DYNAMIC SAFETY ANALYSIS USING ADVANCED APPROACHES

NIMA KHAKZAD ROSTAMI

Dynamic Safety Analysis using Advanced Approaches

by

© Nima Khakzad Rostami

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

September 2012

St. John's Newfoundland

Dedicated to my

Father-Reza, mother-Fatemeh, grandmother-Rafat, sisters-Neda, Sareh, Nastaran, and brother-Sina

ABSTRACT

Process systems are prone to accidents as they deal with hazardous material at high temperature and/or pressure. Process plants are also characterized as complex systems where a dense cluster of pipes and equipment may cause a chain of accidents. Therefore, implementation and maintenance of safety measures through risk assessment is crucial to maintain risk below the acceptance criteria. Risk assessment methodologies such as quantitative risk analysis (QRA) and probabilistic safety analysis (PSA) comprise different steps among which accident scenario analysis is a common task. Accident scenario analysis includes accident sequence modeling and associated consequence assessment. Among many techniques available to conduct accident scenario analysis, bow-tie (BT) and Bayesian network (BN) are the most popular. Both techniques are graphical methods illustrating an accident scenario completely and taking advantage of robust probabilistic reasoning engines. BT technique addresses causes and consequences of an accident scenario in a transparent manner that is readily tractable and communicable with stakeholders. However, it suffers limitations of being static and unable to model conditional dependencies. These limitations significantly reduce BT's efficacy to do dynamic risk analysis. In the present study, Bayesian updating and real-time monitoring of operational parameters in the form of physical reliability models are used to overcome these limitations. Physical reliability models provided the analyst with a deepr insight into the behavior of risk while Bayes' rule helps to capture variations over time and to learn from experiences. Bayesian network is an alternative technique to conventional methods such as fault tree and bow-tie, with ample potential in risk

assessment and safety analysis. Mapping fault tree and bow-tie into Bayesian network, it is shown that how conditional dependencies, multi-state variables, common cause failures can be considered and most importantly, probability updating can be conducted. Advanced aspects of Bayesian networks such as object-oriented Bayesian networks (OOBN) and discrete-time Bayesian networks (DTBN) are examined in this study. The former decomposes a large network to sub-models with desired level of abstraction, facilitating the modeling and capturing of dependencies. The latter explicitly takes time into account to model sequential failures by means of dynamic gates. To improve the performance of DTBN, an innovative algorithm is introduced to reduce the size of probability tables. Further, two new relationships are developed for dynamic gates cold spare and sequential enforcing gates to make them compatible with most distribution functions. Applying Bayesian networks in the field of domino effects, both propagation pattern and probability of domino effect at different stages are calculated. In this study, the efficacy of BN in safety analysis and accident scenario modeling of a variety of applications such as loss of well control, risk-based design of safety systems and domino effect is examined.

ACKNOWLEDGEMENTS

I would like to express my sincere and profound sense of gratitude and respect to my supervisor Dr. Faisal Khan and my co-supervisor Dr. Paul Amyotte for their expert guidance and untiring support throughout my research at Memorial University of Newfoundland. Without their encouragement and advice, this thesis might not have been completed successfully. I am especially thankful to Dr. Faisal Khan for his friendship and sharing his vast experience and knowledge over past three years. I am also thankful to my supervisory committee member, Dr. Syed Imtiaz, and my proposal examiners Drs Mahamoud Haddara and Shawn Kenny for their critical comments and constructive suggestions.

I am grateful to my family members, especially my father, mother, grandmother, sisters and brother for their unconditional love and affection during all these years.

Table of Contents

ABSTRACT iii

ACKNOWLEDGEMENTS v

Table of Contents vi

List of Table xiv

List of Figures xvii

List of Symbols, Nomenclature or Abbreviations xxii

1 Introduction 1

1.1 Overview 1

1.2 Risk Assessment Methods 2

1.3 Dynamic Risk Analysis 3

1.4 Motivation 4

1.4.1 Application of Bow-tie Approach in Dynamic Safety Analysis 5

1.4.2 Application of Bayesian Network Approach in Dynamic Safety Analysis .. 6

1.5 Organization of the Thesis 7

1.6 References 9

2 Novelty and Contribution 15

2.1 Overview 15

2.2 Innovative application of advance methods in dynamic safety analysis 15

2.2.1 Mapping fault tree into Bayesian network 15
2.2.2 Mapping Bow-tie into Bayesian network 16
2.2.3 Dynamic bow-tie 16
2.2.4 Application of Discrete-time Bayesian network in risk-based design 16
2.2.5 Application of Bayesian networks in domino effect modeling 17
2.3 Proposed modification to discrete-time Bayesian network 17
2.3.1 Cold spare gate and Sequential enforcing gate 17
2.3.2 Neutral dependency algorithm 17
3 Literature Review 19
3.1 Risk Assessment 19
3.2 Conventional Methods 20
3.2.1 Fault Tree 20
3.2.2 Event Tree 21
3.2.3 Bow-tie 22
3.3 Bayesian Methods 23
3.3.1 Bayes' Theorem 23
3.3.2 Bayesian Networks 24
3.3.3 Dynamic Bayesian Networks 28
3.4 References 30

4 Safety Analysis in Process Facilities: Comparison of Fault Tree and Bayesian Network Approaches 36

4.1 Introduction 37

4.2 Failure Analysis Techniques 41

4.2.1 Fault Tree 41

4.2.2 Bayesian Network 42

4.2.3 Mapping Fault Trees to Bayesian Networks 43

4.3 Safety Analysis 45

4.3.1 Case Study 45

4.3.2 Fault Tree Analysis 46

4.3.3 Bayesian Network Analysis 49

4.3.4 Probability Updating 51

4.4 Modeling Techniques 53

4.4.1 Multi-state Variables and Dependent Failures 54

4.4.2 Functional Uncertainty and Expert Opinion 56

4.5 Conclusion 59

4.6 References 61

5 Dynamic risk analysis using bow-tie approach 66

5.1 Introduction 67

5.2 Bow-tie approach 70

5.3 Bow-tie updating 71

5.3.1 Fault tree revising: use of physical reliability models 72

5.3.2 Event tree updating: use of Bayes' theorem 75

5.3.3 Consequence updating 77

5.4 Case Study: Sugar Refinery Explosion 78

5.5 Application of the Methodology 82

5.5.1 Fault tree revising 82

5.5.2 Event tree updating 85

5.5.3 Dynamic risk assessment 87

5.6 Conclusion 90

5.7 Appendix 92

5.8 References 94

6 Dynamic Safety Analysis of Process Systems by Mapping Bow-tie into Bayesian Network 99

6.1 Introduction 100

6.2 Safety Analysis Techniques 103

6.2.1 Bow-tie model 103

6.2.2 Bayesian Network 104

6.2.3 Mapping Algorithm 105
6.3 Case Study: Vapor Ignition 111
6.4 Methodology Application 112
6.4.1 Bow-tie Analysis 112
6.4.2 Bayesian Network Analysis 116
6.5 Conclusion 122
6.6 References 123
7 Risk-based design of process systems using discrete-time Bayesian network 127
7.1 Introduction 128
7.2 Bayesian network 135
7.2.1 An overview 135
7.2.2 Discrete-time Bayesian network 136
7.3 Dynamic gates: a new formalism 137
7.3.1 Cold spare gate 137
7.3.2 Sequence enforcing gate 143
7.4 Neutral dependency 144
7.4.1 Priority-AND gate 145
7.4.2 Static gates 150
7.5 Application: risk-based design 152

7.5.1 Case study: heat exchanger explosion 152

7.5.2 Accident modeling 154

7.6 Conclusion 162

7.7 References 167

8 Risk Analysis of Deepwater Drilling Blowouts: A Bayesian Approach 170

8.1 Introduction 171

8.2 Well control 177

8.2.1 Kick mechanism 177

8.2.2 Kick detection 180

8.2.3 Blowout 183

8.3 Risk analysis methods 184

8.3.1 Bow-tie 184

8.3.2 Bayesian network 186

8.3.3 Object-oriented Bayesian network 186

8.4 Well control modeling 188

8.4.1 Case-study description 188

8.4.2 Bow-tie modeling 189

8.4.3 Bayesian network modeling 196

8.5 Conclusion 201

8.6 References 202

9 Domino effect analysis using Bayesian networks 206

9.1 Introduction 207

9.2 Domino effect: terminology and characteristics 211

9.2.1 Accident propagation 211

9.2.2 Escalation probability 213

9.3 Bayesian networks 215

9.4 Domino modeling 216

9.4.1 Propagation pattern 216

9.4.2 Domino probability 221

9.4.3 An example 227

9.5 Application 230

9.5.1 Case-study 230

9.5.2 Results and discussion 233

9.6 Conclusion 239

9.7 References 241

10 Summary, Conclusions, and Recommendations 246

10.1 Summary 246

10.2 Conclusions 247

10.2.1 Mapping fault tree into Bayesian network 247

10.2.2 Mapping bow-tie into Bayesian network 248

10.2.3 Application of Object-oriented Bayesian network in complex systems ... 249

10.2.4 Application of physical reliability models in dynamic risk analysis 249

10.2.5 Application of dynamic Bayesian networks in risk-based design 250

10.2.6 Improving the performance of discrete-time Bayesian networks 250

10.2.7 Application of Bayesian networks in domino effect modeling 251

10.3 Recommendations 252

10.3.1 Non-conjugate probability distributions 252

10.3.2 Data requirement 253

10.3.3 Uncertainty handling 253

10.3.4 Lack of availability of commercial tools 254

List of Table

Table 4.1. Different events related to an accident scenario in the feed control system and their occurrence probabilities 45

Table 4.2. Top event probability and improvement indices for FT and BN analysis 47

Table 4.3. Comparison between prior and posterior probabilities in different modeling steps 53

Table 5.1. Data used to estimate the unknown parameters of Weibull distribution for PE4 80

Table 5.2. Prior probabilities of primary events of fault tree 81

Table 5.3. Prior parameters of safety barriers. 82

Table 5.4. Scenarios leading to the same top event probability, i.e. P(TE) = 0.12 85

Table 5.5. Cumulative number of consequences over 5 years of process operation. 86

Table 5.6. Estimated damage of consequences 88

Table 6.1. Possible states of Consequence based on the state combination of Gasoline release and Ignition 108

Table 6.2. Components of the bow-tie in Figure 6.7 and their probabilities 113

Table 6.3. Consequences of the vapor overflow accident scenario 114

Table 6.4. Accident analysis results for BT and BN techniques 115

Table 6.5. Experience used to adapt the prior probabilities 118

Table 7.1. Marginal probability table of node *A* (or *B*). 138

Table 7.2. Conditional probability table of spare B. 139

Table 7.3. Conditional probability table of CSP gate. 139

Table 7.4. Comparison of results for CSP gate. 142

Table 7.5. Comparison of results for SEQ gate. 144

Table 7.6. Conventional CPT for PAND gate. 146

Table 7.7. CPT for PAND gate which is only dependent on B. 147

Table 7.8. CPT for apparent (but neutralized) dependency of B on A. 148

Table 7.9. Comparison of MC and the current study for PAND gate. 149

Table 7.10. CPT of B for an OR gate structure populated using Equation 7.11 151

Table 7.11. CPT of B for an AND gate structure populated using Equation 7.12. 151

Table 7.12. Failure probabilities of the events of DFT in Figure 7.13. 158

Table 8.1. The components of the kick FT in Figure 8.5 and their probabilities [9, 29].191

Table 8.2. The components of the kick detection FT in Figure 8.6 and their probabilities [9, 29]. 192

Table 8.3. The safety barriers of the ET in Figure 8.7 and their probabilities 194

Table 8.4. Accident precursors during the 5 weeks of drilling operation. 200

Table 9.1. The CPT assigned to the auxiliary node L_1 showing that it is conditionally dependent on its parents through an OR-gate. 223

Table 9.2. The AND-gate CPT of node DL_1. 224

Table 9.3. CPT of X_3 to estimate the domino-driven probability, where $P13 = PX3X1$. 225

Table 9.4. CPT of X_3 to estimate the domino-affected probability. The primary probability of X_3 is considered as a leak probability. 226

Table 9.5. Vessel characteristic. 227

Table 9.6. Distances (m) among the units in the tank farm layout in Figure 9.8..... 231

Table 9.7. Overpressure escalation vectors (kPa) [35]. 232

Table 9.8. Heat radiation escalation vectors (kW/m^2). 233

Table 9.9. Domino effect probabilities. 236

List of Figures

Figure 3.1. Generic Bow-tie model 22

Figure 3.2. Various types of nodes in Bayesian networks 25

Figure 3.3. Joint probability distributions based on the chain rule and d-separation (Wilson and Huzurbazar, 2007) 26

Figure 4.1. Mapping fault tree into Bayesian network 44

Figure 4.2. Fault tree for malfunction of the Feed system 47

Figure 4.3. Bayesian network structure based on the fault tree in Figure 4.2 50

Figure 4.4. Bayesian network structure for feed control system with alarm system 55

Figure 4.5. Modified BN to capture functional uncertainty and expert opinion 58

Figure 5.1. Generic bow-tie 70

Figure 5.2. Schematic of BT updating 78

Figure 5.3. Bow-tie modeling of sugar dust explosion at Imperial Sugar manufacturing facility 79

Figure 5.4. Event probability updating for different air velocities (V). 83

Figure 5.5. Top event probability updating for different pipe diameters (d). 83

Figure 5.6. Top event probability updating for different conveyor belt speeds (V_B). 84

Figure 5.7. Top event probability contours for belt speed (V_B) and air velocity (V). 85

Figure 5.8. Posterior failure probabilities of safety barriers. 87

Figure 5.9. Updated probability of consequence *Near miss* using covariates V_B and V and updated safety barriers for year 1 (left) and 5 (right). (d is kept constant, i.e., d = 0.1 m). 88

Figure 5.10. Risk surface for different V_B and V (d is kept constant, i.e., $d = 0.1$ m). 89

Figure 5.11. Risk contours for different V_B and V ($d = 0.1$ m). 90

Figure 6.1. Generic Bow-tie model..... 104

Figure 6.2. Bow-tie model for gasoline release accident scenario. For the sake of brevity, the fault tree part is not completely illustrated..... 107

Figure 6.3. BN model for gasoline release accident scenario..... 108

Figure 6.4. Mapping algorithm from bow-tie into BN. 109

Figure 6.5. Generic BN potentially equivalent to the bow-tie in Figure 6.1. 110

Figure 6.6. Mixing tank and safety measures (CSB, 2007). 112

Figure 6.7. BT model for the heat exchanger accident scenario (CSB, 2007). 113

Figure 6.8. Corresponding BN of bow-tie in Figure 6.7..... 116

Figure 6.9. Updated probabilities of the primary events and the top event (Vapor). 119

Figure 6.10. Updated probabilities of the safety barriers..... 120

Figure 6.11. Updated probability of C_8 over the course of 4 years. 121

Figure 7.1. SFT (left), DFT (middle) and MC (right) models for a three-component parallel system in which A must fail before B. The dashed parts in the MC are not accounted for in the system failure due to the representation of improper failure sequences. $\boldsymbol{\lambda}$ is the failure rate of components. 131

Figure 7.2. Converting a CSP gate into interval-based (middle) and instant-based (right) BN structures. 133

Figure 7.3. Time line intervals [12]. 136

Figure 7.4. CSP gate mapping into DTBN [6]..... 138

Figure 7.5. Shifted probability distribution of spare B. 141

Figure 7.6. General Markov chain for CSP and SEQ gates. 142

Figure 7.7. SEQ gate mapping into DTBN. Either *A* or *B* could be different basic events or subsystems. 143

Figure 7.8. Mapping PAND gate into DTBN. 146

Figure 7.9. Modified PAND gate structure in DTBN. 147

Figure 7.10. Markov Chain of PAND gate. 149

Figure 7.11. AND/OR gate corresponding structure in DTBN using Neutral Dependency. 150

Figure 7.12. Schematic of the heat exchanger in the Goodyear accident [19]. 153

Figure 7.13. SFT and DFT of the heat exchanger explosion (safety scenario 1). For the sake of brevity, only the modified part of the DFT is illustrated. 156

Figure 7.14. BN of the explosion in the heat exchanger. 157

Figure 7.15. Modified DFT in which BV_3 is opened if PRP fails to release the pressure. The parts which are not drawn are the same as Figure 7.13. 159

Figure 7.16. A comparison between prior (the upper row) and posterior probability distributions (type 1 in the 2nd row and type 2 in the 3rd row) of BV_1, BV_3 and RD..... 161

Figure 8.1. Schematic of well control procedure. 172

Figure 8.2. The relation between the penetration rate and the drilling margin [20]. V_0 is the rate of penetration when $\Delta P = 0$. 182

Figure 8.3. Typical bow-tie model consisting of a fault tree on the left and an event tree on the right-hand side. 185

Figure 8.4. Using OOBN to modularize BN into sub-networks. A BN (left) is constructed using hierarchical structures with arbitrary levels of abstraction (middle) and consequently shown using instance nodes (right). 188
Figure 8.5. Kick fault tree. 190
Figure 8.6. Kick detection fault tree. 192
Figure 8.7. Escalation of kick into blowout event tree. 193
Figure 8.8. Bow-tie model for loss of well control. PE5 in the kick FT and PE11 in the kick detection FT have common cause failures (colored in orange) as well as PE1 in the kick FT and Casing in the safety barrier ET (colored in yellow). 195
Figure 8.9. OOBN for the loss of well control, including instance nodes and the usual node Consequence. 197
Figure 8.10. Collapsed form of the OOBN for the loss of well control. 198
Figure 8.11. The updated probabilities of kick and blowout based on sequential learning. 201
Figure 9.1. Domino effect where an accident in X_1 can trigger secondary accidents in X_2, X_3, and X_4. According to threshold values, X_5 and X_6 are not impacted by X_1. 212
Figure 9.2. A likely propagation pattern of the domino effect. The numbers in parentheses show the occurrence orders of events (Step 4 of the methodology). 217
Figure 9.3. Procedure to develop the propagation pattern of domino effect. 220
Figure 9.4. Modified BN to incorporate the union of tertiary and quaternary events using auxiliary nodes L_1 and L_2, respectively. 222

Figure 9.5. The complete BN for propagation pattern and occurrence probability estimation of the domino effect. 224
Figure 9.6. Case study for domino accident analysis. 227
Figure 9.7. BN developed for the example in Figure 9.6. 228
Figure 9.8. Schematic of storage tanks in a tank farm. 231
Figure 9.9. Propagation pattern of the domino effect in the tank farm. 234
Figure 9.10. BN to model domino effect in the tank farm. 235
Figure 9.11. Modified propagation pattern of the domino effect. 239

List of Symbols, Nomenclature or Abbreviations

Abbreviations

ASME: American Society of Mechanical Engineers

BHP: Bottom Hole Pressure

BHP_0: Initial Bottom Hole Pressure

BlowFAM: Blowout Frequency Assessment Model

BN: Bayesian Network

BOP: Blowout Preventer

BP: British Petroleum

BT: Bow-tie

C: Consequence

CBFT: Condition-based Fault Tree

CCPS: Center for Chemical Process Safety

CDF: Cumulative Density Function

CPT: Conditional Probability Table

CSB: Chemical Safety Board

CSP: Cold Spare gate

CTBN: Continuous Time Bayesian Network

DBN: Dynamic Bayesian Network

DFT: Dynamic Fault Tree

DL: Domino Level

DTBN: Discrete-time Bayesian Network

E: Evidence

ERCB: Energy Resources Conservation Board, Canada

ET: Event Tree

FDEP: Functional Dependency gate

FT: Fault Tree

GoM: Gulf of Mexico

HUGIN: Bayesian Network Software Tool

IE: Intermediate Event

IM: Importance index

LPG: Liquefied Petroleum Gas

LS: Least Square Method

LWC: Loss of Well Control

MC: Markov Chain

MIMAH: Methodology for Identification of Major Accident Hazards

MIRAS: Methodology for Identification of Reference Accident Scenarios

MLC: Most Likely Configuration

MLE: Maximum Likelihood Estimation

MPE: Most Probable Explanation

NSERC: Natural Sciences and Engineering Research Council of Canada

OCS: Outer Continental Shelf

OOBN: Object-oriented Bayesian Network

ORA: Optimal Risk Analysis

OREDA: Offshore Reliability Data Handbook

PAND: Priority AND gate

PDEP: Probability Dependency gate

PDF: Probability Density Function

PE: Primary Event

PF: Pool Fire

PRAC: Petroleum Research Atlantic Canada

PSA: Probabilistic Safety Analysis

QRA: Quantitative Risk Analysis

RADYBAN: Reliability Analysis with Dynamic Bayesian Network

SB: Safety Barrier

SCSSV: Surface-Controlled Subsurface Safety Valve

SEQ: Sequential Enforcing gate

SFT: Static Fault Tree

SINTEF: Offshore Blowout Database

TBN: Temporal Bayesian Network

TE: Top Event

USD: United State Dollar

VCE: Vapor Cloud Explosion

WinBUGS: Windows Bayesian Inference Using Gibbs Sampling

WOAD: World Offshore Accident Databank, Norway

2TBN: 2 Time-sliced Bayesian Network

Symbols

a_0: Constant

a_1: Constant

a_2: Constant

A: Vector of unknown parameters

A_i: Random variable

d: Pipe diameter

e: Exponential number ~ 2.718281828

E (.): Expected value

Exp (.): Exponential function

f (.): Probability density function

F (.): Cumulative density function

F_P: Fracture pressure

g (.): Positive function

h: Height of mud column

k: Strength

L (.): Likelihood function

Ln: Natural logarithm

M: Minimum cut-set

N: number of time intervals

P_{Leak}: Probability of leak

Pa (.): Parent set

Pr (.): Probability

P_f: Frictional pressure

P_h: Hydrostatic pressure

P_P: Pore pressure

P_{sg}: Surge pressure

P_{sw}: Swabbing pressure

Q: Component

Q: Heat radiation

Q_{th}: Heat radiation threshold

r: number of failures

t: time

T: Operational time

ttf: Time to failure of equipment due to heat radiation

U (.): Set of variables

V: Escalation vector

V: Air velocity

V_B: Conveyor belt speed

V_S: Sugar flow velocity

X: Vector of covariates

Y: Stress

α: Distribution parameter

β: Shape factor

Γ (.): Gamma function

Δ: Time interval

ΔP_L: Lower drilling margin

ΔP_U: Upper drilling margin

θ: Scale factor

$\boldsymbol{\lambda}_0$: Baseline failure rate

$\boldsymbol{\lambda}$: Failure rate

ρ: Density of drilling mud

ϕ: Cumulative density function of standard normal distribution

$\cup$: Union

$\cap$: Intersection

∞: Infinity

1 Introduction

1.1 Overview

Risk analysis is important in processing facilities as they deal with a large amount of hazardous chemicals; also, process areas are congested with complex piping, high-pressure compressors, and separators of which malfunctions and mishaps may lead to catastrophic accidents (Khan et al., 2001; Torres-Toledano and Sucar, 1998).

There have been many fatal explosions and fires imposing major capital loss and considerable death toll in the past two decades. On 23 March 2005, the BP refinery explosion in Texas City caused 15 deaths and more than 170 injuries (CNN, 2005). According to the final report issued by BP (2005), a lack of process safety measures and insufficient risk reduction measures were to blame for the accident. On 7 February 2010, the Kleen Energy power plant exploded in Middletown, Connecticut, killing 6 and injuring at least 12. The explosion was one of the worst industrial disasters in the U.S. in recent years (Reuters, 2010a). Most recently, on 20 April 2010, explosion and fire on Transocean Ltd's drilling rig killed 11 and injured 17 in the Gulf of Mexico. The failure of a blowout preventer (BOP) has been determined as the primary cause of the accident (Reuters, 2010b). It is important to broaden the risk analysis scope by considering accident scenario and real-time safety analysis to predict and continuously update the likelihood of catastrophic accidents and to take actions to prevent them.

Forecasting likely accident scenarios is the most important step in safety analysis. Khan (2001) proposed a *maximum credible accident scenario* approach that short-lists the

important scenarios based on both their consequences and the likelihood of accident occurrence. Delvosalle et al. (2006) used two methodologies: *MIMAH* (Methodology for Identification of Major Accident Hazards), in which no safety system was considered, and *MIRAS* (Methodology for Identification of Reference Accident Scenarios), in which all the actual safety functions and barriers were included in the analysis.

1.2 Risk Assessment Methods

Risk analysis focuses on quantifying the occurrence probability of the selected accident scenarios. There are many techniques available, among which fault tree (FT), event tree (ET), bow-tie (BT), safety barrier diagram, and Bayesian network (BN) are very popular. Although conventional risk assessment methods have played an important role in identifying major risks and maintaining safety in process facilities, they suffer limitations which restrict their application in the risk analysis of complex and interlinked systems.

For example, conventional FTs, as one of the most popular techniques used in quantitative risk analysis, are not suitable for analyzing large systems, particularly if the system presents redundant failures, common cause failures, or dependent primary events. More importantly, events in a conventional FT are assumed independent, which is not usually a valid assumption (Bobbio et al., 2001; Torres-Toledano and Sucar, 1998; Simon et al., 2007).

Likewise, most of the limitations of conventional techniques such as FT and ET arise due to the static nature of these methods that fails to catch up with the dynamic operation environment of process systems. This dynamic nature can be either due to any change in the process environment or operational situation such as variations in temperature,

pressure, humidity and geometry or due to change in analyst's initial beliefs based on observed near-misses, mishaps, incidents, and accidents.

1.3 Dynamic Risk Analysis

There have been efforts to make risk assessment methods dynamically adapted as real-time changes occur in a process. Shalev and Tiran (2007) introduced condition-based fault tree in which failure rates of components are periodically updated using information obtained through predictive maintenance. Consequently, the failure probability of the top event is updated by recalculating the FT for new failure rates. However, this method has to be implemented in specific conditions where, for example, gradual deterioration process of a component can be discretized into several stages. And at each of stage there should be a correlation between residual time of the component and its total failure time.

The issue of deficiency of conventional methods in dynamic risk analysis has remarkably been addressed by introducing the application of Bayesian techniques in the field of risk assessment and safety analysis in the late 1970s (Apostolakis, 1978; Parry and Winter, 1981). Bayesian methods have proven to be an effective technique in handling sparse data as well as different sources of information, and also a well suited framework for subjective probability domains such as decision making under uncertainty (Siu and Kelly 1998). Accordingly, several forms of Bayesian analysis such as two-stage Bayesian methods (Kaplan, 1983) and empirical Bayes methods (e.g., Carlin and Lous, 1989; Martiz and Lwin, 1989) have been applied in the context of probabilistic risk analysis. Consequently, there have been many attempts to equip conventional risk analysis methods such as FT and ET with Bayesian techniques for dynamic risk analysis. For

example, Ching and Leu (2009) also used Bayesian theory to update FT while Kalantarnia et al. (2009), Meel and Seider (2006), and Rathnayaka et al. (2011) used Bayesian theory to update the failure probability of the safety functions of an ET.

Apart from the aforementioned efforts, other researchers have attempted to substitute Bayesian network (BN) for reliability block diagrams (Torres-Toledano and Sucar, 1998), static FTs (Bobbio et al, 2001), Dynamic FTs (Boudali and Dugan, 2005; Montani et al., 2008) and ETs (Bearfield & Marsh, 2005).

BNs have provided a promising framework for system safety analysis and risk management (Mahadevan et al., 2001). A comprehensive and state of the art application of Bayesian inference and Bayesian network in risk analysis can be found in Kelly and Smith (2009), Siu and Kelly (1998) and Weber et al. (2010). Further, there are attempts to substitute Markov models for FT (Xing et al., 1996) or to construct dynamic FT and ET from corresponding Markov models such that time-dependent failures can be taken into account (Bucci et al., 2008). However, the application of Markov models in complex systems has been limited due to the well-known problem of state-space explosion and also the error-prone mapping procedure (Boudali and Dugan, 2005).

1.4 Motivation

In this research, the application of advanced risk analysis methods such as BT and BN are investigated and discussed in the context of dynamic safety analysis of process systems. In the following sections, a brief description of these methods as well as the motivation of this research is explained.

1.4.1 Application of Bow-tie Approach in Dynamic Safety Analysis

Among accident analysis models, BT has been well proven to be a reliable and efficient tool, due to its ability to incorporate causes and consequences of an accident in a graphical model. It has been widely used in different safety and risk contexts such as process safety analysis (Markowski et al., 2009), accident risk assessment (Chevreau et al., 2006; Delvosalle et al., 2005; Delvosalle et al., 2006; Dianous and Fievez , 2006; Gowland 2006) and risk management (Cockshott, 2005).

The most important motivations of this research are to utilize unique features of BT and also overcome its limitations including:

- BT consists of a FT and an ET. Conventional FTs and ETs cannot adapt themselves to the dynamic nature of accidents. These techniques are unable to use the real-time information directly obtained through the operational time of the process of interest to update prior beliefs.
- Comprising of a FT and ET, BT suffers limitations of both techniques. For example, it is not suitable for accident scenarios where common cause failures or dependent failures take place. Further, it is not capable of incorporating multi-state variables, which are frequently encountered in process systems modeling.
- In BT, it is not possible to model potential conditional dependencies among the primary events of the FT and the safety barriers of the ET. Also, the conditional failure probabilities of a safety barrier given that the initiating event of the ET (i.e. the top event of the FT) has not occurred could not be modeled.

1.4.2 Application of Bayesian Network Approach in Dynamic Safety Analysis

In recent years, Bayesian Network (BN) approach has begun to be used in engineering applications. BN is a graphical inference technique used to express the causal relationships among variables. BNs are used either to predict the probability of unknown variables or to update the probability of known variables given new information of other variables (evidence). Updating is done through the process of probability propagation and reasoning which is based on Bayes' theorem.

The important motivations of the present work of using BN approach are:

- Although BNs have widely been used in the context of reliability engineering (Langseth and Portinale, 2007) and risk assessment (Weber et al., 2010), their application in probabilistic safety analysis is yet to be explored.
- Flexible structure and robust inference engine of BN make it possible to conduct dynamic risk assessment and safety analysis for a wide variety of process system.
- Incorporating multi-state variables and dependent failures and also handling various types of structural and functional uncertainties are strong modeling features of BN relying on which most of limitations of conventional risk analysis methods can be relaxed to a great extent.
- BN can perform probability updating using chain rule and d-separation criteria which cannot be done using conventional methods unless they are coupled with Bayes' theorem.
- Aside from probability updating, BN is able to perform sequential updating or probability adapting. Through sequential updating, experiences gathered from the

process of interest over time can be taken into account to adapt the probability values of the system considering real observations. This is of great importance in the frequency estimation of rare events based on frequent accident precursors.

1.5 Organization of the Thesis

This thesis is written in manuscript format (paper based). Outline of each chapter is explained below:

Chapter 2 discusses the novelties and contributions this thesis has made to the safety analysis of process systems. It comprises innovative applications of bow-tie and Bayesian network (particularly in the field of safety analysis) as well as new algorithms and proposed improvements in both approaches.

Chapter 3 presents the literature review pertinent to this thesis. The literature review mainly deals with risk analysis methods such as fault tree and event tree as well as advanced approaches such as bow-tie and Bayesian approaches.

Chapter 4 discusses process safety analysis. This chapter briefly presents analyses performed using conventional fault tree and Bayesian network. Subsequently, it is shown how the limitation of fault tree can be relaxed using the latter approach. It also highlights various modeling techniques of Bayesian network. This chapter was published in the *Journal of Reliability Engineering and System Safety 2011; 96: 25-32.*

Chapter 5 introduces bow-tie approach and its application in risk assessment and safety analysis. Similar to Chapter 4, a comparison is made between bow-tie and Bayesian network, and it is shown how limitations of bow-tie can be effectively addressed by mapping it into Bayesian network. This chapter was published in the *Process Safety and Environmental Protection 2012, doi:10.1016/j.psep.2012.01.005.*

Chapter 6 discusses the application of bow-tie approach in dynamic risk analysis of process systems. Physical reliability models and Bayes' theorem are used to make bow-tie suitable for dynamic risk analysis. This chapter was published in the *Journal of Reliability Engineering and System Safety 2012; 104: 36-44.*

Chapter 7 presents the application of dynamic Bayesian network to risk-based design of process system. In this chapter, unique developments of Bayesian network approach in discrete time domain is discussed. This chapter also introduces innovative revisions in existing analysis. This form of Bayesian is most applicable in process safety system design. This chapter was accepted for publication by the *Journal of Reliability Engineering and System Safety* for publication.

Chapter 8 presents another application of bow-tie and Bayesian network in highly complex and interlinked system of well control risk analysis. In this chapter, Object-Oriented Bayesian network (OOBN) is used to reduce the complexity of the model and make it tractable. This chapter was submitted for publication to the *Safety Science.*

Chapter 9 is devoted to the application of Bayesian networks to the modeling of domino accidents in process plants. It illustrates how using noisy gates and auxiliary nodes the complex behavior of domino effects can effectively be modeled using Bayesian networks. This chapter has been accepted for publication by the *International Journal of Risk Analysis*.

Chapter 10 reports the summary of the thesis and the main conclusions drawn through this work. Recommendations for future work are presented towards the end of the chapter.

1.6 References

Apostolakis G. Probability and risk assessment: the subjectivistic viewpoint and some suggestions. Nuclear Safety, 1978; 19: 305-315.

Bearfield G, Marsh W. Generalizing event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science 2005; 3688: 52-66.

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Journal of Reliability Engineering and System Safety, 71, 249-260.

Boudali, H., & Dugan, J.B. (2005). A new Bayesian approach to solve dynamic FTs. Proceedings of Reliability and Maintainability Symposium (RAMS'05), 451-456.

BP. (2005). http://www.bp.com/genericarticle.do?categoryId=2012968 & contentId =7012963 (last checked on 29.06.10)

Bucci P, Kirschenbaum J, Mangan LA, Aldemir T, Smith C, Wood T. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliability Engineering and System Safety 2008; 93: 1616-1627.

Carlin BR, Louis TA. Bayes and Empirical Bayes Methods for Data Analysis. Chapman and Hall, London, 1996.

Ching, J., & Leu, S.S. (2009). Bayesian updating of reliability of civil infrastructure facilities based on condition-state data and fault-tree model. Journal of Reliability Engineering and System Safety, 94, 1962-1974.

CNN. (2005). http://www.cnn.com/2005/US/03/23/plant.blast/index.html (last checked on 29.06.10).

Chevreau FR, Wybo JL, Cauchois D. Organizing learning processes on risks by using the bow-tie representation. Journal of Hazardous Materials 2006; 130: 276-83.

Cockshott JE. Probability bow-ties a transparent risk management tool. Process Safety and Environmental Protection 2005; 83: 307-16.

Delvosalle C, Fievez C, Pipart A, Casal Fabrega J, Planas E, Christou M, Mushtaq F. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety 2005; 90: 238-46.

Delvosalle, C., Fievez, C., Pipart, A., & Debray, B. (2006). ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. Journal of Hazardous Materials, 130, 200-219.

Dianous VD, Fievez C. ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. Journal of Hazardous Materials 2006; 130: 220-33.

Gowland R. The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: a step forward towards convergent practices in risk assessment? Journal of Hazardous Materials 2006; 130: 307-10.

Jensen, F.V., & Nielsen, T.D. (2007) Bayesian networks and decision graphs. 2nd edition, New York, Springer.

Kalantarnia M, Khan F, Hawboldt K. Dynamic risk assessment using failure assessment and Bayesian theory. Loss Prevention in the Process Industries 2009; 22: 600-6.

Kaplan S. On a 'two-stage' Bayesian procedure for determining failure rates. IEEE Transaction on Power Apparatus and Systems, 1983; PAS-102: 195-262.

Kelly DL, Smith CL. Bayesian inference in probabilistic risk assessment- The current state of the art. Reliability Engineering and System Safety 2009; 94: 628-43.

Khakzad N, Khan F, Amyotte P. Safety Analysis in safety facilities: comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety 2011; 96: 925-32.

Khakzad N, Khan F, Amyotte P. Dynamic Safety Analysis of Process Systems by Mapping Bow-tie into Bayesian Network. Process Safety and Environmental Protection 2012; doi: 10.1016/j.psep.2012.01.005.

Khan, F.I., Sadiq, R., & Husain, T. (2001). Risk-based process safety assessment and control measures design for offshore process facilities. Journal of Hazardous Materials, A94, 1-36.

Khan, F.I. (2001). Use maximum-credible accident scenarios for realistic and reliable risk assessment. Chemical Engineering Progress, 11, 56-64.

Kjaerulff, U.B., & Madsen, A.L. (2007). Bayesian networks and influence diagrams_A guide to construction and analysis. New York, Springer.

Lampis, M., & Andrews, D. (2009). Bayesian belief networks for system fault diagnostics. International Journal of Quality and Reliability Engineering, 25, 409-426.

Langseth, H., & Portinale, L. (2007). Bayesian networks in reliability. Journal of Reliability Engineering and System Safety, 92, 92-108.

Mahadevan, S., Zhang, R., & Smith, N. (2001). Bayesian networks for system reliability reassessment. Journal of Structural Safety, 23, 231-251.

Maritz JS, Lwin T. Empirical Bayes Methods, 2nd edn. Chapman and Hall, London, 1989.

Markowski, A.S., Mannan, M.S., & Bigoszewska, A. (2009). Fuzzy logic for process safety analysis. Journal of Loss Prevention in the Process Industries, 22, 695-702.

Marquez D, Neil M, Fenton N. Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering and System Safety 2010; 95: 412-25.

Meel A, Seider WD. Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science 2006; 61: 7036-56.

Montani, S., Portinale, L., Bobbio, A., & Codetta-Raiteri, D. (2006). Automatically translating dynamic FTs into dynamic Bayesian networks by means of a software tool. Proceedings of Reliability and Maintainability Symposium (RAMS'06), 434-441.

Montani, S., Portinale, L., Bobbio, A., & Codetta-Raiteri, D. (2008). RADYBAN: A tool for reliability analysis of dynamic FTs through conversion into dynamic Bayesian networks. Journal of Reliability Engineering and System Safety, 93, 922-932.

Parry GW, Winter PW. Characterization and evaluation of uncertainty in probabilistic risk analysis. Nuclear Safety, 1981; 22: 28-42.

Rathnayaka S, Khan F, Amyotte P. SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study. Process Safety and Environmental Protection 2011b; 89: 75-88.

Reuters. (2010a). http://www.reuters.com/article/idUSTRE61619Q20100207 (last checked on 25.06.10)

Reuters. (2010b). http://www.reuters.com/article/idUSTRE6482L220100510 (last checked on 29.06.10)

Shalev, D.M., & Tiran, J. (2007). Condition-based FT analysis (CBFTA): A new method for improved fault tee analysis (FTA), reliability and safety calculations. Journal of Reliability Engineering and System Safety, 92, 1231-1241.

Simon, C., Weber, P., & Levrat, E. (2007). Bayesian networks and evidence theory to model complex systems reliability. Journal of Computers, 2, 33-43.

Siu NO, Kelly DL. Bayesian parameter estimation in probabilistic risk assessment. Reliability Engineering and System Safety 1998; 62: 89-116.

Torres-Toledano, J.G., & Sucar, L.E. (1998). Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science, 1484, 195-206.

Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2010). Overview on Bayesian networks applications for dependability, risk analysis, and maintenance areas. Engineering Application of Artificial Intelligence, doi: 10.1016/j.engappai.2010.06.002.

Wilson, A.G., & Huzurbazar, A.V. (2007). Bayesian networks for multilevel system reliability. Journal of Reliability Engineering and System Safety, 92, 1413-1420.

Xing L, Fleming KN, Loh WT. Comparison of Markov model and fault tree approach in determining initiating event frequency for systems with two train configurations. Reliability Engineering and System Safety 1996; 53: 17-29.

2 Novelty and Contribution

2.1 Overview

The novelties and contributions of this work are classified into two categories:

- Innovative application of advanced methods in dynamic safety analysis, and
- Modification of discrete-time Bayesian network using new algorithms and equations.

In this chapter, these novelties are briefly explained while the details are presented in the relevant chapters.

2.2 Innovative application of advance methods in dynamic safety analysis

2.2.1 Mapping fault tree into Bayesian network

In this research, fault tree is mapped into Bayesian network to perform safety analysis in process systems where multi-state variables and dependent failures are frequently encountered. Although such a technique has widely been used in the field of reliability engineering and fault diagnosis, its application in safety analysis is not well recognized. Further, functional uncertainty and expert opinion are explicitly modeled by modifying the network. Also, the most critical minimum cut-set in fault tree is found to be analogous to the most probable explanation concept in Bayesian network. This contribution is discussed in more detail in Chapter 4.

2.2.2 Mapping Bow-tie into Bayesian network

In this research a methodology is introduced for mapping bow-tie model into Bayesian network. This methodology makes it possible to model conditional dependencies among the components of the model. Further, the concept of probability adapting or sequential learning is applied along with probability updating. Following this methodology, it is further illustrated how a large and complex system, which is intractable through bow-tie model, can be modeled using object-oriented Bayesian network. This contribution is drawn from Chapters 6 and 8.

2.2.3 Dynamic bow-tie

In this research, a methodology is developed to make bow-tie approach well suited to dynamic risk analysis. The methodology is based on physical reliability models and Bayes' theorem. Although condition monitoring and physic-based failure models are widely used in reliability engineering and maintenance engineering, the application of physical reliability models in the field of risk analysis is for the first time introduced here. The methodology is explained in detail in Chapter 5.

2.2.4 Application of Discrete-time Bayesian network in risk-based design

This research illustrates the effective application of dynamic Bayesian networks in risk-based design of process systems. The main focus of past works was mainly on layers of protection, this study shows how the system safety can be improved without introducing additional safety barriers. In other words, the main focus in this work is on the placement and time sequence of safety barriers. This contribution is the foundation of Chapter 7.

2.2.5 Application of Bayesian networks in domino effect modeling

In this work, an innovative methodology is developed to model and analyze domino effect accidents using Bayesian networks. Complex probabilistic causal relationships among components of the system of interest are modeled using noisy gates and leak probability. This contribution is the basis of Chapter 9.

2.3 Proposed modification to discrete-time Bayesian network

2.3.1 Cold spare gate and Sequential enforcing gate

In this work, a new equation is derived for cold spare gate (CSP gate) in dynamic Bayesian networks. The equation has the advantage of modeling components with non-exponential probability distributions. The equation is shown to have closed-form analytical solution for most probability distributions. The equation can also be used to model sequential enforcing gate (SEQ gate) as a special case of cold spare gate. Comparison with analytical methods such as Markov Chain demonstrates the accuracy and applicability of the newly developed equations. This contribution is discussed in Chapter 7.

2.3.2 Neutral dependency algorithm

A novel algorithm, neutral dependency, is introduced in this research to reduce the size of large and intractable conditional probability tables. The algorithm decomposes a sparse matrix of size $(n+1)^3$ to an identity matrix and a lower triangular matrix, both of size $(n+1)^2$. The algorithm is effectively used to model priority And gate (PAND gate). Due

to its compact and structured relations, the algorithm can also be applied to traditional AND gate and OR gate in discrete-time Bayesian networks. This contribution is fully developed and discussed in Chapter 7.

3 Literature Review

3.1 Risk Assessment

There are many methods for risk assessment of envisaged accident scenarios in the process industries, such as quantitative risk assessment (QRA), probabilistic safety analysis (PSA), and maximum credible accident analysis (Khan, 2001; Khan & Abbasi, 1998). Although these methods consist of different steps and follow specific procedures, accident scenario identification in terms of both mechanism and likelihood is a common and central step to all of them. Among the different models available to identify and analyze accident scenarios, fault tree model (FT), event tree model (ET), and bow-tie model (BT) have been well proven to be a reliable and efficient tool.

Although conventional risk assessment methods have played an important role in identifying major risks and maintaining safety in process facilities, they have the disadvantage of being static and using generic failure data (Meel & Seider, 2006). So, a probabilistic method based on Bayes' rule, i.e., Bayesian network (BN), has began to become popular among risk society and safety experts. The following sections briefly discuss former methods, mostly known as conventional methods, and the latter method, i.e., BN.

3.2 Conventional Methods

3.2.1 Fault Tree

FT is a deductive, structured methodology to determine the potential causes of an undesired event, referred to as the top event. The top event usually represents a major accident causing safety hazards or economic loss (Lewis, 1994). While the top event is placed at the top of the tree, the tree is constructed downwards, dissecting the system for further detail until the primary events leading to the top event are known. Primary events are considered binary (with two states) and statistically independent In a FT, the relationships between events are represented by means of gates, of which *AND-gates* and *OR-gates* are the most widely used.

Once completed, the FT can be analyzed both qualitatively and quantitatively. In the qualitative evaluation, using Boolean algebra, an expression is derived for the top event in terms of combinations of primary events. In the quantitative part, the probability of the top event is expressed in terms of the occurrence probability of the primary events or in terms of the minimal cut-sets.

Small FTs can be evaluated manually; however, large and complex FTs require the aid of computerized methods for evaluation. Methods for FT analysis include the analytical method, Monte Carlo simulation, and binary decision diagram. Due to limitations in using the Monte Carlo simulation, an analytical approach (e.g., minimal cut-sets determination) is more frequently used for evaluation of a FT. To reduce the margin of error due to inaccuracy and incompleteness of the data of the primary events, some

authors have recently used fuzzy set theory and evidence theory in FT analysis (Ferdous et al., 2009; Lin & Wang, 1997; Markowski et al., 2009; Yuhua & Datao, 2005).

Although having some limitations, FTs are extensively used in the field of risk analysis of process systems (Khan et al., 2001; Ferdous et al., 2009; Ferdous et al., 2007) and fault diagnosis (Khoo et al., 2001; Bartlett et al., 2009; Kavcic and Juricic, 2001). Standard FTs are not suitable for analyzing large systems, particularly if the system presents redundant failures, common cause failures, or mutually exclusive primary events. More importantly, events in a FT are assumed independent, which is not usually a valid assumption (Bobbio et al., 2001; Torres-Toledano and Sucar, 1998; Simon et al., 2007).

3.2.2 Event Tree

ET is an inductive method widely used in quantified risk analysis and safety assessment. ET is used to analyze possible progression routes originating from an initiating event while affected by a sequence of other events commonly placed in chronological order. In safety analysis, ET is used to quantify the probability of possible accident scenarios resulting from the occurrence of a hazardous event, as initiating event. The initiating event's progression can be either mitigated or escalated depending on the successful operation or failure of subsequent safety barriers, respectively. When reaching a safety barrier, ET is usually branched in two; the upward branch denotes the operation of the safety barrier while the lower represent its failure.

ET has been used in the field of accident modeling (Bearfield and Marsh, 2005; Rathnayaka et al., 2011), dynamic failure assessment (Meel and Seider, 2006), and dynamic risk assessment (Kalantarni et al., 2009; Kalantarnia et al., 2010).

3.2.3 Bow-tie

BT is one of the best graphical approaches to represent a complete accident scenario, starting from accident causes and ending with its consequences. While centered on a critical event, BT is composed of a fault tree on the left-hand side identifying the possible events causing the critical event, and an event tree on the right-hand side showing the possible consequences of the critical event based on the failure or success of safety functions (Delvossale et al., 2005; Delvossale et al., 2006). Figure 3.1 shows a typical BT, composing of different components such as primary events (*PE*), intermediate events, (*IE*), the top event, (*TE*), safety barriers, (*SB*), and accident consequences, (*C*).

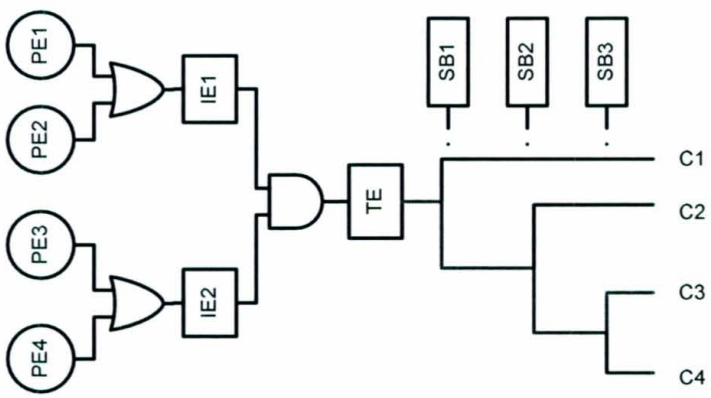


Figure 3.1. Generic Bow-tie model

It helps to understand which possible combination of primary events will lead to the top event in the fault tree and which safety function failures will escalate the top event to a

particular consequence in the event tree. For example, the occurrence probability of consequence $C3$ in Figure 3.1 can be assessed as:

$$\boldsymbol{P(C3) = P(TE)P(SB1)P(SB2)(1 - P(SB3))} \quad \textbf{3.1}$$

Where $P(TE)$ is the top event probability, and $P(SB1)$, $P(SB2)$ and $P(SB3)$ refer to the failure probabilities of $SB1$, $SB2$ and $SB3$, respectively.

BT has been well proven to be a reliable and efficient tool. It has been used in a broad range of applications such as in process safety analysis (Markowski et al., 2009), accident risk assessment (Delvosalle et al., 2005; Delvosalle et al., 2006; Dianous and Fievez , 2006; Gowland 2006), risk management (Cockshott, 2005), and barrier implementation (Badreddine and Ben Amor, 2010).

3.3 Bayesian Methods

3.3.1 Bayes' Theorem

Bayes theory has been usually coupled with conventional methods such as ET (Meel and Seider, 2006; Kalantarnia et al., 2009; Kalantarnia et al., 2010; Rathnayaka et al., 2011) and BT (Badreddine and Ben Amor, 2010; Khakzad et al., 2011) in dynamic risk assessment and safety analysis. Such hybrid methods take advantage of Bayes theory to update initial beliefs or prior probabilities of events using data observed from the accident studied:

$$\boldsymbol{P(x|data) = \frac{P(x)P(data|x)}{P(data)}} \quad \textbf{3.2}$$

Where $P(x)$ is the prior failure probability of event x, $P(data|x)$ is the likelihood function of x, $P(data)$ is the probability of data observed (commonly called as evidence), and $P(x|data)$ is the posterior probability of x. According to Ferson (2005), the estimation of $P(data)$ is probably the most difficult part of the calculation. If the prior and likelihood function are *conjugate* (Ferson, 2005; Meel and Seider, 2006), the posterior distribution would be the same as that of prior, making calculation very easy. For example, if prior probability has a *Beta* distribution (or *Gamma*) and the likelihood function has a *Bernoulli* (or *Poisson*) distribution, the distribution of the posterior will be *Beta* (*Gamma*). However, in the case of non-conjugate distributions, the posterior distribution should be calculated using numerical methods, making the application of the method restricted.

3.3.2 Bayesian Networks

BNs are increasingly used for the construction of system reliability models, risk management, and safety analysis based on probabilistic and uncertain knowledge. Similar to other graphical probabilistic methods (e.g., fault tree and reliability block diagram), BNs consist of both qualitative and quantitative parts. BNs are directed acyclic graphs, in which the nodes represent variables, arcs signify direct causal relationships between the linked nodes, and the conditional probability tables assigned to the nodes specify how strongly the linked nodes influence each other (Torres-Toledano & Sucar, 1998).

In BNs, the nodes without any arc directed into them are called root nodes, possessing marginal prior probabilities. All other nodes are intermediate nodes and each one is assigned a conditional probability table (CPT). Among intermediate nodes, the nodes

having arcs directed into them are called child nodes and the nodes that have arcs directed from them are called parent nodes (Figure 3.2). Each child has an associated CPT, given all combinations of the states of its parent nodes. Nodes without any child are also called leaf nodes.

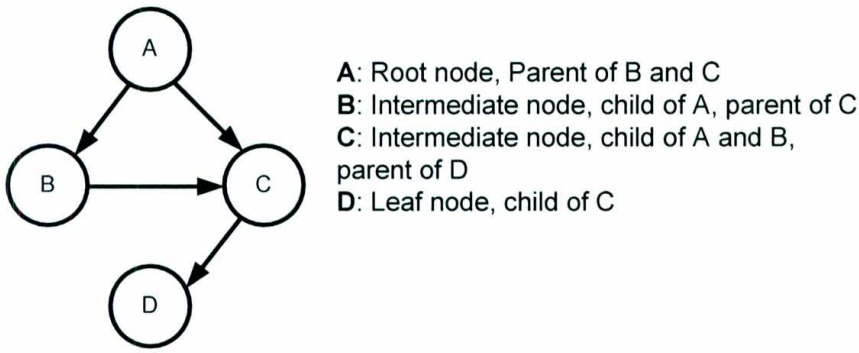


Figure 3.2. Various types of nodes in Bayesian networks

BN takes advantage of the "*d-separation*" criterion (Pearl, 1998; Jensen and Nielsen, 2004; Kjaerulff and Madsen, 2007) and the chain rule to do quantitative analysis. Node A is d-separated from node C if node B blocks the path between A and C. In this case, A is conditionally independent of C given B; i.e., $P(A|B,C) = P(A|B)$. In either a serial path or a diverging path (Figure 3.3a and 3.3b), A and C are d-separated from each other if the state of B is known. In a converging path (Figure 3.3c), A and C are independent if the state of B is unknown. Based on these three conditions, in a BN all root nodes are conditionally independent of each other and the other nodes are conditionally dependent on only their direct parents (Bobbio et al., 2001).

According to the conditional independence and the chain rule, BNs represent the joint probability distribution $P(U)$ of variables $U = \{A_1, A_2, \ldots, A_n\}$ included in the network as:

$$\boldsymbol{P(U) = \prod_{i=1}^{n} P(A_i | Pa(A_i))} \qquad \textbf{3.3}$$

where $Pa(A_i)$ is the parents of A_i in the BN, and $P(U)$ reflects the properties of the BN (Jensen and Nielsen, 2007). Figure 3.3 summarizes the three probabilistic relationships commonly used in a BN (Wilson and Huzurbazar, 2007).

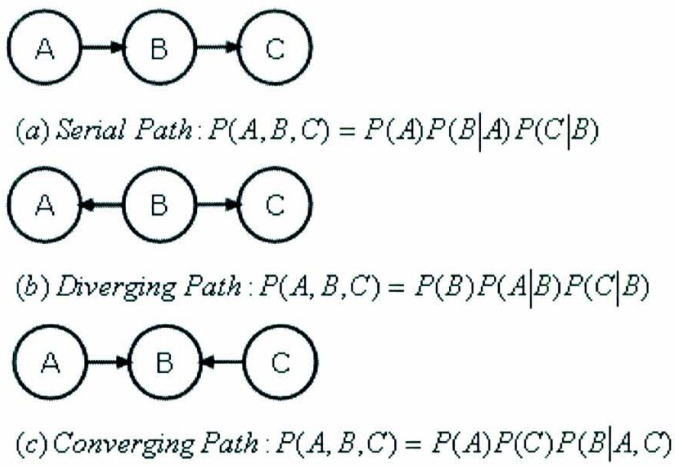


Figure 3.3. Joint probability distributions based on the chain rule and d-separation (Wilson and Huzurbazar, 2007)

Using Equation 3.3, the joint probability distribution of the variables included in the BN in Figure 3.2 would be represented as $P(U) = P(A,B,C,D) = P(A)P(B|A)P(C|A,B)P(D|C)$.

BN's main application in accident analysis is an inference engine for updating the prior occurrence probability of events given new information, called evidence *E*. The new information is usually operational data including occurrence or non-occurrence of the accident or primary events:

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \quad \textbf{3.4}$$

Equation 3.4 can be used for either probability prediction or probability updating. In predictive analysis, conditional probabilities of the form $P(Accident|event)$ are calculated, indicating the occurrence probability of a particular accident given the occurrence or non-occurrence of a certain primary event. On the other hand, in updating analysis, those of the form $P(event|Accident)$ are evaluated, showing the occurrence probability of a particular event given the occurrence of a certain accident (Przytula and Thompson, 2000).

BNs are increasingly used in reliability assessment (Langseth & Portinale, 2007; Mahadevan et al., 2001; Torres-Toledano & Sucar, 1998; Wilson & Huzurbazar, 2007), fault diagnosis (Przytula & Thompson, 2000; Huang et al., 2008), and updating the failure probability of safety systems (Giribone & Valette, 2004). Boudali and Dugan (2005) have examined the parallels between BNs and FTs and have shown the obvious superiority of BNs over FTs in terms of modeling and analysis capabilities. Bobbio et al. (2001) showed that the limitations of FTs can be relaxed to a great extent by relying on BNs. Other relevant works have been done by either mapping static FTs to BNs (Simon et al., 2007; Graves et al., 2007; Lampis and Andrews, 2009; Khakzad et al, 2011) or mapping dynamic FTs into the corresponding dynamic BNs (Montani et al., 2008;

Montani et al., 2006; Boudali and Dugan, 2005). A comprehensive review of Bayesian network application in risk analysis, safety assessment, and reliability engineering can be found in Weber et al. (2010).

3.3.3 Dynamic Bayesian Networks

Dynamic fault tree (DFT) was introduced as an extension to SFT to model sequentially dependent failures in dynamic systems (Dugan et al. 1992). In a dynamic system, the failure sequence of events is as important as their combinations for the system to be unavailable or to fail. In other words, compared to SFT in which it only matters which components participate in a minimal cut set, in DFT the failure sequence of the participating components is also important (Boudali and Dugan, 2005a). DFT takes the sequential dependencies into account by using several dynamic gates such as a functional dependency gate (FDEP), cold spare gate (CSP), sequence enforcing gate (SEQ) (Dugan et al., 1992) and priority-AND gate (PAND) (Fussel et al., 1976).

Due to the sequential dependencies and dynamic behavior among the components of the system, DFT cannot be analyzed using conventional algorithms available for SFT. In this regard, DFT has traditionally been converted to the corresponding Markov chain model (MC) for which well-established and efficient solving techniques have been developed. Nevertheless, converting DFT into MC is an error-prone and cumbersome exercise (Dugan et al., 1992). Moreover, the state space of the MC (i.e., the set of its nodes) grows exponentially with the number of components of the corresponding DFT, making the MC very large and intractable. Indeed, for a MC equivalent to a DFT with m binary-state components (i.e., work/fail) for which k out of m components are sequentially dependent,

the number of states is proportional to the product of 2^m (the number of state combinations) and k! (the possible number of sequence combinations) (Boudali and Dugan, 2005b). This problem is frequently encountered in Markov processes and is referred to as the state space explosion. It should be noted that even a relatively simple DFT can result in a complicated and time-consuming MC, particularly in the presence of dynamic gates cascade (Boudali and Dugan, 2005b; Dugan et al., 1992; Boudali and Dugan, 2005a; Marquez et al., 2010). Also, MC has been mentioned to have limitations in modeling dependencies among components with non-exponential failure time distributions (Marquez et al., 2010).

Considering the abovementioned problems encountered in converting DFT into MC, temporal Bayesian networks (TBNs) have alternatively been proposed to explicitly incorporate time in the modeling of sequential dependencies without resort to MC. Accordingly, two different approaches have been adopted: instant-based (time-sliced) approach and interval-based (event-based) approach (Boudali and Dugan, 2006). In the first approach, the time line is divided into a finite number of time instants (e.g., t_{i-1}, t_i, t_{i+1}), and identical BN structures are generated for each time instant, connected to each other by means of temporal arcs (e.g., Montani et al., 2008; Portinale et al., 2010). In the second approach, the time line is partitioned into a finite number of time intervals (e.g., $]t_{i-1}, t_i],]t_i, t_{i+1}]$), and only one BN is generated, each node of which has a finite number of states equal to the number of time intervals (Boudali and Dugan, 2005b; Marquez et al., 2010; Boudali and Dugan, 2006).

Following the instant-based approach, Montani et al. (2008) developed the RADYBAN software tool for reliability analysis of dynamic systems by converting DFT into a 2-time-slice BN. They also introduced the probability dependency gate (PDEP) as a probabilistic case of FDEP proposed by Dugan et al. (1992). Their work was further developed by Portinale et al. (2010), enabling the modeling of repairable systems by introducing the repair box gate. The instant-based approach has been criticized for either being too general or resulting in unnecessarily large networks due to repeating the same structure for each time instance (Boudali and Dugan, 2005b). However, 2TBN as an instant-based approach models any time horizon using only 2 slices, effectively addressing the foregoing drawback (Montani et al., 2008; Portinale et al., 2010).

3.4 References

Badreddine, A., & Ben Amor, N. (2010). A dynamic barriers implementation in Bayesian-based bow tie diagrams for risk analysis. Proceedings of International Conference on Computer Systems and Applications, 1-8.

Bartlett, L.M, Hurdle, E.E., & Kelly E.M. (2009). Integrated system fault diagnostics utilizing diagraph and FT-based approach. Journal of Reliability Engineering and System Safety, 94, 1107-1115.

Bearfield G, Marsh W. Generalizing event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science 2005; 3688: 52-66.

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Reliability Engineering and System Safety 2001; 71: 249-60.

Boudali H, Dugan JB. A new Bayesian approach to solve dynamic FTs. Proceedings of Reliability and Maintainability Symposium (RAMS 05) 2005a: 451-6.

Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 2005b; 87: 337-49.

Boudali H, Dugan JB. A continuous-time Bayesian network reliability modeling and analysis framework. IEEE Transaction on Reliability 2006; 55: 86-97.

Cockshott, J.E. (2005). Probability bow-ties a transparent risk management tool. Process Safety and Environmental Protection, 83, 307-316.

Delvosalle, C., Fievez, C., Pipart, A., Casal Fabrega, J., Planas, E., Christou, M., and Mushtaq, F. (2005). Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety, 90, 238-246.

Delvosalle C, Fievez C, Pipart A, Debray B. ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. Journal of Hazardous Materials 2006; 130: 200-19.

Dianous V.D., & Fievez, C. (2006). ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. Journal of Hazardous Materials, 130, 220-233.

Dugan JB, Bavuso SJ, Boyd MA. Dynamic fault tree models for fault tolerant computer systems. IEEE Transaction on Reliability 1992; 41: 363-77.

Ferdous, R., Khan, F.I., Veitch, B., & Amyotte, P. (2007). Methodology for computer-aided FT analysis. Process Safety and Environmental Protection, 85, 70-80.

Ferdous, R., Khan, F.I., Veitch, B., & Amyotte, P. (2009). Methodology for computer aided fuzzy FT analysis. Journal of Process safety and Environmental Protection, 87, 217-226.

Ferson, S. (2005). Bayesian methods in risk assessment. Unpublished report prepared for the Bureau de Recherches Geologiques et Minieres (BRGM), New York.

Fussell JB, Aber EF, Rahl RG. On the quantification analysis of priority-AND failure logic. IEEE Transaction on Reliability 1976; 25: 324-26.

Giribone, R., & Valette, B. (2004). Principles of failure probability assessment (PoF). International Journal of Pressure Vessels and Piping, 81, 797-806.

Gowland, R. (2006). The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: a step forward towards convergent practices in risk assessment?. Journal of Hazardous Materials, 130, 307-310.

Huang, Y., McMurran, R., Dhadyalla, G., & Jones, R.P. (2008). Probability based vehicle fault diagnosis: Bayesian network method. Journal of Intelligent Manufacturing, 19, 301-311.

Jensen FV, Nielsen TD. Bayesian networks and decision graphs. 2nd ed. New York: Springer; 2007.

Kalantarnia, M., Khan, F., & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. Journal of Loss Prevention in the Process Industries, 22, 600-606.

Kavcic, M., & Juricic, D. (2001). CAD for FT-based diagnosis of industrial processes. Journal of Engineering Application of Artificial Intelligence, 14, 203-216.

Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety 2011; 96: 925-32.

Khan, F., & Abbasi, S. A. (1998). Techniques and methodologies for risk analysis in chemical process industries. Journal of Loss Prevention in the Process Industries, 11, 261-277.

Khan, F.I. (2001). Use maximum-credible accident scenarios for realistic and reliable risk assessment. Chemical Engineering Progress, 11, 56-64.

Khan, F.I., Sadiq, R., & Husain, T. (2001). Risk-based process safety assessment and control measures design for offshore process facilities. Journal of Hazardous Materials, A94, 1-36.

Khoo, L.P., Tor, S.B., & Li, J.R. (2001). A rough set approach to the ordering of basic events in a FT for fault diagnosis. International Journal of Advanced Manufacturing Technology, 17, 769-774.

Kjaerulff, U.B., & Madsen, A.L. (2007). Bayesian networks and influence diagrams A guide to construction and analysis. New York, Springer.

Lampis, M., & Andrews, D. (2009). Bayesian belief networks for system fault diagnostics. International Journal of Quality and Reliability Engineering, 25, 409-426.

Langseth H, Portinale L. Bayesian networks in reliability. Reliability Engineering and System Safety 2007; 92: 92-108.

Lewis, E.E. (1994). Introduction to reliability engineering. 2nd edition, New York, John Wiley& Sons.

Lin, C.-T., & Wang, M.-J.J. (1997). Hybrid FT analysis using fuzzy sets. Journal of Reliability Engineering and System Safety, 58, 205-123.

Mahadevan, S., Zhang, R., & Smith, N. (2001). Bayesian networks for system reliability reassessment. Journal of Structural Safety, 23, 231-251.

Markowski, A.S., Mannan, M.S., & Bigoszewska, A. (2009). Fuzzy logic for process safety analysis. Journal of Loss Prevention in the Process Industries, 22, 695-702.

Marquez D, Neil M, Fenton N. Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering and System Safety 2010; 95: 412-25.

Meel, A., & Seider, W. D. (2006). Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science, 61, 7036-7056.

Montani, S., Portinale, L., Bobbio, A., & Codetta-Raiteri, D. (2006). Automatically translating dynamic FTs into dynamic Bayesian networks by means of a software tool. Proceedings of Reliability and Maintainability Symposium (RAMS'06), 434-441.

Montani S, Portinale L, Bobbio A, Codetta-Raiteri D. RADYBAN: a tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks. Reliability Engineering and System Safety 2008; 93: 922-32.

Pearl, J. (1988). Probabilistic Reasoning in Intelligent Systems, Morgan Kaufmann, San Francisco, California. ISBN 0-934613-73-7.

Portinale L, Codetta-Raiteri D, Montani S. Supporting reliability engineers in exploiting the power of dynamic Bayesian networks. International Journal of Approximate Reasoning 2010; 51: 179-95.

Przytula, K.W., & Thompson, D. (2000). Construction of Bayesian networks for diagnostics. Proceedings of IEEE Aerospace Conference, 5, 193-200.

Rathnayaka, S., Khan, F., & Amyotte, P. (2011). SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study. Process Safety and Environmental Protection, 89, 75-88.

Simon, C., Weber, P., & Levrat, E. (2007). Bayesian networks and evidence theory to model complex systems reliability. Journal of Computers, 2, 33-43.

Torres-Toledano JG, Sucar LE. Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science 1998; 1484: 195-206.

Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2010). Overview on Bayesian networks applications for dependability, risk analysis, and maintenance areas. Engineering Application of Artificial Intelligence, doi: 10.1016/j.engappai.2010.06.002.

Wilson, A.G., & Huzurbazar, A.V. (2007). Bayesian networks for multilevel system reliability. Journal of Reliability Engineering and System Safety, 92, 1413-1420.

Yuhua, D., & Datao, Y. (2005). Estimation of failure probability of oil and gas transmission pipelines by fuzzy FT analysis. Journal of Loss Prevention in the Process Industries, 18, 83-88.

4 Safety Analysis in Process Facilities: Comparison of Fault Tree and Bayesian Network Approaches*

Preface

A version of this manuscript has been published in the *Journal of Reliability Engineering and System Safety*. The co-authors, Dr Khan and Amyotte supervised the principal author, Khakzad, to develop the research on the entitled topic and helped him to conceptualize the techniques and theories available for this topic. Khakzad conducted accident modeling and associated analyses while Khan and Amyotte reviewed the manuscript and provided the necessary suggestions.

Abstract

Dynamic safety analysis in gas process facilities is necessary to prevent unwanted events that may cause catastrophic accidents. Accident scenario analysis with probability updating is the key to dynamic safety analysis. Although conventional failure assessment techniques such as fault tree (FT) have been used effectively for this purpose, they suffer severe limitations of static structure and uncertainty handling, which are of great significance in process dynamic safety analysis. Bayesian network (BN) is an alternative technique with ample potential for application in safety analysis. BNs have a strong similarity to FTs in many respects; however, the distinct advantages making them more suitable than FTs are their ability in explicitly representing the dependencies of events,

---

* Khakzad et al. Journal of Reliability Engineering and System Safety 2011.

updating probabilities, and coping with uncertainties. The objective of this paper is to demonstrate the application of BNs in dynamic safety analysis of process systems. The first part of the paper shows those modeling aspects which are common between FT and BN, giving preference to BN due to its ability to update probabilities. The second part is devoted to various modeling features of BN, helping to incorporate multi-state variables, dependent failures, functional uncertainty, and expert opinion which are frequently encountered in safety analysis, but cannot be considered by FT. The paper concludes that BN is a superior technique in dynamic safety analysis because of its flexible structure, allowing it to fit a wide variety of accident scenarios.

Keywords: Bayesian network, Fault tree analysis, Dynamic accident analysis, Uncertainty modeling.

4.1 Introduction

Safety analysis is very important in gas process facilities as they deal with a large amount of flammable chemicals; also, process areas are congested with complex piping, high-pressure compressors, and separators of which malfunctions and mishaps may lead to catastrophic accidents (Khan et al., 2001; Torres-Toledano and Sucar, 1998).

There have been many fatal explosions and fires imposing major capital loss and considerable death toll in the past two decades. On 23 March 2005, the BP refinery explosion in Texas City caused 15 deaths and more than 170 injuries (CNN, 2005). According to the final report issued by BP (2005), a lack of process safety measures and insufficient risk reduction measures were entirely to blame for the accident. On 7 February 2010, the Kleen Energy power plant exploded in Middletown, Connecticut,

U.S., killing 6 and injuring at least 12. The explosion was one of the worst industrial disasters in the U.S. in recent years (Reuters, 2010a). Most recently, on 20 April 2010, explosion and fire on Transocean Ltd's drilling rig killed 11 and injured 17 in the Gulf of Mexico. The failure of a blowout preventer has been determined as the primary cause of the accident (Reuters, 2010b). It is important to broaden the risk analysis scope by considering accident scenario and real-time safety analysis in order to predict and continuously update the likelihood of catastrophic accidents and to take actions to prevent them.

Forecasting likely accident scenarios is the most important step in safety analysis. Khan (2001) proposed a "maximum credible accident scenario" approach that short-lists the important scenarios based on both their consequences and the likelihood of accident occurrence. Delvosalle et al. (2006) used two methodologies: MIMAH for the identification of major accident hazards, in which no safety system was considered, and MIRAS for the identification of reference accident scenarios, in which all the actual safety functions and barriers were included in the analysis. The next step in safety analysis is to quantify the occurrence probability of the selected accident scenarios. For this, there are many techniques available, among which fault tree (FT) is very popular.

Although having some limitations, FTs are extensively used in the field of risk analysis of process systems (Khan et al., 2001; Ferdous et al., 2009; Ferdous et al., 2007) and fault diagnosis (Khoo et al., 2001; Bartlett et al., 2009; Kavcic and Juricic, 2001). Standard FTs are not suitable for analyzing large systems, particularly if the system presents redundant failures, common cause failures, or mutually exclusive primary events. More

importantly, events in a FT are assumed independent, which is not usually a valid assumption (Bobbio et al., 2001; Torres-Toledano and Sucar, 1998; Simon et al., 2007).

In recent years, a Bayesian Network (BN) methodology has begun to be used in engineering applications. A BN is a graphical inference technique used to express the causal relationships among variables. BNs are used either to predict the probability of unknown variables or to update the probability of known variables given the certain state of other variables (evidence) through the process of probability propagation or reasoning. The reasoning is based on Bayes' theorem. Due to this ability, BNs have provided a promising framework for system safety analysis and risk management (Mahadevan et al., 2001).

BNs are increasingly used in reliability assessment (Langseth & Portinale, 2007; Mahadevan et al., 2001; Torres-Toledano & Sucar, 1998; Wilson & Huzurbazar, 2007), fault diagnosis (Przytula & Thompson, 2000; Huang et al., 2008), and updating the failure probability of safety systems (Giribone & Valette, 2004). Boudali and Dugan (2005) have examined the parallels between BNs and FTs and have shown the obvious superiority of BNs over FTs in terms of modeling and analysis capabilities. Bobbio et al. (2001) showed that the limitations of FTs can be relaxed to a great extent by relying on BNs. Other relevant works have been done by either mapping static FTs to BNs (Simon et al., 2007; Graves et al., 2007; Lampis and Andrews, 2009) or mapping dynamic FTs into the corresponding dynamic BNs (Montani et al., 2008; Montani et al., 2006; Boudali and Dugan, 2005).

Many authors have investigated different techniques in accident scenario analysis, very few of whom have used BNs in their work. Sklet (2004) qualitatively compared some commonly used methods such as FT analysis, event tree analysis, and barrier analysis for accident analysis. The comparison was made based on criteria such as graphical representation and the ability to support safety barriers. Nivolianitou et al. (2004) used FT, event tree, and Petri nets for a qualitative accident scenario analysis in an ammonia storage plant, concluding that Petri nets are able to incorporate the evidence through scenario analysis and thus are more appropriate for dynamic accident analysis. Zheng and Liu (2009) made a comparison among some widely used methods for accident forecasting. Although FT as a scenario analysis method and BN were briefly discussed, the main focus in their research was devoted to methods such as regression models, time-series methods, and neural networks.

Most recently, Weber et al. (2010) gave an exhaustive statistical review of BN application in different areas such as risk and maintenance analysis, in which BN was qualitatively compared with other methods such as FTs, Markov chains and Petri nets. The present work is aimed at showing the parallels between FTs and BNs in the specific area of accident modeling and process safety analysis, which have not been studied thus far. The paper also discusses the modeling potential offered by BNs, making them a superior method compared to FTs for dynamic safety analysis.

A brief description of the fundamentals of FTs, BNs, and the mapping algorithm are presented in section 4.2. The comparison of the two methods is done in section 4.3, where a simple accident scenario is modeled using both methods. Section 4.4 is devoted

to the application of BN to more complicated scenarios which cannot be modeled using FTs. The conclusions and recommendations for future work are presented in section 4.5.

4.2 Failure Analysis Techniques

Many approaches have been developed for accident analysis, among which FT analysis is the most common. Recently BNs have drawn much attention. In the subsequent subsections, both approaches are described, and the mapping algorithm from FT to BN is recapitulated.

4.2.1 Fault Tree

FT is a deductive, structured methodology to determine the potential causes of an undesired event, referred to as the top event. The top event usually represents a major accident causing safety hazards or economic loss (Lewis, 1994). While the top event is placed at the top of the tree, the tree is constructed downwards, dissecting the system for further detail until the primary events leading to the top event are known. Primary events are considered binary (with two states) and statistically independent In a FT, the relationships between events are represented by means of gates, of which AND-gates and OR-gates are the most widely used.

Once completed, the FT can be analyzed both qualitatively and quantitatively. In the qualitative evaluation, using Boolean algebra, an expression is derived for the top event in terms of combinations of primary events. In the quantitative part, the probability of the top event is expressed in terms of the occurrence probability of the primary events or in terms of the minimal cut-sets.

Small FTs can be evaluated manually; however, large and complex FTs require the aid of computerized methods for evaluation. Methods for FT analysis include the analytical method, Monte Carlo simulation, and binary decision diagram. Due to limitations in using the Monte Carlo simulation, an analytical approach (e.g., minimal cut-sets determination) is more frequently used for evaluation of a FT. To reduce the margin of error due to inaccuracy and incompleteness of the data of the primary events, some authors have recently used fuzzy set theory and evidence theory in FT analysis (Ferdous et al., 2009; Lin & Wang, 1997; Markowski et al., 2009; Yuhua & Datao, 2005).

4.2.2 Bayesian Network

BNs are increasingly used for the construction of system reliability models, risk management, and safety analysis based on probabilistic and uncertain knowledge. Similar to FTs, BNs consist of both qualitative and quantitative parts. BNs are directed acyclic graphs, in which the nodes represent variables, arcs signify direct causal relationships between the linked nodes, and the conditional probability tables assigned to the nodes specify how strongly the linked nodes influence each other (Torres-Toledano & Sucar, 1998).

BN takes advantage of the "d-separation" criterion (Jensen and Nielsen, 2004) and the chain rule to perform quantitative analysis. Based on d-separation criteria, all root nodes are conditionally independent and the other nodes are conditionally dependent on only their direct parents (Bobbio et al., 2001).

According to the conditional independence and the chain rule, BNs represent the joint probability distribution $P(U)$ of variables $U = \{A_1, A_2, \dots, A_n\}$ included in the network as:

$$\boldsymbol{P(U) = \prod_{i=1}^{n} P(A_i|Pa(A_i))} \quad \textbf{4.1}$$

Where $Pa(A_i)$ are the parents of A_i in the BN, and $P(U)$ reflects the properties of the BN (Jensen and Nielsen, 2007).

BNs' main application in accident analysis is an inference engine for updating the prior occurrence probability of events given new information, called evidence E. The new information is usually operational data including occurrence or non-occurrence of the accident or primary events:

$$\boldsymbol{P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)}} \quad \textbf{4.2}$$

Equation 4.2 can be used for either probability prediction or probability updating. In predictive analysis, conditional probabilities of the form $P(Accident|event)$ are calculated, indicating the occurrence probability of a particular accident given the occurrence or non-occurrence of a certain primary event. On the other hand, in updating analysis, those of the form $P(event|Accident)$ are evaluated, showing the occurrence probability of a particular event given the occurrence of a certain accident (Przytula and Thompson, 2000).

4.2.3 Mapping Fault Trees to Bayesian Networks

A mapping algorithm includes graphical and numerical tasks. In graphical mapping, primary events, intermediate events, and the top event of the FT are represented as root

nodes, intermediate nodes, and the leaf node in the corresponding BN, respectively. The nodes of a BN are connected in the same way as corresponding components in the FT. In numerical mapping, the occurrence probabilities of the primary events are assigned to the corresponding root nodes as prior probabilities. For each intermediate node as well as leaf node, a CPT (Conditional Probability Table) is developed. The CPTs are developed according to the type of gate (Bobbio et al., 2001; Lampis and Andrews, 2009). Figure 4.1 illustrates the simplified procedure of mapping FTs into BNs.

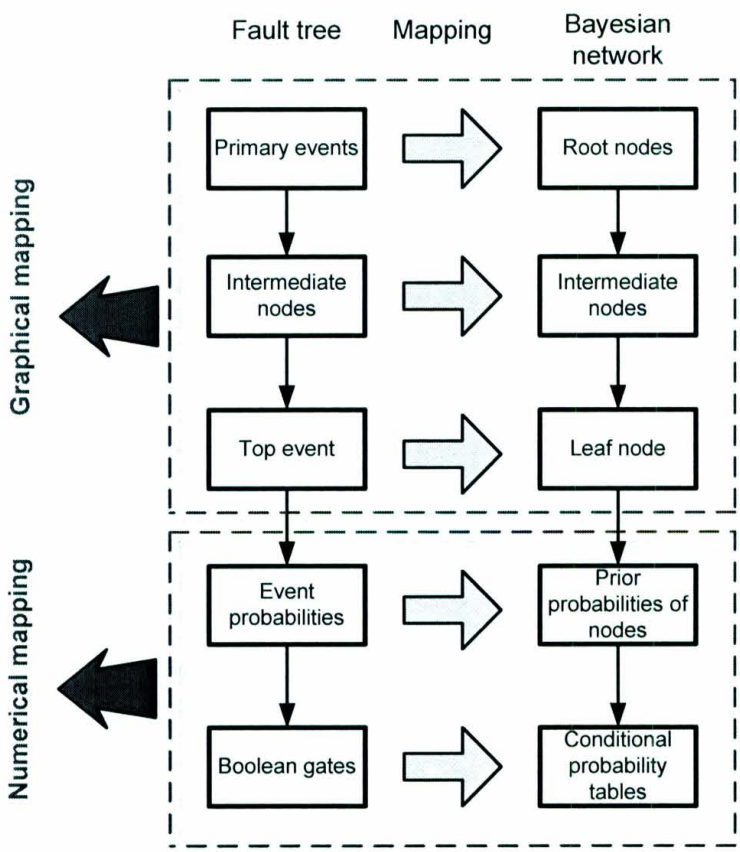


Figure 4.1. Mapping fault tree into Bayesian network

4.3 Safety Analysis

4.3.1 Case Study

The performance of a feeding control system transferring propane from a propane evaporator to a scrubbing column is selected to illustrate the methodology for the purpose of safety analysis. To maintain a specified pressure inside the scrubbing column, the feed pipeline is equipped with an automatic valve operated by an actuator. Immediate and proper functioning of the actuator depends on a pressure relay and signals that are received from a pressure controller via a pressure transmitter. A manual valve is also considered to avoid pressure increase in case of malfunction of the automatic valve. All components are assumed binary (Work/Fail). The occurrence frequency data of primary events that would contribute to the occurrence of this accident scenario is presented in Table 4.1, while intermediate events and the top event have been identified by the type of gates leading to these events.

Table 4.1. Different events related to an accident scenario in the feed control system and their occurrence probabilities

Number	Component	Symbol	Probability
1	Pressure transmitter failure	PT	0.1647
2	Pressure controller failure	PC	0.2818
3	No signal received by pressure controller	PC_signal	OR-gate
4	Pressure relay failure	PY	0.1538
5	No signal received by actuator	Act_signal	OR-gate
6	Automatic valve mechanical failure	A_valve	0.3403
7	Actuator mechanical failure	Actuator	0.2015

8	Automatic valve improper control	A_valve_ctrl	OR-gate
9	Human failure in operating manual valve	Hum_error	0.2696
10	Manual valve mechanical failure	M_valve	0.1393
11	Manual valve improper control	M_valve_ctrl	OR-gate
12	Feed system improper control	Feed_ctrl	AND-gate

4.3.2 Fault Tree Analysis

Considering the behavior of the components and the intermediate events, the FT is constructed as shown in Figure 4.2. Occurrence probabilities presented in Table 4.1 are then assigned to each primary event. Considering the probabilities, the prior probability of the top event is calculated as 0.2720.

For comprehensive accident scenario analysis and effective safety decision-making, it is necessary to determine the critical primary events and also minimal cut-sets leading to the top event occurrence (Lewis, 1994). To this end, the contribution of each event (e.g., C_i) is estimated by repeating the FT analysis while keeping that particular event absent, i.e. $P(C_i = 1) = 0$. Subsequently, the contribution of each event is transformed into an "*improvement index*" (Khan et al., 2001) that signifies the percent contribution of that event in leading to the top event (Table 4.2). The higher the index of an event, the more vulnerable it is in leading to the top event. As may be noticed in Table 4.2, events C_9, C_{10}, C_6, and C_2 have the highest improvement indices (components are numbered according to Table 4.1). Therefore, in order to improve the safety of the system these events are considered first.

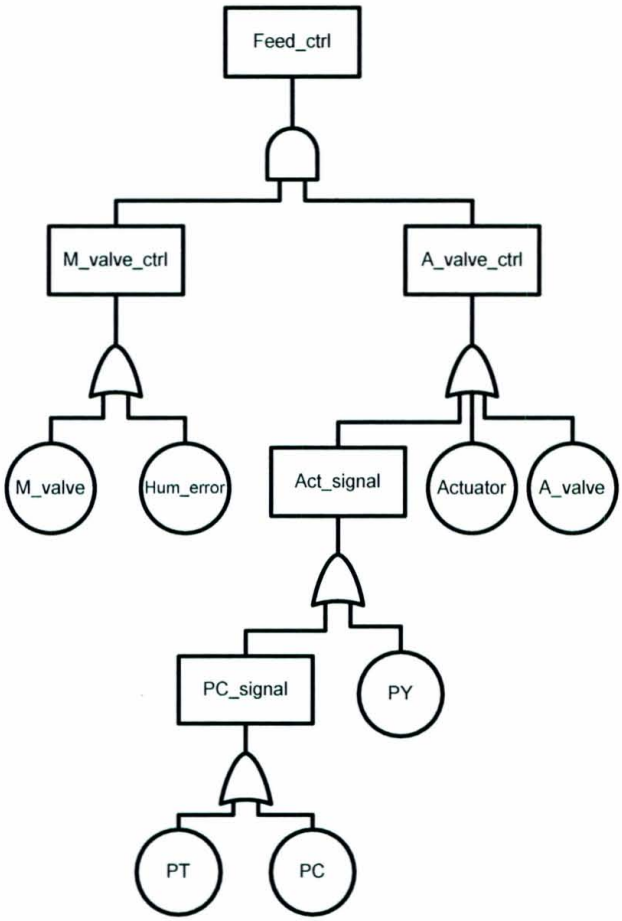


Figure 4.2. Fault tree for malfunction of the Feed system

Table 4.2. Top event probability and improvement indices for FT and BN analysis

	Fault Tree Analysis		Bayesian Network Analysis	
Event not occurring	Probability	Improvement Index (%)	Probability	Improvement Index (%)
0	0.2720	0.0	0.2720	0.0
C_1	0.2525	5.2	0.2525	5.2
C_2	0.2331	10.5	0.2331	10.5
C_4	0.2540	4.8	0.2540	4.8

C_6	0.2208	13.8	0.2208	13.8
C_7	0.2470	6.7	0.2470	6.7
C_9	0.1020	45.7	0.1020	45.7
C_{10}	0.1975	20.0	0.1975	20.0

The FT in Figure 4.2 may be expressed as the union of 10 minimal cut-sets:

$$\boldsymbol{TE = M_1 \cup M_2 \cup \ldots \cup M_{10}} \qquad \textbf{4.3}$$

Where M_i represents the *ith* minimal cut-set. Each minimal cut-set consists of the intersection of the minimal number of primary events required to cause the top event:

$$\boldsymbol{M = C_i \cap C_j} \begin{cases} \boldsymbol{i = 1, 2, 4, 6, 7} \\ \boldsymbol{j = 9, 10} \end{cases} \qquad \textbf{4.4}$$

Knowing the minimal cut-sets, the following considerations would be of great help (Lewis 1994):

Rank of each minimal cut-set defined by the number of its primary events. This would help to identify the shortest path in accident causation and consequently help to devise measures against such an occurrence.

This would help to identify the most probable minimal cut-set in the accident causation sequence. The cut-set importance for the *ith* minimal cut-set is defined as:

$$\boldsymbol{IM_i = \frac{P(M_i)}{P(TE)}} \qquad \textbf{4.5}$$

If each event C_i has the probability of occurrence $P(C_i)$, the probability of the cut-set is defined as:

$$\boldsymbol{P(M) = \prod_{i \in M} P(C_i)} \qquad \textbf{4.6}$$

Equation 4.6 implies that the primary events included in the minimal cut-set are assumed independent. It is important to note that $P(C_i)$ refers to the prior occurrence probability of each event; therefore, Equation 4.6 yields a prior importance. According to the above discussion, all minimal cut-sets of the FT in Figure 4.2 are twines, that is, they all consist of two events; therefore, all of them are of the same ranking. Also, the most important minimal cut-set is $M = C_6 \cap C_9$ with IM=0.3373, showing that mechanical failure of automatic valve (*A_valve*) and failure of the operator to close the manual valves (*Hum_error*) are the likely explanations for system failure.

4.3.3 Bayesian Network Analysis

Using the algorithm described in section 4.2.3, the Bayesian network is constructed for the accident scenario in the feed control system (Figure 4.3). Once developed, BN is analyzed using HUGIN 7.3 (http://www.hugin.com).

The prior probability of the leaf node in the BN is calculated to be *P*(*Feed_ctrl*)=0.2720, which is the same as that of the FT. The improvement indices are estimated for each event (Table 4.2) by instantiating that particular event (i.e., $C_i = 0$) and subsequently calculating the conditional probability $P(Feed\_ctrl|C_i = 0)$. As shown in Table 4.2, the events C_9, C_{10}, C_6, and C_2 are again identified to contribute most to the leaf node (*Feed_ctrl*).

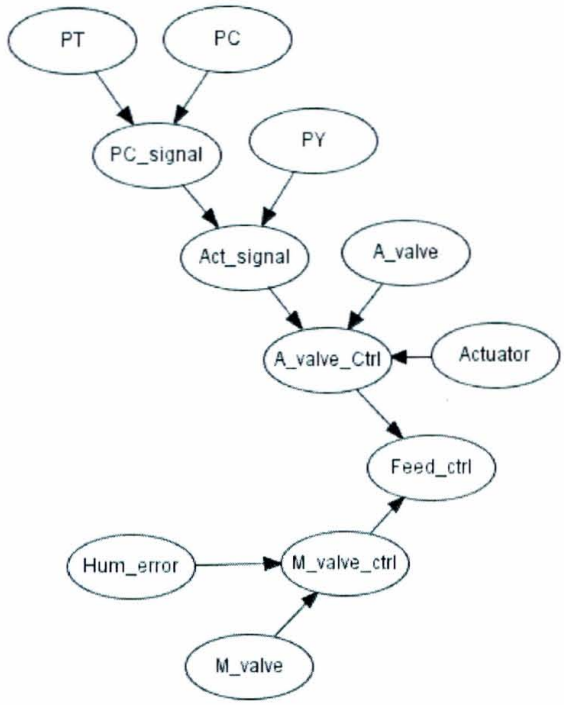


Figure 4.3. Bayesian network structure based on the fault tree in Figure 4.2

It is worth noting that during predictive analysis to calculate the scenario occurrence probability (*deductive reasoning*), the BN provides similar results to those of the traditional FT as long as primary events are independent of each other. However, one of the unique characteristics of BN for dynamic accident scenario analysis is its ability for *abductive reasoning*, aimed at updating the occurrence probability of the primary events given the occurrence of the accident precursors. (Kjaerulff & Madsen, 2005). Throughout abductive reasoning, two inherent features of BNs are revealed, i.e., probability updating and uncertainty reducing, both of which are of great importance in dynamic safety analysis.

Although some authors have combined FTs with other methods to accommodate the two aforementioned features, these methods are to be implemented under specific conditions, making their application limited in accident scenario and safety analysis. For instance, Shalev & Tiran (2007) coupled FT analysis with condition monitoring to obtain an up-to-date FT. Also, Ferdous et al. (2010) and Markowski et al. (2009) have equipped FTs with fuzzy theory and evidence theory to cope with parameter uncertainty due to using data obtained from similar accidents or expert knowledge.

On the other hand, BNs are naturally able to reduce parameter uncertainty through probability updating. In BN analysis, the posterior probabilities reflect the characteristics of the accident studied more specifically than prior probabilities and hence are less uncertain. This is because posteriors, unlike priors, are probabilities that have been updated using the accident's latest information. BN can repetitively substitute the posteriors for priors in the accident re-analysis when a new set of accident-related information is observed. This substitution not only continuously reduces the data uncertainty, but it also provides the accident scenario with real-time and up-to-date analysis.

4.3.4 Probability Updating

Beyond the usual measures available in FTs, BN is able to perform probability updating analysis, given new observations (Bobbio et al., 2001). In this regard, the computation of the posterior marginal probabilities of root nodes given the scenario occurrence is the most popular (i.e., abductive reasoning). To this end, the posterior probability of each

root node C_i is calculated using $P(C_i|Feed\_ctrl)$, indicating the probability of C_i conditioned to the *Feed_ctrl* malfunction (column 4 of Table 4.3).

It may be observed from Table 4.3 that the occurrence probability of the events C_9, C_{10}, and C_{11} had the highest increase. Also, event severity ranking based on posteriors is different from that based on priors. Based on the event posterior probabilities, the most important minimal cut-set is defined as $M = C_6 \cap C_9$ (the same as in the FT) with the posterior importance index as IM=0.3372. It is to be noted that in the calculation of the posterior importance index, $P(Feed_{ctrl}) = 1$ is considered.

The posterior joint probability of all the primary events given the accident occurrence is much more helpful than the most important minimal cut-set if a precise and comprehensive safety analysis is desired. This is because the latter does not provide any information about the occurrence or non-occurrence of the primary events not included in it (Bobbio et al., 2001).

To determine the most probable state of all the variables given the accident occurrence, *the most probable configuration*, the BN searches over the state space of each variable to identify weak links. Using the most probable explanation concept, the most probable state given the accident occurrence is the one corresponding to the occurrence of the primary events C_6, C_9, and C_{10}, and the non-occurrence of the other primary events: $P(\bar{C}_1, \bar{C}_2, \bar{C}_4, C_6, \bar{C}_7, C_9, C_{10}|Feed_{ctrl}) = 0.1179$

It is important to note that unlike the posterior minimal cut-set, which identifies C_6 and C_9 as the most likely causes for system failure, the most probable explanation provides more information by adding C_{10} to the foregoing set. Also, it implies that the other non-

mentioned events do not contribute to system failure. In this regard, using BN in safety analysis helps to identify critical events and allocate preventative safety barriers not only to the primary events directly leading to the top event but also to weak links (combination of non-critical events).

Table 4.3. Comparison between prior and posterior probabilities in different modeling steps

		First Modeling		Alarm Modeling		Uncertainty Modeling	
Number	Component	Prior	Posterior	Prior	Posterior	Prior	Posterior
1	PT	0.1647	0.2248	0.1647	0.2248	0.1647	0.2186
2	PC	0.2818	0.3847	0.2818	0.3847	0.2818	0.3687
3	PC_signal	0.4001	0.5461	0.4001	0.5461	0.3117	0.4496
4	PY	0.1538	0.2099	0.1538	0.2099	0.1538	0.2219
5	Act_signal	0.4924	0.6721	0.4924	0.6721	0.4175	0.6024
6	A_valve	0.3403	0.4645	0.3403	0.4645	0.3403	0.4909
7	Actuator	0.2015	0.2751	0.2015	0.2751	0.2015	0.2907
8	A_valve_ctrl	0.7326	1.0000	0.7326	1.0000	0.6932	1.0000
9	Hum_error	0.2696	0.7260	0.2696	0.1272	0.3112	0.1907
10	M_valve	0.1393	0.3751	0.1393	0.8905	0.1393	0.8359
11	M_valve_ctrl	0.3713	1.0000	0.3713	1.0000	0.4017	1.0000
12	Feed_ctrl	0.2720	1.0000	0.1146	1.0000	0.1155	1.0000
13	Alarm			0.2614, 0.0134	0.0639, 0.0000	0.3031, 0.0190	0.1302, 0.0000

4.4 Modeling Techniques

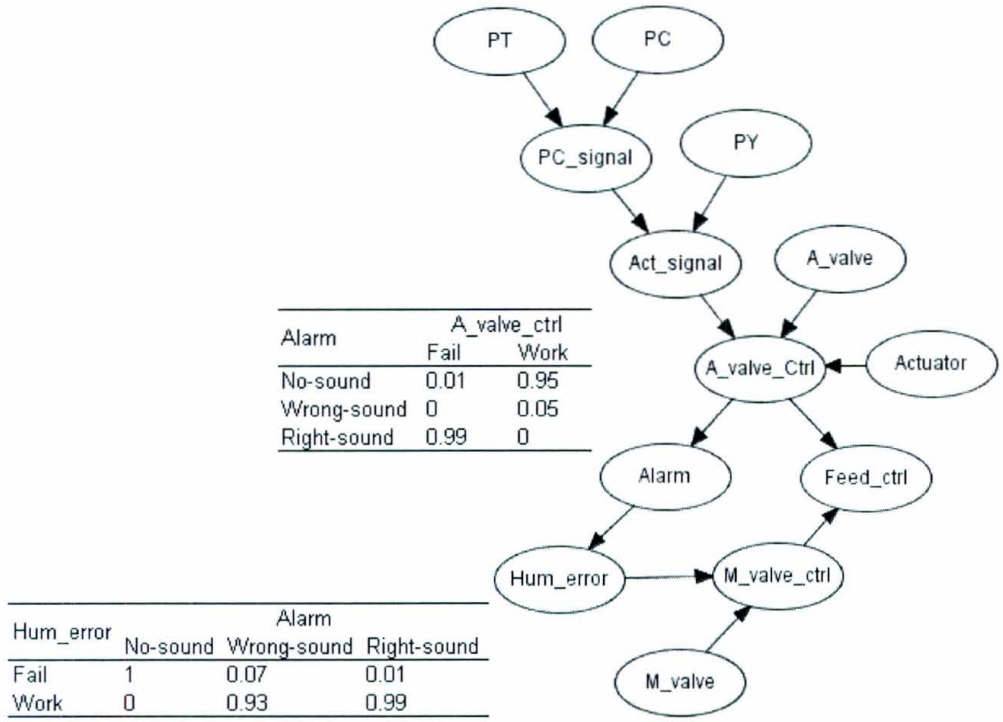
Modeling aspects of BN such as handling multi-state variables, sequentially dependent failures, and uncertainty handling are discussed in this section to demonstrate that BN has

a more flexible structure than FT, and is also a preferred option over FT for modeling some accident scenarios.

4.4.1 Multi-state Variables and Dependent Failures

To make the aforementioned accident scenario more realistic, it is assumed that the manual valve is closed by the operator only if an alarm system sounds due to the automatic valve failure (i.e, *A_valve_ctrl* occurrence). As before, all components are assumed binary, except the alarm system which is considered ternary, i.e., having three states: *No-sound* (alarm fails to sound), *Wrong-sound* (alarm sounds although automatic valve works), and *Right-sound* (alarm sounds when automatic valve fails). It has also been assumed that human failure probabilities to close the manual valve differ for wrong and right alarm sounds.

Based on the causal relationships among the aforementioned components and their failure probabilities, a BN was developed to predict the probability of improper operation of the control system (Figure 4.4). The occurrence probabilities of the BN components are the same as before, except *Alarm* and *Hum_error* which are assigned CPTs. For ease of comparison in subsequent calculations, CPT values have been identified such that the prior probability of *Hum_error* would be 0.2696 (as before).



Alarm	A_valve_ctrl	
	Fail	Work
No-sound	0.01	0.95
Wrong-sound	0	0.05
Right-sound	0.99	0

Hum_error	Alarm		
	No-sound	Wrong-sound	Right-sound
Fail	1	0.07	0.01
Work	0	0.93	0.99

Figure 4.4. Bayesian network structure for feed control system with alarm system

When constructed, the BN was modeled using the HUGIN 7.3 and the failure probability of *Feed_ctrl*; the prior probabilities of the intermediate nodes were also calculated (column 5 of Table 4.3). It should be noted that the two numbers for *Alarm* are for the *No-sound* and *Wrong-sound* states, respectively; the prior probability of *Right-sound* is readily calculated by subtracting the summation of *No-sound* and *Wrong-sound* priors from unity.

To determine the most critical primary events, abductive reasoning was performed given the accident occurrence (i.e., the malfunction of the feeding control system), yielding updated probabilities (column 6 of Table 4.3). Also, the most probable configuration of

the primary events leading to the accident was specified to be the occurrence of the components C_6 and C_9 , and the non-occurrence of the rest, with the probability of $P(\bar{C}_1, \bar{C}_2, \bar{C}_4, C_6, \bar{C}_7, \bar{C}_9, C_{10}, \bar{C}_{13} | Feed\_ctrl) = 0.1643$.

Although adding an alarm system to the accident scenario did not change the prior probability of human failure, it significantly decreased its posterior probability, excluding it from the most probable configuration. According to the new most probable explanation, mechanical failure of the automatic valve is to blame for *A_valve_ctrl* occurrence, triggering the alarm system (*Alarm=Right-sound*). Despite alarm system proper functioning, the manual valve cannot be closed because of mechanical failure, not the operator failure. So mechanical failure of the automatic and manual valve i.e., *A_valve* and *M_valve*, eventually caused the feed system to not work properly. If prior probabilities of accident occurrence (priors of *Feed_ctrl*) are compared before and after Alarm is added to the system, it can be seen that using the alarm system helps the operator to intervene more effectively in accident occurrence prevention. This decreases the probability of accident occurrence from 0.2720 to 0.1179.

4.4.2 Functional Uncertainty and Expert Opinion

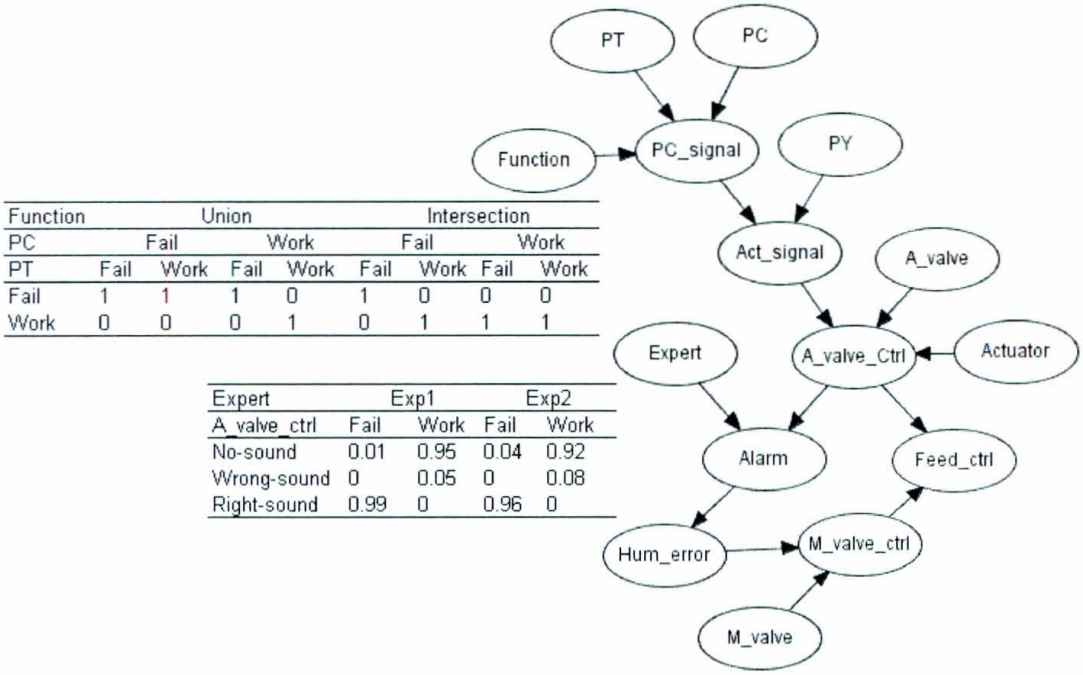
While BN reduces the uncertainty of prior beliefs through probability updating, there are other modeling techniques that help to capture some types of uncertainty (Kjaerulff & Madsen, 2007). Among these, functional uncertainty and uncertainty due to expert opinion are of significant importance in accident analysis.

Functional uncertainty is due to the lack of certitude in accurate determination of a causal function among nodes. However, to handle this kind of uncertainty, alternative functions

and their relative frequencies must be known. Two common functions used to link a child to its parents in BNs are intersection and union of variables (corresponding to OR-gate and AND-gate in FTs).

As an example, it is assumed that in the BN shown in Figure 4.2, it is not clear whether $PC\_signal = PC \cup PT$ or $PC\_signal = PC \cap PT$, but it is known that the likelihood of the former is three times that of the later, i.e., $P(\cup) = 3P(\cap)$. This lack in certainty can be modeled by adding another parent to *PC_signal*'s parent set, e.g., node *Function* with two states $\cup$ and $\cap$ such that $P(Function) = P(\cup,\cap) = (0.75,0.25)$, and also by modifying its corresponding CPT (Figure 4.5).

As previously mentioned, most prior beliefs used to construct the model are based on domain experts' opinions. So, it is likely to have different beliefs about probability parameters due to different experts assessing the model values. BN allows the incorporation of different judgments in the network structure by adding an auxiliary node to the parent set of the node of interest. The newly added node has one state for each expert, and its prior probability represents the reliability degree of each expert. For instance, it is assumed that two experts (e.g., *Exp1* and *Exp2*) have been asked to assess the causal effect of *A_valve_ctrl* on Alarm. So, node *Expert* with two states *Exp1* and *Exp2* is added to parent set of *Alarm* in which the reliability of the first expert is 60% and that of the second is 40% (i.e., $P(Expert) = P(Exp1, Exp2) = (0.6,0.4)$.



Function	Union				Intersection			
PC	Fail		Work		Fail		Work	
PT	Fail	Work	Fail	Work	Fail	Work	Fail	Work
Fail	1	1	1	0	1	0	0	0
Work	0	0	0	1	0	1	1	1

Expert	Exp1		Exp2	
A_valve_ctrl	Fail	Work	Fail	Work
No-sound	0.01	0.95	0.04	0.92
Wrong-sound	0	0.05	0	0.08
Right-sound	0.99	0	0.96	0

Figure 4.5. Modified BN to capture functional uncertainty and expert opinion

The different opinions of experts about the conditional dependence of *Alarm* on *A_valve_ctrl* are included in the corresponding CPT (Figure 4.5).

The prior and posterior probabilities of the modified BN have been also listed in Table 4.3 (columns 7 and 8, respectively). For ease of comparison, variables *Function* and *Expert* are not included in Table 3; however, their posterior probabilities given failure of *Feed_ctrl* are $P(Function) = (0.793,0.205)$, showing an increase in the likelihood of union relationship between *PT* and *PC*, and $P(Expert) = (0.563,0.437)$, showing an increase in the reliability degree of *Exp2*. It is to be noted that after the foregoing modifications, the prior probability of the leaf node, i.e., *Feed_ctrl*, increases from 0.115 to 0.116, showing the effect of uncertainty consideration in the model.

The most probable configuration of events, leading to *Feed_ctrl* failure after the modifications, is identified to be the same as before, but with a different probability as 0.0734. The new most probable configuration determines that the states of *Function* and *Expert* have to be *Union* and *Exp1*, respectively.

4.5 Conclusion

The present study has illustrated the use of BNs in both accident occurrence probability estimation and updating in the light of new information. It also focused on various modeling techniques to capture some types of uncertainty which are common in accident analysis and risk assessment. The first half of the paper was devoted to common features of FT and BN, where a FT was used to construct a corresponding BN. Although both methods resulted in similar estimations for accident occurrence probability, it was the BN that was able to update the prior beliefs about the accident by taking new information into account and by taking advantage of probability updating. The second half of the paper discussed those aspects and modeling issues of BN which FT is incapable of handling, such as multi-state variables, dependent failures and uncertainty. The main conclusions of this study can be summarized as follows:

1. By propagation of new observations through the network, BN updates the prior probabilities, yielding posterior probabilities. These posteriors, unlike priors that are based mainly on generic data and expert knowledge, are more specific to the accident studied and better reflect its characteristics.

2. The calculation of CPTs requires a comprehensive study of causal relationships and a huge amount of data usually provided by domain experts. However, the current

study has shown that a BN is a superior technique to a traditional FT even if its CPTs are developed deterministically (Figure 3). This may be helpful in situations where there is not enough information to estimate the CPT values probabilistically.

3. Considering minimal cut-set importance, it is observed that BN produces a more reliable measure of such importance by providing the most probable configuration of primary events leading to an accident. Unlike minimal cut-sets, the most probable configuration provides information about both occurrence and non-occurrence of primary events.

4. Each FT can be mapped to its corresponding BN, while a BN does not necessarily have an equivalent FT due to multi-state variables, different causal relationships rather than simple Boolean functions such as OR-gate and AND-gate, and sequentially dependent failures. BNs are also able to handle uncertainty without coupling by other methods i.e., by simply modifying their structure.

In general, BN has a much more flexible structure than FT, fitting to a wide range of accident scenarios. Its ability for abductive reasoning and uncertainty handling makes it a more suitable technique for real-time accident analysis and more importantly, for design and evaluation of safety measures. However, before BNs can be used in a comprehensive accident risk assessment, their applicability in accident consequence analysis, safety barrier implementation, and decision making must be examined thoroughly.

Acknowledgement

The authors gratefully acknowledge the support provided by Qatar National Research Foundation through National Priority Research Program (08-074-2-015) and the Natural Sciences and Engineering Research Council of Canada.

4.6 References

Bartlett, L.M, Hurdle, E.E., & Kelly E.M. (2009). Integrated system fault diagnostics utilizing diagraph and FT-based approach. Journal of Reliability Engineering and System Safety, 94, 1107-1115.

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Journal of Reliability Engineering and System Safety, 71, 249-260.

Boudali, H., & Dugan, J.B. (2005). A new Bayesian approach to solve dynamic FTs. Proceedings of Reliability and Maintainability Symposium (RAMS'05), 451-456.

BP. (2005). http://www.bp.com/genericarticle.do?categoryId=2012968 & contentId =7012963 (last checked on 29.06.10)

Ching, J., & Leu, S.S. (2009). Bayesian updating of reliability of civil infrastructure facilities based on condition-state data and fault-tree model. Journal of Reliability Engineering and System Safety, 94, 1962-1974.

CNN. (2005). http://www.cnn.com/2005/US/03/23/plant.blast/index.html (last checked on 29.06.10)

Delvosalle, C., Fievez, C., Pipart, A., & Debray, B. (2006). ARAMIS project: A comprehensive methodology for the identification of reference accident scenarios in process industries. Journal of Hazardous Materials, 130, 200-219.

Ferdous, R., Khan, F.I., Veitch, B., & Amyotte, P. (2007). Methodology for computer-aided FT analysis. Process Safety and Environmental Protection, 85, 70-80.

Ferdous, R., Khan, F.I., Veitch, B., & Amyotte, P. (2009). Methodology for computer aided fuzzy FT analysis. Journal of Process safety and Environmental Protection, 87, 217-226.

Giribone, R., & Valette, B. (2004). Principles of failure probability assessment (PoF). International Journal of Pressure Vessels and Piping, 81, 797-806.

Graves, T.L., Hamada, M.S., Klamann, R., Koehler, A., & Martz, H.F. (2007). A fully Bayesian approach for combining multi-level information in multi-state FT quantification. Journal of Reliability Engineering and System Safety, 92, 1476-1483.

Huang, Y., McMurran, R., Dhadyalla, G., & Jones, R.P. (2008). Probability based vehicle fault diagnosis: Bayesian network method. Journal of Intelligent Manufacturing, 19, 301-311.

HUGIN Expert software version 7.3 (2010). http://www.hugin.com.

Jensen, F.V., & Nielsen, T.D. (2007) Bayesian networks and decision graphs. 2nd edition, New York, Springer.

Kavcic, M., & Juricic, D. (2001). CAD for FT-based diagnosis of industrial processes. Journal of Engineering Application of Artificial Intelligence, 14, 203-216.

Khan, F.I., Sadiq, R., & Husain, T. (2001). Risk-based process safety assessment and control measures design for offshore process facilities. Journal of Hazardous Materials, A94, 1-36.

Khan, F.I. (2001). Use maximum-credible accident scenarios for realistic and reliable risk assessment. Chemical Engineering Progress, 11, 56-64.

Khoo, L.P., Tor, S.B., & Li, J.R. (2001). A rough set approach to the ordering of basic events in a FT for fault diagnosis. International Journal of Advanced Manufacturing Technology, 17, 769-774.

Kjaerulff, U.B., & Madsen, A.L. (2007). Bayesian networks and influence diagrams A guide to construction and analysis. New York, Springer.

Lampis, M., & Andrews, D. (2009). Bayesian belief networks for system fault diagnostics. International Journal of Quality and Reliability Engineering, 25, 409-426.

Langseth, H., & Portinale, L. (2007). Bayesian networks in reliability. Journal of Reliability Engineering and System Safety, 92, 92-108.

Lewis, E.E. (1994). Introduction to reliability engineering. 2nd edition, New York, John Wiley& Sons.

Lin, C.-T., & Wang, M.-J.J. (1997). Hybrid FT analysis using fuzzy sets. Journal of Reliability Engineering and System Safety, 58, 205-123.

Mahadevan, S., Zhang, R., & Smith, N. (2001). Bayesian networks for system reliability reassessment. Journal of Structural Safety, 23, 231-251.

Markowski, A.S., Mannan, M.S., & Bigoszewska, A. (2009). Fuzzy logic for process safety analysis. Journal of Loss Prevention in the Process Industries, 22, 695-702.

Montani, S., Portinale, L., Bobbio, A., & Codetta-Raiteri, D. (2006). Automatically translating dynamic FTs into dynamic Bayesian networks by means of a software tool. Proceedings of Reliability and Maintainability Symposium (RAMS'06), 434-441.

Montani, S., Portinale, L., Bobbio, A., & Codetta-Raiteri, D. (2008). RADYBAN: A tool for reliability analysis of dynamic FTs through conversion into dynamic Bayesian networks. Journal of Reliability Engineering and System Safety, 93, 922-932.

Nivolianitou, Z.S., Leopoulos, V.N., & Konstantinidou, M. (2004). Comparison of techniques for accident scenario analysis in hazardous systems. Journal of Loss Prevention in the Process Industries, 17, 467-475.

Przytula, K.W., & Thompson, D. (2000). Construction of Bayesian networks for diagnostics. Proceedings of IEEE Aerospace Conference, 5, 193-200.

Reuters. (2010a). http://www.reuters.com/article/idUSTRE61619Q20100207 (last checked on 25.06.10)

Reuters. (2010b). http://www.reuters.com/article/idUSTRE6482L220100510 (last checked on 29.06.10)

Shalev, D.M., & Tiran, J. (2007). Condition-based FT analysis (CBFTA): A new method for improved fault tee analysis (FTA), reliability and safety calculations. Journal of Reliability Engineering and System Safety, 92, 1231-1241.

Simon, C., Weber, P., & Levrat, E. (2007). Bayesian networks and evidence theory to model complex systems reliability. Journal of Computers, 2, 33-43.

Sklet, S. (2004). Comparison of some selected methods for accident investigation. Journal of Hazardous Materials, 111, 29-37.

Torres-Toledano, J.G., & Sucar, L.E. (1998). Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science, 1484, 195-206.

Weber, P., Medina-Oliva, G., Simon, C., & Iung, B. (2010). Overview on Bayesian networks applications for dependability, risk analysis, and maintenance areas. Engineering Application of Artificial Intelligence, doi: 10.1016/j.engappai.2010.06.002.

Wilson, A.G., & Huzurbazar, A.V. (2007). Bayesian networks for multilevel system reliability. Journal of Reliability Engineering and System Safety, 92, 1413-1420.

Yuhua, D., & Datao, Y. (2005). Estimation of failure probability of oil and gas transmission pipelines by fuzzy FT analysis. Journal of Loss Prevention in the Process Industries, 18, 83-88.

Zheng, X., & Liu, M. (2009). An overview of accident forecasting methodologies. Journal of Loss Prevention in the Process Industries, 22, 484-491.

5 Dynamic risk analysis using bow-tie approach[†]

Preface

A version of this manuscript has been published in the *Journal of Reliability Engineering and System Safety*. The co-authors, Dr. Khan and Amyotte supervised the principal author, Khakzad, to develop the research on the entitled topic and helped him to conceptualize the techniques and theories available for this topic. Khakzad conducted accident modeling and associated analyses while Khan and Amyotte reviewed the manuscript and provided the necessary suggestions.

Abstract

Among many techniques available, bow-tie model (BT) is very popular because it represent the accident scenario altogether including causes and consequences. However, it suffers a static structure limiting its application in real-time monitoring and probability updating which are key factors in dynamic risk analysis. The present work is focused on using BT approach in a dynamic environment in which the occurrence probability of accident consequences changes. In this method, on one hand, failure probability of primary events of BT, leading to the top event, are developed using physical reliability models, and constantly revised as physical parameters (e.g., pressure, velocity, dimension, temperature) change. And, on the other hand, the failure probability of safety

[†] Khakzad et al. Journal of Reliability Engineering and System Safety 2012.

barriers of the BT are periodically updated using Bayes' theorem as new information becomes available over time. Finally, the resulting, updated BT is used to estimate the posterior probability of the consequences which in turn results in an updated risk profile.

Keywords: Dynamic risk analysis, Bow-tie approach, Bayes' theorem, Physical reliability models.

5.1 Introduction

There are many methods for risk assessment of envisaged accident scenarios in the process industries, such as quantitative risk assessment (QRA), probabilistic safety analysis (PSA), and maximum credible accident analysis (Khan, 2001; Khan and Abbassi, 1998). Although these methods consist of different steps and follow specific procedures, accident scenario identification in terms of both mechanism and likelihood is a common and central step to all of them.

While conventional risk assessment methods have played an important role in identifying major risks and maintaining safety in process facilities, they have the disadvantage of being static and using generic failure data (Meel and Seider, 2006; Shalev and Tiran, 2007). The static structure of the aforementioned methods fails to catch up with the variations which almost always occur during the operational time of a process. Also, using generic data prevents the analysis from being case-specific and brings uncertainty into the results.

On the other hand, a dynamic risk assessment method should be able to take any new information into account and to tailor itself to the dynamic environment which is dominant in process system risk and safety analyses. A risk assessment method not only

can be employed at the design phase of a process system, but it can also be considered during the system's life time as a decision support and risk management tool (Shalev and Tiran, 2007).

Dynamic risk assessment methods take advantage of case-specific data and updating mechanisms to revise the failure probabilities obtained from the initial generic data in the design phase of the system. In non-Bayesian updating approaches, new data which is supplied by real-time monitoring of parameters or inspection of process equipment is usually substituted for generic data to obtain updated failure rates using physics-based models, structural models, mechanical models, or condition-based models (Ching and Leu, 2009). On the other hand, Bayesian approaches employ new data in the form of likelihood functions to update prior failure rates using Bayes' theorem (Ferson, 2005; Kelly and Smith, 2009; Siu and Kelly, 1998).

There have been efforts to make risk assessment methods dynamically adapted as real-time changes occur in a process. Shalev and Tiran (2007) introduced condition-based fault tree in which failure rates of components are periodically updated using information obtained through predictive maintenance. Consequently, the failure probability of the top event is updated by recalculating the fault tree (FT) for new failure rates. However, their method has to be implemented in specific conditions where, for example, gradual deterioration process of a component can be discretized into several stages at each of which there should be a correlation between residual time of the component and its total failure time.

In the context of Bayesian updating, Meel and Seider (2006), Kalantarnia et al. (2009, 2010), and Rathnayaka et al. (2011) used Bayes' theorem to update the failure probability of event tree (ET) based on the occurrence number of consequences recorded over time. Other researchers have also attempted to use Bayesian network (BN) instead of FT (Bobbio et al., 2001; Boudali and Dugan, 2005; Khakzad et al., 2011; Marquez et al., 2010), ET (Bearfield and Marsh, 2005) and Bow-tie (BT) model (Khakzad et al., 2012) for probability updating. A comprehensive and state of the art application of Bayesian inference and Bayesian network in risk analysis can be found in Kelly and Smith (2009), Siu and Kelly (1998), and Weber et al. (2010). Further, there are attempts to substitute Markov models for FT (Xing et al., 1996) or to construct dynamic FT and ET from corresponding Markov models such that time-dependent failures can be taken into account (Bucci et al., 2008). However, the application of Markov models in complex systems has been limited due to the well-known problem of state-space explosion and also the error-prone mapping procedure.

Among the different models available to identify and analyze accident scenarios, BT has been well proven to be a reliable and efficient tool. It has been used in a broad range of applications such as in process safety analysis (Markowski et al, 2009), risk management (Cockshott, 2005), and recently in ARAMIS project for accident risk analysis Chevreau et al, 2006, Delvosalle et al., 2005 and 2006; Dianous et al., 2006; Gowland, 2006). Nevertheless, as BT is composed of FT and ET, it is influenced by the same limitations as its constituents (i.e., FT & ET) in dynamic risk assessment.

The present work is aimed at showing the importance of dynamic BTs in real-time risk assessment. In this method, the FT part of BT is updated using varying physical parameters supplied by continuous monitoring of process equipment. For this purpose, failure distributions of primary events are developed using physical reliability models, allowing to substitute newly observed parameters in the model and therefore to recalculate the top event (TE) probability (i.e., physics-based updating). On the other hand, the ET part is updated using Bayes' theorem which in turn employs the periodically recorded number of accident consequences in the form of likelihood functions (i.e., evidence-based updating). Finally, the resulting updated BT is used to estimate the posterior probability of the consequences and subsequently to estimate updated risk.

Section 5.2 provides a brief description of BT model. Section 5.3 explains the methods used in this work to update the BT. The application of the method to a real-life case study and the discussion of the results are included in sections 5.4 and 5.5, respectively. Section 5.6 is devoted to the conclusions and recommendations for future work.

5.2 Bow-tie approach

BT is a graphical tool to illustrate an accident scenario, starting from accident causes and ending with its consequences. While centered on a critical event, BT is composed of a FT on the left-hand side identifying the possible events causing the critical event (or top event), and an ET on the right-hand side showing the possible consequences of the critical event based on the failure or success of safety barriers. Figure 5.1 illustrates a typical BT in which PE, IE and TE are primary, intermediate and the top event, respectively. Also, SB and C stand for safety barrier and accident consequence.

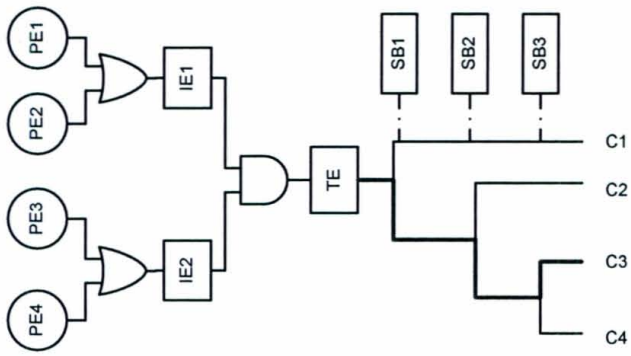


Figure 5.1. Generic bow-tie

BT represents a complete accident scenario qualitatively and quantitatively. From a qualitative perspective, BT clearly illustrates the logical relationship among the components of an accident scenario. It helps to understand which possible combination of primary events would lead to the top event and which safety barriers' failure would escalate the top event to a particular consequence.

Once BT has been structured, quantitative analysis can be carried out by assigning probabilities to the primary events of the FT and the safety barriers of the ET. In a FT, the occurrence probability of the top event can be calculated as the union of minimal cut sets. A minimal cut set is defined as the intersection of the minimum number of primary events, the occurrence of which is necessary to cause the top event to occur. The ET of the BT model starts from the top event provided by the FT and proceeds toward each branch to calculate the occurrence probability of each consequence based on failure or success of various safety barriers. For example, the occurrence probability of consequence (or end event) C_2 in Figure 5.1 can be calculated as:

$$P(C_2) = P(TE)P(SB_1)P(\overline{SB}_2) \quad 5.1$$

Where $P(TE)$ is top event probability, and $P(SB_1)$ and $P(\overline{SB}_2)$ refer to the failure and non-failure probability of safety barriers SB_1 and SB_2, respectively.

5.3 Bow-tie Updating

There are many efforts in the literature attempting to update conventional FT and ET given new observations. However, the works dedicated to update BT are few, particularly in the field of risk assessment and safety analysis. Recently, Khakzad et al. (2012) introduced a methodology for dynamic safety analysis of process systems based on mapping BT into the corresponding BN. As a result, the probable conditional dependencies between the top event and the safety barriers could be considered. They also suggested performing probability adapting rather than probability updating when the cumulative number of failures over a time period is available.

However, this study aims to apply BT in the context of dynamic risk analysis without resort to BNs. This BT should thus be capable of being updated as new data, whether associated with the primary events or safety barriers, is observed. Consequently, the probability of accident consequences can be re-calculated as the probability of the top event (due to primary events) and safety barriers are updated separately or some together. Using the updated probabilities of accident consequences, the estimated risk can be revised.

5.3.1 Fault Tree Revising: Use of Physical Reliability Models

In the current research, the concept of physical reliability models Ebeling, 1997) is used to revise the probability of primary events of FT, which, in turn, results in top event updating. Physical reliability models aim to explain the reliability (or failure) of a component as a multivariate function of operational physical parameters. Physical models particularly structural models, mechanical models, and physics-of-failure models have long been recognized in reliability and maintainability analysis in civil and mechanical engineering (Ching and Leu, 2009; Hull and Strutt, 2003). However, their application is not widely adopted in process safety and risk analysis. This section aims to illustrate how physical reliability models can effectively be used for real-time and dynamic risk assessment of process systems. Among different types of physical reliability models, covariate models and static models are used in this study to incorporate operational physical parameters in the failure probabilities of the FT's components.

5.3.1.1 Covariate models

Operational physical parameters, also called covariates, may be temperature, velocity, pressure, or vibration amplitude. Covariate models explain the failure rate of a component as a function of the dominant physical parameters (covariates) (Ebeling, 1997):

$$\lambda(t, X) = \lambda_0(t)\, g(X, A) \qquad \textbf{5.2}$$

Where $\lambda(t, X)$ is the failure rate as a function of time and the covariates; $\lambda_0(t)$ is the baseline failure rate just as a function of time; $g(X, A)$ is a positive function which is

independent of time, incorporating the effect of covariates in the failure rate; $X = (x_1, x_2, ..., x_n)$ is a vector of covariates; $A = (a_1, a_2, ..., a_n)$ is a vector of unknown parameters such that a_i is the coefficient of x_i. The value of a_i is often estimated using least-squares method or maximum likelihood estimation (MLE) (Ebeling, 1997).

In order to make the failure rate of Weibull distribution dependent on covariates, it is common practice to assume the scale factor θ as a function of covariates, i.e. $\theta(X) = Exp(\sum_{i=0}^{n} a_i x_i)$. The time-dependent failure rate of Weibull distribution is given by:

$$\lambda(t) = \beta t^{\beta-1} \theta^{-\beta} \qquad \textbf{5.3}$$

Where β is the shape factor. Substituting $\theta(x)$ in equation 5.3 results in:

$$\lambda(t, X) = \beta t^{\beta-1} \left\{ Exp(\sum_{i=0}^{n} a_i x_i) \right\}^{-\beta} \qquad \textbf{5.4}$$

In which $x_0 = 1$ by convention. Therefore, the covariate model for failure probability $F(t)$ will be:

$$F(t) = 1 - Exp\left\{ -\left(\frac{t}{Exp(\sum_{i=0}^{n} a_i x_i)} \right)^{\beta} \right\} \qquad \textbf{5.5}$$

It is evident from Equation 5.5 that with any change in covariate x_i, the failure probability $F(t)$ will change.

5.3.1.2 Static models

Static models, on the other hand, do not consider time as an influential parameter and only count on the component's strength and stresses. Similar to covariates, stresses are often considered as physical or chemical parameters affecting a component's operation. Strength is defined as the highest amount of stress that a component can bear. According to the definitions of stress and strength, a failure occurs when the stress on the component exceeds its strength (Ebeling, 1997). Both stress and strength can be constant or considered as random variables having probability distribution functions. For example, the failure probability of component Q having a constant strength, k, and being under a random stress, Y, can be defined as the probability of Y being greater than k:

$$\Pr(Q) = \Pr(Y > k) = \int_{k}^{\infty} f_Y(y)dy \qquad \textbf{5.6}$$

In which $f_Y(y)$ is the probability density function (PDF) of the stress, Y. Assuming an exponential distribution for $f_Y(y)$, Equation 6 can be written as:

$$\Pr(Q) = \int_{k}^{\infty} \lambda e^{-\lambda y} dy = e^{-\lambda k} \qquad \textbf{5.7}$$

Since in the exponential distribution $\lambda = \frac{1}{E(Y)}$, Equation 5.7 becomes as:

$$\Pr(Q) = e^{-\frac{k}{E(Y)}} \qquad \textbf{5.8}$$

In which $E(Y)$ is the expected value of the stress. Therefore, the failure probability of component Q can be reassessed when a new value for k is observed.

5.3.2 Event tree updating: use of Bayes' theorem

Bayes' theorem has frequently been used for probability updating in dynamic risk analysis. In this regard, the number of failures over time or over a number of trials is usually taken into account to form likelihood functions. Due to mathematical convenience, it has been common practice to choose a prior distribution and its corresponding likelihood function from well known conjugate families which in turn result in a posterior distribution from the same family (Meel and Seider, 2006). However, recent developments in probabilistic software tools such as WinBUGS (Bayesian inference Using Gibbs Sampling) (Lunn et al., 2000) have made it possible to choose from a wide range of probability distributions of arbitrary complexity.

Siu and Kelly (1998) suggested using gamma prior distribution for failure rates of events and Poisson likelihood function for the number of failures over time intervals. On the other hand, Meel and Seider (2006) and Kalantarnia et al. (2009, 2010) chose a Beta prior distribution for failure probabilities and a Binomial likelihood function based on the number of failures. In situations where no parametric likelihood function can be considered, nonparametric or empirical likelihood functions can also be directly extracted from the data (Rathnayaka et al., 2011). However, such likelihood functions must be applied cautiously to avoid *zero preservation problems* in which any likelihood function equal to zero prevents the updating process from proceeding (Ferson, 2005). This is because a likelihood function equal to zero over some region of the parameter leads to a posterior equal to zero (over that region) which cannot be updated in the next updating try, no matter what additional data is used.

In the present study, it is assumed that prior failure rates of safety barriers follow gamma distribution:

$$f(\lambda) = \frac{\beta^{\alpha}\lambda^{\alpha-1}}{\Gamma(\alpha)}e^{-\beta\lambda} \qquad \textbf{5.9}$$

Where $f(\lambda)$ is gamma distribution of λ, λ is the failure rate, α and β are distribution parameters, and $\Gamma(\alpha) = \int_0^{\infty} x^{\alpha-1}e^{-x}dx$ is gamma function. Further, for the number of failures over time, Poisson likelihood function is considered as:

$$L(r \mid \lambda) = \frac{(\lambda t)^{r}}{r!}e^{-\lambda t} \qquad \textbf{5.10}$$

In the above equation $L(r \mid \lambda)$ is the likelihood function of r given λ, and r is the number of failures in $[0,t]$ interval. Using Bayes' theorem, the posterior failure rates given in Equation 5.11 have also gamma distribution yet with different parameters:

$$f(\lambda \mid r) = \frac{f(\lambda)L(r \mid \lambda)}{\int_{\lambda} f(\lambda)L(r \mid \lambda)d\lambda} = \frac{\beta'^{\alpha'}\lambda^{\alpha'-1}}{\Gamma(\alpha')}e^{-\beta'\lambda} \qquad \textbf{5.11}$$

Where $f(\lambda \mid r)$ is the posterior distribution of the failure rate; $\beta' = \beta + t$ and $\alpha' = \alpha + r$ are new distribution parameters. The mean value of the prior gamma distribution, $E(\lambda) = \frac{\alpha}{\beta}$, thus changes to

$$E(\lambda') = \frac{\alpha'}{\beta'} = \frac{\alpha + r}{\beta + t} \qquad \textbf{5.12}$$

5.3.3 Consequence updating

Having a BT either the top event of which can be updated using physical reliability models (Section 5.3.1) or the safety barriers of which can be updated using Bayes' theorem (Section 5.3.2), it is possible to update the probability of the consequences (C_i in Figure 5.1). The reason is that the probabilities of consequences in a BT are calculated by multiplication of the top event and the safety barriers' probabilities (see Equation 5.1). Using the updated probabilities of the consequences, the estimated risk can thus be updated. Figure 5.2 schematically illustrates the updating process described in detail in the aforementioned sections. In the next sections, it is shown how different kinds of information, such as changes in physical parameters (through application of physical reliability models) or changes in our beliefs as more information becomes available over time (through application of Bayes' theorem), can be used to update the estimated risk.

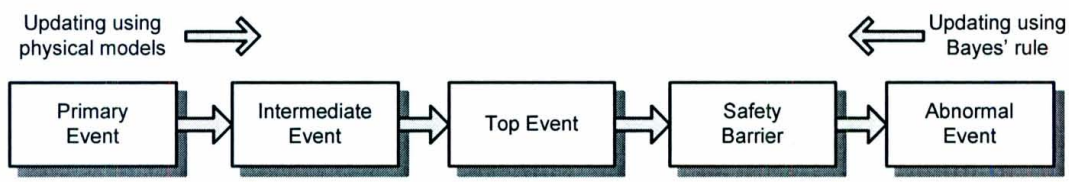


Figure 5.2. Schematic of BT updating

5.4 Case Study: Sugar Refinery Explosion

In February 2008, a devastating dust explosion occurred at the Imperial Sugar manufacturing facility, Georgia, U.S. This accident was chosen to implement the

methodology proposed here. The refinery plant included equipment to produce granulated sugar from raw sugar, conveyor belts and bucket elevators to transport granulated sugar to the silos and from the silos to the packing building, and grinding and packing machines.

According to the final report issued by the U.S. Chemical Safety Board (2009), faults in design and maintenance of equipment such as the conveyor belts and the packing machine, inadequate housekeeping, and defects in the dust removal system resulted in significant accumulations of granulated sugar and airborne sugar dust in the work area. These combustible forms of sugar along with deficient safety measures caused a primary explosion whish was escalated into a secondary, much more devastating explosion. The primary explosion was reportedly due to high concentration of sugar dust inside a recently enclosed conveyor belt and an overheated bearing as ignition source. Based on the detailed investigation carried out by the U.S. Chemical Safety Board, different accident scenarios were envisaged using a BT model (Figure 5.3).

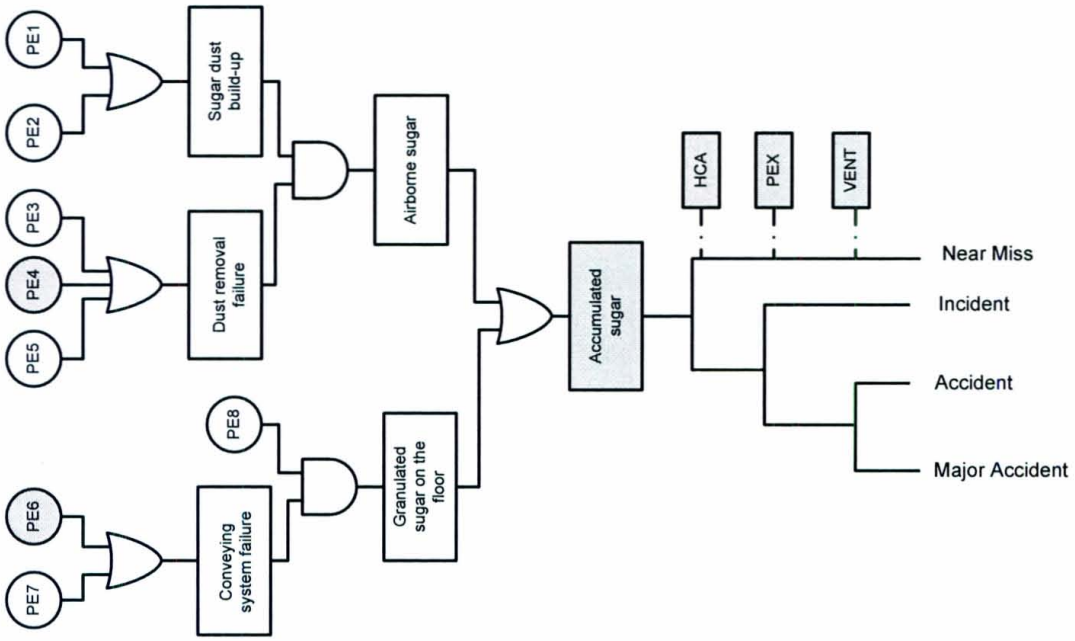


Figure 5.3. Bow-tie modeling of sugar dust explosion at Imperial Sugar manufacturing facility

In order to show the updating procedure, it is assumed that all primary events follow a time-dependent exponential distribution, except *Dust pipes clogged with dust* (*PE4*) and *Blockage of sugar flow* (*PE6*) which are explained in the form of covariate and static models, respectively. In this regard, it has been considered that *PE4* has a Weibull distribution whose scale parameter, θ, is a function of covariates such as air velocity inside the pipe (V) and pipe diameter (d), i.e., $\theta(X) = Exp(a_0 + a_1 V + a_2 d)$. Covariate models demand for experiments and laboratory data or data taken during operation of commercial scale equipment to establish regression coefficients using MLE or least-squares methods (see Appendix). In this study, using the data in Table 5.1, the failure

distribution parameters of *PE4* were estimated as $\beta = 1.5$, $a_0 = 0.01$, $a_1 = 0.2$ and $a_2 = 6.75$ applying the least square method.

Table 5.1. Data used to estimate the unknown parameters of Weibull distribution for PE4

Failure time t (year)	Air velocity V (m/s)	Pipe diameter d (m)
0.86	2	0.08
1.6	2.3	0.07
2.67	3	0.06
3.27	2.5	0.04

On the other hand, the failure distribution of *PE6* is developed using static models with conveyor belt speed (V_B) as the strength and the velocity of sugar (V_S) flowing from silo openings on the conveyor belt as the stress. Assuming that V_B is a constant and V_S has an exponential distribution with the mean value $E(V_S) = 1.5\ m/s$, Equation 8 can be used to estimate the probability of PE6 as $P(PE6) = Exp(-\frac{V_B}{1.5})$. In other words, it is considered that sugar blockage occurs when the speed of the belt is less than the velocity of sugar flowing from silos, i.e., $V_B < 1.5\ m/s$.

The prior probabilities of the remaining primary events are determined based on data recorded by, for example, Center for Chemical Process Safety (2000), Offshore Reliability Data Handbook (2002), CSB historical records, and using expert judgment. Table 5.2 illustrates the prior failure rates of the primary events. The initial values of

distribution parameters and covariates have been chosen as $V_B = 2\ m/s$, $V = 2\ m/s$, and $d = 0.1\ m$.

Table 5.2. Prior probabilities of primary events of fault tree.

Index	Components	λ (per year)	Probability
PE1	Grinding machine	0.3	0.2592
PE2	Packaging machine	0.2	0.1813
PE3	Roof dust collector disrepair	0.02	0.0198
PE4	Dust pipe clogged with dust	Physical model	0.1783
PE5	Undersized filters	0.01	0.01
PE6	Blockage of sugar flow	Physical model	0.2636
PE7	Not properly sealed	0.005	0.005
PE8	Poor housekeeping	0.1	0.0952

In the BT model, three safety barriers have been considered, that is, high concentration alarm barrier (*HCA*), primary explosion barrier (*PEX*), and venting barrier (*VENT*), for which prior failure rates are assumed to have gamma distribution with parameters listed in Table 5.3. The failure rates of safety barriers are determined as mean value of the distributions. It is also considered that safety barriers follow an exponential distribution. *HCA* has been devised to warn staffs about sugar dust concentrations above the minimum explosible concentration (*Near miss*). If this barrier fails to work, or staffs ignore the alarm and neglect to remedy the high concentration, *PEX* is supposed to prevent the dust from igniting (*Incident*). On the condition that a primary explosion occurs, *VENT* can prevent it from escalating to a secondary explosion (*Accident*). Otherwise, a primary

explosion propagates through the packaging building, causing a stronger and more destructive explosion (*Major accident*).

Table 5.3. Prior parameters of safety barriers.

SB_i	α	β	λ
HCA	0.88	2.53	0.349
PEX	0.81	4.74	0.1707
VENT	1.72	8.98	0.1917

5.5 Application of the Methodology

5.5.1 Fault tree revising

Figures 5.4 through 5.6 show the application of physical reliability models in FT reassessment. In Figures 5.4 and 5.5, probability of the top event is recalculated for different values of covariates $V = 1.5 \sim 10.5\ m/s$ and $d = 0.01 \sim 0.1\ m$, respectively, via *PE4* and using Equation 5.5.

Similarly, in Figure 5.6, probability of the top event is shown for different values of covariate $V_B = 0.5 \sim 5\ m/s$ via *PE6* and using Equation 5.8. These revised probabilities of the top event directly affect the probabilities of consequences (see Equation 5.1), which in turn result in updated estimates of risk.

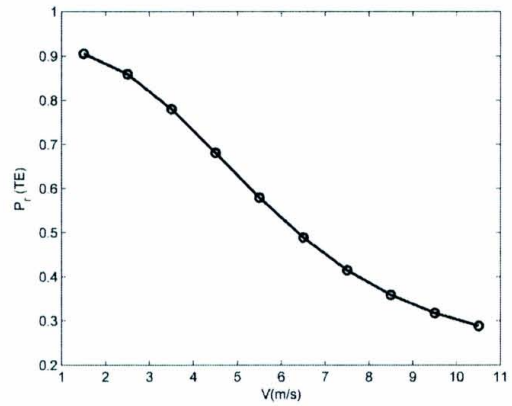


Figure 5.4. Event probability updating for different air velocities (*V*).

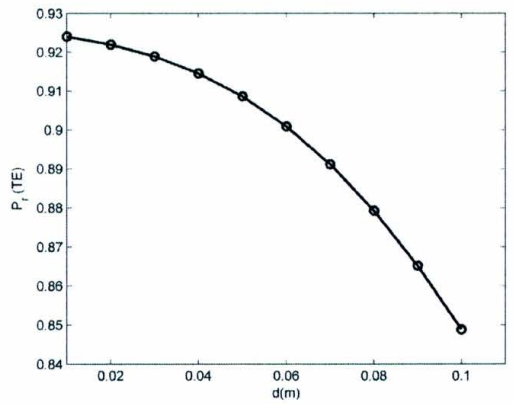


Figure 5.5. Top event probability updating for different pipe diameters (*d*).

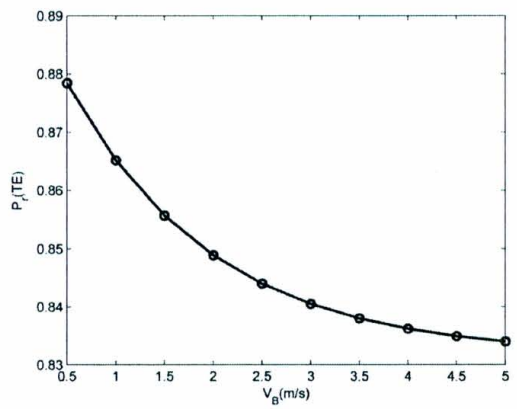


Figure 5.6. Top event probability updating for different conveyor belt speeds (V_B).

The top event probability can also be re-quantified using different pairs of covariates, making it possible to investigate the simultaneous effects of several covariates on the top event probability. Figure 5.7 shows the top event probability contours for the covariates V_B and V. Through the combinations of such contours, it is possible to determine several sets of scenarios for which the top event probability is constant in spite of changing covariates.

Table 5.4 represents, as an instance, six different scenarios leading to $P(TE) = 0.2$, while having different covariates. For example, by comparing scenario 2 and 4 in Table 5.3, it can be seen that increases in V_B from 3 to 4 m/s and in V from 1 to 3.5 m/s compensate for a decrease in d from 0.09 to 0.01 m. However, among different scenarios, the most practical one should be chosen based on operational limitations and economic considerations.

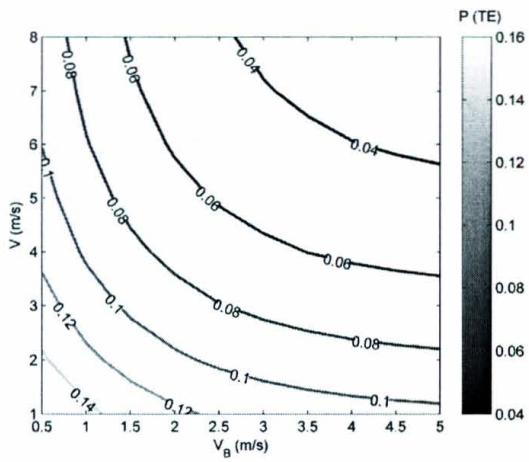


Figure 5.7. Top event probability contours for belt speed (V_B) and air velocity (V).

Table 5.4. Scenarios leading to the same top event probability, i.e. P(TE) = 0.12.

Scenario	V_B (m/s)	V (m/s)	d (m)
1	5	1	0.08
2	4	3.5	0.01
3	3	2	0.06
4	3	1	0.09
5	2	3.5	0.03
6	2	2.5	0.06

5.5.2 Event tree updating

As described in Section 5.3.2, the number of failures r is used to develop Poisson likelihood function (Equation 5.10). In this regard, r for each safety barrier equals the number of consequences resulted from that safety barrier's failure. For demonstration purposes, the cumulative number of each consequence over the course of 5 years is listed in Table 5.5. For example, r for safety barrier *HCA* at the end of the 4th year is calculated as $r_{HCA} = N_{Incident} + N_{Accident} + N_{major\ accident} = 4 + 3 + 1 = 7$.

Where N_i refers to the occurrence number of consequence C_i. It is because according to the BT in Figure 5.3, the occurrence of each of consequences *Incident*, *Accident* or *Major accident* implies that safety barrier *HCA* has failed.

Table 5.5. Cumulative number of consequences over 5 years of process operation.

C_i	Year 1	Year 2	Year 3	Year 4	Year 5
Near miss	2	3	5	6	9

Incident	0	0	1	4	5
Accident	0	1	2	3	4
Major Accident	1	1	1	1	1

As mentioned earlier, the posterior failure rates of the safety barriers also follow gamma distribution with the expected values equal to $(\hat{\lambda}) = \frac{\alpha+r}{\beta+t}$. Thus, taking into account the number of failures, *r*, at the end of each year *t*, it is possible to obtain the posterior failure rate of each safety barrier as the expected value of its updated distribution. Accordingly, the posterior average failure rate of safety barrier *HCA* is estimated as $E(\hat{\lambda}) = \frac{0.88+7}{2.53+4} = 1.207$ (compare with its prior failure rate 0.349). Figure 5.8 shows the posterior failure probability of the safety barriers. It should be noted that failure probability of safety barriers is calculated using $F(t) = 1 - e^{E(\hat{\lambda})t}$.

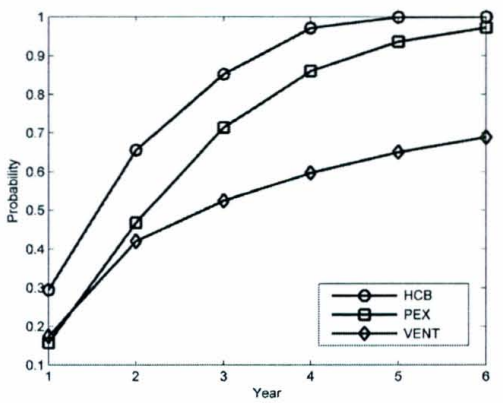


Figure 5.8. Posterior failure probabilities of safety barriers.

5.5.3 Dynamic risk assessment

The methods proposed in the present study enable updating of FT and ET. This helps to revise the accident risk profile as new relevant information becomes available for either part of BT. The updated probabilities of the top event and safety barriers directly affect the probabilities of the consequences, which subsequently lead to an updated risk profile. Figure 5.9 illustrates, as an example, the probability of consequence *Near miss* for different V_B, V and updated safety barriers in two different years.

Similarly, the change in the probability of other consequences can be shown for every pair of covariates in different years. This helps to determine what safety measures are required and where they should be allocated to most efficiently prevent or mitigate the accident. It is even more beneficial if the change in the risk profile behavior, instead of change in consequences, is depicted for different covariates.

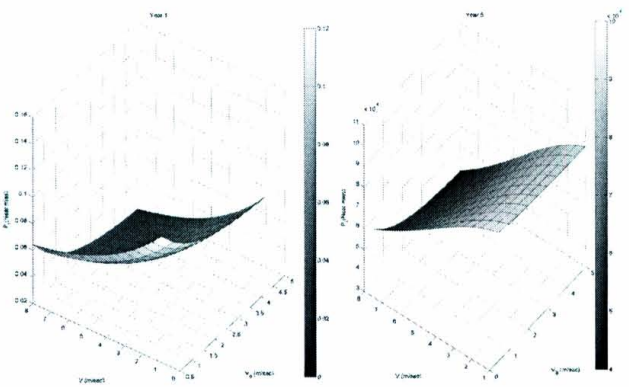


Figure 5.9. Updated probability of consequence *Near miss* using covariates V_B and V and updated safety barriers for year 1 (left) and 5 (right). (d is kept constant, i.e., d = 0.1 m).

As risk is defined as the multiplication of the probability and severity of consequences, the severity of each consequent is listed in Table 5.6 in dollar amount. The numbers presented here are for illustrative purposes only.

Table 5.6. Estimated damage of consequences

C_i	Damage (US$)
Near miss	5000
Incident	50000
Accident	1000000
Major accident	10000000

Figure 5.10 shows the risk profile as a function of V_B and V for the 5th year of process operation (d = 0.1 m). Similar profiles drawn with different pairs of covariates, as illustrated in Figure 5.10, provide decision makers with a clearer vision of how the risk profile dynamically changes due to variations in process parameters. Therefore, appropriate safety measures can effectively be applied to maintain the risk within defined acceptance criteria.

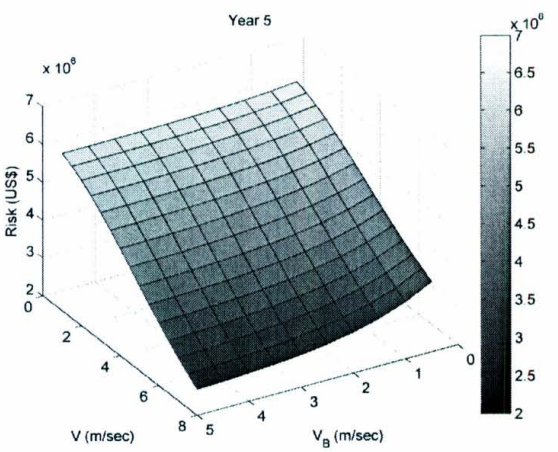


Figure 5.10. Risk surface for different V_B and V (d is kept constant, i.e., d = 0.1 m).

Figure 5.11 shows the risk contours derived from the risk profile in Figure 5.10. For example, it is evident from Figure 5.11 that for d= 0.1 m and V > 6 m/s, the estimated risk is less than *3 E 04 USD*, regardless of the amount of V_B.

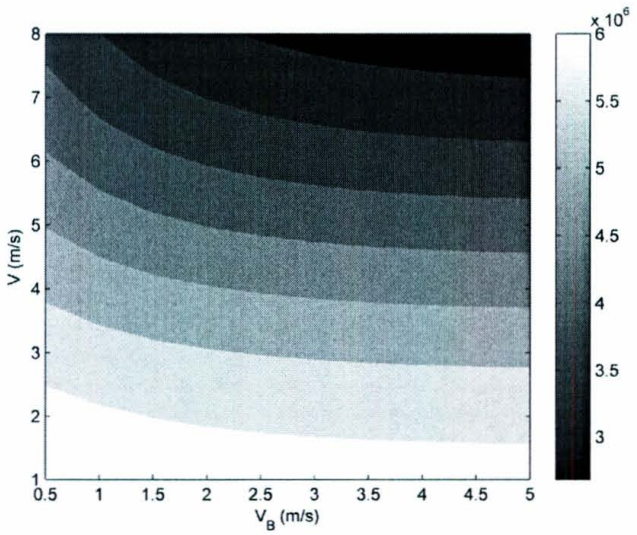


Figure 5.11. Risk contours for different V_B and V (d = 0.1 m).

It can also be noted that for a constant d, the effect of V on risk profile is much larger than that of V_B. Thus, in the present study, the most attention have to be given to air velocity variation, V, in the pipes rather than to the conveyor belt speed, V_B, in order to keep the estimated risk as low as possible.

5.6 Conclusion

This paper has demonstrated the role of updated BT in dynamic risk assessment. Physical reliability models such as covariate and static models were employed to investigate the effect of real-time variation of physical parameters on the top event probability. It was illustrated that these physical models provide a deeper insight into the behavior of process risk by incorporating the influential physical parameters into the failure distribution functions. Once physical reliability models are developed for primary events of BT in design phase, the top event probability and consequently the initially estimated risk can be readily revised as new physical parameters are monitored and observed during process operation time. Although physical models demand experimental and site data to be established, this research showed they could provide the analyst with a quick and practical method for real-time probability estimation.

This study has also used Bayes' theorem to update safety barriers of BT, directly affecting the probability of consequences and the estimated risk as a result. It used Bayes' theorem besides physical models in BT to capture all kinds of information available to revise the risk. In other words, Bayesian inference helped to incorporate those kinds of information in the updating procedure which were not possible to be considered by physical models, i.e., changes in initial estimates over time.

Overall, the applied updating methodology has been shown to be an effective technique in BT updating, which in turn results in real-time and dynamic risk analysis. It was also demonstrated how changes in either physical parameters (supplied by continuous

monitoring of equipment) or the initial estimates (resulted from occurrence of accidents over time) were taken into account to obtain a dynamically updated risk estimate.

Acknowledgment

The authors thankfully acknowledge the financial support provided by Natural Science and Engineering Research Council (NSERC) of Canada and Petroleum Research Atlantic Canada (PRAC).

5.7 Appendix

Given a sample of failure times $\{t_1, \dots, t_n\}$ and the set of covariates x_{ij} associated with each failure time (x_{ij} is the value of the i-th covariate which is associated with the j-th failure time), methods such as Maximum Likelihood Estimate (MLE) or least-square method can be applied to estimate unknown parameters of the distribution.

(i) MLE method

The probability density function of Weibull distribution is given by:

$$f(t \mid \beta, \theta) = \frac{\beta}{\theta}(\frac{t}{\theta})^{\beta-1} Exp(-(\frac{t}{\theta})^{\beta}) \qquad \textbf{5.13}$$

According to unknown parameters β and θ, the likelihood function of parameters is found as:

$$L(\beta, \theta) = \prod_{j=1}^{n} f(t_j \mid \beta, \theta) = (\frac{\beta}{\theta})^{n} (\frac{\prod_{j=1}^{n} t_j}{\theta^n})^{\beta-1} Exp(-\sum_{j=1}^{n}(\frac{t_j}{\theta})^{\beta}) \qquad \textbf{5.14}$$

Due to the multiplicative form of the likelihood function, its natural logarithm yields the additive form which is usually easer to solve considering the derivation procedure:

$$Ln\,L(\beta,\theta) = Ln(\frac{\beta}{\theta})^{n} + Ln(\frac{\prod_{j=1}^{n} t_j}{\theta^{n}})^{\beta-1} + Ln\,Exp(-\sum_{j=1}^{n}(\frac{t_j}{\theta})^{\beta}) \qquad \textbf{5.15}$$

Which can alternatively be written as:

$$Ln\,L(\beta,\theta) = n\,Ln(\frac{\beta}{\theta}) + (\beta-1)\,Ln(\frac{\prod_{j=1}^{n} t_j}{\theta^{n}}) - \sum_{j=1}^{n}(\frac{t_j}{\theta})^{\beta} = \qquad \textbf{5.16}$$

$$n\,Ln\beta - n\beta\,Ln\theta + (\beta-1)\,Ln\prod_{j=1}^{n} t_j - \sum_{j=1}^{n}(\frac{t_j}{\theta})^{\beta}$$

To find the best estimate of any unknown parameter of interest, the first derivative of the likelihood function (or its natural logarithm), with respect to that parameter should be equal to zero. For example, to find the best estimate of β, the following derivative should be solved:

$$\frac{\partial\,Ln\,L(\beta,\theta)}{\partial\beta} = \frac{n}{\beta} - n\,Ln\theta + \sum_{j=1}^{n} Ln\,t_j - \sum_{j=1}^{n}(\frac{t_j}{\theta})^{\beta}\,Ln(\frac{t_j}{\theta}) = 0 \qquad \textbf{5.17}$$

Which in turn leads to a system of n nonlinear equations (i.e., one equation for each failure time). According to the present study, since $\theta = Exp(a_0 + a_1 V + a_2 d)$, the set of nonlinear equations represented by Equation 5.17 can be solved only if the values of covariates V and d are known for each failure time t_j (see Table 5.1). Methods such as Newton-Raphson method can be used to solve the aforementioned system of equations (Ebeling, 1997).

(ii) Least square method

The cumulative density function of Weibull distribution is given by:

$$F(t) = 1 - Exp(-(\frac{t}{\theta})^{\beta}) \qquad \textbf{5.18}$$

Following the common procedure of least square method and seeking for a regression equation in the form of $y = ax + b$, Equation 5.19 is derived by taking the natural logarithm of Equation 5.18 twice:

$$Ln(Ln\frac{1}{1-F(t_j)}) = \beta Lnt_j - \beta\sum_{i=0}^{k} a_i x_{ij} \qquad \textbf{5.19}$$

Assuming $y_j = Ln(Ln\frac{1}{1-F(t_j)})$, Equation 5.19 would become as:

$$y_j = \beta Lnt_j - \beta a_0 - \beta a_1 x_{1j} - \beta a_2 x_{2j} \qquad \textbf{5.20}$$

Thus, having a sample of failure times and the associated covariates, such as those listed in Table 5.1, the regression line $y = b_1 + b_2 Lnt + b_3 x_1 + b_4 x_2$ can be determined using multiple regression models. In the regression line, $b_1 = -\beta a_0$, $b_2 = \beta$, $b_3 = -\beta a_1$ and $b_4 = -\beta a_2$.

5.8 References

Bearfield G, Marsh W. Generalizing event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science 2005; 3688: 52-66.

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improvement the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety 2001; 71: 249-60.

Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 2005; 87: 337-49.

Bucci P, Kirschenbaum J, Mangan LA, Aldemir T, Smith C, Wood T. Construction of event-tree/fault-tree models from a Markov approach to dynamic system reliability. Reliability Engineering and System Safety 2008; 93: 1616-1627.

CCPS. Guidelines for chemical process quantitative risk analysis. 2nd edition, AIChE. Center for Chemical Process Safety, New York; 2000.

Chevreau FR, Wybo JL, Cauchois D. Organizing learning processes on risks by using the bow-tie representation. Journal of Hazardous Materials 2006; 130: 276-83.

Ching J, Leu SS. Bayesian updating of reliability of civil infrastructure facilities based on condition-state data and fault-tree model. Reliability Engineering and System Safety 2009; 94: 1962-74.

Cockshott JE. Probability bow-ties a transparent risk management tool. Process Safety and Environmental Protection 2005; 83: 307-16.

CSB. Imperial sugar dust explosion and fire final investigation report. http://www.csb.gov/; 2009 (last checked on 20.7.2011).

Delvosalle C, Fievez C, Pipart A, Casal Fabrega J, Planas E, Christou M, Mushtaq F. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety 2005; 90: 238-46.

Delvosalle C, Fievez C, Pipart A, Debray B. ARAMIS project: a comprehensive methodology for the identification of refernce scenarios in process industries. Journal of Hazardous Materials 2006; 130: 200-19.

Dianous VD, Fievez C. ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. Journal of Hazardous Materials 2006; 130: 220-33.

Ebeling CE. An introduction to reliability and maintainability engineering. 2nd Edition, New Delhi, McGraw Hill; 1997.

Ferson, S. Bayesian methods in risk assessment. Unpublished report prepared for the Bureau de Recherches Geologiques et Minieres (BRGM), New York; 2005.

Gowland R. The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: a step forward towards convergent practices in risk assessment? Journal of Hazardous Materials 2006; 130: 307-10.

Hall PL, Strutt JE. Probabilistic physics-of-failure models for component reliabilities using Monte Carlo simulation and Weibull analysis: A parametric study. Reliability Engineering and System Safety 2003; 80: 233-42.

Kalantarnia M, Khan F, Hawboldt K. Dynamic risk assessment using failure assessment and Bayesian theory. Loss Prevention in the Process Industries 2009; 22: 600-6.

Kalantarnia M, Khan F, Hawboldt K. Modeling of BP Texas City refinery accident using dynamic risk assessment approach. Process Safety and Environmental Protection Industries 2010; 88: 191-99.

Kelly DL, Smith CL. Bayesian inference in probabilistic risk assessment- The current state of the art. Reliability Engineering and System Safety 2009; 94: 628-43.

Khakzad N, Khan F, Amyotte P. Safety Analysis in safety facilities: comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety 2011; 96: 925-32.

Khakzad N, Khan F, Amyotte P. Dynamic Safety Analysis of Process Systems by Mapping Bow-tie into Bayesian Network. Process Safety and Environmental Protection 2012; doi: 10.1016/j.psep.2012.01.005.

Khan F. Use maximum credible accident scenarios for realistic and reliable risk assessment. Chemical Engineering Progress 2001; 11: 56-64.

Khan F, Abbasi SA. Techniques and methodologies for risk analysis in chemical process industries. Loss Prevention in the Process Industries 1998; 11: 261-77.

Lunn DJ, Thomas A, Best N, Spiegelhalter D. WinBUGS- a Bayesian modeling framework: concepts, structure, and extensibility. Statistics and Computing 2000; 10: 325-37.

Markowski AS, Mannan MS, Bigoszewska A. Fuzzy logic for process safety analysis. Loss Prevention in the Process Industries 2009; 22: 695-702.

Marquez D, Neil M, Fenton N. Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering and System Safety 2010; 95: 412-25.

Meel A, Seider WD. Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science 2006; 61: 7036-56.

OREDA. Offshore Reliability Data Handbook. SINTEF Industrial Management. Det Norske Veritas; 2002.

Rathnayaka S, Khan F, Amyotte P. SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study. Process Safety and Environmental Protection 2011b; 89: 75-88.

Siu NO, Kelly DL. Bayesian parameter estimation in probabilistic risk assessment. Reliability Engineering and System Safety 1998; 62: 89-116.

Shalev DM, Tiran J. Condition-based fault tree analysis (CBFTA): A new method for improved fault tree analysis (FTA), reliability and safety calculations. Reliability Engineering and System Safety 2007; 92: 1231-41.

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 2010, doi: 10.1016/j.engappai.2010.06.002.

Xing L, Fleming KN, Loh WT. Comparison of Markov model and fault tree approach in determining initiating event frequency for systems with two train configurations. Reliability Engineering and System Safety 1996; 53: 17-29.

6 Dynamic Safety Analysis of Process Systems by Mapping Bow-tie into Bayesian Network[‡]

Preface

A version of this manuscript has been published in the *Journal of Process Safety and Environmental Protection*. The co-authors, Dr. Khan and Amyotte supervised the principal author, Khakzad, to develop the research on the entitled topic and helped him to conceptualize the techniques and theories available for this topic. Khakzad conducted accident modeling and associated analyses while Khan and Amyotte reviewed the manuscript and provided the necessary suggestions.

Abstract

Among the various techniques used for safety analysis of process systems, bow-tie (BT) analysis is becoming a popular technique as it represents an accident scenario from causes to effects. However, the BT application in the dynamic safety analysis is limited due to the static nature of its components, i.e. fault tree and event tree. It is therefore difficult in BT to take accident precursors into account to update the probability of events and the consequent risk. Also, BT is unable to represent conditional dependency. Event dependency is common among primary events and safety barriers. The current paper

[‡] Khakzad et al. Process Safety and Environmental Protection 2012.

scenarios due to its flexible structure. This paper also introduces the application of probability adapting in dynamic safety analysis rather than probability updating. A case study from the U.S. Chemical Safety Board has been used to illustrate the application of both BT and BN techniques, with a comparison of the results from each technique.

Keywords: Dynamic safety analysis, Bow-tie approach, Bayesian network, Probability adapting.

6.1 Introduction

Process systems are prone to devastating accidents because they deal with hazardous material at high temperature and/or pressure. Process plants are also characterized as complex systems where a dense cluster of pipes and facilities makes it likely that an accident in a given facility causes loss in neighboring facilities, leading to a chain of accidents (Khan & Abbasi, 1998). So, the implementation of safety measures followed by a comprehensive risk assessment is crucial to maintain the level of risk below the acceptance criteria. Risk assessment methodologies such as quantitative risk analysis (QRA), probabilistic safety analysis (PSA), and optimal risk analysis (ORA) comprise different steps among which accident scenario analysis is a common task. Accident scenario analysis includes accident sequence modeling and consequence assessment (Khan, 2001). Several methodologies have been used for accident scenario analysis, each of which benefits from different techniques. For example, Sklet (2006) used barrier block diagrams to investigate hydrocarbon release accidents on offshore platforms. Delvosalle et al. (2005) used the bow-tie (BT) technique in ARAMIS project to identify major and

reference accident scenarios in process plants. However, it is difficult to find a single technique to completely capture different phases of an accident from the beginning to the end, and also being flexible enough to fit a variety of accidents. Nivolianitou et al. (2004) made a comparison between some selected techniques such as fault trees, event trees, and Petri nets for accident investigation, considering criteria such as event sequence, event dependency, and modeling assumptions. There are also other relevant works in the literature such as that of Khan & Abbasi (1998), Sklet (2004), and Zheng & Liu (2009), devoted to qualitative comparison among different techniques.

Among accident analysis models, BT has been well proven to be a reliable and efficient tool, partly due to its ability to incorporate both causes and consequences of an accident in a graphical model. It has been widely used in different safety and risk contexts such as process safety analysis (Markowski et al., 2009), accident risk assessment (Chevreau et al., 2006; Delvosalle et al., 2005; Delvosalle et al., 2006; Dianous and Fievez , 2006; Gowland 2006), risk management (Cockshott, 2005), and safety barrier implementation (Badreddine and Ben Amor, 2010).

However, as BT consists of a fault tree and an event tree, it suffers limitations of both the constituents. For example, standard fault trees are not suitable for accident scenarios where redundant, common cause or dependent failures take place (Bobbio et al., 2001, Khakzad et al., 2011). Fault trees are also incapable of incorporating multi-state variables, which are frequently encountered in process systems modeling. More importantly, due to their static structures, fault trees and event trees cannot adapt themselves to the dynamicity of accidents. In other words, these techniques cannot use

the real-time information directly obtained from a facility to update prior beliefs, i.e. prior failure probability of primary events and safety barriers.

To relax the discussed limitations of the abovementioned approaches, some authors have used Bayesian inference, in which uncertainty handling and belief updating are inherent characteristics. In such approaches, Bayes' theorem is coupled with standard fault tree (Ching & Leu, 2009), event tree (Meel & Seider, 2006; Kalantarnia et al., 2009; Rathnayaka et al., 2011), and bow-tie analysis (Badreddine & Ben Amor, 2010). Although Bayes' theorem helps to obtain posterior probabilities, it necessitates identifying likelihood functions, which is a difficult task if it is not a conjugate distribution to prior probability (Ferson, 2005; Meel and Seider, 2006).

On the other hand, the BN not only benefits from Bayes' theorem to provide updated probabilities, it also takes full advantage of its flexible structure to fit a wide variety of accidents. Bobbio et al. (2001), Boudali & Dugan (2005), Marsh & Bearfield (2007), Montani et al. (2008), and Khakzad et al. (2011) mapped fault trees into BNs, while Bearfield & Marsh (2005) performed similar mapping for an event tree. Recently, Weber et al. (2010) presented an exhaustive review of BN application in dependability, maintenance and risk analysis, and also compared BNs with other methods such as fault trees, Markov chains, and Petri nets.

The present study demonstrates how the limitations of BT, resulting mostly from its static constituents, can be relaxed by mapping it into a corresponding BN. The study also considers various practical modeling aspects offered by BN, making it a well-suited technique for dynamic safety analysis. A brief description of BT, BN, and the mapping

algorithm from BT to BN, mostly based on the works of Bobbio et al. (2001) and Bearfield & Marsh (2005), is presented in Section 6.2. Section 6.3 briefly describes a process accident used as the case study while Section 6.4 applies the methodology to dynamic safety analysis of the accident scenario, comparing the results and showing the BN modeling features of which the BT is incapable. Section 6.5 is devoted to the conclusions of the current work.

6.2 Safety Analysis Techniques

6.2.1 Bow-tie model

BT is one of the best graphical approaches to represent a complete accident scenario, starting from accident causes and ending with its consequences. While centered on a critical event, BT is composed of a fault tree on the left-hand side identifying the possible events causing the critical event, and an event tree on the right-hand side showing the possible consequences of the critical event based on the failure or success of safety functions (Delvossale et al., 2005; Delvossale et al., 2006). Figure 6.1 shows a typical BT, comprised of different components such as primary events, PE_i, intermediate events, IE_i, top event, TE, safety barriers, SB_i, and accident consequences, C_i.

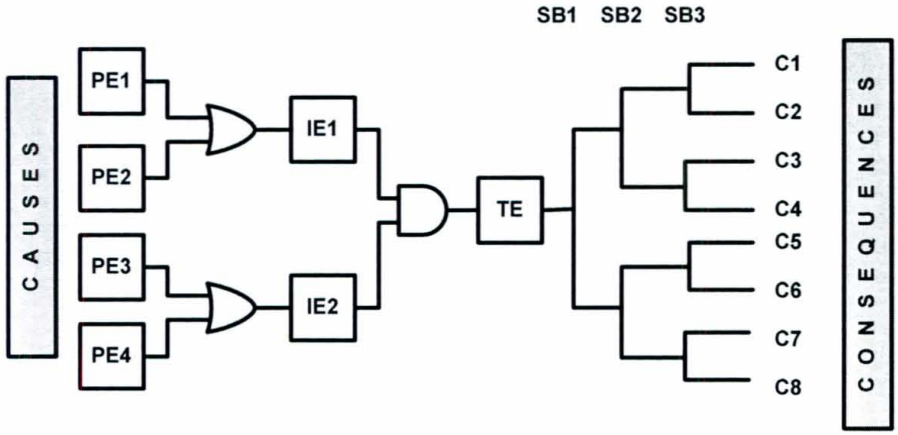


Figure 6.1. Generic Bow-tie model

It helps to understand which possible combination of primary events will lead to the top event in the fault tree and which safety function failures will escalate the top event to a particular consequence in the event tree. For example, the occurrence probability of consequence C_4 in Figure 6.1 can be assessed as:

$$P(C_4) = P(TE)P(\overline{SB}_1)P(SB_2)P(SB_3) \quad 6.1$$

Where $P(TE)$ is the top event probability; $P(\overline{SB}_1)$ refers to the non-failure probability of SB_1 while $P(SB_2)$ and $P(SB_3)$ refer to the failure probability of SB_2 and SB_3, respectively.

6.2.2 Bayesian Network

Similar to BT, BN is a graphical technique, which has been widely used in risk and safety analysis based on probabilistic and uncertain knowledge. BN is a directed acyclic graph, in which the nodes represent variables, arcs signify direct causal relationships between

the linked nodes, and Conditional Probability Tables (CPTs) assigned to the nodes denote conditional dependencies.

Based on the conditional independence, resulting from the d-separation concept (Pearl, 1988), and the chain rule, BN represents the joint probability distribution $P(U)$ of variables $U = \{A_1, \dots, A_n\}$, included in the network as:

$$\boldsymbol{P(U) = \prod_{i=1}^{n} P(A_i | Pa(A_i))} \qquad \textbf{6.2}$$

where $Pa(A_i)$ is the parent set of A_i (Jensen and Nielsen, 2007).

BN takes advantage of Bayes theorem to update the prior occurrence (or failure) probability of events given new information, called evidence E, thus yielding the posteriors. This new information usually becomes available during the operational life of a process, including occurrence or non-occurrence of accident or primary events:

$$\boldsymbol{P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)}} \qquad \textbf{6.3}$$

6.2.3 Mapping Algorithm

6.2.3.1 Fault Tree Mapping

Mapping from the fault tree into the BN is based on the work of Bobbio et al. (2001), including a graphical and numerical translation. In the graphical step, the structure of BN is developed from the fault tree such that primary events, intermediate events, and the top event of the fault tree are represented as root nodes, intermediate nodes, and the leaf node in the equivalent BN, respectively.

The nodes of BN are connected in the same way as the corresponding events in the fault tree. In the numerical step, occurrence probabilities of the primary events are assigned to the corresponding root nodes as prior probabilities. For each intermediate node as well as the leaf node, a CPT is assigned. CPTs illustrate how intermediate nodes are related to precedent intermediate or root nodes (e.g., see Bobbio et al., 2001).

6.2.3.2 Event Tree Mapping

Mapping from the event tree into the BN is mainly based on the work of Bearfield & Marsh (2005). Each safety barrier of the event tree is represented by a safety node having two states, one for the failure and the other for the success of the safety barrier. Also, a consequence node having as many states as the number of the event tree consequences (i.e., C_i in Figure 6.1) is added to the network.

When mapping event tree into BN, the safety node SB_i is connected to the previous safety node, SB_{i-1}, only if the failure probability of SB_i depends on whether SB_{i-1} has worked or failed. In other words, SB_i must be connected to SB_{i-1} only if $P(SB_i|SB_{i-1}) \neq P(SB_i|\overline{SB}_{i-1})$. Similarly, the safety node SB_{i+1} must also be connected to SB_{i-1} if $P(SB_{i+1}|SB_{i-1}, SB_i) \neq P(SB_{i+1}|\overline{SB}_{i-1}, SB_i)$. In addition, there must be a connection between each safety node and the consequence node only if the probabilities of the states of the consequence node are influenced by the failure or the success of that safety node. After the BN is constructed, the probabilities of safety barriers are considered as the prior probabilities of safety nodes, and a CPT is assigned to the consequence node, as well as to the intermediate safety nodes. It is worth noting that

while the CPT of the consequence node acts like a logical AND-gate, the CPTs assigned to the safety nodes represent simple causal relationships, different from logical AND and OR-gates frequently encountered in fault-tree based BNs.

6.2.3.3 Bow-tie Mapping

After the equivalent BNs of the fault tree and the event tree are developed, they are connected to each other via the top event as a pivot node. The top event node is connected to the consequence node, and also other states, e.g., *Safe state*, is added to the consequence node, taking into account the effect of the non-occurrence of the top event on the consequence node. For example, consider the BT in Figure 6.2, in which a set of primary events causes a gasoline release.

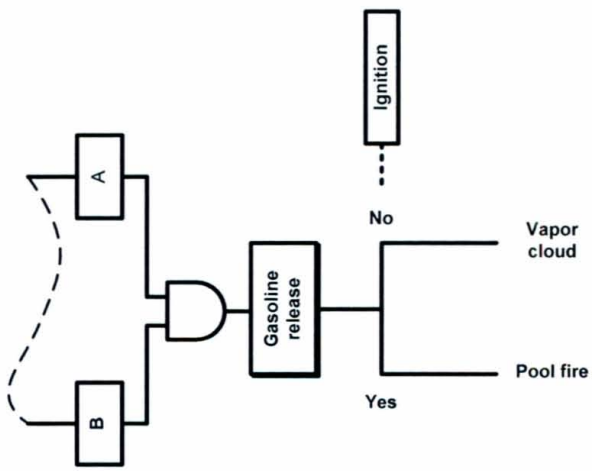


Figure 6.2. Bow-tie model for gasoline release accident scenario. For the sake of brevity, the fault tree part is not completely illustrated

Depending on the states of the ignition source, the gasoline release accident could result in two consequences, i.e., a pool fire (*Ignition* = *yes*) or vapor cloud (*Ignition* = *no*). However, when the corresponding BN is developed (Figure 6.3), another consequence can also be resulted from the state combination of nodes *Gasoline release* and *Ignition* (Table 6.1).

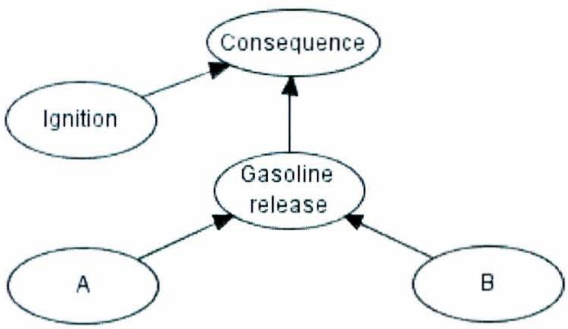


Figure 6.3. BN model for gasoline release accident scenario

Table 6.1. Possible states of Consequence based on the state combination of Gasoline release and Ignition

Gasoline release	Ignition	Consequence
Yes	Yes	Pool fire
Yes	No	Vapor cloud
No	Yes	Safe
No	No	Safe

So, unlike the BT, the node Consequence in the BN of Figure 6.3 has three states, namely *pool fire*, *vapor cloud* and *safe*. It is worth noting that as the sates of node *Consequence* are influenced by node *gasoline release*, there should be a causal arc from the latter to the

former. On the other hand, because the probability of ignition does not presumably depend on whether there is a release or not, node *gasoline release* is not connected to node *Ignition*. Generally, if $P(SB_i|TE) \neq P(SB_i|\overline{TE})$, a causal arc must be directed from the top event, TE, to the safety barrier SB_i. Figure 6.4 illustrates the simplified mapping algorithm of BT into BN.

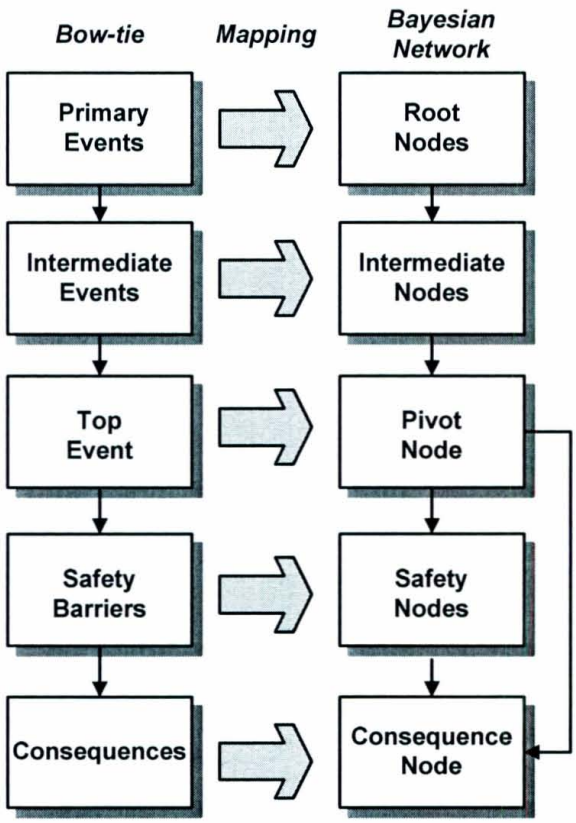


Figure 6.4. Mapping algorithm from bow-tie into BN.

Although able to consider the dependency of sequential safety barriers, BT cannot capture the dependency of safety barriers on the top event. This is because the top event is simply an initiating event for the event tree, and cannot influence the failure or success probability of safety barriers. On the other hand, BN accommodates such dependence by means of causal arcs drawn from the top event to those safety barriers whose failure probabilities depend on the occurrence and non-occurrence of the top event. For example, according to the accident scenario described above, *Gasoline release* and *Ignition* would be no longer independent if static electricity were generated due to the release (Crowl and Louvar, 2002), increasing the ignition probability. Figure 6.5 shows a generic BN which can be equivalent to the BT in Figure 6.1.

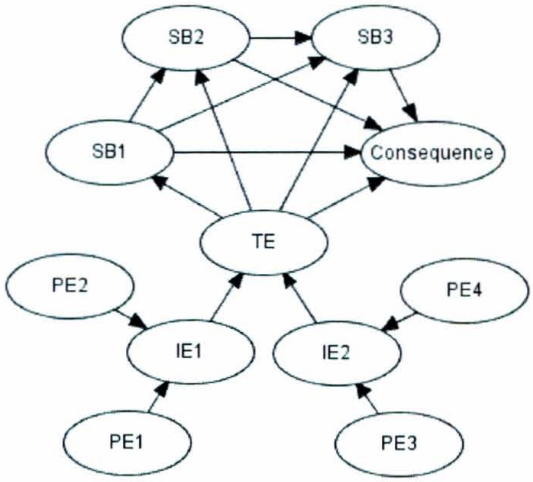


Figure 6.5. Generic BN potentially equivalent to the bow-tie in Figure 6.1.

6.3 Case Study: Vapor Ignition

To implement the previously described methodology, a vapor cloud ignition at Universal Form Clamp, Inc., Bellwood, Illinois, U.S. on June 14, 2006 was selected as the accident scenario. According to the case study issued by the U.S. Chemical Safety Board (CSB, 2007), a flammable vapor cloud consisting of heptanes and mineral spirits overflowed from an open top mixing and heating tank. The vapor cloud ignited as it met unknown ignition sources, leading to one death, two injuries and significant business interruption.

The tank was equipped with steam coils supplying it with heat needed for the mixing process. A temperature controller composed of a temperature sensor and a pneumatic control unit was installed to operate the steam valves based on the mixture temperature. In addition to the aforementioned control system, an operator was supposed to check the temperature using an infrared thermometer and to take any necessary actions. The tank was also equipped with local exhaust ventilation at the top to control vapors (Figure 6.6).

According to the full-scale investigation conducted by the Chemical Safety Board (CSB, 2007), a malfunction of the temperature control system allowed the steam valves to remain open long enough to heat the mixture to its boiling point, generating a high volume of vapor. Consequently, the failure of the local ventilation system due to a broken fan belt caused the vapor cloud to spill from the tank and finally ignites when exposed to an ignition source. It was also found that even if the ventilation system had been working, it would not have had enough capacity to collect such a high volume of vapor.

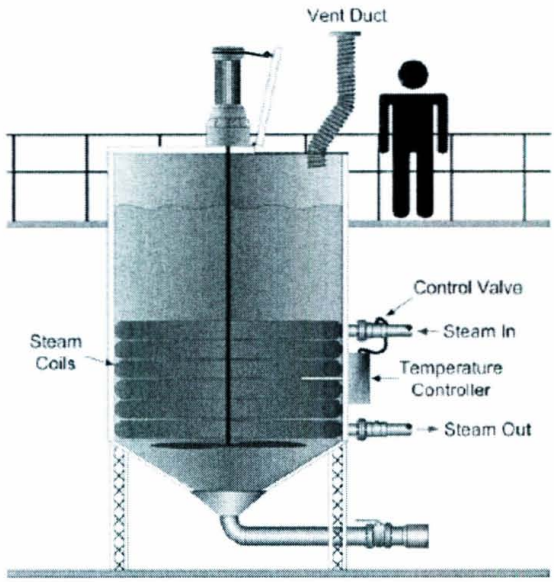


Figure 6.6. Mixing tank and safety measures (CSB, 2007).

6.4 Methodology Application

6.4.1 Bow-tie Analysis

Following the accident description, a BT was developed to investigate the envisaged accident scenarios and the effectiveness of the various safety measures (Figure 6.7). The accident components, their symbols and failure probabilities (OREDA, 2002) are listed in Table 6.2. Because the vapor cloud is non-toxic, it has been assumed that any fatalities or injuries are due to vapor ignition, not the vapor itself.

It should be noted that the failure probabilities of safety barriers *Sprinkler* and *Alarm* are influenced by either safety barrier *Ignition* or top event *Vapor*, showing the conditional dependency of the former on the latter. *Sprinkler* and *Alarm* are activated if vapor is

ignited, i.e. when *Vapor= Overflow* and *Ignition= Spark*, but with failure probabilities equal to 0.04 and 0.0013, respectively. On the other hand, *Alarm* can also be stimulated by a particular amount of vapor concentration in the air even if it is not ignited, i.e. when *Vapor= Overflow* and *Ignition= No spark*, but with a failure probability equal to 0.225.

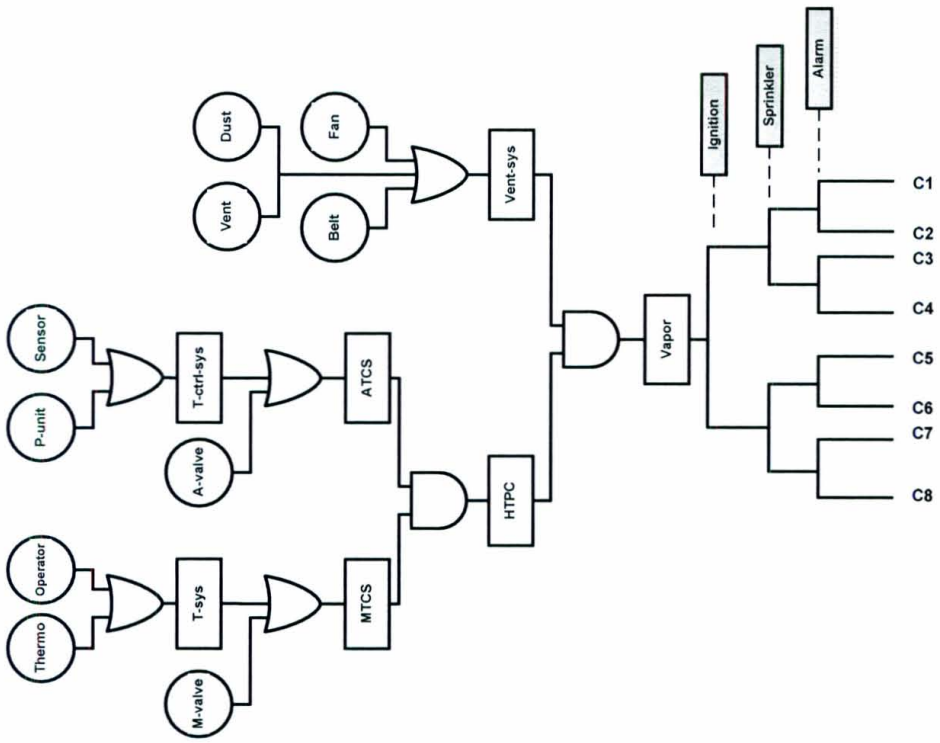


Figure 6.7. BT model for the heat exchanger accident scenario (CSB, 2007).

Table 6.2. Components of the bow-tie in Figure 6.7 and their probabilities

Event	Symbol	Failure Probability
Sensor	Sensor	0.0400

Pneumatic unit	P-unit	0.2015
Temperature control system	T-ctrl-sys	OR-gate
Operator	Operator	0.0200
Infrared Thermometer	Thermo	0.0468
Temperature measurement system	T-sys	OR-gate
Manual steam valve	M-valve	0.0243
Automatic steam valve	A-valve	0.0276
Automatic temperature control system	ATCS	OR-gate
Manual temperature control system	MTCS	OR-gate
High temperature protection system	HTPS	AND-gate
Inadequate ventilation	Vent	0.0150
Fan failure	Fan	0.0100
Belt failure	Belt	0.0500
Duct plugging	Duct	0.0010
Ventilation system	Vent-sys	OR-gate
Vapor overflow	Vapor	AND-gate
Ignition barrier	Ignition	0.1000
Water sprinkler system	Sprinkler	0.0400
Alarm system	Alarm	0.0013, 0.2250

Table 6.3 shows eight consequences that can be envisaged for the accident scenario depending on the success or failure of the sequential safety barriers. It has been assumed that even if there is no fire (i.e. *Ignition= No spark*), the operation of *Sprinkler* will lead to a safer mode compared to its failure. This is because the operation of *Sprinkler* can possibly reduce the probability of latter ignitions (delayed ignitions). Thus, consequences C_1 and C_2 are less severe than C_3 and C_4, respectively.

Table 6.3. Consequences of the vapor overflow accident scenario

Event	Symbol

Safe evacuation	C_1
Wet vapor cloud near the ground	C_2
Safe evacuation with possibility of delayed ignition	C_3
Vapor cloud with possibility of delayed ignition	C_4
Fire, moderate property damage, low death toll	C_5
Fire, moderate property damage, high death toll	C_6
Fire, high property damage, low death toll	C_7
Fire, high property damage, high death toll	C_8

Assigning the probabilities listed in Table 6.2 to the primary events and the safety barriers of the BT, the probabilities of top event, and accident consequences are calculated and presented in Table 6.4.

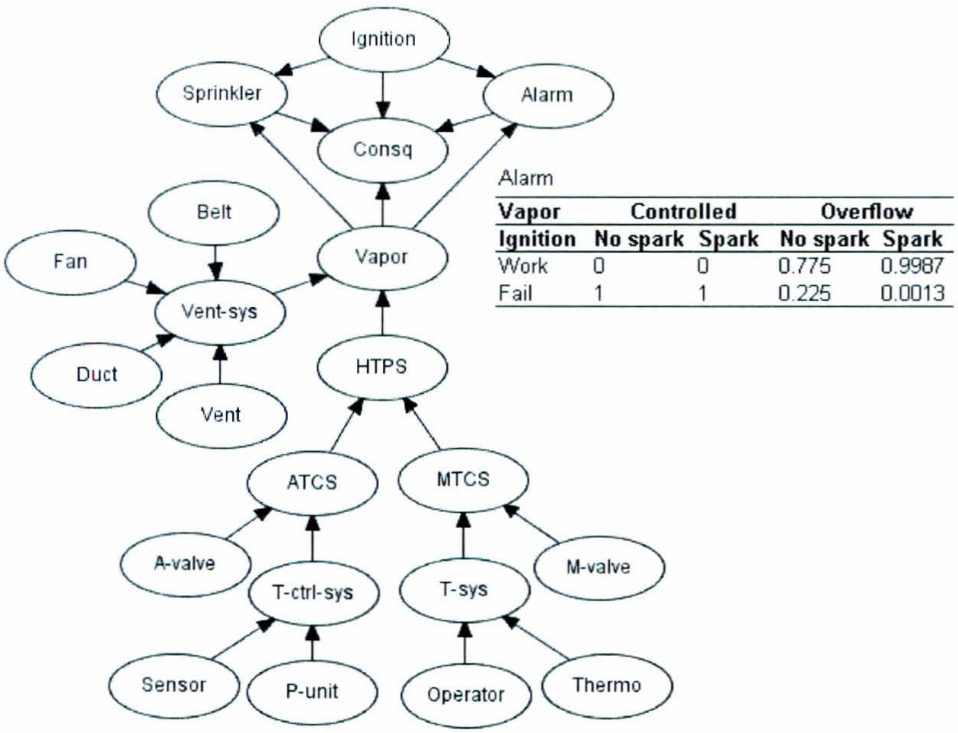
Table 6.4. Accident analysis results for BT and BN techniques

Symbol	Probability
Vapor	1.68E-03
C_1	0.00E+00
C_2	0.00E+00
C_3	1.04E-03
C_4	3.03E-04
C_5	3.23E-04
C_6	4.21E-07
C_7	1.35E-05
C_8	1.75E-08

6.4.2 Bayesian Network Analysis

6.4.2.1 Accident Analysis

To verify the mapping procedure introduced in this study, a BN (Figure 6.8) was developed from the BT in Figure 6.7, following the steps illustrated in Figure 6.4. All the nodes of the BN have been previously described in the BT except the node *Consq*, which is the consequence node, added to accommodate the outcomes of the BT.



Alarm

Vapor	Controlled		Overflow	
Ignition	No spark	Spark	No spark	Spark
Work	0	0	0.775	0.9987
Fail	1	1	0.225	0.0013

Figure 6.8. Corresponding BN of bow-tie in Figure 6.7.

By connecting node *Vapor* to *Consq*, another state, namely *Safe* state, is added to the state set including consequences C_1 to C_8 to account for the non-occurrence of the top event, i.e. *Vapor= Controlled*. To show the dependency among the safety barriers and the top event, causal arcs are also drawn from *Ignition* and *Vapor* to *Sprinkler* and *Alarm*. As an example, the CPT of *Alarm* is embedded in Figure 6.8. It is worth noting that since various combinations of the failure and success of the sequential safety barriers result in different consequences in the BT, all the safety nodes of the BN are connected to node *Consq*. Assigning the probabilities listed in Table 6.2 as the priors, the BN is analyzed using HUGIN 7.4 (http://www.hugin.com), resulting in the same probabilities as those obtained from the BT (Table 6.4).

6.4.2.2 Probability Updating

Once it is confirmed that the BT and BN are equally able to analyze the accident scenario, the BN is used to update the probabilities by taking the evidence into account, a task which BT is incapable of doing. Two types of probability updating can be performed using BN, depending on the type of evidence propagated in the network.

The first type, commonly referred to as probability updating, calculates the posterior probability of event x_i given a certain state of event Q, i.e. $P(x_i|Q)$. It is usually performed to find the most probable explanation (MPE) of event states leading to the accident or a specific consequence (Bobbio et al., 2001; Khakzad et al., 2011).

In the current study, the state of node *Consq* was instantiated to C_5 denoting that it is known a fire with moderate property damage and low number of fatality is observed in

the process plant. After the posterior probability of the other nodes due to this evidence, i.e. $P(x_i|Consq = C_5)$, is calculated, the most probable explanation is determined to be the failure of *P-unit*, *Thermo* and *Belt*, causing the *Vapor*, which in turn results in *Fire* (C_5), provided that *Ignition* = *Spark*, *Sprinkler* = *Work* and *Alarm* = *Work*. The probability of MPE is 0.244.

6.4.2.3 Probability adapting

The second type of updating, referred to as probability adapting, calculates the posterior probability of event x_i given that event Q has been occurred n times, i.e. $P(x_i|Q = n)$. It uses prior experience to perform probability updating, in which conditional probability distributions are adapted using the cumulative information collected during a time interval, e.g. one year, as evidence. Although this kind of evidence is widely used to develop likelihood functions for probability updating using Bayes theorem (e.g. Meel & Seider, 2006; Kalantarnia et al., 2009; Rathnayaka et al., 2011), it has not been commonly used in accident scenario modeling and process safety assessment conducted using the BN technique. In the present study, the hypothetical prior experience obtained during four years of process operation is used for illustrative purposes. Table 6.5 shows the occurrence number of consequences in each year.

Table 6.5. Experience used to adapt the prior probabilities.

Consequence	Year 1	Year 2	Year 3	Year 4
C_3	3	1	2	1
C_5	-	1	-	-
C_6	-	-	-	1

For example, updated probabilities using information at the end of the second year are estimated using probabilities in the form of $P(x_i|Consq = 4C_3\ and\ C_5)$, showing the posterior probability of event x_i given that C_3 has cumulatively occurred four times during the first two years, while C_5 has occurred one time. Figures 6.9 and 6.10 show the probability adapting results for primary events, top event, and safety barriers, respectively, which have been cumulatively updated at the end of each year for four sequential years. In these figures, year 0 denotes the priors.

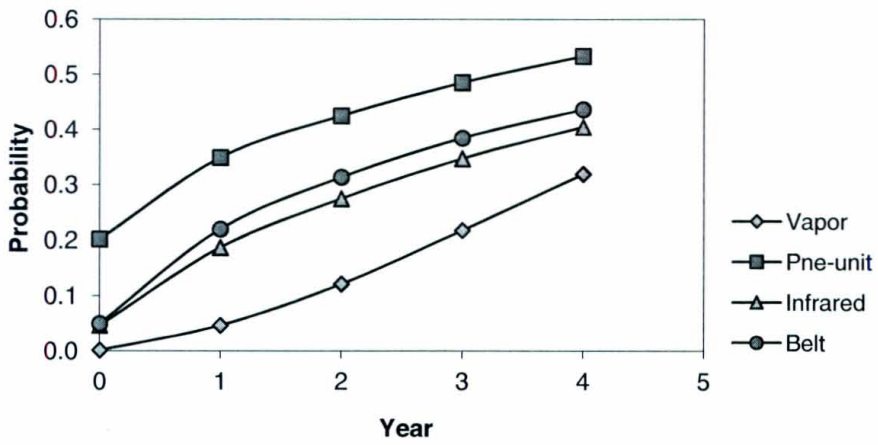


Figure 6.9. Updated probabilities of the primary events and the top event (Vapor).

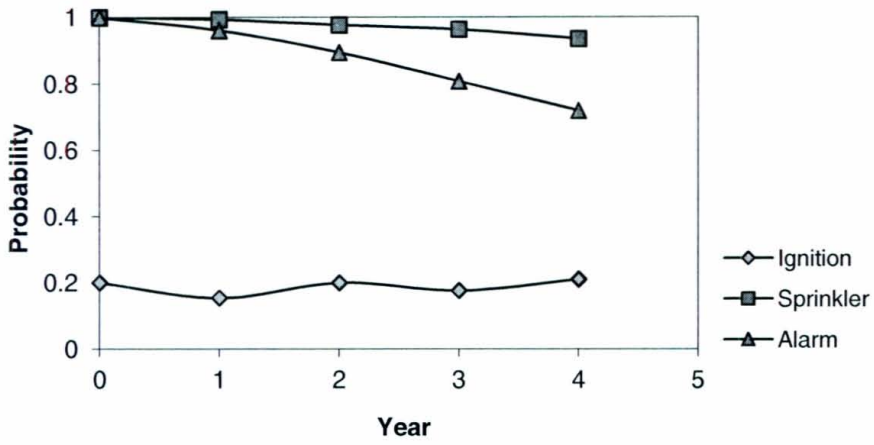


Figure 6.10. Updated probabilities of the safety barriers.

It is worth noting that the failure probabilities of the primary events and top event are increasing while those of the safety barriers either remain constant or decrease. This can be described using, for example, the data of year 4, i.e. the occurrence of consequences C_3 and C_6. The occurrence of C_3 implies that *Ignition* = *No spark*, *Sprinkler* = *Fail*, and *Alarm* = *Work*, while the occurrence of C_6 means that *Ignition* = *Spark*, *Sprinkle* = *Work*, and *Alarm* = *Fail*. In other words, there are observations suggesting that each safety barrier has been equally observed working or failing during the year. This is why the failure probabilities of the safety barriers illustrate either a constant or declining trend

On the other hand, the occurrences of C_3 and C_6 demonstrate that the accident's top event (i.e. vapor overflow) has occurred two times during the same year. Thus, the occurrence number of the top event is always greater than or equal to the maximum failure numbers of each safety barrier. Therefore, its occurrence probability increases rapidly. Also, the information about the occurrence frequency of the top event propagates backwards

through the network, increasing the probability of the primary events. It can also be implied from Figure 6.10 that although *Ignition* has the lowest failure probability among the safety barriers shown, its failure probability illustrates an approximately constant trend, showing it has gained the lowest attention compared to the other two safety barriers.

Using the updated top event and safety barriers, it is possible to dynamically update the probability of those consequences for which no information is available. For example, Figure 6.11 represents the updated probability of consequence C_8 even though it is not observed until the end of year 4 (Table 6.5).

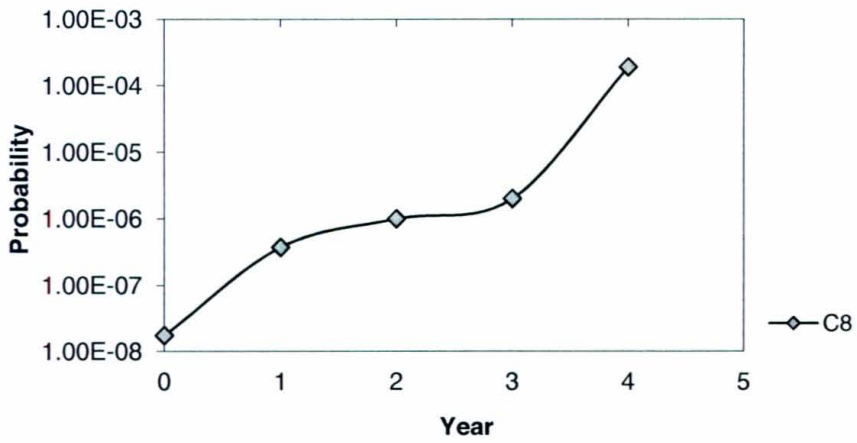


Figure 6.11. Updated probability of C_8 over the course of 4 years.

Figure 6.11 illustrates that during four years, the occurrence frequency of the most damaging consequence, i.e. C_8, has increased by four orders of magnitude. Thus, if the safety measures of the system are not improved, the occurrence of C_8 can be expected in

the near future. Probability adapting can be therefore effectively used as a predictive tool to investigate the effectiveness and adequacy of a system's safety measures.

Through probability adapting and using sequentially observed accident precursors, the generic prior probabilities which are assigned to the events at the design stage are updated to more case-specific posterior probabilities. So, the generality arisen from using the generic priors is gradually reduced by using the accident-derived data.

6.5 Conclusion

The present study has illustrated that BN is an effective technique for dynamic safety analysis of process systems. It also has been shown that by mapping BT into BN, the BT's limitations (mainly resulting from its static constituents) can be relaxed. In addition, conditional dependencies can be better illustrated in BN by means of direct causal arcs among dependent variables. The paper has also used unique BN modeling aspects to dynamically update probabilities, to gradually replace generic priors with more case-specific posteriors, and to predict occurrence frequency of consequences as well as accident components.

The current paper applied probability adapting, rather than probability updating, to dynamically revise the prior probability of accident components; this is a new approach for process system safety analysis. In probability updating, the information about a node instantiated to one of its states is used as evidence; it is mainly used to determine the most probable explanation leading to that particular state. On the other hand, in probability adapting, the information about the cumulative number of times an accident

has occurred during a time interval is used as evidence. This helps to dynamically assess the system's safety and to predict the occurrence likelihood of consequences.

The present study has shown that probability adapting is more effective than probability updating in dynamic safety analysis although it has not been considered in process safety analysis as much as probability updating. Through probability adapting, the effect of generic prior probabilities reduces as they are updated using the accident observations.

Acknowledgment

The authors gratefully acknowledge the financial support provided by the Natural Sciences and Engineering Research Council (NSERC) of Canada and Petroleum Research Atlantic Canada (PRAC). The first author would also like to thank anonymous reviewers whose comments helped to improve the work.

6.6 References

Badreddine, A., & Ben Amor, N. (2010). A dynamic barriers implementation in Bayesian-based bow tie diagrams for risk analysis. Proceedings of International Conference on Computer Systems and Applications, 1-8.

Bearfield, G., & Marsh, W. (2005). Generalising event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science, 3688, 52-66.

Bobbio, A., Portinale, L., Minichino, M., & Ciancamerla, E. (2001). Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Journal of Reliability Engineering and System Safety, 71, 249-260.

Boudali, H., & Dugan, J.B. (2005). A new Bayesian approach to solve dynamic FTs. Proceedings of Reliability and Maintainability Symposium (RAMS'05), 451-456.

CSB. (2007). Mixing and heating a flammable liquid in an open top tank. Investigation No. 2006-08-I-IL, April 2007, Washington, DC. http://www.csb.gov/assets/document/CSBUniversalFormClampCaseStudy.pdf (last checked on 20.04.2011).

Ching, J., & Leu, S.S. (2009). Bayesian updating of reliability of civil infrastructure facilities based on condition-state data and fault-tree model. Journal of Reliability Engineering and System Safety, 94, 1962-1974.

Cockshott, J.E. (2005). Probability bow-ties a transparent risk management tool. Process Safety and Environmental Protection, 83, 307-316.

Crowl, D.A., & Louvar J.F. (2002). Chemical process safety: fundamentals with applications. 2nd edition. Prentice Hall PTR. New Jersey.

Delvosalle, C., Fievez, C., Pipart, A., Casal Fabrega, J., Planas, E., Christou, M., and Mushtaq, F. (2005). Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety, 90, 238-246.

Delvosalle, C., Fievez, C., Pipart, A., & Debray, B. (2006). ARAMIS project: a comprehensive methodology for the identification of refernce scenarios in process industries. Journal of Hazardous Materials, 130, 200-219.

Dianous V.D., & Fievez, C. (2006). ARAMIS project: a more explicit demonstration of risk control through the use of bow-tie diagrams and the evaluation of safety barrier performance. Journal of Hazardous Materials, 130, 220-233.

Ferson, S. (2005). Bayesian methods in risk assessment. Unpublished report prepared for the Bureau de Recherches Geologiques et Minieres (BRGM), New York.

Gowland, R. (2006). The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: a step forward towards convergent practices in risk assessment?. Journal of Hazardous Materials, 130, 307-310.

HUGIN Expert software version 7.4 (2010). http://www.hugin.com.

Kalantarnia, M., Khan, F., & Hawboldt, K. (2009). Dynamic risk assessment using failure assessment and Bayesian theory. Journal of Loss Prevention in the Process Industries, 22, 600-606.

Khakzad, N., Khan, F., & Amyotte, P. (2011). Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. Journal of Reliability Engineering and System Safety, doi:10.1016/j.ress.2011.03.012.

Khan, F., & Abbasi, S. A. (1998). Techniques and methodologies for risk analysis in chemical process industries. Journal of Loss Prevention in the Process Industries, 11, 261-277.

Khan, F. (2001). Use maximum-credible accident scenario for realistic and reliable risk assessment. Chemical Engineering Progress, 11, 56-64.

Markowski, A.S., Mannan, M.S., & Bigoszewska, A. (2009). Fuzzy logic for process safety analysis. Journal of Loss Prevention in the Process Industries, 22, 695-702.

Marsh, W., & Bearfield, G. (2007). Representing parameterised fault trees using Bayesian networks. Lecture Notes in Computer Science, 4680, 120-133.

Meel, A., & Seider, W. D. (2006). Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science, 61, 7036-7056.

Montani, S., Portinale, L., Bobbio, A., & Codetta-Raiteri, D. (2008). RADYBAN: A tool for reliability analysis of dynamic FTs through conversion into dynamic Bayesian networks. Journal of Reliability Engineering and System Safety, 93, 922-932.

Nivolianitou, Z.S., Leopoulos, V.N., & Konstantinidou, M. (2004). Comparison of techniques for accident scenario analysis in hazardous systems. Journal of Loss Prevention in the Process Industries, 17, 467-475.

OREDA. (2002). Offshore Reliability Data Handbook. SINTEF Industrial Management. Det Norske Veritas.

Pearl, J. (1988). Probabilistic Reasoning in Intelligent Systems, Morgan Kaufmann, San Francisco, California. ISBN 0-934613-73-7.

Rathnayaka, S., Khan, F., & Amyotte, P. (2011). SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study. Process Safety and Environmental Protection, 89, 75-88.

Sklet, S. (2006). Hydrocarbon release on oil and gas production platforms: release scenarios and safety barriers. Journal of Loss Prevention in the Process Industries, 19, 481-493.

Zheng, X., & Liu, M. (2009). An overview of accident forecasting methodologies. Journal of Loss Prevention in the Process Industries, 22, 484-491.

7 Risk-based design of process systems using discrete-time Bayesian network[§]

Preface

A version of this manuscript has been published in the *Journal of Reliability Engineering and System Safety*. The co-authors, Dr. Khan and Amyotte supervised the principal author, Khakzad, to develop the research on the entitled topic and helped him to conceptualize the techniques and theories available for this topic. Khakzad conducted accident modeling and associated analyses while Khan and Amyotte reviewed the manuscript and provided the necessary suggestions.

Abstract

Temporal Bayesian networks have gained popularity as a robust technique to model dynamic systems in which the components' sequential dependency, as well as their functional dependency, cannot be ignored. In this regard, discrete-time Bayesian networks have been proposed as a viable alternative to solve dynamic fault trees without resort to Markov chains. This approach overcomes the drawbacks of Markov chains such as the state-space explosion and the error-prone conversion procedure from dynamic fault tree. It also benefits from the inherent advantages of Bayesian networks such as probability updating. However, effective mapping of the dynamic gates of dynamic fault

[§] Khakzad et al. Journal of Reliability Engineering and System Safety.

trees into Bayesian networks while avoiding the consequent huge multi-dimensional probability tables has always been a matter of concern. In this paper, a new general formalism has been developed to model two important elements of dynamic fault tree, i.e., cold spare gate and sequential enforcing gate, with any arbitrary probability distribution functions. Also, an innovative *Neutral Dependency* algorithm has been introduced to model dynamic gates such as priority-AND gate, thus reducing the dimension of conditional probability tables by an order of magnitude. The second part of the paper is devoted to the application of discrete-time Bayesian networks in the risk assessment and safety analysis of complex process systems. It has been shown how dynamic techniques can effectively be applied for optimal allocation of safety systems to obtain maximum risk reduction.

Keywords: Discrete-time Bayesian network, Dynamic fault tree, Markov chain, Neutral dependency, Safety analysis, Probabilistic risk assessment

7.1 Introduction

Among several techniques available to quantify the occurrence probability of accident scenarios or to estimate the failure probability of systems in the context of quantitative risk assessment, probabilistic safety analysis and reliability engineering, the fault tree (FT) method is the most recognized and widely used. FT is a deductive, user-friendly methodology constructed intuitively, dissecting the system for further detail until the primary causes of the system's failure or unavailability are known. FT could also be analyzed using well-established algorithms such as binary decision diagrams or analytical methods such as minimal cut sets. However, conventional or static fault trees (SFTs) are

characterized by limitations constraining their application in complex systems where, for instance, redundant failures, multi-state variables and/or sequential and functional dependencies are common.

In recent years, Bayesian networks (BNs) have become popular for reliability and risk analysis of complex systems as a robust and viable alternative to most conventional methods such as reliability block diagrams (Torres-Toledano and Sucar, 1998), FT (Bobbio et al, 2001; Langseth and Portinale, 2007; Khakzad et al., 2011) and event tree (ET) analysis (Bearfield and Marsh, 2005). BN is a probabilistic method for reasoning under uncertainty which factorizes the joint probability distribution of a set of variables by considering local dependencies, significantly reducing both the system complexity and the computational time (Bobbio et al, 2001; Langseth and Portinale, 2007; Khakzad et al., 2011 ; Boudali and Dugan, 2005; weber et al., 2010). Most recently, Weber et al. (2010) have given a statistical review of BN application and shown the appeal of Bayesian approaches in various areas of reliability, risk and maintenance engineering since 2000.

Many authors have shown the parallels between FT and BN and have examined the extent to which the limitations of the former can be relaxed by relying on the later. Bobbio et al. (2001) were the first to map FT into BN to incorporate multi-state variables and common cause failures by means of the leaking noisy-or model. They also performed a sequentially dependent failure analysis which was an example of functional dependency, i.e., without considering the temporal sequence of failures (like the performance of the functional dependency gate in dynamic fault trees). Similar efforts have been made by Langseth and Portinale (2007) to account for coverage factors in

redundant systems by means of the noisy-and model, and also by Khakzad et al. (2011) to explicitly model functional uncertainty and expert opinion in the safety analysis of process systems.

Dynamic fault tree (DFT) was introduced as an extension to SFT to model sequentially dependent failures in dynamic systems Dugan et al., 1992). In a dynamic system, the failure sequence of events is as important as their combinations for the system to be unavailable or to fail. In other words, compared to SFT in which it only matters which components participate in a minimal cut set, in DFT the failure sequence of the participating components is also important (Boudali and Dugan, 2005). DFT takes the sequential dependencies into account by using several dynamic gates such as a functional dependency gate (FDEP), cold spare gate (CSP), sequence enforcing gate (SEQ) (Dugan et al., 1992) and priority-AND gate (PAND) (Fussel et al., 1976).

Due to the sequential dependencies and dynamic behavior among the components of the system, DFT cannot be analyzed using conventional algorithms available for SFT. In this regard, DFT has traditionally been converted to the corresponding Markov chain model (MC) for which well-established and efficient solving techniques have been developed. Nevertheless, converting DFT into MC is an error-prone and cumbersome exercise (Dugan et al., 1992). Moreover, the state space of the MC (i.e., the set of its nodes) grows exponentially with the number of components of the corresponding DFT, making the MC very large and intractable. Indeed, for a MC equivalent to a DFT with m binary-state components (i.e., work/fail) for which k out of m components are sequentially dependent, the number of states is proportional to the product of 2^m (the number of state

combinations) and k! (the possible number of sequence combinations) (Boudali and Dugan, 2005). This problem is frequently encountered in Markov processes and is referred to as the state space explosion. It should be noted that even a relatively simple DFT can result in a complicated and time-consuming MC, particularly in the presence of dynamic gates cascade (Boudali and Dugan, 2005; Dugan et al., 1992; Marquez et al., 2010). Also, MC has been mentioned to have limitations in modeling dependencies among components with non-exponential failure time distributions (Marquez, 2010).

As an example, consider a parallel system consisting of three pumps A, B and C of different failure rates, in which B is planned to only operate as a standby to A. In other words, not only all three pumps have to fail for the system to fail, but also A must fail before B. Figure 7.1 illustrates the SFT (left), the DFT (middle) and the equivalent MC (right) for the failure analysis of the system.

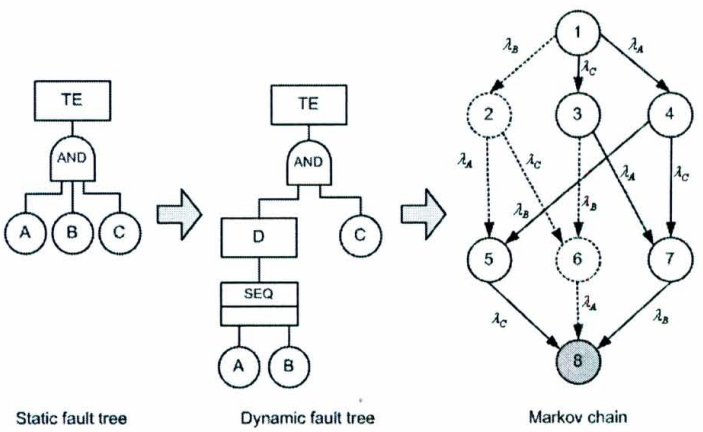


Figure 7.1. SFT (left), DFT (middle) and MC (right) models for a three-component parallel system in which A must fail before B. The dashed parts in the MC are not accounted for in the system failure due to the representation of improper failure sequences. λ is the failure rate of components.

As the SFT cannot capture sequential failures, it ignores the sequential dependence between A and B, approximating the system failure using an AND gate. On the other hand, the DFT employs a cascade of SEQ gate and AND gate to model the dynamic behavior. The DFT is then conventionally converted to the MC to be solved. Assuming a mission time of t = 100 hr and the failure rates 0.3E-03, 0.5E-03 and 0.7E-03 for A, B and C, respectively, the failure probability of the system is calculated as 9.76E-05 and 4.94E-05 using SFT and DFT (MC), respectively. This example demonstrates how the failure probability and also the consequently envisaged risk in dynamic systems can be overestimated (here by a factor of two) if dependency conditions are ignored or simplified through using static techniques.

Considering the abovementioned problems encountered in converting DFT into MC, temporal Bayesian networks (TBNs) have alternatively been proposed to explicitly incorporate time in the modeling of sequential dependencies without resort to MC. Accordingly, two different approaches have been adopted, namely: instant-based (time-sliced) approach and interval-based (event-based) approach (Boudali and Dugan, 2006). In the first approach, the time line is divided into a finite number of time instants (e.g., t_{i-1}, t_i, t_{i+1}), and identical BN structures are generated for each time instant, connected to each other by means of temporal arcs (e.g., Montani et al., 2008; Portinale et al., 2010). In the second approach, the time line is partitioned into a finite number of time intervals (e.g., $]t_{i-1}, t_i]$, $]t_i, t_{i+1}]$), and only one BN is generated, each node of which has a finite number of states equal to the number of time intervals (Boudali and Dugan, 2005; Marquez et al., 2010; Boudali and Dugan, 2006). Figure 7.2 illustrates how a CSP gate is

converted into interval-based and instant-based (here, a 2-time-slice) BN structures, respectively.

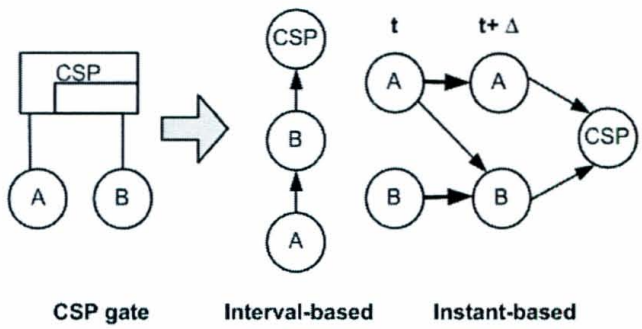


Figure 7.2. Converting a CSP gate into interval-based (middle) and instant-based (right) BN structures.

Following the instant-based approach, Montani et al. (2008) developed the RADYBAN software tool for reliability analysis of dynamic systems by converting DFT into a 2-time-slice BN. They also introduced the probability dependency gate (PDEP) as a probabilistic case of FDEP proposed by Dugan et al. (Dugan et al., 1992). Their work was further developed by Portinale et al. (2010), enabling the modeling of repairable systems by introducing the repair box gate. However, the instant-based approach has been criticized for either being too general or resulting in unnecessarily large networks due to repeating the same structure for each time instance (Boudali and Dugan, 2005).

Considering the interval-based approach, Boudali and Dugan (2005) suggested a discrete-time BN (DTBN). Although being straightforward and consistent with the majority of conventional inference algorithms, DTBN could potentially result in huge and intractable conditional probability tables (CPTs) in particular for large number of time intervals

(Marquez et al., 2010; Boudali and Dugan, 2006). It is worth noting that the problem is still much easier to manipulate than the state space explosion problem in MC. It also requires numerical simulation for non-exponential distribution functions (Marquez et al., 2010). To address the foregoing issues, Boudali and Dugan (2006) presented a continuous-time BN (CTBN) in which parametric functions were substituted for multi-dimensional CPTs, resulting in lesser computational time and required memory capacity. Recently, Marquez et al. (2010) developed a hybrid BN to incorporate both discrete and continuous variables. They also used a dynamic time discretization as opposed to the static time discretization employed by Boudali and Dougan (2005).

In accordance with the interval-based approach, this paper aims to extend the DTBN methodology developed by Boudali and Dugan (2005) such that it could be applied to a broader range of probabilistic distribution functions. In this regard, a new general formalism is developed for the CSP gate for which input variables can have any arbitrary (not necessarily exponential) failure distributions. The formalism is also applicable for the SEQ gate as a special case of the CSP gate. The paper proceeds by introducing an innovative algorithm, named *Neutral Dependency*, which reduces the dimension of multi-dimensional CPTs by an order of magnitude. The paper shows how the algorithm could efficiently be used to populate the CPTs of PAND gates and also static gates such as AND and OR. In each step, the results are compared with those obtained from both analytical methods such as MC and conventional methods in the literature.

In Section 7.2, after a brief review of the fundamentals of BN, the modeling framework of DTBN is recapitulated. Section 7.3 presents the new approach developed in this study

to model CSP gates and SEQ gates in DTBN. The approach is shown to not only replicate the results in the literature but also be in better agreement with MC analysis. Section 4 is dedicated to the introduction of the Neutral Dependency algorithm, where this algorithm is efficiently used to reduce the dimension of CPTs. In Section 7.5, a practical application of the method in the risk analysis of dynamic systems is presented while the conclusions from this work are discussed in Section 7.6.

7.2 Bayesian network

7.2.1 An overview

BN is a directed acyclic graph for reasoning under uncertainty in which the nodes represent variables and are connected by means of directed arcs. The arcs denote dependencies or causal relationship between the linked nodes, and the conditional probability tables assigned to the nodes determine how the linked nodes are dependent on each other (Torres-Toledano and Sucar, 1998; Jensen and Nielsen, 2007).

Based on the conditional independency theorem and the chain rule, BN factorizes the joint probability distribution of a set of random variables $U = \{A_1, A_2, \dots, A_n\}$ by considering local dependencies. In this regard, the joint probability distribution can be decomposed as the product of the probabilities of the nodes given their immediate parents (Jensen and Nielsen, 2007):

$$\boldsymbol{P(U) = \prod_{i=1}^{n} P(A_i | Pa(A_i))} \qquad \textbf{7.1}$$

where $P(U)$ is the joint probability distribution of variables and $Pa(A_i)$ is the parent set of variable A_i.

The main application of BN in reliability and risk analysis was in probability updating until it was also considered as a viable alternative to DFT for modeling the dynamic behavior of dependent components. BN takes advantage of Bayes theorem to update the probability of events given new observations, called evidence E, to yield the posterior probability:

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \qquad 7.2$$

Using Equation 7.2, probability updating can be done for versatile types of E such as knowing that the system has failed during the mission time T or the system has failed in the time interval $]t_{i-1}, t_i]$ (Section 7.2.3).

7.2.2 Discrete-time Bayesian network

As previously mentioned, DTBN was developed to account for the sequential dependencies among components by explicit incorporation of time in the BN formalism. In this regard, the time line $]0, +\infty]$ is divided into $n+1$ intervals, partitioning the mission time $]0, T]$ into n intervals and leaving the $]T, +\infty[$ as the last or $(n+1)$-th interval (Boudali and Dugan, 2005). In this way, each node has a finite number $n+1$ of states equal to the number of time intervals (Figure 7.3).

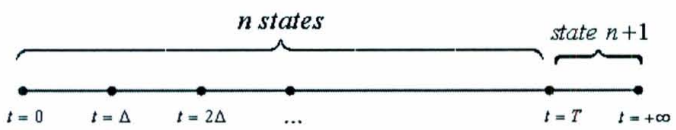


Figure 7.3. Time line intervals (Boudali and Dugan, 2006).

In accordance with the terminology introduced in (Boudali and Dugan, 2005), if random variable A is mentioned to be in state i $(1 \leq i \leq n)$, or $A = i$, it simply means A has failed in the *i-th* interval or $t_A \in](i-1)\Delta, i\Delta]$:

$$P(A=i) = P((i-1)\Delta < t_A \leq i\Delta) = \int_{(i-1)\Delta}^{i\Delta} f_A(t)dt = F_A(i\Delta) - F_A((i-1)\Delta) \quad \textbf{7.3}$$

where t_A is the failure time of component A, F_A is the cumulative distribution, Δ is the interval length $\Delta = \frac{T}{n}$, and n is the time granularity (Boudali and Dugan, 2005).

Similarly, if A is said to be in state $n+1$, this means A has survived the mission time T:

$$P(A=n+1) = P(t_A > T) = \int_{T}^{\infty} f_A(t)dt = 1 - F_A(T) \quad \textbf{7.4}$$

7.3 Dynamic gates: a new formalism

7.3.1 Cold spare gate

Spare gates are used to model subsystems with redundant components in which a failed primary component is immediately replaced by its spares, one after another. Representing a parallel subsystem, a spare gate does not fail unless all its components, i.e. primary and spares, fail or are unavailable in case of shared spares (Dugan et al., 1992). Although being identical to the primary component, a spare component could have a different failure rate from the primary as long as it is dormant (not recruited to function) (Montani et al., 2008).

With a CSP gate, the failure rate of a dormant spare is equal to zero, implying that it is impossible for the spare to fail or degrade before or even at the same time as the primary (Dugan et al., 1992). Figure 7.4 shows a CSP gate and its equivalent structure in DTBN (Boudali and Dugan, 2005).

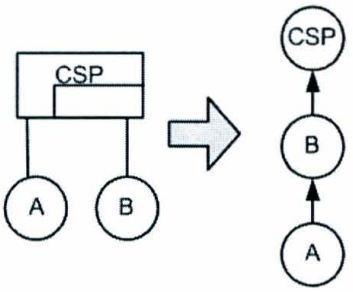


Figure 7.4. CSP gate mapping into DTBN (Boudali and Dugan, 2005).

According to the formalism recapitulated in Section 7.2.2, CSP gates can be modeled by allocating arbitrary marginal probability tables to primary A, and appropriate CPTs to spare B and CSP gate. It should be noted that for the sake of simplicity, n= 2 is used (i.e., three time intervals) in this example and also in all the following sections.

Table 7.1 shows the marginal probability table of A, where P_i is calculated using Equation 3 for i= 1, 2 and $P_3 = 1 - P_1 - P_2$.

Table 7.1. Marginal probability table of node *A* (or *B*).

A	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$
P(A)	P_1	P_2	P_3

According to the definition of a CSP gate, spare B cannot fail before primary A, justifying zero entries in Table 7.2; furthermore, entries of unity in the identity matrix illustrated in Table 7.3 imply that the failures of CSP gate and spare B occur at the same time.

Table 7.2. Conditional probability table of spare B.

A	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$
$]0,\Delta]$	0	0	0
$]\Delta,T]$	P_{21}	0	0
$]T,\infty[$	P_{31}	1	1

Table 7.3. Conditional probability table of CSP gate.

B	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$
$]0,\Delta]$	1	0	0
$]\Delta,T]$	0	1	0
$]T,\infty[$	0	0	1

The most important task in the simulation of a CSP gate in DTBN is to obtain an analytical form for conditional probabilities P_{ij} in Table 7.2, denoting the probability of B failing in the *i-th* interval given that A has failed in the *j-th* interval, i.e.:

$$P_{ij} = P(B = i \mid A = j) = P((i-1)\Delta < t_B \leq i\Delta \mid (j-1)\Delta < t_A \leq j\Delta) \quad \textbf{7.5}$$

Since B cannot fail before the *j-th* interval, $P(B = i|A = j)$ can be simply approximated to $P(B = i|B > j)$, resulting in:

$$P(B=i \mid A=j) = P(B=i \mid B>j) = \frac{P(B=i \cap B>j)}{P(B>j)} =$$

$$\begin{cases} \dfrac{P(B=i)}{P(B>j)} & if\ i>j \\ 0 & otherwise \end{cases} \qquad \textbf{7.6}$$

If the calculation proceeds for $i > j$:

$$P(B=i|A=j) = \frac{P(B=i)}{P(B>j)} = \frac{\int_{(i-1)\Delta}^{i\Delta} f_B(t)dt}{\int_{j\Delta}^{\infty} f_B(t)dt} = \frac{F_B(i\Delta) - F_B((i-1)\Delta)}{1 - F_B(j\Delta)} \qquad \textbf{7.7}$$

It is worth noting that Equation 7.7 has a closed-form solution for a majority of probability density functions. For instance, it could be customized by assuming an exponential density function for B:

$$P(B=i|A=j) = \frac{\int_{(i-1)\Delta}^{i\Delta} \lambda e^{-\lambda t} dt}{\int_{j\Delta}^{\infty} \lambda e^{-\lambda t} dt} = e^{-\lambda\Delta(i-j)}(e^{\lambda\Delta} - 1) \qquad \textbf{7.8}$$

It should be noted that Equation 7.8 can be further simplified for infinitesimal values of $\lambda\Delta$ (because $lim_{\lambda\Delta\to 0}(e^{\lambda\Delta} - 1) = \boldsymbol{\lambda\Delta}$) to yield the equation suggested in [6] in which the failure rates of both A and B are included, showing the generality of Equation 7.8 as opposed to that proposed in (Boudali and Dugan, 2005). Equation 7.8 can be manipulated by solving the denominator integral to obtain another form of solution for the exponential density function:

$$P(B=i|A=j)=\frac{\int_{(i-1)\Delta}^{i\Delta}\lambda e^{-\lambda t}dt}{e^{-\lambda j\Delta}}=\int_{(i-1)\Delta}^{i\Delta}\lambda e^{-\lambda(t-j\Delta)}dt= \quad \textbf{7.9}$$
$$F_B(i\Delta-j\Delta)-F_B((i-1)\Delta-j\Delta)$$

Equation 7.9 is identical to that proposed by Boudali & Dugan (2005) for a CSP gate, showing that the new formalism developed in this study replicates the previous results in the literature, i.e., (Boudali and Dugan, 2005). Figure 7.5 explains the time shift $j\Delta$ in the probability distribution of B in Equation 7.9; because B cannot fail before A, its distribution is shifted to the right by an amount equal to the failure time of A, i.e., $j\Delta$.

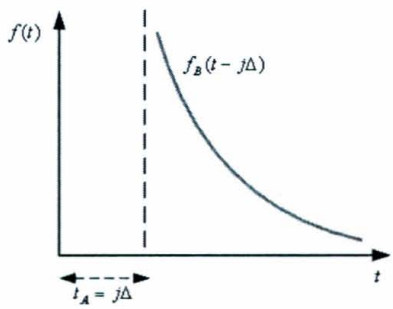
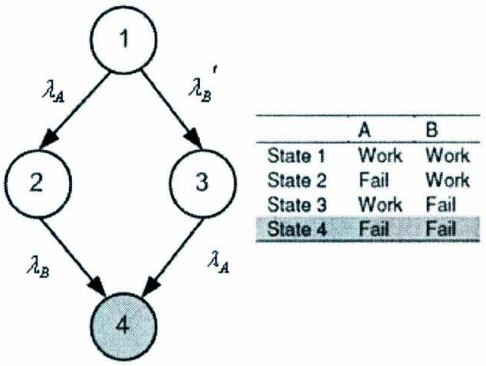


Figure 7.5. Shifted probability distribution of spare B.

To validate the formalism developed in Equation 7.7, its exponential form presented by Equation 7.8 is compared to MC analysis. Figure 7.6 shows a general MC which can be used to analyze different types of spare gates and also a SEQ gate (in Section 7.3.2).

In Figure 7.6, in the case of CSP gate analysis, $\acute{\lambda_B} = 0$ and $\lambda_A = \boldsymbol{\lambda_B} = \boldsymbol{\lambda}$. Due to $\acute{\lambda_B} = 0$, State 3 in Figure 7.6 would not exist in practice.



	A	B
State 1	Work	Work
State 2	Fail	Work
State 3	Work	Fail
State 4	Fail	Fail

Figure 7.6. General Markov chain for CSP and SEQ gates.

According to Figure 7.6, the failure probability of the system (i.e., the probability of State 4) is $P_4 = 1 - e^{-\lambda t} - \lambda t e^{-\lambda t}$. The result of this study, i.e. Equation 7.8, Boudali and Dugan [6] and MC are compared in Table 7.4 for $T = 10\ hrs$, $\Delta = 2\ hrs$ and different failure rates.

Table 7.4. Comparison of results for CSP gate.

$\lambda(hr^{-1})$	Ref. [6]	Equation 7.8	MC
0.1	2.03E-01	2.25E-01	2.64E-01
0.01	3.73E-03	3.77E-03	4.68E-03
0.001	3.97E-05	3.98E-05	4.97E-05

As seen in Table 7.4, the results of the current study are in better agreement with those of MC analysis, showing that Equation 7.8 (or Equation 7.7 in general) is at least as reliable as the equation developed in Boudali and Dugan (2005).

7.3.2 Sequence enforcing gate

The sequential enforcing gate (SEQ) is used to model events that have to fail in a strictly predefined sequential order. Similar to the CSP gate, the inputs of a SEQ gate are recruited to function one after another in the left-to-right order (Dugan et al., 1992). However, unlike a CSP gate, the inputs do not need to be identical nor have the same failure rates. So, a SEQ gate can be considered as a CSP gate that could accept any basic or subsystem event as input (Montani et al., 2008).

Figure 7.7 shows a SEQ gate and its corresponding structure in DTBN. Since Equation 7.8 does not depend on the failure rate of the primary component (A in Figures 7.3 and 7.6), it could be used to model either a CSP gate where $\lambda_B = \boldsymbol{\lambda_A}$ or a SEQ gate where $\lambda_B \neq \lambda_A$.

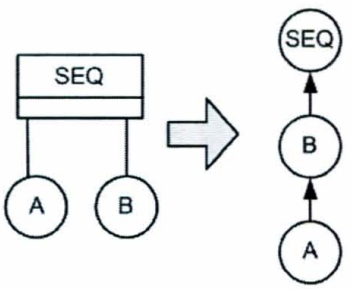


Figure 7.7. SEQ gate mapping into DTBN. Either *A* or *B* could be different basic events or subsystems.

To verify whether Equation 7.8 could be effectively used to approximate a SEQ gate, its results and those of MC are compared in Table 7.5 for $\lambda_A = 0.05$, $\lambda_B = 0.1, 0.01, 0.001,$

$T = 10\ hrs$ and $\Delta = 2\ hrs, 1\ hr$. It should be noted that the results of MC in Table 7.5 are obtained using Figure 7.6 for $\lambda_B' = 0$ but $\lambda_A \neq \lambda_B$, resulting in the system failure probability as $P_4 = 1 - e^{-\lambda_A t} - \frac{\lambda_A}{\lambda_A - \lambda_B}(e^{-\lambda_B t} - e^{-\lambda_A t})$.

Table 7.5. Comparison of results for SEQ gate.

$\lambda_B\ (hr^{-1})$	$\Delta = 2\,hr$	$\Delta = 1\,hr$	MC
0.1	1.30E-01	1.43E-01	1.55E-01
0.01	1.67E-02	1.87E-02	2.06E-02
0.001	1.73E-03	1.93E-03	2.12E-03

According to Table 7.5, it is evident that Equation 7.8 can also be used to model a SEQ gate in DTBN. On the other hand, if the relationship proposed in Boudali and Dugan (2005) for CSP is modified to model a SEQ gate by considering different failure rates for A and B, it results in an expression for P_{ij} which is always negative no matter what values are chosen for distribution parameters such as λ_A, λ_B, and Δ (Appendix 1).

7.4 Neutral dependency

As mentioned earlier, DTBN has been criticized for potentially having enormous multi-dimensional CPTs Marquez et al., 2010; Boudali and Dugan, 2006). Modeling techniques such as parent divorcing (Jensen and Nielsen, 2007) have widely been used in conventional BN to reduce the size of probability tables by dividing the parent set of a node into subsets. However, the probability table of a node (gate) in DTBN can become intractable even with a small set of parents (inputs).

This section aims to develop an innovative algorithm, *Neutral Dependency*, to reduce the size of multi-dimensional CPTs in DTBN, increasing their efficiency and decreasing the computational time.

7.4.1 Priority-AND gate

7.4.1.1 Conventional approach

Priority-AND (Fussell et al., 1976), commonly known as a PAND gate, is another dynamic gate frequently used to model the interaction between dependant components in complex systems (Boudali and Dugan, 2005; Marquez et al., 2010). Similar to the previously discussed dynamic gates, a PAND gate fails when all its inputs fail but only in the left-to-right order.

Unlike a SEQ gate which forces its inputs to fail exclusively in a pre-assigned order, a PAND gate allows its inputs to fail in any arbitrary sequence whereas it gives priority to that failure sequence in which the primary input (leftmost) fails before or at the same time as the secondary input(s) (Dugan et al., 1992; Montani et al., 2008).

Figure 7.8 depicts a PAND gate and its equivalent structure in DTBN for which the CPT in Table 7.6 is developed. It should be noted that entries of unity in the table imply that the gate fails only if secondary B fails after or at the same time as primary A.

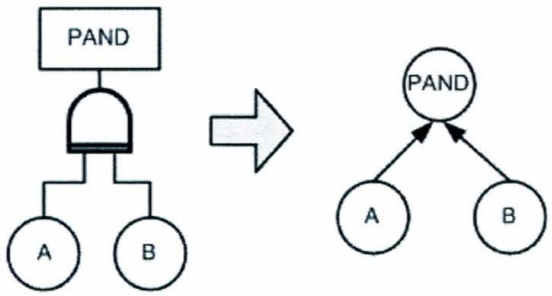


Figure 7.8. Mapping PAND gate into DTBN.

Table 7.6. Conventional CPT for PAND gate.

A		$]0,\Delta]$			$]\Delta,T]$			$]T,\infty[$	
B	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$
$]0,\Delta]$	1	0	0	0	0	0	0	0	0
$]\Delta,T]$	0	1	0	0	1	0	0	0	0
$]T,\infty[$	0	0	1	1	0	1	1	1	1

Since in the numerical simulation of dynamic systems the CPTs tend to be taken into account as matrices, such sparse matrices as the one illustrated in Table 7.6 could adversely affect the computational time and modeling efficiency. The problem could worsen as the size of the matrix grows exponentially due to larger time granularities.

7.4.1.2 Neutral dependency approach

To avoid sparse matrices, the structure of a PAND node is modified to decrease the number of its parents from two to one, reducing the dimension of the CPT by an order of magnitude (Figure 7.9).

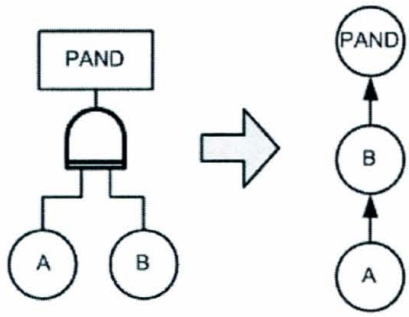


Figure 7.9. Modified PAND gate structure in DTBN.

By changing the gate structure, it is assumed that on the one hand, similar to a CSP or SEQ gate, a PAND gate fails when B fails, resulting in an identity matrix of size $(n + 1)$ for the PAND gate (Table 7.7). And, on the other hand, B is made apparently dependent on A (though it really is not), resulting in a lower triangular matrix of size $(n + 1)$ for B (Table 7.8). However, by assigning $P(B|A) = P(B)$ in the corresponding CPT shown in Table 7.8, this apparent dependency is neutralized (Appendix 2).

Table 7.7. CPT for PAND gate which is only dependent on B.

B	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$
$]0,\Delta]$	1	0	0
$]\Delta,T]$	0	1	0
$]T,\infty[$	0	0	1

Table 7.8. CPT for apparent (but neutralized) dependency of B on A.

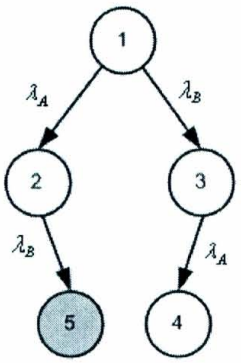
A	$]0,\Delta]$	$]\Delta,T]$	$]T,\infty[$
$]0,\Delta]$	P(B=1)	0	0
$]\Delta,T]$	P(B=2)	P(B=2)	0
$]T,\infty[$	P(B=3)	P(B=3)+**P(B=1)**	P(B=3)+P(B=2)+P(B=1)

As can be seen, the sparse matrix used in the conventional approach (Table 7.6) with $(n+1)^3$ entries is successfully decomposed into an identity matrix (Table 7.7) and a lower triangular matrix (Table 7.8), both of which have $(n+1)^2$ entries, offering CPTs an order of magnitude smaller in dimension.

It is worth noting that Table 7.8 could be populated using:

$$P(B=i \mid A=j)=\begin{cases} P(B=i) & if \quad i \geq j \\ 0 & if \quad i<j \\ 1-\sum_{k=1}^{n} P(B=k) & if \quad i=n+1 \end{cases} \qquad \textbf{7.10}$$

To verify the Neutral Dependency algorithm, the results are compared with the corresponding MC in Figure 7.10, for which State 5 is considered as the PAND gate failure. It should be noted that although both states 4 and 5 could be considered as the system failure (i.e., both A and B failed), the later state is given priority over the former due to the failure sequence of its components (A fails before B).



	A	B
State 1	Work	Work
State 2	Fail	Work
State 3	Work	Fail
State 4	Fail	Fail
State 5	Fail	Fail

Figure 7.10. Markov Chain of PAND gate.

According to the MC in Figure 7.10, the failure probability of a PAND gate (or the failure probability of State 5) is $P_5 = -e^{-\lambda_B t} + \frac{\lambda_B}{\lambda_A+\lambda_B}(e^{-(\lambda_A+\lambda_B)t} + 1)$. Table 7.9 compares the results obtained from Equation 7.10 and MC for $\lambda_A = 0.05, T = 10\ hrs$, and $\Delta = 1\ hr$, and different values of λ_B. Results are in a good agreement, showing that the Neutral Dependency technique can be successfully applied to model a PAND gate in DTBN.

Table 7.9. Comparison of MC and the current study for PAND gate.

λ_B	MC	This study
0.1	1.14E-01	1.27E-01
0.01	2.00E-02	2.18E-02
0.001	2.11E-03	2.31E-03

7.4.2 Static gates

Since it is possible to employ conventional OR gates and AND gates along with dynamic gates to model a complex system, these static gates also need to be modeled as discrete-time gates to conform with the rest of DTBN. Similar to the conventional PAND gate (section 7.4.1.1), CPTs of the foregoing static gates could potentially become very large. In this regard, the Neutral Dependency technique (Figure 7.11) can also be applied to reduce the size of multi-dimensional CPTs.

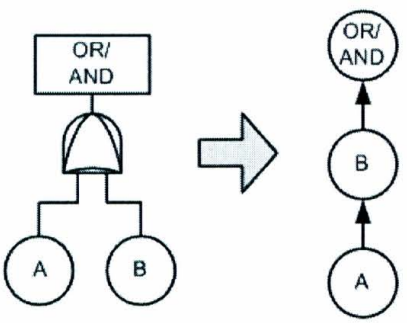


Figure 7.11. AND/OR gate corresponding structure in DTBN using Neutral Dependency.

In this regard, the CPT of an OR/AND gate, which is only dependent on B, is the same as Table 7.7 while the values of the CPT of B are calculated using Equation 7.11 (as shown in Table 7.10) and Equation 7.12 (as shown in Table 7.11) for an OR gate and AND gate, respectively.

CPT of B in an OR gate:

$$P(B=i \mid A=j)=\begin{cases} 0 & if \quad i>j \\ \sum_{k=i}^{n+1} P(B=k) & if \quad i=j \\ P(B=i) & if \quad i<j \end{cases} \qquad 7.11$$

Table 7.10. CPT of B for an OR gate structure populated using Equation 7.11.

A	]0,Δ]	]Δ,T]	]T,∞]
]0,Δ]	P(B=1)+P(B=2)+P(B=3)	P(B=1)	P(B=1)
]Δ,T]	0	P(B=2)+P(B=3)	P(B=2)
]T,∞]	0	0	P(B=3)

CPT of B in an AND gate:

$$P(B=i \mid A=j)=\begin{cases} P(B=i) & if \quad i>j \\ \sum_{k=1}^{i} P(B=k) & if \quad i=j \\ 0 & if \quad i<j \end{cases} \qquad 7.12$$

Table 7.11. CPT of B for an AND gate structure populated using Equation 7.12.

A	]0,Δ]	]Δ,T]	]T,∞]
]0,Δ]	P(B=1)	0	0
]Δ,T]	P(B=2)	P(B=1)+P(B=2)	0
]T,∞]	P(B=3)	P(B=3)	P(B=1)+P(B=2)+P(B=3)

7.5 Application: risk-based design

Safety system modeling is an integral part of risk assessment studies. In this regard, safety systems planned to avoid, prevent, limit or control accidents are evaluated to examine the extent to which they are effective in reducing the risk of the accident to an acceptable level.

In the past, the effectiveness of safety systems has been studied using static methods such as bow-tie approach (Delvosalle et al., 2006), barrier block diagram Aven et al., 2006) and safety-barrier diagram (Duijm, 2009). These methods, however, are not appropriate for the safety analysis of dynamic systems. For example, in the MIRAS methodology (Delvosalle et al, 2006), aimed at investigating the influence of safety systems on the occurrence probability of accidents, preventive and mitigative safety barriers are placed upstream and downstream of events, respectively, without considering sequential dependencies. Also, the optimal placement of safety systems in accident prevention and mitigation has not been focused, causing unnecessary complexity and cost for the system studied.

This section aims to illustrate how DTBN could be used to optimally allocate safety systems through a risk-based approach. This allocation for dynamic systems would result in the maximum risk reduction and a cost-effective safety management.

7.5.1 Case study: heat exchanger explosion

To implement the methodology, a heat exchanger explosion at the Goodyear Tire and Rubber Company plant in Houston, Texas, U.S. in 2008 was selected as the accident

scenario (CSB, 2011). Ammonia liquid was used as a coolant in the heat exchanger to control the temperature of the process. Due to absorbing heat, ammonia liquid transforms into ammonia vapor, leaving the heat exchanger in a cooling system through a pipeline equipped by a pressure control valve (CV) and three block valves (BV_i). The block valves are aimed at isolating CV in the case of maintenance. A schematic of the heat exchanger adapted from (CSB, 2011) is depicted in Figure 7.12.

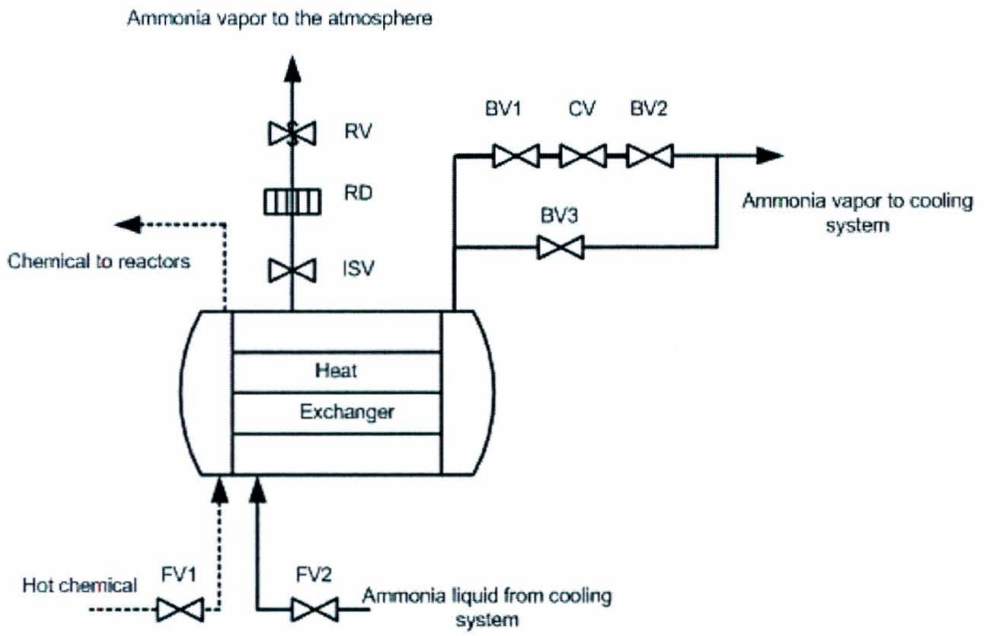


Figure 7.12. Schematic of the heat exchanger in the Goodyear accident (CSB, 2011)].

CV was designed to maintain ammonia pressure at 150 psig. A rupture disk (RD) and a relief valve (RV) were also devised to relieve ammonia vapor to the atmosphere in the

case of overpressure (i.e., above 300 psig). Further, an isolation valve (ISV) was included to separate RD and RV from the heat exchanger in the case of maintenance.

Based on a full-scale investigation conducted by the U.S. Chemical Safety Board (2011), ISV and BVs were closed for the maintenance of RD and the cleaning of the heat exchanger, respectively. So, the heat exchanger was isolated from its pressure protection (i.e., CV) and pressure relief (i.e., RD and RV) equipment when an overpressure gave rise to an explosion. One worker was killed because of the explosion, and six others injured due to the exposure to ammonia. According to the recommendations of the *ASME* code for pressure vessels (ASME, 2004), the accident could have been prevented if a worker would have continuously monitored the heat exchanger and manually released the pressure.

Considering "manual release of the pressure" as the safety function, two safety scenarios were examined to find the optimal allocation of safety systems:

Scenario 1: the worker opens BV_3 as the heat exchanger pressure rises above 150 psig, implying that pressure control package PCP (including BV_1, CV and BV_2) does not work properly, i.e., either BV_1 or BV_2 is plugged (or closed), or CV does not work.

Scenario 2: the worker does not open BV_3 until the pressure rises above 300 psig, inferring that pressure relief package PRP (including ISV, RD and RV) also does not work properly, i.e., ISV is plugged (or closed), or either RD or RV fails to work.

7.5.2 Accident modeling

7.5.2.1 Fault tree analysis

Ignoring the dynamic characteristics of the system, the logical model of the heat exchanger explosion is illustrated in Figure 7.13 using a SFT (leftmost) showing only the functional dependencies among the components. However, to model sequential dependencies, the SFT is modified to the DFT (Figure 7.13, rightmost) based on the assumptions below:

CV and RV are designed to operate at 150 and 300 psig, respectively, implying that PCP is more likely to fail before PRP. This sequential failure is taken into account by replacing the corresponding AND gate (shown as AND (1) in Figure 7.13) with a PAND gate.

BV_3 is located in parallel with BV_1, CV, and BV_2. Also, it is not supposed to be opened unless either BV_1 or BV_2 cannot pass ammonia vapor or CV fails to operate at 150 psig (scenario 1). BV_3 thus acts like a spare component for PCP, called on demand only if PCP fails to work properly. This dynamic behavior is modeled by replacing the corresponding AND gate (shown as AND (2) in Figure 7.13) with a SEQ gate. However, if BV_3 and PCP were of the same type and had identical failure rates, a CSP gate would be used instead of a SEQ gate.

For the sake of clarity, the static gates and their dynamic substitutes are highlighted in Figure 7.13.

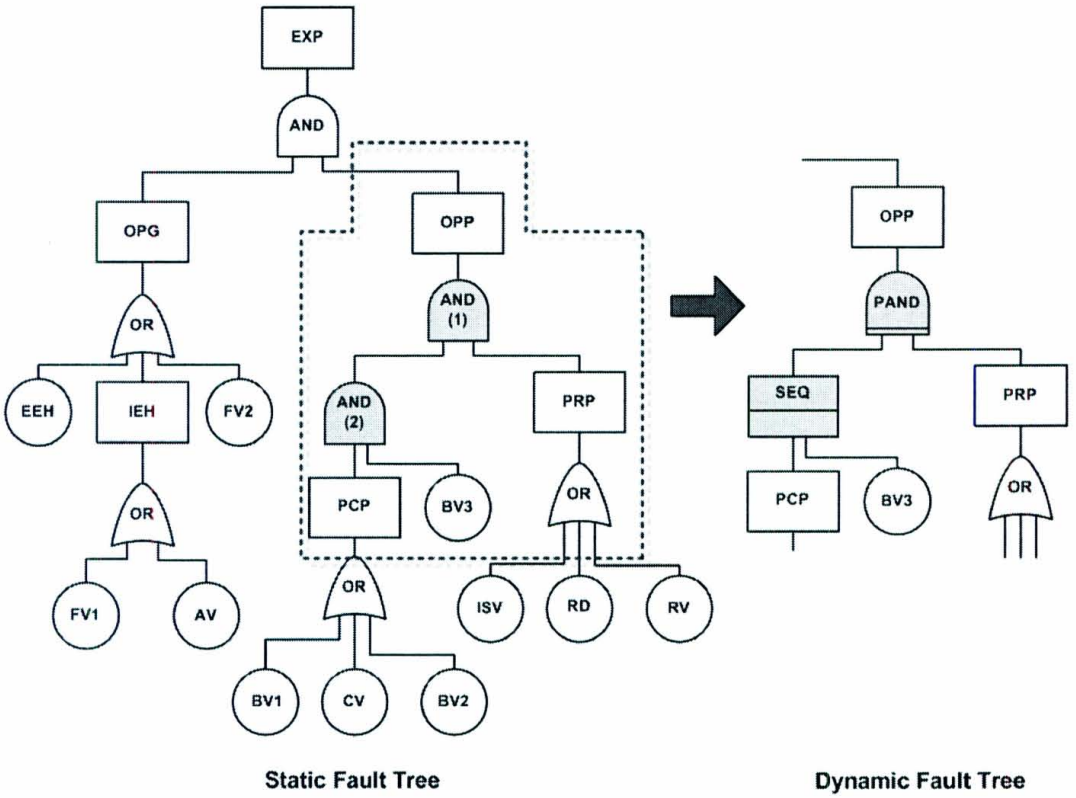


Figure 7.13. SFT and DFT of the heat exchanger explosion (safety scenario 1). For the sake of brevity, only the modified part of the DFT is illustrated.

As mentioned earlier, if the DFT is converted to a MC to be solved, the MC could potentially have $2^{11} \times 7!$ states, making it computationally very costly to solve unless simplifying assumptions are used.

7.5.2.2 Bayesian analysis

To solve the DFT shown in Figure 13 and also to conduct probability updating using different observations, the DFT is converted to the corresponding DTBN structure in Figure 7.14, considering a mission time $T = 10\ hrs$ and a time interval $\Delta = 1\ hr$. It

should be noted that, using the parent divorcing technique (Jensen and Nielsen, 2007), the dimensions of CPTs of OPG, PCP and PRP (all three originally had more than two parents) are decreased by introducing the auxiliary nodes EEH-FV2, BV1-CV and ISV-RV in Figure 7.14, respectively.

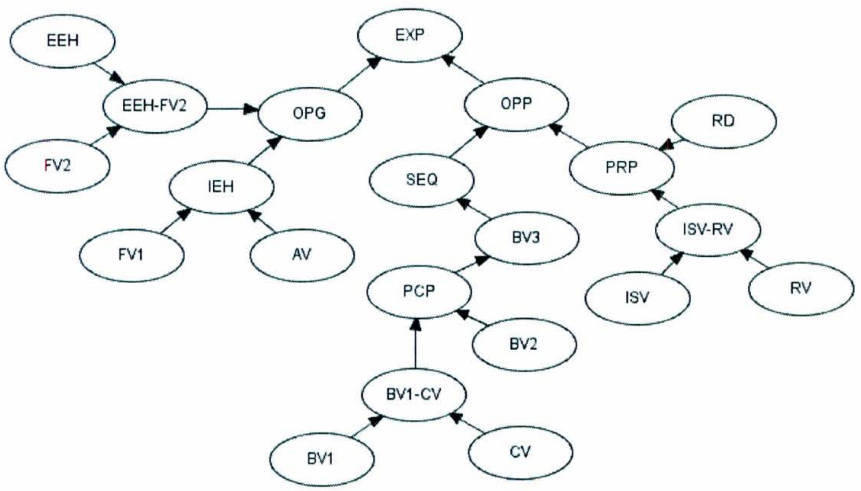


Figure 7.14. BN of the explosion in the heat exchanger.

Then, using HUGIN software 7.4 and the probabilities of the basic components presented in Table 7.12, the occurrence probability of the explosion is calculated as P(EXP) = 4.83E-11. It is worth noting that modeling the accident using the SFT would result in P(EXP) = 2.93E-10, different from dynamic modeling by an order of magnitude.

Table 7.12. Failure probabilities of the events of DFT in Figure 7.13.

Event	Symbol	Description	λ (10^{-4})
Explosion	EXP	Top event	
Overpressure Generation	OPG	Intermediate event	
Internal Excessive Heat	IEH	Intermediate event	
Feed Valve for Chemical	FV_1	Failure of valve to regulate the inflow of hot chemical	2.06
Ammonia Vapor	AV	Failure of cooling system to condensate ammonia vapor	2.19
Feed Valve for Ammonia	FV_2	Failure of valve to regulate the inflow of ammonia liquid	2.06
External Excessive Heat	EEH	Jet fire, radiation, steam, other	1.54
Overpressure Protection	OPP	Intermediate event	
Pressure Control Package	PCP	Failure to control the pressure	
Control Valve	CV	Failure of check valve to operate at 150 psig	0.28
Block Valve	$BV_{1,2}$	Failure of valve due to plugging, choking, structural flaw	0.59
Block Valve	BV_3	Failure of valve to open on demand	3.98
Pressure Relief Package	PRP	Failure to release the pressure	
Isolation Valve	ISV	Failure of valve due to plugging, choking, structural flaw	0.59
Rupture Disk	RD	Failure of rupture disk to burst	3.3
Relief Valve	RV	Failure of relief valve to operate at 300 psig	2.59

To investigate the effect of scenario 2 on the accident probability which in turn affects the envisaged risk of the accident, the DFT is slightly modified such that BV_3 acts as a spare to PRP. In other words, BV_3 is connected to PRP using a SEQ gate (Figure 7.15). By converting the modified DFT into the corresponding DTBN, the probability of the explosion is calculated as P(EXP) = 9.67E-11, implying a 100% increase in the envisaged risk as opposed to scenario 1. As can be seen, the safety function "manual release of the pressure" is more effectively implemented by opening BV_3 as the safety system in the case of PCP malfunction (scenario 1) rather than PRP failure (scenario 2).

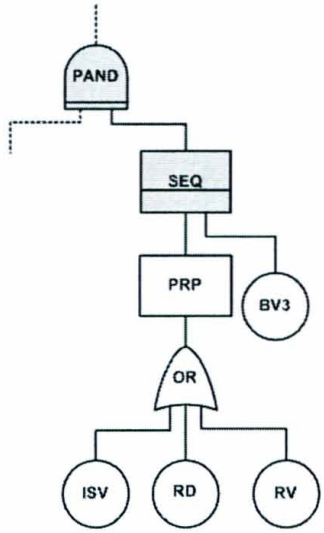


Figure 7.15. Modified DFT in which BV_3 is opened if PRP fails to release the pressure. The parts which are not drawn are the same as Figure 7.13.

7.5.2.3 Probability updating

One of the valuable advantages of DTBN over conventional methods such as MC in solving dynamic systems is its ability to perform probability updating (or diagnosis analysis) given new observations. The prior probability of events are updated given a specific state of the top event and also the most likely configuration (MLC) of events, leading to the top event, are determined (Bobbio et al., 2001; Khakzad et al., 2001; Boudali and Dugan, 2005). In this way, the most critical events are identified, and preventive safety measures are consequently designed. In the present study, probability updating is performed for two different types of observation:

Type 1: the accident has occurred during the mission time, i.e., $t \in]0, T]$.

Type 2: the accident has occurred at the i-th time interval, i.e., $t \in]t_{i-1}, t_i]$.

Regarding the observation of type 1, the posterior probability of the components are calculated by inserting the evidence $P(EXP = n + 1) = 0$ in the analysis, showing EXP has occurred during the mission time without knowing the exact time interval. The updated probabilities due to this observation, i.e., $P(EXP = 11) = 0$ are calculated and compared with the prior ones. The updated probability distributions of BV_1, BV3, and RD are illustrated in Figure 7.16 (the middle row). Also, MLC of the basic components is the failure of AV, BV_1, and BV_2 in the first interval, the failure of RD and BV_3 in the second interval and the non-failure of the other basic components with $P(MLC) = 3.48E - 05$.

Concerning the observation of type 2, the probability of EXP being in the *i*th time interval is set to one, i.e., $P(EXP = i) = 1$, and propagated in the network to yield the posterior probabilities. Assuming $i = 8$, the posterior probability distributions of BV_1, BV3, and RD are again illustrated in Figure 7.16 (the lower row). Likewise, the probability of MLC is calculated as $P(MLC) = 2.046E - 04$, including the failure of AV in the eighth interval, the failure of BV_1 and BV_2 in the first interval, the failure of RD and BV_3 in the second interval and the non-failure of the other basic components.

According to Figure 7.16, BV_1 has the highest updated failure probability in the first interval no matter which type of observation is used, implying BV_1 (and also BV_2) is the most unreliable component. So, proper and immediate safety measures should be allocated for this component during the early hours of operation. The criticality of BV_1 (and BV_2) is further acknowledged as it appears in both MLCs, failing in the same time interval, i.e., the first interval.

Figure 7.16 shows that BV_3 is most likely to fail in the sixth and eighth intervals due to observations type 1 and 2, respectively. On the contrary, both MLCs demonstrate that the most probable failure interval for BV_3 is the second interval. This difference occurs because in the MLC analysis, BN searches over the state space of each component to identify the weakest links while considering the other components' states [4]. So, it is concluded that MLC provides the analyst with more reliable and holistic results by considering the whole system.

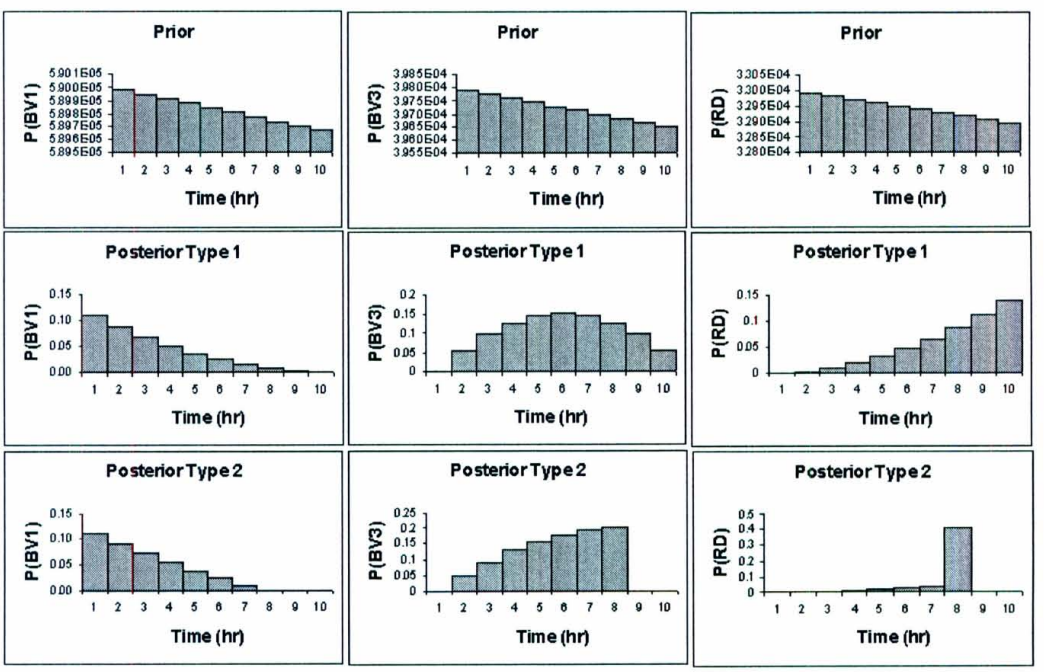


Figure 7.16. A comparison between prior (the upper row) and posterior probability distributions (type 1 in the 2nd row and type 2 in the 3rd row) of BV_1, BV_3 and RD.

7.6 Conclusion

The present study has improved the power of DTBN in dependability analysis of dynamic complex systems. In this regard, a new approach has been proposed for dynamic gates such as a CSP gate, which does not necessitate the use of exponential distribution functions for input variables. The approach was also shown to be successful in SEQ gate modeling. A comparison between this study and the existing techniques in the literature demonstrates that the present study not only replicates the results of the previous works, but it also is in better agreement with analytical techniques such as MC.

Further, a new algorithm called Neutral Dependency was introduced to model dynamic gates such as a PAND gate and static gates such as an AND/OR gate. Using this algorithm, the conditional probability table of a gate is decomposed into two tables, both of which are smaller in size than the original table (usually by an order of magnitude). This way, the problem of large and intractable multi-dimensional tables for which DTBN has been criticized is addressed.

This paper has also shown the application of the proposed approach in the risk assessment and safety analysis of process systems. It has been demonstrated that DTBN can be used as a safety evaluation tool to optimally allocate safety systems in process facilities. DTBN can be employed in the design phase of process systems to identify the best arrangement of safety systems to reduce the envisaged risk. It could also be used as an inductive tool to analyze system failure in light of new observations.

It may be concluded that using temporal BN in the risk analysis of dependable systems not only avoids problems such as the state-space explosion and the error-prone

conversion procedure which are common in MC analysis, but also enables the analyst to perform probability updating. It is of great importance in the real-time design, monitoring, and evaluation of safety systems. This is not feasible with continuous-time approaches such as MC. DTBN is relatively simple to construct and can be solved using standard inference algorithms provided in most Bayesian software. It also offers the analyst the opportunity to obtain failure probability distributions rather than single values for the whole time mission.

Acknowledgement

The authors gratefully acknowledge the support provided by Vale Inc. and the Natural Sciences and Engineering Research Council (NSERC) of Canada.

Appendix 1

Boudali and Dugan (2005) have introduced the following formalism to calculate P_{ij} values (in their work P_{yx}) in Table 2:

$$P(B=y \mid A=x)=\frac{\int_{(x-1)\Delta}^{x\Delta}\int_{(y-1)\Delta}^{y\Delta}\lambda e^{-\lambda(b-a)}\lambda e^{-\lambda a}\,da\,db}{\int_{(x-1)\Delta}^{x\Delta}\lambda e^{-\lambda a}\,da}= \tag{7.13}$$

$$\frac{\lambda\Delta\int_{(y-1)\Delta}^{y\Delta}\lambda e^{-\lambda b}\,db}{\int_{(x-1)\Delta}^{x\Delta}\lambda e^{-\lambda a}\,da}=\lambda\Delta e^{\lambda x\Delta}e^{-\lambda y\Delta}$$

in which $\lambda_A = \lambda_B = \lambda$.

However, if Equation 7.13 is modified to be used for a SEQ gate by considering different failure rates of A and B, it results in Equation 7.14 which is always negative no matter what numerical values are used for its parameters, i.e., $\lambda_A, \lambda_B, and\ \Delta$:

$$P(B = y \mid A = x) = \frac{\int_{(x-1)\Delta}^{x\Delta} \int_{(y-1)\Delta}^{y\Delta} \lambda_B e^{-\lambda_B(b-a)} \lambda_A e^{-\lambda_A a}\, db\, da}{\int_{(x-1)\Delta}^{x\Delta} \lambda_A e^{-\lambda_A a}\, da} = \frac{\lambda_A}{\lambda_B - \lambda_A} \frac{e^{\lambda_B \Delta} - 1}{e^{\lambda_A \Delta} - 1} (1 - e^{(\lambda_B - \lambda_A)\Delta})\, e^{-\lambda_B (y-x)\Delta} \quad \textbf{7.14}$$

Appendix 2

To obtain the entries of Table 7.8, the joint probability distributions of both the conventional structure of Figure 7.8 and the modified structure of Figure 7.9 are expanded, and the latter is forced to replicate the results of the former.

According to Figure 7.8, the probability of a PAND gate being in the i-th interval could be obtained by marginalizing the joint probability distribution with respect to A and B as follows:

$$P(PAND = i) = \sum_{A,B} P(A)P(B)P(PAND = i \mid A, B) \quad \textbf{7.15}$$

In fact, Table 6 determines whether or not $P(A)P(B)$ in Equation 7.15 participates in the calculation of $P(PAND = i)$, for $P(PAND = i|A, B)$ equal to one or zero, respectively. So, $P(PAND = i)$ for different time intervals is as follows:

$$P(PAND = 1) = P(A = 1)P(B = 1) \quad \textbf{7.15.1}$$

$$P(PAND=2)=P(A=1)P(B=2)+P(A=2)P(B=2) \quad \textbf{7.15.2}$$

$$P(PAND=3)=P(A=1)P(B=3)+P(A=2)P(B=3)+ P(A=3)P(B=3)+P(A=2)P(B=1)+P(A=3)P(B=1)+ P(A=3)P(B=2) \quad \textbf{7.15.3}$$

According to Figure 7.9, the same marginalization as Figure 7.8 can be done but with a different joint distribution to find $P(PAND=i)$:

$$P(PAND=i)=\sum_{A,B} P(A)P(B\mid A)P(PAND=i\mid B) \quad \textbf{7.16}$$

Similar to Table 7.6, Table 7.7 determines whether or not $P(A)P(B|A)$ in Equation 7.16 participates in the calculation of $P(PAND=i)$, for $P(PAND=i|B)$ equal to one or zero, respectively. So, $P(PAND=i)$ for different time intervals is as follows:

$$P(PAND=1)=P(A=1)P(B=1\mid A=1)P(PAND=1\mid B=1) \quad \textbf{7.16.1}$$

According to Table 7.7, $P(PAND=1|B=1)$, and if $P(B=1|A=1)$ in Table 7.8 is replaced by $P(B=1)$ for the sake of neutral dependency, Equation 7.16.1 is thus simplified to Equation 7.15.1.

$$P(PAND=2)= P(A=1)P(B=2\mid A=1)P(PAND=2\mid B=2)+ P(A=2)P(B=2\mid A=2)P(PAND=2\mid B=2) \quad \textbf{7.16.2}$$

According to Table 7.7, $P(PAND=2|B=2)=1$, and if $P(B=2|A=1)$ and $P(B=2|A=2)$in Table 7.8 are replaced by $P(B=2)$, each, Equation 7.16.2 is consequently simplified to Equation 7.15.2.

$$
\begin{aligned}
&P(PAND=3)= \\
&P(A=1)P(B=3\,|\,A=1)P(PAND=3\,|\,B=3)+ \\
&P(A=2)P(B=3\,|\,A=2)P(PAND=3\,|\,B=3)+ \\
&P(A=3)P(B=3\,|\,A=3)P(PAND=3\,|\,B=3)+ \\
&P(A=2)P(B=1\,|\,A=2)P(PAND=3\,|\,B=1)+ \\
&P(A=3)P(B=1\,|\,A=3)P(PAND=3\,|\,B=1)+ \\
&P(A=3)P(B=2\,|\,A=3)P(PAND=3\,|\,B=2)
\end{aligned}
\qquad \textbf{7.16.3}
$$

According to Table 7.7, $P(PAND = 3|B = 3) = 1$, and if each of $P(B = 3|A = 1)$, $P(B = 3|A = 2)$, and $P(B = 3|A = 3)$in Table 7.8 are replaced by $P(B = 3)$, the first three sentences on the right hand side of Equation 7.16.3 become equal to the first three sentences on the right hand side of Equation 7.15.3.

The last three sentences on the right hand side of Equation 7.16.3 are equal to zero (see Table 7.7) unless $P(PAND = 3|B = 1)$ in the fourth and fifth sentences and also $P(PAND = 3|B = 2)$ in the sixth sentence are replaced by $(PAND = 3|B = 3)$.

Finally if, according to Neutral Dependency, $P(B = 1|A = 2)$ and $P(B = 1|A = 3)$ are replaced by $P(B = 1)$, and $P(B = 2|A = 3)$ is replaced with $P(B = 2)$ in Table 7.8, the last three sentences of Equation 7.16.3 become equal to the last three sentences of Equation 7.15.3. These terms appear in boldface in Table 7.8 for ease of viewing.

It should be noted that replacing $P(PAND = 3|B = 1)$ and $P(PAND = 3|B = 2)$ with $P(PAND = 3|B = 3)$ does not really change $P(PAND = 3)$. Indeed, this replacement only helps the last three sentences remain in the calculation process by transferring them to the last row of Table 8, where they can be accounted for $P(PAND = 3)$.

Alternatively, one can avoid the foregoing procedure of obtaining $P(PAND = 3)$ by recognizing that the summation of probabilities in each column of a CPT must be equal

to one. So, after the conditional probabilities of the first and second rows of Table 7.8 are determined using Equation 7.16.1 and 7.16.2, respectively, the conditional probabilities of the third row (the last one) could simply be achieved.

7.7 References

American Society of Mechanical Engineers (ASME). Boiler and Pressure Vessel Code, Section VIII, Division I, 2004.

Aven T, Sklet S, Vinnem JE. Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description. Journal of Hazardous Materials 2006; 137: 681-91.

Bearfield G, Marsh W. Generalizing event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science 2005; 3688: 52-66.

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Reliability Engineering and System Safety 2001; 71: 249-60.

Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 2005; 87: 337-49.

Boudali H, Dugan JB. A new Bayesian approach to solve dynamic FTs. Proceedings of Reliability and Maintainability Symposium (RAMS 05) 2005: 451-6.

Boudali H, Dugan JB. A continuous-time Bayesian network reliability modeling and analysis framework. IEEE Transaction on Reliability 2006; 55: 86-97.

CSB. Goodyear heat exchanger rupture, 2011. Investigation No. 2008-06-I-TX. http://www.csb.gov/assets/document/Case_Study.pdf. (Last checked on 04.10.2011).

Delvosalle C, Fievez C, Pipart A, Debray B. ARAMIS project: a comprehensive methodology for the identification of reference accident scenarios in process industries. Journal of Hazardous Materials 2006; 130: 200-19.

Dugan JB, Bavuso SJ, Boyd MA. Dynamic fault tree models for fault tolerant computer systems. IEEE Transaction on Reliability 1992; 41: 363-77.

Duijm NJ. Safety-barrier diagrams as a safety management tool. Reliability Engineering and System Safety 2009; 94: 332-41.

Fussell JB, Aber EF, Rahl RG. On the quantification analysis of priority-AND failure logic. IEEE Transaction on Reliability 1976; 25: 324-26.

HUGIN Expert software version 7.4 (2010). <http://www.hugin.com>.

Jensen FV, Nielsen TD. Bayesian networks and decision graphs. 2nd ed. New York: Springer; 2007.

Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety 2011; 96: 925-32.

Langseth H, Portinale L. Bayesian networks in reliability. Reliability Engineering and System Safety 2007; 92: 92-108.

Marquez D, Neil M, Fenton N. Improved reliability modeling using Bayesian networks and dynamic discretization. Reliability Engineering and System Safety 2010; 95: 412-25.

Montani S, Portinale L, Bobbio A, Codetta-Raiteri D. RADYBAN: a tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks. Reliability Engineering and System Safety 2008; 93: 922-32.

Portinale L, Codetta-Raiteri D, Montani S. Supporting reliability engineers in exploiting the power of dynamic Bayesian networks. International Journal of Approximate Reasoning 2010; 51: 179-95.

Torres-Toledano JG, Sucar LE. Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science 1998; 1484: 195-206.

Weber P, Medina-Oliva G, Simon C, Iung B. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Application of Artificial Intelligence 2010; doi: 10.1016/j.engappai.2010.06.002.

8 Risk Analysis of Deepwater Drilling Blowouts: A Bayesian Approach**

Preface

A version of this manuscript has been published in the *Journal of Safety Science*. The co-authors, Dr. Khan and Amyotte supervised the principal author, Khakzad, to develop the research on the entitled topic and helped him to conceptualize the techniques and theories available for this topic. Khakzad conducted accident modeling and associated analyses while Khan and Amyotte reviewed the manuscript and provided the necessary suggestions.

Abstract

Blowouts are amongst the most undesired and feared accident as the ultimate result of the loss of well control. The dynamic nature of blowout accidents, resulting from both dynamic physical parameters and dynamic barriers, necessitates techniques capable of considering changes and being updated as new observations are made during the lifetime of a well. The present work is aimed at showing the application of bow-tie method and Bayesian network to the risk analysis of deepwater drilling blowouts. Considering the former method, fault trees and an event tree are developed for the kick, kick detection and the blowout prevention, respectively, and then combined to build a bow-tie model. In the latter method, the fault trees and the event tree are mapped into respective Bayesian

** Khakzad et al. Safety Science 2012.

networks and finally an object-oriented Bayesian network is constructed by connecting individual Bayesian networks. The Bayesian network method is taken priority over the bow-tie model since not only it can consider common cause failures and conditional dependencies but it also makes it possible to perform probability updating and sequential learning using near misses and incidents as accident precursors.

Keywords: Risk analysis, Deepwater drilling, Kick, Blowout, Bow-tie approach, Object-oriented Bayesian network, Sequential learning

8.1 Introduction

Risk analysis is very important for offshore activities since given an accident the rescue and evacuation actions are usually performed with difficulty due to the harsh environment and remoteness. The compact cluster of equipment and staffs on a relatively small area, e.g. drill ships and offshore installations, also makes any accident give rise to far more severe consequences than for onshore plants. In offshore industry, drilling accidents are reportedly more frequent than the others. Regarding drilling accidents, blowouts, though rare, are presumably the most feared and violent accidents significantly threatening human lives, environment and material assets (Holland, 1997).

Generally, blowout is an uncontrolled flow of hydrocarbons (gas, condensate, or even saltwater) from a well to the surrounding environment whether the atmosphere (surface blowout) or other exposed formations (underground blowout) as the ultimate consequence of kick. Kick is an unwanted influx of formation fluids into the wellbore as a result of loss of well control (LWC), in which the pressure of formation fluids, i.e. pore pressure (P_P), exceeds the pressure exerted by the column of drilling fluid on the bottom

of the wellbore, i.e. bottom hole pressure (*BHP*). A kick can finally end up with a blowout if not timely detected and properly prevented. Well control measures whether technical, managerial or organizational are aimed at maintaining the well integrity and reducing the risk of LWC through kick prevention, kick detection, blowout prevention and kill operations (Figure 8.1).

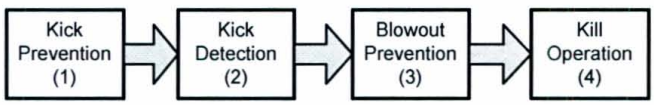


Figure 8.1. Schematic of well control procedure.

Figure 8.1 shows the sequential steps followed to maintain the well integrity. The first three steps are related to the *loss of well control* while the last one is related to the *regain of well control* and is performed only if a blowout can be prevented. Recently, a complex series of human errors and mechanical failures resulted in a LWC in Macondo Well on April 20, 2010, which finally led to a blowout, leaving totally 28 deaths and injuries and a significant amount of hydrocarbon spill. The fire and explosions that followed the blowout finally caused the Deepwater Horizon drilling rig to sink. According to the report provided by BP incident investigation team (BP, 2010), a chain of events was to blame for the LWC. Of these events, those such as replacing the drilling mud with seawater and poor cementing caused a kick to occur (i.e., failure of step 1 in Figure 8.1) while failing to notice the kick indications such as changes in the flow rate and the wellbore pressure made the kick not being detected until it flowed up into the riser (i.e.,

failure of step 2 in Figure 8.1). The failure of the blowout preventer (BOP) to close in the well also escalated the kick into a blowout (i.e., failure of step 3 in Figure 8.1). Since the kill lines as well as choke lines of the BOP were damaged, it was also impossible to perform kill procedure to re-establish the well control (i.e., failure of step 4 in Figure 8.1).

The risk of blowout cannot be eliminated, but can be reduced through preventive and mitigative safety measures. Since risk is defined as the product of probability and consequence, preventive safety measures are used to reduce the probability whereas mitigative measures are applied to alleviate consequences. However, the priority is usually given to the former, i.e., preventive measures (Holland, 1997). Safety measures, whether preventive or mitigative, are normally contemplated and allocated to the system of interest through risk assessment studies. Risk analysis not only determines if the risk is acceptable, but it also identifies the risk major contributing factors for which reducing measures should be applied. Conducting the blowout risk analyses, the blowout probability estimation is the first task usually carried out using statistical methods or traditional quantitative risk analysis techniques.

The blowout probability estimations using statistical data have often been questioned (Holland, 1997). The reason is that such estimations apply a wide range of data which differ in terms of the place of blowouts (e.g., North Sea or Canadian arctic waters), the type of wells (e.g., exploratory or development well), the depth of drilling (e.g., shallow or deep water drilling), and the time of blowouts (e.g., during drilling or tripping). From the place point of view, factors such as the weather condition, formation temperature,

pressure, permeability and porosity differ from place to place (Holland, 1997; Andersen, 1998; Nielsen et al., 2001). Therefore, the data resources used for blowout frequency estimation should be applied with extreme caution. For example, ERCB database (Energy Resources Conservation Board, Canada) covers onshore blowouts while WOAD (World Offshore Accident Databank, Norway) (1994) contains offshore blowouts as well as other offshore accidents. SINTEF Offshore Blowout Database (1995) covers both exploratory and development blowouts from the North Sea and the U.S. GoM OCS (Gulf of Mexico Outer Continental Shelf).

However, even having reliable and up-to-date historical blowout data, these generic data do not identify the series of events which finally resulted in a blowout. Thus, not only the well-specific data such as the pore pressure (P_P), bottom hole pressure (BHP), fracturing pressure (F_P) and the type of barriers are not taken into account, but also the causes of the blowout whether human errors or mechanical failures are not considered in the frequency estimation.

To overcome the aforementioned drawback of statistical methods, there have been attempts to localize generic data to the case of interest using adjustment factors. These adjustment factors reflect well-specific data (e.g., pore pressure) as well as company-specific data (e.g., kick management policies) the applications of which result in site-specific blowout frequencies. As an example of such statistical-based adjusting methods, BlowFAM (Blowout Frequency Assessment Model, 2004) is based on the SINTEF database and examines different elements such as drilling activities, reservoir characteristics and management parameters to identify total adjustment factor.

On the other hand, many researchers broke down the blowout phenomenon to its components such that the causal relationships among the components as well as the well-specific and company-specific parameters could be analyzed in a systematic manner. Bercha et al. (1978) used fault tree model (FT) to estimate the blowout probability of both exploratory and development wells in Canadian arctic waters. Although the application of event tree (ET) has briefly been discussed to represent the blowout as a potential consequence of the kick, the whole accident, starting from the causes of the kick and ending with the blowout, has finally been modeled using FT in their work. Later, Andersen (1998) proposed a stochastic model based on the physical mechanism of the kick as the initiating event of the blowout. The FT method was then applied to estimate the probability of the kick within each drilling sub-operation. Grouping of the drilling operation into sub-operations such as drilling, tripping and casing was advised due to different primary causes and safety barriers involved in each sub-operation.

Although being extensively used in the risk analysis of kicks and blowouts (Andersen, 1998; BP, 2010; Nielsen et al., 2001; Bercha, 1978; Arild et al., 2008; Worth et al., 2008; Arild et al., 2009) static FT is not suitable for large systems where, for example, dependent failures or common cause failures are present (bobbio et al., 2001; Khakzad et al., 2011; Khakzad et al., 2012). Further, aside from presumably static parameters such as formation porosity and permeability, there are dynamic parameters such as formation temperature and pressure which varies over time as the well goes deeper. Also, drilling parameters such as the weight and the volume of the drilling mud are always prone to unexpected changes because of, for example, unexpected gas pockets, losses into

formation and improper wellbore fill up in case of tripping (Holland, 1997). More importantly, dynamic safety barriers, unlike static barriers, are due to replacement as the well process proceeds from one phase (e.g., drilling phase) to another (e.g., production phase), which need to be taken into account when conducting the risk analysis for blowouts.

Bayesian networks (BNs) are probabilistic inference techniques for reasoning under uncertainty, being used in the field of risk analysis and safety assessment since the last decade. BNs apply d-separation and chain rule to represent causal relationships among a set of random variables considering local dependencies (Jensen and Nielsen, 2007). Many authors have shown the parallels between FT and BN (Bobbio et al., 2001; Khakzad et al., 2011; Torres-Toledano and Sucar, 1998; Boudali and Dugan, 2005) and discussed how the limitations of the former technique can to a large extent be addressed by the latter technique. However, the main advantage of BN making it a superior technique for the risk analysis of dynamic systems such as well control is the ability to perform probability updating. Applying Bayes' theorem, BN updates the initial beliefs as new information about the system becomes available over time. Therefore, not only the risk analysis can be used as a decision making tool to decide between various scenarios at the design stage of the well operation, but it can also be applied during the well lifecycle to identify risk factors helping to allocate proper safety measures as real-time changes take place in the well system. The merit of BN models in risk analysis of well control becomes accentuated when having more frequent accident precursors such as kicks can

be interpreted as indicators for relatively rarer major accidents such as blowouts (Skogdalen et al., 2011).

The present work is aimed at showing the application of BNs in the risk analysis of LWC and making a comparison with other conventional methods such as bow-tie (BT). The scope of the work is limited to the first three steps of the well control (Figure 8.1), investigating the probability of kick and its propagation into a blowout. In other words, the well control regain is not covered in this study. The current study is mainly based on the work of Andersen (1998) and Bercha et al. (1978). The rest of the paper is organized as follows. The well control event including the physical mechanism of kick, kick detection and the escalation of kick into blowout and the relevant barriers are discussed in Section 8.2. A brief description of risk analysis methods, BT and BN, is reviewed in Section 8.3. Section 8.4 is devoted to the application of BT and BN to the well control risk analysis while the conclusion is presented in Section 8.5.

8.2 Well control

8.2.1 Kick mechanism

Defined as an uncontrolled and unwanted influx of formation fluids into the wellbore, kick is the initial event which can potentially escalate into blowout unless detected at early phases and promptly prevented. Even if kick is controlled, it takes a while to circulate out the influx and re-establish the wellbore pressure balance. In the meanwhile, extra costs are imposed to the drilling rig in terms of additional recovery works and

several days of delay in resuming the drilling procedure (Nielsen et al., 2001). In some cases, the kick-induced damage is so severe that the well is plugged and abandoned.

A kick occurs as a result of the failure of the well primary barrier, i.e. the column of drilling mud, in the drilling phase of a well. The drilling mud, as a barrier, is aimed at maintaining the wellbore bottom hole pressure (BHP) greater than the pore pressure (P_P) but lesser than the fracturing pressure (F_P), i.e. $P_P < BHP < F_P$ (Andersen, 1998). The reason is that BHP greater than P_P prevents the formation fluids from flowing into the wellbore, whereas being smaller than F_P assures that the formation is not fractured, thus not causing the drilling mud to escape from the wellbore to the fractured formation. It should be noted that in the case of a fracture, owing to annular losses (i.e., a drop in the amount of the drilling mud), the hydrostatic pressure as a main component of BHP decreases and a kick occurrence is very likely.

While primarily provided by the drilling mud, BHP is decomposed to several pressure components (Equation 8.1) to better account for the variations in the drilling parameters and characteristics (Andersen, 1998; Arild et al., 2009).

$$BHP = P_h + P_f - P_{sw} + P_{sg} \qquad 8.1$$

Where P_h is the hydrostatic pressure due to the height of the drilling mud column above the wellbore bottom; P_f is the frictional pressure due to the pumping of the drilling mud through the drillstring; P_{sw} and P_{sg} are the swabbing and surging pressures due to the drillstring tripping out and in the wellbore, respectively.

The drilling operation, whether exploratory or development can also be categorized into sub-operations such as drilling, tripping, casing and cementing to explore the effective

contribution of each pressure component on the entire *BHP* (Arild et al., 2009). For example, during drilling sub-operation, where a column of drilling mud is present (hydrostatic pressure) and pumps are circulating the mud in the wellbore (frictional pressure), *BHP* can be expected as $BHP = P_h + P_f$. Likewise, if the drillstring is pulled out of the well (tripping out) to, for example, add a joint, and the pumps are off in the meanwhile, *BHP* would be as $BHP = P_h - P_{sw}$.

The hydrostatic pressure, P_h, is a function of the drilling mud's height (h) and density (ρ). Therefore, factors which either cause h to decrease (e.g., annular losses) or cause ρ to decrease (e.g., gas cut mud) result in a decline in P_h and consequently in *BHP*. Likewise, since the frictional pressure, P_f, is related to the pumping rate, a pump failure or power outage would cause a drop in P_f and thus in *BHP*. When pulling the drillstring out of the wellbore, a negative pressure gradient, P_{sw}, is created which may help a kick to occur by reducing *BHP*. This effect is called swabbing. The amount of P_{sw} depends on the speed of tripping, the viscosity of the mud and the diameter of the wellbore (Nguyen, 1996). The narrower the wellbore, the more sever the swabbing effect would be. On the other hand, a positive pressure gradient, P_{sg}, is created when the drillstring is run into the wellbore (tripping in). The effect is called surging.

Whether a decrease in *BHP* would cause a kick or not depends on the drilling margin or the down-hole differential pressure (Andersen, 1998). The lower drilling margin, ΔP_L, is defined as the difference between the initial bottom hole pressure, BHP_0, and the pore pressure, i.e. $\Delta P_L = BHP_0 - P_P$, while the upper drilling margin, ΔP_U, is defined as the difference between the fracture pressure and the initial bottom hole pressure, i.e. $\Delta P_U =$

$F_P - BHP_0$. Assuming both a constant pore pressure and a constant fracture pressure, as long as the decrease in *BHP* is smaller than ΔP_L, or the increase in *BHP* is smaller than ΔP_U, neither a kick nor a fracture occurs. The drilling margins are decided by the type of drilling. In shallow waters an overbalanced drilling policy ($\Delta P_L > 0$) is usually taken whereas in deep waters, the near-balanced drilling ($\Delta P_L \cong 0$) is preferred since it results in a higher drilling speed. Although the overbalanced drilling seems more desirable from the kick prevention point of view, a major overbalanced drilling ($\Delta P_L \gg 0$ or $\Delta P_U \cong 0$) may give rise to the formation fracturing which in turn causes annular losses and thus a kick is likely to occur. It should be noted that a sudden increase in *BHP*, for example due to P_{sg}, would readily escalate an overbalanced drilling into a major overbalanced drilling. On the contrary, although the near-balanced drilling advantageously results in a higher rate of penetration, a sudden drop in *BHP*, for example due to an unexpected gas pocket or circulation cut off, would result in an underbalanced condition ($\Delta P_L < 0$) and cause a kick to occur. However, from the kick detection perspective, a near-balanced drilling is suggested (see Section 8.2.2) (Nguyen, 1996).

8.2.2 Kick detection

Whether a kick would escalate into a blowout or not is highly dependent on how quickly it is detected and how properly and timely the mitigative barriers are implemented. In this case, the kick is controlled using kill operations, circulated out, and the well control is regained. In shallow water drillings (depths less than 1200 m), however, the priority is given over kick prevention rather than kick mitigation (Holland, 1997). The reason is that

in shallow water drillings, due to the insufficient strength of the formation, it is not safe to use blowout preventers (BOP) to close in the well and control the kick. In other words, if the well is shut in using a BOP, the risk of underground blowouts and the consequent cratering is impending. The cratering, in turn, can cause the drilling rig to tilt or even to capsize. This is why drilling companies have focused on the diverting of the kick (using diverter systems or riserless drilling methods) instead of trying to suppress the kick using BOP (Holland, 1997). However, regardless of a drilling company policy to divert (common in shallow water drilling) or suppress the kick (common in deep water drilling), early detection of the kick is crucial in terms of the well and the personnel safety.

Drilling parameters such as the rate of penetration and the drillstring torque, operational parameters such as the volume of mud tanks, and also mud characteristics such as temperature and gas content are continuously monitored and recorded through mud logging and wire-line logging. These data are then used not only to determine if the well safety is secured but also to obtain geological information about the formation during the drilling process (Nguyen, 1996).

Among drilling parameters, the rate of penetration is of great importance. An increase in the rate of penetration implies that either the bit has reached a porous or fractured formation or the lower drilling margin (ΔP_L) has decreased due to a drop in BHP or a rise in P_P. In the former condition, i.e. reaching to a porous formation, the risk of annular losses and in the latter condition, i.e. a decrease in drilling margin, the risk of underbalanced pressure is imminent. In either condition, a kick is very likely to occur.

According to the relation between the rate of penetration and the drilling margin, as shown in Figure 8.2 (Nguyen, 1996), when drilling with a high differential pressure (e.g., point d in Figure 8.2), a kick-induced drop in the pressure (e.g., the decrease of the pressure from point d to c) has a small effect on the penetration rate (i.e. $\Delta 1$), and is very likely not to be noticed. On the other hand, when drilling with a low differential pressure (e.g. point b), a decrease in the pressure (e.g., the decrease of the pressure from point b to a) has a noticeable influence on the penetration rate (i.e., $\Delta 2$). Thus, from the kick detection point of view, the smaller the drilling differential pressure, the likelier is the variation of the penetration rate (and consequently the kick) to be noticed. Likewise, the variations in either the drillstring torque or the pumping pressure can be interpreted as kick indicators.

Similar to for drilling parameters, the abnormal variations in operational parameters can be used to measure the extent to which the well is exposed to LWC, particularly the kick. Accordingly, the irregular changes in the volume of the drilling mud in the mud tanks as well as the trip tank can be taken as kick signs. An anomalous decrease in the mud volume may indicate annular losses, possibly due to the fractured formation, while an increase in the mud volume implies a water or gas influx into the wellbore, i.e. a kick occurrence. A more direct way to monitor the abnormal variations in the mud volume can be performed using flow meters installed on the inlet and outlet of the mud flow and comparing the differences (Bercha 1978; Nguyen, 1996).

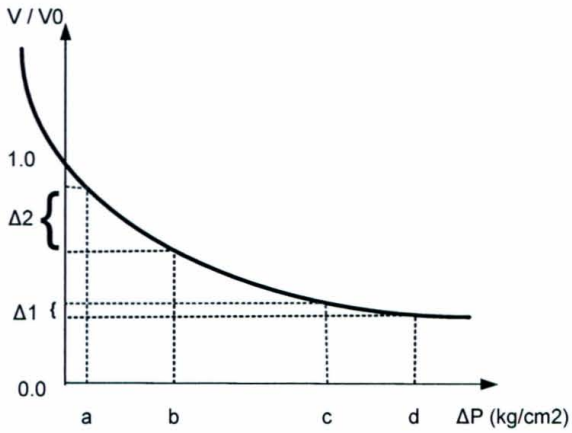


Figure 8.2. The relation between the penetration rate and the drilling margin [20]. V_0 is the rate of penetration when $\Delta P = 0$.

In addition to the abovementioned parameters, the mud characteristics can also be examined for any trace of the kick occurrence. In this regard, monitoring the changes in mud density and conductivity is of great importance. These changes can be due to water, gas or oil influxes into the well as a sign of kick. In the case of gas influx, aside from the decreasing influence the gas has on the mud density and consequently on the hydrostatic pressure, the type of gas, particularly CO_2, indicates the vicinity of an efficient hydrocarbon reservoir and thus a contingent risk of kick (Nguyen, 1996).

8.2.3 Blowout

Similar to a kick, a blowout occurs as a result of the failure of the well secondary barriers. In fact, in the case of a kick occurrence, the kick can escalate into a blowout either due to the mechanical failure of the secondary barriers or due to the non-detection

of the kick and consequently not putting the barriers into action. Except for the formation and the casing which are present in most phases as passive secondary barriers, the secondary barriers vary in type and placement during the various phases. Regardless of shallow water drillings in which the drilling mud acts as both the primary and the secondary barrier, BOP, Kelly valve and/or the drillstring safety valve are considered as secondary barriers in the drilling phase. In the production phase, on the other hand, a surface-controlled subsurface safety valve (SCSSV) and a Christmas tree are used as secondary barriers instead of BOP while in the wire-line phase a wire-line BOP is added to the safety barriers to compensate for the disabled SCSSV (Holland, 1997).

To take into account the effect of the secondary barriers on the well control process, it is also important to determine the blowout path. In fact, a kick can rise up in the wellbore through various paths such as the drillstring, the annulus and also between the casing (Holland, 1997). For example, in the case of an influx through the drillstring, the Kelly valve or the string safety valve can prevent the flow from entering the atmosphere while in the case of an influx through the annulus, a BOP can be activated. The BOP comprises an annular preventer, pipe rams and a blind or shear ram to prevent the kick from exiting the wellbore (i.e. blowout) as well as choke lines and kill lines to circulate out the kick and regain the well control. Generally, the blowouts are more frequent during the drilling phase and through the annulus path (Holland, 1997).

8.3 Risk analysis methods

8.3.1 Bow-tie

BT is an effective graphical method commonly used for the risk analysis of accident scenarios (Khakzad et al, 2012; Delvosalle et al., 2005; Khakzad et al., 2012). Focused on an undesired event as the pivot node, BT applies both a FT and an ET to determine the potential causes and consequences of the undesired event, respectively. The undesired event is indeed the top event of the FT. Figure 8.3 illustrates a typical BT in which components such as primary events (PE), intermediate events (IE), top event (TE), safety barriers (SB) and consequences (C) are shown.

The probability of the TE is calculated using the FT while the probabilities of the consequences are determined using the ET, based on the failures or successes of subsequent safety barriers. For example, the probability of C3 in Figure 8.3 can be estimated as $P\ (C3) = P(TE)P(SB1)P(SB2)\ (1 - P(SB3))$.

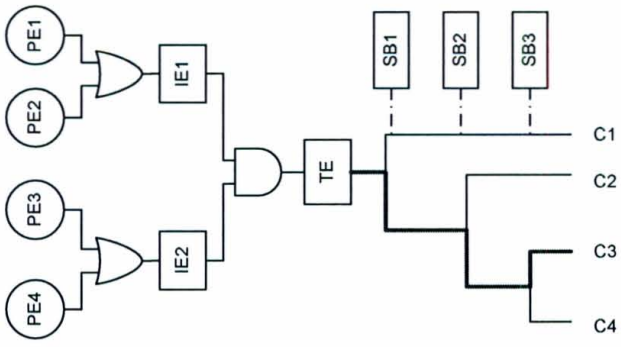


Figure 8.3. Typical bow-tie model consisting of a fault tree on the left and an event tree on the right-hand side.

Although taking advantage of FT and ET to construct a robust and transparent risk analysis method, the application of BT in the risk analysis of large systems, where common cause failures and dependent failures (conditional dependencies) are present, is limited. More importantly, because of being composed of static methods such as FT and ET, BT has not widely been recognized in the context of dynamic risk analysis (Khakzad et al., 2012) where the information about frequent accident precursors (e.g. kick) can be effectively used to update the estimated risk of rare major accidents (e.g. blowout) (Skogdalen et al., 2011). To take the new information into account to develop a dynamic risk framework, the abovementioned methods, i.e. FT, ET and BT, have been either coupled with Bayes' theorem (Khakzad et al., 2012; Kelly and Smith, 2009) or mapped into Bayesian networks (Bobbio et al., 2001; Khakzad et al., 2011; Bearfield and Marsh, 2005). In the present study, the latter approach is applied.

8.3.2 Bayesian network

BN is a graphical technique that has started to be widely applied in the field of risk analysis. Known as an inference probabilistic method, BN is composed of nodes, arcs and probability tables to represent a set of random variables and the conditional dependencies among them. Due to its flexible structure and probabilistic reasoning engine, BN has been focused as a promising method for the risk analysis of large and complex systems.

Considering the conditional dependencies of variables, BN represents the joint probability distribution $P(U)$ of variables $U=\{A_1,\ldots,A_n\}$, as:

$$P(U) = \prod_{i=1}^{n} P(A_i|Pa(A_i)) \quad 8.2$$

Where $Pa(A_i)$ is the parent set of variable A_i [16]. Accordingly, the probability of A_i is calculated as:

$$P(A_i) = \sum_{U \setminus A_i} P(U) \quad 8.3$$

Where the summation is taken over all the variables except A_i. The main application of BN is in probability updating. BN takes advantage of Bayes' theorem to update the prior probabilities of variables given new observations, called evidence E, rendering the updated or posterior probabilities:

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \quad 8.4$$

8.3.3 Object-oriented Bayesian network

Object-oriented Bayesian network (OOBN) is a type of BN, comprising both instance nodes and usual nodes. An instance node is indeed a sub-network, representing another BN. Using OOBNs, a large complex BN can be constructed as a hierarchy of sub-networks with desired levels of abstraction (HUGIN, 2010). Therefore, the model construction is facilitated and the communication between model's sub-networks is more effectively performed. Further, the tedious task of repeating identical structure fragments and probability tables is to a large extent alleviated, particularly in the case of repetitive networks such as time-sliced BN.

Instance nodes are connected to other nodes through interface nodes, including input and output nodes. Input nodes accept the same probability values as of their immediate parents. Thus, each input node cannot have more than one parent. In contrast, output

nodes are ordinary nodes, conveying their probability values to other input nodes or affecting the probabilities of other usual nodes. Therefore, each output node can have more than one child.

Figure 8.4 illustrates, as an example, how a simple BN (left) can be developed using a hierarchy of smaller and simpler BNs (middle). As can be seen, node 4 is selected both as the output node (with thick border) in instance node A and as the input node (with dashed border) in instance node B to connect the instance nodes together. The BN can finally be represented briefly using only instance nodes A and B (right).

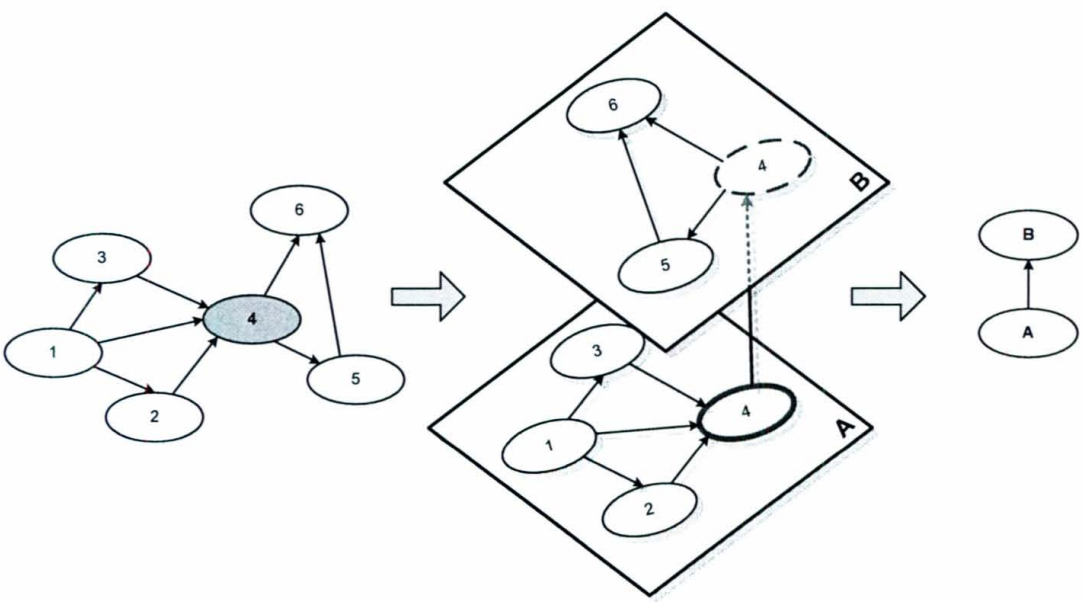


Figure 8.4. Using OOBN to modularize BN into sub-networks. A BN (left) is constructed using hierarchical structures with arbitrary levels of abstraction (middle) and consequently shown using instance nodes (right).

8.4 Well control modeling

8.4.1 Case-study description

Before a well control risk analysis, it should be determined that for which well phase the analysis is to be conducted. As mentioned earlier, the type and placement of safety barriers for the drilling phase differ from those of the production phase. In the case of drilling phase, it matters if it is shallow water or deep water drilling as well as if it is exploratory or development drilling. Dividing the drilling phase into sub-operations such as drilling, tripping, casing or cementing also helps to better identify the primary causes of LWC.

In the present study, the risk analysis is performed for drilling phase since the frequency of blowouts is higher for this phase. Also, it is assumed that the drilling is performed in deep waters and for a development well. Therefore, in contrast to shallow water drilling, both primary and secondary barriers are present and also a near-balanced drilling policy is preferred to an overbalanced drilling. Further, as compared to exploratory drilling, the required information about the formation properties such as P_P and F_P is presumably available during the development drilling. The total risk of drilling phase equals the sum of the risk of respective drilling sub-operation. In this study however, for illustrative purposes, the risk analysis for the drilling sub-operation is carried out in which the wellbore is initially filled with drilling mud and the circulation is in progress, implying that both P_h and P_f contribute to BHP.

8.4.2 Bow-tie modeling

8.4.2.1 Kick fault tree

Kick is the first undesired event in a series of events leading to LWC (see Figure 8.1). Thus, according the foregoing case-study, a FT is developed in Figure 8.5 to estimate the kick probability. It should be noted that since a near-balanced drilling is performed, it is assumed that a decrease in either P_h or P_f will cause a decrease in BHP such that a negative differential pressure (i.e. $\Delta P_L < 0$) would be likely to occur. This is why in the FT of Figure 8.5 intermediate events "Low hydrostatic pressure" and "Lost circulation" contribute to "Negative differential pressure" via an OR gate. The FT components and probabilities are shown in Table 8.1 (Bercha, 1978; OREDA; 2002)]. Assigning the probabilities to the primary events of the FT, the probability of the kick is calculated as 1.22E-02.

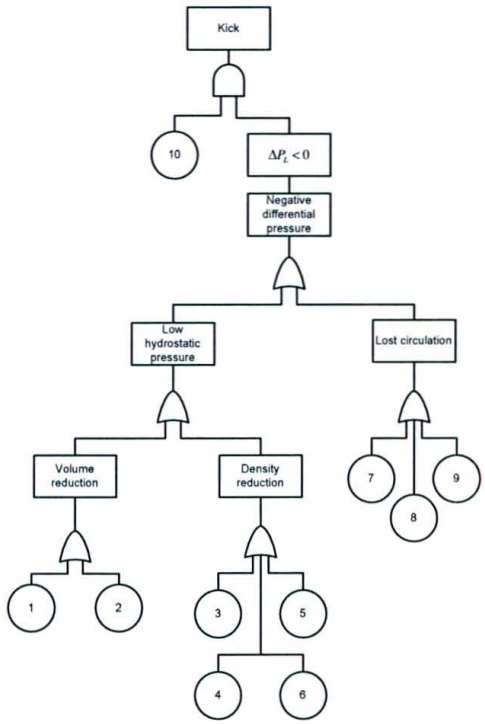


Figure 8.5. Kick fault tree.

Table 8.1. The components of the kick FT in Figure 8.5 and their probabilities

Index	Description	Probability	Updated probability
1	Annular losses	1.00E-02	5.46E-01
2	Riser rupture	1.00E-02	5.67E-02
3	Temperature effects	2.50E-03	1.42E-02
4	Gas-cut mud	7.00E-03	3.97E-02
5	Failure in density measurement equipment	2.00E-04	3.40E-03
6	Operator failure in mixing the right density	3.00E-02	1.70E-01
7	Pump failure	4.00E-02	2.27E-01
8	Power failure	2.70E-04	1.50E-03
9	Pump control failure	1.00E-03	5.70E-03
10	Efficient hydrocarbon formation	1.25E-01	1.00E+00

8.4.2.2 Kick detection fault tree

Following the kick indicators briefly described in Section 8.2.2, a FT is developed (Figure 8.6) to estimate the failure probability of the kick detection. As can be seen from Figure 8.6, a variety of drilling parameters, operational parameters and mud characteristics is used as the kick signs. However, a combination of equipment failures and human errors would result in the kick non-detection. It is worth noting that the mud volume can be monitored using either mud tank indicators or flow meters installed on flow lines. Likewise, as the rate of penetration and the pressure are related to each other (see Figure 8.2), both of them can be taken into consideration to observe changes in the circulation pressure. The FT components and their probabilities are listed in Table 8.2. Assigning these probabilities to the primary events of the FT, the failure probability of the kick detection is calculated as 8.60E-06.

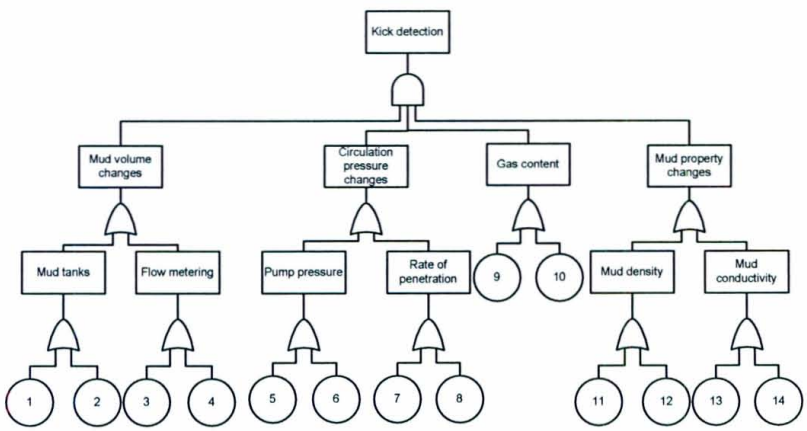


Figure 8.6. Kick detection fault tree.

Table 8.2. The components of the kick detection FT in Figure 8.6 and their probabilities.

Index	Description	Probability	Updated probability
1	Failure of tank level indicator (float system)	1.40E-04	2.00E-04
2	Failure of operator to notice tank level changes	1.00E-01	1.21E-01
3	Failure of flow meter	1.10E-04	1.00E-04
4	Failure of operator to notice the flow meter	5.00E-03	6.10E-03
5	Failure of pressure gage	1.65E-02	1.87E-02
6	Failure of operator to notice the pressure change	1.00E-01	1.13E-01
7	Failure of displacement sensor (related to penetration rate)	2.00E-04	2.00E-04
8	Failure of operator to notice the change in penetration rate	5.00E-02	5.65E-02
9	Failure of gas detector	2.00E-04	3.00E-04
10	Failure of operator to notice the gas	5.00E-02	7.34E-02
11	Failure of density meter (column-type)	2.00E-04	3.40E-03
12	Failure of operator to notice density changes	5.00E-03	1.59E-02
13	Failure of resistivity sensor	2.00E-04	6.00E-04
14	Failure of operator to notice conductivity changes	5.00E-03	1.59E-02

8.4.2.3 Safety barriers event tree

Beside the kick detection as a barrier crucially required for blowout prevention, a high pressure 4-stage BOP stack including two pipe rams, a blind/shear ram and an annular preventer is also considered as safety barrier (Nguyen, 1997). It should be noted that even if the kick is detected and the BOP is activated, the blowout would not be prevented unless the casing is strong enough to hold the kick inside the wellbore (Bercha, 1978). The ET in Figure 8.7 illustrates the sequence of safety barriers devised for the blowout prevention. Except for the kick as the initiating event and the kick detection as the first barrier the probabilities of which are obtained from the FTs in Figures 8.5 and 8.6, respectively, the failure probabilities of the other barriers are shown in Table 8.3.

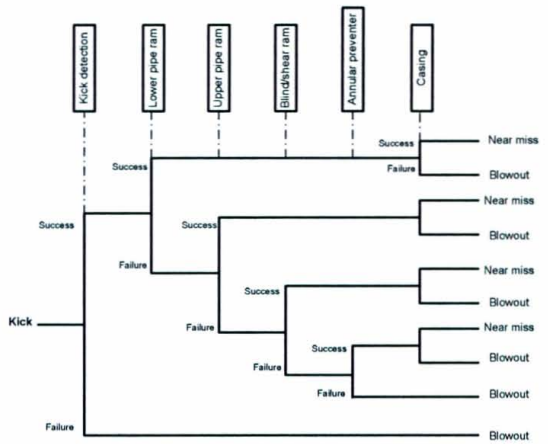


Figure 8.7. Escalation of kick into blowout event tree.

Table 8.3. The safety barriers of the ET in Figure 8.7 and their probabilities

Index	Description	Probability	Updated probability
1	Kick non-detection	8.60E-06	2.48E-02
2	Lower pipe ram	1.00E-04	1.00E-04
3	Upper pipe ram	1.00E-04	1.00E-04
4	Blind/shear ram	1.00E-04	1.00E-04
5	Annular preventer	1.00E-04	1.00E-04
6	Casing	2.00E-04	9.75E-01

8.4.2.4 Blowout bow-tie

Using the FTs and the ET developed in the previous sections, the BT model for the LWC is generated in Figure 8.8. Assigning the probabilities listed in Tables 8.1, 8.2 and 8.3 to the components of the BT, the probability of the blowout is consequently estimated as 2.55E-06.

As mentioned earlier, BT suffers limitations of both FT and ET as sub-models. As a result, it is not possible in a BT to take into account the probable common cause failures and conditional dependencies among the primary events of the FT and the safety barriers of the ET (Khakzad et al., 2012). For example, consider a case where the same density meter is used to measure the mud density both when the mud is mixed to the right density to be pumped into the wellbore and when the mud is brought back to the surface to be tested for kick signs.

Therefore, primary event 5 in the kick FT (Figure 8.5) and primary event 11 in the kick detection FT (Figure 8.6) would have a common cause failure, i.e. the failure of the density meter with the probability of 2.00E-04.

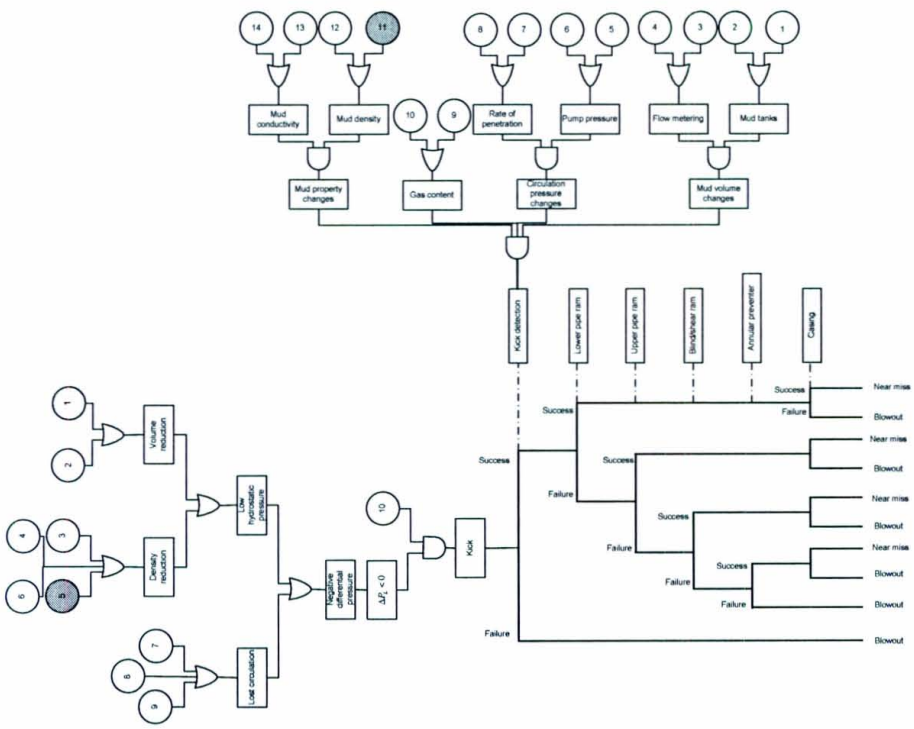


Figure 8.8. Bow-tie model for loss of well control. PE5 in the kick FT and PE11 in the kick detection FT have common cause failures (colored in orange) as well as PE1 in the kick FT and Casing in the safety barrier ET (colored in yellow).

Consequently, the top events of the respective FTs can no longer be considered independent from each other. In other words, both the initiating event (i.e. kick) and the first safety barrier (i.e. kick detection) of the ET (Figure 8.7) would become conditionally dependent although this dependency cannot be captured in the BT.

Likewise, the same problem would arise if the annular losses of the drilling mud and the casing failure are both related to the poor cementing problem. In this case, primary event 1 in the kick FT (Figure 8.5) and the last safety barrier in the ET (Figure 8.7) share the poor cementing as the common cause failure, making top event *Kick* and safety barrier *Casing* conditionally dependent. Accordingly, for illustrative purposes, it is assumed that in the case of poor cementing, the probability of annular losses would increase from 0.01 (Table 8.1) to 0.1.

8.4.3 Bayesian network modeling

8.4.3.1 Mapping from bow-tie

To overcome the aforementioned limitations, the BT in Figure 8.8 is used to construct the corresponding BN shown in Figure 8.9. In fact, after the respective BNs are developed for the previously developed FTs and ET, they are included in the OOBN of Figure 8.9 as instance nodes.

In the OOBN, instance nodes *Kick* and *Kick_Detection* are mapped from the FTs in Figures 8.5 and 8.6, respectively, while instance node *Barriers* is mapped from the ET in Figure 8.7. It also should be noted that node *BOP* in instance node *Barriers* is itself an instance node comprising safety nodes *Lower pipe ram*, *Upper pipe ram*, *Blind/shear ram* and *Annular preventer*.

Further, another instance node, namely *Common_cause_failures*, is added to the network to account for the conditional dependencies among the foregoing instance nodes. As mentioned earlier, the failure of *Density meter* contributes to the failure probabilities of *Kick* and *Kick_Detection* through primary nodes 5 and 11, respectively, while *Cementing* affects the failure probabilities of *Kick* and *Barrier* through primary nodes 1 and *Casing*, respectively. The BOP cannot be activated unless the kick is detected. This is why *Kick_Detection* is connected to *Barriers* to take into account such dependency. Note that when mapping the BT into the OOBN, *Kick* is connected to *Consequence*, adding another state, namely Safe state to node *Consequence* to account for the non-occurrence of *Kick* .After the OOBN is analyzed using HUGIN 7.4 software (http://www.hugin.com), the probability of the blowout is calculated as 4.60E-06.

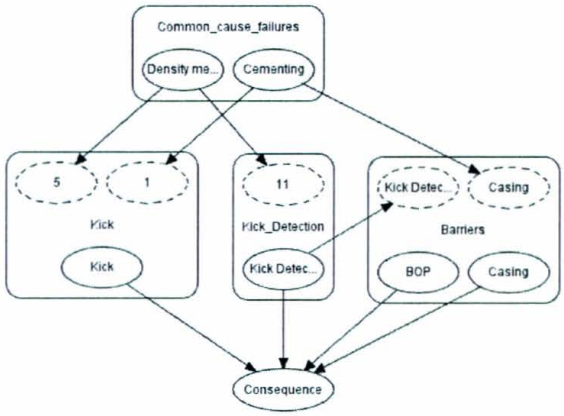


Figure 8.9. OOBN for the loss of well control, including instance nodes and the usual node Consequence.

As can be seen from Figure 8.9, only interface nodes, i.e., input and output nodes, are presented for each instance node, making the network less complex and more tractable. However, it is possible to illustrate the model even more briefly by showing only the instance nodes (Figure 8.10).

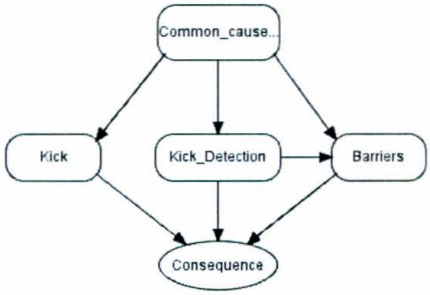


Figure 8.10. Collapsed form of the OOBN for the loss of well control.

8.4.3.2 Probability updating

In addition to offering a flexible structure and a robust reasoning engine, the main application of BN is in probability updating which cannot be done by BT unless equipped with other techniques such as Bayes' theorem or physical models. In probability updating, not only the posterior probability of event x_i is calculated given a piece of evidence, but also the most probable configuration of events leading to that evidence is determined. The most common type of evidence used in such probability updating is the knowledge about the top event or consequences being in one of their states according to which the probabilities of the primary events are updated.

In the present study, the posterior probabilities of events, assuming that a blowout has occurred, i.e. $P(x_i \mid Consequence = Blowout)$, are estimated and shown in the last columns of Tables 8.1, 8.2 and 8.3. Also, regarding the most probable configuration of events, it is determined that the failure of casing led to the annular losses which in turn caused a negative differential pressure. Due to the presence of an effective hydrocarbon reservoir, this negative pressure caused an influx of the reservoir fluids into the well, resulting in a kick. Although the kick was detected and the BOP was accordingly activated and properly worked, the casing failed to hold the influx in the well and thus a blowout occurred. The probability of this configuration of events is estimated as 0.35.

8.4.3.3 Sequential learning: application of accident precursors

Using BN for risk analysis of domains also makes it possible to take advantage of sequential learning (Spiegelhalter et al., 1990) to adapt the probability values of the

system as changes take place over time. This method is also known as probability adapting or sequential updating, and is particularly useful when modeling dynamic systems (Spiegelhalter et al., 1990). Knowing the causal relationships and the prior probability distributions for the system under study, sequential learning takes new observations, sequentially made over time, into account to revise the probability distributions of nodes for which these observations have been recorded. While propagating throughout the network, these new observations would also update other nodes' probability distributions as long as these nodes are not d-separated from the observed nodes (Jensen and Nielsen, 2007).

In the risk analysis of major accidents, which are low in probability and severe in consequences, sequential learning can be implemented based on accident precursor observations, which are more frequent but less severe (Mel and Seider, 2006). Considering major accidents as accidents resulting in at least 5 deaths and significant assets lost, accident precursors can be taken as incidents and near misses with no significant consequences which, however, have the potential to escalate into major accidents. Accordingly, in the context of well control risk analysis, kicks as well as near misses such as loss of circulation or loss of drilling mud which can lead to a blowout can be used as accident precursors (Skogdalen et al., 2011). In the present study, for illustrative purposes, it is assumed that the near misses and incidents in Table 8.4 are observed and recorded over the course of 5 weeks of the drilling.

Table 8.4. Accident precursors during the 5 weeks of drilling operation.

Week	1	2	3	4	5
Pump failure	-	1	-	-	-
Pump control failure	1	-	2	1	-
Power failure	1	-	-	-	1
Gas-cut mud	-	1	-	1	2

Using these data, the prior probability distributions of the observed nodes Pump, Pump control, Power and Gas-cut mud (the primary events of the FT in Figure 8.5) are revised, resulting in updated probabilities for the kick and blowout (Figure 8.10). As can be seen from Figure 8.10, the probabilities of the kick and the blowout have increased more than 4 and 7 times, respectively, compared to their initial estimates at the start of the drilling operation, i.e. week 0.

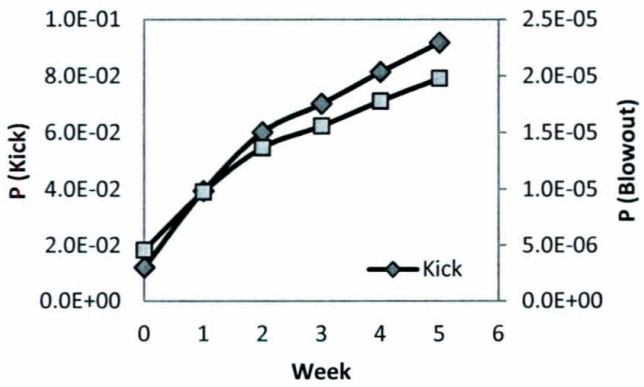


Figure 8.11. The updated probabilities of kick and blowout based on sequential learning.

8.5 Conclusion

In this work, the risk analysis for loss of well control was carried out using both bow-tie and Bayesian network approaches. Bayesian network was shown to be taken priority over bow-tie since it can consider common cause failures as well as conditional dependencies among the primary events of the well control system. In the present study, object-oriented Bayesian network was used to model the complex and interlinked domain of well control with significant levels of abstraction. Thus, the model became tractable, and the dependencies among the model segments were better shown, resulting in a more effective modeling and communication with stakeholders. It is also concluded that using Bayesian networks to model well control events makes it possible to take advantage of Bayesian updating as new information becomes available. This information can be used either for probability updating and identification of the most probable configuration of events or for sequential learning. However, this study showed that due to the scarcity of blowout data, sequential learning can effectively be applied for probability adapting while near misses and incidents are considered as accident precursors.

Acknowledgment

The authors thankfully acknowledge the financial support provided by Natural Science and Engineering Research Council (NSERC) of Canada and Petroleum Research Atlantic Canada (PRAC).

8.6 References

Andersen LB. Stochastic modeling for the analysis of blowout risk in exploration drilling. Reliability Engineering and System Safety 1998; 61: 53-63.

Arild O, Fjelde KK, Merlo A, Daireaux B, Loberg T. BlowFlow- a new tool within blowout risk management. SPE 114568, IADC/SPE Asia Pacific Drilling Technology Conference and Exhibition, Jakarta, Indonesia, 25-27 August 2008.

Arild O, Ford EP, Loberg T, Baringbing JWT. KickRisk- a well specific approach to the quantification of well control risks. SPE 124024, 2009 SPE Asia Pasific Oil and Gas Conference and Exhibition, Jakarta, Indonesia, 4-6 August 2009.

Bearfield G, Marsh W. Generalizing event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science 2005; 3688: 52-66.

Bercha FG. Probabilities of blowout in Canadian arctic waters. Canadian Environmental Impact Control Directorate, Report no. EPS 3-EC-78-12, 1978.

Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improvement the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety 2001; 71: 249-60.

Boudali H, Dugan JB. A discrete-time Bayesian network reliability modeling and analysis framework. Reliability Engineering and System Safety 2005; 87: 337-49.

BP. Deepwater Horizon Accident Investigation Report, 2010.

Delvosalle C, Fievez C, Pipart A, Casal Fabrega J, Planas E, Christou M, Mushtaq F. Identification of reference accident scenarios in SEVESO establishments. Reliability Engineering and System Safety 2005; 90: 238-46.

Dervo HJ, Blom-Jensen B. Comparison of quantitative blowout risk assessment approaches. SPE 86706, The Seventh SPE International Conference on Health, Safety, and Environment in Oil and Gas Exploration and Production, Calgary, Canada 29-31 March, 2004.

ERCB, Energy Resources Conservation Board, Alberta, Canada. http://www.ercb.ca.

Kelly DL, Smith CL. Bayesian inference in probabilistic risk assessment- The current state of the art. Reliability Engineering and System Safety 2009; 94: 628-43.

Khakzad N, Khan F, Amyotte P. Dynamic Safety Analysis of Process Systems by Mapping Bow-tie into Bayesian Network. Process Safety and Environmental Protection 2012; doi: 10.1016/j.psep.2012.01.005.

Khakzad N, Khan F, Amyotte P. Safety Analysis in process facilities: comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety 2011; 96: 925-32.

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

Holland P. Offshore blowouts: causes and control. Gulf Publishing Company, Houston, Texas 1997.

HUGIN Expert software version 7.4 (2010). http://www.hugin.com.

Jensen FV, Nielsen TD. Bayesian networks and decision graphs. 2nd ed. New York: Springer; 2007.

Meel A, Seider WD. Plant-specific dynamic failure assessment using Bayesian theory. Chemical Engineering Science 2006; 61: 7036-56.

Nilsen T, Sandoy M, Rommetveit R, Guarneri. Risk-based well control planning: the integration of random and known quantities in a computerized risk management tool. SPE 68447, SPE/ICoTA Coiled Tubing Roundtable, Houston, USA, 7-8 March, 2001.

Nguyen JP. Drilling. Editions Technip, Paris 1996.

OREDA. Offshore Reliability Data Handbook. SINTEF Industrial Management. Det Norske Veritas; 2002.

SINTEF Offshore Blowout Database, April 1995 Release, incl Users' Manual, Trondheim, Norway 1995.

Siu NO, Kelly DL. Bayesian parameter estimation in probabilistic risk assessment. Reliability Engineering and System Safety 1998; 62: 89-116.

Skogdalen JE, Utne IB, Vinnem JE. Developing safety indicators for preventing offshore oil and gas deepwater drilling blowouts. Safety Science 2011; doi: 10.1016/j.ssci.2011.03.012.

Spiegelhalter DJ, Lauritzen SL. Sequential updating of conditional probabilities on directed graphical structures. Networks 1990; 20: 579-605.

Torres-Toledano JG, Sucar LE. Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science 1998; 1484: 195-206.

WOAD, World Offshore Accident Databank, Statistical Report 1994, DNV Technica, Norway 1994.

9 Domino effect analysis using Bayesian networks[††]

Preface

A version of this manuscript has been published in the *Journal of Risk Analysis*. The co-authors, Dr. Khan, Amyotte, and Cozzani supervised the principal author, Khakzad, to develop the research on the entitled topic and helped him to conceptualize the techniques and theories available for this topic. Khakzad conducted accident modeling and associated analyses while Khan, Amyotte, and Cozzani reviewed the manuscript and provided the necessary suggestions.

Abstract

A new methodology is introduced based on Bayesian network both to model domino effect propagation pattern and to estimate the domino effect probability at different levels. The flexible structure and the unique modeling techniques offered by Bayesian network make it possible to analyze domino effects through a probabilistic framework, considering synergistic effects, noisy probabilities and common cause failures. Further, the uncertainties and the complex interactions among the domino effect components are captured using Bayesian network. The probabilities of events are updated in the light of new information, and the most probable path of the domino effect is determined on the basis of the new data gathered. The present study shows how probability updating helps

[††] Khakzad et al. Journal of Risk Analysis 2012.

to update the domino effect model either qualitatively or quantitatively. The methodology is applied to a hypothetical example and also to an earlier-studied case-study. These examples accentuate the effectiveness of Bayesian network in modeling domino effects in processing facility.

Keywords: Domino effect, Bayesian network, Risk assessment.

9.1 Introduction

Domino effects or chains of accidents in which an accident in a unit propagates into nearby units have recently been recognized as a priority issue among the risk and safety community experts (e.g. see the requirements of the EU Seveso-II Directive (1996) and its amendments). This is partly owing to the fact that today's ever growing industries are complex and congested by dense pipelines, process equipment and storage tanks most of which contain or transport hazardous material. Thus, it is not unlikely for a primary event to evolve to a much more severe sequence of secondary accidents as nearby equipment items or units are involved in the accident by means of heat, overpressure, and/or by the impact of explosion-induced airborne fragments.

While a remarkable progress in the risk and safety analysis of individual accident scenarios, limited to a single unit, has been achieved in recent years, domino accidents have gained less attention in the context of quantitative risk assessment (QRA) both due to their lower probability and higher complexity. However, frequent violent domino accidents took place in the last decade (e.g., see Abdolhamidzadeh et al., 2011; Darbra et al., 2010) such as that occurred in the BP Texas City refinery, where a vapor cloud

explosion (VCE) was followed by several other fires and explosions (CSB, 2007) These severe events have urgently raised the demand for consideration of domino scenarios in quantitative risk analysis and safety reports.

Accordingly, the study of domino effects in the literature has primarily been focused either on damage probability or on domino effect frequency estimation. Damage probability, alternatively known as escalation probability, has been estimated using distance-based models (Bagster and Pitblado, 1991), threshold values (Gledhill and Lines, 1998), probit models (Eisenberg et al., 1975; Vilchez et al., 2001; Cozzani and Salzano, 2004), combination of threshold values and probit models (Khan and Abbassi, 1998; Cozzani et al., 2006), and mathematical models based on the characteristics of secondary units and the surrounding environment (Khan and Abbassi, 1998; Landucci et al., 2009).

Although the frequency estimation and the sequence of accidents in domino effects have been investigated using statistical surveys (Darbra et al., 2010; Vilchez et al., 1995; Kourniotis et al., 2000), there are few works devoted to domino modeling and accident propagation, particularly in the context of QRA (Khan and Abbassi, 1998; reniers and Dullaert, 2007).

However, these works have drawbacks such as being mostly deterministic or using oversimplified assumptions limiting their application in the framework of QRA. More importantly, most of the previous research has neither recognized nor included the higher levels of domino effects, but only the first level of accidents where primary and secondary events are taking place. This shortcoming not only gives rise to an

underestimation of the potential risk, but it also leads to an improper allocation of safety measures (e.g., safety distances among adjacent units) since higher order events (e.g., tertiary events) and the synergistic effect of events of different orders are not considered in the modeling. Furthermore, in almost all foregoing works, the evolution pattern of domino accidents has not been taken into account, leading to the analysis of a cluster of accidents rather than a chain of accidents. Thus, a holistic probability has been calculated for domino effects, neither specifying the actual time-line of the escalation process nor privileging the more likely time-sequences of the domino scenario.

For example, Cozzani et al. (2005) took all possible accident scenarios triggered by a primary event into account in order to cope with the uncertainty arisen from the lack of knowledge about the actual accident propagation pattern. In their work, each accident scenario is a combination of the failure and non-failure of all secondary units which are likely to be impacted by the primary event, and frequency is estimated as a multiplication of probabilities. Later, Cozzani et al. (2006) and Antonioni et al. (2009) implemented the approach in a GIS-based software tool, Aripar-GIS, to allow its application in the analysis of industrial facilities or extended industrial areas. Most recently, Abdolhamidzadeh et al. (2010) applied Monte Carlo simulation to capture the dependencies between the primary event and the secondary events. However, the selection of secondary events was similar to that of Cozzani et al. (2005) and was based on randomly generated numbers, ignoring the actual accident propagation path.

It is worth noting that knowing the likely pattern and time-line of accident propagation not only results in a more realistic and accurate probability calculation, but it also helps

the analyst choose the most efficient placement of safety barriers, whether passive or active, to impede the progress of an accident or cease it in the early stages.

Bayesian network (BN) is a probabilistic graphical method for reasoning under uncertainty (Jensen and Nielsen, 2007) which has recently started to be used as a promising substitute for the majority of conventional methods in risk analysis and reliability engineering. A comprehensive statistical review of BN application can be found in (Weber et al., 2010), where the growing appeal of BN in various areas of reliability, risk and maintenance engineering has been shown over the last decade.

The reason for the popularity of BN among analysts lies in the fact that it benefits from both qualitative and quantitative modeling techniques. On the one hand, BN takes advantage of its highly flexible graphical structure to show the causal relationships among the nodes of the network. And, on the other hand, it determines the strength of such causal relationships through conditional probabilities assigned to the nodes. If the system under study (e.g., a chemical process plant comprising several units) could be considered as a set of variables (i.e., each variable stands for a unit or an equipment item, depending on the level of detail of the analysis), BN would be used to factorize the joint probability distribution of variables using the chain rule and d-separation rule, significantly reducing the system complexity.

This paper introduces a new methodology based on BN for probability estimation and propagation path determination of domino effects. After the propagation network is developed based on escalation vectors and threshold values, it is modified to estimate the probability of domino effect in different levels. The study also takes into account the

possible synergistic effects of the primary event and secondary events to examine the possibility of domino effect escalation to higher order events such as tertiary events and so forth.

As the main purpose of the present work is to establish a methodology for modeling and risk assessment of domino effects, it does not focus in detail on the methods used either to estimate escalation probabilities or to calculate physical effects such as heat radiation or explosion overpressure needed for escalation probability estimation. The paper benefits from generic data available in the literature or applies simple methods to obtain those data lacking in the literature.

Since the domino effect definition, characteristics, components, and relevant case studies have been comprehensively discussed in the literature, only the terminology and main concepts used in the present paper are recapitulated in Section 9.2. After a brief review of the fundamentals of BN in Section 9.3, the modeling framework of domino effect is presented in Section 9.4, in which both propagation path and probability estimation are modeled. In Section 9.5, a practical application of the methodology is presented while the conclusions from this work are discussed in Section 9.6.

9.2 Domino effect: terminology and characteristics

9.2.1 Accident propagation

Domino effect takes place when an accident in a unit, known as a "primary event", triggers other accidents in adjacent units by means of escalation vectors. Escalation vectors are physical effects such as fire impingement, fire engulfment, heat radiation,

overpressure or explosion-induced projectile fragments, depending on a variety of factors such as the type of the primary event and the distance between the accident epicenter and nearby units. There are several methods to calculate escalation vectors, such as analytical models, integral models and averaged models which are a combination of the two former models (CCPS, 2000; Assael and Kakosimos, 2010).

To determine which nearby units are impacted, the escalation vectors exerted by the primary event on the nearby units are compared with predefined threshold values. The escalation vectors well above the relevant thresholds are strong enough to cause credible damage to the nearby units, resulting in loss of containment or loss of physical integrity. Thus, based on a comparison between escalation vectors and threshold values, a preliminary screening of the nearby units is performed, leading to the specification of potential secondary targets. Figure 9.1 shows the outset of a domino effect in which the primary event in unit X_1 impacts its neighboring units. It is assumed that based on threshold values, units X_2, X_3, and X_4 are selected as potential secondary target units.

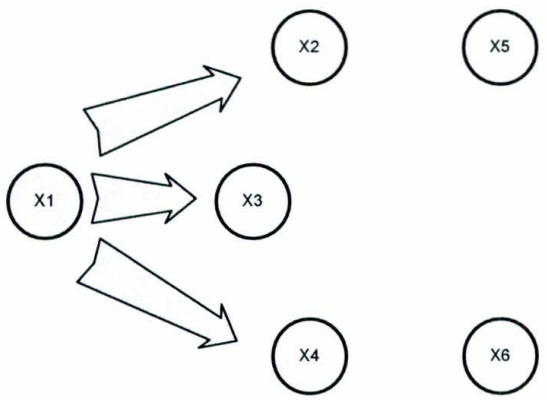


Figure 9.1. Domino effect where an accident in X_1 can trigger secondary accidents in X_2, X_3, and X_4. According to threshold values, X_5 and X_6 are not impacted by X_1.

In other words, potential secondary units are those adjacent units that are more likely to contribute to the domino effect. The inclusion of secondary units in the domino effect not only intensifies the accident causing more severe consequences, but also helps the domino effect escalate to the next level by impacting tertiary units. The escalation vectors originating from secondary events in turn trigger other accidents in tertiary units either by themselves or through synergistic effects.

Generally speaking, through synergistic effects, the escalation vectors of newly engaged units (of order i) cooperate with those of already engaged units (of order i-1) to impact the units of higher order (of order i+1) which had not passed the threshold criteria in previous levels. For example, according to Figure 9.1, units X_5 and X_6 are more likely to be involved in the domino effect as the escalation vectors of the secondary units X_2, X_3, and X_4 are added to that of the primary unit X_1, promoting the domino effect from the first level to the second level.

9.2.2 Escalation probability

As mentioned earlier, the initial selection of potentially vulnerable units in each level of domino effect is performed based on a comparison between escalation vectors and threshold values. By this procedure, although a qualitative propagation pattern of the domino effect would be schematized, the model cannot be quantitatively analyzed unless the escalation probabilities of vulnerable units are determined.

Among methods proposed in the literature, probit methods have been widely used to estimate the escalation probability of equipment due to simplicity and flexibility enabling application to a wide variety of equipment (Cozzani and Salzano, 2004). Probit methods may consider both the type of equipment (e.g., atmospheric or pressurized) and the type of escalation vector the equipment receives (e.g., heat radiation or explosion overpressure) to calculate the probit value Y (e.g., see Cozzani et al., 2005).

Generally, Y can be obtained using Equation 9.1:

$$\boldsymbol{Y = a + b\, Ln(V)} \qquad \textbf{9.1}$$

Where a and b are probit coefficients determined using experimental data and regression methods, and V is either the escalation vector (e.g., static overpressure ΔP (kPa) in the case of explosion) or an escalation-related parameter (e.g., time to failure of the vulnerable equipment, ttf (s), in the case of heat radiation). After Y is determined, the escalation probability, $P_{Escalation}$, could be calculated as:

$$\boldsymbol{P_{Escalation} = \phi(Y - 5)} \qquad \textbf{9.2}$$

Where ϕ is the cumulative density function of standard normal distribution. In the current study, the probit methods proposed by Cozzani et al. (2005) are used to obtain the probit values for overpressure and heat radiation.

Single hit dose-response models such as probit models express the escalation probabilities as a function of escalation vectors. However significant uncertainty arising from the lack of information or the extrapolation of escalation vectors has caused the probit models to lead to different results (Rai and Rayzin, 1981). Therefore, multi hit dose-response models have been proposed to overcome such limitations with a promising

potential of application in domino effect modeling. However, as the main aim of the present work is to introduce a new methodology based on BN, it does not further discuss such models, that are an important area of future exploration.

9.3 Bayesian networks

BN is a directed acyclic graph for reasoning under uncertainty in which the nodes represent variables and are connected by means of directed arcs. The arcs denote dependencies or causal relationships between the linked nodes, while the conditional probability tables (CPTs) assigned to the nodes determine the type and strength of such dependencies. In BN, nodes from which arcs are directed are called parent nodes whereas nodes to which arcs are directed are called child nodes. In fact, a node can simultaneously be the child of a node and the parent of another node. The nodes with no parent and the nodes with no children are also called root nodes and leaf nodes, respectively (Jensen and Nielsen, 2007).

Using the chain rule and the d-separation criterion, BN expands the joint probability distribution of a set of linked nodes, e.g., $U = \{X_1, X_2, \dots, X_n\}$. In other words, by considering only local dependencies, BN factorizes the joint probability distribution as the multiplication of the probabilities of the nodes given their immediate parents (Jensen and Nielsen, 2007):

$$\boldsymbol{P(U) = \prod_{i=1}^{n} P(X_i | Pa(X_i))} \qquad \textbf{9.3}$$

Where $P(U)$ is the joint probability distribution of variables and $Pa(X_i)$ is the parent set of variable X_i. The main application of BN is in probability updating. BN takes

advantage of Bayes theorem to update the probability of variables given new observations, called evidence E, to yield the posterior probability:

$$P(U|E) = \frac{P(U,E)}{P(E)} = \frac{P(U,E)}{\sum_U P(U,E)} \quad 9.4$$

In addition to its ability for probability updating, the flexible structure and modeling techniques of BN, which allow incorporating conditional probabilities, multi-state variables and common cause failures, have helped it emerge as a reliable alternative to most conventional methods.

However, the capability of BN in the modeling of domino effects, where complex interactions of variables cannot be neglected, has not yet been examined. So, the next section is aimed at showing how BN can be employed for either qualitative or quantitative investigation of domino effects.

9.4 Domino modeling

9.4.1 Propagation pattern

In order to model the likely propagation path of domino effect, the following steps are taken:

Step 1- According to the layout of the process plant of concern, a node is assigned to each process unit. These units are either susceptible to the accident or capable of escalating the accident, including distillation columns and atmospheric and pressurized storage tanks. For example, assume a process plant with six units (X_i, with i ranging from 1 to 6. See Figure 9.2).

Step 2- Using safety reports usually available for process plants or through risk assessment methods, the primary unit where the domino accident is likely to start is determined (e.g., X_1 in Figure 9.2). It is worth noting that considerations such as having a reasonably high occurrence probability and having enough inventory of hazardous material to produce credible escalation vectors should be taken into account when choosing the primary unit.

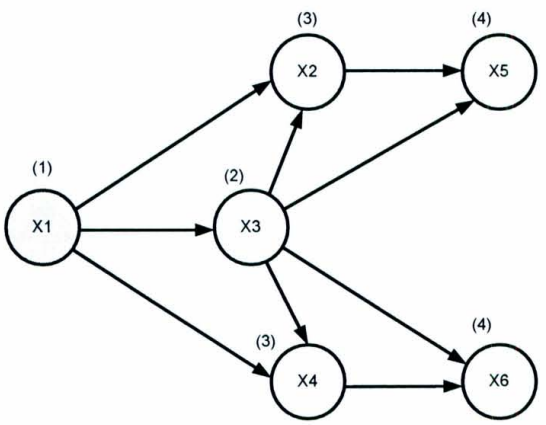


Figure 9.2. A likely propagation pattern of the domino effect. The numbers in parentheses show the occurrence orders of events (Step 4 of the methodology).

Step 3- According to the type of possible accident scenarios in the primary unit, the escalation vectors transmitted by the primary unit to nearby units are specified (e.g., see Cozzani et al., 2005; Antonioni et al., 2009) for different accident-related escalation vectors) and calculated. Methods for calculation of escalation vectors such as heat

radiation and explosion overpressure can be found in CCPS (2000), the TNO Yellow Book (1997) and Assael and Kakosimos (2010).

Step 4.1- Based on a comparison between predefined threshold values and escalation vectors, those nearby units for which the received escalation vectors exceed the threshold values are defined as potential secondary units (e.g., X_2, X_3 and X_4 in Figure 9.2).

Step 4.2- In the case of fire or explosion, the probit values (Y) are calculated for the potential secondary units.

Step 4.3- Using the probit values, the escalation probability of potential secondary units given the primary event, i.e., $P(X_2|X_1)$, $P(X_3|X_1)$ and $P(X_4|X_1)$, are calculated. It should be noted that in the case of fragment impact, conditional damage probabilities may be calculated by other approaches as those suggested by Nguyen et al. (2009).

Step 4.4- Among the potential secondary units, the one(s) with the highest escalation probability is chosen as the secondary unit (for example X_3 in Figure 9.2). Since the secondary events are caused by the primary event, a causal arc must be directed from X_1 to X_3, showing that the occurrence of X_3 is conditional on the occurrence of X_1.

Step 5- Given that the secondary units have been damaged, potential accident scenarios and their occurrence probabilities for the secondary units are specified. For example, if a pressurized LPG storage is damaged, two accident scenarios can be envisaged depending on the type of release and the proximity of ignition sources. For example, an instantaneous release along with immediate ignition would result in a fireball, whereas a release over the course of 10 minutes along with a delayed ignition would result in a vapor cloud explosion (VCE) (Cozzani et al., 2005).

Step 6- Substituting the secondary units for the primary unit, steps 3 to 5 are repeated to determine potential tertiary units (e.g., X_2 and X_4), potential quaternary units (e.g., X_5 and X_6) and so forth. In this case, it has been assumed since X_2 and X_4 (X_5 and X_6) have the same escalation probabilities; they both are selected as tertiary (quaternary) units. Figure 9.3 illustrates the flow diagram consisting of the above-mentioned steps which are taken to develop the propagation pattern of the domino effect.

It is worth noting that when repeating the same procedure (i.e., steps 3 to 5) for either the secondary units or higher order units, synergistic effects should be considered. For example in Figure 9.2, X_2 and X_3 cooperate with each other (i.e., their escalation vectors are superimposed) to trigger an accident in X_5. So, causal arcs have to be directed from X_2 and X_3 to X_5, showing the conditional dependency of the latter on the former units. Accordingly, when assigning the CPT of X_5, the escalation probability of X_5 due to the synergistic effect is also considered as $P(X_5|X_2, X_3)$.

After the likely propagation pattern of the domino effect is developed as a BN, and the probability of the primary event and the conditional probabilities of other events are calculated, the joint probability distribution of the events contributing to the domino effect can be derived. For instance, in Figure 9.2, the joint probability distribution of the events contributing to the domino effect $U = \{X_1, \dots, X_6\}$ is calculated as:

$$P(U) = P(X_1)P(X_3 \mid X_1)P(X_2 \mid X_1, X_3) \\ P(X_4 \mid X_1, X_3)P(X_5 \mid X_2, X_3)P(X_6 \mid X_3, X_4) \qquad \textbf{9.5}$$

It should be noted that choosing another starting point rather than X_1 would result in a BN different from that developed in Figure 9.2 and consequently a joint probability

distribution different from that shown in Equation 5. However, assuming X_1 as the primary unit and according to Figure 9.2 and Equation 9.5, the likely timeline or sequential order of the events would be as $X_1 \rightarrow X_3 \rightarrow X_2/X_4 \rightarrow X_5/X_6$.

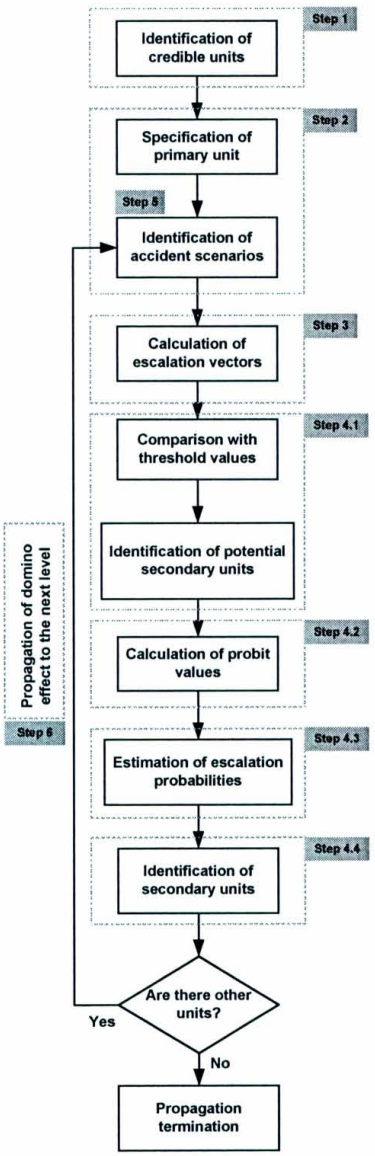


Figure 9.3. Procedure to develop the propagation pattern of domino effect.

9.4.2 Domino probability

Knowing the propagation pattern of the domino effect, the occurrence probability of the domino effect at different levels can be estimated. Generally, the probability of the domino effect (P_{Domino}) is calculated as the multiplication of the probability of the primary event ($P_{Primary}$) and the escalation probability of the impacted units ($P_{Escalation}$):

$$P_{Domino} = P_{Primary} \times P_{Escalation} \quad \textbf{9.6}$$

For a domino effect to be in the first level, it is necessary that the accident in the primary unit propagates into at least one of the nearby units. For example in Figure 9.2, considering X_3 as the secondary unit, the probability of the first-level domino effect is calculated as:

$$P_{First-level} = P(X_1)P(X_3|X_1) \quad \textbf{9.7}$$

Similarly, the domino effect could proceed to the second level only if at least one of the tertiary units X_2 and X_4 is impacted by the first-level domino accident (i.e., by a combination of X_1 and X_2). Accordingly, the probability of the second-level domino effect is calculated as:

$$P_{Second-level} = P(X_1)P(X_3 \mid X_1)P(X_2 \cup X_4|X_1, X_3) \quad \textbf{9.8}$$

To account for the union of X_2 and X_4 represented in Equation 9.8, Figure 9.2 can be modified by adding the auxiliary node L_1 such that $L_1 = X_2 \cup X_4$ (Figure 9.4). So, X_2 and X_4 are connected to L_1 using OR-gate causal arcs, resulting in the CPT shown in Table 9.1 for the node L_1. It should be noted that the probability of L_1 equals the propagation

probability of the domino effect to the second level, i.e., the probability that at least one of the tertiary units X_2 and X_4 is involved in the accident.

Likewise, for the domino effect to proceed to the third level, it is necessary that the accident in the tertiary units propagate into at least one of the quaternary units. For example, according to Figure 9.2, either X_5 or X_6 has to be impacted by the second-level domino effect to have a third-level domino effect. In this way, the probability of the third-level domino effect is:

$$P_{Third-level} = P(X_1)P(X_3 \mid X_1) \\ P(X_2 \cup X_4 \mid X_1, X_3).P(X_5 \cup X_6 \mid X_2, X_3, X_4) \quad \textbf{9.9}$$

As for X_2 and X_4, the union of X_5 and X_6 could be accounted for by adding another auxiliary node L_2 to the BN (Figure 9.4) such that $L_2 = X_5 \cup X_6$.

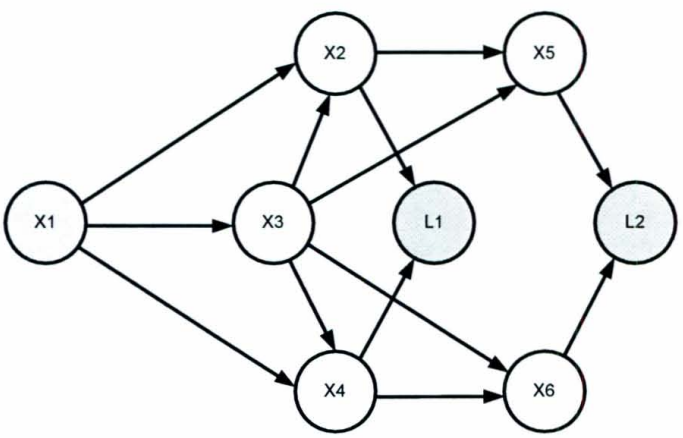


Figure 9.4. Modified BN to incorporate the union of tertiary and quaternary events using auxiliary nodes L_1 and L_2, respectively.

Table 9.1. The CPT assigned to the auxiliary node L_1 showing that it is conditionally dependent on its parents through an OR-gate.

		$P(L_1 \mid X_2, X_4)$	
X_2	X_4	Accident	Safe
Accident	Accident	1	0
Accident	Safe	1	0
Safe	Accident	1	0
Safe	Safe	0	1

Figure 9.4 can further be developed to directly render the probabilities of different-level domino effects. To this end, the nodes DL_1, DL_2 and DL_3 are added to the BN, standing for the three sequential levels of the domino effect, i.e., the first, the second and the third-level, respectively (Figure 9.5).

According to Equation 9.7, the probability of the first-level domino effect can be estimated as the product of $P(X_1)$ and $P(X_3|X_1)$. So, if DL_1 is connected to X_1 and X_3 by AND-gate causal arcs, $P(DL_1)$ would be equal to the probability of the first-level domino effect. This implies that for the first-level domino effect to occur, not only the primary event X_1, but also the secondary event X_3 is needed.

Likewise, according to Equation 9.8, if DL_2 is connected to nodes DL_1 and L_1 by AND-gate causal arcs, $P(DL_2)$ would be equal to the probability of the second-level domino effect. This indicates that for the second-level domino effect to occur, not only the first-level domino effect (i.e., DL_1), but at least one of the tertiary events is also needed, i.e., L_1.

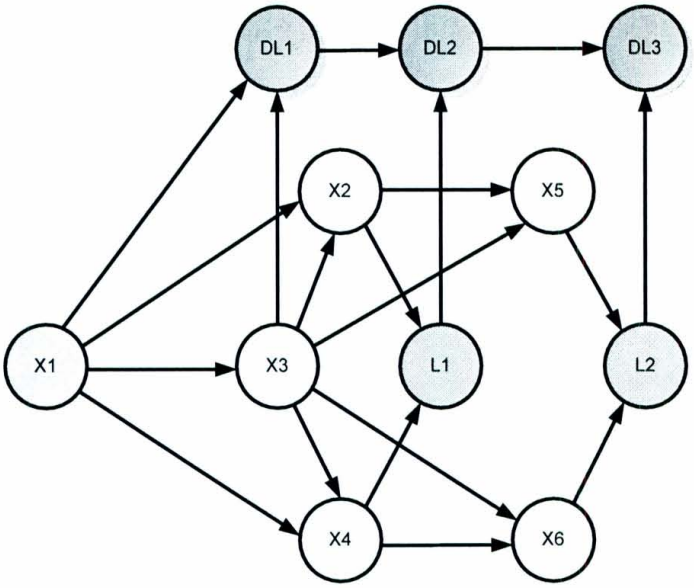


Figure 9.5. The complete BN for propagation pattern and occurrence probability estimation of the domino effect.

Table 9.3 shows the CPT which has to be assigned to DL_1 (and also DL_2) to model intersection dependencies. In the same way, according to Equation 9.9, if DL_3 is connected to nodes DL_2 and L_2 by AND-gate causal arcs, $P(DL_3)$ would be equal to the probability of the third-level domino effect.

Table 9.2. The AND-gate CPT of node DL_1.

		$P(DL_1 \mid X_1, X_3)$	
X_1	X_3	Accident	Safe
Accident	Accident	1	0
Accident	Safe	0	1
Safe	Accident	0	1
Safe	Safe	0	1

In addition to the domino effect probability, the probability of each event due to the domino effect can be calculated by marginalizing the joint probability distribution of the domino effect propagation network (i.e., Equation 9.5). For example, according to Figure 9.2, the probability of accident in X_3 caused exclusively by the domino effect is calculated as:

$$P(X_3) = \sum_{U \setminus X_3} P(U) = \sum_{X_1} P(X_1) P(X_3 \mid X_1) \qquad \textbf{9.10}$$

where $U \setminus X_3$ states that the marginalization should be implemented over all variables except X_3 (CCSP, 2000). Equation 9.10 can be used either to estimate the domino-driven probability of X_3 or to estimate the domino-affected probability of X_3. In the first case, it is assumed that there would be an accident in X_3 only if there is an accident in X_1, i.e., only because of the domino effect (domino-driven probability). In this way, the CPT of X_3 is such as that illustrated in Table 9.3, in which P_{13} is the escalation probability of X_3 given the primary event in X_1, i.e., $P_{13} = P(X_3|X_1)$.

Table 9.3. CPT of X_3 to estimate the domino-driven probability, where $P_{13} = P(X_3|X_1)$.

	X_3	
X_1	Accident	Safe
Accident	P_{13}	$1-P_{13}$
Safe	0	1

In the second case, however, it is supposed that there would be an accident probability for X_3 even if the domino effect does not occur, that is the primary probability of X_3. So,

given the domino effect, the probability of X_3 would increase (domino-affected probability). In this regard, one of the BN modeling techniques, known as the noisy-OR gate, can be used to incorporate the primary probability of X_3 as a leak probability in the analysis. Using the noisy-OR technique, if a child node is influenced by its parents independently of one another (disjunctive interaction), the total effect of all the parents on the child can be estimated as:

$$P(X \mid Pa(X)) = 1 - \prod_{i \in Pa(X)} (1 - P_i) \qquad \textbf{9.11}$$

in which P_i is the probability of X given that its i-th parent is true and the rest is false. Assuming the primary probability of X, P_{Leak}, as an independent parent, the probability of X, considering its parents and also its primary probability, would be as:

$$P(X \mid Pa(X)) = 1 - (1 - P_{Leak}) \prod_{i \in Pa(X)} (1 - P_i) \qquad \textbf{9.12}$$

In this regard, the CPT of X_3 is such as that illustrated in Table 9.4.

Table 9.4. CPT of X_3 to estimate the domino-affected probability. The primary probability of X_3 is considered as a leak probability.

	X_3	
X_1	Accident	Safe
Accident	$1-(1-P_{Leak})(1-P_{13})$	$(1-P_{Leak})(1-P_{13})$
Safe	P_{Leak}	$(1-P_{Leak})$

9.4.3 An example

For the sake of clarity, the application of the methodology developed in the previous sections is shown using a simple example. Figure 9.6 depicts a tank farm consisting of three atmospheric storage tanks (Step 1). The characteristics of the tanks are listed in Table 9.5.

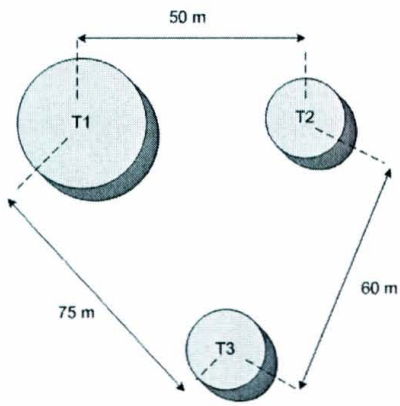


Figure 9.6. Case study for domino accident analysis.

Table 9.5. Vessel characteristic.

Vessel	Type	Substance	Content (t)	Accident scenario	Primary probability	Escalation vector
T_1	Atmospheric	Gasoline	500	Pool fire	1.0E-05	Heat radiation
T_2	Atmospheric	Xylene	200	Pool fire	1.0E-05	Heat radiation
T_3	Atmospheric	Gasoline	200	Pool fire	1.0E-05	Heat radiation

Because of the illustrative purpose, only one accident scenario (i.e., pool fire) and escalation vector (i.e., heat radiation) are assumed for the units. Since the primary

probabilities are identical for all three units, T_1 is selected as the primary unit (Step 2) because it can produce stronger escalation vectors (due to the larger inventory of hazardous substance). Also, the threshold value for radiation effect on atmospheric vessels is selected as $Q_{th} = 15\ kW/m^2$ (Cozzani et al., 2005).

To determine the possible secondary units, the intensity of heat radiation received by T_2 and T_3 in the case of a pool fire in T_1 is calculated as $Q_{12} = 19.3\ kW/m^2$ and $Q_{13} = 8.3\ kW/m^2$, respectively (Step 3). As can be seen, based on a comparison between the received heat intensity and the relevant threshold value (i.e., Q_{th}), T_2 is more likely to be the secondary unit impacted by T_1 (Step 4.1). Accordingly, in the corresponding BN, a causal arc is directed from node T_1 to node T_2 (Figure 9.7). To form the CPT of node T_2, the escalation probability of T_2 given the pool fire in T_1 is calculated using the probit functions proposed in [16] as $P(T_2|T_1) = 3.041E - 06$ (Steps 4.2 and 4.3).

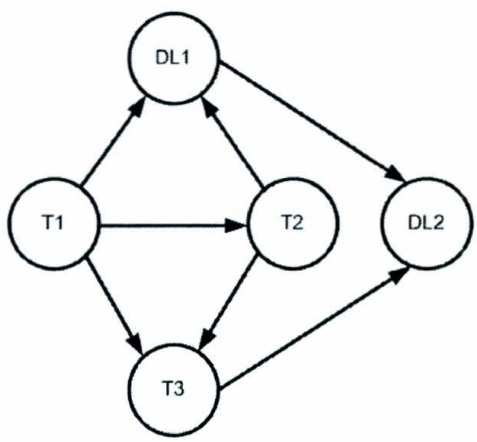


Figure 9.7. BN developed for the example in Figure 9.6.

As noted previously, based on a comparison between Q_{th} and Q_{13}, T_3 did not exceed the threshold criteria, thus it is not selected as a secondary unit. However, to examine the possibility of T_3 being impacted as a tertiary unit, the received radiation intensity by T_3 due to T_2 is calculated as Q_{23}= *9.3 kW/m*^{2}. Compared to Q_{th}, the pool fire in T_2 does not produce sufficiently intense heat radiation to impact T_3. Nevertheless, considering the synergistic effect of T_1 and T_2, it can be seen that the total heat radiation received by T_3 due to both T_1 and T_2 would be sufficiently above the threshold value to damage T_3 (i.e., $Q_{13} + Q_{23} = 17.6\ kW/m^2$). So, T_3 is a tertiary unit involved in the domino accident, enabling the domino effect to proceed to the second level (Step 6). Accordingly, since T_3 is influenced by T_1 and T_2 together, it is connected to both of these nodes in the corresponding BN in Figure 9.7. Again, in order to populate the CPT of node T_3, its escalation probability given the pool fires in T_1 and T_2 is calculated using the probit method as $P(T_3|T_1, T_2) = 1.197E - 06$.

It should be noted that Step 4.4 was skipped since the only available potential secondary unit is T_2. So, there would be no need to make a comparison among competitive potential units to select the secondary unit. Step 5 has also been neglected in this example as the primary and secondary accidents of all units are determined in Table 9.5. To estimate the probability of the domino effect at different levels, nodes DL_1 and DL_2 are added to the network. It should be noted that since there is only one secondary and one tertiary event, auxiliary nodes to model the union of the same order units need not to be added to the network. To account for the first-level domino effect, DL_1 is connected to the primary unit T_1 and the secondary unit T_2 such that $P(DL_1) = P(T_1)P(T_2|T_1)$. Similarly, to

consider the second-level domino effect, DL_2 is connected to the first-level domino effect node DL_1 and the tertiary unit T_3 such that $P(DL_2) = P(DL_1)P(T_3)$ After the BN is modeled using the HUGIN software tool (2010), the probability values *3.04E-11* and *3.64E-17* are obtained for the first and the second-level domino effects, respectively. So, as opposed to the probabilities listed in Table 9.5, the occurrence of domino effects seems unlikely, particularly the second-level domino effect.

9.5 Application

9.5.1 Case-study

To apply the current methodology to domino effects including a wider range of accident scenarios than in the example previously discussed (Section 9.4.3), a case-study from (Cozzani and Salzano, 2004) is adapted and modeled in this section. Figure 9.8 illustrates the schematic of a tank farm comprised of 8 atmospheric storage tanks with fixed roofs (D_1-D_8). The tanks contain gasoline with the capacity of 2000 metric tons, each. Table 9.6 shows the distances among the storage tanks.

To consider the influence of different accident scenarios on the domino effect modeling, it is assumed that either a pool fire or VCE can be envisaged as the likely accident scenario for a damaged storage tank. In this regard, the primary probability values assumed for pool fire and VCE are *1E-05* and *2E-06*, respectively. However, after a storage tank is impacted through the domino effect, its likelihood to develop a pool fire or VCE is assumed to be equal, i.e., 0.5.

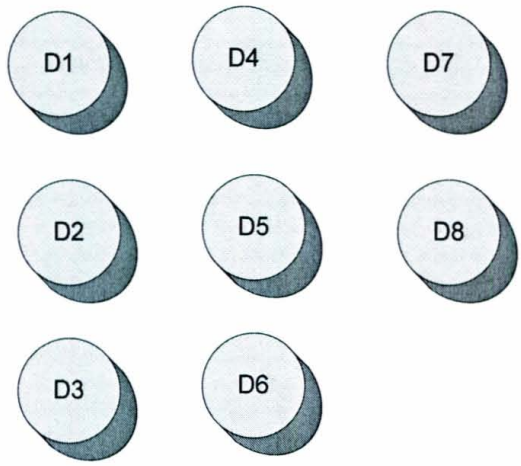


Figure 9.8. Schematic of storage tanks in a tank farm.

Table 9.6. Distances (m) among the units in the tank farm layout in Figure 9.8.

	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
D_1	-	50	100	50	71	112	100	112
D_2	50	-	50	71	50	71	112	100
D_3	100	50	-	112	71	50	142	112
D_4	50	71	112	-	50	100	50	71
D_5	71	50	71	50	-	50	71	50
D_6	112	71	50	100	50	-	112	71
D_7	100	112	142	50	71	112	-	50
D_8	112	100	112	71	50	71	50	-

To commence modeling, the following assumptions are made:

The storage tank D_1 is determined as the primary unit, from which the domino effect modeling starts.

The events of the same order, e.g., secondary events, take place simultaneously. Therefore, it is not possible for them to impact one another. In other words, in the corresponding BN, there is no causal arc between units of the same order.

Unlike pool fire accidents which may last for several hours or even days (based on the amount of fuel and the burning rate), the shock waves resulting from explosions (responsible for overpressure damages) lasts for at most several seconds (Khan and Abbassi, 1999). To consider the synergistic effect of overpressure, the assumption of the concurrence of events of the same order is inevitable.

The threshold values of heat radiation and overpressure are selected as $Q_{th} = 15\ kW/m^2$ and $\Delta P_{th} = 7\ kPa$ for atmospheric storage tanks with fixed roofs.

In order to specify the propagation pattern and escalation probabilities, the overpressure (Cozzani and Salzano, 2004) and heat radiation escalation vectors are calculated and illustrated in Tables 9.7 and 9.8, respectively.

Table 9.7. Overpressure escalation vectors (kPa) (Cozzani and Salzano, 2004).

	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
D_1	-	10	4	10	8	4	4	4
D_2	10	-	10	8	10	8	4	4
D_3	4	10	-	4	8	10	2	4
D_4	10	8	4	-	10	4	10	8
D_5	8	10	8	10	-	10	8	10
D_6	4	8	10	4	10	-	4	8
D_7	4	4	2	10	8	4	-	10
D_8	4	4	4	8	10	8	10	-

Table 9.8. Heat radiation escalation vectors (kW/m^2).

	D_1	D_2	D_3	D_4	D_5	D_6	D_7	D_8
D_1	-	19.3	4.6	19.3	9.3	3.6	4.6	3.6
D_2	19.3	-	19.3	9.3	19.3	9.3	3.6	4.6
D_3	4.6	19.3	-	3.6	9.3	19.3	2.2	3.6
D_4	19.3	9.3	3.6	-	19.3	4.6	19.3	9.3
D_5	9.3	19.3	9.3	19.3	-	19.3	9.3	19.3
D_6	3.6	9.3	19.3	4.6	19.3	-	3.6	9.3
D_7	4.6	3.6	2.2	19.3	9.3	3.6	-	19.3
D_8	3.6	4.6	3.6	9.3	19.3	9.3	19.3	-

9.5.2 Results and discussion

Because the likely accident scenarios for D_1 are pool fire and VCE, D_1 can impact nearby units by means of either heat radiation or overpressure. Based on a comparison among the threshold values and the escalation vectors in Tables 9.7 and 9.8, D_1 can impact D_2 and D_4 by either heat radiation or overpressure while it affects D_5 only by overpressure. Thus, D_2 and D_4 are selected as the secondary units due to their higher escalation probabilities, which in turn can result in pool fire or VCE (with equal probabilities). In this regard, causal arcs are directed from D_1 to the aforementioned nodes in the corresponding BN in Figure 9.9.

Similarly, the secondary units are likely to trigger other accidents in the tertiary or quaternary units. In this case study, regardless of the type of accidents in D_2 and D_4, units D_3, D_5 and D_7 can be involved in the domino effect as tertiary units.

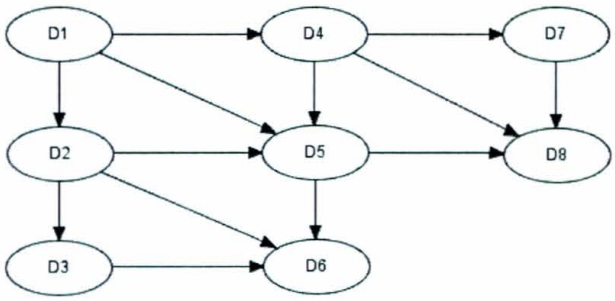


Figure 9.9. Propagation pattern of the domino effect in the tank farm.

It is worth noting that among the tertiary units; only D_5 is impacted by the synergistic effect of the primary and the secondary units. Likewise, units D_6 and D_8 are impacted as quaternary units in the domino effect. Drawing causal arcs from the parent units to the associated children units, the likely propagation pattern of the domino effect in the tank farm would be as shown in Figure 9.9.

To calculate the probability of the domino effect, the escalation probabilities of units D_2 to D_8 for every state combination of their parents are calculated using the probit models suggested in Cozzani et al. (2005), considering synergistic effect and noisy gates. For example, the escalation probability of D_5 given VCE in D_1, PF in D_2 and also VCE in D_4, i.e., $P(D_5|D_1 = VCE, D_2 = PF, D_4 = VCE)$, can be calculated using the noisy-OR gate probability as follows:

If $P(D_5|D_1 = VCE) = 0.0211$, $P(D_5|D_2 = PF) = 5.43E - 06$ and $P(D_5|D_4 = VCE) = 0.0685$, then $P(D_5|D_1 = VCE, D_2 = PF, D_4 = VCE) = 1 - (1 - 0.0211)(1 - 5.43E - 0 - 6)(1 - 0.0685)$, of which there is a 50% probability to have either a pool fire (PF) or VCE, i.e., $4.408E - 02$.

To calculate the domino effect probabilities, nodes L_1, L_2, L_3, DL_1, DL_2, and DL_3 are added to the BN (Figure 9.10). After the CPTs are assigned to the nodes, the BN is analyzed using HUGIN software. The accident probabilities and the probability of the domino effect at sequential levels are listed in Table 9.9 (columns 2 and 3). It should be remarked that in Table 9.9 that the values listed for DL_0, DL_1, DL_2 and DL_3 include both the probabilities of PF and VCE. It should be noted that the probability of the zero-level domino effect, $P(DL_0)$, equals the probability of the primary event, $P(D_1)$.

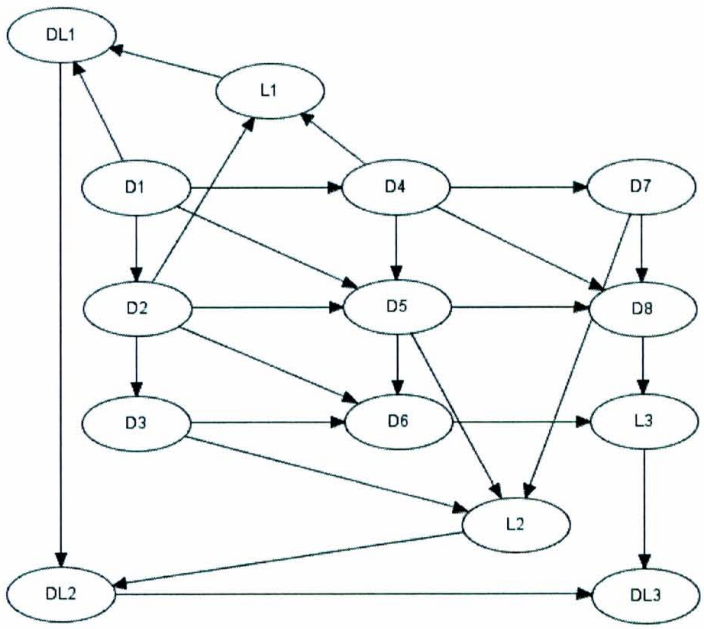


Figure 9.10. BN to model domino effect in the tank farm.

Table 9.9. Domino effect probabilities.

	First modeling				Second modeling			
	Priors		Posteriors given D_6 = PF		Priors		Posteriors given D_6 = PF	
Unit	PF	VCE	PF	VCE	PF	VCE	PF	VCE
D_1	1.00E-05	2.00E-06	2.00E-04	9.99E-01	1.00E-05	2.00E-06	2.00E-04	9.99E-01
D_2	6.86E-08	6.86E-08	1.60E-02	5.51E-01	6.86E-08	6.86E-08	1.57E-02	5.60E-01
D_3	2.35E-09	2.35E-09	1.68E-02	7.80E-02	2.71E-09	2.71E-09	4.62E-02	4.62E-02
D_4	6.86E-08	6.86E-08	3.23E-02	9.04E-02	6.86E-08	6.86E-08	3.43E-02	3.43E-02
D_5	2.62E-08	2.62E-08	2.46E-02	5.59E-01	2.11E-08	2.11E-08	4.90E-03	5.49E-01
D_6	1.72E-09	1.72E-09	1.00E+00	0.00E+00	1.59E-09	1.59E-09	1.00E+00	0.00E+00
D_7	2.35E-09	2.35E-09	3.10E-03	3.10E-03	2.71E-09	2.71E-09	1.06E-02	1.06E-02
D_8	1.72E-09	1.72E-09	2.07E-02	2.07E-02	1.59E-09	1.59E-09	2.28E-02	2.28E-02
DL_0*	1.20E-05		1.00E+00		1.20E-05		1.00E+00	
DL_1	2.65E-07		6.36E-01		3.02E-07		1.00E+00	
DL_2	2.42E-08		2.87E-01		1.63E-08		1.00E+00	
DL_3	1.92E-09		2.87E-01		-		-	

***The probability of the zero-level domino effect, $P(DL_0)$, equals the sum of the probability of the different accident scenarios (PF and VCE) of the primary event, i.e., $P(D_1 = PF) + P(D_1 = VCE)$.**

According to the prior probabilities in columns 2 and 3 of Table 9.9, among the tertiary events, i.e., D_3, D_5 and D_7, the probability of D_5 is an order of magnitude higher than the others. This is because of the fact that, unlike D_3 and D_7 which are impacted only by the secondary units, D_5 benefits from the escalation vectors of both the primary unit D_1 and the secondary units. Its escalation probability is therefore expected to be higher as opposed to that of D_3 and D_7.

On the other hand, the escalation probabilities of the quaternary units D_6 and D_8 are of the same order. The reason is that all these units are likely to be triggered by either heat

radiation or overpressure emitted by the tertiary units, exposing them to almost the same level of vulnerability.

Comparing the domino effect probabilities at different levels, it is also noted that except for $P(DL_0)$ and $P(DL_1)$ which differ in amount by two orders of magnitude, the difference between sequential domino levels is one order of magnitude. This implies that even though the probability of the first-level domino effect given the primary event is not very high, its propagation from the first-level to the second-level and from the second-level to the third-level is significant and cannot be neglected. Consequently, in the allocation of safety measures, multi-level domino effects should be taken into consideration.

As previously mentioned, the BN takes new information into account to update the prior probabilities (see Equation 9.4). This way, the posterior probability of events given an item of evidence (e.g., the knowledge about the state of a node) and also the most probable configuration of events leading to the evidence, are often of significant importance.

To perform probability updating in this case-study, the updated probabilities of events (posteriors) are calculated given that a pool fire has been observed in D_6, i.e., $P(D_i|D_6 = PF)$ in which $i \neq 6$. The posteriors are listed in Table 9.9 (columns 4 and 5). Also, the most probable configuration of events leading to the pool fire in D_6 is determined as $(D_1 = VCE) \rightarrow (D_5 = VCE) \rightarrow (D_6 = PF)$ whereas the other units are in the safe state.

Considering the most probable configuration, it can be seen that the domino effect has proceeded to the second level, escalating D_5, without passing through the first level, resulting in no escalation of D_2 or D_4. This is also evident from the posterior probabilities of the sequential levels of the domino effect (the last four numbers in column 3 of Table 9.9); despite the observation of a pool fire in D_6 which implies that the domino effect must be in its third level (i.e., $P(DL_3) = 1.0$), the probability of the third-level domino effect is noticeably below 1.0, i.e., $P(DL_3) = 2.871E - 01$. Furthermore, being in the third level necessitates the domino effect having already passed the first and second levels, i.e., $P(DL_1) = P(DL_2) = 1.0$. However, according to Table 9.9, these values also differ from what is expected.

As mentioned previously, the primary unit, D_1, is capable of impacting D_5 by means of overpressure even if D_2 or D_4 does not contribute through the synergistic effect. This fact and also the abovementioned most probable configuration of events, where D_5 occurs after D_1, increase the possibility of D_5 being involved in the domino effect as a secondary unit. Accordingly, shifting D_5 to the set of secondary events, the updated propagation pattern of the domino effect would be as shown in Figure 9.11.

In this way, D_2, D_4 and D_5 are involved in the domino effect as secondary events while D_3, D_6, D_7 and D_8 contribute to the domino effect as tertiary events. Modeling the modified network in HUGIN, the new prior probabilities shown in Table 9.9 (columns 5 and 6) are obtained.

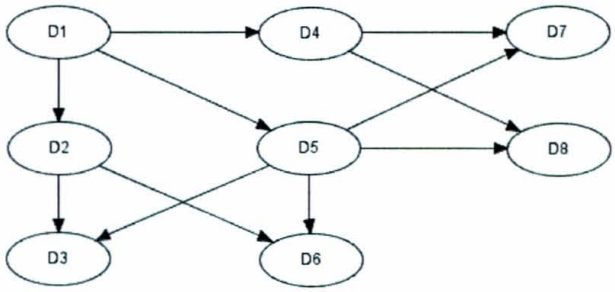


Figure 9.11. Modified propagation pattern of the domino effect.

It also should be noted that by adding D_5 to the secondary events, the highest level of the domino effect is reduced in the second level. Using the posterior probabilities to verify the modified network, the most probable configuration of the events causing the pool fire in D_6 is determined as $(D_1 = VCE) \rightarrow (D_2 = VCE) \rightarrow (D_6 = PF)$, showing that a logical sequence of events of different orders has been fulfilled. The posterior probabilities of the modified network given the pool fire in D_6 are also displayed in columns 7 and 8 of Table 9.9. It is worth noting that the posterior probabilities of the sequential levels of the domino effect equal unity.

9.6 Conclusion

The present study has introduced a new methodology for probabilistic analysis of domino effects in chemical process plants based on BNs. The likely propagation pattern of domino effect starting from a primary event was developed in the form of a BN. The BN was then further modified to account for the probability of the domino effect at subsequent levels. To take the complex interactions among adjacent equipment into

account, the conditional probability tables assigned to events were populated considering synergistic effects and noisy probabilities.

The application of the methodology to a real case-study showed that the BN is effectively suitable for the analysis of domino effects from both qualitative and quantitative points of view. From a qualitative perspective, the flexible structure of BN makes it possible to fit to a wide range of accident scenarios and also to embed versatile types of information in the network by adding auxiliary nodes. The graphical representation of units and escalation vectors by means of nodes and causal arcs through BN remarkably helps to visualize the propagation pattern of the domino effect, which is not easy with most deterministic and probabilistic methods.

From a quantitative point of view, BN takes advantage of robust CPTs to model different types of causal relationships among events. CPTs help in considering the synergistic effect of contributing events by either adding similar escalation vectors or using noisy probabilities in the case of different escalation vectors. Considering the complex interaction and conditional dependencies among the units involved in the domino effect, several limiting assumptions such as independent events or random or binomial selection of target units can be relaxed.

More importantly, using new observations as evidence, BN employs Bayes' theorem to update the prior probabilities. Consequently, the posterior probabilities are obtained in the light of new observations and also the most probable configuration of events leading to that observation can be determined. Considering posterior probabilities as well as the most probable configuration, the most likely propagation path of the domino effect can be

identified. The present study showed that using the new information, not only the quantitative part but also the qualitative part of the domino model can be updated.

Acknowledgment

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

9.7 References

Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi S.A. Domino effect in process industry accidents- an inventory of past events and identification of some patterns. Journal of Loss Prevention in the Process Industries 2011; 24: 575-593.

Antonioni G, Spadoni G, Cozzani V. Application of domino effect quantitative risk assessment to an extended industrial area. J Loss Prevention in Process Industries 2009; 614-624.

Abdolhamidzadeh B, Abbasi T, Rashtchian D, Abbasi S.A. A new method for assessing domino effect in chemical process industry. Journal of Hazardous Materials 2010; 182: 416-426.

Assael MJ, Kakosimos KE. Fires, Explosions, and Toxic Gas Dispersions: Effects Calculation and Risk Analysis. CRC Press, Taylor and Francis Group, NW, 2010.

Bagster D.F, Pitblado R.M. The estimation of domino incident frequencies-an approach. Process Safety and Environmental Protection 1991; 69: 195-199.

Bobbio A, Portinale L, Minichino M, & Ciancamerla E. (2001). Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Journal of Reliability Engineering and System Safety 2001; 71: 249-260.

Bearfield G, Marsh W. Generalizing event trees using Bayesian networks with a case study of train derailment. Lecture Notes in Computer Science 2005; 3688: 52-66.

Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances. Official Journal of the European Communities, L 10/13 , Brussels, 14.1.97.

Cozzani V, Salzano E. The quantitative assessment of domino effects caused by overpressure part I. Probit models. Journal of Hazardous Materials 2004; A107: 67-80.

CSB. Refinery explosion and fire, 2007. Investigation report No. 2005-04-I-TX. http://www.csb.gov/assets/document/CSBFinalReportBP.pdf. (Last checked on 18.1.2012).

Cozzani, G. Gubinelli, E. Salzano. Escalation thresholds in the assessment of domino accidental events. Journal of Hazardous Materials 129:1-21 (2006)

Cozzani V, Gubinelli G, Antonioni G, Spadoni G, Zanelli S. The assessment of risk caused by domino effect in quantitative area risk analysis. Journal of Hazard. Material 2005; 14-30.

Cozzani, G. Antonioni, G. Spadoni. Quantitative assessment of domino scenarios by a GIS-based software tool. Journal of Loss Prevention in the Process Industry 19:463-477 (2006)

CCPS, Guidelines for chemical process quantitative risk analysis, second edition, AIChE, New York 2000.

Cozzani V, Salzano E. The quantitative assessment of domino effects caused by overpressure part II. Case studies. Journal of Hazardous Materials 2004; A107: 81-94.

Darbra, R. M., Palacios, A., Casal, J. Domino effect in chemical accidents: main features and accident sequences. Journal of Hazardous Materials 183 (2010) 565-573.

Eisenberg N.A, Lynch C.J, Breeding R.J. Vulnerability model: a simulation system for assessing damage resulting from marine spills, Report CG-D-136-75, Enviro Control Inc., Rockville, MD, 1975.

Gledhill J, Lines I. Development of methods to assess the significance of domino effects from major hazard sites, CR Report 183, Health and Safety Executive, 1998.

HUGIN Expert Software version 7.4 (2010). (http//www.hugin.com).

Jensen FV, Nielsen TD. Bayesian Networks and Decision Graphs, 2nd edition. New York: Springer; 2007.

Khakzad N, Khan F, Amyotte P. Safety analysis in process facilities: comparison of fault tree and Bayesian network approaches. Reliability Engineering and System Safety 2011; 96: 925-32.

Khan F, Abbasi S.A. Assessment of risks posed by chemical industries-application of a new computer automated tool MAXCRED III. Journal of Loss Prevention in the Process Industries 1999; 12: 455-469.

Khan F, Abbasi S.A. Models for domino analysis in chemical process industries. Process Safety Progress 1998; 17: 107-123.

Khan F, Abbasi S.A. DOMIFFECT (DOMIno eFFECT): user-friendly software for domino effect analysis. Environmental Modeling and Software 1998; 13: 163-177.

Kourniotis S.P, Kiranoudis C.D, Markatos N.C. Statistical analysis of domino chemical accidents. Journal of Hazardous Materials 2000; 71: 239-252.

Khakzad N, Khan F, Amyotte P. Dynamic Safety Analysis of Process Systems by Mapping Bow-tie into Bayesian Network. Process Safety and Environmental Protection 2012. doi: 10.1016/j.psep.2012.01.005.

Landucci, G. Gubinelli, G. Antonioni, V. Cozzani. The assessment of the damage probability of storage tanks in domino events. Accident Analysis and Prevention 41:1206-1215 (2009).

Nguyen Q.B, Mebarki A, Ami Saada R, Reimeringer M. Integrated probabilistic framework for domino effect and risk analysis. Journal of Advances in Engineering Software 2009; 40: 892-901.

Reniers, G.L.L., Dullaert, W., Ale, B.J.M., & Soudan, K., (2005). The use of current risk analysis tools evaluated towards preventing external domino accidents. J. Loss Prev.Proc. Industries, 18,119

Reniers, G.L.L., Dullaert W., (2007). DomPrevPlanning: User-friendly software for planning domino effects prevention. Safety Science, 45(10), 1060.

Rai K, Van Ryzin J. A generalized multihit dose-response model for low-dose extrapolation. Biometrics 1981; 37: 341-352.

Torres-Toledano JG, Sucar LE. Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science 1998; 1484: 195-206.

Vilchez A.J, Montiel H, Casal J. Arnaldos J. Analytical expressions for the calculation of damage percentage using the probit methodology. Journal of Loss Prevention in the Process Industries 2001; 14: 193-197.

Vilchez A.J, Sevilla S, Montiel H, Casal J. Historical analysis of accidents in chemical plants and in the transportation of hazardous materials. Journal of Loss Prevention in Process Industries 1995; 8: 87-96.

Van Den Bosh CJH, Weterings RAMP. Methods for the calculation of physical effects (Yellow Book), Committee for the Prevention of Disasters, the Hague (NL), 1997.

Weber P, Medina-Oliva G, Simon C, Iung B. Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas. Engineering Application of Artificial Intelligence 2010; doi: 10.1016/j.engappai.2010.06.002.

10 Summary, Conclusions, and Recommendations

10.1 Summary

The present study has illustrated the use of Bow-tie and Bayesian network in dynamic risk assessment and safety analysis of process systems. It has focused on innovative applications of both methods to consider the complex behavior of interlinked and dynamic systems, and also extended the modeling power of these techniques by introducing new algorithms and formulas.

From an application point of view, the aforementioned methods have effectively been applied to model a wide range of complex accident scenarios from process systems to offshore drilling operations and to risk-based design of process equipment to domino effect accidents. From a model development perspective, several innovations such as application of physical reliability models in dynamic risk analysis, developing an algorithm to map Bow-tie into Bayesian network, introduction of new relationships for dynamic gates as well as a novel methodology , neutral dependency, to enhance the performance of dynamic Bayesian networks have been represented.

Bow-tie has been used to represent a transparent logical connection among the accident scenario components. It is of great importance among the experts due to being tractable and communicable. However, it suffers limitations such as being static and incapable of capturing conditional dependencies and common cause failures. These limitations may be relaxed through application of Bayesian approaches or physical models, or mapping bow-tie into Bayesian network.

Bayesian network, on the other hand, take advantage of its flexible structure and robust reasoning engine to model a wide variety of accident scenarios. Aside from its capability to consider multi-state variables, common cause failures, conditional dependencies, and expert judgment, Bayesian network is able to perform probability updating, a task that is difficult to do with Bow-tie. Owing to the foregoing features, Bayesian network was given priority over bow-tie. One of the main issues identified in Bayesian network application is the population of conditional probability tables.

10.2 Conclusions

The main conclusions of this study are:

10.2.1 Mapping fault tree into Bayesian network

This study showed that each fault tree can be mapped into a corresponding Bayesian network; however, a Bayesian network does not necessarily have an equivalent fault tree. Although conditional probability tables of such a Bayesian network are deterministically populated based on the fault tree AND/OR gates, this Bayesian network is still a much effective technique than its respective fault tree. It is because Bayesian network is able to model multi-state components, sequentially dependent failures, and more importantly to conduct probability updating in the light of new observations.

Bayesian network takes new observations into account to reduce the uncertainty arising from historical data and expert judgment in the form of prior probabilities, making the probabilities more case-specific in the form of posterior probabilities as new information

becomes available. It is also illustrated that, compared to minimal cut-set concept in fault trees, Bayesian network produces a more effective definition in form of the most probable configuration of primary events leading to the top event (accident).

10.2.2 Mapping bow-tie into Bayesian network

This study introduced a mapping algorithm from bow-tie approach into a corresponding Bayesian network, relaxing its limitations. As a result, the conditional dependencies among all components of bow-tie can be modeled. Although a bow-tie can consider the conditional dependencies among its safety barriers, it is not capable of modeling such dependencies among the primary causes of the accident and the safety barriers. In addition, as a bow-tie is composed of a fault tree and an event tree, it carries the limitations of the both techniques.

Mapping a bow-tie into a corresponding Bayesian network solve the above-mentioned problem, and also provides the analyst with effective features of Bayesian network for conducting probability updating and sequential learning (probability adapting). In contrast to probability updating in which knowledge about a node's state is used to update other probabilities, in sequential learning, the cumulative information of a system which has been observed and recorded over time is taken into account for probability updating (adapting). Probability adapting is more effective than probability updating in dynamic safety analysis although it has not been considered in process safety analysis.

10.2.3 Application of Object-oriented Bayesian network in complex systems

Mapping a bow-tie into its corresponding Bayesian network provides the analyst with outstanding modeling merits such as probability updating and considering conditional dependent failures. However, like bow-tie approach, the standard Bayesian network of a complex and interlinked system such as well control risk analysis can potentially result in an intractable and complicated network of nodes and arcs.

Object-oriented Bayesian networks, on the other hand, make it possible to model such a complex system with several levels of abstraction. Regarding object-oriented Bayesian network technique, the system of interest can be divided to sub-models for each of which a detailed Bayesian network can be developed. These individual Bayesian networks are then combined using interface nodes, significantly facilitating the interpretation of the model and better illustrating dependencies among the model segments.

10.2.4 Application of physical reliability models in dynamic risk analysis

To enable the application of conventional risk analysis techniques in dynamic risk analysis, Bayes' theorem has long been used to update the probabilities in the light of new information. This study proposed physical reliability models as an alternative to directly incorporate the effect of changing environment in risk analysis.

Using physical reliability models, varying operational parameters such as dimension, temperature and pressure, contributing to the risk of an accident scenario are directly taken into account to revise the probability of the accident. This, in turn, leads to revised

risk estimation as the system's operational parameters change dynamically. Physical reliability models demand a number of experimental, site-specific inventories of data to be developed through regression methods.

10.2.5 Application of dynamic Bayesian networks in risk-based design

In the risk-based design of process systems, the focus is on the augmentation of the layers of protection, i.e., by contemplating extra safety measures to mitigate the consequences of an undesired event. Accordingly, risk analysis is repeated for the system under study in the presence of different layers of safety barriers, not necessarily leading to the most cost-effective design.

This study illustrated that dynamic Bayesian networks can potentially be applied as an effective tool for risk-based design of process systems. Using dynamic Bayesian network, not only different combination of safety measures but their sequential failure can be accounted for to identify the best spatial and temporal arrangement of safety measures. Compared to other time-including methods such as Markov chains, dynamic Bayesian networks are relatively simpler to construct and avoid the notorious issue of state-space explosion. In addition, dynamic Bayesian networks make it possible to revise the system design through probability updating given that an accident has occurred.

10.2.6 Improving the performance of discrete-time Bayesian networks

Discrete-time Bayesian networks model dependable systems using dynamic gates such as cold spare gate, sequentially enforcing gate and priority AND gate. The conventional forms of the foregoing dynamic gates have drawbacks such as not easily being applicable to non-exponential distribution functions or resulting in intractably huge conditional probability tables.

The present study improved the power of discrete-time Bayesian networks by modifying the conventional forms of cold spare gate and sequentially enforcing gate such that for most probability distribution functions, closed-form analytical solutions can be obtained without resort to numerical integration methods or simplifying assumptions.

Further, to improve the performance of conventional priority AND gates which, in the simplest case, lead to huge conditional probability tables of size $(n+1)^3$, a new algorithm, neutral dependency, was introduced. Using this algorithm, the conditional probability table of a gate is decomposed into two tables, both of which are smaller in size than the original table (usually by an order of magnitude). This way, the problem of large and intractable multi-dimensional tables for which discrete-time Bayesian networks have been criticized is addressed.

10.2.7 Application of Bayesian networks in domino effect modeling

The present study has introduced a new methodology based on Bayesian networks for probabilistic analysis of domino effects in chemical process plants. Instead of relying on

oversimplified assumptions such as considering independent events or random target units, the likely propagation pattern of domino effect was developed in the form of a Bayesian network, reflecting the underlying mechanisms of domino effects.

The graphical representation of units and escalation vectors by means of nodes and causal arcs through Bayesian network remarkably helps to visualize the propagation pattern of the domino effect, which cannot easy be modeled with most deterministic and probabilistic methods. In addition, Bayesian networks take advantage of conditional probability tables to model the highly complex interaction of units in a domino effect considering synergistic effects and using noisy probabilities. Performing probability updating given an accident in a unit, posterior probabilities of other units as well as the most probable configuration of units leading to that accident can be identified.

10.3 Recommendations

The present work attempts to introduce new concepts and also overcome the limitations of existing techniques in the field of dynamic risk analysis and safety assessment of process industries as well as Oil and Gas industries. This study, however, can be extended further as suggested below:

10.3.1 Non-conjugate probability distributions

This study has shown the role of Bayes' theorem in probability updating of components of a bow-tie. However, probability distributions used for priors and likelihood functions were chosen from conjugate families, e.g., Poisson-Gamma or Beta-Binomial

distributions. These conjugate pairs were selected due to resulting in closed-form standard posteriors and avoiding numerical methods. However, with advent of advanced approaches for Markov Chain Monte Carlo sampling and availability of open source software such as WinBUGS and OpenBUGS, a wide variety of probability distribution can be used for probability updating. Therefore, it seems no longer necessary to restrict the modeling to conjugate family distributions for the sake of mathematical convenience in future work.

10.3.2 Data requirement

Most of proposed approaches in this study demand high amount of quality data which are often difficult to obtain. For example, although physical reliability models illustrate an efficient approach for real-time revising of probabilities, they need a large inventory of experimental as well as test data to be developed using regression methods.

Likewise, although it was shown that probabilistic populating of conditional probability tables using noisy gates remarkably augments the reasoning strength of Bayesian networks, these noisy gates cannot be developed unless individual influence of each parent node on a child node is identified. This in turn demands a considerable amount of cause-effect data not easily available.

According to these data-intensive approaches, data gathering from other similar case studies, applications and also expert opinions with different levels of expertise seems inevitable. Hierarchical Bayesian methods are an efficient tool to handle these multi-source data which can be considered in future studies.

10.3.3 Uncertainty handling

Since this study was aimed at introducing new methodologies in safety management and risk-based decision making, the focus was on methods rather than numbers. However, both epistemic and aleatory uncertainty contents resulting from our incomplete state of knowledge in modeling of accidents and stochastic nature of accidents themselves, respectively, need to be introduced and handled in the proposed methods. Monte Carlo Bayesian networks, fuzzy Bayesian networks, and hierarchical Bayesian approaches can be applied to either handle or reduce uncertainties arisen from data variability and hidden in point estimates.

10.3.4 Lack of availability of commercial tools

This study illustrated that bow-tie approach and Bayesian network can be effectively applied in the context of dynamic quantitative risk assessment and safety analysis. Although there is a lot of software available to perform aforementioned methods particularly Bayesian analysis, there is not such tool available to conduct dynamic risk analysis. There is need to develop a tool for dynamic risk analysis.