Journal of Loss Prevention in the Process Industries 41 (2016) 399–410

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Bayesian network based dynamic operational risk assessment

Shubharthi Barua*, Xiaodan Gao, Hans Pasman, M. Sam Mannan

Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843-3122, USA

ARTICLE INFO

Article history:
Received 1 May 2015
Received in revised form
20 November 2015
Accepted 26 November 2015
Available online 30 November 2015

Keywords:
Bayesian networks
Dynamic
Risk assessment
Fault tree

ABSTRACT

The oil/gas, chemical, petrochemical, food, power, papermaking and other process industries consist of numerous equipment and unit operations, thousands of control loops, and exhibit dynamic behavior. Chemical process plants are subjected to different types of process risks in daily operations, which include risks due to reactivity, toxicity and mechanical hazards, fire and explosion risks etc. Failure to manage or minimize hazards can result in serious incidents. Therefore, it is very important to identify hazards, perform risk assessments, and take proper initiatives to minimize/remove hazards and risks; else a catastrophic accident may result. Dynamic characteristics such as stochastic processes, operator response times, inspection and testing time intervals, ageing of equipment/components, season changes, sequential dependencies of equipment/components and timing of safety system operation also have great influence on the dynamic processes. Conventional risk assessment methodologies generally used in oil/gas and petrochemical plants have limited capacity in quantifying these time dependent characteristics. Therefore, it is important to develop a method that can address time-dependent effects in risk calculation and provide precise estimation. This study proposes a risk assessment methodology for dynamic systems based on Bayesian network, which represents the dependencies among variables graphically and captures the changes of variables over time by the dynamic Bayesian network. This study proposes to develop dynamic fault tree for a chemical process system/sub-system. Then a procedure to map the developed dynamic fault tree to map into the Bayesian network and the dynamic Bayesian network is provided to demonstrate the dynamic operational risk assessment methodology. A case study on a level control system is provided to illustrate the methodology's ability in capturing dynamic operational changes in process due to sequential dependency of one equipment/component on others.

1. Introduction

Chemical process industries such as offshore and onshore oil and gas exploration, and production, pipeline transfer, refinery operation, production of different chemicals and petrochemicals, involve numerous equipment and unit operations, thousands of control loops, and exhibit dynamic behavior. It is very important to understand hazards and risks associate with the process; perform risk assessment to identify them and take proper actions to remove or minimize hazards and risks; else a catastrophic accident may result. For example, process facilities involve a large numbers of pumps, compressors, separators, complex piping system and storage tanks, etc. in a congested area. A small mistake by an operator or a problem in the process system may escalate into a disastrous event as the process area is congested with process equipment and piping systems, and has limited ventilation and escape routes. Case histories showed that catastrophic accidents have a significant effect on people, environment, and society as they involved fatalities and great financial loss. For example, a vapor cloud explosion occurred at the BP Texas City refinery in 2005 resulted in 15 fatalities, 180 injuries and $1.5 billion in losses (U.S. CSB, 2007). The investigation revealed that insufficient process safety and lack of risk reduction measures contributed to this catastrophic accident. The U.S. CSB investigation on natural gas explosion at the ConAgra foods processing facility in North Carolina in 2009 and the Kleen Energy Power Plant Connecticut in 2020, reported failure to adopt inherently safer method from fire and explosion hazard perspective led to explosions (Khakzad et al., 2011). In 2010, a fire and explosion, resulting from a blowout, at the Macondo well resulted in 11 deaths and 17 injuries (U.S. National Commission on BP accident, 2011). Also the continuous spill from the wellhead for 87 days had disastrous effects on the environment and wildlife surrounding

* Corresponding author.
E-mail address: shubharthi.barua@ymail.com (S. Barua).

http://dx.doi.org/10.1016/j.jlp.2015.11.024
0950-4230/

the Gulf of Mexico. These accidents have significantly affected people's perception, and contributed greatly to raise concern to emphasize process safety. The U.S. Chemical Safety Board's (U.S. CSB) investigations of catastrophic accidents have reported insufficient process safety, inadequate management of change and lack of risk reductions measures as root causes of these accidents. It is explicit that effective risk assessment and adequate process safety management can prevent or reduce the severity of accidents. Therefore, continuous attention should be provided to improve available risk assessment methodologies. Also, it is important to develop new risk assessment techniques that can provide more information and flexibility to the industry for better risk management than the available techniques.

Process industries are complicated and dynamic in nature. Dynamic characteristics involve various time-dependent effects such as changes in seasons, ageing of process equipment/component, stochastic processes, human error, inspection and testing time intervals, hardware failures, process disturbances, sequential dependencies and timing of safety system operations. It is important to quantify risks arising from above stated time-dependent effects. Conventional risk assessment methodologies, i.e., HAZOP, What-if Analysis, Fault Tree, Event Tree, Bow-Tie Analysis, Layer of Protection Analysis have limited ability to quantify dynamic changes in processes. These methods can incorporate system's dynamic response to time, variations of process variables, operator actions and sequential dependencies in estimating risk with limited capacity. For example, a fault tree or event tree describes the relationship between the final outcome and different component/equipment failure, but hardly incorporate system's dynamic response to time, variations of process variables, operator actions, sequential dependencies, etc. Catastrophic accidents may result when critical process parameters exceed the safe operating region without being detected due to protective system failure, or timing of safety system operations (Yang and Mannan, 2010a,b). Hence, it is important to develop a method that has the ability to quantify risk arising due to different time-dependent effects.

Siu (1994) summarized different methods available for performing dynamic process systems risk assessment. Markov modeling is one of the widely accepted methods for dynamic risk analysis. State transition diagram is constructed to represent possible system states and transition from one state to another. One of the limitations of the Markov process is that the number of states increases with the increase of the system size. It makes construction of the system state transition diagram and computation complex (Reliability Analysis Center, 2003). Also, the Markov theory based models do not consider the effect of inspection on system-state transitions. Dynamic Logical Analytical Methodology (DYLAM) approach was proposed by Cacciabue et al. (1986). Nivolianitou et al. (1986) demonstrated the application of DYLAM approach for reliability analysis of chemical processes. This method has the ability to quantify different time dependent effects by incorporating dynamic aspects of a process. The DYLAM has limited ability to treat large number of scenarios and scenario calculations can be time consuming and costly (Siu, 1994). In the dynamic event tree (Acosta and Siu, 1993), branching is allowed to take at different points in time, and it can be applied for accident sequence analysis. Yang and Mannan (2010a,b) proposed a semi-markovian approach named dynamic operational risk assessment (DORA) methodology, with the ability to quantify risks for component failure and component's abnormal events, and also incorporated inspection/testing time schedule to understand its effect on risk. Monte Carlo simulation was performed to understand the system abnormal condition due to each individual component's transition from one state to another, and then prolonged simulation was performed to understand the effect of inspection and testing time on the probability of component abnormal event.

In recent years, Bayesian network (BN), a graphical model based on application of Bayes' theorem for probability reasoning to quantify complex dependencies, are being applied in engineering applications. A Bayesian network describes causal influence relations among variables via a directed acyclic graph. It represents a set of random variables in nodes and their conditional dependencies by drawing the edges from one node to another (see Fig. 1).

In a binary network, nodes and arcs represent variables and causal relationships among different nodes. Conditional probability tables or defined probabilistic relationships among nodes represent how one variable is linked another one or multi-variables. The nodes that influence other variables and have unconditional probability are called parent or root nodes. Nodes that are conditionally dependent on their direct parents are called intermediate nodes. The end node is defined as a leaf node.

Let $N = (G, P)$ be a Bayesian network, where
$G = (V, E)$ is a directed acyclic graph (DAG); V (random variables) represents nodes; and E represents edges between pairs of nodes of DAG.

P represents probability distribution over V and $V = \{X_1, X_2, \ldots, X_n\}$ can be either discrete or continuous random variables (Donohue and Dugan, 2003). These random variables are assigned to the nodes and the edges. Bayesian networks can be represented by the joint probability distribution, *P(V)*;

$$P(V) = \sum_{X \in V} P\{X|pa(X)\} = P(X_1, X_2, \ldots, X_N) = \sum\nolimits_{i=1}^{n} P\{X_i|pa(X_i)\}$$

Here $pa(X_i)$ = parent nodes of X_i.

A general Bayesian network is static in nature, i.e., the joint probability distribution is usually a representation of a fixed point or an interval of time (McNaught and Zagorecki, 2010). A dynamic Bayesian network describes the evolution of joint probability distribution over time and thus extends the general Bayesian network. Discrete time modeling represents the progression of time in the dynamic Bayesian network was proposed by Dean and Kanazawa (1989). In a dynamic Bayesian network, arcs links nodes from previous time slice to that of the next time slice to represent temporal dependencies among them. Kjaerulff (1995) demonstrated that Markov assumption can be held true for the dynamic Bayesian network if the variable state at future time slice '(n + 1)-th' time slice is independent of past given the present 'n-th' time slice. Bayesian network (BN) has the ability to calculate the probability unknown parameters as well as to update the probability of known variables using conditional probability. Therefore, the application of Bayesian network (BN) would provide more flexibility for risk analysis.

Weber et al. (2012) provides a summary of the Bayesian network's application in the field of dependability, risk analysis and maintenance. Bobbio et al. (2001) described method to map the fault tree into the Bayesian network in the area of dependability and performed an analysis of dependable systems. Also, Boudali and Dugan (2005) demonstrated sequential dependencies of events and Montani et al. (2005) included temporal aspects in performing reliability analysis to demonstrate capabilities of Bayesian network in dependability analysis. Delic et al. (1995) stated potential application of Bayesian network in software safety cases as a part of Safety of Hazardous Industrial Processes