Process Safety and Environmental Protection 97 (2015) 25–36

Contents lists available at ScienceDirect

Process Safety and Environmental Protection

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

# Fault propagation behavior study and root cause reasoning with dynamic Bayesian network based framework

Jinqiu Hu[a,*], Laibin Zhang[a], Zhansheng Cai[b], Yu Wang[a], Anqi Wang[a]

[a] College of Mechanical and Transportation Engineering, China University of Petroleum, Beijing 102249, China
[b] CNOOC Zhong Jie Petrochemical Co., Ltd, Cang Zhou 061101, China

ARTICLE INFO

*Article history:*
Received 9 September 2014
Received in revised form
24 January 2015
Accepted 4 February 2015
Available online 7 April 2015

*Keywords:*
Process safety
Root cause reasoning
HAZOP
Dynamic Bayesian network

ABSTRACT

The Bhopal disaster was a gas leak incident in India, considered the world's worst industrial disaster happened around process facilities. Nowadays the process facilities in petrochemical industries have becoming increasingly large and automatic. There are many risk factors with complex relationships among them. Unfortunately, some operators have poor access to abnormal situation management experience due to the lack of knowledge. However these interdependencies are seldom accounted for in current risk and safety analyses, which also belonged to the main factor causing Bhopal tragedy. Fault propagation behavior of process system is studied in this paper, and a dynamic Bayesian network based framework for root cause reasoning is proposed to deal with abnormal situation. It will help operators to fully understand the relationships among all the risk factors, identify the causes that lead to the abnormal situations, and consider all available safety measures to cope with the situation. Examples from a case study for process facilities are included to illustrate the effectiveness of the proposed approach. It also provides a method to help us do things better in the future and to make sure that another such terrible accident never happens again.


## 1. Introduction

The Bhopal disaster (1984) was a gas leak incident in India, considered the world's worst industrial disaster happened around process facilities. While the workplace in the process industry now is quite different and represents hazards of a different nature, many programs, management systems, and technologies have reduced the hazards and consequences extensively. Growing economies and global competition have led to more complex processes involving the use of hazardous chemicals, exotic chemistry, and extreme operating conditions. The complexity of the process plants has increased due to extensive heat and mass integration. Thus, the plant operation becomes more demanding with multiple unit operation interactions. It is their scale, nonlinearities, interconnectedness, and interactions with humans and the environment that can make these complex systems fragile, when the cumulative effects of multiple abnormalities can propagate in numerous ways to cause systemic failures (Zhang and Hu, 2013). It can also lead to "emergent" behavior, i.e., the behavior of the whole is more than the sum of its parts that can be difficult to anticipate and control. In complex petrochemical systems, once failure occurs in any subsystem or component, it often leads to chain reaction, causing catastrophic safety accidents with significant loss of production as the Bhopal disaster. Postmortem investigations of disasters have shown that systemic failures rarely occur due to a single failure of a component or personnel, and in particular the main reason causing accidents and

*Abbreviations:* ASM, abnormal situation management; DBN, dynamic Bayesian network; HAZOP, hazard and operability study; FCCU, fluid catalytic cracking unit; CPTs, conditional probability tables; 2TBN, two-slice temporal Bayesian net.

* *Corresponding author*. Tel.: +86 13401021372.
E-mail address: hujinqiu@gmail.com (J. Hu).

http://dx.doi.org/10.1016/j.psep.2015.02.003

their consequences lies in the complex nonlinear interactions among a large number of failure causing factors.

"The legacy of Bhopal" (Mannan et al., 2005) indicated that "there are significant areas of need where research must be funded if advances are to be made in technology, management systems, and other aspects of process safety." Abnormal situation management (ASM) is one of these research areas, which develops fault diagnosis strategies that monitor process variables and detect differences from normal behavior. As Leveson (2015) mentioned that there were always warning signs before a major accident. In fact, most major accidents have multiple precursors and cues that an accident is likely to happen. Before an accident, such "weak signals" are often perceived only as noise. The problem then becomes how to distinguish the important signals from the noise. Abnormal situation identification and diagnosis are the ways to prevent accidents.

Abnormal situation is a general term used for any departure of the process from an acceptable range of operation. So ASM involves timely identification and mitigation of any significant departure of the process from an acceptable normal range of operation. Ineffective ASM has significant safety and economic impact on the industry (Vedam et al., 1999). Given the size, scope and complexity of the systems and interactions, it is becoming increasingly difficult for plant personnel to anticipate, diagnose and control serious abnormal events in a timely manner. The reason for this is that a system is more than the sum of its elements (Rasmussen, 1997). Often we found that attempts to improve the safety of a system from models of local features were compensated by people adapting to the change in an unpredicted way.

Nowadays there exist considerable achievements in developing appropriate prognostic and diagnostic methodologies for monitoring and controlling such abnormal situations for complex systems. Effective diagnosis of the fault root causes and prediction of their consequence can provide an early warning on the behavior of the petrochemical process systems, which will enhance the reliability and safety of the given system and reduce the operating risk.

Recognizing the importance of ASM systems, the chemical process industry has developed operator decision support systems like AEGIS (Honeywell, 1995) to aid the operator in efficient ASM. It began to put more focus on the fault diagnosis research. Early in 1999, the Op-Aide, an intelligent operator decision support system, was developed by the Laboratory for Intelligent Process Systems of Purdue University to assist the operator in quantitative diagnosis and assessment of abnormal situations (Vedam et al., 1999). In Op-Aide independent modules provided data acquisition, process monitoring, fault diagnosis, and situation assessment capabilities. To better support computer integrated ASM, a multi-agent system architecture was proposed within which user and functional agents cooperated based on a collaboration mechanism (Yang and Lu, 2000). Interactions among functional agents were represented by an ASM activity diagram and an extended signed digraph. Although these systems were sophisticated and were able to apply to complex processes, the analysis performed by these systems was largely qualitative. Use of qualitative knowledge alone significantly hampered their capability to differentiate between abnormal situations at different risk levels. As another weakness, these systems usually failed to reveal the fault propagation behavior in the system.

In order to study the fault propagation behavior, deep-level diagnosis methods can be mainly divided into two categories: model-based diagnosis methods and historical data-based diagnosis methods (Venkatasubramanian et al., 2003a,b,c). In model-based methods, SDG model which has been widely studied can reflect the relationship between parameters of the process, and is conducive to find the fault root causes. However the process of the model development mostly needs background and expert knowledge. It may be prone to be idealized with obvious subjectivity and some differences from practice. In addition, causality relationship between the process parameters expressed by SDG model is not comprehensive enough, and the expression of the node states is quite limited. In contrast historical data-based methods, such as artificial neural network, have the ability of self-learning and fault tolerance, depending less on subjective knowledge. However with its "black box" characteristic, it is usually difficult to give an elaborate explanation of its own behavior and the output results.

Dynamic Bayesian network (DBN) has the advantage both of model-based and data-based methods. It is a possible approach for modeling and predicting the dynamic fault propagation behavior, by introducing temporal dependencies in the network. DBN is a powerful tool for reasoning under uncertainty (which is a typical characteristic of risk), using well-established theoretical foundations of probability calculus as the base for performing inference and handling uncertainty. Codetta-Raiteri et al. (2012) provided a dynamic Bayesian network based framework to evaluate cascading effects in a power grid. Ramírez and Utne (2015) proposed a dynamic Bayesian network for assessing the life extension of aging repairable systems. Hu et al. (2012) presented a DBN for safety prognosis and assessment of fault propagation paths in complex degrading systems. In contrast with the available techniques, DBN offers a good trade-off between the analytical tractability and the representation of the propagation of the dynamic fault behavior.

This paper deals with the modeling of the dynamic fault propagation effects in a petrochemical system. Firstly hazard and operability (HAZOP) study is carried out on the basis of the fully understanding of the petrochemical system, by which all the possible deviations and their corresponding potential fault causes and consequences are analyzed carefully. Then dynamic Bayesian network (DBN) is introduced, which is further used to build the fault causal relationships in the complex system. Finally by the inherent inference mechanism of DBN, the most possible initial reason(s) happened in the fault interdependency network can be found out accurately when abnormal events or parameter deviations are detected by a condition monitoring system (e.g. DCS).

The rest of this paper is organized as follows. Section 2 goes deep into the failure propagation behavior in complex process system. Section 3 defines the fundamental theory of BN and DBN. In Section 4, a DBN based framework for root cause reasoning with detailed step-by-step procedures is developed. In Section 5, the proposed approach is applied to abnormal situation management in a FCCU case study. The conclusions are drawn in Section 6.

## 2. Fault propagation behavior in complex petrochemical system

The complexity of the accident causes and consequences in the complex petrochemical system is related to the limitation of subjective cognitive ability and also the objective