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

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

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:

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

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,