Reliability Engineering and System Safety 96 (2011) 925–932

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Safety analysis in process facilities: Comparison of fault tree and Bayesian network approaches

Nima Khakzad [a], Faisal Khan [a,*], Paul Amyotte [b]

[a] Process Engineering, Faculty of Engineering & Applied Science, Memorial University, St. John's, NL, Canada A1B 3X5
[b] Department of Process Engineering & Applied Science, Dalhousie University, Halifax, NS, Canada B3J 2X4

ARTICLE INFO

Article history:
Received 24 July 2010
Received in revised form
4 March 2011
Accepted 15 March 2011
Available online 23 March 2011

Keywords:
Bayesian network
Fault tree analysis
Accident analysis
Uncertainty modeling

ABSTRACT

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 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, updating probabilities, and coping with uncertainties. The objective of this paper is to demonstrate the application of BNs in safety analysis of process systems. The first part of the paper shows those modeling aspects that 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 safety analysis because of its flexible structure, allowing it to fit a wide variety of accident scenarios.

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 [1,2].

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 [3]. According to the final report issued by BP [4], 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 [5]. 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 [6]. 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 [7] 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. [8] 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 [1,9,10] and fault diagnosis [11–13]. 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 [2,14,15].

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

* Corresponding author.
E-mail address: fikhan@mun.ca (F. Khan).

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.03.012

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 [16].

BNs are increasingly used in reliability assessment [2,16–18], fault diagnosis [19,20], and updating the failure probability of safety systems [21,22] 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. [14] 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 [15,23,24] or mapping dynamic FTs into the corresponding dynamic BNs [22,25,26].

Many authors have investigated different techniques in accident scenario analysis, very few of whom have used BNs in their work. Sklet [27] 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. [28] 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 [29] 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. [30] 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 2. The comparison of the two methods is done in Section 3, where a simple accident scenario is modeled using both methods. Section 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 5.

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.

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 [31]. 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 an 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 [9,32–34].

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 [2].

BN takes advantage of the "*d-separation*" criterion (Jensen and Nielsen, 2007) 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 [14].

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

$$P(U)=\prod_{i=1}^{n} P(A_i|Pa(A_i)) \tag{1}$$

where $Pa(A_i)$ are the parents of A_i in the BN, and $P(U)$ reflects the properties of the BN [35].

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:

$$P(U|E)=\frac{P(U,E)}{P(E)}=\frac{P(U,E)}{\sum_U P(U,E)} \tag{2}$$

Eq. (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 [19].

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 conditional probability table (CPT) is developed. The CPTs are developed according to the type of gate [14,24]. Fig. 1 illustrates the simplified procedure of mapping FTs into BNs.

3. Safety analysis

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 1, while intermediate events and the top event have been identified by the type of gate leading to these events.

3.2. Fault tree analysis

Considering the behavior of the components and the intermediate events, the FT is constructed as shown in Fig. 2. Occurrence probabilities presented in Table 1 are then assigned to each primary event. Considering the probabilities, the prior probability of the top event is calculated as 0.2720.

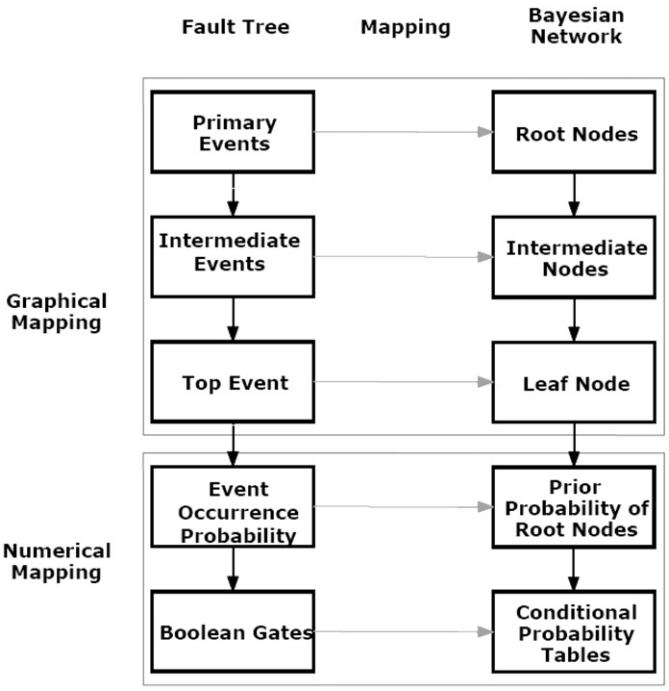


Fig. 1. Mapping FT to BN.

Table 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*

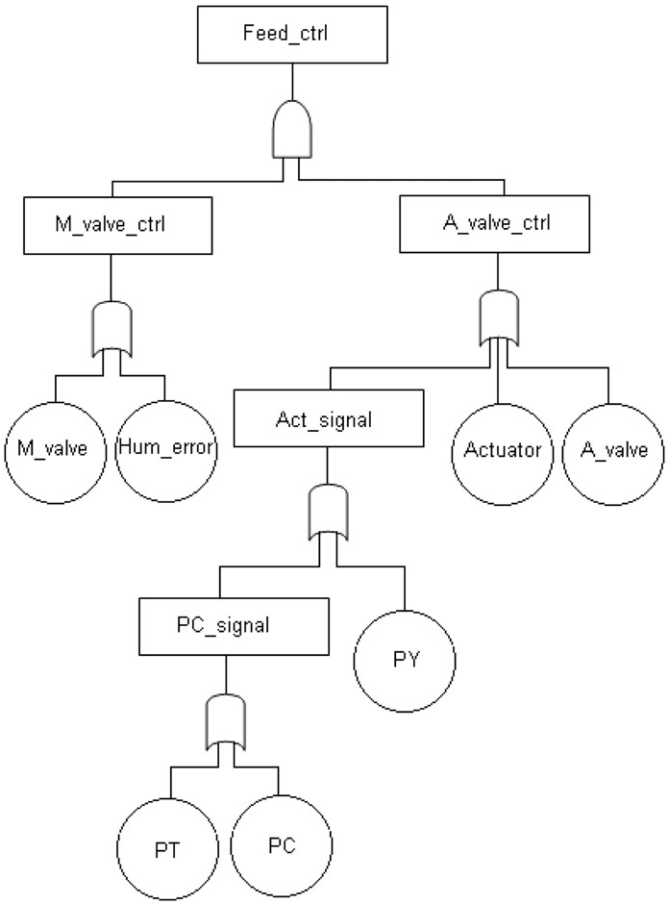


Fig. 2. FT for the malfunction of feed system.

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 [31]. 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*" [1] that signifies the percent contribution of that event in leading to the top event (Table 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 2, events C_9, C_{10}, C_6, and C_2 have the highest improvement indices (components are numbered

Table 2
Top event probability and improvement indices for FT and BN analysis.

Event not occurring	Fault tree analysis		Bayesian network analysis	
	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

according to Table 1). Therefore, in order to improve the safety of the system these events are considered first.

The FT in Fig. 2 may be expressed as the union of 10 minimal cut-sets:

$$TE = M_1 \cup M_2 \cup \ldots \cup M_{10} \tag{3}$$

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:

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

Knowing the minimal cut-sets, the following considerations would be of great help [31]:

- 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.
- Importance of each minimal cut-set. 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

$$IM_i = \frac{P(M_i)}{P(TE)} \tag{5}$$

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

$$P(M) = \prod_{i \in M} P(C_i) \tag{6}$$

Eq. (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, Eq. (6) yields a prior importance. According to the above discussion, all minimal cut-sets of the FT in Fig. 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.

3.3. Bayesian network analysis

Using the algorithm described in Section 2.3, the Bayesian network is constructed for the accident scenario in the feed control system (Fig. 3). Once developed, BN is analyzed using HUGIN 7.3 (http://www.hugin.com) [38].

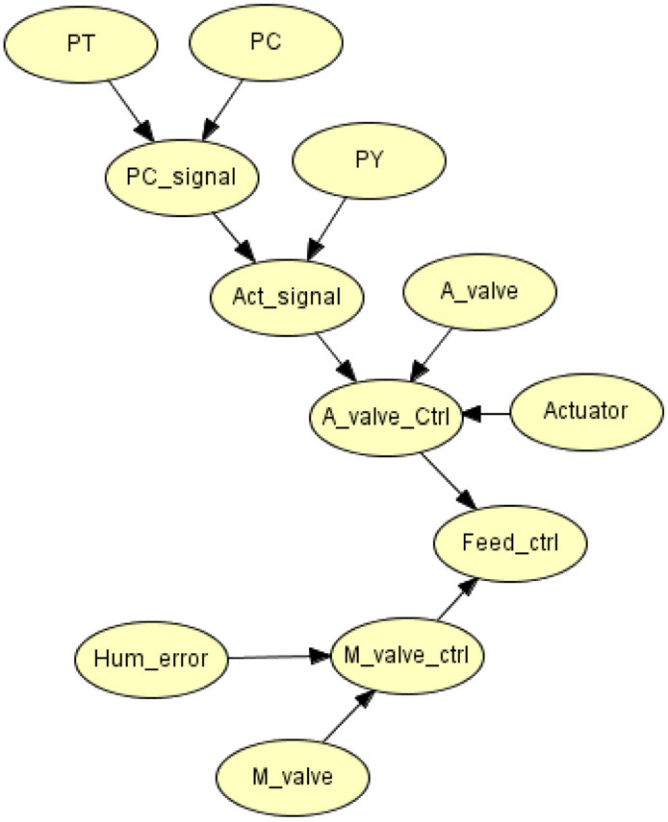


Fig. 3. BN structure based on the FT in Fig. 2.

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 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 2, the events C_9, C_{10}, C_6, and C_2 are again identified to contribute most to the leaf node (*Feed_ctrl*).

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 and Madsen, 2007). 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 and Tiran [36] coupled FT analysis with condition monitoring to obtain an up-to-date FT. Also, Ferdous et al. (2009) and Markowski et al. [33] 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.

3.4. Probability updating

Beyond the usual measures available in FTs, BN is able to perform probability updating analysis, given new observations [14]. 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 3).

It may be observed from Table 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 [14].

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:

$$P(\overline{C}_1,\overline{C}_2,\overline{C}_4,C_6,\overline{C}_7,C_9,C_{10}|Feed\_ctrl)=0.1179$$

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).

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.

4.1. 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.

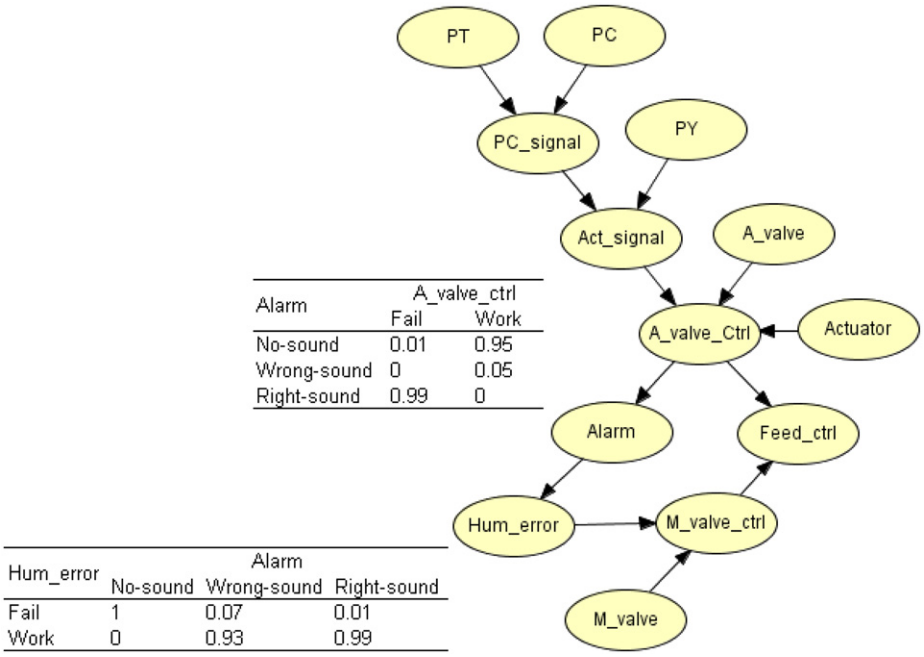
Based on the causal relationships among the aforementioned components and their failure probabilities, a BN was developed to predict the probability of improper operation of the control system (Fig. 4). The occurrence probability of the BN components are the same as before, except *Alarm* and *Hum_error* 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).

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 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 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_{10}, and the non-occurrence of the rest, with the probability of $P(\overline{C}_1,\overline{C}_2,\overline{C}_4,C_6,\overline{C}_7,\overline{C}_9,C_{10},\overline{C}_{13}|Feed\_ctrl)=0.1643$.

Table 3
Comparison between prior and posterior probabilities in different modeling steps.

Number	Component	First modeling		Alarm modeling		Uncertainty modeling	
		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



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

Fig. 4. BN structure for feed control system with alarm system.

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.

4.2. 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 [37]. 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 Fig. 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., $\Pr(\cup) = 3\Pr(\cap)$. 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 $Pr(Function) = Pr(\cup,\cap) = (0.75,0.25)$, and also by modifying its corresponding CPT (Fig. 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., Exp_1 and Exp_2) have been asked to assess the causal effect of *A_valve_ctrl* on *Alarm*. So, node *Expert* with two states Exp_1 and Exp_2 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., $Pr(Expert) = Pr(Exp_1,Exp_2) = (0.6,0.4)$).

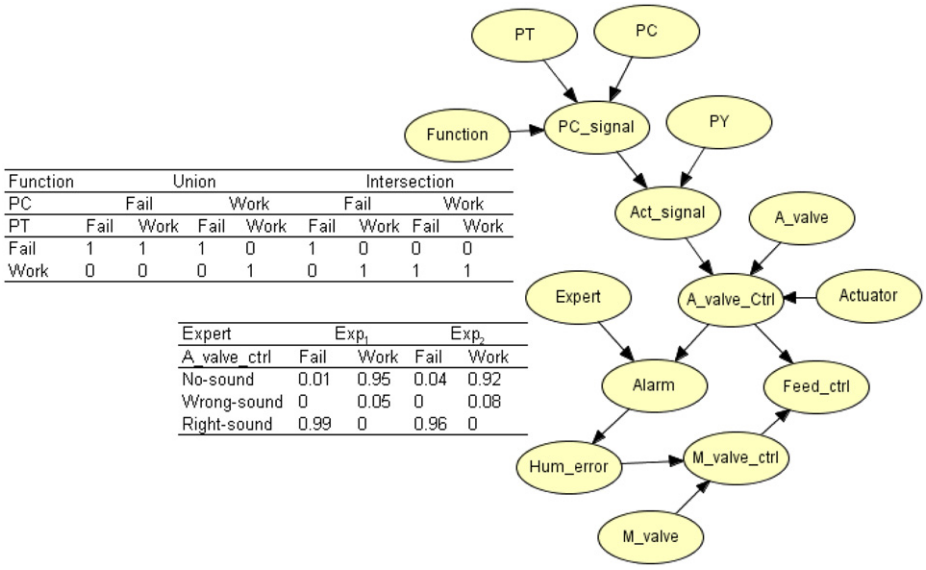
The different opinions of experts about the conditional dependence of *Alarm* on *A_valve_ctrl* are included in the corresponding CPT (Fig. 5).

The prior and posterior probabilities of the modified BN have been also listed in Table 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 $Pr(Function) = (0.7926,0.2047)$, showing an increase in the likelihood of union relationship between *PT* and *PC*, and $Pr(Expert) = (0.5632,0.4368)$, showing an increase in the reliability degree of Exp_2. It is to be noted that after the foregoing modifications, the prior probability of the leaf node, i.e., *Feed_ctrl*, increases from 0.1146 to 0.1155, 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 Exp_1, respectively.

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 that are common in accident analysis and risk assessment. The first half of the



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	Exp_1		Exp_2	
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

Fig. 5. Modified BN to capture functional uncertainty and expert opinion.

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 (Fig. 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.

Acknowledgment

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.

References

[1] Khan FI, Sadiq R, Husain T. Risk-based process safety assessment and control measures design for offshore process facilities. Journal of Hazardous Materials 2001;A94:1–36.
[2] Torres-Toledano JG, Sucar LE. Bayesian networks for reliability analysis of complex systems. Lecture notes in computer science 1998;1484:195–206.
[3] CNN. (2005). 〈http://www.cnn.com/2005/US/03/23/plant.blast/index.html〉 (last checked on 29.06.10).
[4] BP. (2005). 〈http://www.bp.com/genericarticle.do?categoryId=2012968〉 & contentId=7012963 (last checked on 29.06.10).
[5] Reuters. (2010). 〈http://www.reuters.com/article/idUSTRE61619Q20100207〉 (last checked on 25.06.10).
[6] Reuters. (2010). 〈http://www.reuters.com/article/idUSTRE6482L220100510〉 (last checked on 29.06.10).
[7] Khan FI. Use maximum-credible accident scenarios for realistic and reliable risk assessment. Chemical Engineering Progress 2001;11:56–64.
[8] 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.
[9] Ferdous R, Khan FI, Veitch B, Amyotte P. Methodology for computer aided fuzzy FT analysis. Journal of Process safety and Environmental Protection 2009;87:217–26.
[10] Ferdous R, Khan FI, Veitch B, Amyotte P. Methodology for computer-aided FT analysis. Process Safety and Environmental Protection 2007;85:70–80.
[11] Khoo LP, Tor SB, Li JR. A rough set approach to the ordering of basic events in a FT for fault diagnosis. International Journal of Advanced Manufacturing Technology 2001;17:769–74.
[12] Bartlett LM, Hurdle EE, Kelly EM. Integrated system fault diagnostics utilizing diagraph and FT-based approach. Journal of Reliability Engineering and System Safety 2009;94:1107–15.
[13] Kavcic M, Juricic D. CAD for FT-based diagnosis of industrial processes. Journal of Engineering Application of Artificial Intelligence 2001;14:203–16.
[14] Bobbio A, Portinale L, Minichino M, Ciancamerla E. Improving the analysis of dependable systems by mapping FTs into Bayesian networks. Journal of Reliability Engineering and System Safety 2001;71:249–60.
[15] Simon C, Weber P, Levrat E. Bayesian networks and evidence theory to model complex systems reliability. Journal of Computers 2007;2:33–43.

[16] Mahadevan S, Zhang R, Smith N. Bayesian networks for system reliability reassessment. Journal of Structural Safety 2001;23:231–51.
[17] Langseth H, Portinale L. Bayesian networks in reliability. Journal of Reliability Engineering and System Safety 2007;92:92–108.
[18] Wilson AG, Huzurbazar AV. Bayesian networks for multilevel system reliability. Journal of Reliability Engineering and System Safety 2007;92:1413–20.
[19] Przytula, K.W., & Thompson, D. (2000). Construction of Bayesian networks for diagnostics. In: Proceedings of IEEE aerospace conference, vol.5. p. 193–200.
[20] Huang Y, McMurran R, Dhadyalla G, Jones RP. Probability based vehicle fault diagnosis: Bayesian network method. Journal of Intelligent Manufacturing 2008;19:301–11.
[21] Giribone R, Valette B. Principles of failure probability assessment (PoF). International Journal of Pressure Vessels and Piping 2004;81:797–806.
[22] Boudali H, Dugan JB. A new Bayesian approach to solve dynamic FTs. Proceedings of Reliability and Maintainability Symposium (RAMS'05) 2005:451–6.
[23] Graves TL, Hamada MS, Klamann R, Koehler A, Martz HF. A fully Bayesian approach for combining multi-level information in multi-state FT quantification. Journal of Reliability Engineering and System Safety 2007;92:1476–83.
[24] Lampis M, Andrews D. Bayesian belief networks for system fault diagnostics. International Journal of Quality and Reliability Engineering 2009;25:409–26.
[25] Montani S, Portinale L, Bobbio A, Codetta-Raiteri D. RADYBAN: a tool for reliability analysis of dynamic FTs through conversion into dynamic Bayesian networks. Journal of Reliability Engineering and System Safety 2008;93:922–32.
[26] Montani S, Portinale L, Bobbio A, Codetta-Raiteri D. Automatically translating dynamic FTs into dynamic Bayesian networks by means of a software tool. Proceedings of Reliability and Maintainability Symposium (RAMS'06) 2006:434–41.
[27] Sklet S. Comparison of some selected methods for accident investigation. Journal of Hazardous Materials 2004;111:29–37.
[28] Nivolianitou ZS, Leopoulos VN, Konstantinidou M. Comparison of techniques for accident scenario analysis in hazardous systems. Journal of Loss Prevention in the Process Industries 2004;17:467–75.
[29] Zheng X, Liu M. An overview of accident forecasting methodologies. Journal of Loss Prevention in the Process Industries 2009;22:484–91.
[30] 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.
[31] Lewis EE. Introduction to reliability engineering. 2nd ed. New York: John Wiley& Sons; 1994.
[32] Lin C-T, Wang M-JJ. Hybrid FT analysis using fuzzy sets. Journal of Reliability Engineering and System Safety 1997;58:205–13.
[33] Markowski AS, Mannan MS, Bigoszewska A. Fuzzy logic for process safety analysis. Journal of Loss Prevention in the Process Industries 2009;22:695–702.
[34] Yuhua D, Datao Y. Estimation of failure probability of oil and gas transmission pipelines by fuzzy FT analysis. Journal of Loss Prevention in the Process Industries 2005;18:83–8.
[35] Jensen FV, Nielsen TD. Bayesian networks and decision graphs. 2nd ed. New York: Springer; 2007.
[36] Shalev DM, Tiran J. 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 2007;92:1231–41.
[37] Kjaerulff UB, Madsen AL. Bayesian networks and influence diagrams: a guide to construction and analysis. New York: Springer; 2007.
[38] HUGIN Expert software version 7.3 (2010). 〈http://www.hugin.com〉.