0

The obtained ID in Figure 7 visually shows the risk reduction process with the proposed measures. For example, the measure "education for level estimation" reduces the integrated overfilling risk by reducing the incorrect estimation of the level. This visual diagram helps to detect which causal factors still do not have measures, thereby providing help for further measure proposal. For instance, the causal factor "failure of the transmitter" does not have a reduction measure. It reminds experts whether measures are available to reduce the failure of the transmitter when additional measures are needed. Furthermore, when numerous factors and measures are involved in a complicated problem, it is difficult for managers to select proper strategies which include multi-measures. This model can conveniently calculate the cost and effects of strategies on accidental and intentional risks. Thus, this model facilitates strategy selection for complicated problems.

The management measures need to reduce the probability of overfilling to an acceptable level. Furthermore, the cost of selected measures needs to be smaller than the budget allocation. Thus, the measures (strategies) should first satisfy the requirement of a probability reduction of overfilling. Then, among all the satisfied measures (strategies) for probability reduction, the economical ones are selected to manage overfilling risk. Assume that the budget for risk management is \$10,000. To analyze efficiency and cost of measures, each of the four measures is set as "application" by turn, while the other three measures are set as "no application." The cost of each measure and corresponding probabilities of overfilling, intentional overfilling, and accidental overfilling are obtained and shown in Table 5.

The overfilling probabilities after using corresponding measures are displayed in rows 3–6 and column 4 of Table 5, while the overfilling probability without applying measures is shown in row 2 and column 4 of Table 5. Comparing the overfilling probabilities before and after applying corresponding measures, it shows that all measures can significantly reduce the probability of overfilling. However, the measure "education for level estimation" only reduces the probability of accidental overfilling (see row 3 and columns 2, 3 of Table 5), while the other three measures reduce both accidental and intentional overfilling probabilities (see rows 4–6 and columns 2, 3 of Table 5). If the security risk is not included in this analysis, the effects of those three measures are underestimated. For example, after applying the independent high-level alarm, the overfilling probability reduces from 1.48 E −2 to 2.41 E −3. If the security risk is not considered, the effect of the measure "installation of the independent high-level alarm" is underestimated by 1.35 E −3. The error value is even more substantial than the acceptance criteria (1.00 E −3). Thus, the error cannot be ignored. Since

Table 5. The effect and cost of each measure.

Measures	Intentional Overfilling Probability	Accidental Overfilling Probability	Overfilling Probability	Cost of Measures
No	2.35 E−3	1.25 E−2	1.48 E−2	0
Education for level estimation	2.35 E−3	2.70 E−3	5.03 E−3	\$500
Inspection and maintenance of level measure gauge	1.67 E−3	1.24 E−3	2.91 E−3	\$1,000
Installation of an independent high-level alarm	1.00 E−3	1.41 E−3	2.41 E−3	\$2,000
Installation of an automatic overfilling prevention system	1.43 E−4	7.59 E−4	8.96 E−4	\$20,000

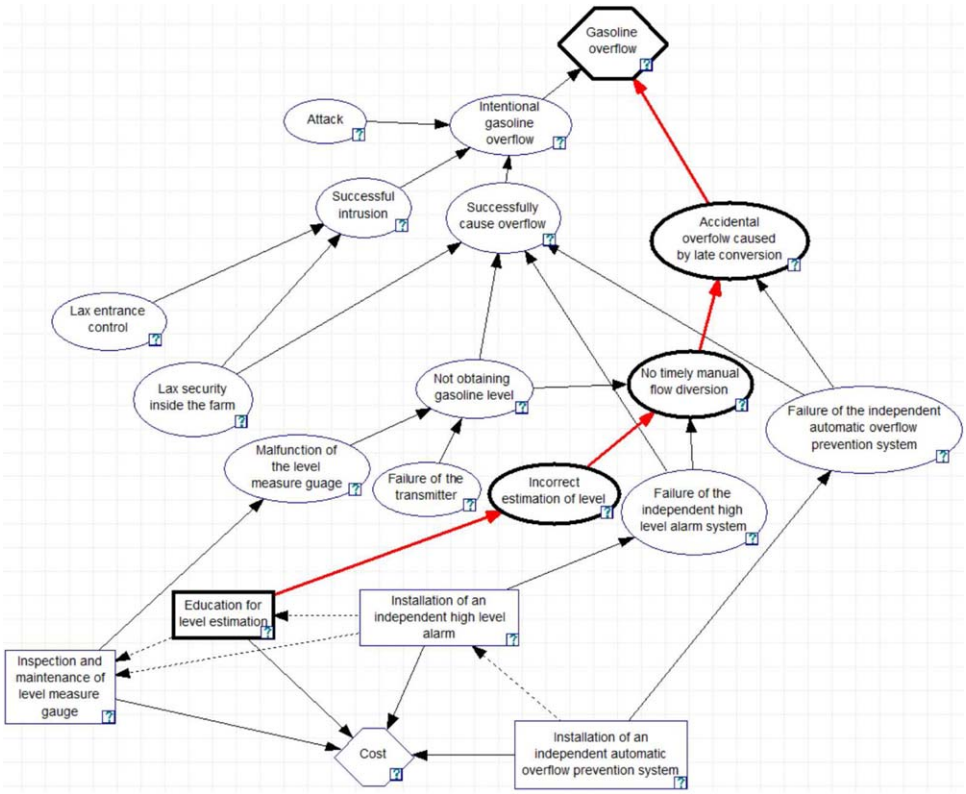

Figure 7. The ID for overfilling of a storage tank. [Color figure can be viewed at **wileyonlinelibrary.com**]

risk reduction efficiency is an essential criterion for measure selection, if the effects of measures are underestimated, it may negatively influence the decision of risk reduction measures. This proposed model avoids such underestimation and thus helps to select appropriate measures based on their actual effects.

According to the overfilling probabilities in rows 3–6 and column 4 of Table 5, only the measure "installation of an automatic overfilling prevention system" reduces the probability of overflow to an acceptable level. However, its cost exceeds the budget allowance. This means that no single measure can satisfy the requirements of risk reduction efficiency and cost control. Thus, the strategy which includes two measures is analyzed. Since the measure "installation of an automatic overfilling prevention system" cannot satisfy the budget requirement, only three measures are left to form strategies. Three strategies are obtained by combining two of the three measures. These strategies are set as applications by turn in the ID, and the effects and costs of the three strategies are shown in Table 6.

As Table 6 demonstrates, the probability of overfilling (9.79 E −4) reduces to an acceptable level, and the cost ($3,000) is kept within the budget requirement only after the application of strategy 3. Thus, strategy 3 is selected to protect the storage tank from overfilling. To avoid overfilling, measures "inspection and maintenance of level measure gauge' and 'installation of an independent high-level alarm" are applied in the tank farm.

Discussion

Rows 2–4 and column 6 of Table 6 show the cost increases from strategy 1 to strategy 3. According to an interview with a safety manager of Yancon Cathay Coal Chemicals CO., LTD in China, the plant prefers typically conservative measures for safety management. For some potential hazards, they only take simple measures such as "recording the abnormal event to remind workers to be cautious". Comparing the effects of strategies 1 and 3 in rows 2 and 4 and column 5 reveals that if only pursuing less cost, the strategy (measure) may not achieve the expected goal of risk reduction. The facility may still be exposed to unacceptable risk with the applied measures. Thus, the effect assessment of measures is essential. This was demonstrated by a rupture of the heat exchanger at Tesoro Anacortes Refinery of Washington that occurred in 2010 [31]. The heat exchanger catastrophically ruptured due to a High Temperature Hydrogen Attack (HTHA), and the highly flammable hydrogen and naphtha were released and ignited. This caused an explosion and an intense fire, burning for more than 3 h. The rupture fatally injured seven employees, and it became the largest fatal incident at a U.S. petroleum refinery since the BP Texas City accident in March 2005 [31]. According to the CSB investigation [31], mechanical integrity programs at the Tesoro Anacortes refinery emphasized inspection strategies to control the HTHA mechanism that ultimately caused the major process incident. However, inspection for HTHA is tough because the damage can be microscopic and may exist only in small localized areas of equipment. Furthermore, to identify HTHA by inspection, equipment must already be damaged by HTHA [31]. Thus, the inspection was unreliable and failed to prevent the rupture. The Tesoro Anacortes refinery simply cited nonspecific, judgment-based qualitative measures to reduce the risk of HTHA mechanisms without rigorous analyses of their effects [31]. This practical event reveals the importance of assessing the effects of measures before making the decision instead

Table 6. Effects and costs of different strategies.

Number	Strategies	Intentional Overfilling Probability	Accidental Overfilling Probability	Overfilling Probability	Cost of Strategies
1	Inspection and maintenance of level measure gauge & Education for level estimation	1.67 E−3	5.53 E−4	2.22 E−3	$2,000
2	Education for level estimation & Installation of an independent high-level alarm	1.00 E−3	4.29 E−4	1.43 E−3	$2,500
3	Inspection and maintenance of level measure gauge & Installation of an independent high-level alarm	7.12 E−4	2.68 E−4	9.79 E−4	$3,000

of focusing on the measures' cost. The proposed method provides a tool for managers to assess the effects of potential measures (strategies).

The results in Table 5 can guide strategy selection since they show the specific probabilities of either accidental overfilling or intentional overfilling. For example, among all the financially acceptable measures, the installation of an independent high-level alarm has the best effect of risk reduction. However, after its application, the intentional overflow probability is 1.00 E −3, which is not smaller than the accepted standard. This means if a measure is selected to form a strategy with the installation of an independent high-level alarm, the measure must enable the reduction of intentional overfilling. Thus, the safety measures which only work for accidental overfilling are not considered. This guides measure selection to form an effective strategy. This point is confirmed by the application results of the strategies in rows 3 and 4 and columns 3–5 of Table 6.

If intentional overfilling is ignored while conducting risk analysis and only accidental risk is considered as in previous research [14,15], the accidental overfilling probability is seen as the overfilling probability. According to row 3, column 4 and row 4, column 4 of Table 6, strategies 2 and 3 can reduce the overfilling probability (i.e., accidental overfilling probability) to 4.29 E −4 and 2.68 E −4, respectively. These overfilling probabilities are acceptable compared to the acceptance standard (1.00 E −3). Thus, both strategies 2 and 3 can satisfy the risk reduction requirement. Since the cost of strategy 2 is smaller than that of strategy 3, the conclusion would be to select strategy 2. However, this decision leaves the storage tank with an unacceptable risk, since the hidden risk (security risk) after applying strategy 2 is ignored. This proposed model can detect the hidden risk and help conduct effective risk management.

This model clearly shows the component change in the overfilling risk after the application of different strategies. According to rows 2–4 and columns 3–4 of Table 6 and row 2 and columns 2–3 of Table 5, after the application of safety strategies, the accidental overfilling probability has more significant reduction than that of intentional overfilling. Consequently, although in the original state, accidental overfilling is the significant hazard with an occurrence probability 1.25 E −2, after application of each of the three safety strategies, the probability of intentional overfilling becomes higher than that of accidental overfilling. This means that intentional acts become the major contributor to the occurrence of overfilling. For example, when strategy 2 is applied, the probability of intentional overfilling is 1.00 E −3, while its accidental counterpart reduces to 4.29 E −4. These results provide an opportunity for managers to learn significant risk sources.

CONCLUSIONS AND FUTURE WORK

This study proposed a risk-based decision-making method for integrated risk management of hazardous processing facilities. This ID-based method incorporated security risk into the risk management system. It considered the dependency of safety and security-related factors and demonstrated how measures reduce accidental and intentional risks. Potential measures (strategies) were assessed using the proposed method according to three criteria. A case study of the overfilling of storage tanks was analyzed to demonstrate the utility and effectiveness of the proposed method. The key highlights of the proposed method are:

1. Visually representing the dependency between safety and security, and showing the relationship between measures and causal factors.
2. Flexibly representing the effects of measures on causal factors. Thus, the model structure does not need to change when avoiding measures are applied.
3. Avoiding underestimation of the efficiency of measures. This provides the real measure effect which is essential for decision making.
4. Detecting the hidden risk, thereby ensuring that the selected measures (strategies) reduce the real risk to an acceptable range.
5. Enabling obtaining the accidental and intentional risks before and after the application of different measures (strategies). Not only can this inform the managers about the significant risk source, but it can also guide the selection of measures to form an effective strategy.

In future work, more interactive relationships of safety and security can be analyzed using complex engineering cases. Specifically, an engineering case can include measures with opposite effects on safety and security. Furthermore, in the complex and highly digitized modern plant, cybersecurity and physical security are also highly dependent. For example, by breaking cybersecurity, hackers can cause fire and explosion (physical events) [32]. In future work, cyber security can also be included in the integrated risk management.

ACKNOWLEDGMENTS

The authors acknowledge the financial support provided by China Scholarship Council (CSC), the Natural Sciences and Engineering Research Council of Canada (NSERC), and Canada Research Chair Program (Tier I) in Offshore Safety and Risk Engineering.

LITERATURE CITED

1. M.A. van Staalduinen, F. Khan, and V. Gadag, SVAPP methodology: A predictive security vulnerability assessment

modeling method, J Loss Prev Process Ind 43 (2016), 397–413.
2. Alex Scott, Terrorist attack hits U.S.-owned chemical plant in France. c & en Chemical & Engineering News. Available at: **https://cen.acs.org/articles/93/web/2015/06/Terrorist-Attack-Hits-US-Owned.html** (accessed 25/03/18).
3. French minister says double plant blast was criminal act. CNS news. Available at: **https://www.cnsnews.com/news/article/french-minister-says-double-plant-blast-was-criminal-act** (accessed 25/03/18).
4. Algerian gas plant hit by a rocket attack. Aljazeera. Available at: **http://www.aljazeera.com/news/2016/03/algerian-gas-plant-hit-rocket-attack-160318102631104.html** (accessed 25/03/18).
5. Reuters Staff. Islamic State fighters target Libya's main oil terminals. Reuters. Available at: **https://www.reuters.com/article/us-libya-security-port/islamic-state-fighters-target-libyas-main-oil-terminals-idUSKBN0UI18D20160104** (accessed 25/03/18).
6. Reuters Staff. Saudi Arabia says foils bombing attempt on Aramco fuel distribution terminal. Reuters. Available at: **https://www.reuters.com/article/us-saudi-security-aramco/saudi-arabia-says-foils-bombing-attempt-on-aramco-fuel-distribution-terminal-idUSKBN17S1PQ** (accessed 25/03/18).
7. L. Pietre-Cambacedes and M. Bouissou, "Modelling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes)," IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010), Istanbul, Turkey (2010), pp. 2852–2861.
8. T. Aven, A unified framework for risk and vulnerability analysis covering both safety and security, Reliab Eng Syst Saf 92 (2007), 745–754.
9. G. Reniers, P. Van Lerberghe, and C. Van Gulijk, Security risk assessment and protection in the chemical and process industry, Process Saf Prog 34 (2015), 72–83.
10. G. Song, F. Khan, and M. Yang, Probabilistic assessment of integrated safety and security related abnormal events: A Case of Chemical Plants. Safety Science (under review).
11. V. Villa, N. Paltrinieri, F. Khan, and V. Cozzani, Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry, Saf Sci 89 (2016), 77–93.
12. B.C. Ezell, S.P. Bennett, D. von Winterfeldt, J. Sokolowski, and A.J. Collins, Probabilistic risk analysis and terrorism risk, Risk Anal 30 (2010), 575–589.
13. I. Nai Fovino, M. Masera, and A. De Cian, Integrating cyber attacks within fault trees, Reliab Eng Syst Saf 94 (2009), 1394–1402.
14. Z. Yuan, N. Khakzad, F. Khan, and P. Amyotte, Risk-based optimal safety measure allocation for dust explosions, Saf Sci 74 (2015), 79–92.
15. K. Sedki, P. Polet, and F. Vanderhaegen, Using the BCD model for risk analysis: An influence diagram based approach, Eng Appl Artif Intell 26 (2013), 2172–2183.
16. V. Villa, G.L.L. Reniers, N. Paltrinieri, and V. Cozzani, Development of an economic model for counter-terrorism measures in the process industry, J Loss Prev Process Ind 49 (2017), 437–460.
17. M.G. Stewart, Risk-informed decision support for assessing the costs and benefits of protective counter-terrorism measures for infrastructure, Int J Crit Infrastruct Prot 3 (2010), 29–40.
18. T. Aven, Risk analysis and management. Basic concepts and principles, R&RATA 2 (2009), 57–73.
19. G. Reniers and P. Amyotte, Prevention in the chemical and process industries: Future directions, J Loss Prev Process Ind 25 (2012), 227–231.
20. G. Song, F. Khan, H. Wang, S. Leighton, Z. Yuan, and H. Liu, Dynamic occupational risk model for offshore operations in harsh environments, Reliab Eng Syst Saf 150 (2016), 58–64.
21. B.S. Dhillon, Human Reliability and Error in Transportation Systems - (Springer Series in Reliability Engineering), Springer-Verlag, London, 2007.
22. M. Grozdanovic and E. Stojiljkovic, Framework for human error quantification, Facta Universitatis, Series: Philosophy, Sociology and Psychology, 5 (2006), 131–144.
23. M. Arias and F.J. Díez, Cost-effectiveness analysis with influence diagrams, Methods Inf Med 54 (2015), 353–358.
24. D.N. Barton, T. Saloranta, S.J. Moe, H.O. Eggestad, and S. Kuikka, Bayesian belief networks as a meta-modelling tool in integrated river basin management - Pros and cons in evaluating nutrient abatement decisions under uncertainty in a Norwegian river basin, Ecol Econ 66 (2008), 91–104.
25. U.S. Chemical Safety and Hazard Investigation Board. Final investigation report. Final report: MGPI Case Study. Available at: **http://www.csb.gov/mgpi-processing-inc-toxic-chemical-release-/** (accessed 25/03/18).
26. Z. Yuan, N. Khakzad, F. Khan, P. Amyotte, and G. Reniers, Risk-based design of safety measures to prevent and mitigate dust explosion hazards, Ind Eng Chem Res 52 (2013), 18095–18108.
27. U.S. Chemical Safety and Hazard Investigation Board. Caribbean petroleum tank terminal explosion and multiple tank fires. Final investigation report. Available at: **http://www.csb.gov/caribbean-petroleum-refining-tank-explosion-and-fire/** (accessed 25/03/18).
28. Buncefield Major Incident Investigation Board. The Buncefield Incident 11 December 2005, 1 (2008). Available at: **http://www.hse.gov.uk/comah/buncefield/miib-final-volume1.pdf** (accessed 25/03/18).
29. T.R. Moss, The Reliability Data Handbook, London: Professional Engineering, 2005.
30. D. Gertman and H.S. Blackman, Human Reliability and Safety Analysis Data Handbook, New York; Toronto: Wiley, 1994.
31. U.S. Chemical Safety and Hazard Investigation Board. Catastrophic Rupture of Heat Exchanger (Seven Fatalities). Final investigation report. Available at: **http://www.csb.gov/assets/1/19/Tesoro_Anacortes_2014-Jan-29_Draft_for_Public_Comment.pdf** (accessed 25/03/18).
32. N. Perlroth and C. Krauss. A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. The New York Times. Available at: **https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html** (accessed 25/03/18).