DYNAMIC SAFETY AND SECURITY RISK MANAGEMENT OF HAZARDOUS OPERATIONS

By

© Guozheng Song

A Thesis submitted to the

School of Graduate Studies

in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Faculty of Engineering and Applied Science

Memorial University of Newfoundland

October 2018

St. John's Newfoundland

ABSTRACT

Hazardous operations, such as the operations in process plants, are confronted by three major risks: occupational, process and intentional damage risks. Previous works have studied these risks independently. Furthermore, these works failed to consider many important elements. For example: 1) Hazardous operations are expanding to remote areas in harsh environments, and thus harsh environmental factors need to be included in the assessment model to deal with this emerging challenge. 2) Scarce prior data can cause uncertainty of assessment results. Conventional assessment methods, such as fault trees, produce static outcomes which neither reduce the uncertainty caused by scarce data nor reflect the latest risks. 3) Variables in the models are considered to be discrete (normally binary). This approximation reduces the accuracy of assessment results. 4) Influence of intrusion scenarios on security risks is not considered. 5) Safety and security have interactions which can influence the real risk level and decision making. Existing works neither conduct a dynamic assessment of integrated risk considering such interaction in a robust framework, nor do they analyze the measure selection for the effective prevention of integrated risks.

To overcome these limitations, this research establishes a dynamic model which includes harsh environmental factors to quantify the occupational risks and identify the critical causal factors. Moreover, a continuous Bayesian network is proposed to represent the continuous variables. Intrusion scenarios have been included in the

dynamic assessment model for intrusion risk. The critical intrusion scenarios and weak links of the security system are identified. Then the interaction of safety and security is analyzed in an integrated framework. Its influence on risk level and decision making is studied using a Bayesian network and influence diagram. These methods applied in this research not only reduce the uncertainty of assessment results, but also explore a new area of integrated risk assessment and management.

ACKNOWLEDGEMENTS

My deepest gratitude gives to my supervisor Dr. Faisal Khan. Dr. Khan provides great support and guidance for my research based on his extensive knowledge and broad vision. He leads me to explore the interesting academic topic and shows me how to conduct research. He works so efficiently and I can always get his timely and valuable responses. He shows us what an outstanding professor and supervisor behaves like. Without Dr. Khan's support, I can never complete the PhD program smoothly.

I also want to thank the committee members Dr. Salim Ahmed and Dr. Ming Yang. Their contributions provide significant support for my courses and research works. I never forgot Dr. Ahmed's encouragement before my comprehensive exam. He suggested me to be relaxed and suggested me to write out the answer which was difficult to orally clarify. His encouragement and suggestions were very valuable and helpful. Dr. Yang is involved in most of my research works and he provided much help for the manuscript writing. Besides research, Dr. Yang also provided great supports in daily life.

My gratitude also goes to the members of C-RISE. They are so helpful and always glad to share their experiences. It is my fortune to work with so kind colleagues in my PhD stage.

Pursuing PhD abroad is kind of a challenge, especially at the starting stage. Fortunately,

the accompanying of friends makes my life colorful. We share the same value and admire each other. I can feel that they know me and really care about me. They let me know that I am not alone and I have a kind community belonging to. Thanks to my friends for their accompanying and supports.

I can never express how much I appreciate my family − my parents, sister and brother. They always stand behind through my ups and downs. I can always obtain their supports and get their suggestions to overcome the challenges. I believe it is the family full of love makes me become a reliable, considerate and nice man; family's support gives me the energy to pursue doctor degree and to keep me heading for higher goals in the future.

Table of Contents

List of Tables

List of Figures

List of Symbols and Abbreviations

STFs	Slips, trips and falls from height
BN	Bayesian network
CPTs	Conditional probability tables
CBN	Continuous Bayesian network
BDMP	Boolean logic Driven Markov Processes
PPE	Personal protective equipment
CTMV	The cargo tank motor vehicle
HTHA	High Temperature Hydrogen Attack
FT	Fault tree
BT	Bow-tie model
AT	Attack tree
ET	Event tree
QRA	Quantitative risk assessment
ID	Influence diagram
MCMC	Markov chain Monte Carlo method
H	High
M	Medium
L	Low
VL	Very low
TE	Top event

IE	Intermediate event
CCTV	Closed-circuit television
ILO	International Labor Organization
HSE	Health, safety and the environment

1. Introduction

1.1 Problem statement

With rapid industrialization in the 20th century, complex processes accompanied by increasing hazardous substances and risky operation conditions have significantly increased the risk in hazardous operations. [1, 2] The major risks confronted by hazardous facilities (e.g., chemical plants) come from three sources: occupational, process and intentional origins. Occupational risks and process risks are the safety risk and they have been a concern for a long time [3, 4], while the intentional risk of hazardous operations started to attract attention after 9/11, 2001. [5, 6] Safety concerns are caused by accidental failures, and in contrast, a security risk is caused by a human with harmful intention. [6] The concept of process safety started to be applied in industrial practice with the occurrence of catastrophes across the world between 1960 and 1990 [3]. With catastrophic damage to humans, facilities and the environment, these well-publicized events (see Table 1.1) have served as a driving force for the evolution of process safety [2].

Table 1.1 The catastrophic events influencing the evolution of process safety [2]

Accidents	Years	Countries	Consequences
Flixborough explosion	1974	United Kingdom	28 deaths and 36 injured
Seveso disaster	1976	Italy	Extermination of more than 80,000 animals; medical examination of thousands of people; allowance of abortion, based on the mother's decision

Bhopal gas tragedy	1984	India	At least 3,800 deaths [7]
San Juanico Disaster	1984	Mexico	550 deaths and 7000 others need medical help; severe damage on an area of about 100,000 m^2 [8]
Sandoz Chemical Spill	1986	Switzerland	14 people were treated in hospital; killed half a million fish [9]
Piper Alpha	1988	United Kingdom	167 deaths
Exxon Valdez Spill	1989	United States	Causing one of the most devastating human-caused environmental disasters.
Phillips 66	1989	United States	23 deaths and hundreds of people injured
Baia Mare Cyanide Spill	2000	Romania	About 80% of life in the Serbian section of the Tisza has been killed; caused the worst environmental disaster since the Chernobyl nuclear leak in 1986 [10]
AZF Factory Explosion	2001	France	31 deaths and numerous others injured; material damages of two billion Euros [11]
BP Texas City	2005	United States	15 deaths and almost 200 injured
T2 Explosion	2007	United States	Four deaths and 32 injured; damaged buildings within one quarter mile of the facility
Deepwater Horizon	2010	United States	11 deaths and caused an uncontrolled oil spill lasting for almost 90 days
West Fertilizer Explosion	2013	United States	15 deaths and more than 160 injured; More than 150 buildings were damaged

Another safety risk, occupational risk, started to become a topic of interest for organizations in the 19th century [12]. Occupational events can directly threaten (injure or kill) workers in hazardous operations; thus, they are a significant challenge for risk

management. The distinction between occupational accidents and process accidents is that occupational ones (e.g., slips) occur in a working life context and that the main influences are limited to the involved workers. [13] The workers are often the contributors to and the victims of occupational accidents [13]. Occupational accidents occur more often than process accidents (e.g., explosions and fire). The international Labor Organization (ILO) reports that over 313 million occupational accidents occur worldwide each year [12]. Because of the high frequency, losses caused by occupational accidents are significant. For example, UK HSE states that more than a third of all major injuries reported each year were caused by slips or trips. [14] The death of workers in the oil and gas industry was six times more likely to be caused by a fall than from an explosion. [14] Occupational events not only have serious physical and emotional influences on employees, but also lead to a loss of approximately 4% of the global gross domestic product [12].

To protect workers and facilities from occupational and process risks, research has been conducted to enhance the risk analysis of hazardous operations. [1－3, 13, 15] These studies can be classified into qualitative, semi-quantitative and quantitative. [2] Qualitative analysis involves a risk with non-numerical results [2]. Semi-quantitative analysis provides approximate results rather than exact values by assessing risk using a scoring method. Quantitative analysis can provide numerical estimation results, which create better understanding and informed decision making [2, 3] The qualitative models

include ranking, risk matrix and HAZOP etc. [2], while quantitative models contain fault tree (FT), Bow-tie (BT) and Bayesian network (BN) etc. The increasing use of quantitative risk assessment (QRA) methods has become a trend [2] and the majority of new research has focused on quantitative development [3].

Applied in diverse industries (e.g., the nuclear industry and chemical process industry), quantitative risk is measured by numerical estimation of accident likelihood and consequences. [2] A typical QRA is constituted with the following stages: (1) hazard identification; (2) probability calculation; (3) consequence assessment and (4) risk measure. [15]

Although conventional quantitative assessment methods have made great contributions to safety, they suffer from some drawbacks facing the emerging challenges. [1] Firstly, some hazardous operations (e.g., offshore oil industry) have expanded to remote areas (e.g., Arctic) with harsh environmental factors, such as extreme temperatures and strong winds. Employees are confronted by greater occupational risks working in such a harsh environment. To deal with this challenge, assessment methods including the harsh environmental factors need to be developed to support effective risk management in the new operational environment. Secondly, the conventional assessment methods (e.g., FT and BT) are static; thus, they cannot capture the risk changes caused by deviations in hazardous operations. The risk can change with various factors such as the aging of

facilities; thus, the risk may have increased after the initial assessment and the obtained static risk could be outdated for the management of the latest risks. Often only scarce data is available for risk assessment. As a result, the input data could be inaccurate, which influences the assessment accuracy. The dynamic assessment can involve the new observed information from practice and update an assessment result with these observations. Thus, dynamic assessment can reduce the uncertainty caused by scarce data. The dynamic assessment results can reflect the latest risk with a high accuracy to support effective risk management. Thirdly, the variables (i.e., causal factors, accidents and consequences) are assumed to be discrete (normally binary) in the conventional risk assessment model. The changes of continuous variables continuously influence real-time risk. When the conventional methods convert continuous variables into discrete ones, the continuous influence cannot be captured due to the discrete approximation and thus uncertainty is introduced in the assessment. In this way, the discrete assumption in the conventional models reduces the accuracy of risk assessment. This proposed research partially aims to overcome these limitations of traditional quantitative risk assessment methods.

Safety concerns have been studied for a long time. However, besides accidental failures, damage in hazardous operations can also be caused by intentional acts. After 9/11, intentional threats on hazardous facilities started to attract attention. Hazardous facilities (e.g., chemical plants) raise terrorists' interests due to their significant damage potential.

Attacks on hazardous facilities have occurred repeatedly (see Table 1.2). These attacks have caused major events, such as fire and explosions. [16,17] In such a situation, only managing accidental risks is not sufficient; security risks can no longer be ignored [18, 19]. Realizing the security challenges, some works have studied security risks of hazardous facilities. [20, 21－28] These works analyzed the vulnerability of facilities based on defence measures, but did not consider the effects of intrusion scenarios. However, in practice, the security risk level is not only related to security measures, but also depends on what it is protecting against. [29] A plant well designed for preventing the clandestine entry of strangers may have significant vulnerability in the case of a direct attack with guns. Without including the information of intrusion scenarios, the assessment result cannot reflect the real security level of hazardous facilities.

Table 1.2 Physical attacks on hazardous operations

Year	Country	Event description
2005	Spain	Suspected Basque separatists detonated bombs at two chemical plants. [30]
2006	Saudi Arabia	Two vehicles carrying explosives attempted to attack a major oil production facility. [31]
2015	France	A deliveryman attacked a US-owned chemical plant. [17]
2015	Iraq	Islamic State militants detonated explosives and set fire to the key infrastructure in Iraq's largest refinery. [16]
2015	France	Double blast was caused by criminal acts in two huge fuel tanks at a petrochemical plant. [33]
2016	Algeria	An Algerian gas plant was attacked by a rocket. [32]
2016	Iraq	Several Islamic State bombers attacked a gas plant. [34]
2016	Libya	Suicide car bombers attacked main oil terminals. [35]
2017	Saudi Arabia	A speedboat laden with explosives was used to blow up an Aramco fuel terminal. [36]

Safety and security share many commonalities. [37] Both types of events can cause damage to hazardous systems. [38] Their risk levels can be determined by the occurrence frequency of abnormal events (accidents or intentional events) and their consequences. Both of the risks need to be assessed and measures are needed once the risk levels become unacceptable. [39] These commonalities provide the basis to manage safety and security risks together. These two types of risks have interactions which can change the risk level and the effects of management measures. [19, 40] One hazardous factor of safety (security) may also contribute to security (safety) risk. Thus, if the interaction is not considered, the negative effects of hazardous factors will be partly ignored, and the real risk can be underestimated. Similarly, a measure may influence both safety and security risks. If the safety and security are not managed together, the effects of measures may be underestimated. If the measures are decided based on their effects and cost, such an underestimation could lead to incorrect selection of measures. To effectively manage risks for hazardous operations, the safety and security risks need to be assessed in an integrated framework in which measures are decided considering their effects on both safety and security risks. Because of this, some industries (e.g., aerospace industry) have conducted the analysis of safety and security risks together. [37] However, these industries mainly focus on cyber security instead of physical security. [37] In this research, safety and security risks are assessed and managed in an integrated perspective considering the interactions of safety and physical security.

1.2 Knowledge and technical gaps

Previous works have conducted research on the risk assessment and management of hazardous operations. Much research has focused on causal factor analysis of occupational accidents. [41 − 45] Researchers analyzed the causal factors for occupational accidents, such as slips, trips and falls from height (STFs), in different industries such as helicopter manufacture, the residential construction industry and the offshore oil industry. [41 − 45] Besides the works on causal factor analysis, some researchers assessed the occupational risk using different risk models, such as BT and quantitative models they proposed [14, 46, 47]. However, these works did not explore dynamic occupational risk assessment. Therefore, their works did not capture the changes and calculate the latest risks which are important to guide effective risk control. Also, their static assessment could not reduce the uncertainty caused by the inaccurate inputs. Moreover, those models did not consider the harsh environmental factors. Thus, they cannot be applied to hazardous operations in remote areas (e.g., the Arctic).

Process risk has been quantitatively studied using different models. Among these models, the discrete BN is widely used for process risk assessment in recent works. [48 − 51] It has been used to analyze the risk of a vapor ignition, drilling accidents and dust explosion, and its ability to represent dependency and conduct a dynamic assessment is demonstrated. [48 − 51] However, these studies approximate continuous variables using discrete ones. Process variables often have continuous change and continuously

influence the process risk. Discrete BN models cannot capture such continuous influence and thus their assessment accuracy is degraded by the discrete assumption. Having recognized the drawback, some researchers have attempted to incorporate continuous nodes into BNs. [52 − 54] However, limited studies have explored the development and implementation of a continuous assessment method to reduce the uncertainty caused by the discrete assumption of variables.

After 9/11, security studies have been conducted for attack process analysis, vulnerability assessment, security system development and security risk management of hazardous operations. [20, 21, 22, 26 − 28] However, the defensive ability of a system varies with different intrusion scenarios. These works only analyzed the defenders' countermeasures without considering intrusion scenarios of attackers; thus, the likelihood of a successful attack and the weakness of barriers for specific intrusion scenarios cannot be decided. Furthermore, each intrusion scenario has a corresponding intrusion feature. Without considering the intrusion scenarios, the intrusion principle and process for different intrusion scenarios cannot be clarified. Moreover, the security barriers to prevent the launching of an attack also influence the security risks. Previous models did not consider such security barriers.

The preceding works have separately conducted safety and security risk analysis. Since safety and security risks exist in the same system and have strong interconnections,

accidental and intentional factors are supposed to be studied together [19]. Few works have been undertaken on integrated safety and physical security risks. [18] Since terrorists have targeted hazardous operations (see Table 1.2), physical security and its interaction with safety need to be studied to effectively manage the risks in hazardous operations. Previous works also separately studied the decision-making for safety and security risk management of hazardous operations based on cost-effective analysis of measures. [55 − 58] A decision model for integrated risks considering both safety and security aspects is lacking. No existing studies have analyzed the influence of the interaction of safety and security on risk reduction effects of measures. Those previous studies may have underestimated the effect of measures, misleading the decision-making.

Based on this analysis, the following gaps are identified:

(1) Previous works did not consider the complete risk in hazardous operations from three major sources − occupational, process and intentional origins. Thus, the hazardous facilities could be exposed to another high risk even if one certain risk (e.g., occupational risk) is well controlled.

(2) Hazardous operations are expanding to remote areas with harsh environments. To cope with this challenge, a risk assessment model including harsh environmental factors is needed to support the risk management of hazardous operations in remote areas.

(3) Dynamic models to reduce the uncertainty caused by data scarcity and to provide the latest risks are missing for the occupational risk assessment of hazardous facilities (e.g., offshore oil facilities).

(4) Discrete assumptions of the conventional risk assessment models deteriorate the assessment accuracy. The assessment models which can represent a continuous variable and capture the influence of its continuous change are lacking.

(5) Security risk analyses of facilities only consider the security measures. The influences of intrusion scenarios are not included.

(6) Safety and security risks have interactions which can change the real risk level and the effects of measures. Safety and security risk assessment and management in an integrated framework considering their interactions are absent.

1.3 Scope and objectives

This study targets the risk assessment and management of hazardous operations, chiefly in the chemical and oil industries, considering three risk sources. It dynamically assesses the risks confronted by hazardous facilities and manages risks in an integrated way. In this research, hazardous operations refer to the operations dealing with hazardous substances. Hazardous facilities mean the facilities involved in hazardous operations. Considering the priority of preventing accident occurrences over mitigating consequences, this study focuses on assessment and management of occurrence probability of abnormal events (i.e., accidents and intentional events) instead of loss analysis. The research improves risk assessment accuracy in the following areas. Three major occupational accidents (STFs) are

studied to obtain the occupational risks in the offshore oil industry. This study represents the real logic relationships to reduce the uncertainty of assessment results. It includes harsh environmental factors to analyze the impacts of a harsh environment on occupational risks. The risk is updated using the available evidence and critical factors are identified to effectively guide risk management. Furthermore, the discrete assumption of conventional assessment methods is relaxed to accurately assess the occurrence probability of an abnormal event. Moreover, the successful intrusion probabilities considering different intrusion scenarios are assessed to support the security risk analysis. The analysis of attack motivations and the damage process are not covered in this study. After overcoming these drawbacks of the existing risk assessment methods, the safety and security risks are studied in an integrated framework, and the influence of the interaction of safety and security on the occurrence probability of abnormal events is analyzed. Since hazardous facilities attract attackers mainly due to their significant damage potential, attackers targeting hazardous facilities normally aim to cause major abnormal events such as explosions (see Table 1.2) instead of just hurting workers by causing occupational events. Thus, the security risk has a stronger interaction with process risks (risks of major accidents). Considering this, the research focuses on the interaction of process risk and security risk, and the dependency of security risk and occupational risk is not covered. This security risk focuses on the physical intentional risk, not covering the cyber causes and state conflicts.

The objectives of this study are to:

(1) Develop dynamical methods to increase risk assessment accuracy of hazardous operations considering three major risk origins.

(2) Deal with the challenge of risk assessment for hazardous facilities located in a harsh environment.

(3) Develop effective assessment and management approaches for integrated risks considering the interaction of safety and security.

The innovations of this work are identified as follows. It conducts dynamic risk assessment for hazardous facilities considering three major sources. The dynamic assessment model can obtain the latest risk and reduce the uncertainty caused by scarce data. Harsh environmental factors are included in the model to cope with the emerging challenge. The discrete assumption of previous methods is relaxed to improve the accuracy of risk assessment. The proposed assessment model for security risk considers intrusion scenarios and launching barriers. It conducts a dynamic assessment of the defensive ability of process plants and dynamic identification of critical intrusion scenarios and weak links in a security system for different intrusion scenarios. The safety and security related risk factors are analyzed in a unified framework. The integrated risk in hazardous operations is dynamically assessed and measures are decided considering the dependency of safety and security.

1.4 Organization of the thesis

This thesis is organized in a manuscript format, including five journal papers as chapters. Table 1.3 shows the journal papers completed during the research and also demonstrates the objectives and related tasks.

Table 1.3 The objectives and tasks of each chapter

Papers as chapters	Objectives	Associated tasks
Chapter 2 Dynamic Occupational Risk Model for Offshore Operations in Harsh Environments	Obtain the dynamic occupational risk of hazardous operations considering harsh environmental factors	◆ Visually represent the occurrence and escalation of occupational accidents using BTs ◆ Quantitatively represent the real logic of causal factors and occupational accidents using conditional probability tables (CPTs) ◆ Dynamically assess occupational risk with observed evidence ◆ Identify the critical causal factors to support occupational risk control
Chapter 3 Predictive Abnormal Events Analysis using Continuous Bayesian Network	Reduce the uncertainty caused by discrete assumption for dynamically probabilistic assessment and diagnosis of abnormal events of facilities	◆ Establish a continuous Bayesian network (CBN) to represent continuous variables ◆ Use Markov Chain Monte Carlo to solve CBN ◆ Demonstrate the merits of CBN for dynamically probabilistic assessment and diagnosis of abnormal events of facilities

Chapter 4 Security assessment of process facilities—Intrusion modeling	◆ Decide the defensive ability of system against different intrusion scenarios ◆ Identify critical intrusion scenarios and the weak links within the security system	◆Identify potential intrusion scenarios ◆Propose graphical models to represent the intrusion processes of different intrusion scenarios ◆Propose BN to quantify successful intrusion probabilities and security potential in different scenarios ◆Update intrusion probabilities and security potential using evidence
Chapter 5 Probabilistic Assessment of Integrated Safety and Security Related Abnormal Events: A Case of Chemical Plants	◆ Analyze the interaction of safety and security ◆ Dynamically assess the integrated probability of abnormal events considering the dependency of safety and security	◆Propose an integrated framework to incorporate safety and security-related factors ◆Establish BN to represent the dependency of safety and security ◆Dynamically analyze the influence of the interaction of safety and security on the integrated risk and causal factors' significance using BN
Chapter 6 Integrated risk management of hazardous processing facilities	◆Analyze how the interaction of safety and security influences measure decision ◆Effectively manage integrated risk considering both safety and security-related factors	◆Establish influence diagram (ID)-based management model ◆Analyze the real effects and cost of measures using ID ◆Measure selection to effectively reduce real risk to an acceptable level

The overview of each chapter is explained as follows:

Chapters 2 − 4 improve risk assessment methods to increase assessment accuracy and to fit the emerging challenge. Chapters 5 and 6 assess and manage the safety and security risks in an integrated framework. In this way, this research assesses risk in an integrated perspective with improved assessment methods to obtain the real risks and to effectively manage risks. The detailed contents are as follows:

Chapter 2: BT models are established to systematically represent the occurrence and escalation process of three occupational accidents (STFs) in the offshore oil industry considering the harsh environmental factors. Then the BTs are converted to BNs to quantitatively calculate the probabilities of occurrence and consequences of STFs. Using CPTs, the BNs represent the real logical relationships (Noisy-OR) between causal factors and occupational accidents. The occurrence probabilities and consequences of STFs are updated with observed evidence. The critical factors are identified based on their posterior occurrence probabilities and likelihood to cause the STFs, given their occurrence.

Chapter 3: The drawbacks of traditional discrete assessment models are clarified. To overcome those drawbacks, a CBN is proposed to represent the continuous variables which continuously influence the abnormal event. This CBN is used to assess the probability of abnormal events of facilities and diagnose the states of causal factors. The results show that the CBN can incorporate continuous variables and assess the

abnormal events of facilities with a higher accuracy. CBN includes various continuous distributions and thus it is difficult to solve. The Markov Chain Monte Carlo algorithm (MCMC) is used to calculate the complex CBN.

Chapter 4: The defensive ability of hazardous facilities against intrusions varies for different intrusion scenarios, which influences the security risk. The intrusion processes and principles for different intrusion scenarios are clarified using graphical models. The defensive ability of hazardous facilities is dynamically quantified for different intrusion scenarios and weak links within security systems are dynamically identified based on a proposed BN model. The BN model establishes links between different intrusion scenarios, enabling to use evidence from one intrusion scenario to update probabilities in another intrusion scenario.

Chapter 5: The occurrence probabilities of process accidents and intentional abnormal events have interactions, which could change the real risk level and significance of causal factors in critical infrastructures. This chapter establishes the dependency of safety and security, analyzes how safety and security interact, and quantifies the influence of their interaction on the risk level. The integrated risk is dynamically assessed considering the dependency of safety and security, and the real significance of causal factors is dynamically analyzed to identify critical causal factors.

Chapter 6: Hazardous operations are confronted by both accidental and intentional risks. If only accidental risk is considered for risk management, there could be hidden risk (intentional risk) after the application of measures; thus, the real risk level is still unacceptable. To effectively reduce risk, safety and security risks need to be managed together. Since a management measure may work for different risks, managing safety and security risks together can help scientifically decide the measures. This chapter established an ID-based risk management model which includes intentional factors and accidental factors. The effects and costs of potential measures are assessed, based on which the proper measures are selected.

References

[1] Faisal Khan, Seyed Javad Hashemi, Nicola Paltrinieri, Paul Amyotte, Valerio Cozzani, Genserik Reniers. Dynamic risk management: a contemporary approach to process safety management. Current Opinion in Chemical Engineering. 2016, 14: 9–17

[2] M. Sam Mannan, Olga Reyes-Valdes, Prerna Jain, Nafiz Tamim, Monir Ahammad. The Evolution of Process Safety: Current Status and Future Direction. 2016, 7: 135–162

[3] Faisal Khan, Samith Rathnayaka, Salim Ahmed. Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection. 2015, 98: 116–147

[4] Paul Swuste, Coen van Gulijk, Walter Zwaard. Safety metaphors and theories, a review of the occupational safety literature of the US, UK and The Netherlands, till the first part of the 20th century. Safety Science. 2010, 48: 1000–1018

[5] Mark Adrian van Staalduinen, Faisal Khan, Veeresh Gadag. SVAPP methodology: A predictive security vulnerability assessment modeling method. Journal of Loss Prevention in the Process Industries. 2016, 43: 397 − 413

[6] Genserik Reniers, Paul Amyotte. Prevention in the chemical and process industries: Future directions. Journal of Loss Prevention in the Process Industries. 2012, 25: 227 − 231

[7] Edward Broughton. The Bhopal disaster and its aftermath: a review. Environment Health. 2005, 4: 1−6.

[8] Arturson G.. The tragedy of San Juanico – the most severe LPG disaster in history. Burns. 1987, 13: 87-102

[9] BBC on this day. 1986: Chemical spill turns Rhine red. BBC news. Available at: <http://news.bbc.co.uk/onthisday/hi/dates/stories/november/1/newsid_4679000/4679789.stm>. [Accessed 04.10.2018]

[10] Batha E.. Death of a river. BBC news, 2000. Available at: <http://news.bbc.co.uk/2/hi/europe/642880.stm>. [Accessed 04.10.2018]

[11] Guiochon G.. On the Catastrophic Explosion of the AZF Plant in Toulouse. AIChE Spring Meeting and Global Congress on Process Safety, 2012. Available at: <http://azf.danieldissy.net/Guiochon/AZF-Toulouse-Houston.htm>. [Accessed

04.10.2018]

[12] Pieter A. Cornelissen, Joris J. Van Hoof, Menno D.T. De Jong. Determinants of safety outcomes and performance: A systematic literature review of research in four high-risk industries. Journal of Safety Research. 2017, 62: 127–141

[13] Jan Hovden, Eirik Albrechtsen, Ivonne A. Herrera. Is there a need for new theories, models and approaches to occupational accident prevention? Safety Science. 2010, 48: 950–956

[14] D. Attwood, F. Khan and B. Veitch. Can we predict occupational accident frequency? Process Safety and Environmental Protection. 2006, 84: 208–221

[15] Faisal I. Khan, S. A. Abbasi. Techniques and methodologies for risk analysis in chemical process industries. Journal of Loss Prevention in the Process Industries. 1998, 11: 261–277

[16] Stephen Snyder. An Iraqi oil refinery that was too important to destroy has just been destroyed. PRI's The World. Available at: <http://www.pri.org/stories/2015-05-27/iraqi-oil-refinery-was-too-important-destroy-has-just-been-destroyed>. [Accessed 17. 07. 18]

[17] 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 17. 07. 18]

[18] Terje Aven. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering and System Safety. 2007, 92: 745–754

[19] Ludovic Pietre-Cambacedes, Marc BouissOU. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). in: IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010). Istanbul, Turkey, 2010: 2852–2861

[20] Mark van Staalduinen, Faisal Khan. A barrier based methodology to assess site security risk. 2015 In: Proceedings of SPE E&P health, safety, security, and environmental conference. Denver, USA, 2015: 1–25.

[21] Shailendra Bajpai, J.P. Gupta. Site security for chemical process industries. Journal of Loss Prevention in the Process Industries. 2005, 18: 301–309

[22] Genserik Reniers, Paul Van Lerberghe, and Coen Van Gulijk. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Safety Progress. 2015, 34: 72–83

[23] Francesca Argenti, Gabriele Landucci, Valerio Cozzani, Genserik Reniers. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Safety Science. 2017, 94: 181–196

[24] Gabriele Landucci, Genserik Reniers, Valerio Cozzani, Ernesto Salzano. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliability Engineering and System Safety. 2015,143: 53–62

[25] Ilker Akgun, Ahmet Kandakoglu, Ahmet Fahri Ozok. Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism.

Expert Systems with Applications. 2010, 37: 3561–3573

[26] Francesca Argenti, Gabriele Landucci, Genserik Reniers, Valerio Cozzani. Vulnerability Assessment of Chemical Facilities to Intentional Attacks based on Bayesian Network. Reliability Engineering and System Safety. 2018, 169: 515–530.

[27] Donya Fakhravar, Nima Khakzad, Genserik Reniers,Valerio Cozzani. Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network. Process Safety and Environmental Protection. 2017, 111: 714–725

[28] W. L. McGill and B. M. Ayyub, Multicriteria security system performance assessment using fuzzy logic, The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology. 2007, 4: 356 − 376

[29] Union of Concerned Scientists. Available at: <http://www.ucsusa.org/nuclear-power/nuclear-plant-security#.WUloF2eGOL6>. [Accessed 17. 07. 18]

[30] Three hurt in Basque bomb blasts. BBC News. Available at: <http://news.bbc.co.uk/2/hi/europe/4549379.stm>. [Accessed 17. 07. 18]

[31] Simon Henderson. Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil. The Washington Institute. Available at: < http://www.washingtoninstitute.org/ policy-analysis/view/al-qaeda-attack-on-abqaiq-the-vulnerability-of-saudi-oil>. [Accessed 17. 07. 18]

[32] Algerian gas plant hit by rocket attack. ALJAZEERA. Available at: < http://www.aljazeera.com/news/2016/03/algerian-gas-plant-hit-rocket-attack-

160318102631104.html>. [Accessed 17. 07. 18]

[33] French minister says double plant blast was criminal act. cnsnews. Available at: < https://www.cnsnews.com/news/article/french-minister-says-double-plant-blast-was-criminal-act >. [Accessed 09. 12. 17]

[34] Ghassan Adnan and Asa Fitch. Islamic State Attacks Iraqi Gas Plant. The Wall Street Journal. Available at: <https://www.wsj.com/articles/islamic-state-attacks-iraqi-gas-plant-1463313986>. [Accessed 17. 07. 18]

[35] Ayman Al-Warfalli, Patrick Markey and Aidan Lewis. Islamic State fighters target Libya's main oil terminals. Reuters. Available at: < http://www.reuters.com/article/us-libya-security-port-idUSKBN0UI18D20160104 >. [Accessed 17. 07. 18]

[36] 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 17. 07. 18]

[37] Siwar Kriaa, Ludovic Pietre-Cambacedes, Marc Bouissou, Yoran Halgand. A survey of approaches combining safety and security for industrial control systems. Reliability Engineering and System Safety. 2015, 139:156–178

[38] Kornecki A, Liu M. Fault tree analysis for safety/security verification in aviation software. Electronics. 2013, 2: 41–56.

[39] Eames DP, Moffett JD. The integration of safety and security requirements. In:

Proceedings of the 18th international conference on computer safety, reliability and security, London, UK; 1999: 468–480.

[40] Guozheng Song, Faisal Khan, Ming Yang. Integrated risk management of hazardous processing facilities. Process Safety Progress. (In press)

[41] Amandus H, Bell J, Tiesman H, Biddle E. The Epidemiology of Slips, Trips, and Falls in a Helicopter Manufacturing Plant. Human Factors. 2012, 54: 387–395.

[42] Nenonen N. Analysing factors related to slipping, stumbling, and falling accidents at work: Application of data mining methods to Finnish occupational accidents and diseases statistics database. Applied Ergonomics. 2013, 44: 215 − 224.

[43] Courtney TK, Sorock GS, Manning DP, Collins JW, Holbein-jenny MA. Occupational slip, trip, and fall-related injuries − can the contribution of slipperiness be isolated? Ergonomics. 2001; 44: 1118 − 1137.

[44] Bentley T, Hide S, Tappin D, Moore D, Legg S, Ashby L, Parker R. Investigating risk factors for slips, trips and falls in New Zealand residential construction using incident-centred and incident-independent techniques. Ergonomics. 2006, 49: 62–77.

[45] Attwood D, Khan F, Veitch B. Offshore oil and gas occupational accidents—What is important? Journal of Loss Prevention in the Process Industries. 2006, 19: 386–398.

[46] Jacinto C, Silva C. A semi-quantitative assessment of occupational risks using bow-tie representation. Safety Science. 2010, 48: 973–979.

[47] Ale B, Baksteen H, Bellamy LJ. Quantifying occupational risk: The development of an occupational risk model. Safety Science. 2008, 46: 176–185.

[48] Khakzad N, Khan F, Amyotte P. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science. 2013, 57: 108–117.

[49] Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection. 2013, 91: 46–53.

[50] Yuan Z, Khakzad N, Khan F, Amyotte P. Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks. Risk Analysis. 2015, 35: 278 − 291.

[51] Abimbola M., Khan F., Khakzad N., Butt S. Safety and risk analysis of managed pressure drilling operation using Bayesian network. Safety Science. 2015, 76: 133–144.

[52] Yang M., Khan F., Lye L.. Precursor-based hierarchical Bayesian approach for rare event frequency estimation: A case of oil spill accidents. Process Safety and Environmental Protection. 2013, 91: 333–342.

[53] Khakzad N., Khakzad S., Khan F.. Probabilistic risk assessment of major accidents: application to offshore blowouts in the Gulf of Mexico. Nat Hazards. 2014, 74: 1759–1771

[54] Shenoy PP. Inference in hybrid Bayesian networks using mixtures of Gaussians. In: Proceedings of the 22nd conference on uncertainty in artificial intelligence, 2006: 428–36.

[55] Yuan Z., Khakzad N., Khan F., Amyotte P.. Risk-based optimal safety measure allocation for dust explosions. Safety Science. 2015, 74: 79–92

[56] Sedki K., Polet P., Vanderhaegen F.. Using the BCD model for risk analysis: An influence diagram based approach. Engineering Applications of Artificial Intelligence. 2013, 26: 2172–2183

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

[58] Stewart M.. Risk-informed decision support for assessing the costs and benefits of protective counter-terrorism measures for infrastructure. International journal of critical infrastructure protection. 2010, 3: 29–40

2. Dynamic Occupational Risk Model for Offshore Operations in Harsh Environments

Preface

A version of this chapter has been published in the Journal of Reliability Engineering and System Safety 2016; 150: 58－64. As the primary author, I reviewed related literatures, developed the BT and BN models and applied these models to analyze risks of STFs. I completed the first version of the manuscript and further revised according to the suggestions of co-authors and reviewers. Dr. Faisal Khan helped to identify the research topic and scope. Dr. Hangzhou Wang, Dr. Zhi Yuan and Hanwen Liu reviewed the manuscript and provided revision suggestions. Shelly Leighton helped to collect data from industry for the case study.

Abstract

The expansion of offshore oil exploitation into remote areas (e.g., Arctic) with harsh environments has significantly increased occupational risks. Among occupational accidents, slips, trips and falls from height (STFs) account for a significant portion. Thus, a dynamic risk assessment of the three main occupational accidents is meaningful to decrease offshore occupational risks. Bow-tie Models (BTs) were established in this study for the risk analysis of STFs considering extreme environmental factors. To relax the limitations of BTs, Bayesian networks (BNs) were developed based on BTs to dynamically assess risks of STFs. The occurrence and consequence probabilities of

STFs were respectively calculated using BTs and BNs, and the obtained probabilities verified BNs' rationality and advantage. Furthermore, the probability adaptation for STFs was accomplished in a specific scenario with BNs. Finally, posterior probabilities of basic events were achieved through diagnostic analysis, and critical basic events were analyzed based on their posterior likelihood to cause occupational accidents. The highlight is systematically analyzing STF accidents for offshore operations and dynamically assessing their risks considering the harsh environmental factors. This study can guide the allocation of prevention resources and benefit the safety management of offshore operations.

Keywords: Occupational accident; dynamic risk assessment; harsh environment; Bayesian network; Bow-tie model

2.1 Introduction

Occupational accidents are of major concern in the offshore oil industry. Statistics indicates fatalities are more likely to be caused by occupational accidents than by catastrophic events such as explosions or air transport incidents [1]. According to the RIDDOR report [2], slips, trips and falls from height (STFs) lead to approximately one third of all injuries in the offshore industry. With the recent expansion to remote areas, offshore oil exploitation meets particular challenges caused by the increasingly harsh environment, coupled with the remoteness of offshore platforms [3]. The harsh environment for offshore oil industry includes poor natural conditions (e.g., strong wind

and ice, etc.), as well as the workplace conditions deteriorating the safety situation, such as vessel motion. Risk assessment for STFs becomes more meaningful in the offshore oil industry while confronted by such increasing challenges.

Some research has been conducted about STFs. Amandus et al. [4] evaluated the causes and costs of STFs in a helicopter manufacturing plant by investigating the records of 4070 helicopter plant workers. Nenonen [5] applied the data mining method to analyze factors related to slipping, stumbling, and falling accidents at work. Courtney et al. [6] analyzed the likelihood of isolating the contribution of slipperiness to STF-related injuries from injury surveillance systems in the USA. Bentley et al. [7] identified large numbers of risk factors for STFs in residential construction through incident-centered and incident-independent methods of investigation. These studies mainly focus on cause analysis of STFs instead of quantifying risks. Furthermore, very few literatures were related to risk analysis of STFs of offshore oil industry. Attwood et al. [1, 8] determined the relative importance of influencing factors of offshore occupational accidents, and established a prediction model for the frequency and costs of offshore occupational accidents. However, this model only includes general causes, which limits its capacity to provide specific risk information of STFs. Moreover, it cannot dynamically assess the occupational risks. In the current research, the risks of STFs in offshore operations were dynamically assessed using Bayesian Networks (BNs). A novel point is the involvement of harsh environmental factors suffered by offshore platform workers.

This paper is organized as follows: Section 2.2 introduces the fundamentals of Bow-tie Models (BTs) and BNs. The dynamic assessment model of occupational risks is presented in Section 2.3. Section 2.4 explains the model application (i.e., probability calculation, probability update and critical factor analysis), and the conclusions are presented in Section 2.5.

2.2 Background

BT and BN are two powerful risk analysis models. BT is the combination of a fault tree (FT) and an event tree (ET). Its left part is the FT where the detailed causes are systematically identified following a Boolean logic; the right is the ET which starts with an accident and identifies the potential consequences depending on the states (success or failure) of safety barriers. Therefore, both causes and consequences can be incorporated in a graphical BT model [9, 10], thereby clearly presenting the accident process and potential consequences. As for BN, it is a directed acyclic graph with Bayes' theorem as the key mechanism [11, 12]. The variables in BN (i.e., risk factors, accidents, safety measures and potential consequences) are represented by nodes, while arcs are used between the nodes to reveal variable causality. The dependency degree of nodes is indicated by the conditional probability tables (CPTs). To complete BNs, the prior probabilities of root nodes and CPTs for other nodes should be provided [12]. BNs work with two inference methods, namely predictive (forward) inference and diagnostic (backward) inference [9], which are illustrated using a basic BN (Fig. 2.1) [12]. For the predictive inference, probability A is obtained according to its CPT and probability B,

following the law of total probability (equation 2.1). Diagnostic inference updates probability B given the certain state of node A (evidence) according to the Bayes' theorem (equation 2.2). The forward inference can predict the probability of rear variables, while the backward inference enables to update the probability of precedent variables given evidence. Thus, BNs can conduct predictions as well as diagnostics.

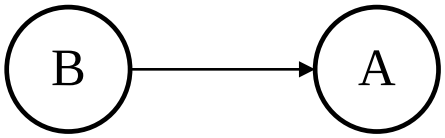


Fig. 2.1 Basic BN [12]

$$P(A) = \sum_{i=1}^{n} P(A \mid B_i) P(B_i) \tag{2.1}$$

$$P(B_k \mid A) = \frac{P(B_k) \bullet P(A \mid B_k)}{\sum_{i=1}^{n} P(B_i) \bullet P(A \mid B_i)} \tag{2.2}$$

where *n* represents the total state of *B* and *k* is the *k*th state of *B*.

BTs outperform BNs in some aspects. In a cause-accident-consequence order, BTs are an organized tool to clarify the occurrence and escalation process of accidents. Furthermore, comparing with the fact that no specific semantic guides BNs development [12], BTs can be easily established following the development procedure of FTs and ETs. However, BTs are unsuitable to dynamically quantify the occupational risks because of the limited logic relationship and static structure [10]. Fortunately,

these limitations enable to be relaxed by coupling BTs with BNs. The principle for BN to relax BT in the area of occupational risk analysis is illustrated in this paper.

As powerful assessment tools, BTs and BNs are extensively used in research. Jacinto and Silva [13] proposed a semi-quantitative assessment methodology of occupational risks for the ship building industry, in which BT was used to qualitatively identify causal pathways and consequences of relevant accidents. Ale et al. [14] introduced the concepts and overall structure of a BT-based quantifying occupational model. Martín et al. [15] used BNs to establish dependency relationships between different causes of falls from height and identified the major causes. Chen and Leu [16] assessed fall risks in bridge construction projects using BNs. Bobbio et al. [17] mapped FTs into BNs and explored the capabilities of BNs for the analysis of dependable systems. A few papers [9, 10, 18] performed dynamic risk analysis in process safety areas by transforming BTs into BNs. However, as discussed in this paper, occupational accidents often have a logic more complex than traditional OR-gates or AND-gates. Thus, only consisting of 0 and 1, the CPTs of BNs for process accidents [9] do not fit occupational accidents.

2.3 The dynamic assessment model of occupational risks

2.3.1 BT-based occupational risk model

The risk factors, safety measures and potential consequences were identified for offshore STFs (Tables 2.1 and 2.2) according to literature reviews [19－29] and

professionals' knowledge. Then BTs for STFs were respectively established based on the identified components. For the sake of simplification, this paper only presented the BT of slips (Fig. 2.2) whose symbols can be found in Tables 2.1 and 2.2. The occurrence and escalation process of slips is clearly presented through the BT-based occupational risk model in Fig. 2.2.

The prior probabilities of basic events should be assigned first to quantify occupational risks, and they were obtained using Kirsten method [30]. In this method, experts provide the qualitative evaluation using their experience and best judgment, and then corresponding probabilities can be obtained according to Table 2.3 [30－32]. This method can not only effectively involve expert experience, but also avoids the difficulty that experts meet when they directly provide probability values. A group of experts from the offshore oil industry (e.g., UTEC Survey Canada) were invited to determine prior probabilities of basic events, and the averages are shown in Table 2.1.

Table 2.1 Prior probabilities of basic events

Symbols	Description	Probability	Symbols	Description	Probability
X_1	Spillages of chemicals on floor	1.0×10^{-2}	X_{23}	Litter on floor	1.0×10^{-6}
X_2	Oil on floor	1.0×10^{-1}	X_{24}	Debris on floor	1.0×10^{-5}
X_3	Water on floor	1.0×10^{-1}	X_{25}	Other obstacles on floor	1.0×10^{-5}
X_4	Dust on floor	5.5×10^{-6}	X_{26}	Damaged floor surface	5.5×10^{-5}

X_5	Slips caused by slippery floor material	5.5×10^{-6}	X_{27}	Loose floor surface	5.5×10^{-5}
X_6	Storm	1.0×10^{-1}	X_{28}	Uneven floor surface	1.0×10^{-4}
X_7	Darkness	5.5×10^{-4}	X_{29}	Changes in level of floor	1.0×10^{-4}
X_8	Ice and snow on floor	1.0×10^{-1}	X_{30}	Unreasonable workplace arrangement	1.0×10^{-4}
X_9	Strong wind	1.0×10^{-1}	X_{31}	Crowded area	1.0×10^{-5}
X_{10}	Vessel motion	1.0×10^{-1}	X_{32}	Lighting glare	5.5×10^{-4}
X_{11}	Poor fitness	1.0×10^{-4}	X_{33}	Sudden noise	5.5×10^{-4}
X_{12}	Fatigue	1.0×10^{-1}	X_{34}	Trip caused by poor footwear	1.0×10^{-7}
X_{13}	Loads carrying	1.0×10^{-3}	X_{35}	Low quality of materials of high workplace floor and ladders	1.0×10^{-3}
X_{14}	Lack of experience	1.0×10^{-1}	X_{36}	Old age of high workplace floor and ladders	1.0×10^{-3}
X_{15}	Passive attitudes	1.0×10^{-3}	X_{37}	No handrails	1.0×10^{-6}
X_{16}	Distraction	1.0×10^{-1}	X_{38}	Slippery high workplace floor and ladders	1.0×10^{-5}
X_{17}	Stress and limited time	1.0×10^{-2}	X_{39}	Holes in high workplace floor and ladders	1.0×10^{-6}
X_{18}	Poor supervision	5.5×10^{-4}	X_{40}	Extreme low temperature	1.0×10^{-2}
X_{19}	Poor safety culture	1.0×10^{-6}	X_{41}	Poor motivation	1.0×10^{-3}
X_{20}	Poor housekeeping and maintenance	5.5×10^{-5}	X_{42}	Abnormal intelligence	1.0×10^{-3}
X_{21}	Poor safety regulation	1.0×10^{-6}	X_{43}	Poor safety training for	1.0×10^{-2}

				high place work	
X_{22}	No sign of warnings	5.5×10^{-4}	X_{44}	No warning and fencing around holes	1.0×10^{-1}

Table 2.2 Intermediate events, safety barriers and consequences

Symbols	Factors	Symbols	Factors
IE_1	Slips caused by contamination on floor	IE_{16}	Falls caused by poor situation of ladders and high workplaces
IE_2	Slips caused by poor floor condition	IE_{17}	Falls caused by harsh environments
IE_3	Slips caused by harsh environments	IE_{18}	Falls caused by poor human factors
IE_4	Slips caused by poor physical situation	IE_{19}	Falls caused by poor management
IE_5	Slips caused by lack of attention	SB_1	Handrails
IE_6	Slips caused by poor human factors	SB_2	No sharp edge materials & holes nearby
IE_7	Slips caused by poor management	SB_3	PPE
IE_8	Trips caused by contamination on floor	SB_4	Emergency rescue
IE_9	Trips caused by poor floor surface condition	SB_1'	Harness & backscratchers
IE_{10}	Trips caused by poor underfoot condition	SB_2'	Falls within two meters & no sharp edge materials at landing spots
IE_{11}	Trips caused by harsh environments	C_1	Near miss
IE_{12}	Trips caused by poor physical situation	C_2	Minor injury
IE_{13}	Trips caused by lack of attention	C_3	Lost working-time injury
IE_{14}	Trips caused by poor human factors	C_4	Unrecoverable major injury
IE_{15}	Trips caused by poor management	C_5	Fatality

Table 2.3 Classes for probabilities of occurrence [30 − 32]

Qualitative evaluation	Quantitative evaluation
Certain	1
Very high	10^{-1}
High	10^{-2}
Moderate	10^{-3}
Low	10^{-4}
Very low	10^{-5}
Extremely low	10^{-6}
Practically zero	10^{-7}

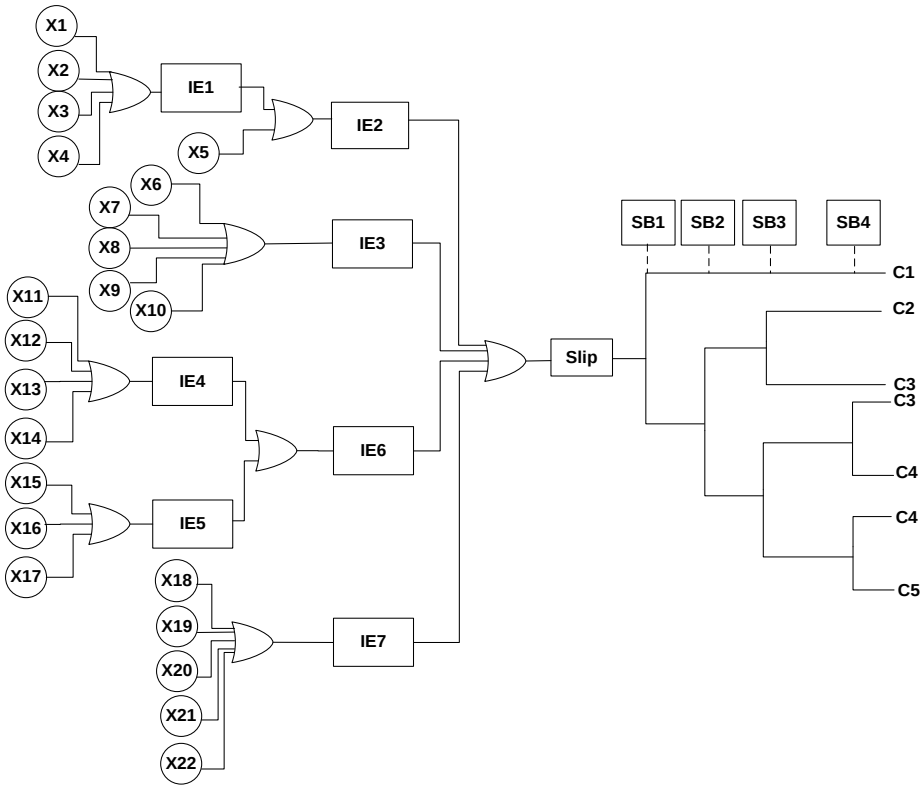


Fig. 2.2 Bow-tie model for slips (refer to tables 2.1 and 2.2)

Although BT is an excellent risk analysis tool, it has limitations to quantify occupational risks. The three main limitations are discussed as follows:

(1) The traditional logic gates of BTs may not fit occupational accidents. Most basic events of STFs have the likelihood to independently cause upper events. However,

the occurrence of such a basic event does not necessarily lead to the upper event. For example, the event X_3 (water on floor) can lead to slips (shown in Fig. 2.2), but not all people who walk on the wet floor slip in practice. Therefore, the logic gates of BTs cannot express the real logic relationship of occupational accidents.

(2) BTs cannot accurately describe the potential consequences. Human factors are involved in occupational accidents, complicating the consequence determination. Particularly, when the same safety barriers fail, it does not necessarily lead to the same consequence to humans. For example, even if a worker slips with the failure of all safety barriers (refer to Fig. 2.2), several potential consequences (e.g., minor injuries, lost working-time injuries, unrecoverable major injuries and fatality) may occur in practice with their corresponding probabilities. However, the BT in Fig. 2.2 only assigns one consequence (fatality) to this scenario. Actually, BTs usually consider the most likely potential result for one scenario as the only consequence, which is often unrealistic for occupational accidents.

(3) BTs cannot dynamically assess occupational risks because of its static structure [10]. According to the changing operations and working environments, offshore occupational risks change over time. The proposed safety measures based on static risk analysis may not effectively prevent and mitigate the latest risk. Therefore, dynamic risk analysis is required for related decision making in offshore occupational areas.

2.3.2 BN-based dynamic occupational risk model

BNs were developed based on the established BTs to relax aforementioned limitations, because it has the following advantages:

(1) BNs can represent the real logic (Noisy-OR) [17] between basic events and their upper events of occupational accidents using CPTs, which facilitates the quantification of occupational risks.

(2) CPTs can represent the probability of different potential consequences given the same barrier failure.

(3) BNs are expert in dynamic risk assessment [18, 33]. Thus, it enables to quantify the latest occupational risk in offshore operations.

BNs were established for STFs (Figs. 2.3—2.5) based on BTs through two main steps. Firstly, the components of BTs (the basic events, intermediate events, top events, safety barriers and consequences) are correspondingly converted into root nodes, intermediate nodes, pivot nodes, safety nodes and consequence nodes of BNs [9]. These nodes are connected by arcs based on their causality. Secondly, CPTs of BNs are achieved according to the weights of events which came from the same survey with prior probabilities of basic events. The weight of an event refers to the occurrence likelihood of its upper events given the event occurrence. The development process of the CPT for node IE4 (Fig. 2.3) is demonstrated as follows. $\overline{X}_{11}$, $\overline{X}_{12}$ and $\overline{X}_{13}$ represent nonoccurrence of these events, and the weights of X_{11} X_{12} X_{13} are a_1 (0.001), a_2 (0.001)

and a_3 (0.01) respectively. If X_{11} and X_{12} occur while X_{13} does not take place, the occurrence probability $P(IE_4)=a_1+a_2$ (0.002). This value is added to the CPT of node IE4 (column 4 in Table 2.4). Following this rule, $P(IE_4)$ in different scenarios can be calculated and then the CPT of node IE4 can be completed (Table 2.4).

Table 2.4 The CPT of node IE4 for slips

Scenario	$X_{11}X_{12}X_{13}$	$X_{11}\overline{X}_{12}X_{13}$	$X_{11}X_{12}\overline{X}_{13}$	$\overline{X}_{11}X_{12}X_{13}$	$\overline{X}_{11}\overline{X}_{12}X_{13}$	$\overline{X}_{11}X_{12}\overline{X}_{13}$	$X_{11}\overline{X}_{12}\overline{X}_{13}$	$\overline{X}_{11}\overline{X}_{12}\overline{X}_{13}$
$P(IE_4)$	0.012	0.011	0.002	0.011	0.010	0.001	0.001	0

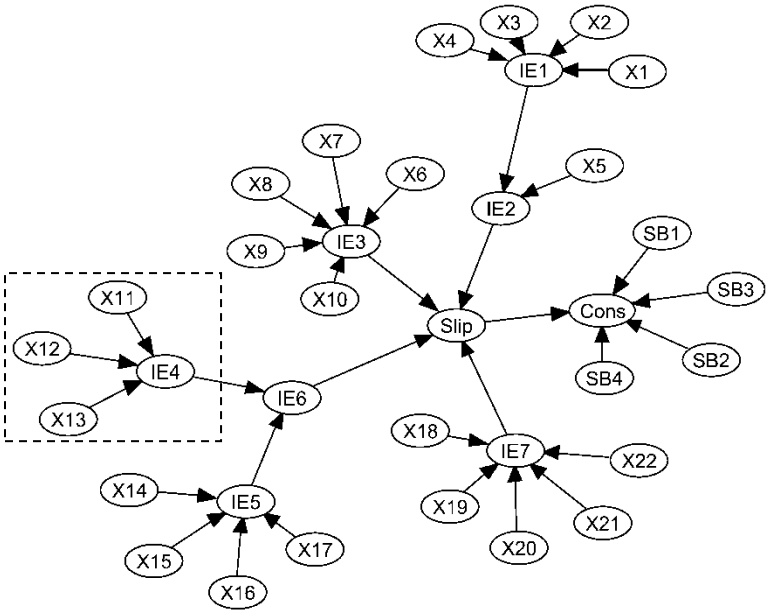


Fig. 2.3 BN for slips (refer to tables 2.1 and 2.2)

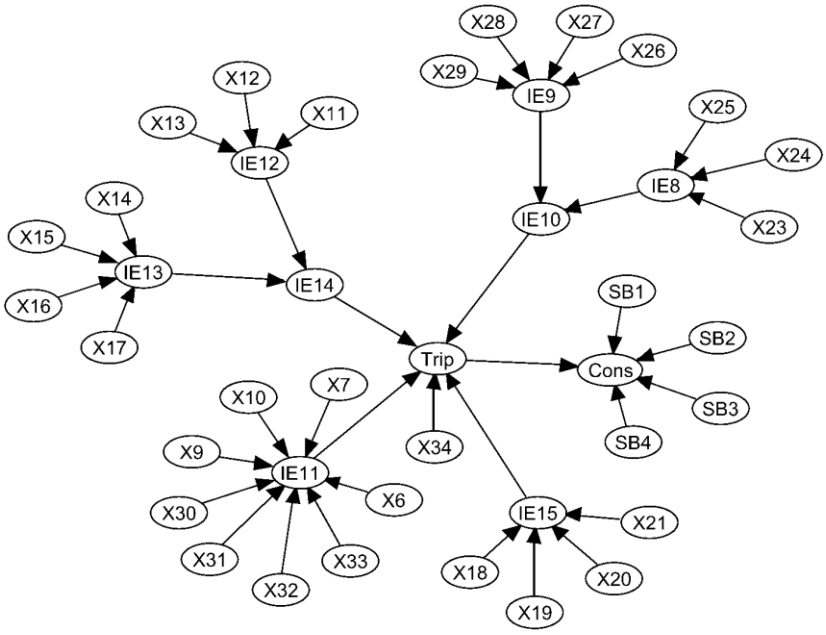


Fig. 2.4 BN for trips (refer to tables 2.1 and 2.2)

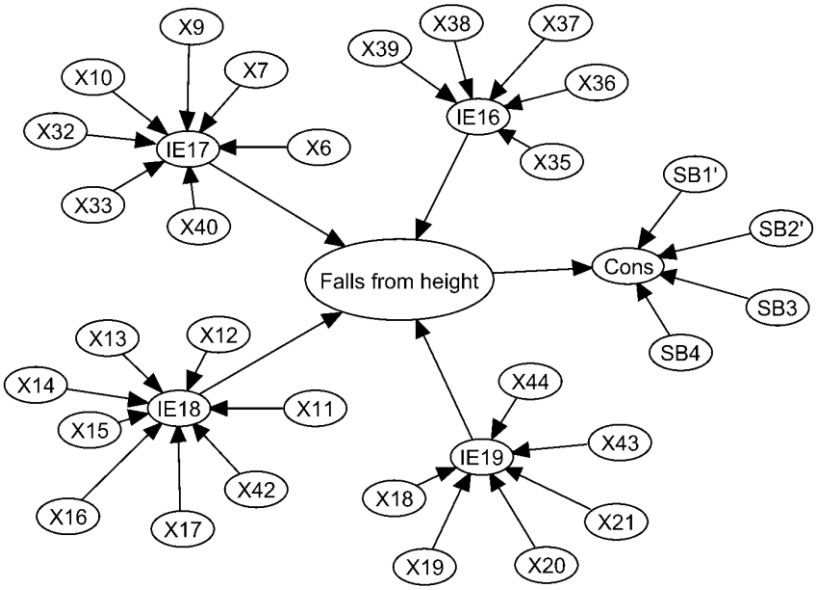


Fig. 2.5 BN for falls from height (refer to tables 2.1 and 2.2)

2.4 Application of occupational risk model

2.4.1 Probability calculation of accidents and consequences

BTs and BNs were used to calculate occurrence and consequence probabilities of STFs and the results are shown in Table 2.5. According to Table 2.5, the accident probabilities calculated by BTs are much higher than those from BNs. UK HSE [2] states that the rate of STFs in the deck operations on mobile installations was 0.025. It is obvious that the accident probabilities obtained from BTs are too large (all bigger than 0.6) compared with those from industry. Such large difference is caused by the fact that BT's logical gates do not fit occupational accidents. In comparison, the results from BNs (column 4 in Table 2.5) are closer to the practical data of UK HSE, which shows the advantage of BNs over BTs in occupational risk analysis. Furthermore, the fatality probability (column 5 in Table 2.5) shows BNs' rationality. According to UK HSE [34], falls from height were the most common cause of fatalities. The result from BNs shows that the fatality probability caused by falls from height is much higher than that caused by slips and trips, which is consistent with the industry. Moreover, the occurrence probability of falls from height calculated by BN is the lowest among the three types of accidents, while its fatality probability is the highest. This fits the accident characteristics that the consequence severity of falls from height is more difficult to mitigate compared with slips and trips.

Table 2.5 Accident and fatality probabilities

Accidents	Occurrence probability (BT)	Fatality Probability (BT)	Occurrence probability (BN)	Fatality Probability (BN)
Slips	9.24×10^{-1}	1.07×10^{-4}	2.08×10^{-2}	2.03×10^{-6}
Trips	6.15×10^{-1}	9.23×10^{-5}	1.38×10^{-2}	1.34×10^{-6}
Falls from height	7.35×10^{-1}	5.88×10^{-4}	5.39×10^{-3}	5.62×10^{-5}

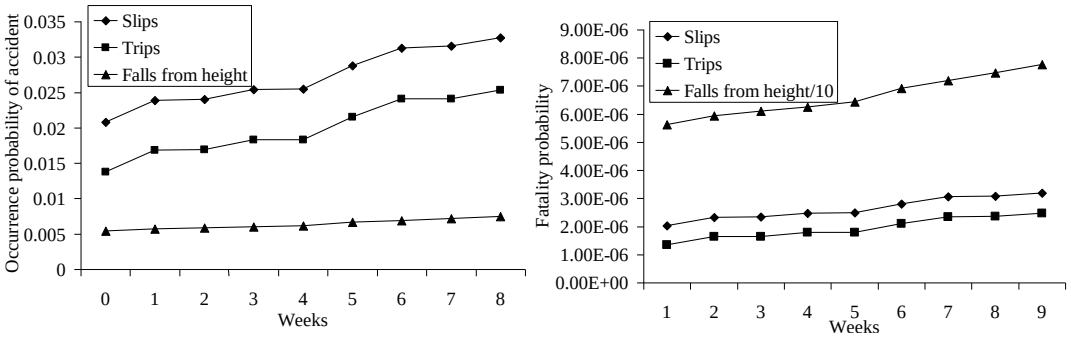
2.4.2 Occupational risk update

One feature of BNs is the sequential updating (adaptation). When the occurrence of basic events is observed, occurrence and consequence probabilities of STFs can be updated using the observed evidence. In a certain scenario, it is assumed that four basic events (strong wind, lack of experience, stress and limited time, and poor housing and maintenance) are observed during eight weeks (Table 2.6). Taking advantage of the evidence, BNs updated both the occurrence probabilities and fatality probabilities of STFs (Fig. 2.6). As Fig. 2.6 shows, the occurrence and fatality probabilities of STFs increased over time. Especially for trips, these probabilities almost doubled through the eight weeks. Furthermore, although the increase rate for occurrence probability of falls from height is smaller than that of slips and trips, its fatality probability has the largest growth. This shows that the changes of the four observed basic events cause more severe deterioration to the consequence severity of falls from height. Interestingly, the great increases on occurrence and fatality probabilities of STFs in week 1 (with the increased percentages 22.4%, 14.8% and 5.7% respectively) are only caused by the harsh environmental factor (strong wind). Thus, as a harsh environmental factor, strong wind

can considerably deteriorate STFs, which indicates the importance of considering harsh environments in offshore risk analysis. Through the adaptation analysis, the updated occurrence and fatality probabilities of STFs were obtained, and corresponding safety measures can be proposed to effectively reduce risks.

Table 2.6 Observed abnormal events during eight weeks

Week	1	2	3	4	5	6	7	8
Strong wind	2	—	1	—	—	2	—	1
Lack of experience	—	1	—	—	1	—	2	—
Stress and limited time	—	—	—	1	—	—	—	1
Poor housekeeping and maintenance	—	—	—	—	1	—	—	—



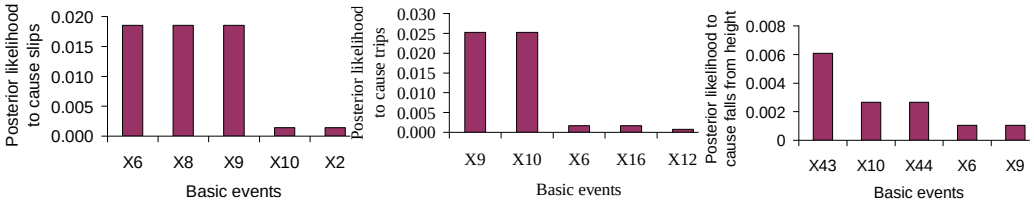
(a) Occurrence probability of STFs **(b) Fatality probability of STFs**

Fig. 2.6 Dynamic occurrence and fatality probabilities of STFs

2.4.3 Critical factor analysis

Another feature of BNs is the backward (diagnostic) analysis, which can be used to update probabilities of root nodes given accident occurrence. The updated probabilities (posterior probabilities) of the basic events mean their most likely probabilities when the accident occurs. The basic events with large posterior likelihood to cause STFs are

considered as the critical factors in this study. The posterior likelihood can be measured by the product of the weights and posterior probabilities of basic events. Two steps were taken to obtain the posterior likelihood of basic events. Firstly, the posterior probabilities of root nodes were obtained with the help of GeNIe software [35]. Then, the posterior likelihood of each basic event to lead to STFs was calculated according to its weight and posterior probability, and the basic events with top five biggest posterior likelihood are shown in Fig. 2.7.



(a) Slips **(b) Trips** **(c) Falls from height**

Fig. 2.7 Basic events with bigger posterior likelihood to cause STFs (refer to tables 2.1 and 2.2)

According to Fig. 2.7, critical factors causing STFs were determined. Specifically, the posterior likelihood of X_6 (storm), X_8 (ice and snow on floor) and X_9 (strong wind) to cause slips is much bigger than other basic events, thus they were selected as the critical factors for slips. Similarly, X_9 (strong wind) and X_{10} (vessel motion) were identified as the critical factors for trips. For falls from height, the critical factors are X_{43} (poor safety training for high place work), X_{10} (vessel motion) and X_{44} (no warning and fencing around holes). Through the analysis, the critical factors for slips, trips and falls from height are different. Thus, when different occupational accidents occur, corresponding

critical factors should be given priority for the effective prevention of future accidents. Furthermore, X_{43}, with a lower prior probability (0.01), has the largest posterior likelihood to cause falls from height, which partly results from its large posterior probability (0.11). Moreover, environmental factors (e.g., X_6, X_8, X_9 and X_{10}) can be found among the critical factors for all STFs accidents. Especially for slips and trips, all the critical factors are harsh environmental factors. This reveals occupational risks can be significantly influenced by harsh offshore environments.

2.5 Conclusions

This study established BTs to better illustrate the occurrence and escalation process of STFs, and then the limitations of BTs were relaxed using BNs. The accident probabilities as well as fatality probabilities obtained from BTs and BNs were analyzed. These probabilities indicate the rationality and advantage of BNs to quantify occupational risks. Furthermore, probability adaptation was completed in a certain scenario. Through the adaptation, it is found both accident probabilities and fatality probabilities increase over time, and the adaptation consequences also indicate the harsh environmental factors can significantly deteriorate STFs. Moreover, the critical factors were identified according to their posterior likelihood to cause STFs. It is found environmental factors exist among the critical basic factors for all STFs accidents. This further reveals that harsh environmental factors pose significant potential hazards to occupational safety. Thus, measures should be presented to cope with the influence of harsh environments.

Some points can be further improved in the future study. Slips, trips and falls from height have an interactive relationship. For example, slips may cause falls from height. The interactive relationship can be modeled, thereby identifying effective measures to prevent various accidents at the same time.

Acknowledgements

The authors acknowledge the financial support provided by China Scholarship Council (CSC), the Natural Sciences and Engineering Research Council of Canada (NSERC) and a Vale Research Chair Grant. The first author also thanks Dr. Ming Yang for his valuable suggestions.

References

[1] Attwood D, Khan F, Veitch B. Can we predict occupational accident frequency? Process Safety and Environmental Protection, 2006; 84 (B3): 208–221.

[2] UK HSE. Support information for slips, trips and falls from height offshore. Offshore technology report 2002/002, Prepared by BOMEL Ltd. for the HSE; 2002.

[3] Ponsonby W, Mika F, Irons G. Offshore industry: medical emergency response in the offshore oil and gas industry. Occupational Medicine, 2009; 59: 298–303.

[4] Amandus H, Bell J, Tiesman H, Biddle E. The Epidemiology of Slips, Trips, and Falls in a Helicopter Manufacturing Plant. Human Factors, 2012; 54 (3): 387–395.

[5] Nenonen N. Analysing factors related to slipping, stumbling, and falling accidents at work: Application of data mining methods to Finnish occupational accidents and

diseases statistics database. Applied Ergonomics, 2013; 44: 215－224.

[6] Courtney TK, Sorock GS, Manning DP, Collins JW, Holbein-jenny MA. Occupational slip, trip, and fall-related injuries － can the contribution of slipperiness be isolated? Ergonomics, 2001; 44: 1118－1137.

[7] Bentley T, Hide S, Tappin D, Moore D, Legg S, Ashby L, Parker R. Investigating risk factors for slips, trips and falls in New Zealand residential construction using incident-centred and incident-independent techniques. Ergonomics, 2006; 49: 62–77.

[8] Attwood D, Khan F, Veitch B. Offshore oil and gas occupational accidents—What is important? Journal of Loss Prevention in the Process Industries, 2006; 19: 386–398.

[9] Yuan Z, Khakzad N, Khan F, Amyotte P. Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks. Risk Analysis, 2015; 35: 278－291.

[10] Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection, 2013; 91: 46–53.

[11] Zheng X, Liu M. An overview of accident forecasting methodologies. Journal of Loss Prevention in the Process Industries, 2009; 22: 484–491.

[12] Weber P., Medina-Oliva G., Simon C., Iung B.. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence, 2012; 25: 671－682

[13] Jacinto C, Silva C. A semi-quantitative assessment of occupational risks using bow-tie representation. Safety Science, 2010; 48: 973–979.

[14] Ale B, Baksteen H, Bellamy LJ. Quantifying occupational risk: The development of an occupational risk model. Safety Science, 2008; 46: 176–185.

[15] Martín JE, Rivas T, Matías JM, Taboada J, Argüelles A. A Bayesian network analysis of workplace accidents caused by falls from a height. Safety Science, 2009; 47: 206–214.

[16] Chen T, Leu S. Fall risk assessment of cantilever bridge projects using Bayesian network. Safety Science, 2014; 70: 161–171.

[17] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety, 2001; 71: 249–260.

[18] Khakzad N, Khan F, Amyotte P. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science, 2013; 57: 108–117.

[19] UK HSE. Slips, trips and falls from height offshore. Offshore technology report 2002/001, Prepared by BOMEL Ltd. for the HSE; 2002.

[20] Hauptmanns U, Marx M, Knetsch T. GAP—a fault-tree based methodology for analyzing occupational hazards. Journal of Loss Prevention in the Process Industries, 2005; 18: 107–113.

[21] Aneziris ON, Papazoglou IA, Baksteen H, Mud M, Ale BJ, Bellamy LJ, Hale AR, Bloemhoff A, Post J, Oh J. Quantified risk assessment for fall from height. Safety

Science, 2008; 46: 198–220.

[22] Brandsæter A. Risk assessment in the offshore industry. Safety Science, 2002; 40: 231－269.

[23] American Bureau of Shipping. Job safety analysis for the marine and offshore industry. ABS guide notes; 2013.

[24] UK HSE. Getting to grips with slips and trips. Available at: <http://www.hse.gov.uk/slips/downloads/gettingtogrips.pdf.> [Accessed 17. 07. 2018]

[25] Aneziris ON, Papazoglou IA, Mud M, Damen M, Bellamy LJ, Manuel HJ, Oh J. Occupational risk quantification owing to falling objects. Safety Science, 2014; 69: 57－70.

[26] Carnero M, Pedregal D. Modelling and forecasting occupational accidents of different severity levels in Spain. Reliability Engineering and System Safety, 2010; 95: 1134－11141.

[27] Njumo D. Fault tree analysis (FTA) – Formal safety assessment (FSA) in ship repair industry a made easy approach. International Journal of Maritime Engineering, 2013; 155: 23－32.

[28] Ohdo K, Hino Y, Takahashi H. Research on fall prevention and protection from heights in Japan. Industrial Health, 2014; 52: 399－406.

[29] Gilks J, Logan R. Occupational Injuries and Diseases in Canada, 1996－2008. Occupational Health and Safety Division Labour Programs, Human Resources and

Development; 2010.

[30] Kirsten H. Workshop on Evaluation of Risk as Decision Making with the Criterion, Denver, CO, 1999.

[31] Ariavie G. O., Sadjere G. E.. Development of Fault Tree Diagram for the Production Line of a Soft Drink Bottling Company in Benin City, Nigeria. In: Proceedings of the World Congress on Engineering: 2012; London, U.K..

[32] Iverson S., Kerkering J. C., P. Coleman. Using Fault Tree Analysis To Focus Mine Safety Research. In: Proceedings of the 108th Annual Meeting of the Society for Mining, Metallurgy, and Exploration: 2001; 1–10.

[33] Khakzad N, Khan F, Amyotte P. Risk-based design of process systems using discrete-time Bayesian networks. Reliability Engineering and System Safety, 2013; 109: 5–17.

[34] UK HSE. Slips & trips and falls from height in Great Britain, 2014. Available at: <http://www.hse.gov.uk/statistics/causinj/slips-trips-and-falls.pdf>. [Accessed 12.12.2015]

[35] GeNIe. Version 2.0.5494.1, 2015. Available at: <https://dslpitt.org>. [Accessed 12.12.2015]

3. Predictive Abnormal Events Analysis Using Continuous Bayesian Network

Preface

A version of this chapter has been published in the ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering. 2017; 3: 1—7. I am the primary author of this paper. I defined the specific research aim, developed the methods and completed the analysis of case study. I completed and improved the manuscript. Dr. Faisal Khan suggested the general research topic and provided feedbacks on the manuscript. Dr. Ming Yang helped revise the original manuscript to make the argument clearer. Dr. Hangzhou Wang suggested MCMC algorithm to solve the established model and helped to learn this algorithm.

Abstract

The reliable prediction and diagnosis of abnormal events provide much needed guidance for risk management. The traditional Bayesian Network (traditional BN) has been used to dynamically predict and diagnose abnormal events. However, its inherent limitation caused by discrete categorization of random variables degrades the assessment reliability. This paper applied a continuous Bayesian Network (CBN) based model to reduce the above-mentioned limitation. To compute complex posterior distributions of CBN, the Markov chain Monte Carlo method (MCMC) was used. A case study was conducted to demonstrate the application of CBN, based on which a

comparative analysis of the traditional BN and CBN was presented. This work highlights that the use of CBN can overcome the drawbacks of traditional BN to make dynamic prediction and diagnosis analysis more reliable.

Keywords: Dynamic analysis, Abnormal events, Uncertainty, Continuous Bayesian network, Markov chain Monte Carlo method

3.1 Introduction

Risk analysis helps propose effective prevention and mitigative measures of accidents [1]. The prediction and diagnosis of abnormal events are an important part of risk analysis and management. Many qualitative and quantitative assessment methods have been presented. Among them, the Bayesian network (BN) based approach is one of the most robust quantitative tools, since it has the capability to analyze dynamic risks given new information or data collected from ongoing operations [2－4]. Especially for events with very low frequency but severe consequences such as the Macondo blowout accident, BN-based approaches can utilize the relatively abundant precursor data to estimate accident probability and reduce uncertainty by considering the interdependency among the causes of the accident. Khakzad et al illustrated the specific process of converting BT into BN, and took accident precursors and conditional dependency into account to update the probability of events and the consequent risk for a vapor ignition accident using BN [2]. In another study, they conducted risk analysis of drilling operations using an object-oriented Bayesian network. The object-oriented

Bayesian network makes the model tractable, and demonstrates the dependencies of events more clearly. [1] Yuan et al. applied BN to dynamically assess the risks of dust explosion considering common cause failures and dependencies among root events and possible consequences, and also identified the critical factors given the occurrence of a dust explosion [3]. Abimbola et al. used BN to update the belief about the operational data considering the dependencies in the constant bottom-hole pressure drilling technique [4].

However, the modeling flexibility and preciseness of a BN-based approach is degraded by the use of discrete nodes [5－7]. Normally, for the sake of calculation, traditional BN based risk models treat causal factors with a continuous nature as discrete variables (frequently Boolean). This approximation introduces uncertainty to the assessment process. Many variables continuously change with the variation of their causal factors, which often fails to be modeled by discrete nodes of traditional BN. For instance, 'strong wind', as a causal factor for a 'high wave', is defined as wind with a speed of over 10.8 m/s. Although winds of 1 m/s and 9 m/s have significantly different effects on wave height in practice, both are categorized as the discrete state of 'no strong wind' in a traditional BN. Consequently, they will be assigned the same conditional probabilities in the conditional probability tables (CPTs) [2, 3]. This means their contributions to a 'high wave' are considered as identical in this BN. This becomes one of the main sources of uncertainty of such BN.

To overcome this limitation, a continuous Bayesian network (CBN) is applied to deal with continuous factors. CBN is defined as the specific Bayesian network, the nodes of which are variables represented by continuous distributions. A few studies have been conducted to investigate continuous nodes in BN models [8－10]. However, to the authors' knowledge, limited work has been conducted on the development of a CBN based safety analysis approach and the implementation of CBN to overcome the uncertainty caused by the assumption of discrete states of nodes in traditional BN. The rare application of continuous nodes in BN is mainly because of the difficulty in computing posterior distributions due to the involvement of various continuous distributions and multiple dependent variables. Some research [11－13] uses the conjugate method to solve the CBN based on the assumption that the prior and likelihood distributions are conjugate pairs (i.e., the posterior distributions are in the same family as the prior distributions). However, this assumption produces some level of uncertainty.

This paper proposes the development method of CBN and applies the Markov chain Monte Carlo method (MCMC) to compute CBN. Although CBN has a higher computational cost than traditional BN, it can be solved efficiently using software by a personal computer, even given a reasonably large number of nodes in the network. The application of CBN is demonstrated using a case study and results are compared with those of the traditional BN to prove the effectiveness of CBN in reducing uncertainty

of risk analysis. The work is organized as follows: Section 3.2 illustrates the process of converting traditional BN to CBN, while Section 3.3 introduces the use of MCMC to solve CBN. A case study is presented in Section 3.4 to reveal the advantages of CBN for the prediction and diagnosis analysis of abnormal events. Finally, Section 3.5 captures the conclusions.

3.2 The algorithm of converting traditional BN to CBN

The development of traditional BN has been well documented in the existing literature. However, there is limited study of the establishment of CBN based on continuous nodes and conditional probabilities. A fault tree (FT), an effective tool used to systematically analyze the causes of accidents following top down Boolean logic, can be mapped into traditional BN [14]. An FT can be easily established due to its organized structure. However, an FT is hard to convert directly to CBN, because they not only have completely different model structures, but also have different variable types (i.e. FT has discrete variables while CBN uses continuous variables.) Since traditional BN has the same variable types as FT and an identical structure as CBN, in order to develop CBN with ease, FT can be developed first and then converted into traditional BN, followed by the conversion of traditional BN to CBN.

3.2.1 The distinction between traditional BN and CBN

Figuring out the distinctions is essential to determine how to convert traditional BN to CBN. The analytical mechanism of CBN is fundamentally different from that of

traditional BN. In CBN, parental nodes are considered to be contributing quantitatively to the physical values of their child nodes. This quantitative relationship can be represented in the form of a mathematical expression that links the value of the child nodes to that of the parental nodes. In contrast, traditional BN links the probability of discrete states of child nodes to the discrete state combination of parental nodes using CPTs. To quantitatively represent child nodes using parental nodes in CBN, two main changes are required from traditional BN. Firstly, the nodes of CBN need to be represented using measurable variables rather than discrete states. Secondly, the values or distribution parameters of child nodes in CBN are represented as the function of the value of parental nodes. Thus, the CPT of traditional BN are converted to conditional probability distributions or functions representing the relationship between values of child and parental nodes. Compared with traditional BN, CBN is able to obtain the continuous state distribution of each node, and this distribution can provide more information about the occurrence of an abnormal event and its causal factors.

3.2.2 Converting traditional BN to CBN

To develop CBN, FT is applied first to identify the causes of abnormal events and determine the logic relationships. Then FT is mapped into traditional BN, and consecutively traditional BN is converted to CBN. As the existing literature [14] has provided the method of mapping FT into traditional BN, this paper mainly illustrates the process to convert traditional BN to CBN (shown in Fig. 3.1).

Firstly, the measurable variables reflecting continuous states of the nodes of traditional BN are identified to replace the discrete states. For example, wind speed can be identified as the measurable variable of ‘strong wind’, and thus the discrete node of ‘strong wind’ is converted to the continuous node of wind speed. This process to obtain continuous nodes of CBN is shown in Fig. 3.2. These continuous nodes are linked according to their dependent relationships. Then the prior distributions of root nodes as well as the quantitative relationships between nodes are determined according to historical data and expert's experience. It is worth noting that the relationships between nodes of CBN have two types (probabilistic and deterministic) [15]. The probabilistic relationship refers to conditional probability distributions. In this case, the parameters of probabilistic distribution of child nodes are represented as the function of the value of the parental nodes. Thus, even if parental values are determined, the values of child nodes are still random in nature. On the contrary, in a deterministic relationship, the values of parental nodes usually directly determine the value of child nodes. It is important to determine the proper relationship type between nodes, since it can influence the calculation process of CBN. The deterministic link needs to be ignored while inferring the full conditional distribution of CBN using the Gibbs algorithm of MCMC [15]. After CBN is established, the distributions of nodes can be updated through forward and backward inference when evidence is available.

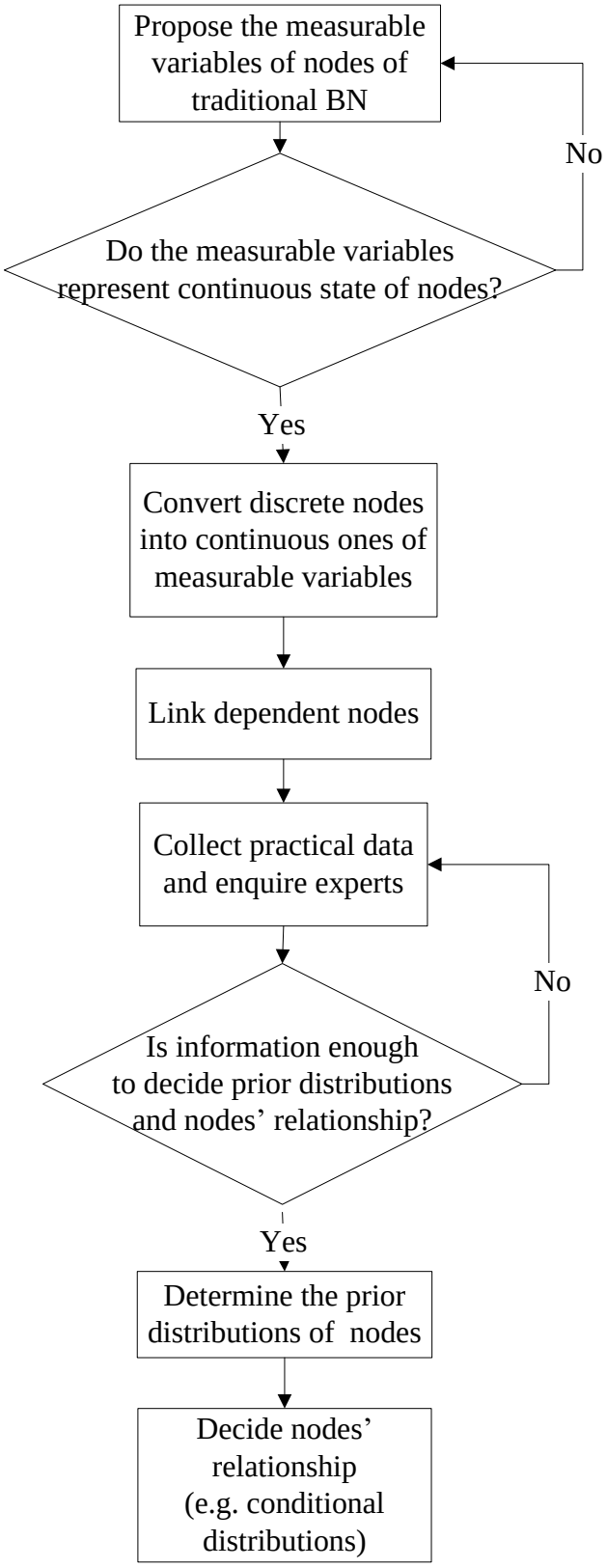


Fig. 3.1 Procedure to convert traditional BN into CBN

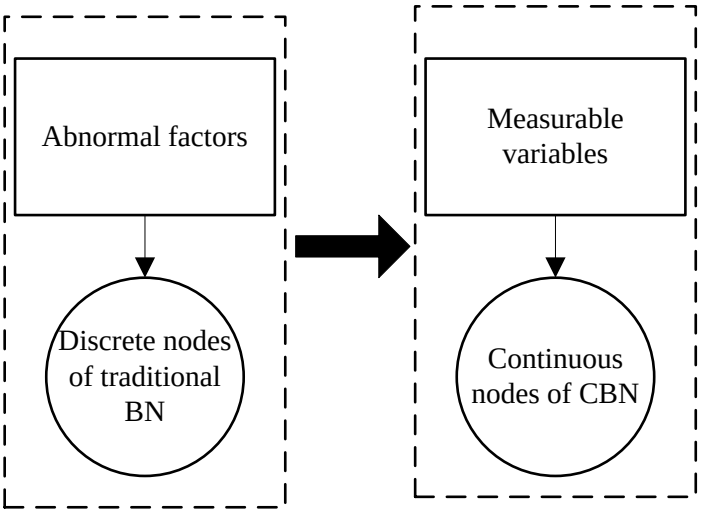


Fig. 3.2 The process to obtain continuous nodes of CBN

3.3 CBN analysis using MCMC

The analytical method is unable to compute the complicated posteriors in CBN. MCMC has the capacity of deriving complicated distributions with high dimensions. To clearly understand MCMC, it is necessary to illustrate its relationship with the Monte Carlo and Markov chain. Monte Carlo simulation is a class of computational algorithms used to obtain numerical consequences depending on random samples. This method samples numerous random data following certain rules (e.g. a distribution), and these sampled data are then analyzed to obtain the desired consequences such as mean, variance and distribution density function. However, Monte Carlo simulation cannot directly sample from complicated distributions containing various dependent variables. To overcome this limitation, the Markov chain is applied to help Monte Carlo sampling, and thus MCMC is proposed. The basic principle of MCMC is achieving Monte Carlo sampling through the Markov chain [15]. The Markov chain is a random process that starts in one

state and moves from one state to another on the state space with appropriate transition probabilities. Its next state is only dependent on the current state rather than on previous ones. The state transition of a point on the state space of a Markov chain is actually the sampling process of Monte Carlo simulation. The state parameters of the point in the Markov chain are the sampled variable values from Monte Carlo. Detailed information about MCMC and its algorithms (e.g., Metropolis-Hastings, Gibbs and slice sampling) can be obtained from [15－17].

A simple CBN (Fig. 3.3) is applied to illustrate the process of solving CBN with MCMC.

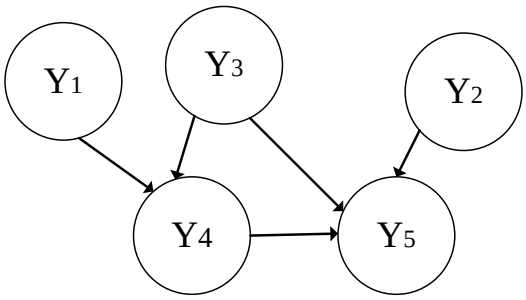


Fig. 3.3 A simple CBN

The prior and conditional distributions for the variables of the CBN in Fig. 3.3 are assumed as follows:

$Y_1 \sim Gamma(\alpha, \beta)$, $Y_2 \sim Normal(\mu, \delta^2)$, $Y_3 \sim Exponential(\lambda)$,

$p(Y_4 \mid Y_1 Y_3) \sim Gamma(y_3, y_1)$, $p(Y_5 \mid Y_2 Y_3 Y_4) \sim Gamma(y_2 + y_3, y_4)$

where $\alpha, \beta, \mu, \delta, \lambda$ are constants, and y_i are the values of variables Y_i (i=1,2,3,4,5).

The calculation of $p(Y_1 \mid Y_5)$ is taken as an example to illustrate how to use MCMC to compute the posterior probability distribution of CBN. According to Bayesian theory, the posterior probability distribution of Y_1 given Y_5 is represented as equation (3.1).

$$\begin{aligned} p(Y_1 \mid Y_5) &= \frac{p(Y_1 Y_5)}{p(Y_5)} = \frac{\iiint p(Y_1 Y_2 Y_3 Y_4 Y_5) dY_2 dY_3 dY_4}{\iint\iint p(Y_1 Y_2 Y_3 Y_4 Y_5) dY_1 dY_2 dY_3 dY_4} \propto \iiint p(Y_1 Y_2 Y_3 Y_4 Y_5) dY_2 dY_3 dY_4 \\ &= \iiint p(Y_1) p(Y_2) p(Y_3) p(Y_4 \mid Y_1 Y_3) p(Y_5 \mid Y_2 Y_3 Y_4) dY_2 dY_3 dY_4 \\ &= \iiint \frac{\beta^{\alpha}}{\Gamma(\alpha)} Y_1^{\alpha-1} e^{-\beta Y_1} * \frac{1}{\delta\sqrt{2\pi}} e^{-\frac{(Y_2-\mu)^2}{2\delta^2}} * \lambda e^{-\lambda Y_3} * \frac{Y_1^{Y_3}}{\Gamma(Y_3)} Y_4^{Y_3-1} e^{-Y_1 Y_4} * \frac{Y_4^{Y_2+Y_3}}{\Gamma(Y_2+Y_3)} Y_5^{Y_2+Y_3-1} e^{-Y_4 Y_5} dY_2 dY_3 dY_4 \end{aligned} \tag{3.1}$$

From equation (3.1) it can be seen that to calculate $p(Y_1 \mid Y_5)$, five variables and three integrations need to be dealt with, and among them, Y_3 and Y_4 are dependent. This posterior distribution is too complicated to be solved with an analytic method or Monte Carlo simulation. To overcome the limitation, the Gibbs algorithm of MCMC is applied to solve the posterior distributions of Y_1 given Y_5. Firstly, the full conditional distributions of the CBN in Fig. 3.3 are obtained as equations (3.2)—(3.6):

$$p(Y_1 \mid Y_2 Y_3 Y_4 Y_5) \propto p(Y_1 \mid \alpha, \beta) p(Y_4 \mid Y_1 Y_3) \tag{3.2}$$

$$p(Y_2 \mid Y_1 Y_3 Y_4 Y_5) \propto p(Y_2 \mid \mu, \delta) p(Y_5 \mid Y_2 Y_3 Y_4) \tag{3.3}$$

$$p(Y_3 \mid Y_1 Y_2 Y_4 Y_5) \propto p(Y_3 \mid \lambda) p(Y_4 \mid Y_1 Y_3) p(Y_5 \mid Y_2 Y_3 Y_4) \tag{3.4}$$

$$p(Y_4 \mid Y_1 Y_2 Y_3 Y_5) \propto p(Y_4 \mid Y_1 Y_3) p(Y_5 \mid Y_2 Y_3 Y_4) \tag{3.5}$$

$$p(Y_5 \mid Y_1 Y_2 Y_3 Y_4) \propto p(Y_5 \mid Y_2 Y_3 Y_4) \tag{3.6}$$

The original values for the variables of the CBN (Fig. 3.3) are provided as ${y_1}^0, {y_2}^0, {y_3}^0, {y_4}^0$, and the evidence ${y_5}^e$ is constant during the MCMC simulation. The full conditional distribution of Y_1 is further inferred as in equation (3.7). It is found that the full conditional distribution of Y_1 is a Gamma distribution with parameters $\alpha + y_3$ and $\beta + y_4$. This kind of posterior distribution with closed form can be directly simulated with standard algorithms [16] (e.g., Monte Carlo). Thus, a new value ${y_1}^1$ can be sampled from Gamma ($\alpha + {y_3}^0$, $\beta + {y_4}^0$). It replaces ${y_1}^0$ to serve as the parameter of Y_3.

$$p(Y_1 \mid Y_2 Y_3 Y_4 Y_5) \propto p(Y_1 \mid \alpha, \beta)\, p(Y_4 \mid Y_1 Y_3) \propto Gamma(\alpha + y_3, \beta + y_4) \tag{3.7}$$

The full conditional distribution of Y_3 is further inferred as equation (3.8).

$$\begin{aligned} p(Y_3 \mid Y_1 Y_2 Y_4 Y_5) &\propto p(Y_3 \mid \lambda)\, p(Y_4 \mid Y_1 Y_3)\, p(Y_5 \mid Y_2 Y_3 Y_4) = \lambda e^{-\lambda Y_3} * \frac{({y_1}^1)^{Y_3}}{\Gamma(Y_3)} ({y_4}^0)^{Y_3 - 1} e^{-{y_1}^1 {y_4}^0} \\ * \frac{({y_4}^0)^{{y_2}^0 + Y_3}}{\Gamma({y_2}^0 + Y_3)} ({y_5}^e)^{{y_2}^0 + Y_3 - 1} e^{-{y_4}^0 {y_5}^e} &\propto e^{-\lambda Y_3} * \frac{({y_1}^1)^{Y_3}}{\Gamma(Y_3)} ({y_4}^0)^{Y_3 - 1} * \frac{({y_4}^0)^{{y_2}^0 + Y_3}}{\Gamma({y_2}^0 + Y_3)} ({y_5}^e)^{{y_2}^0 + Y_3 - 1} \end{aligned} \tag{3.8}$$

As shown in equation (3.8), the full conditional distribution of Y_3 is the product of an exponential and two Gamma distributions, and it does not have the closed form. To solve this complex full conditional distribution, some other algorithms (e.g., slice sampling and Metropolis-Hastings) are required. If the Metropolis-Hastings algorithm is applied to deal with the full conditional distribution of Y_3, a proposed distribution

Gamma (1,2) can be presented first. Samples are drawn from Gamma (1,2) and an assessment is made depending on the assessment standard [15], to determine whether to accept samples. The accepted sample is $y_3^{\,1}$ and it replaces $y_3^{\,0}$ to serve as the parameters of the full conditional distributions of other variables. On the other hand, if the slice sampling is used to deal with the full conditional distribution of Y_3, an auxiliary variable Z needs to be introduced. [17] It is assumed $f(Y_3) = e^{-\lambda Y_3} * \frac{(y_1^{\,1})^{Y_3}}{\Gamma(Y_3)} (y_4^{\,0})^{Y_3-1} * \frac{(y_4^{\,0})^{y_2^{\,0}+Y_3}}{\Gamma(y_2^{\,0}+Y_3)} (y_5^{\,e})^{y_2^{\,0}+Y_3-1}$, and the joint distribution of Y_3 and Z is defined as uniform over the region $U = \{(Y_3, Z) : 0 < Z < f(Y_3)\}$. To sample Y_3, we can sample jointly for (Y_3, Z) and then ignore Z. The process to obtain (Y_3, Z) is as follows: the initial value $y_3^{\,0}$ is provided and Z^0 is sampled uniformly at random from the interval (0, $e^{-\lambda y_3^{\,0}} \frac{(y_1^{\,1})^{y_3^{\,0}}}{\Gamma(y_3^{\,0})} (y_4^{\,0})^{y_3^{\,0}-1} \frac{(y_4^{\,0})^{y_2^{\,0}+y_3^{\,0}}}{\Gamma(y_2^{\,0}+y_3^{\,0})} (y_5^{\,e})^{y_2^{\,0}+y_3^{\,0}-1}$). Then $y_3^{\,1}$ is sampled uniformly at random in the region $S = \{Y_3 : f(Y_3) > Z^0\}$. The obtained $y_3^{\,1}$ replaces $y_3^{\,0}$ to serve as the parameters of the full conditional distributions of other variables. Through a similar process as described above, $y_2^{\,1}$ and $y_4^{\,1}$ can be sampled from their full conditional distributions.

After $y_1^{\,1}$, $y_2^{\,1}$, $y_3^{\,1}$ and $y_4^{\,1}$ are sampled, the second round of simulation is conducted, and $y_1^{\,2}$, $y_2^{\,2}$, $y_3^{\,2}$ and $y_4^{\,2}$ are obtained. Following this procedure, numerous y_1 can be obtained. The y_1 sampled from the converged Markov chain can be considered as data from $p(Y_1 \mid Y_5)$. Then the posterior distribution of Y_1 given Y_5 is

analyzed through these samples. The whole process to obtain the posterior distribution of Y_I is the Gibbs simulation, in which slice sampling and Metropolis-Hastings are tried to solve the full conditional distributions.

As described above, MCMC enables solving the complicated posterior distributions which Monte Carlo cannot deal with, although it may have a higher computational cost than does Monte Carlo.

3.4 Case study

This case study is used to demonstrate the advantages of CBN compared with traditional BN. The dynamic probability prediction and diagnosis of severe vessel roll is presented, and the result from CBN is compared with that from traditional BN to illustrate the capability of CBN to reduce uncertainty.

3.4.1 The development of traditional BN for the severe vessel roll

A common hazard for vessels, the ‘severe roll’ is an important contributor to the crew falling on vessels. Therefore, it is meaningful to study the occurrence probabilities of ‘severe roll’ and diagnose its causal factors. This hazard is mainly caused by waves, including wind waves, swells and beachcombers. The roll studied in this paper results from a wind wave. Theoretically, wave height and wavelength contribute to the vessel roll, but for the sake of simplification, wavelength was not considered due to its very

complex relationship with wind and vessel roll [18]. Besides waves, vessel width and the wind directly acting on vessels contribute to roll as well. Following the steps mentioned in Section 3.2, FT was established first (shown in Fig. 3.4), and the meaning of symbols is shown in the two left columns of Table 3.1. The classification criteria of discrete states are shown in Table 3.2. According to Beaufort wind scale [19], we define 'strong wind' as wind with a speed of over 10.8m/s, and a 'rough sea' is defined as waves with a height of over 2.5m/s, based on the Douglas sea scale [20]. After consulting the staff working on an international freighter, the severe roll angle for falling down has been defined as over 10^{o}. The vessel with a width of less than 10m is assumed to be a 'small vessel'.

Table 3.1 Description of symbols in FT, traditional BN and CBN

Symbols in FT and traditional BN	Description	Symbols in CBN	Description
X_1	Strong wind	I_1	Wind speed
X_2	Rough sea	I_2	Wave height
X_3	Small vessel	I_3	Vessel width
TE	Severe roll	ITE	Roll angle

Table 3.2 Classification criteria of discrete states

Discrete states	Criteria
Strong wind	Wind speed >10.8m/s [19]
Rough sea	Wave height>2.5m [20]
Small vessel	Vessel width<10m
Severe roll	Roll angle>10^{o}

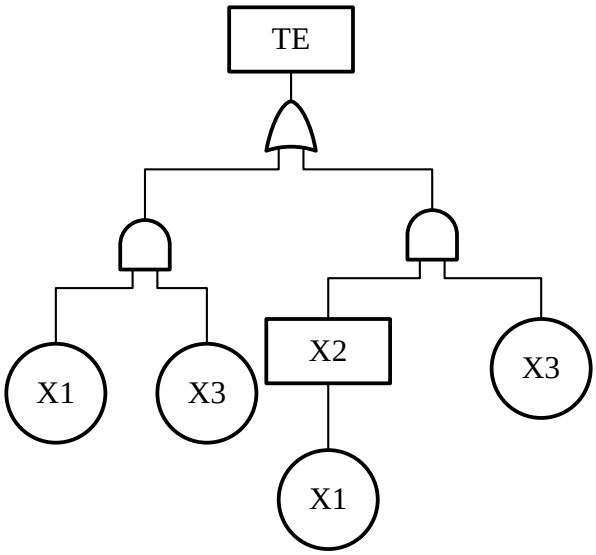


Fig. 3.4 FT for 'severe roll'

Then the FT was converted to traditional BN (shown in Fig. 3.5) where all nodes are discrete. The prior probabilities of 'strong wind' and 'small vessel' were defined and shown in Table 3.3. The CPTs of the traditional BN were also obtained and the CPT of 'rough sea (X_2)' is shown in Table 3.4.

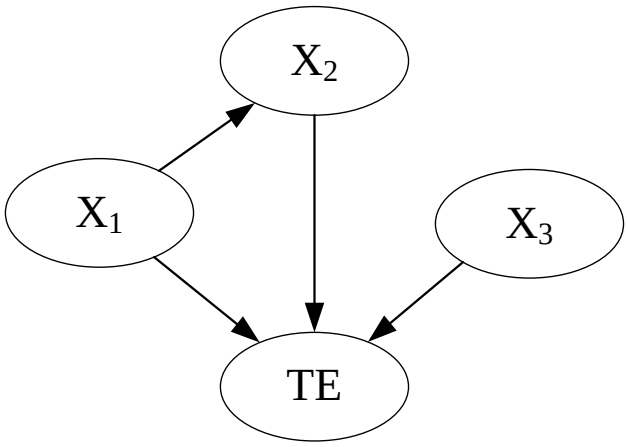


Fig. 3.5 The traditional BN for 'severe roll'

Table 3.3 Prior probability

Factors	Prior probability
X_1	0.1
X_3	0.8

Table 3.4 The CPT for 'rough sea (X2)'

	X_1	X_1'
X_2	0.8	0
X_2'	0.2	1

3.4.2 The development of CBN for vessel roll

Following the process mentioned in Section 3.2, the traditional BN for 'severe roll' was converted to CBN (Fig. 3.6). Measurable variables of causal factors and abnormal events were determined correspondingly (see the right two columns of Table 3.1). The continuous nodes of measurable variables were used to replace traditional BN discrete nodes. The prior and conditional distributions of these continuous nodes were assumed as shown in Tables 3.5 and 3.6. In practice, this information can be obtained through historical data and expert opinion.

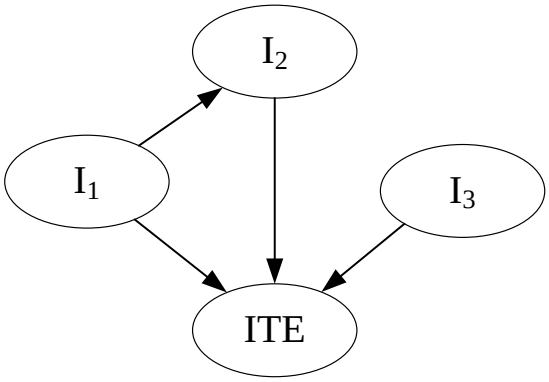


Fig. 3.6 CBN for vessel roll

Table 3.5 Prior distributions

Factors	Prior distributions
I_1	Weibull (2, 3.780)
I_3	Gamma (15, 2)

Table 3.6 Conditional distributions

Factors	Conditional distributions
$p(I_2\|I_1)$	Lognormal (I_1/20, 0.2553)
$p(ITE\|I_1, I_2, I_3)$	Gamma(I_1*(180*I_2/100/(1-(I_3*2/100)*(I_3*2/100))), 2)

3.4.3 The calculation of traditional BN and CBN for severe vessel roll

CBN and traditional BN can both be used to analyze the occurrence of severe vessel roll. Furthermore, like traditional BN, CBN can update nodes when evidence is available. Thus, it can dynamically assess the occurrence probabilities of abnormal events (forward inference) and diagnose the latest situation of causal factors (backward inference). More importantly, CBN can significantly reduce the uncertainty of traditional BN in these two types of inferences. In this study, GeNie software [21] was applied to perform the inference of traditional BN, and OPENBUGS software [22] was used to perform the CBN calculation. According to the prior probabilities and CPTs, the occurrence probability of 'severe roll' is 0.0808 from traditional BN; while that probability is 0.0841 from CBN, based on the prior and conditional distributions. The original occurrence probabilities of 'severe roll' obtained through traditional BN and CBN are very close.

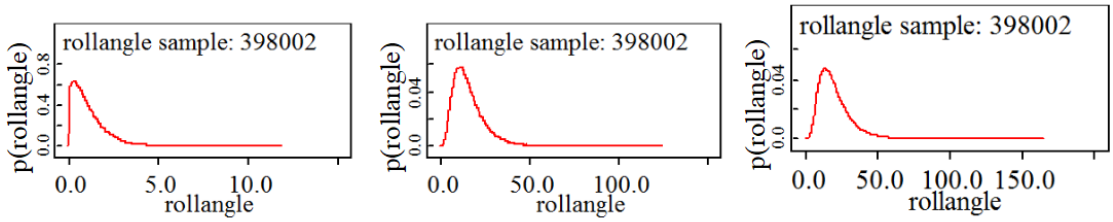
3.4.3.1 Forward inference

In this case, the evidence includes wind speeds of 1m/s, 9.5m/s and 11m/s. This

evidence was used to update the distribution of roll angles in the CBN. Then the obtained distribution was analyzed to determine the updated probability of 'severe roll'. According to the criterion of 'strong wind' (Table 3.2), the discrete states ('strong wind' or 'no strong wind') of this evidence can be respectively obtained. When the discrete states of wind were implemented in traditional BN, the probabilities of 'severe roll' were updated. With wind speeds of 1m/s, 9.5m/s and 11m/s, the probabilities of 'severe roll' were calculated as 0, 0 and 0.808 using traditional BN. The former two have the same probabilities, because their observed wind speeds belong to the same discrete state ('no strong wind') and consequently have the same conditional probability in the CPTs of the traditional BN. This indicates that the traditional BN cannot effectively reflect the influence of the change of wind speeds on vessel roll when wind speeds are in the same discrete states (Table 3.2). In contrast, according to the results obtained through the CBN, the distribution of roll angles for the wind speed of 1m/s (Fig. 3.7 (a)) has an obvious change compared to that corresponding to the wind speed of 9.5m/s (Fig. 3.7 (b)) though these two wind speeds belong to the same discrete state. Furthermore, the probabilities of 'severe roll' increase significantly from 1.5075E-05 to 0.7310. In this way, CBN overcomes the drawback of traditional BN and captures the dynamic changes of causal factors.

In traditional BN, the probabilities of 'severe roll' corresponding to 1m/s and 9.5m/s are the same (i.e., 0), but it has a much higher probability (0.808) given the wind speed of 11m/s. This result is not reasonable, because practically the probabilities of 'severe

roll' should be close for the similar levels of wind speed (9.5m/s and 11m/s) given other fixed causal factors. According to Fig. 3.7 (a), (b) and (c), the roll angles from CBN have far less change with an increase of wind speed from 9.5m/s to 11m/s than their change caused by the increase of wind speed from 1m/s to 9.5m/s. Unlike the results obtained from traditional BN, the probability of 'severe roll' calculated by CBN given the wind speed of 11m/s (0.8459) is close to that corresponding to 9.5m/s (0.7310). This shows CBN can better reflect the change of roll angles over the changes of causal factors than traditional BN. For the simulations of roll angle distributions (Fig. 3.7), two Markov chains were used for each scenario. Each chain generated 200000 samples and the first 999 ones were discarded (burn-in). It was found that the historical traces of the two chains of each scenario overlapped; thus, the Markov chains are believed to be converged [23]. Also, MC errors (0.002, 0.015 and 0.018) of roll angles for the three scenarios are smaller than 0.05; thus, the simulation accuracy is acceptable [23]. The calculation of roll angles is a forward inference. Thus, samples are obtained from standard distributions (i.e., Weibull, Lognormal and Gamma distributions) using standard algorithms [16] in the simulations, and the acceptance rate is 1.



(a) wind speed 1m/s **(b) wind speed 9.5m/s** **(c) wind speed 11m/s**

Fig. 3.7 Distribution density of roll angles over different wind speeds

Note: the practical roll angles should be within 0 to 90º. In the case study, when the result is larger than 90º, it is considered to be 90º.

3.4.3.2 Diagnosis analysis

One of the features of BN is the diagnosis analysis (backward inference). Normally, when the abnormal event has been observed, the states of its causal factors can be inferred using diagnosis analysis. CBN can also help to reduce the uncertainty existing in the diagnosis process of traditional BN.

Assuming roll angles were observed as 1^{o}, 9.5^{o}, 10.5^{o} and 30^{o}, the probabilities of causal factors were updated. For traditional BN, the discrete states ('severe roll' or 'no severe roll') of these observed angles were obtained according to Table 3.2 and used as the evidence for the update. Meanwhile, with these observed angles, the distributions of causal factors were also updated using CBN.

The results obtained from traditional BN are shown in the second row of Table 3.7. When the roll angles are 1^{o}, 9.5^{o}, 10.5^{o} and 30^{o}, the corresponding posterior

probabilities of ‘rough sea’ are 0.0070, 0.0070, 0.9109 and 0.9109 respectively. Thus, traditional BN failed to predict the state change of causal factors given different roll angles (e.g., 1^{o} and 9.5^{o}), because these observed angles belong to the same discrete state according to Table 3.2. Furthermore, when the roll angles are very close (e.g., 9.5^{o} and 10.5^{o}), the diagnosis consequences are very different (0.0070 and 0.9109). However, in practice, the likely probabilities of causal factors are believed to be similar, given alike evidence of abnormal events. When CBN was applied to conduct the backward analysis, the posterior distributions of causal factors were obtained, and then the posterior probabilities of abnormal states of these factors were calculated depending on the classification criteria (Table 3.2). The posterior distribution density of wave heights from CBN is shown in Fig. 3.8, and the posterior probabilities of ‘rough sea’ are shown in row 3 of Table 3.7. The results from CBN show that the states of ‘rough sea’ change given different roll angles which even belong to the same discrete state (e.g., 1^{o} and 9.5^{o}), and also the posterior probabilities of ‘rough sea’ are close (0.1934 and 0.2475) given small difference in roll angles (9.5^{o} and 10.5^{o}) as evidence. The diagnosis results reveal that CBN is able to better capture the changes of abnormal events and reflect them in the state change of causal factors through backward analysis. Two Markov chains were used for each scenario following the slice algorithm, and each chain generated 20000 samples with the burn-in of 999 samples. The acceptance rate of simulation for all scenarios is 1. Moreover, following the procedure described in Section 3.4.3.1, it was verified that the Markov chains converged, and the simulation accuracy

is acceptable.

Table 3.7 The diagnosis of 'rough sea' from traditional BN and CBN

Evidence (roll angles)	1^o	9.5^o	10.5^o	30^o
Probabilities of 'rough sea' from traditional BN	0.0070	0.0070	0.9109	0.9109
Probabilities of 'rough sea' from CBN	0.0061	0.1934	0.2475	0.9888

Accurate diagnosis results are important for the prioritization of causal factors and development of countermeasures to effectively prevent abnormal events. After obtaining the posterior probabilities of causal factors according to CBN, the factors with bigger posterior probability can be identified, and the mean increase of roll angles can be respectively calculated given the unit increase of each causal factor. The causal factors with larger posterior probability and leading to a bigger increase of roll angles are critical factors. These factors should be given priority when deciding countermeasures. In this case, it is of little value to identify the critical causal factors, because none of them can be controlled in order to reduce the probability of the abnormal event. Since the causal factors in this case study tend to be uncontrollable, critical factors are not identified here. However, the way of identifying critical factors can be used when analyzing risks in other areas.

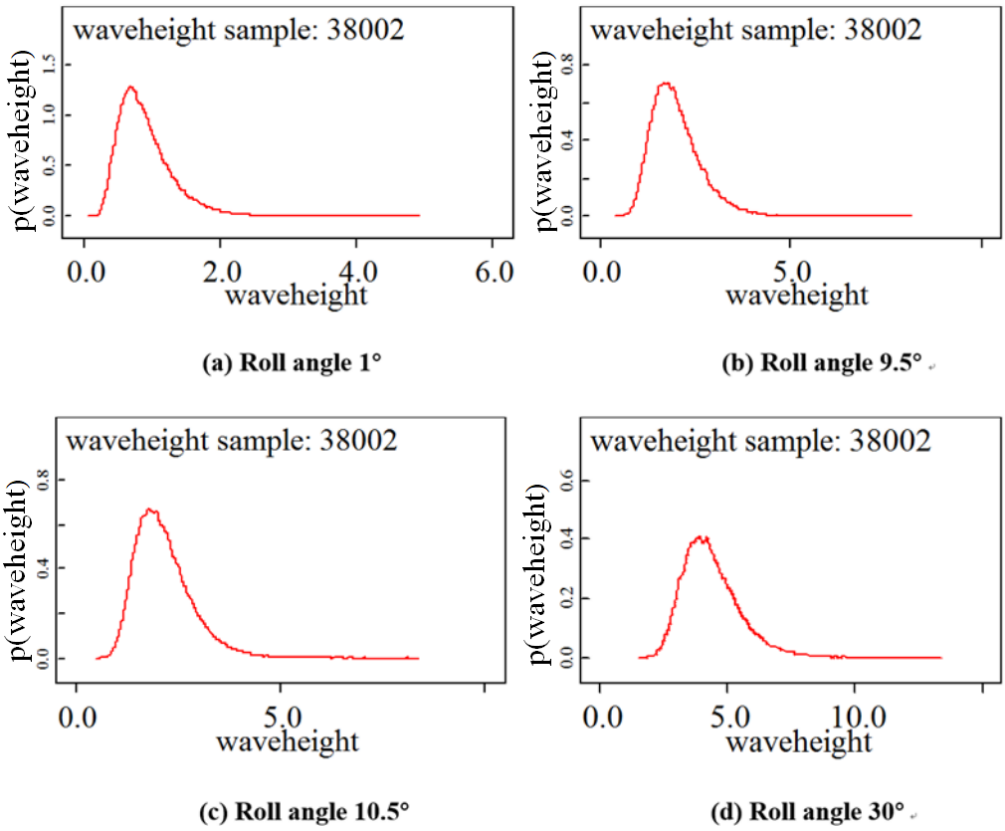


Fig. 3.8 Distribution density of wave heights

3.4.3.3 Flexibility of CBN

'Severe roll' can lead to different types of accidents. For different accidents, the criteria used to define 'severe roll' may differ. For example, a roll angle greater than 10^{o} can be considered a 'severe roll' in the case of crew falling on a vessel; while for vessel capsizing, it is more reasonable to use a bigger roll angle (e.g., above 80^{o}) to define 'severe roll'. CBN is open to the flexibility of definition of accident type and the associated criteria used to define abnormal states. For example, in this case, CBN is able to sample numerous roll angles, and once a specific type of accident is determined, the probability of 'severe roll' can be computed as the percentage of the roll angles of more than the defined criteria. Given the criteria defined for 'severe roll' mentioned

above, the probability of ‘severe roll’ for capsizing corresponding to the wind speed of 11m/s is 0.0014, while the probability of ‘severe roll’ for falling down is 0.8114. However, traditional BN can only calculate the probability of abnormal events for one accident.

3.5 Conclusions

This paper applied a CBN-based method to predict the probability of an abnormal event and diagnose its causal factors to reduce the uncertainty caused by the assumption of a discrete state made in a traditional BN. The comparative analysis of traditional BN and CBN shows that CBN is able to produce a more reasonable prediction of abnormal events and reflect the effects of any measurable change of casual factors on the probability variation of abnormal events. CBN can also better infer the state of causal factors than traditional BN given the observation of abnormal events. Furthermore, CBN has flexibility that helps calculate the probabilities of abnormal events for various accidents. The case study presented in this paper partially validated the usefulness of the proposed approach. Future work will be necessary to validate the approach using a real-world case. Moreover, it will also be valuable to develop a generic risk management framework that adopts the CBN-based approach as the basis.

Acknowledgements

The authors acknowledge the financial support provided by China Scholarship Council (CSC), and the Natural Sciences and Engineering Research Council of Canada

(NSERC).

References

[1] Khakzad N, Khan F, Amyotte P. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science, 2013; 57: 108–117.

[2] Khakzad N, Khan F, Amyotte P. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection, 2013; 91: 46–53.

[3] Yuan Z, Khakzad N, Khan F, Amyotte P. Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks. Risk Analysis, 2015; 35: 278－291.

[4] Abimbola M., Khan F., Khakzad N., Butt S. Safety and risk analysis of managed pressure drilling operation using Bayesian network. Safety Science. 2015, 76: 133–144.

[5] Leu S., Chang C.. Bayesian-network-based safety risk assessment for steel construction projects. Accident Analysis and Prevention, 2013, 54: 122－133

[6] Zhang L., Wu X, Skibniewski M.J., Zhong J., Lu Y.. Bayesian-network-based safety risk analysis in construction projects. Reliability Engineering and System Safety, 2014, 131: 29－39

[7] Chen T., Leu S.. Fall risk assessment of cantilever bridge projects using Bayesian network. Safety Science, 2014; 70:161–171

[8] Yang M., Khan F., Lye L.. Precursor-based hierarchical Bayesian approach for rare event frequency estimation: A case of oil spill accidents. Process Safety and

Environmental Protection, 2 0 1 3, 9 1: 333–342.

[9] Khakzad N., Khakzad S., Khan F.. Probabilistic risk assessment of major accidents: application to offshore blowouts in the Gulf of Mexico. Nat Hazards, 2014, 74: 1759–1771

[10] Shenoy PP. Inference in hybrid Bayesian networks using mixtures of Gaussians. In: Proceedings of the 22nd conference on uncertainty in artificial intelligence, 2006. p. 428–36.

[11] Meel A., Seider W. D.. Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science, 2006, 61: 7036–7056

[12] Khakzad N., Khan F., Amyotte P.. Dynamic risk analysis using bow-tie approach. Reliability Engineering and System Safety, 2012, 104: 36–44

[13] Thodi P. N., Khan F., Haddara M. R.. The Development of Posterior Probability Models in Risk-Based Integrity Modeling. Risk Analysis, 2010, 30: 400－420.

[14] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety, 2001; 71: 249–260.

[15] Gilks W.R.. Markov Chain Monte Carlo in Practice. Published by Chapman & Hall, London, UK, 1996.

[16] Lund D., Thomas A., Best N., Spiegelhalter D.. WinBUGS－A Bayesian modelling framework: Concepts, structure, and extensibility. Statistics and Computing. 2000, 10: 325–337

[17] R. Neal. Slice sampling. Annals of Statistics, 2003, 31: 705－767.

[18] Bergdahl L..Wave-Induced Loads and Ship Motions. Chalmers report, 2009. Available at <http://publications.lib.chalmers.se/records/fulltext/184947/local_184947.pdf>. [Accessed 17. 07. 2018]

[19] Hau E. Wind turbines – fundamentals, technologies, application, economics. 2nd ed. Berlin, Heidelberg: Springer-Verlag; 2006.

[20] UK Meteorological Office Fact Sheet 6. Available at: <http://www.metoffice.gov.uk/media/pdf/b/7/Fact_sheet_No._6.pdf.> [Accessed 10.07.2016]

[21] GeNIe 2.0. Version 2.0.5494.1, 2015. Available at: <https://dslpitt.org> [Accessed 18.01.2016]

[22] OpenBUGS. Version 3.2.3 rev 1012, 2014. Available at: <http://www.openbugs.net>. [Accessed 18.01.2016]

[23] Manual of OpenBUGS. Available at: <http://www.openbugs.net/Manuals/Tutorial.html#CheckingConvergence> [Accessed 10.07.2016]

4. Security Assessment of Process Facilities − Intrusion Modeling

Preface

A version of this chapter has been published in the Journal of Process Safety and Environmental Protection 2018; 117: 639－650. As the primary author, I developed the models and applied them in a case study. I completed the manuscript and improved it according to the feedbacks of co-authors and reviewers. Dr. Faisal Khan helped to identify the research topic and provide suggestions for manuscript improvement. Dr. Ming Yang helped to revise the original manuscript.

Abstract

The process industry is confronted with terrorism threats. Effective security management demands the ability to defend facilities against different intrusion scenarios. This study first presented various intrusion scenarios to explain the corresponding intrusion process using graphical barriers. Subsequently, this work dynamically analyzed the successful intrusion probabilities and security potentials of barriers using a Bayesian network considering the dependency of barriers and interaction of different intrusion scenarios. It was observed that successful intrusion probabilities and security potentials are strong functions of intrusion scenarios. Therefore, extensive intrusion scenarios must be considered while assessing and designing the security systems of process facilities.

Keywords: Intrusion scenarios; Intrusion process analysis; Bayesian network model; Dependency modelling; Probability update

4.1 Introduction

Terrorism is increasingly becoming a pressing concern across the world. The attacks on process facilities [1－10] demonstrate that the process industry is now an attractive target for terrorists. The process industry plays an essential role in the social and economic development, and large amounts of hazardous substances are processed in process plants every day. Attacking a process plant not only results in substantial economic losses [2] but also generates severe societal impact [11]. Thus, decent security management is urgently needed to protect process plants from terrorist attacks. Vulnerability assessment provides required information for security management. Vulnerability constitutes of two parts: the likelihood of successful intrusion and successful damage. Since prevention of intentional damage is very difficult once the intrusion is successful, especially for attacks with weapons, intrusion prevention accounts for a significant part of security management. Thus, effective intrusion assessment greatly supports the security management of process plants. Whether the existing barriers can effectively prevent intrusions becomes an interesting topic. However, as argued in [12], the adequacy of a security system depends on what it is protecting against. If the threat has been underestimated, readiness could be overestimated [12]. One feature of a security problem is that it includes two active sides － attackers and defenders, making successful intrusion depend on both

countermeasures of defenders and the intrusion pattern of attackers. The countermeasures which perform well in one kind of intrusion scenario do not necessarily work in another one. This means a facility well secured against one intrusion scenario could be vulnerable to others. If the intrusion assessment is conducted without the consideration of intrusion scenarios, the security risk of a plant could be significantly underestimated. To solve this problem, this study analyzes impacts of intrusion scenarios on successful intrusion probabilities.

The following works have conducted assessments of vulnerability and security risks. Reniers et al. [13] described a systematic development of a practical security system in the process industry. The authors stated that the probability of each type of intrusion scenario must be defined in the security risk assessment process [13], but they did not research the influence of different types of intrusion scenarios. Bajpai et al. [11] explained the steps of security risk management, including threat analysis, vulnerability analysis, security countermeasures and emergency response. Although terrorists, disgruntled employees, contractors and criminals were identified as sources of threats [11], intrusion scenarios were not discussed in their work. Argenti [14] clarified the collection process of related data based on expert experience to support the vulnerability assessment of physical protection systems. However, the influence of intrusion scenarios on related vulnerability data was not considered during expert surveys. Landucci [15] et al. investigated the possibility that a shock wave generated by

improvised explosives could damage process equipment and/or trigger an escalation sequence leading to a domino scenario. This study supports vulnerability assessments of industrial plants for a shock wave caused by improvised explosive devices. However, it did not research intrusion processes and scenarios. Van Staalduinen et al. used a graphical attack model to represent the process of state changes from safe conditions to successful attacks by breaching security barriers. Then a Bayesian network (BN) model was applied to calculate failure probabilities of barriers and consequence probabilities [5]. However, this model did not consider the influence of intrusion scenarios, and thus the assessment result cannot accurately reflect defensive ability for a specific intrusion scenario. Furthermore, not every security barrier works for all intrusion scenarios. Their graphical model cannot reflect how attackers achieve intrusion by destroying corresponding barriers in different intrusion scenarios. Thus, the intrusion process could not be well understood, and effective countermeasures could not be proposed for a specific intrusion scenario. Akgun et al. [16] presented a fuzzy integrated model to assess the vulnerability of a critical facility under multiple qualitative/quantitative criteria in a group decision-making environment. This model considered the interdependencies among the system functions (i.e., logical dependencies), but intrusion scenarios were not included in their assessment. Argenti et al. [17] applied a BN model to assess the vulnerability of chemical facilities to deliberate attacks quantitatively. However, they considered only the damage pattern (e.g., deliberate misoperation) instead of intrusion scenarios. Thus, the influence of intrusion scenarios on the

performance of physical security systems was not included. Furthermore, the interactions of different intrusion scenarios and dependency among causal factors (e.g., the dependency between CCTV and intrusion detection by security guards) were missing. Fakhravar et al. [18] developed a Discrete-time BN to investigate the vulnerability of a gas pipeline considering the performance of security countermeasures. This work did not analyze specific intrusion processes in different scenarios and did not consider the influence of intrusion scenarios on vulnerability. McGill et al. [19] assessed the non-performance of a security system based on the probability of adversary success using fuzzy logic. This work approximated the relationship between defensive capabilities and probability of adversary success based on the effectiveness of six defensive criteria. However, this model assumed a fixed initiating event; thus, it did not analyze the influence of intrusion scenarios on the probability of adversary success.

To the authors' knowledge, few works have considered the effects of intrusion scenarios on the success likelihood of intrusion. Van Staalduinen et al. [2] classified the attacks into three scenarios (manned, vehicle, and aerial-drone), and the consequence probabilities of the three scenarios were respectively calculated using BN models. However, this work did not analyze the damage process of barriers in specific intrusion scenarios, nor identify the security potentials of barriers in different intrusion scenarios. Moreover, since their work did not include the interactions of different intrusion scenarios, it cannot predict the latest successful intrusion probability of a scenario given

evidence from another scenario. This function is vital to obtain reliable intrusion probabilities with limited available information. Furthermore, this work failed to consider important barriers (e.g., tools' availability) for specific intrusion scenarios.

The current paper proposes an innovative approach to model the effects of intrusion scenarios on a successful intrusion. This work will help to identify critical scenarios and the weak links which can be strengthened to make the security system robust. Specifically, this study identified potential intrusion scenarios and visually represented specific intrusion processes by destroying corresponding barriers in a graphical model. Then a BN model was established based on the graphical model to assess success intrusion probabilities and analyze the security potentials of barriers in different intrusion scenarios. In this study, a barrier's security potential reflects the ability of the barrier to intrusion prevention in its current state. It is measured by the product of occurrence likelihood of an insecure barrier and the likelihood that the insecure barrier leads to intrusion success. The bigger the product is, the smaller security potential the barrier has. An insecure barrier means a barrier with a weak security state. Taking the barrier of workers in workplaces as an example, if the workers have a reduced ability to detect attackers and to timely report to security personnel, the barrier of workers in workplaces is an insecure barrier. Various factors can lead to the poor state of a barrier (i.e., an insecure barrier), which include technical factors, human factors [20] and organizational factors. For example, the poor state of the barrier of workers in

workplaces could be caused by the lack of training and regulations; the barrier of the fence could be in its weak state due to the design flaw, material defects or the lack of maintenance. Compared to previous works, this study clarifies intrusion processes by destroying corresponding barriers in different scenarios and quantitatively analyzes the influence of intrusion scenarios on the likelihood of successful intrusions and the security potentials of barriers. It includes attackers' features in the ability assessment of a defensive system. Furthermore, by including launching barriers, it can help defenders estimate what intrusion scenarios attackers would prefer, which will be discussed later. Moreover, this work enables the prediction of the latest successful intrusion probability in a scenario given evidence from another. Based on the updated result, the latest critical intrusion scenarios and weak links can be identified.

To facilitate a functional demonstration of the proposed method, several assumptions are made in this study: a) the attack target is located inside process plants; b) the attackers' goal is to destroy process facilities instead of gathering intelligence; c) the attackers know potential intrusion scenarios, but only one intrusion scenario is applied per time; d) no reinforcements of attackers come after starting the intrusion; e) in an intrusion stage, attackers seek the largest likelihood of successful intrusion regardless of cost; f) for internal intrusions, the terrorists first have an attack motivation and then they attempt to become employees in order to launch internal attacks; and g) all defenders aim to protect facilities, and none of them intend to cause damage. This study

only focuses on the intrusion processes of physical terrorism attacks instead of cyber attacks, wars or other causes. The damage to targeted facilities given successful intrusion is not covered in this work. The methodology framework of this work is shown in Fig. 4.1. The novel contributions of this work are: a) quantitatively analyzing the impacts of intrusion scenarios on the defensive ability of process plants; b) including the security layer for preventing the launching of an attack; and c) demonstrating dynamic assessment to support the dynamic identification of critical intrusion scenarios and dynamic detection of weak links in a security system.

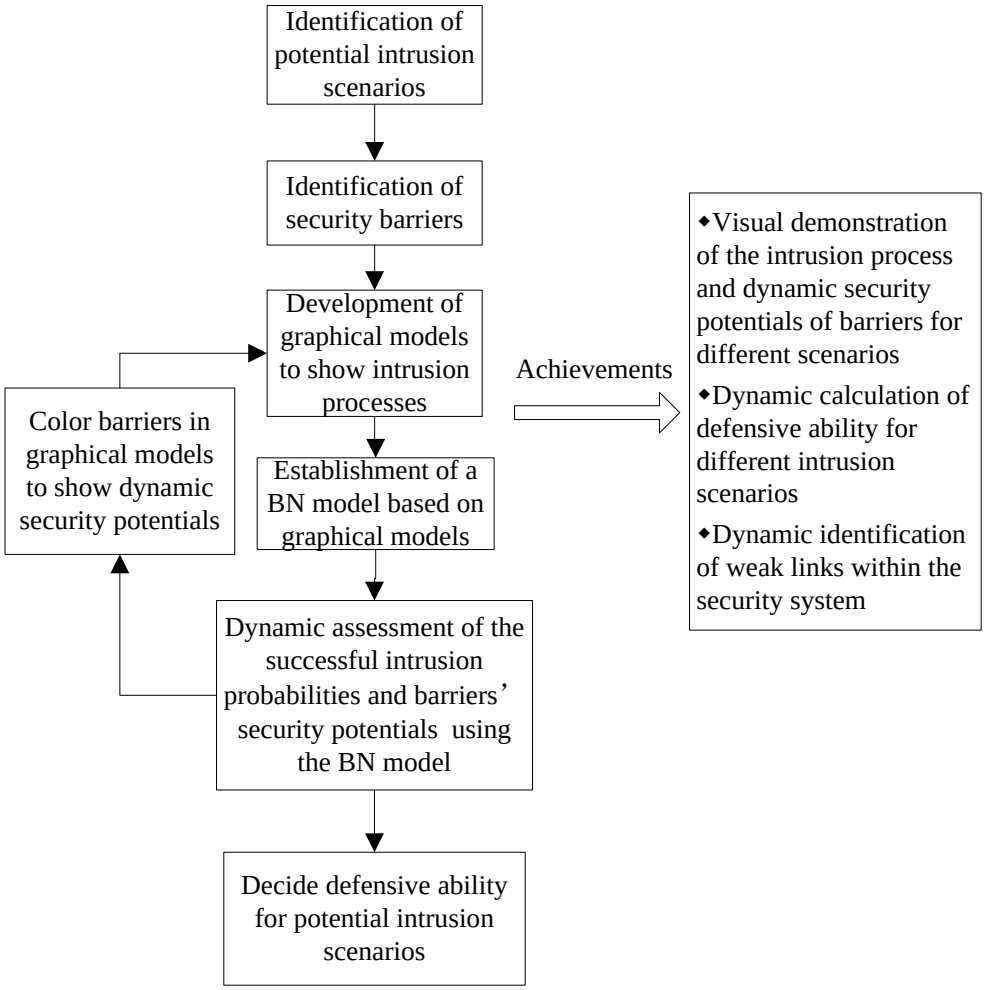


Fig. 4.1 Methodology framework for intrusion modelling

This paper is organized as follows: Section 4.2 identifies intrusion scenarios and security barriers. Section 4.3 presents graphical intrusion models and illustrates their advantages compared to the Swiss cheese model. In Section 4.4, a BN model is established, and it is applied to calculate and update successful intrusion probabilities as well as the security potentials of barriers for four intrusion scenarios. Section 4.5 provides conclusions.

4.2 The identification of intrusion scenarios and security barriers

4.2.1 Intrusion scenario identification

In this study, an intrusion refers to a process in which attackers or their attack tools (e.g., drones) reach the target by destroying related security barriers, given an attack motivation. This means that the arrival of attack tools to targets is also considered as a successful intrusion. The significant parameters to feature different intrusion scenarios in this work include attackers' background (insiders or outsiders), the devices used during the intrusion, and whether the intrusion is direct through violence. Table 4.1 shows the intrusion classification determined by records of previous terrorism attacks [3, 5－7, 21, 22] and related literature [2, 13].

Table 4.1 Intrusion classification

Intrusion categories	Intrusion types	Intrusion scenarios
External intrusion	Creep into	Creep in without guns
		Creep in with guns
		Direct attacks with firearms

	Direct intrusion by violence	Direct vehicle attacks with firearms
		Rocket attacks
		Drone attacks carrying explosives
Intrusion by insiders	Intrusion by insiders	Intrusion by employees
		Intrusion by contractors

The intrusion categories are divided based on the attackers' background. External intrusion is conducted by strangers or visitors, while intrusion by insiders is launched by workers or contractors. According to whether attackers need to avoid detection, the external intrusion is classified into two types—'creep into' and 'direct intrusion by violence'. For the intrusion type of 'creep into', attackers secretly intrude to avoid detection, while for the latter one, attackers directly intrude and destroy activated security measures using violence. Normally, in direct intrusion by violence, attackers have the strong capacity (e.g., being equipped with weapons) to damage the plant defences and the security in the area is very weak. In such a case, attackers have the confidence to achieve their goal even if they are detected (e.g., the attacks in Algeria [23]). Each intrusion type includes several intrusion scenarios. The type of 'creep into' is divided into 'creep in without guns' and 'creep in with guns' considering the significant difference of intrusion difficulty level caused by firearms. 'Direct intrusion by violence' is classified into 'direct attacks with firearms', 'direct vehicle attacks with firearms', 'rocket attacks' and 'drone attacks carrying explosives', based on the difference of applied intrusion devices [2]. The 'intrusion by insiders' is divided into 'intrusion by employees' and 'intrusion by contractors', based on the intruder's identity.

The employees' intrusion is considered much easier than the contractors'. Interviewing workers from a Chinese chemical plant, it was learned that contractors have different badges and work clothes from employees and that patrollers usually pay more attention to contractors. Compared with employees, in some companies, contractors may have limited access and less familiarity with the plant.

Table 4.1 demonstrates that attackers have various options to reach their targets. In practice, plants' security measures mainly focus on thieves who creep into plants, without paying enough attention to potential attacks which include different intrusion scenarios. Such security management leaves plants with a high vulnerability level.

4.2.2 Security barrier identification

Three security layers are identified based on three intrusion stages—launching, entrance and reaching targets within plants. The definitions of the three security layers are:

(1) Launching layer. When an attacker has an attack motivation for a given target, some conditions (e.g., obtaining required tools) must be satisfied to launch the attack. Thus, preparation of launching conditions is the first stage and the security layer working in this stage is called the launching layer. The launching layer comprises some launching barriers.

(2) Entrance layer. The target is assumed to be inside process plants, and attackers or their tools must enter the plant before reaching the target. Thus, the second stage is

to enter the plant. The security layer preventing attackers from entering plants is the entrance layer, which is constituted by entrance barriers.

(3) Interior layer. In the last intrusion stage, the attackers or their tools head for targets inside plants until reaching the target. The layer working in this stage is called the interior layer. It is made up of interior barriers.

The security barriers of each security layer are identified [11, 13, 19, 24, 25] and shown in Table 4.2. The target is a storage tank located in open air within a process plant. The security layers are noted for each security barrier in Table 4.2 to support the establishment of the graphical models in Section 4.3. Thereinto, L is the launching layer; E represents the entrance layer; and I is the interior layer.

Table 4.2 The identified security barriers [11, 13, 19, 24, 25]

Symbols	Meanings	Security layers	Prior probabilities of insecure barriers
B1	Intelligence collection and suppression of terrorism by the security agency	L	0.300
B2	Accessibility of intrusion tools	L	—
B3	Satisfaction of ability requirements for staff	L	0.100
B4	Background screening for employment	L	—
B5	Report of abnormal words and actions of colleagues	L	0.450
B6	Fence	E	0.100
B7	Patrol	E & I	—
B8	CCTV	E & I	0.010
B9	Folding gate	E	0.006
B10	Guard	E	0.150
B11	Local police	E & I	—

B12	Workers escorting visitors	I	0.001
B13	Workers in workplaces	I	0.200

The practical meanings of parts of the security barriers in Table 4.2 are illustrated below.

(1) Intelligence collection and suppression of terrorism by the security agency. The security agency collects terrorism intelligence, including information regarding terrorist groups, individuals, weapons and attack plots, to help suppress terrorist activities. Intense suppression can help cut the financial sources of terrorist groups, causing an impediment to weapons' purchase (e.g., rockets). Thus, good intelligence collection and suppression of terrorism can detect and destroy a potential attack in a timely way and limit terrorists' ability to launch attacks.

(2) Accessibility of intrusion tools. For some intrusion scenarios, tools (e.g., firearms) are required to launch an attack. Thus, the accessibility of similar tools limits the occurrence of such intrusion scenarios.

(3) Satisfaction of ability requirements for staff. For intrusion by insiders, attackers must become employees or contractors. They must satisfy the ability requirements to have an opportunity to be hired.

(4) Report of abnormal words and actions of colleagues. For intrusion by insiders, when workers or contractors have a motivation to launch an attack, they may use abnormal words or actions in daily life. Other workers may notice such abnormality and report it to related institutions. In this way, this barrier could prevent the launching of an internal attack.

(5) Workers escorting visitors. Based on the visitor escorting policy, workers should be assigned to escort visitors. These workers will prevent the visitors from approaching unauthorized facilities. This policy is a barrier to prevent intrusion launched by a visitor.

(6) Workers in workplaces. Many plants have a policy that workers take charge of their own work areas. Normally, when strangers enter workplaces, workers interrogate them and report to security personnel. These workers constitute a barrier for a successful intrusion.

4.3 Intrusion process analysis for different scenarios

4.3.1 Swiss cheese model and its limitations to represent intrusion process

The Swiss cheese model has been applied to represent accident causation in previous work [26]. In the model, slices were used to model barriers which represent defences against failure. A hole in a slice represents a weakness in the system. Accidents occur when the holes in the slices are aligned [5]. If a Swiss cheese model (see Fig. 4.2) is used to describe the principle of the successful intrusion, ‘S’ represents security barriers between attack motivation and successful intrusion. It can be observed from Fig. 4.2 that successful intrusion occurs due to the failures of security barriers. However, for each intrusion scenario, the corresponding barriers may be different. If existing barriers are analyzed without considering the intrusion scenarios, the principle and process of barrier damage in each intrusion scenario cannot be understood. Thus, corresponding

countermeasures cannot be adequately proposed for specific intrusion scenarios. For example, although all barriers in Fig. 4.2 can help to prevent intrusion, listing only all existing barriers without considering the intrusion scenario, the Swiss cheese model cannot clarify what barriers work for which intrusion scenario and what barriers exist in different intrusion stages.

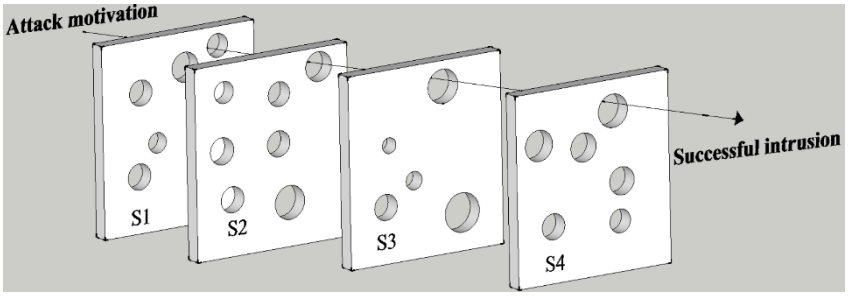


Fig. 4.2 Schematic Swiss cheese model for successful intrusion

Furthermore, a Swiss cheese model has limitations to model intrusion process due to its linear nature, and below is a brief review of the impractical points.

(1) The barriers are represented by a linear sequence in Fig. 4.2, but in practice, the barriers do not necessarily function in a strict sequence. Some barriers may have a parallel relationship (e.g., gates and fences).

(2) Barriers may not be destroyed one by one, since the following barriers may be skipped automatically when the previous barrier fails. Fig. 4.2 cannot reflect this point.

(3) Some barriers can only work together with other barriers, which cannot be represented in Fig. 4.2.

4.3.2 The establishment of graphical models and their merits

To overcome the limitations of the Swiss cheese model, a graphical intrusion model is proposed in this study. Not only can the graphical intrusion model represent the nonlinear feature of intrusion issue, but it also clarifies the processes for specific intrusion scenarios. A general graphical model is shown in Fig. 4.3. This model includes three security layers, and corresponding security barriers are assigned inside the layers. The security layers are represented using large rectangles, while security barriers are shown as small rectangles. The intrusion is achieved through the damage of security barriers and the intrusion processes in a particular scenario are represented by different sets of arrows starting from attack motivation and ending with the successful intrusion.

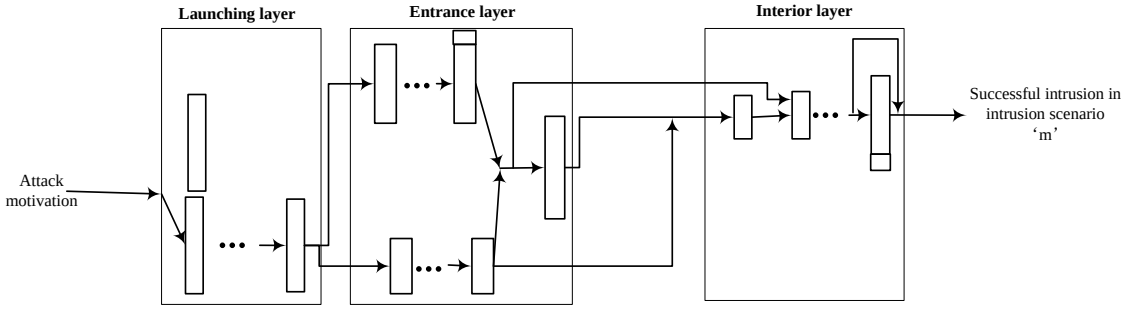


Fig. 4.3 A general graphical model for an intrusion scenario

This study presents graphical models for four intrusion scenarios: i) creeping in without guns, ii) direct vehicle attacks with firearms, iii) drone attacks carrying explosives, and iv) intrusion by employees. The security layers and intrusion scenarios are listed in Table 4.3. The attack target is a storage tank located in open air within a process plant.

To highlight the merits of the proposed graphical models, a Swiss cheese model is also established for the comparison purpose. Fig. 4.4 is a Swiss cheese model demonstrating the process of a successful intrusion, while Fig. 4.5 shows the graphical models developed for these four intrusion scenarios.

Table 4.3 Successful intrusion scenarios and their security layers

Symbols	Meanings
ML1	Launching layer for ‘creep in without guns’
ME1	Entrance layer for ‘creep in without guns’
MI1	Interior layer for ‘creep in without guns’
ML2	Launching layer for direct vehicle attacks with firearms
ME2	Entrance layer for direct vehicle attacks with firearms
MI2	Interior layer for direct vehicle attacks with firearms
ML3	Launching layer for drone attacks carrying explosives
ME3	Entrance layer for drone attacks carrying explosives
MI3	Interior layer for drone attacks carrying explosives
ML4	Launching layer for intrusion by employees
ME4	Entrance layer for intrusion by employees
MI4	Interior layer for intrusion by employees
C	Successful intrusion of ‘creep in without guns’
V	Successful intrusion of direct vehicle attacks with firearms
D	Successful intrusion of drone attacks carrying explosives
E	Successful of intrusion by employees

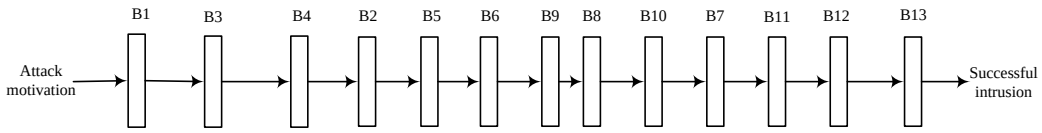


Fig. 4.4 Swiss cheese model for successful intrusion (refer to Table 4.2 for meanings of symbols)

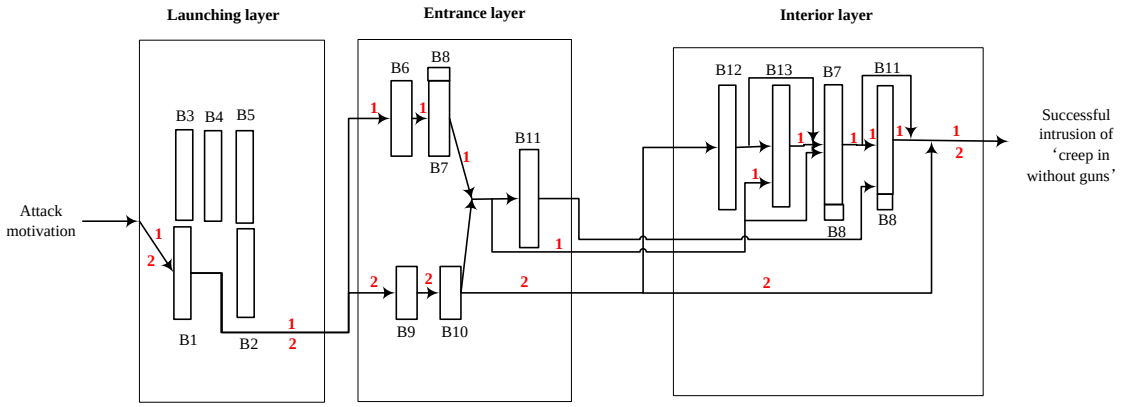


Fig. 4.5 (a) Graphical intrusion model for 'creep in without guns'

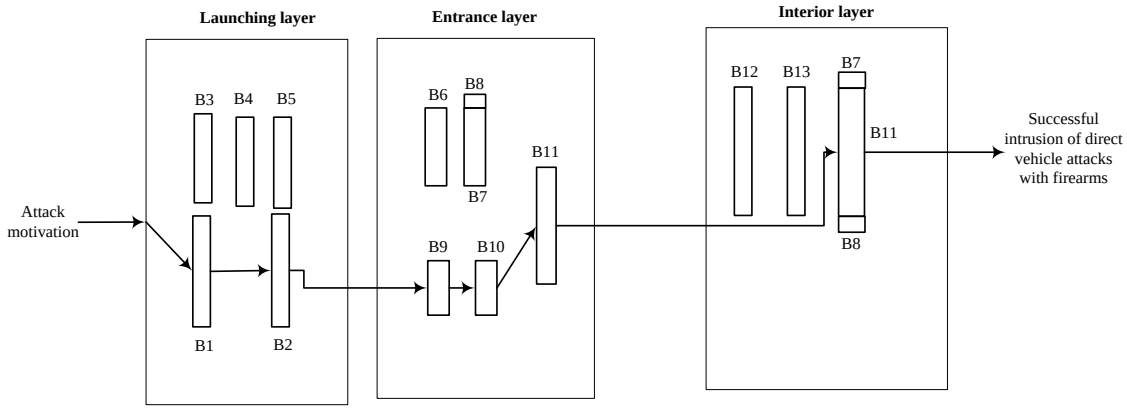


Fig. 4.5 (b) Graphical intrusion model for direct vehicle attacks with firearms

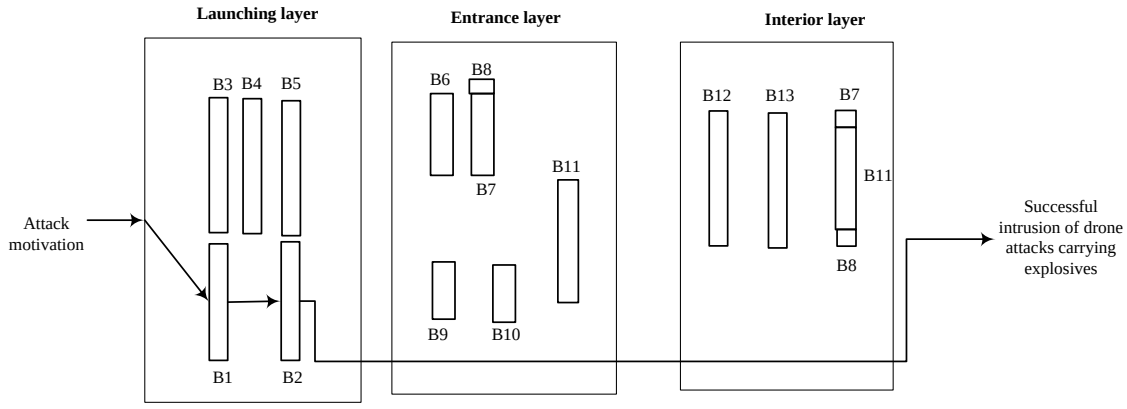


Fig. 4.5 (c) Graphical intrusion model for drone attacks carrying explosives

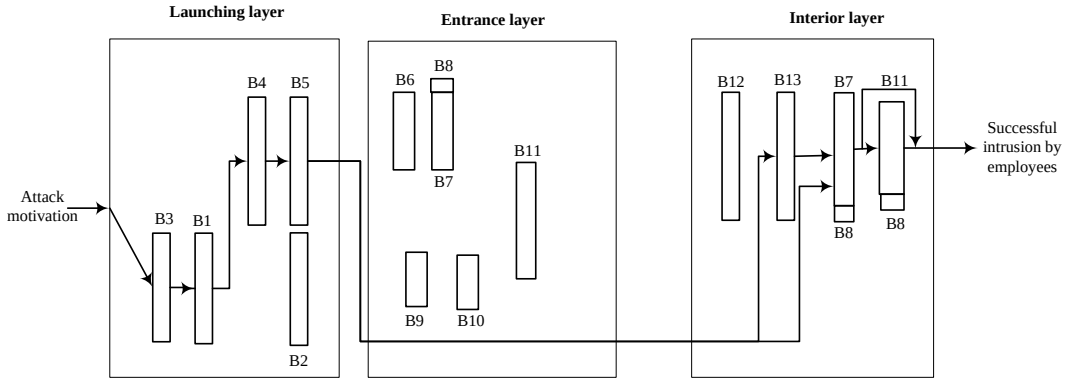


Fig. 4.5 (d) Graphical intrusion model for intrusion by employees

Fig. 4.5 Graphical intrusion models for different intrusion scenarios (refer to Table 4.2 for meanings of symbols)

Unlike the Swiss cheese model in Fig. 4.4, the graphical models in Fig. 4.5 clearly show intrusion processes. For example, Fig. 4.5(a) includes various intrusion processes for 'creep in without guns', two of which are explained below. These two processes are noted using '1' and '2' in Fig. 4.5(a).

(1) In intrusion process 1, a person with an attack motivation overcomes the intelligence collection and suppression of terrorism by the security agency (B1), and launches the attack of 'creep in without guns'. The person enters the plant by breaching fences (B6) without being detected by patrol (B7). In the plant, the attacker is detected by workers in workplaces (B13) who then report to the patrol (B7). Unfortunately, the patrols are unable to control the attacker, and they call local police (B11). However, before local police arrive, the attacker reaches the storage tank.

(2) In intrusion process 2, a person with attack motivations overcomes the intelligence collection and suppression of terrorism by the security agency (B1) and launches an attack of 'creep in without guns'. The person enters the plant from the folding gates (B9) without being detected by guards (B10). In the plant, the attacker is not detected by workers in the workplaces or the patrol, successfully reaching the storage tank.

Apart from this merit, the proposed graphical models (Fig. 4.5) include the nonlinear relationship between barriers. Specifically, they have the following advantages, compared to the Swiss cheese model in Fig. 4.4:

- They consider that attackers could destroy alternative barriers to reach their targets. For example, in Fig. 4.5(a), when attackers creep into a plant, they could enter through gates or, alternatively, through fences. In this scenario, the gate and fence are not destroyed in sequence.
- They consider that attackers could skip barriers instead of destroying one by one in sequence to reach their targets. In the entrance stage of Fig. 4.5(a), when the patrol or guards detect attackers, the local police could be informed, and they then become an element of the entrance layer. Otherwise, the barrier of local police is skipped.
- They represent the fact that some barriers only function while cooperating with other barriers. Fig. 4.5(a) shows that CCTV helps patrols and local police detect

attackers. However, if no officers are watching, the CCTV itself could not prevent intrusions.

- They identify what barriers exist in different intrusion stages for a specific intrusion scenario. This can help to guide the selection of a countermeasure. For example, managers hope to prevent an attack as early as possible. If one measure can enhance the interior barrier and another measure can enhance the launching barrier, both of which have similar prevention effects and cost, priority should be given to the latter one.
- They demonstrate what barriers are destroyed in different intrusion scenarios. This visual information can provide support to decide what barriers can be enhanced to prevent specific intrusion scenarios. For example, according to Fig. 4.5 (d), background screening could prevent the launching of an internal attack. If an internal attack is launched, to prevent such an attack from reoccurring, resources can be allocated to enhance background screening. This is consistent with the practical case. In the 2015 terrorist attack on a French chemical plant, the deliveryman of the plant was on a terrorist list but was not identified due to inadequate background screening [3].

4.3.3 The features of different intrusion scenarios

Some features of the four intrusion scenarios are observed in Fig. 4.5. According to Fig. 4.5(a) and Fig. 4.5(b), all three security layers work for ‘creep in without guns’ and direct vehicle attacks with firearms. All entrance and interior barriers contribute to the

intrusion prevention of ‘creep in without guns’, but only one launching barrier has prevention effects for that intrusion scenario. This is because the attack of ‘creep in without guns’ does not need many attackers and special attack tools; thus, it is easy to conduct and hard to detect before launching.

According to Fig. 4.5(c), the entrance and interior layers do not work for the intrusion scenario of drone attacks carrying explosives. Existing barriers tend to be designed to prevent attacks launched on the ground instead of an air attack; thus, drone attacks with explosives have the least barriers among the four intrusion scenarios, as shown in Fig. 4.5. Drones are emerging products, and they have been used for attacks. ISIS has recently conducted drone attacks in Iraq, and the FBI detected plots of launching small drones with bombs targeting the Pentagon and the capitol of the US in 2011 [22]. To prevent a drone attack carrying explosives, the existing barriers need to be enhanced, for example, by taking stricter control of explosives. Also, extra barriers can be added, such as applying interference devices to disable drone flights above the chemical plant area. Moreover, legislation could be passed to define process plants as no-fly zones (some nations have taken this measure) and to require that manufacturers design drones which cannot fly above process plants.

Fig. 4.5(d) shows that the entrance layer also does not work for intrusion by employees, which is because the attackers have the authority to enter the plant in this scenario.

However, attackers need to overcome four launching barriers to start an internal attack as demonstrated in Fig. 4.5(d). This leaves more options to prevent the launching of intrusion by employees than other intrusion scenarios shown in Fig. 4.5.

4.4 Quantitative intrusion assessment using a Bayesian network model

In this section, successful intrusion probabilities of the above-mentioned four scenarios are calculated using a BN model. The calculation results are used to assess the defensive ability for each intrusion scenario. The barriers' security potentials are also analyzed considering the prior probabilities of insecure barriers and weights. Subsequently, the defensive ability and barriers' security potentials in different scenarios are dynamically assessed.

4.4.1 The establishment of BN model

Fig. 4.6 shows a general BN model of successful intrusion for ‘m’ potential scenarios. Within this Figure, nodes represent causal factors and target events, while arcs show their dependence. The relationship of dependent nodes is represented with conditional probability tables (CPTs). More detailed information about the basic of BN model can be obtained from [27, 28].

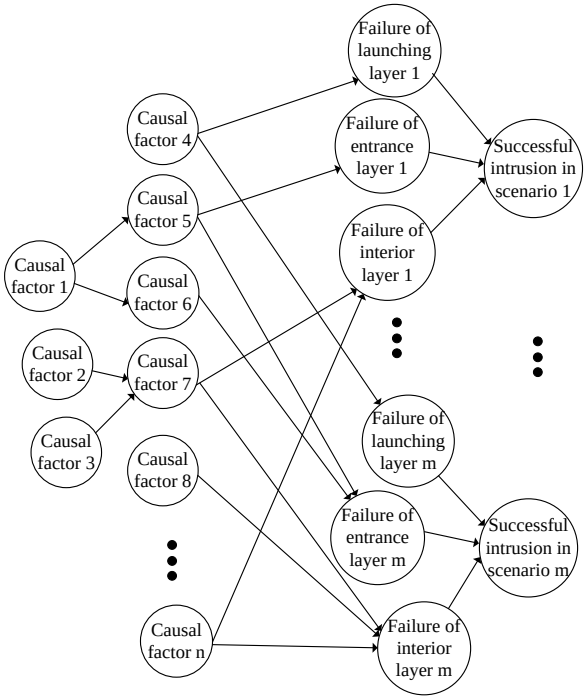


Fig. 4.6 A general Bayesian network model for 'm' intrusion scenarios

The BN model as shown in Fig. 4.7 is established to conduct the quantitative assessment of successful intrusion for these four scenarios. As discussed in Section 4.3, successful intrusion is achieved once security barriers are destroyed. This means barrier failures contribute to the success of intrusion and thus insecure barriers can be considered as causal factors of the successful intrusion. The insecure barriers and failure of security layers serve as the primary and intermediate nodes of the BN model. Fig. 4.5 has provided a clear demonstration of the barriers and layers involved in each intrusion scenario. Based on Fig. 4.5, the related nodes are decided for each intrusion scenario. Then the dependencies among barriers are analyzed and represented as links among the nodes. For example, CCTV helps the patrol and local police to detect and locate attackers; thus, failure of the CCTV may contribute to a failure of the patrol and local

police to defend against attackers. Therefore, CCTV is linked to the patrol and local police in the proposed BN model. Furthermore, some barriers work for more than one intrusion scenario. For example, B1 (Intelligence collection and suppression of terrorism by security agency) influences the successful intrusion probabilities of all four scenarios through influencing the failure probability of their launching layers. To reflect this feature, B1 is linked to four launching layers in the BN. With such linking, the interactions between the four intrusion scenarios are established. In this way, the proposed BN model (Fig. 4.7) represents the quantitative dependencies among barriers and also includes the interactive relationship between different intrusion scenarios. The prior probabilities of insecure barriers are presented in Table 4.2. The prior probabilities could be determined by experts according to the specific situation of the plant. Experts need to consider the causal factors (e.g., technical, human and organizational factors) of insecure barriers to decide their prior probabilities. The analysis results could reflect the practical situation of the specifically targeted plant, and help to manage security in practice. Although the data used in Section 4.4 is hypothetical, it does not influence the function illustration of the proposed BN model. The current paper aims to explain the functions of this model and demonstrate its advantage instead of directly guiding the practical security management with the analysis results.

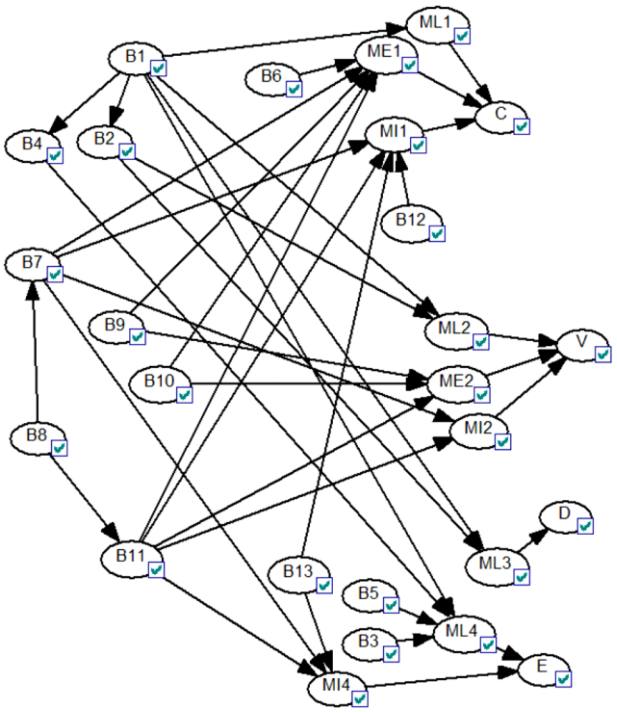


Fig. 4.7 Quantitative intrusion assessment model considering different intrusion scenarios (refer to Tables 4.2 & 4.3 for the meanings of symbols)

4.4.2 The assessment of successful intrusion probabilities and security potentials of barriers

4.4.2.1 The probabilities of successful intrusion in different scenarios

The successful intrusion probabilities and the failure probabilities of security layers are calculated using the established BN model in Fig. 4.7, and the results are shown in rows 2 and 5—7 of Table 4.4. To help understand the defensive ability in each intrusion scenario, the assessment criteria are defined in Table 4.5. “Unacceptable” means the success probability of intrusion cannot be accepted, while “acceptable” means the current defensive state for the intrusion is acceptable. “Tolerable” means the successful intrusion probability is tolerable when the cost of countermeasures is not proportionate

to the probability reduction. It is worth mentioning that the probabilities in Table 4.5 are conditional probabilities, given a precondition that attackers have an attack motivation and are planning to launch an attack on a specific target. The probability 10^{-4} in Table 4.5 can be understood as that for when 10,000 intrusions are planned to be launched, only one intrusion succeeds. The probability smaller than 10^{-4} is acceptable, while that higher than 10^{-3} is unacceptable. According to this explanation, 10^{-4} means that if attackers plan to attack a plant once per 30 days, they may succeed one time in 3×10^5 days (i.e., 822 years).

Table 4.4 The probabilities of successful intrusion and security layer failure in the four intrusion scenarios

	Creep in without guns	**Direct vehicle attacks with firearms**	**Drone attacks carrying explosives**	**Intrusion by employees**
Prior probabilities of the successful intrusion	8.58×10^{-5}	1.55×10^{-4}	4.37×10^{-3}	1.34×10^{-3}
Posterior probabilities of the successful intrusion (given successful drone attack)	9.01×10^{-5}	2.78×10^{-2}	—	5.22×10^{-3}
Posterior probabilities of the successful intrusion (given launched vehicle attacks, but failure to enter)	8.19×10^{-5}	—	7.85×10^{-1}	5.19×10^{-3}
Failure probabilities of launching layers	8.85×10^{-1}	4.19×10^{-3}	4.37×10^{-3}	5.41×10^{-3}
Failure probabilities of entrance layers	4.77×10^{-3}	9.75×10^{-2}	1.00	1.00
Failure probabilities of interior layers	1.77×10^{-2}	3.42×10^{-1}	1.00	2.48×10^{-1}

Table 4.5 Assessment criteria for defensive ability

Defensive ability	Successful intrusion probabilities
Unacceptable	$>10^{-3}$
Tolerable	$10^{-4}—10^{-3}$
Acceptable	$<10^{-4}$

Comparing the successful intrusion probabilities in row 2 of Table 4.4 to the criteria in Table 4.5, it is observed that the abilities to defend against 'a drone attack carrying explosives' and 'intrusion by employees' are unacceptable, while that for 'a direct vehicle attack with firearms' is tolerable. Only the successful intrusion likelihood of 'creep in without guns' is acceptable. Thus, 'a drone attack carrying explosives' and 'intrusion by employees' are critical intrusion scenarios in this case. According to rows 6 and 7 and columns 4 and 5 of Table 4.4 it is observed that the highly successful probabilities given an attack motivation in the two critical scenarios are mainly caused by the high failure probabilities of the entrance and interior layers (all higher than 0.2). This is decided by the intrusion features. As explained in Section 4.3, attackers for internal intrusion are employees or contractors; they have the authorization to enter the plant. Thus, the failure probability of the entrance layer is considered as 1 in this scenario. When attackers are familiar with plant circumstances and patrol schedules, they can exploit deficiencies in the security system to avoid being detected while conducting an intrusion. Thus, with a failure probability of 2.48e-1, the interior layer does not work well for intrusion by employees. A drone attack carrying explosives intrudes from the air. As mentioned in Section 4.3, drone attacks have not been much

considered in security management and countermeasures for drones to enter plants and to approach the targeted facilities located in the open air are unavailable. Thus, a plant normally has very high failure probabilities of the entrance and interior layers for drone attacks carrying explosives. This is why drone attacks carrying explosives have the highest success likelihood (4.37×10^{-3}). In contrast, 'creep in without guns' has the lowest successful probability (8.58×10^{-5}) due to both its small failure probabilities of the entrance and the interior layers (4.77×10^{-3} and 1.77×10^{-2}).

The comparison of results of different intrusion scenarios in Table 4.4 reveals the importance of considering various potential intrusion scenarios in the security assessment. If a security manager only focuses on the prevention of 'creep in without guns', the defensive ability is considered as acceptable with a successful intrusion probability of 8.58×10^{-5}. Therefore, the manager may conclude that no additional security countermeasures are needed for intrusion prevention. However, in practice, attackers could attempt a drone attack carrying explosives which has a high likelihood (4.37×10^{-3}) to achieve the intrusion. Thus, the defence level of the plant is unacceptable in reality. Considering various potential intrusion scenarios is necessary for security management. Furthermore, by considering intrusion scenarios, critical intrusion scenarios can be identified, which provides useful guidance for the security resource assignment. For example, in this case study, priority should be given to countermeasures for drone attacks and intrusion by employees instead of evenly

allocating resources for all scenarios. Moreover, since this assessment model includes launching layers, the results could help security managers estimate what intrusion scenarios attackers are most likely to apply. When attackers select intrusion scenarios, they not only consider whether a launched intrusion could succeed, but also consider whether the intrusion is difficult to launch. Attackers will not prefer an intrusion scenario which is almost impossible to launch, even though once launched it has a high probability to intrude successfully. Thus, without including launching layers, estimating what intrusion scenarios attackers are most likely to apply is unrealistic. The proposed method includes the launching layer in the intrusion analysis, overcoming this drawback. In this case, drone attacks carrying explosives have the highest successful intrusion probability; thus, it is believed attackers prefer drone attacks if they seek high successful intrusion probabilities.

4.4.2.2 The security potential of barriers for each intrusion scenario

Security potential assessment of barriers can help to detect the weak links of the security system. If a barrier has a high probability to be in an insecure state and its insecure state has a significant contribution to a successful intrusion in a scenario, the barrier is considered to have a small security potential in that intrusion scenario. As shown in Table 4.6, security potentials are divided into four levels according to the product of occurrence probabilities of insecure barriers and weights of the insecure barriers of a successful intrusion. To improve the defensive ability of a security system in an

intrusion scenario, improvement of the barriers with small security potentials in that scenario has a priority.

Table 4.6 The classification criteria for security potentials of barriers

Probability * weight	Classification of security potentials	Expression
$[10^{-3},1)$	Very low (VL)	Red
$[10^{-4}, 10^{-3})$	Low (L)	Purple
$[10^{-5}, 10^{-4})$	Medium (M)	Orange
$(0, 10^{-5})$	High (H)	Green

This section analyzes the security potentials of barriers in each intrusion scenario. First, the occurrence probabilities of insecure barriers are calculated with a BN model. The weight of a barrier is calculated as the probability change of successful intrusion given occurrence and nonoccurrence of the insecure barrier using the BN model. Compared to the criteria in Table 4.6, the security potentials of barriers in different intrusion scenarios are decided and shown in Table 4.7. The rows of Table 4.7 represent the security potential of each barrier in different intrusion scenarios. From rows 1 to 14, it can be observed that the security potential of a barrier can vary from high to very low in different intrusion scenarios. For example, B1 (Intelligence collection and suppression of terrorism by security agency) poses a high-security potential for ‘creep in without guns’, but has a very low one for drone attacks carrying explosives. If the aim is to prevent drone attacks carrying explosives, B1 could be given priority. However, if ‘creep in without guns’ requires better prevention, B1 does not have priority to be improved. Each column of Table 4.7 shows what barriers have smaller security potential

in each intrusion scenario. This can help to identify the weakness in each intrusion scenario. However, to assess the weak link of the security system, the critical intrusion scenarios need to be decided first. The barriers with small security potentials in critical scenarios are the weak links of the system. For example, drone attacks carrying explosives and intrusion by employees are critical intrusion scenarios in this case study. Barriers B1—B3 have very low-security potentials for the critical scenarios; therefore, they are the weak links of the security system. It is worth mentioning that the probability-based information could support the decision of countermeasures' priority. However, other factors (e.g., the cost effects) also need to be analyzed to decide the priority of countermeasures finally.

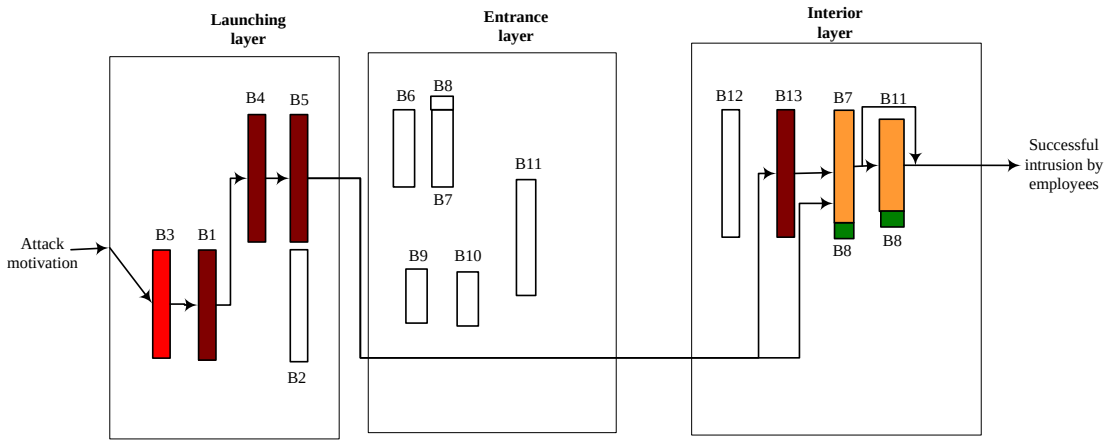
Table 4.7 The security potentials of barriers in each intrusion scenario

Intrusion scenarios / Security potentials (prior/posterior)	Creep in without guns	Vehicle attacks with firearms	Drone attacks carrying explosives	Intrusion by employees
B1	H/H	L/VL	VL/VL	L/VL
B2	—	L/VL	VL/VL	—
B3	—	—	—	VL/VL
B4	—	—	—	L/VL
B5	—	—	—	L/L
B6	M/M	—	—	—
B7	M/M	H/H	—	M/M
B8	H/H	H/H	—	H/H
B9	H/H	H/H	—	—
B10	M/M	H/H	—	—
B11	H/H	M/M	—	M/H
B12	H/H	—	—	—

B13	H/H	—	—	L/L

Note: '—' means the barriers do not work for that intrusion scenario. L represents low-security potential, and M means medium. H means high, while VL represents very low.

The analysis results of security potentials can be presented in the graphical models proposed in Section 4.3 by representing security potentials using different colours (see column 3 of Table 4.6). Fig. 4.8 shows the security potentials of barriers in the scenario of intrusion by employees. It clearly shows all four barriers in the launching layer have low to very low-security potential, while only one barrier in the interior layer has low-security potential. This provides a visual reference for security managers to understand the weakness for intrusion by employees.



Red: very low-security potential; Purple: low; Orange: medium; Green: high. B1: Intelligence collection and suppression of terrorism by security agency; B3: Satisfaction of ability requirements for staff; B4: Background screening for employment; B5: Report of abnormal words and actions of colleagues; B7: Patrol; B8: CCTV; B11: Local police; B13: Workers in workplaces.

Fig. 4.8 Graphical model with security potentials for the scenario of intrusion by employees

4.4.3 The dynamical probability assessment

Because of data scarcity, the prior probabilities of insecure barriers often need to be obtained from experts' experiences in practical assessment, which introduces uncertainty to assessment results. With a dynamic feature, a BN model can update the probability to reduce such uncertainty. Furthermore, the occurrence probabilities of insecure barriers may change over time, which leads to the change of successful intrusion probabilities for different scenarios. This is another source of uncertainty of assessment results. A BN model can diagnose the change of insecure barriers using available evidence. Then successful intrusion probabilities could be updated based on the posterior probabilities of insecure barriers.

4.4.3.1 Dynamic probability assessment given a successful intrusion

By integrating different intrusion scenarios in a BN model, the intrusion information of one scenario could be applied to update the probabilities of successful intrusion of other scenarios. For example, when attackers successfully intrude using a drone carrying explosives, the evidence can be set as ‘successful intrusion of drone attacks carrying explosives’ in the BN model of Fig. 4.7. Then the BN model is updated, and the posterior probabilities of successful intrusions of the other three scenarios are shown in row 3 of Table 4.4. Comparing rows 2 and 3 of Table 4.4, it is observed that the updated successful intrusion probabilities of ‘creep in without guns’, direct vehicle attacks with firearms and intrusion by employees become larger than their prior estimates. This is because when a successful intrusion of a drone attack carrying explosives occurs,

barriers B1 and B2 are believed to have higher probabilities within insecure states than the prior estimation, and their changes increase failure probabilities of launching layers for other scenarios and further lead to the growth of successful intrusion in those scenarios. When the evidence of successful drone intrusion carrying explosives is included in the assessment, the success probability of direct vehicle attacks with firearms has the largest growth, from 1.55×10^{-4} to 2.78×10^{-2}. According to the criteria in Table 4.5, the defensive ability against vehicle intrusion is unacceptable instead of tolerable (the prior result obtained in Section 4.4.2.1). The vehicle intrusion with firearms becomes a critical intrusion scenario for the targeted facility. This analysis reveals that if evidence about one intrusion scenario is observed, the successful intrusion probabilities for other scenarios can be updated, even though evidence related to those intrusion scenarios is unavailable. After an update, it may be observed that more intrusion scenarios are critical ones for the targeted facility. Using the solid evidence to conduct the dynamic assessment, the BN model provides a more reliable assessment of defensive ability.

4.4.3.2 Dynamic probability assessment given a failed intrusion

Many intrusions are effectively prevented in practice. Such an event can also help to update probabilities of successful intrusion in different scenarios. For example, a direct vehicle attack with firearms was launched on a storage tank, but attackers failed to intrude into the plant. The evidence is set as ‘failure of the launching layer for direct vehicle attack with firearms’ and ‘success of the entrance layer for direct vehicle attack

with firearms' in the proposed BN model of Fig. 4.7. Given this evidence, the BN model is updated, and the results are shown in row 4 of Table 4.4.

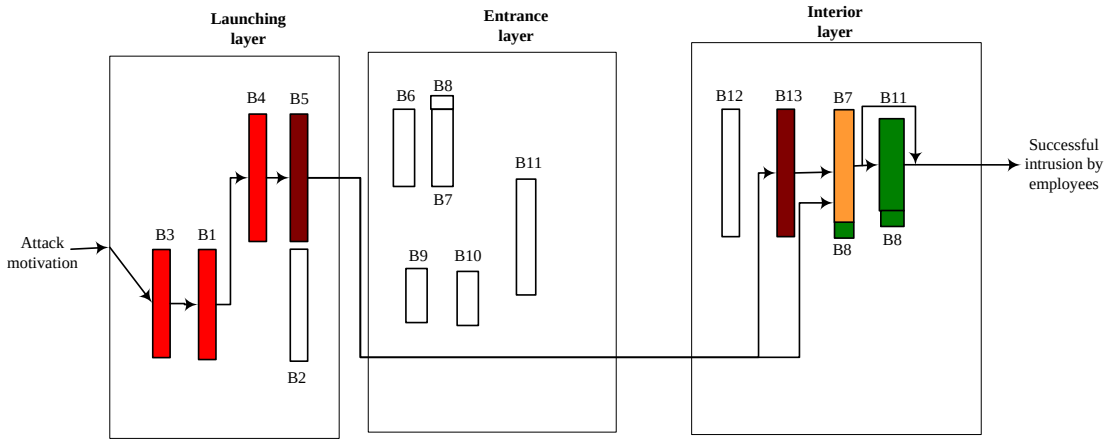
After comparing rows 2 and 4 of Table 4.4, it can be seen that the posterior probabilities of successful intrusion for both the drone attack carrying explosives and intrusion by employees increase. The increase of success probability of a drone attack carrying explosives is much larger than that of intrusion by employees. This is because the launching barriers of drone attacks carrying explosives and direct vehicle attacks with firearms are the same. The launching of the two attacks can be prevented by both 'intelligence collection and suppression of terrorism by security agency' and 'accessibility of intrusion tools'. Thus, when the launching layer for direct vehicle attack fails, the posterior failure probability of the launching layer for drone attacks carrying explosives experiences a significant increase from 4.37×10^{-3} to 7.85×10^{-1}. Intrusion by employees has only one identical launching barrier with direct vehicle attacks with firearms, and the posterior probability of its launching layer increases from 5.41×10^{-3} to 2.10×10^{-2}, which is much smaller than the probability increase of the launching layer for drone attack carrying explosives. This model reveals that the drone attacks carrying explosives and direct vehicle attacks with firearms have similar features. Thus, when the plant is vulnerable to one intrusion scenario, it is more probable to be vulnerable to the other one.

It is interesting to observe that the posterior success probability of ‘creep in without guns’ has a decrease from 8.58×10^{-5} to 8.19×10^{-5}. This is because of the failure probability of entrance layer of ‘creep in without guns’ decreases from 4.77×10^{-3} to 4.28×10^{-3}. The success of the entrance layer for direct vehicle attack with firearms make it believe that the insecure barriers in the entrance layer have smaller posterior occurrence probabilities than the prior belief. This change decreases the posterior failure probabilities of entrance layer of ‘creep in without guns’, which causes the reduction of the successful intrusion probability of ‘creep in without guns’. The updated results demonstrate that the entrance layer has a better ability for entrance prevention in the scenario of ‘creep in without guns’, and the plant has a better defence ability to prevent ‘creep in without guns’ than the prior belief.

4.4.3.3 Dynamic assessment for security potentials of barriers

If a failed intrusion is observed, the security potentials of barriers can also be updated. For example, when the ‘failure of the launching layer for direct vehicle attack with firearms’ and ‘success of the entrance layer for direct vehicle attack with firearms’ are set as the evidence in the BN model of Fig. 4.7, the posterior occurrence probabilities of insecure barriers are calculated using the BN model. Then the updated security potentials of barriers are analyzed following the process mentioned in Section 4.4.2.2, and the results are shown in Table 4.7. According to Table 4.7, it is observed that the security potentials of B1 and B2 in the scenario of a direct vehicle attack with firearms become ‘very low’ instead of ‘low’ (prior security potentials), while the security

potentials of B1 and B4 in the scenario of intrusion by employees become ‘very low’ instead of ‘low’. B11's security potential in the scenario of intrusion by employees becomes high instead of medium. Thus, when evidence is used in the BN model, the posterior security potentials of barriers are obtained, which supports a more reliable weakness identification of a security system. After updating, it is believed B4 also has a very low-security potential for one of the critical intrusion scenarios—intrusion by employees. Thus, apart from B1—B3, B4 is also a weak link of the security system.



Red: very low-security potential; Purple: low; Orange: medium; Green: high. B1: Intelligence collection and suppression of terrorism by security agency; B3: Satisfaction of ability requirements for staff; B4: Background screening for employment; B5: Report of abnormal words and actions of colleagues; B7: Patrol; B8: CCTV; B11: Local police; B13: Workers in workplaces.

Fig. 4.9 Updated graphical model with security potentials for the scenario of intrusion by employees

Fig. 4.9 provides a visual expression of the updated security potentials of barriers for intrusion by employees. Compared to Fig. 4.8, it clearly demonstrates that the security

potentials of B1 and B4 move to very low from low, while that of B11 becomes high instead of medium. The visual form provides security managers with an updated understanding of the weakness for intrusion by employees.

4.5 Conclusions

This study developed a graphical model to visually express principles and processes of barrier damage to achieve an intrusion in different scenarios. Compared with a Swiss cheese model, the proposed graphical model reflected the nonlinear relationship of barriers. Then, a BN model was established based on the graphical model. The BN model has a dynamic feature and includes dependency among barriers and interaction between different intrusion scenarios. The successful intrusion probabilities and security potentials of barriers in four intrusion scenarios were assessed using the proposed BN model. The assessment results revealed that the defensive ability of a process plant and the security potentials of barriers could significantly vary in different intrusion scenarios. According to the assessment results of the BN model, critical intrusion scenarios and weak links in the security system were identified. Then dynamic assessments were demonstrated using the BN model to reduce the uncertainty of prior results. It is observed that the BN model can use evidence from an intrusion scenario to update successful intrusion probabilities in other intrusion scenarios. With limited evidence, a BN model could capture the changes of successful intrusion probabilities and security potentials of barriers to produce more reliable information for security management.

In future work, real-life information will be collected by interviewing related experts (e.g., security managers of chemical plants), and a real case will be analyzed to verify the model. Also, countermeasures can be proposed to address the weak links within the security system, and their cost and effectiveness could be analyzed.

Acknowledgements

The authors acknowledge the financial support provided by China Scholarship Council (CSC), and the Natural Sciences and Engineering Research Council of Canada (NSERC).

References

[1] Mark Adrian van Staalduinen, Faisal Khan, Veeresh Gadag. SVAPP methodology: A predictive security vulnerability assessment modeling method. 2016, Journal of Loss Prevention in the Process Industries. 43(2016): 397–413

[2] Mark Adrian van Staalduinen, Faisal Khan, Veeresh Gadag, Genserik Reniers. Functional quantitative security risk analysis (QSRA) to assist in protecting critical process infrastructure. Reliability Engineering and System Safety 157 (2017): 23–34

[3] 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 09. 12. 17]

[4] Stephen Snyder. An Iraqi oil refinery that was too important to destroy has just been

destroyed. PRI's The World. Available at: http://www.pri.org/stories/2015-05-27/iraqi-oil-refinery-was-too-important-destroy-has-just-been-destroyed. [Accessed 09. 12. 17]

[5] Mark van Staalduinen, Faisal Khan. A barrier based methodology to assess site security risk. In: Proceedings of SPE E&P health, safety, security, and environmental conference. Denver, USA (2015): 1－25.

[6] Algerian gas plant hit by rocket attack. ALJAZEERA. Available at: < http://www.aljazeera.com/news/2016/03/algerian-gas-plant-hit-rocket-attack-160318102631104.html>. [Accessed 09. 12. 17]

[7] French minister says double plant blast was criminal act. cnsnews. Available at: < https://www.cnsnews.com/news/article/french-minister-says-double-plant-blast-was-criminal-act >. [Accessed 09. 12. 17]

[8] Simon Henderson. Al-Qaeda Attack on Abqaiq: The Vulnerability of Saudi Oil. The Washington Institute. Available at: < http://www.washingtoninstitute.org/policy-analysis/view/al-qaeda-attack-on-abqaiq-the-vulnerability-of-saudi-oil>. [Accessed 09. 12. 17]

[9] Ayman Al-Warfalli, Patrick Markey and Aidan Lewis. Islamic State fighters target Libya's main oil terminals. Reuters. Available at: < http://www.reuters.com/article/us-libya-security-port-idUSKBN0UI18D20160104>. [Accessed 09. 12. 17]

[10] Ghassan Adnan and Asa Fitch. Islamic State Attacks Iraqi Gas Plant. The Wall Street Journal. Available at: < https://www.wsj.com/articles/islamic-state-attacks-

iraqi-gas-plant-1463313986>. [Accessed 09. 12. 17]

[11] Shailendra Bajpai, J.P. Gupta. Site security for chemical process industries. Journal of Loss Prevention in the Process Industries 18 (2005) 301–309

[12] Union of Concerned Scientists. Available at: < http://www.ucsusa.org/nuclear-power/nuclear-plant-security#.WUloF2eGOL6>. [Accessed 09. 12. 17]

[13] Genserik Reniers, Paul Van Lerberghe, and Coen Van Gulijk. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Safety Progress 34 (2015) 72－83

[14] Francesca Argenti, Gabriele Landucci, Valerio Cozzani, Genserik Reniers. A study on the performance assessment of anti-terrorism physical protection systems in chemical plants. Safety Science 94 (2017) 181–196

[15] Gabriele Landucci, Genserik Reniers, Valerio Cozzani, Ernesto Salzano. Vulnerability of industrial facilities to attacks with improvised explosive devices aimed at triggering domino scenarios. Reliability Engineering and System Safety 143 (2015) 53–62

[16] Ilker Akgun, Ahmet Kandakoglu, Ahmet Fahri Ozok. Fuzzy integrated vulnerability assessment model for critical facilities in combating the terrorism. Expert Systems with Applications 37 (2010) 3561–3573

[17] Francesca Argenti, Gabriele Landucci, Genserik Reniers, Valerio Cozzani. Vulnerability Assessment of Chemical Facilities to Intentional Attacks based on Bayesian Network. Reliability Engineering and System Safety 169 (2018) 515－

530.

[18] Donya Fakhravar, Nima Khakzad, Genserik Reniers,Valerio Cozzani. Security vulnerability assessment of gas pipelines using Discrete-time Bayesian network. Process Safety and Environmental Protection (2017) 714–725

[19] W. L. McGill and B. M. Ayyub, Multicriteria security system performance assessment using fuzzy logic. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology 4 (2007) 356－376,

[20] Wood C., Banks W.. Human error: An overlooked but significant information security. Computers & Security 12 (1993) 51－60.

[21] RAND Corporation. RAND Database of Worldwide Terrorism Incidents. Available at: <https://www.rand.org/nsrd/projects/terrorism-incidents/ download. html>. [Accessed 09. 12. 17]

[22] Joby Warrick. Use of weaponized drones by ISIS spurs terrorism fears. The Washington Post. Available at: < https://www.washingtonpost.com/world/ national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/ 02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?utm_term=.ddc9604 19cd2>. [Accessed 09. 12. 17]

[23] CBC news. Algeria gas plant attack. http://www.cbc.ca/news2/interactives/algeria-gas-plant-attack/#igImgId_73604. [Accessed 09. 12. 17]

[24] Tatsuya Nakagawa. How Secure is Your Storage Tank? Castagra Official website. Available at: < http://www.castagra.com/2013/08/how-secure-is-your-storage-

tank>. [Accessed 09. 12. 17]

[25] Bubbico R, Mazzarotta B.. Security risk assessment of process plants: The role of layout. IEEE. 2014.

[26] Qureshi, Z.. A review of accident modelling approaches for complex socio-technical systems. In: Proceedings of the Twelfth Australian Workshop on Safety Critical Systems and Software and Safety-Related Programmable Systems. Australian Computer Society, Inc. (2007) 47–59.

[27] Guozheng Song, Faisal Khan, Hangzhou Wang, Shelly Leighton, Zhi Yuan, Hanwen Liu. Dynamic occupational risk model for offshore operations in harsh environments. Reliability Engineering and System Safety. 150 (2016) 58–64

[28] Yuan Z, Khakzad N, Khan F, Amyotte P. Risk analysis of dust explosion scenarios using Bayesian networks. Risk Anal 35 (2015) 278–291

5. Probabilistic Assessment of Integrated Safety and Security Related Abnormal Events: A Case of Chemical Plants

Preface

A version of this chapter has been submitted to the Journal of Safety Science. As the primary author, I reviewed related literatures, developed the models and conducted the case study. I completed the manuscript and revised following the feedbacks of Dr. Faisal Khan. Dr. Faisal Khan helped to decide the research topic and provided suggestions for manuscript improvement. Dr. Ming Yang reviewed the manuscript and helped to revise.

Abstract

Conventional risk assessment of chemical plants considers process accident related causal factors. In the current geopolitical situation, chemical plants have become the target of terrorism attacks, making security concerns as important as safety. To protect the public and environment from undue risks, security related causal factors need to be considered as part of the risk analysis of chemical plants. This paper presents an integrated approach to dynamically assess the occurrence probability of abnormal events. The abnormal event is a state of a process plant arrived either due to a process accident or an intentional (terrorist) threat. This approach considers both safety and security related risk factors in a unified framework. A Bayesian network is used to model specific evolution scenarios of process accidents directly initiated from security related factors and the interaction of causal factors. This model enables to dynamically

analyze the occurrence probabilities of abnormal events and causal factors given evidence; it could also capture the impacts of interaction among safety and security related causal factors on these occurrence probabilities. The proposed approach is applied to an oil storage tank to demonstrate its applicability and effectiveness. It is observed that the effect of dependency between correlative accidental and security related factors significantly change the occurrence probability of abnormal events in dynamical assessment.

Keywords: Safety & security; Interaction effect; Integrated assessment model; Dynamic assessment; Bayesian network

5.1 Introduction

Probabilistic analysis helps generate a risk profile, which supports decision making in chemical process design and operation. Such analysis is essential for chemical plants where large inventories of hazardous materials pose the potential of fires, explosions, or the leak of toxic gases [1]. The high-pressure and high-temperature operational conditions of chemical plants tend to exacerbate the consequences of chemical process accidents [1－3]. For this reason, much research has been presented to analyze the accidental risks of chemical plants [4]. However, these methods only consider accidental causes and ignore the intentional threat [5, 6]. The 9/11 attack causing 2996 deaths called people's attention to security [7]. The past years have seen terrorists using chemical plants as targets. Van Staalduinen et al. have listed some attacks on chemical

plants which have occurred in recent years [6, 8]. Besides their listed ones, more attacks have occurred. A chemical plant explosion caused intentionally by a delivery person in France in 2015 resulted in one death and two injuries [9]. Also, suspected Basque separatists detonated bombs at two chemical plants in Spain in 2005, resulting in injuries from toxic fume inhalation [10]. In 2015, Islamic State militants detonated explosives and set fire to the key infrastructure in Iraq's largest refinery in Baiji [11] which once produced 300,000 barrels of refined petroleum products per day, meeting 50 percent of the country's needs [12]. The attacks closed the plant for several years [11]. These attacks indicate that chemical plants are becoming attractive targets for terrorists these days. In such a situation, even if the accidental process risks are reduced to an extremely low level, the plants could still be exposed to high risks due to the vulnerability of chemical plants. Thus, security related causal factors should not be ignored in the risk assessment system.

In this study, the abnormal event is a state of a process plant arrived either due to a process accident or an intentional (terrorist) threat. Two paths can lead to the occurrence of abnormal events in chemical plants, as shown in Fig. 5.1. The first path has been much studied [4, 5], while the second path needs increasing attention considering the increasing occurrence of terrorist attacks across the world. Some research was undertaken to conduct a security analysis. Bajpai proposed an analysis method of security risk in which a security risk factor table and rankings were applied to determine

security risk status [13]. Van Staalduinen et al. have used the sequential barrier approach to explain the attack process, and fault trees (FTs) and event trees (ETs) have been used to calculate the probabilities of barrier failure and consequence occurrence [6]. Then FTs and ETs were converted into Bayesian networks (BNs) to better reflect reality using the Noisy-AND technique and to dynamically update the probability considering the dependency. In another paper [14], Van Staalduinen et al. conducted both threat and vulnerability assessments concurrently rather than sequentially using BNs. After the risk was assessed, potential countermeasures were proposed and a cost analysis of the countermeasures was completed to decide the optimal solution. Khalil has proposed a probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures [15]. He assumed the time for attackers to compromise specific security layers follows distributions. For each attack trial, the Monte-Carlo method is used to sample the time to compromise the security layer and the time is compared with the estimated mission time. If the attacker can successfully compromise his high-value targets and realized his malicious intent within the estimated mission time, the attack is considered as successful. With numerous attack trial simulations, the probability of successful attack was obtained. Feng et al. have used a game-theoretic method considering the strategic interactions between defenders and attackers to optimize the allocation of defensive resources [16]. Zhang et al. applied game theory for security management. They explored pure and mixed strategies in an illustrative case. [17] In another work, Zhang et al. proposed a game theoretic model (Interval CPP Game) to

deal with the defender's distribution-free uncertainties on the attacker's parameters. [18] McGill et al. [19] proposed a model for assessing system vulnerability given an initiating event based on the subjective evaluation of several security effectiveness or defensive criteria. The approach is "model-free" with fuzzy logic techniques, enabling quick implementation given sufficiently trained security experts. In another work [20], McGill et al. developed a quantitative risk assessment and management framework supporting strategic asset-level security resource allocation decision for critical infrastructure and key resource protection with quantitative benefit-cost analysis. This work provided an in-depth development of an asset-driven risk analysis focusing on security threats. Florentine et al. [21] developed a security risk analysis methodology for meat supply. Bayes theorem was applied to assess the likelihood of terrorist attack by analyzing the observables. The application of Bayesian equation provides an option to deal with the issues of credibility of the information source and help update the likelihood of an attack. Haimes et al. [22] developed a modeling roadmap for strategic responses to terrorism risks of water systems. In this roadmap, state variables reflecting the state of security risks were identified from three major systems — geopolitical environment, terrorism networks and the homeland. These previous works make corresponding contributions to the security risk analysis, but they did not consider accidental factors. As argued in [23], safety and security issues are supposed to be considered together, not only because they concern the same systems in an increasing number of sectors, but also because they have strong interconnections which need

consideration [23]. Safety factors interact with security factors; thus, their states could change vulnerability and further influence the real intentional risks confronted by chemical plants. Above works do not include safety factors, thus some uncertainty could be introduced to their assessment results.

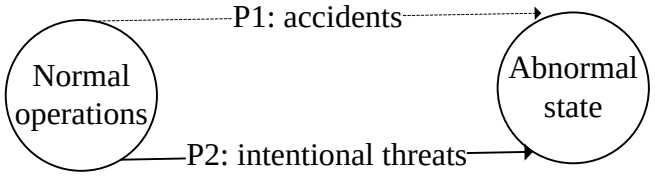


Fig. 5.1 Basic damage pathways in chemical plants

Limited efforts have explored the integrated risks of process accidents and intentional threats. Reniers et al. have developed a security risk assessment and protection methodology which combined the rings-of-protection approach with generic security practices [24]. The authors have briefly described the interaction of safety and security [24], but they have not further quantitatively studied the interaction. Aven has argued that intentional threats need to be included in risk assessment and proposed a unified framework for safety and security [5]. However, this framework only describes a general conceptual procedure for assessing either safety or security risk. The interaction of safety and security has not been studied to obtain integrated risks. Ayyub et al. [25] developed a common quantitative framework accommodating both natural and human-caused hazards for critical asset and portfolio risk analysis to support the cost-effective decision making of risk reduction. This framework could assess risks of natural and intentional hazards. Although this work includes two types of hazards (natural hazard

and intentional hazards), it only considered the dependencies of different assets within a portfolio instead of dependencies of different hazards, and this work does not include process accidents in the safety perspective. Moreover, this work uses equations to calculate risks, thus the accident evolution process and relationships between factors are not visual. Furthermore, the proposed model could not backward update the probabilities of causal factors. Thus, it cannot infer the latest situation of causal factors to guide the risk reduction given different situation (e.g., observing the occurrence of an abnormal event). Fovino et al. have integrated attack trees (ATs) into a pre-existent FT to include potential malicious attacks in the risk analysis [26]. However, they only studied cyber-security, without considering physical attacks. Furthermore, they assumed that the goal of the sub-attack-tree is the causal event of the FT, without considering the scenario that accidental factors can also affect security. Also, they only considered the scenario where attacks destroyed the safety system (e.g., remote shutdown system), making it failed to prevent an accidental initiation. However, they did not consider the specific scenario where an (unintentional) process accident is directly initiated from a poor security factor. Moreover, FTs and ATs used in that work cannot clearly reflect the dependencies of causal factors, and are not capable of updating the predicted probabilities given new information due to their static structures. Pietre-Cambacedes et al. have used Boolean logic Driven Markov Processes (BDMP) to model safety and security interdependencies in critical systems [23]. However, this work did not explore the capacity of dynamical assessment given evidence, and did not include

the scenario where process accidents directly initiate from security related factors. Moreover, this research focus on facility failure related to poor accidental and intentional factors, without considering the intrusion process of attackers. Intrusion prevention is the major strategy to control security risk. Without including the intrusion analysis, the assessment results cannot reflect the real intentional risk. Furthermore, the BDMP model has its limitations as explained by the authors. [23] The situations appropriate for the native Markovian framework of BDMP are limited [23]; the ability of BDMP to conduct sensitivity analysis of different factors is not well established [23]. According to above literature review, the works dealing with both safety and security risks are limited. To the authors' knowledge, no research has conducted a dynamic integrated risk assessment considering the interaction of safety and security with a robust model.

This paper presents a new approach for establishing an integrated dynamic model to help analyze integrated accidental and intentional process risks confronted by chemical plants considering the interaction of safety and security related factors. This work has the following features: (1) the proposed model simultaneously considers accidental and security related causal factors and quantitatively represents their interactions. Thus, it reflects the real-life condition of the correlative causal factors and assists in quantifying the impact of interactions on the occurrence probabilities of causal factors and end events. (2) this model includes the security related factors existing in the intrusion process to conduct a complete probability assessment of abnormal events. (3) this

Bayesian-network-based model could visually represent the relationships between correlative accidental and security related factors, thus it enables to clearly show the specific process accident evolution path directly initiated from security related factors. (4) because the inclusion of safety and security interaction, this model could reflect the real significance of causal factors with sensitivity analysis. (5) this model has dynamic feature and thus it could update the states of abnormal events and causal factors given evidence, especially enables to update states of both types of factors (i.e., accidental and security related factors) given evidence of one type of factors. This dynamic feature not only helps managers learn the latest situation of abnormal events and causal factors, but also assists to reduce the uncertainty caused by scarce data of security issues. Bayesian network has been used to analyze process accidents, occupational accidents and security issues [27－32], but to the best of our knowledge, no work is conducted using BN to exploit the interaction of safety and security. A comparison of current method and previous work described above is shown in Table 5.1. A novel point of this research is the consideration of both safety and security related risk factors in a robust framework, and the quantitatively dynamical analysis of impacts of interactions between safety and security. Note that this research focuses on physical abnormal events related to a chemical plant. It does not consider external threats related to cyber attack, war or other causes.

Table 5.1 Comparison of the current method and related previous work

Methods	Quantitative analysis of impacts of the interaction of safety and security	Dynamic probability assessment using evidence	Visually show the specific accident evolution directly initiated from a poor security factor	Inclusion of physical intrusion process
Bajpai [13]				√
Van Staalduinen [6]		√		√
Van Staalduinen [14]		√		√
Khalil [15]				√
Feng [16]				√
Zhang [17-18]				√
McGill [19]				√
McGill [20]				√
Florentine [21]		√		
Haimes [22]				√
Reniers [24]				√
Aven [5]				√
Ayyub [25]				√
Fovino [26]	√			
Pietre-Cambacedes [23]	√			
Current method	√	√	√	√

This paper is organized as follows: Section 5.2 explains the approach to establish the integrated dynamic model. In Section 5.3, a case study on the probability assessment of an oil storage tank fire is conducted to demonstrate the proposed approach. Section 5.4 presents the conclusions.

5.2 The proposed integrated dynamic probability assessment approach

The approach to obtain the integrated dynamic probability assessment model is shown in Fig. 5.2. FTs are established first and then are converted to BN. After involving the dependency caused by common factors and correlative accidental and security related factors in the BN, the integrated dynamic model is obtained. The detailed process is demonstrated in the following subsections and the schematic diagrams of the FT and BNs are shown in Fig. 5.3 to facilitate the clarification of the approach.

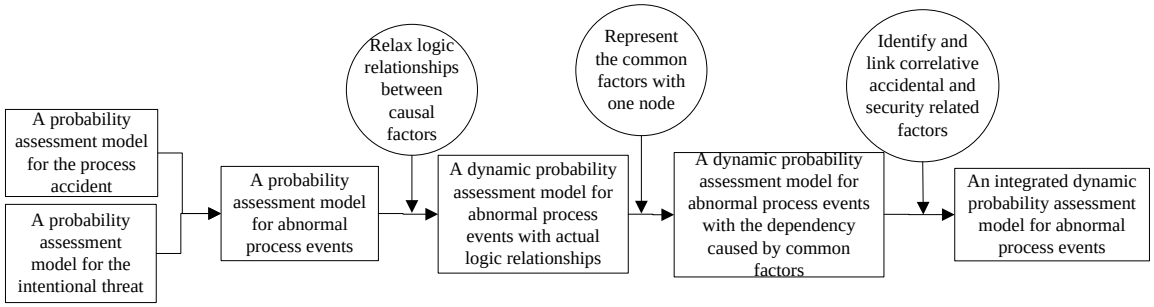
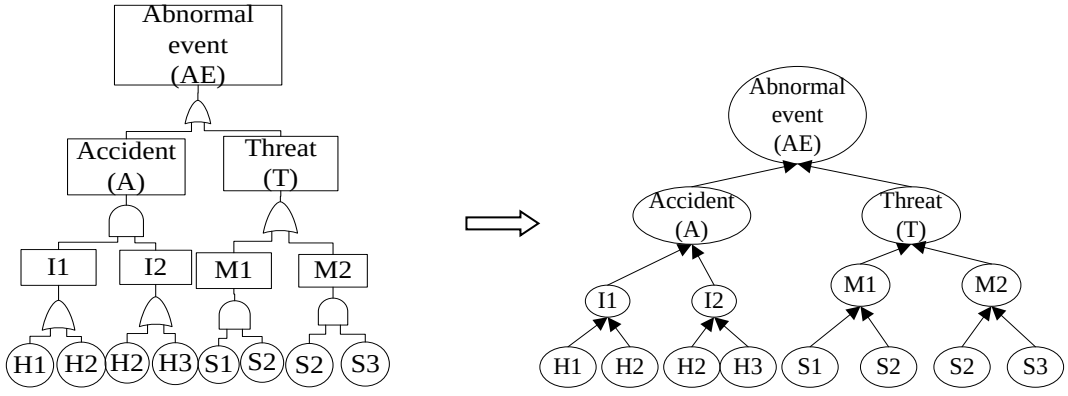
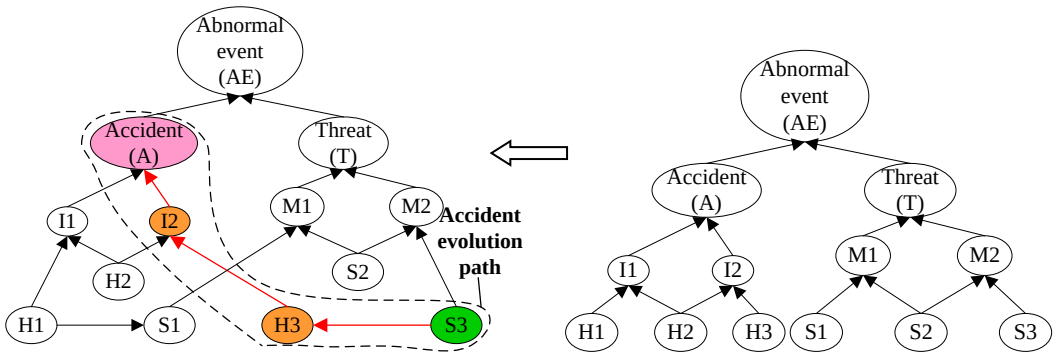


Fig. 5.2 The approach to obtain the integrated dynamic probability assessment model



(a) Schematic FT for the abnormal event **(b) Schematic BN for the abnormal event**



(d) Schematic integrated BN model (c) Schematic BN with dependence caused by common factors

Fig. 5.3 Schematic diagrams of the FT and BNs

5.2.1 FT establishment for integrated probability assessment and its limitation relaxation

Many accidental and security related factors needs to be considered to predict the probability of an abnormal event. FT is an appropriate tool to deal with large numbers of causal factors, and thus it is applied to identify causal factors and clarify their relationships in the proposed approach. First, the process accident and intentional threat are respectively analyzed with FTs and then the two FTs are combined using an OR gate. In this way, the FT of the abnormal event is obtained and its schematic diagram is shown in Fig. 5.3(a). However, as discussed in [29], the logic gates of the FT have limitations to express the actual logic relationships. Furthermore, FTs have static structures and thus they could not conduct dynamic assessment. To accurately represent the logic relationships of causal factors [29] and to obtain the dynamic feature, the schematic FT in Fig. 5.3(a)) is converted to BN (Fig. 5.3(b)) following the procedure mentioned in [33]. The BN in Fig. 5.3 (b) not only represents the NOISY-OR and

NOISY-AND logic gates with conditional probability tables (CPTs) [29], but also enables assessment in a dynamic manner [33].

5.2.2 The involvement of dependence caused by the common factors

Some basic events (e.g., H2 and S2) contribute to various intermediate events, which leads to dependency. The probability calculation of BN in Fig. 5.3(b) cannot involve such dependency. The dependence caused by the common factor H2 can change the probability of a process accident P(A), while the dependence caused by the common factor S2 changes that of an intentional threat P(T). Consequently, the probability of the abnormal event P(AE) is changed by these common factors. The principle related to how the common factor H2 changes P(A) is as follows:

$$P(A)=P(I_1I_2)*P(A|I_1I_2)+P(I_1'I_2)*P(A|I_1'I_2)+P(I_1I_2')*P(A|I_1I_2')+P(I_1'I_2')*P(A|I_1'I_2') \quad (5.1)$$

Since I_1 and I_2 are considered as independent in the BN of Fig. 5.3(b), equation (5.1) can be converted to equation (5.2).

$$\begin{aligned}P(A) &= P(I_1)*P(I_2)*P(A|I_1I_2)+P(I_1')*P(I_2)*P(A|I_1'I_2)+P(I_1)*P(I_2')*P(A|I_1I_2') \\ &+P(I_1')*P(I_2')*P(A|I_1'I_2')\end{aligned} \quad (5.2)$$

However, since H_2 simultaneously contributes to I_1 and I_2, I_1 and I_2 are not independent in practice. This means that $P(I_1I_2)\neq P(I_1)*P(I_2)$ and the result from equation (5.1) does not equal that from equation (5.2). The BN in Fig. 5.3(b) assumes

the independence of I_1 and I_2, which introduces uncertainty when the occurrence probability of the process accident is assessed.

Another drawback of the model in Fig. 5.3(b) is that the common factors are represented separately, thus the common factor (e.g., H_2) may have various posterior probabilities, when the probability of the common factors is updated with the evidence of the occurrence of an abnormal event. However, one causal factor obviously has only one occurrence probability in practice.

To overcome these drawbacks, the common variable needs to be represented with one node in the BN. This not only makes the probability assessment of abnormal events more accurate, but also ensures that one common variable has one posterior value. Thus, the nodes of the common factors in Fig. 5.3(b) are combined to one and the BN considering dependence from common factors is obtained, as shown in Fig. 5.3(c). The occurrence probabilities of the process accident, intentional threat and abnormal event can be calculated respectively according to Fig. 5.3(c). However, the calculation assumes that accidental factors and security related factors do not interact, which is not the case in practice.

5.2.3 Link the correlative accidental and security related factors

By linking the correlative accidental and security related factors of Fig. 5.3(c), the integrated dynamic model is obtained as Fig. 5.3(d). The major reason to study security

and safety in an integrated framework is that the security related factor may influence the accidental factor and vice versa. Because of this, the correlative security related factors can be treated as causal factors of the process accident. If the influence of security related factors on the process accident is not considered, it seems that the causal factors of the process accident are not completely involved. Moreover, if the security related factors are not considered, the state of the correlative accidental factors cannot be specified. Furthermore, process accident evolution path directly initiated from poor security factors could not be identified without considering accidental and security related factors in one framework, which will affect the intervention design. These points are explained through Fig. 5.3(c) and Fig. 5.3(d). In Fig. 5.3, it is assumed S_3 is the security related factor 'lax entry control'; H_3 is the accidental factor 'the lack of professional knowledge'; and I_2 is the accidental factor 'human errors'. As an initiating event, the security related factor 'lax entry control' contributes to 'the lack of professional knowledge' and causes 'human errors', because the chemical plant becomes more accessible to non-employees (e.g., staff's children) when chemical plants have lax entry control. These people may not intend to cause damage in the plant, but they have a high likelihood to cause process accidents due to the lack of required professional knowledge. If the security perspective is not considered while analyzing the probability of the process accident, lax entry control will not be included, and thus the causal factors for the process accident are not complete. This will affect the accuracy of probability prediction of the process accident. Furthermore, in Fig. 5.3(c), managers

may estimate the probability of human error considering accidental factors (e.g., experience related factors). However, practically, human error is also influenced by entry control, as shown in Fig. 5.3(d). For instance, the probability of human error could be 0.1 [34, 35] given good entry control, while its probability may increase to 0.2 given poor entry control. Human error likelihood changes with entry control, and without consideration of the state of the entry control, the probability of human error may not be specified. Moreover, Fig. 5.3(d) reveals the specific process accident evolution path that lax entry control (initiation) is propagated through accidental factors (lacking professional knowledge and human errors), and terminates as process accidents. This is consistent with the process accident in a practical case. In 1998 in Iowa, two teens driving a vehicle approached and destroyed the pipeline by accident and caused a tank explosion, killing two volunteer fire fighters and injuring seven more. The cause was that no fence existed for aboveground propane pipes and tanks [36]. Through above analysis, it can be clearly seen that both accidental and security related causal factors should be considered in an integrated framework to accurately predict the probability of process accidents and effectively design the intervention. With the integrated framework, the impact of each factor could be better reflected. For example, some security related factors such as lax entry control exacerbate both safety and security. The probability growth of such factors can increase both the probabilities of intentional threats and process accidents. Thus, the probability increase of the abnormal event from the integrated dynamic model will be greater than that from Fig. 5.3(c), given the

probability growth of such factors. Sometimes the security related factor may have opposite effects on safety and security, which means it improves safety but exacerbates security or exacerbates safety but improves security. For such factors, only improving their states may not effectively reduce the integrated probabilities of abnormal events. A potential way to deal with these factors is to change their form and remove their contradictory effects, which will be explained in section 5.3.2.2.2.

Another advantage of considering accidental and security related causal factors in an integrated framework is that the observation of a factor could be used to update the probabilities of accidental and security related factors at the same time. In this way, the latest states of both accidental factors and security related factors are obtained from the integrated dynamic model. Consequently, the poor factors can be detected from both safety and security perspectives to help prevent abnormal events.

Through the established models in this paper, the calculation and update results from the models with and without considering the interaction can be compared to quantitatively study the influences of interaction on the probabilities of abnormal events and causal factors. Furthermore, with sensitivity analysis of causal factors on an abnormal event, the correlative causal factors' significance can be identified. The difference between the correlative causal factors' significance obtained with and without the involvement of interaction is studied.

5.3 Case study

The occurrence probability of an oil storage tank fire was analyzed to demonstrate the strength of the integrated dynamic probability assessment model. For the sake of clear demonstration of effects of interaction between safety and security related factors, some simplification is made. The attractiveness and vulnerability altogether influence the occurrence probability of intentional events. Attractiveness could be assessed based on factors like deterrence and visibility [20] and previous work has conducted attractiveness analysis [37]. This case study did not deal with attractiveness assessment and it assumed the storage tank farm is in an area with an attack probability 0.1. Furthermore, attack types (e.g., explosive born vehicle or creep in without guns) could also influence the occurrence probabilities of intentional events [19]. In this case study, the attack type is creeping in without guns, and the influence of different attack types could be included in future work. With this simplification, the considered security factors in this case study are those related to vulnerability.

5.3.1 The establishment of the integrated dynamic probability assessment model

To analyze the probability of an oil storage tank fire, an FT is used first to identify the accidental and security related factors and to determine their logic relationships. The basic events (see Table 5.2) and the intermediate events (see Table 5.3) are identified referring to [24, 38, 39] and the prior probabilities of basic events are assumed partly based on previous literature [30－32]. Then, as mentioned in Section 5.2, the FT is converted to a BN, shown in Fig. 5.4(a). After combining the common factor into one

node, the model becomes the form of Fig. 5.4(b). Then the relationships between the accidental and security related factors are identified and correlative factors are linked to obtain the integrated dynamic model shown in Fig. 5.4(c). As indicated with red arrows in Fig. 5.4(c), a process accident evolution path directly initiating from a security related factor and terminating with a process accident is demonstrated. Along the path, the termination (accidental oil storage tank fire TE1) initiates from X_{52}, and propagates through IE_{32}, X_{20}, IE_{10}, IE_{9}, IE_{27} and IE_{23}. The practical meaning of this evolution path is that guards with poor ability create a chance for non-employees to enter chemical plants, and these untrained people trigger human errors which causes an oil leak and further propagates to become an oil fire. According to this evolution process, two types of countermeasures can be proposed for different stages of the process accident evolution. The first is to prevent the initiation occurrence (e.g., hiring guards with good security skills), and the second option is to block the propagation (e.g., applying safety devices to prevent accidents given human errors).

Table 5.2 Basic events and their prior probabilities [24, 30 − 32, 38, 39]

Symbols	Details of the activity/event or state	Prior probability
X1	No level measurement device	6.70E-02
X2	Failure of level measurement device	1.40E-04
X3	No overflow alarm	4.50E-02
X4	Failure of overflow alarms	9.80E-02
X5	Failure of worker to monitor level	1.25E-01
X6	No level control device	1.45E-01
X7	Failure of level control device	2.52E-03
X8	No routine inspection	1.00E-02

X9	No proper maintenance	1.00E-02
X10	Aging	1.00E-02
X11	Corrosion	7.80E-03
X12	Fatigue	1.00E-01
X13	Material deficiency	1.58E-03
X14	Installation deficiency	5.61E-03
X15	Manufacture deficiency	2.12E-03
X16	Design deficiency	4.00E-02
X17	Earthquake	1.30E-04
X18	Subsidence of foundation	3.40E-02
X19	High pressure liquid backing up from downstream vessels	2.30E-04
X20	Lack of knowledge of operations on site	1.00E-01
X21	Not following operational procedures on site	1.00E-03
X22	Lack of knowledge of remote operations	2.58E-01
X23	Not following dress regulations	1.50E-01
X24	No effective elimination of static	1.00E-02
X25	Static occurrence in equipment operation (e.g., transfer and improper sampling procedures)	4.50E-02
X26	Failure of anti-static measures like grounding of equipment	5.50E-02
X27	Poor signs to help operations and remind of potential hazards	1.20E-01
X28	Non-explosion-proof motor and tools used	3.00E-04
X29	Short Circuit	5.00E-02
X30	Mechanical frictions	6.00E-02
X31	Poor safety awareness	2.68E-02
X32	Not following open fire rules	5.00E-02
X33	Poor monitoring of potential hazardous acts	3.00E-03
X34	No warning sign for open fire	1.00E-02
X35	Spark caused by operations like welding and hitting	2.00E-01
X36	Checking without blind flange	6.00E-03
X37	Hot operation not following procedure	4.50E-02
X38	Lightning	1.00E-06
X39	No lightning arresters	3.00E-05
X40	Improperly placed lightning arresters	1.50E-04
X41	Poor grounding of tanks	2.60E-04
X42	Rim seal leak	6.00E-02
X43	Exothemic runaway reactions	8.90E-04
X44	Heat accumulation to fire point	2.18E-01

X45	Failure of alarm of combustible gas concentration	4.28E-02
X46	Workers do not respond following procedure	1.03E-01
X47	Get keys from staff	1.41E-02
X48	Skills to directly open locks without keys	3.51E-02
X49	Destroy locks using tools like shears	1.53E-01
X50	No effective hindering facility	1.21E-03
X51	Poor security awareness of guard	8.00E-03
X52	Poor ability of guards	1.62E-02
X53	Poor security knowledge of guard	1.42E-03
X54	Bride guard	1.26E-03
X55	Fake identity	1.62E-02
X56	Accidentally destroyed	1.93E-02
X57	Destroyed by attackers	2.51E-01
X58	Insufficient wall height	3.26E-03
X59	No barbed wire on top	2.16E-02
X60	Not following procedures for remote operations	1.00E-03
X61	No receptionist on duty	2.58E-02
X62	Receptionist is controlled by attackers	2.53E-01
X63	No security alarm	5.86E-02
X64	Improperly placed security alarms	1.26E-01
X65	Poor quality of security alarm system	4.32E-02
X66	Poor inspection of security alarm system	2.13E-02
X67	Poor maintenance of security alarm system	2.48E-02
X68	Location of security alarm accessible to attackers	2.14E-01
X69	Attackers are familiar with security alarm system	2.43E-02
X70	No video surveillance	3.54E-02
X71	Improperly placed video surveillance	1.98E-02
X72	Staff in charge of video surveillance does not observe in time	2.02E-01
X73	Poor quality of video surveillance system	1.21E-02
X74	Poor inspection of video surveillance system	2.13E-02
X75	Poor maintenance of video surveillance system	1.28E-02
X76	Location of video surveillance system accessible to attackers	1.04E-01
X77	Attackers are familiar with video surveillance system	4.15E-02
X78	Insufficient frequency of patrol	1.26E-03

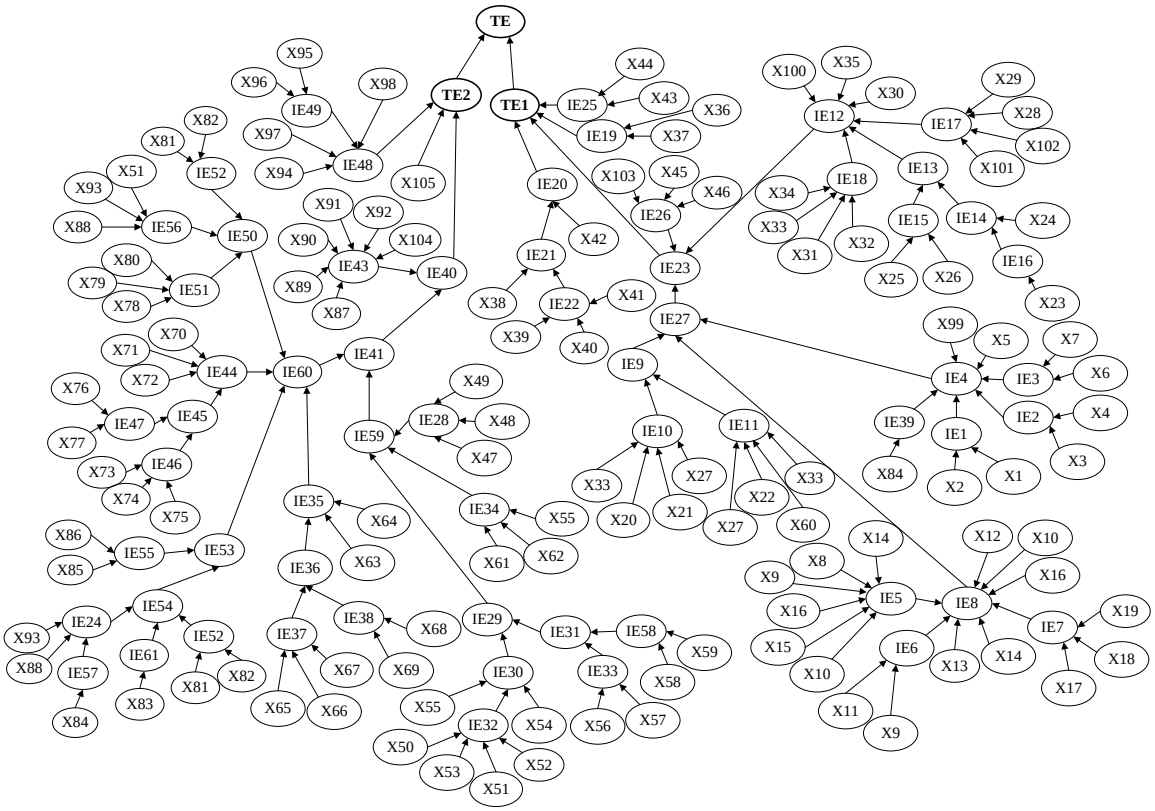
X79	Improper patrol route	2.54E-03
X80	Attackers know the patrol schedule	4.30E-04
X81	Dark circumstances	3.05E-02
X82	Too many obstacles	8.63E-03
X83	Attackers know the work time and area	1.23E-01
X84	Poor education	5.00E-02
X85	Poor reporting regulations	4.72E-02
X86	Poor reporting education	5.00E-02
X87	Destroy pumps	1.02E-01
X88	Attackers have fake badge and work clothes	2.43E-02
X89	Open valves	7.23E-01
X90	Destroy pipes	2.29E-01
X91	Destroy tank body	2.15E-03
X92	Open cover using control button	2.37E-01
X93	Common workers do not have work clothes and badges	6.28E-02
X94	Setting spark by hitting	2.15E-03
X95	Lighter	4.92E-01
X96	Match	4.61E-01
X97	Setting static spark	5.23E-02
X98	Setting electronic spark of equipment	6.85E-02
X99	Loading or transferring oil to storage tank	2.04E-01
X100	Spark from vehicle emission	1.52E-01
X101	Electricity leakage	3.67E-03
X102	Heat caused by overload	2.56E-02
X103	Leak is not observed by workers in time	2.64E-01
X104	Overflow caused by intentional operations	8.00E-02
X105	Attack	1.00E-01

Table 5.3 Intermediate and top events [24, 38, 39]

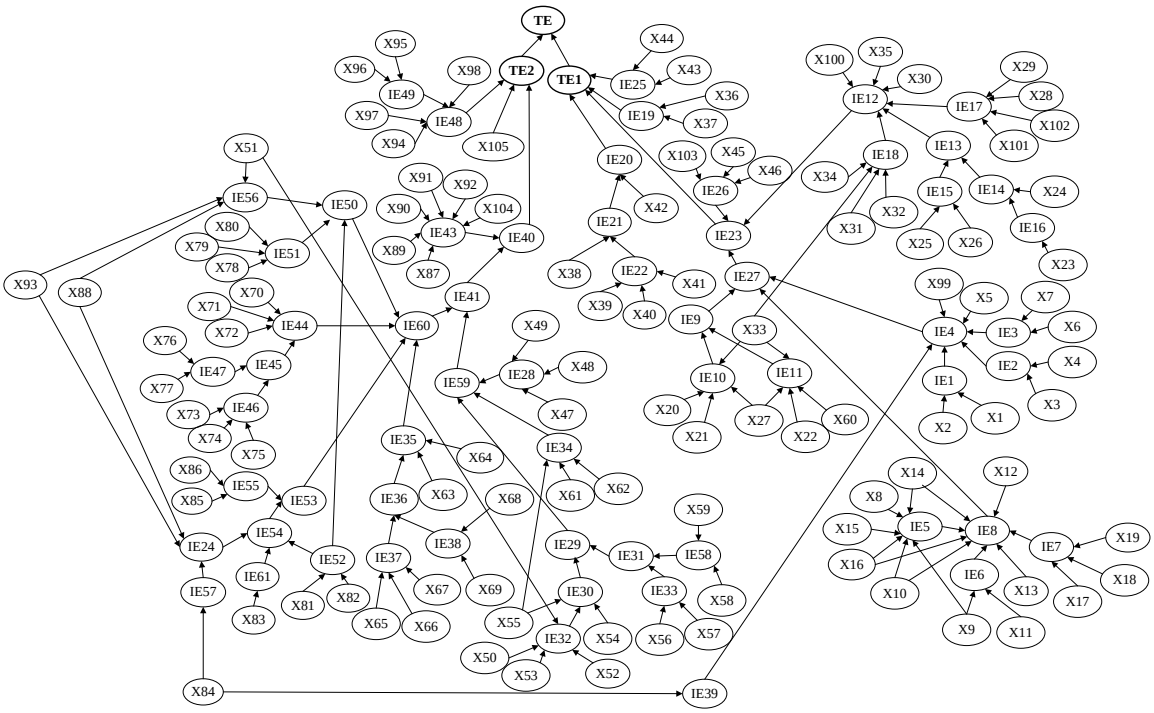
Symbols	Meaning
IE1	No effective level measurement device
IE2	Overflow alarms do not work effectively
IE3	Level control devices do not work effectively
IE4	Overflow
IE5	Valves cannot close
IE6	Corrosion damage
IE7	Too heavy force on the facility
IE8	Facility leak
IE9	Leak caused by unintentional human error
IE10	Human error for operation on site (e.g., valves open accidently on site)

IE11	Human error in remote operations (e.g., press control button to open valves mistakenly)
IE12	Ignition source
IE13	Static spark
IE14	Static from workers
IE15	Static from equipment
IE16	Clothes or shoes generate static
IE17	Spark or heat from electronic equipment
IE18	Open flame caused unintentionally by individuals
IE19	Fire on facility caused by operation against rules (rule-based human error)
IE20	Fire caused by lightning
IE21	Spark resulted from direct stroke or secondary effects (e.g., the bound charge) on tank
IE22	No effective lightning arrester
IE23	Leaked oil on fire
IE24	Workers do not recognize attackers
IE25	Spontanous combustion
IE26	Leak and ignition not managed in time
IE27	Oil leak
IE28	Open or destroyed locks
IE29	Pass fence
IE30	Via entry
IE31	Via wall of wire
IE32	Lax entry control
IE33	Wall destroyed
IE34	Pass receptionist
IE35	Security alarm does not work properly
IE36	Failure of security alarm system
IE37	Natural failure of security alarm system
IE38	Security alarm system destroyed by attackers
IE39	Improper response of workers to overflow alarm
IE40	Success of attackers to access oil
IE41	Intrusion into storage area without being detected
IE43	Destroy facilities (e.g., tank) or intentionally conduct operations to access oil
IE44	Video surveillance does not catch attackers
IE45	Failure of video surveillance system
IE46	Natural failure of video surveillance system
IE47	Video surveillance system destroyed by attackers
IE48	Successfully ignite oil
IE49	Setting open fire

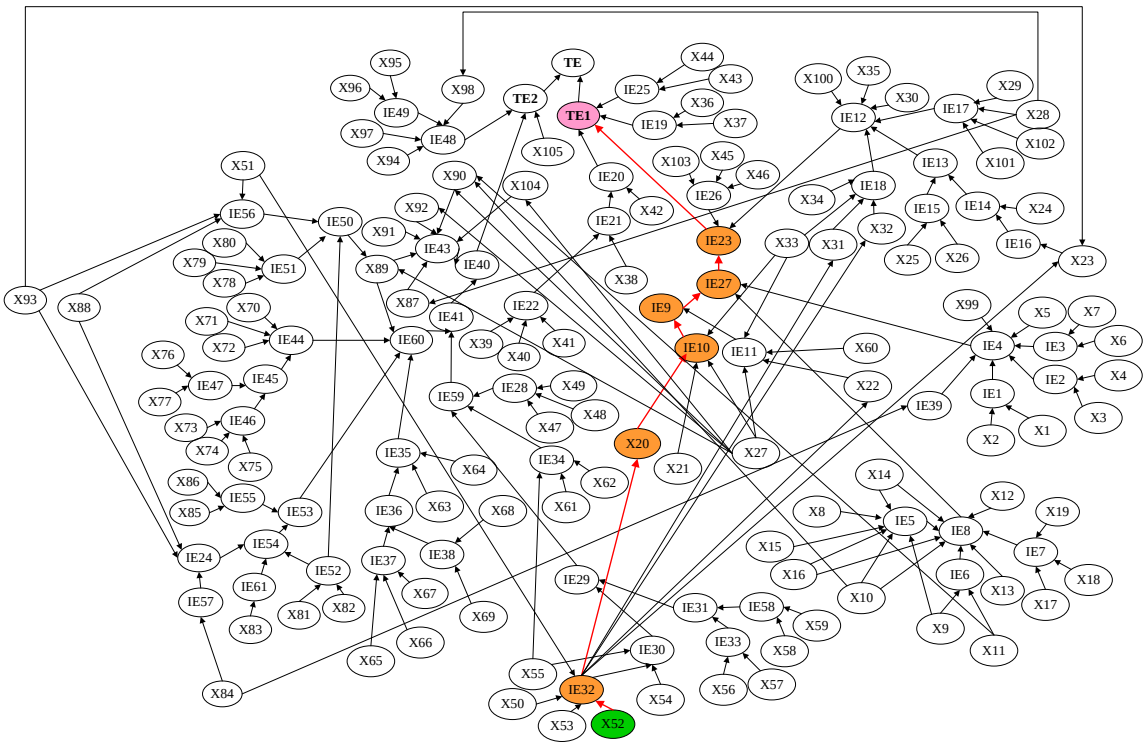
IE50	Patrol does not find attackers
IE51	Patrol does not meet attackers
IE52	Attackers successfully hide
IE53	Workers do not find attackers or incorrectly report the attack
IE54	Workers do not find attackers
IE55	Workers do not correctly report the attack
IE56	Patrol does not recognize attackers
IE57	Poor security awareness of workers
IE58	Poor security of wall
IE59	Go through security defensive line
IE60	Attackers are not detected
IE61	Workers do not meet attackers
TE1	Accidental fire of the oil storage tank
TE2	Intentional fire of the oil storage tank
TE	Fire of the oil storage tank



(a) The BN for oil storage tank fire directly converted from the FT



(b) The BN for oil storage tank fire with dependency caused by common factor



(c) The integrated BN for the oil storage tank fire

Fig. 5.4 The models for oil storage tank fire

5.3.2 Probability analysis with the established BNs

5.3.2.1 Probability calculation and comparison

The probabilities of storage tank fire, accidental storage tank fire and intentional storage tank fire are respectively calculated with the BNs shown in Fig. 5.4, and the results are shown in Table 5.4. Comparing columns 2 and 3 of Table 5.4, the probability of the oil storage tank fire decreases when the common causal factor is treated as one node in the model shown in Fig. 5.4(b). In other words, when the dependence caused by common factors is not considered, the probability of the abnormal event is overestimated. Columns 3 and 4 of Table 5.4 indicate that after considering the dependency among correlative accidental and security related factors, the probability of an accidental storage tank fire increases. This is because the correlative security related factors (e.g., IE_{32}) also serve as causal factors of an accidental storage tank fire and their poor states increase the occurrence probability of the correlative accidental factors (e.g., X_{20}). The model in Fig. 5.4(b) does not consider the correlative security related factors as causal factors of an accidental storage tank fire; thus, the causal factors of accidental fire are not completely involved and its assessment result is underestimated. The probability of intentional storage tank fire decreases, because the accidental factor X_{27} reduces the occurrence likelihood of the poor security related factors (i.e., X_{89}, X_{90}, X_{92} and X_{104}). The increase of the probability of an accidental storage tank fire is much larger than the reduction of its intentional counterpart; thus, the integrated probability of the storage tank fire increases. According to Table 5.4, the dependency caused by common factors

and by interaction among correlative accidental and security related factors can cause the probability changes of abnormal events, although in this case, such changes are minor due to the small occurrence probability of related causal factors. The occurrence of those causal factors can influence safety and security at the same time and thus changes the probability of an abnormal event. However, when their occurrence probabilities are very small, such influences are weak in a static assessment. If the related causal factors are observed in a dynamic assessment, their effects could be more obvious. This point will be further explained in subsection 5.3.2.2.2.

Table 5.4 The probabilities of storage tank fire, accidental storage tank fire and intentional storage tank fire from different BN models

	Results of model in Fig. 5.4(a)	**Results of model in Fig. 5.4(b)**	**Results of the integrated dynamic model**
Probability of storage tank fire	1.7833E-02	1.7429E-02	1.7433E-02
Probability of accidental storage tank fire	1.3991E-02	1.3584E-02	1.3589E-02
Probability of intentional storage tank fire	3.8959E-03	3.8976E-03	3.8972E-03

5.3.2.2 Probability update and comparison

Dynamic assessment is important for effective risk management, since the management measures may need modification with the state change of causal factors and abnormal events over time. Furthermore, the security data is scarce, which causes uncertainty to

the prior probabilities. After updating the prior probability with evidence in a dynamic assessment, the obtained posterior probabilities become more realistic. This integrated dynamic model has more obvious advantages in dynamic assessment.

5.3.2.2.1 The posterior probability calculation of common factors

When the occurrence of an oil storage tank fire is observed as evidence, the integrated dynamic model and BN model of Fig. 5.4(a) are used to update the causal factors. The posterior probability of the common factor X_{33} (poor monitoring of potential hazardous acts) from the integrated dynamic model is 3.44E-03. However, X_{33} has three posterior probabilities (3.04E-03, 3.06E-03 and 3.32E-03) according to the BN model of Fig. 5.4(a). It reveals the integrated dynamic model has the advantage to correctly update the probability of common factors.

5.3.2.2.2 The effects of interaction of correlative causal factors on posterior probability

From columns 3 and 4 of Table 5.4, it is observed that the probability change of storage tank fire caused by the interaction between correlative accidental and security related factors is small. This is because the occurrence likelihood of those correlative factors is small, limiting the influences of their interactions on a storage tank fire. However, when evidence of the correlative factors that exacerbate both safety and security is observed, their influences may significantly change the probability of a storage tank fire. For example, when IE_{32} as 'lax entry control', X_{28} as 'non-explosion-proof motor' and X_{93} as 'common workers do not have work clothes and badges' are observed, the

probabilities of storage tank fire, accidental storage tank fire and intentional storage tank fire from the model of Fig. 5.4(b) and the integrated dynamic model are shown in Table 5.5. Comparing the values between columns 2 and 3 of Table 5.5, all the posterior probabilities of storage tank fire, accidental storage tank fire and intentional storage tank fire from the integrated dynamic model have a much bigger increase than those from Fig. 5.4(b). Among them, the posterior probability of storage tank fire from the integrated dynamic model is 11.3% larger than that from Fig. 5.4(b). This is because the probability growth (from prior probabilities to 100%) of these observed factors can simultaneously increase the probabilities of accidental fire and intentional fire in the integrated dynamic model. However, because of lack of interaction of correlative accidental and security related factors in the model of Fig. 5.4(b), the probability growth of those observed causal factors can only increase the probability of either an accidental or an intentional storage tank fire.

The analysis above shows that, although the interaction between safety and security has little influence on the prior occurrence probability of the abnormal event, when evidence of the factors which simultaneously deteriorate safety and security is observed, the probability of the abnormal event can have big change due to the interaction of safety and security. This reveals the importance of considering the interaction between safety and security while dynamically assessing the occurrence probability of the abnormal event.

Table 5.5 The posterior probability of storage tank fire, accidental and intentional storage tank fire

	Results from model in Fig. 5.4(b)	Results from the integrated dynamic model
Probability of storage tank fire	1.842E-02	2.051E-02
Probability of accidental storage tank fire	1.451E-02	1.635E-02
Probability of intentional storage tank fire	3.973E-03	4.224E-03

Moreover, changes of some causal factors can have opposite effects on changes of accident probability and intentional threat probability. If the dependency between correlative accidental and security related factors is not considered (e.g., the model shown in Fig. 5.4(b)), the effects of such factors cannot be represented. The integrated dynamic model can reflect the effect that when the states of such factors change, the occurrence probabilities of process accidents and intentional threats have opposite changes. Taking X_{27} (poor signs to help operations and remind of potential hazards) as an example, from columns 2 and 3 of Table 5.6, when X_{27} is observed as good signs, the probability of accidental storage tank fire decreases, but that of the intentional storage tank fire increases. Comparing the values in columns 2 and 4, when X_{27} is observed as poor signs, the probability of accidental fire grows, and that of intentional fire decreases. However, no matter how the state of X_{27} changes, it generates either an extra process accident likelihood or an additional threat probability. Fortunately, in this case, the probability reduction of accidental storage tank fire is much bigger than the probability increases of intentional storage tank fire if the state of X_{27} is improved.

However, in some cases, when causal factor states are improved to reduce process accidents, the integrated probability of an abnormal event may increase due to the growth of intentional threat probability. To effectively avoid the conflict effect, the form of such factors needs to be changed. For example, the form of X_{27} can be changed to 'poor guide signs of operations that only staff can read'. In this way, improving X_{27} can help staff operate safely and avoid guiding attackers to destroy facilities.

Table 5.6 The probability comparison of storage tank fire, accidental storage tank fire and intentional storage tank fire given different states of X_{27} from the integrated dynamic model

	X_{27} (No evidence)	**X_{27} (good signs)**	**X_{27} (poor signs)**
Probability of storage tank fire	1.7433E-02	1.7295E-02	1.8443E-02
Probability of accidental storage tank fire	1.3588E-02	1.3450E-02	1.4607E-02
Probability of intentional storage tank fire	3.8972E-03	3.8978E-03	3.8931E-03

Furthermore, the model in Fig. 5.4(b) cannot update security related factors using the evidence of accidental factors, and the observation of security related factors cannot be applied to update accidental factors. This is because the model presented by Fig. 5.4(b) is not capable of modeling the interaction between correlative accidental factors and security related factors. In contrast, the integrated dynamic model can use evidence of either correlative accidental or security related factors to update both correlative accidental factors and security related factors. For example, when the model in Fig. 5.4(b) is updated given the occurrence of the accidental factors X_{20} (Lack of knowledge

of operations on site) and X_{23} (Not following dress regulations), the posterior probability of the security related factor IE_{32} (Lax entry control) is the same as its prior probability. However, when the same evidence is used in the integrated dynamic model, not only can the accidental factors be updated, the posterior probability of the security related factor IE_{32} becomes 1.517E-02, 7.6 times of its prior probability (1.983E-03) as shown in row 2 of Table 5.7. This means when human error occurs on site, and people in the chemical plant do not dress following regulations, the lax entry control is believed to have a bigger occurrence probability. The result from the integrated dynamic model is consistent with practice. In this way, the accidental and security related factors are updated given evidence of accidental factors X_{20} and X_{23}, and then both poor accidental and security related factors can be detected. Similarly, when X_{104} (Overflow caused by intentional operations) is observed, the posterior probabilities of IE_2 (Overflow alarms do not work effectively) and IE_3 (Level control devices do not work effectively) are the same as their prior probabilities based on the model in Fig. 5.4(b). However, their probabilities increase to 2.206E-01 and 4.023E-01 from 1.386E-01 and 1.472E-01 respectively (see rows 3 and 4 of Table 5.7) using the integrated dynamic model. When X_{23} (Not following dress regulations) is observed, the probability of IE_{24} (Workers do not recognize attackers) increases from 2.992E-01 to 3.330E-01 (see row 5 of table 5.7) according to the integrated dynamic model. This means when most employees do not wear work clothes, it is believed workers can hardly detect intruders according to clothing, which lowers the likelihood for workers to recognize attackers.

Table 5.7 The effects of interaction between correlative accidental factors and security related factors in dynamic assessment

Factors	Prior probability	Posterior probability	Evidences
IE_{32}	1.983E-03	1.517E-02	Occurrence of X_{20} & X_{23}
IE_{2}	1.386E-01	2.206E-01	Occurrence of X_{104}
IE_{3}	1.472E-01	4.023E-01	Occurrence of X_{104}
IE_{24}	2.992E-01	3.330E-01	Occurrence of X_{23}

5.3.2.2.3 Significance analysis of correlative factors

The contribution amount of a causal factor to the abnormal event is an important index of this factor's significance, which could guide the decision making of prevention measures. It can be reflected by the probability change of the abnormal event given the occurrence and nonoccurrence of the causal factor. In this section, the contribution amount of correlative accidental and security related factors is calculated to study the effect of their interactions on these factors' significance. For the sake of this study, a critical value of 1.50E-03 was set for the probability change of the abnormal event. When considering the dynamic integrated models, changes of factors X_{10}, X_{20}, X_{22}, X_{31}, X_{32} and IE_{32} (1.82E-03) produced a variation of the abnormal event exceeding the critical value. On the other hand, changes of factors X_{10}, X_{20}, X_{22}, X_{31} and X_{32}, but not IE_{32} (1.11E-05), produced a variation of the abnormal event exceeding the critical value when the model represented by the picture in Fig. 5.4(b) was applied. This is because, when the interaction between safety and security is not considered, IE_{32} is assumed not to influence safety, and the importance of IE_{32} is significantly underestimated. In this way, some important factors could be incorrectly ignored when the prevention resources

are assigned. In comparison, the integrated dynamic model can more accurately reflect the significance of correlative factors, and thus can effectively guide the decisions for prevention measures. For example, according to the result from the integrated dynamic model, IE_{32} (the entry control) needs more resources to be strengthened.

It is worth noting that conditional probabilities of BNs in this case study were assumed, while theoretically these values could be obtained from historical data or expert experiences. However, since the three BNs presented in Fig. 5.4 have the same variables and almost the same conditional probabilities (all the same CPTs for the three models except that the integrated dynamic model has additional ones for the links of correlative accidental and security causal factors), the comparison of their results could reflect the effects of the interaction of safety and security related factors. The case study is for illustration purposes, the results do not mean to directly guide practice. Once data from practice or experts are inputted to the proposed model, it could generate more real results to guide practice.

5.4 Conclusions

This study presented a new approach for modeling accidental and security related factors in an integrated dynamic framework to assess the probabilities of abnormal events. The established model reflected the actual relationship of the correlative causal factors, process accidents, intentional threats and abnormal events, and quantified the effects of the interactions on their occurrence probabilities. The necessity and merits of

considering correlative accidental and security related factors together are clarified. An oil storage tank is studied for fire occurrence probability using the proposed model. The main highlights of the study are:

- The proposed model visually provides specific (unintentional) process accident evolution scenarios from initiation caused by security related factors to propagation and final termination. This helps to design intervention at different stages of event propagation.
- The integrated dynamic model considers dependency caused by common factors, which improves the assessment accuracy of abnormal events and avoids double counting of posterior values of common factors.
- According to the integrated dynamic model, the probability growth of the causal factors which simultaneously exacerbate safety and security results in a larger probability increase of abnormal events compared to that without considering the safety and security dependency. This provides clear evidence of the improved predictability of the model.
- The integrated dynamic model identifies causal factors whose state changes oppositely affect the process accident probability and intentional threat probability. This work helps quantify the impact of such factors and proposes a method to eliminate their opposite impacts on safety and security.
- This integrated dynamic model has dynamic feature; thus, it could obtain the latest states of variables and reduce uncertainty caused by scarce data through probability

update with evidence. A great point is that by considering the interaction between accidental and security related factors, the integrated dynamic model enables to update states of both types of factors (i.e., accidental and security related factors) given evidence of one type of factors. This state updating means the model can identify both accidental and security related factors which are more probable to be of poor states.

- The integrated dynamic model can capture the actual significance of correlative causal factors contributing to the abnormal events by including the interaction of accidental and security related factors.

The current work is mainly aimed to quantitatively show the difference of probabilities of abnormal events and causal factors with and without considering the interaction of safety and security. To clearly demonstrate this point, this paper made some simplification as explained in Section 5.3. In the future work, apart from relaxing those simplification, we could also conduct cost-effective analysis to understand how the interaction of safety and security could influence the cost effect of countermeasures. In this way, the research results will have more direct guidance to risk management and resource assignment. Moreover, a case study containing more factors which have opposite effects on safety and security could be conducted to magnify the effects of such factors.

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.

References

[1] Nima Khakzad and Genserik Reniers. Protecting Chemical Plants against Terrorist Attacks: A Review. J Socialomics. 2015, doi:10.4172/2167-0358.1000142: 1－4

[2] Shailendra Bajpai, Anish Sachdeva, J.P. Gupta. Security risk assessment: Applying the concepts of fuzzy logic. Journal of Hazardous Materials. 2010, 173: 258–264

[3] Edward Broughton. The Bhopal disaster and its aftermath: a review. Environment Health 2005, 4: 1－6.

[4] Faisal Khan, Samith Rathnayaka, Salim Ahmed. Methods and models in process safety and risk management: Past, present and future. Process Safety and Environmental Protection 2015, 98: 116–147

[5] Terje Aven. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering and System Safety 2007, 92: 745–754

[6] Mark Adrian van Staalduinen, Faisal Khan, Veeresh Gadag. SVAPP methodology: A predictive security vulnerability assessment modeling method. 2016, Journal of Loss Prevention in the Process Industries. 2016, 43: 397–413

[7] Brad Plumer. Nine facts about terrorism in the United States since 9/11. The Washington Post. Available at https://www.washingtonpost.com/news/wonk/wp/2013/09/11/nine-facts-about-terrorism-in-the-united-states-since-911/. Accessible

on March 15, 2017.

[8] Mark van Staalduinen, Faisal Khan. A barrier based methodology to assess site security risk. 2015 In: Proceedings of SPE E&P health, safety, security, and environmental conference. 16–March 18, 2015. Denver, USA

[9] Alex Scott. Terrorist Attack Hits U.S.-Owned Chemical Plant In France. c & en Chemical & Engineering News. Available at: http://cen.acs.org/articles/93/web/2015/06/Terrorist-Attack-Hits-US-Owned.html. Accessible on March 15, 2017.

[10] Three hurt in Basque bomb blasts. BBC News. Available at: http://news.bbc.co.uk/2/hi/europe/4549379.stm. Accessible on March 15, 2017.

[11] Stephen Snyder. An Iraqi oil refinery that was too important to destroy has just been destroyed. PRI's The World. Available at: http://www.pri.org/stories/2015-05-27/iraqi-oil-refinery-was-too-important-destroy-has-just-been-destroyed. Accessible on March 15, 2017.

[12] AFP. Islamic State militants attack Iraqs largest oil refinery. The Telegraph. Available at: http://www.telegraph.co.uk/news/worldnews/middleeast/iraq/11530583/Islamic-State-militants-attack-Iraqs-largest-oil-refinery.html. Accessible on March 14, 2017.

[13] Shailendra Bajpai, J.P. Gupta. Site security for chemical process industries. Journal of Loss Prevention in the Process Industries 2005, 18: 301–309

[14] Mark Adrian van Staalduinen, Faisal Khan, Veeresh Gadag, Genserik Reniers. Functional Quantitative Security Risk Analysis (QSRA) to Assist in Protecting

Critical Process Infrastructure. Reliability Engineering & System Safety. 2017, 157: 23–34

[15] Y.F. Khalil. A novel probabilistically timed dynamic model for physical security attack scenarios on critical infrastructures. Process Safety and Environmental Protection. 2016, 102: 473–484

[16] Qilin Feng, Hao Cai, Zhilong Chen, Xudong Zhao, Yicun Chen. Using game theory to optimize allocation of defensive resources to protect multiple chemical facilities in a city against terrorist attacks. Journal of loss prevention in the process industries. 2016, 43: 614－628

[17] L.Zhang, G. Reniers. A Game-Theoretical Model to Improve Process Plant Protection from Terrorist Attacks. Risk Analysis, 2016: 2285-2297

[18] L. Zhang, G. Reniers, X. Qiu. Playing chemical plant protection game with distribution-free uncertainties. Reliability Engineering and System Safety, 2017: 1-11

[19] W. L. McGill, B. M. Ayyub, Multicriteria security system performance assessment using fuzzy logic. J. Defense Model. and Sim., vol. 4, no. 4, 2007: 356－376.

[20] W. L. McGill, B. M. Ayyub, M. Kaminskiy. Risk Analysis for Critical Asset Protection. Risk Analysis, Vol. 27, No. 5, 2007: 1265－1281

[21] Florentine, C., Isenstein, M., Libet, J., Neece, S., Zeng, J., Haimes, Y., & Horowitz, B. (2003, April 24–25). A risk-based methodology for combating terrorism. Paper presented at the Systems and Information Engineering Design Symposium, 2003

IEEE: 157－165.

[22] Haimes, Y. Y. 2002. Strategic responses to risks of terrorism to water resources. Journal of Water Resources Planning and Management 128:383–389.

[23] Ludovic Pietre-Cambacedes, Marc BouissOU. Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). in: IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010). Istanbul, Turkey, 2010: 2852–2861

[24] Genserik Reniers, Paul Van Lerberghe, and Coen Van Gulijk. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Safety Progress. 2015, 34: 72–83

[25] B. M. Ayyub, W. L. McGill, M. Kaminskiy. Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework. Risk Analysis. 2007: 789－801

[26] Igor Nai Fovino, Marcelo Masera, Alessio De Cian. Integrating cyber attacks within fault trees. Reliability Engineering and System Safety. 2009, 94: 1394–1402

[27] Hudson L.,Ware B., Laskey K., Mahoney S. 2002. An application of Bayesian networks to antiterrorism risk management formilitary planners. Technical Report. Digital Sandbox, Inc.

[28] Weber, P., Medina-Oliva, G., Simon, C., Iung, B., 2010. Overview on Bayesian networks application for dependability, risk analysis and maintenance areas. Engineering Applications of Artificial Intelligence 2012, 25:671－682.

[29] Guozheng Song, Faisal Khan, Hangzhou Wang, Shelly Leighton, Zhi Yuan, Hanwen Liu. Dynamic occupational risk model for offshore operations in harsh environments. Dynamic occupational risk model for offshore operations in harsh environments. Reliability Engineering and System Safety. 2016, 150: 58–64.

[30] Zhi Yuan, Nima Khakzad, Faisal Khan, and Paul Amyotte. Risk Analysis of Dust Explosion Scenarios Using Bayesian Networks. Risk Analysis, Vol. 35, No. 2, 2015: 278－291

[31] Nima Khakzad, Faisal Khan, Paul Amyotte. Quantitative risk analysis of offshore drilling operations: A Bayesian approach. Safety Science 2013, 57: 108－117

[32] Majeed Abimbola, Faisal Khan, Nima Khakzad. Dynamic safety risk analysis of offshore drilling. Journal of Loss Prevention in the Process Industries 2014, 30: 74－85

[33] Nima Khakzad, Faisal Khan, Paul Amyotte. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Safety and Environmental Protection. 2013, 91: 46－53.

[34] B. S. Dhillon, Human reliability and error in transportation systems－(Springer series in reliability engineering), Springer-Verlag, London, 2007.

[35] Grozdanovic M., Stojiljkovic E.Framework for human error quantification. Facta Universitatis, series: philosophy, sociology and psychology, 2006, 5:131–144

[36] U. S. Chemical Safety and Hazard Investigation Board. Investigation Report: Herrig Brothers Farm Propane Tank Explosion． Report No. 98-007-I-IA． Access

at http://www.csb.gov/herrig-brothers-farm-propane-tank-explosion/. Available at March 16, 2017.

[37] Francesca Argenti, Gabriele Landucci, Gigliola Spadoni, Valerio Cozzani. The assessment of the attractiveness of process facilities to terrorist attacks. Safety Science 2015, 77: 169–181

[38] James I. Chang, Cheng-Chung Lin. A study of storage tank accidents. Journal of Loss Prevention in the Process Industries, 2006, 19: 51–59.

[39] Jan Erik Vinnem, Willy Røed. Root causes of hydrocarbon leaks on offshore petroleum installations. Journal of Loss Prevention in the Process Industries. 2015, 36: 54–62.

6. Integrated Risk Management of Hazardous Processing Facilities

Preface

A version of this chapter has been accepted for publication by the Journal of Process Safety Progress. I am the primary author of this journal paper. I reviewed literatures, decided research methods, established models and analyzed the case study. I completed the manuscript and revised according to Dr. Faisal Khan's suggestions. Dr. Faisal Khan guided the model development, and then reviewed and revised the manuscript. Dr. Ming Yang provided valuable suggestions in the topic decision and manuscript writing.

Abstract

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.

Keywords: Decision making; safety and security; influence diagram; multi-criteria; hidden risk

6.1 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] modelled 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: Section 6.2 presents the background of integrated risk, an influence diagram and the effects of measures. Section 6.3 explains the risk-based decision-making method. A case study of overfilling of a gasoline tank is demonstrated in Section 6.4. Section 6.5 provides discussion and conclusions.

6.2 Background

6.2.1 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 Fig. 6.1). 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).

Oil fire is taken as an example to explain integrated risk. As shown in Fig. 6.1, 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 Fig. 6.1, 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.

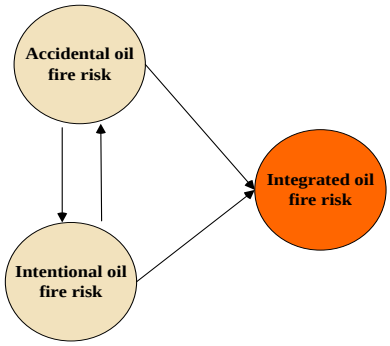


Fig. 6.1 Integrated oil fire risk

6.2.2 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 Fig. 6.2) 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, 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.

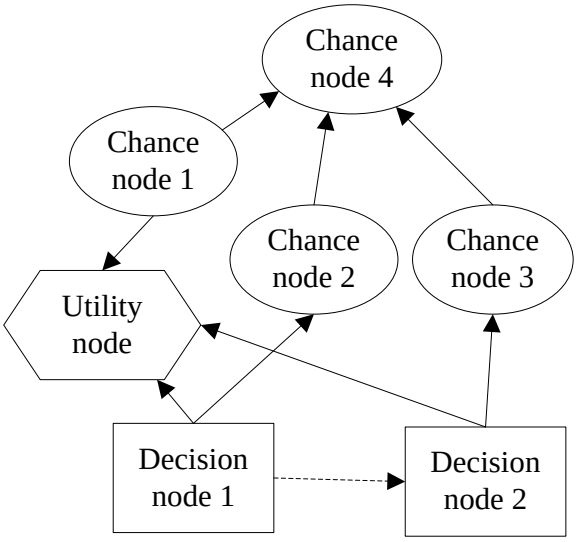


Fig. 6.2 A general influence diagram

6.2.3 Effects of measures on accidental and intentional risks

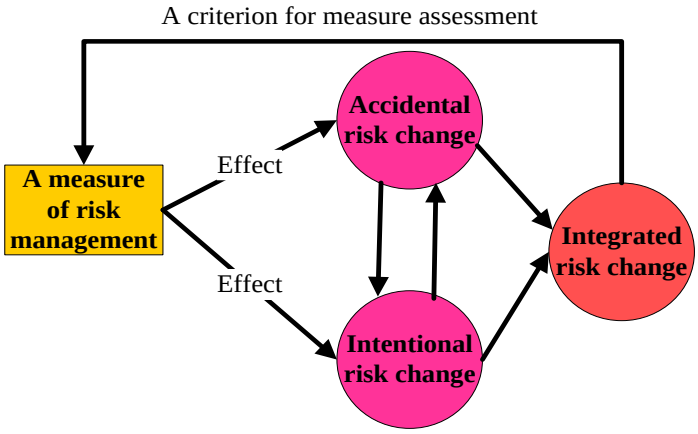


Fig. 6.3 The effects of measures on accidental and intentional risks

Safety and security are dependent, as shown in Fig. 6.3; 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 caused by intentional acts, and thus prevent the intentional damage. 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. Since measures have effects on both safety and security, the decision needs to be made from an integrated perspective. Fig. 6.3 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 US 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.

6.3 Method description

6.3.1 Methodology framework

This ID-based risk management method is divided into two stages. As mentioned in Section 6.2.1, 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 Section 6.3.2.1. 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 Fig. 6.4.

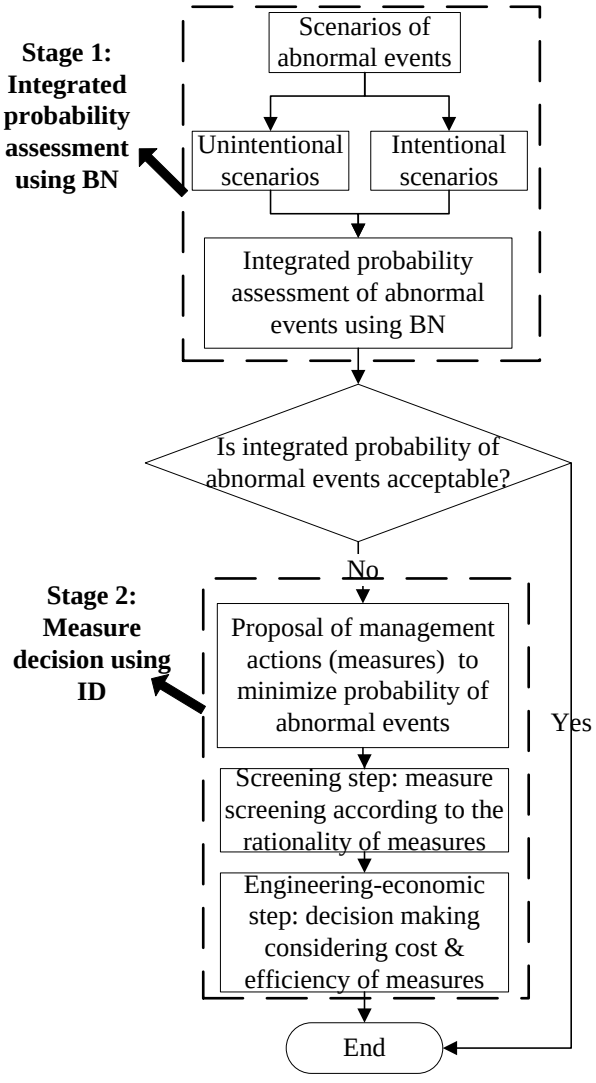


Fig. 6.4 Methodology framework

6.3.2 Approach for risk-based measure decision

6.3.2.1 Criteria of measure assessment

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

(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.

6.3.2.2 Risk assessment

BN is applied to assess the integrated probability of the abnormal event considering the dependency of safety and security, as shown in Fig. 6.5(a). 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 Fig. 6.5(a)), 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.

6.3.2.3 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 Fig. 6.5(b)). 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 Fig. 6.5(b) 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

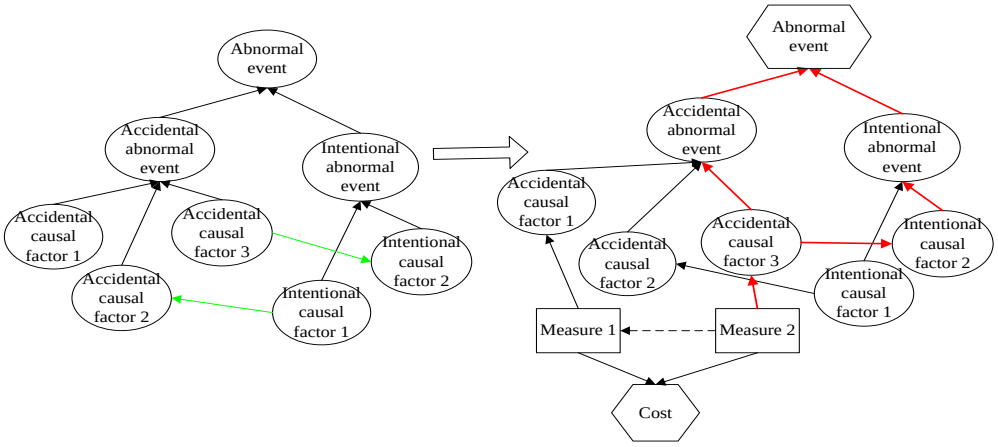
events. This visual form can assist experts to propose further measures, which are explained in Section 6.4. Furthermore, using CPTs, this model has a flexible form to represent the relationship between measures and causal factors. The relationships between measures and factors have two types. The first 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 Fig. 6.5(b) eliminates the safety-related causal factor 3. The proposed model uses a CPT (see Table 6.1) to represent this relationship without a structural change of the model. Table 6.2 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.

Table 6.1 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

Table 6.2 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



(a) BN for risk assessment **(b) ID for risk management**

Fig. 6.5 The establishment of ID based on BN

6.4 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.

6.4.1 Overfilling probability assessment

As described in Section 6.3, 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 6.3. These prior probabilities are decided through an informed estimation based on the available literature [29, 30]. The storage farm has a much weaker 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.

Table 6.3 Root causal factors and prior probabilities [29, 30]

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

After identifying causal factors and analyzing their relationships, the BN is established and shown in Fig. 6.6. 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 overflow’, the dependency between safety and security is established in the model.

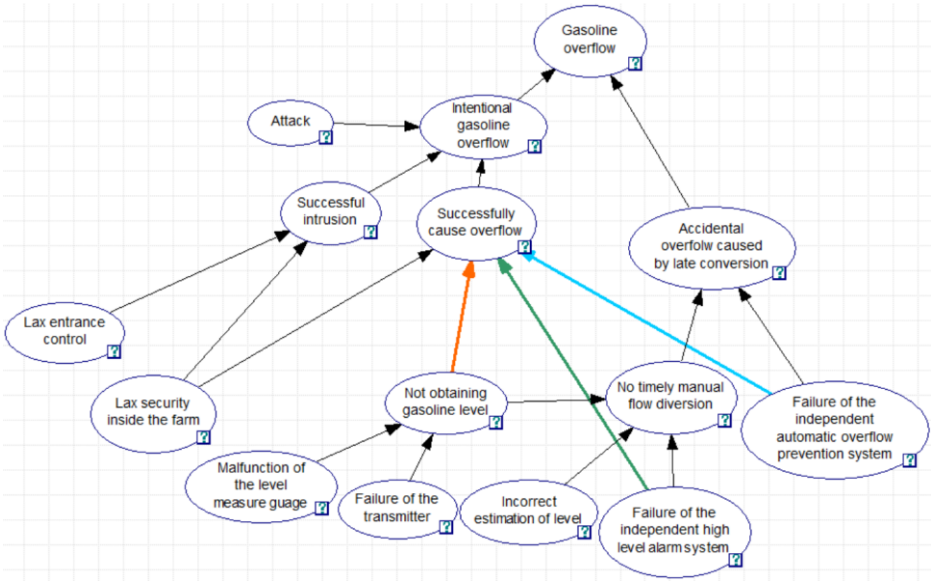


Fig. 6.6 The BN for gasoline overflow assessment

The occurrence probability of gasoline overfilling is calculated using the BN of Fig. 6.6. As shown in row 2 and column 4 of Table 6.5, the occurrence probability of gasoline overflow is 1.48E-2. In this case, the accepted standard for gasoline overflow is considered as 1.00E-3. Then, it is observed that the occurrence probability of overfilling is unacceptable; thus, measures are needed to manage the risk of overflow.

6.4.2 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.

(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 Section 6.3. 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 Fig. 6.6, the ID is obtained, as shown in Fig. 6.7. 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 6.4. 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 6.4 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

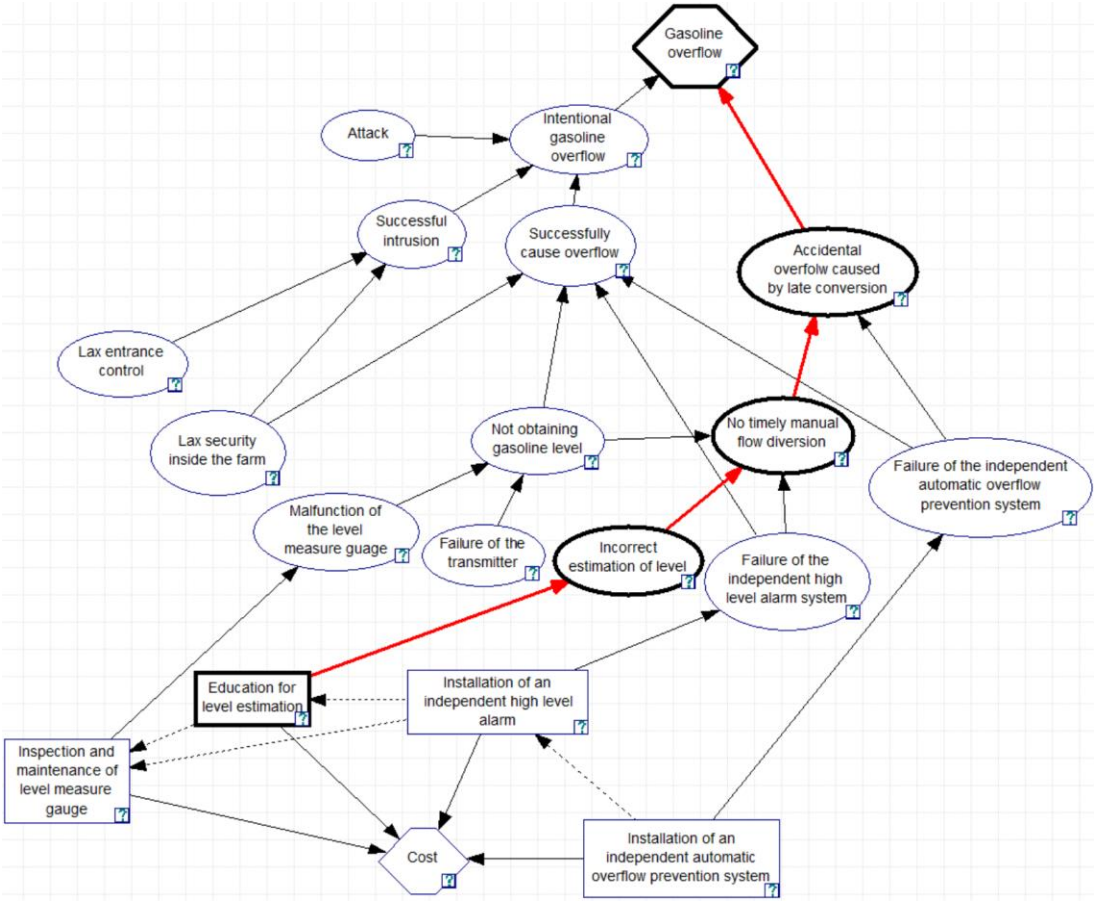


Fig. 6.7 The ID for overfilling of a storage tank

The obtained ID in Fig. 6.7 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 6.5.

Table 6.5 The effect and cost of each measure

Measures	Intentional overfilling probability	Accidental overfilling probability	Overfilling probability	Cost of measures
No	2.35E-3	1.25E-2	1.48E-2	0
Education for level estimation	2.35E-3	2.70E-3	5.03E-3	$500
Inspection and maintenance of	1.67E-3	1.24E-3	2.91E-3	$1000

level measure gauge				
Installation of an independent high-level alarm	1.00E-3	1.41E-3	2.41E-3	$2000
Installation of an automatic overfilling prevention system	1.43E-4	7.59E-4	8.96E-4	$20,000

The overfilling probabilities after using corresponding measures are displayed in rows 3－6 and column 4 of Table 6.5, while the overfilling probability without applying measures is shown in row 2 and column 4 of Table 6.5. 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 6.5), while the other three measures reduce both accidental and intentional overfilling probabilities (see rows 4－6 and columns 2, 3 of Table 6.5). 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 1.48E-2 to 2.41E-3. If the security risk is not considered, the effect of the measure 'installation of the independent high-level alarm' is underestimated by 1.35E-3. The error value is even more substantial than the acceptance criteria (1.00E-3). Thus, the error cannot be ignored. Since 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 6.5, 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 6.6.

Table 6.6 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	1.67E-3	5.53E-4	2.22E-3	$2000
2	Education for level estimation & Installation of	1.00E-3	4.29E-4	1.43E-3	$2500

	an independent high-level alarm				
3	Inspection and maintenance of level measure gauge & Installation of an independent high-level alarm	7.12E-4	2.68E-4	9.79E-4	$3000

As Table 6.6 demonstrates, the probability of overfilling (9.79E-4) reduces to an acceptable level, and the cost ($3000) 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.

6.4.3 Discussion

Rows 2—4 and column 6 of Table 6.6 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 three hours. The rupture fatally injured seven employees, and it became the largest fatal incident at a US 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 non-specific, 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 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 6.5 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 1.00E-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 6.6.

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 6.6, strategies 2 and 3 can reduce the overfilling probability (i.e., accidental overfilling probability) to 4.29E-4 and 2.68E-4, respectively. These overfilling probabilities are acceptable compared to the acceptance standard (1.00E-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 6.6 and row 2 and columns 2－3 of Table 6.5, 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 1.25E-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 1.00E-3, while its accidental counterpart reduces to 4.29E-4. These results provide an opportunity for managers to learn significant risk sources.

6.5 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.

References

[1] Mark Adrian van Staalduinen, Faisal Khan, Veeresh Gadag. SVAPP methodology: A predictive security vulnerability assessment modeling method. 2016, Journal of Loss Prevention in the Process Industries 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. cnsnews. 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] Ludovic Pietre-Cambacedes, Marc BouissOU. Modelling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes). in: IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010). Istanbul, Turkey (2010) 2852–2861

[8] Terje Aven. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering and System Safety 2007, 92: 745–754

[9] Genserik Reniers, Paul Van Lerberghe, and Coen Van Gulijk. Security Risk Assessment and Protection in the Chemical and Process Industry. Process Safety Progress. 2015, 34: 72–83

[10] Guozheng Song, Faisal Khan, Ming Yang. Probabilistic Assessment of Integrated Safety and Security Related Abnormal Events: A Case of Chemical Plants. Safety Science. Under review.

[11] Valeria Villa, Nicola Paltrinieri, Faisal Khan, Valerio Cozzani. Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry. Safety Science 89 (2016) 77–93

[12] Barry Charles Ezell, Steven P. Bennett, Detlof von Winterfeldt, John Sokolowski, and Andrew J. Collins. Probabilistic Risk Analysis and Terrorism Risk. Risk Analysis 30 (2010) 575－589

[13] Igor Nai Fovino, Marcelo Masera, Alessio De Cian. Integrating cyber attacks within fault trees. Reliability Engineering and System Safety 94 (2009) 1394–1402

[14] Zhi Yuan, Nima Khakzad, Faisal Khan, Paul Amyotte. Risk-based optimal safety measure allocation for dust explosions. Safety Science 74 (2015) 79–92

[15] Karima Sedki, Philippe Polet, Frédéric Vanderhaegen. Using the BCD model for risk analysis: An influence diagram based approach. Engineering Applications of Artificial Intelligence 26 (2013) 2172–2183

[16] Valeria Villa, Genserik L.L. Reniers, Nicola Paltrinieri, Valerio Cozzani. Development of an economic model for counter-terrorism measures in the process industry. Journal of Loss Prevention in the Process Industries 49 (2017) 437-460

[17] Mark G. Stewart. Risk-informed decision support for assessing the costs and benefits of protective counter-terrorism measures for infrastructure. International journal of critical infrastructure protection 3 (2010) 29－40

[18] Terje Aven. Risk Analysis and Management. Basic Concepts and Principles. R&RATA 2 (2009) 57－73

[19] Genserik Reniers, Paul Amyotte. Prevention in the chemical and process industries: Future directions. Journal of Loss Prevention in the Process Industries 25 (2012) 227－231.

[20] Guozheng Song, Faisal Khan, Hangzhou Wang, Shelly Leighton, Zhi Yuan, Hanwen Liu. Dynamic occupational risk model for offshore operations in harsh environments. Reliability Engineering and System Safety 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] Grozdanovic M., Stojiljkovic E. Framework for human error quantification. Facta Universitatis, series: philosophy, sociology and psychology 5 (2006) 131－144

[23] M. Arias; 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, 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. Ecological economics 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, 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] David. Gertman, Harold 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] Nicole Perlroth, Clifford 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-cyber attacks.html>. [Accessed 25. 03. 18]

7. Conclusions and Future Work

7.1 Contributions and novelty

7.1.1 Model development for occupational risks of hazardous operations in harsh environments

The logic relationships between causal factors and occupational accidents are more complicated than OR (AND) logic. BN uses the CPTs to express the real logic relationships (Noisy-OR), which is important for accurate risk assessment. Furthermore, the harsh environmental factors are included in the assessment model. Thus, the proposed model also satisfies the risk assessment requirements for hazardous facilities in a harsh environment.

7.1.2 Dynamic risk assessment

The proposed assessment models have a dynamic feature. They can use the evidence of causal factors to forward infer the occurrence probabilities of abnormal events, and can also use the observation of abnormal events to backward infer the states of causal factors. Thus, these models can provide the latest risk updates for effective risk management and also can diagnose new states of causal factors to provide guidance for resource assignment.

7.1.3 The inclusion of continuous variables

Conventional models apply the discrete nodes to approximate the continuous variables,

which deteriorates the assessment accuracy. This research use CBN to represent the continuous variables and capture their continuous changes in a dynamic assessment. This reduces the uncertainty caused by the discrete assumption of conventional assessment models.

7.1.4 Influence analysis of intrusion scenarios

Different intrusion scenarios have different intrusion processes and principles. This research indicates how attackers can achieve their intrusions in different scenarios in a visual form. The influence of intrusion scenarios on the successful intrusion probabilities and security potentials is quantified, based on which the critical intrusion scenarios and weak links of the security system are decided.

7.1.5 The exploration of integrated risk assessment and management

The area of integrated risk for safety and security is a new and promising realm. With the increasing severity of terrorism activities, the security risk needs focused attention. Since safety and security have interactions which may influence the assessment results and measure decision, the integrated risk assessment and management become an interesting topic. This research conducted a dynamic assessment of integrated risk by analyzing safety and security-related factors in a framework. The interaction principle of safety and security is explained and its influence on risk level and the significance of causal factors are dynamically quantified. The cost and effects of measures are analyzed in an integrated framework to demonstrate how the interaction of safety and security

can influence decision-making. By managing the risk in an integrated way, the hidden risks can be detected and the proposed measures can reduce real risk to an acceptable level.

7.2 Conclusions

Hazardous operations face three major risks—occupational, process and intentional damage risks. The first two risks (i.e., safety risk) have been long studied. However, the issues including the emerging challenges of a harsh environment, the static feature of assessment results and the discrete assumption of assessment models have limited the application of existing works and deteriorated their assessment accuracy. The intentional risk of hazardous facilities has caused researchers' attentions after 9/11. However, previous studies on security analysis do not consider the influence of intrusion scenarios. Furthermore, existing works normally study risks caused by either accidents or intentional threats separately. In such a situation, even if a risk is strictly controlled, the hazardous facilities may still be exposed to another major risk. The safety and security risks have interactions which could change both the risk level and the impacts of measures. Works on dynamic risk assessment considering the interaction of safety and security are lacking. The influence of the interaction of safety and security on measure selection has not been studied.

The risk of three occupational accidents (STFs) is assessed first in this thesis. The BT is applied to systematically identify causal factors and clearly represent the evolution

process of STFs. The BN model is established based on BT to dynamically assess the occupational risks and decide the critical causal factors. The harsh environmental factors are included in these assessment models. Then the discrete assumption of traditional assessment models is relaxed by representing continuous variables with CBN. As a result, the uncertainty caused by the discrete assumption of variables is overcome. To improve the security risk assessment, intrusion scenarios are included in the security assessment. The influence of intrusion scenarios on the successful intrusion probabilities and the security potentials of barriers are analyzed. The critical intrusion scenarios and weak links of the security system are dynamically decided. These works have reduced the uncertainty of conventional assessment methods. A robust framework is proposed for the dynamic assessment of integrated safety and security risks and the influence of the interactions of security and safety on risk level and the significance of causal factors are analyzed. Then the measure selection for integrated risk management is analyzed using an ID containing safety and security-related factors. The management actions are decided based on their costs and effects on both accidental and intentional risks.

The methods proposed in this thesis would help providing the latest risk confronted by workers and facilities in hazardous operations. They enable the analysis of risk for operations in a harsh environment, and improve assessment accuracy by relaxing the limitations of previous methods. Furthermore, since this thesis studies risk in an

integrated way, considering interaction of safety and security, it can provide the real risk of hazardous operations and ensure the reduction of real risk to an acceptable level with the selected management actions.

7.3 Future work

This research makes contributions to dynamic risk assessment with high accuracy and integrated risk management considering safety and security related issues. However, the following points can be further improved in the future.

7.3.1. Dependency between different occupational accidents

This research separately studied the risk of three main occupational accidents (STFs). In practice, there may be dependency between different occupational accidents, because various occupational accidents may share the same causal factors. For example, when employees are tired, the likelihood that they suffer from both slips and falls from heights may increase. This means that the control of fatigue can reduce risks of slips and falls from height at the same time. If the dependency of different occupational accidents is studied, such common factors could be identified to more effectively reduce occupational risks.

7.3.2 Distribution decision of continuous variables based on data

In this research, the distributions of continuous variables in CBN are assumed. The case study on vessel roll is conducted for demonstration purposes. If this method is used to solve a practical issue, the data need to be collected and analyzed to make decisions

about distributions of variables and relationships between nodes.

7.3.3 The inclusion of consequence analysis

This research focuses on the dynamic assessment of the probabilities of abnormal events. Since risks are reflected by both probability and consequences, consequence analysis can be included in future work. For example, the influence of interaction of safety and security on consequences of abnormal events can be analyzed. With consequence analysis, the research can provide better guidance for the risk management of hazardous operations.

7.3.4 Inclusion of cyber security risks

For the security perspective, this research focuses on physical attacks. However, in the highly digitized modern plant, cyber attacks are also a security concern. Cyber security could also be incorporated into the integrated risk assessment system in future work. Its dependency with safety and physical security and its influence on the integrated risk can be analyzed.

7.3.5 Development of a software

Since this research deal with multi-risks, many factors and dependency relationships need to be analyzed. This significantly increases the workload. If the methods are used by industry, we cannot expect workers to establish complex models and do probabilistic analysis. Thus, a software including the proposed models could be developed in the future. The workers would only need to input the required parameters; the software can

provide the risk level, measures and visual evolution process of abnormal events.