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
0957-5820/

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 complexity of the accident itself. Both aspects have a close relationship of all kinds of sophisticated nonlinear interaction among parts or units in the system. Based on the study of the principle of integration and interconnection, it is indicated that the interaction is the true ultimate cause of the system failure. Therefore investigation of the interaction of time, structure and hierarchy in system become the premise and foundation to analyze the safety situation of complex system.

Again and again, investigations have shown that the number of accidents caused by coupling factors is alarming. Survey showed that 92% accidents were caused by multiple factors, and average each accident had more than 4.39 basic abnormal events, and the most could reach 20 basic abnormal events. The failure propagation behavior caused by interactions and presented by multiple basic abnormal events has some characteristics such strong randomness and elusiveness, which usually leads to disastrous consequences.

For example in Bhopal gas tragedy, in the early hours of December 3, 1984, an estimated 41 tons of deadly methylisocyanate (MIC) gas leaked out of tank No. 610C of the Union Carbide plant and escaped into the atmosphere. The immediate cause was the building up of pressure in the tank, due to an exothermic reaction caused by water in the tank. This pressure caused the safety valve to rupture and the gas to escape. Such leakage of gas into the atmosphere was a contingency for which the plant should have been prepared. This catastrophe happened because the essential safety systems either failed or were inoperable and the safety procedures were not strictly complied with (Bisarya and Puri Swaraj, 2005).

Therefore in the fault propagation behavior study, the term fault is generally defined as a departure from an acceptable range of an observed variable or a calculated parameter associated with a process (Venkatasubramanian et al., 2003a). This defines a fault as a process abnormality or symptom. The underlying cause(s) of this abnormality, such as a failed coolant pump or a controller, is (are) called the basic event(s) or the root cause(s). The basic event is also referred to as a malfunction or a failure. The failure propagation behavior can be explained as a complicated and dynamic network of the activities of multiple basic abnormal events both in time and space. For instance, first an abnormal event happens and has effect on a few subsystems which have a close relation with it in the complex system; then these affected subsystems become failed or degraded and will further make influence on other related subsystem by certain coupling interaction; further some key subsystems which play an important role in keeping the system's main function will failed caused by former multiple factors. Therefore as the number of failed key subsystems increases, the whole system will partly lose control or finally paralyze which leads to disastrous accidents with inestimable loss.

Accident-causing theory also indicates that accident is the result of a series of continuous changes. Benner's P-theory of accident also believes that the accident process consists of a series of successive events. Deviation sequence in the production process can be expressed as a series of "chain of events", which can be called "hazard scenario", that is the process of the accident. Deviation sequence is constituted by the status parameter deviations, expressing the complete development process from the initial cause to the final consequences of an accident. Deviation sequence includes some variables which cannot be directly observed, but these variables can be reasoned by observed variables in the sequence deviation.

In order to study above fault propagation behaviors and try to discover the root causes of accident for petrochemical plant, three issues have to be well figured out, that are:

- how to systematically model the relationships among the units and their function in a large complex petrochemical process system;
- how to systematically model the fault interdependencies in the petrochemical process especially when the system is running;
- how to ratiocinate the fault causes on each technical or functional level when certain abnormal event or parameter deviation occurs.

Clearly, to cope with such issues with complexity and uncertainty, a dynamic Bayesian network based framework should be developed and used to analyze, predict and explain the behavior of such multiple factors.

3. Dynamic Bayesian network

A Bayesian network (BN) as a probability-based knowledge representation method is appropriate for the modeling of causal processes with uncertainty. A Bayesian network is a directed acyclic graph (DAG) whose nodes represent random variables and links define probabilistic dependences between variables. These relationships are quantified by associating a conditional probability table (CPT) with each node, given any possible configuration of values for its parents (Hu et al., 2011). The set of nodes of BN represents the system variables (which can be discrete or continuous), and the set of directed arcs represents the dependencies or influence among the variables. In discrete BNs, variables are defined over a set of mutually exclusive states, and a probability is associated to each state.

So the fault propagation behaviors can be studied by BN, in which the different states of nodes represent various abnormal conditions of components or unit of the plant system; while directed arcs indicate the system functional relationship and also fault interdependencies. The quantification of probabilities in discrete BNs consists of assigning prior probabilities to the nodes without parents, and defining a CPT for the nodes with parents. The CPT specifies the probability that the node is in a particular state given any combination of parent states. Prior knowledge can be acquired from previous safety analysis, such as HAZOP study, FMEA analysis, Fault Tree analysis, etc.

BNs use probability theory for handling uncertainty. Values of the variables are expressed as probability distributions. As information accumulates (e.g., observations of variables from condition monitoring system in the field), the posterior probability distribution of variables of interest (such as the unknown root causes of a certain abnormal event) can be computed conditioned on the variables that have been observed, and knowledge of the true value of the variables usually increases. Hence, the uncertainty of the value is reduced, and the probability distribution becomes less spread. So BN has the advantage both of model-based and data-based methods for modeling and predicting the dynamic fault propagation behavior. Prior knowledge can be used first to develop BN representing the fault propagation of a system, then as more data are accumulated by condition monitoring system the parameters and structure of BN model can be updated and more and more close to its physical truth.

The static Bayesian network can be extended to a dynamic Bayesian network (DBN) model by introducing relevant temporal dependencies that capture the dynamic behaviors of the domain variables between representations of the static network at different times. DBNs consist of a sequence of time slices, and each slice comprises a static BN describing the system in the corresponding time step. Temporal links between variables in different time slices represent a temporal probabilistic dependence between the variables. Therefore two types of dependencies can be distinguished in a dynamic Bayesian network: contemporaneous dependencies and non-contemporaneous dependencies. Contemporaneous dependencies refer to arcs between nodes that represent variables within the same time period. Non-contemporaneous dependencies refer to arcs between nodes that represent variables at different times (Hu et al., 2012).

Therefore a DBN is a way to model probability distributions over semi-infinite collections of random variables $\{Z_1, Z_2, \ldots\}$. A DBN is defined to be a pair, $(B_1, B_\rightarrow)$, where B_1 is a BN which defines the prior $P(Z_1)$, and $B_\rightarrow$ is a two-slice temporal Bayesian net (2TBN) which defines $P(Z_t|Z_{t-1})$ by means of a DAG as follows:

$$P\left(z_t|Z_{t-1}\right) = \prod_{t=1}^{N} P\left(Z_t^i|Pa\left(Z_t^i\right)\right) \quad (1)$$

where Z_t^i is the ith node at time t and $Pa(Z_t^i)$ are the parents of Z_t^i in the graph.

The nodes in the first slice of a 2TBN do not have any parameters associated with them, but each node in the second slice of the 2TBN has an associated CPT for discrete variables, which defines $P(Z_t^i|Pa(Z_t^i))$ for all $t>1$. The parents of a node $Pa(Z_t^i)$ can either be in the same time slice or in the previous time slice. The arcs between slices are from left to right, reflecting the causal flow of time. If there is an arc from Z_{t-1}^i to Z_t^i, this node is called persistent. The arcs within a slice are arbitrary. Directed arcs within a slice represent "instantaneous" causation. In this paper, the parameters of the CPTs used by the proposed model are assumed time-invariant; i.e., the model is time-homogeneous. The semantics of a DBN can be defined by "unrolling" the 2TBN until there are T time-slices. The resulting joint distribution is then given by:

$$P\left(Z_{1:T}\right) = \prod_{t=1}^{T}\prod_{i=1}^{N} P\left(Z_t^i Pa\left(Z_t^i\right)\right) \quad (2)$$

DBNs are excellent tools for many types of probabilistic inference, such as fault propagation study here, since they encode all relevant qualitative and quantitative information contained in a full probabilistic model. There are three important types of inference used in relation to dynamic models: smoothing, filtering, and prediction. Here for root cause reasoning, the filtering and smoothing are used. By filtering, the unknown state of unobservable nodes (e.g., current fault mode of a certain component) at the current time step can be calculated given related observations; while by smoothing, the root causes can be deduced at a previous time step given the current observable and unobservable variables.

Several inference methods for a discrete-state DBN can be used, i.e., forwards–backwards algorithm, unrolled junction tree, and the frontier algorithm. In this paper, the forwards–backwards method is used for Bayesian inference in the DBN reasoning stage. For a more detailed presentation of the DBN model construction and learning, see, e.g., Murphy (2002) and Khakzad et al. (2013).

4. Development of a DBN-based root cause reasoning approach

Aiming to improve the effectiveness and accuracy of abnormal situation management in complex process system, the fault propagation behavior should be studied and modeled in a scientific and systematic way. A DBN-based framework is proposed for this purpose. The overall workflow is shown in Fig. 1. In the proposed approach, three stages are presented, as shown in Fig. 1.

4.1. *Stage I: hazard scenarios development*

Hazard and operability analysis (HAZOP) is widely accepted as the method for conducting risk analysis and hazard scenarios

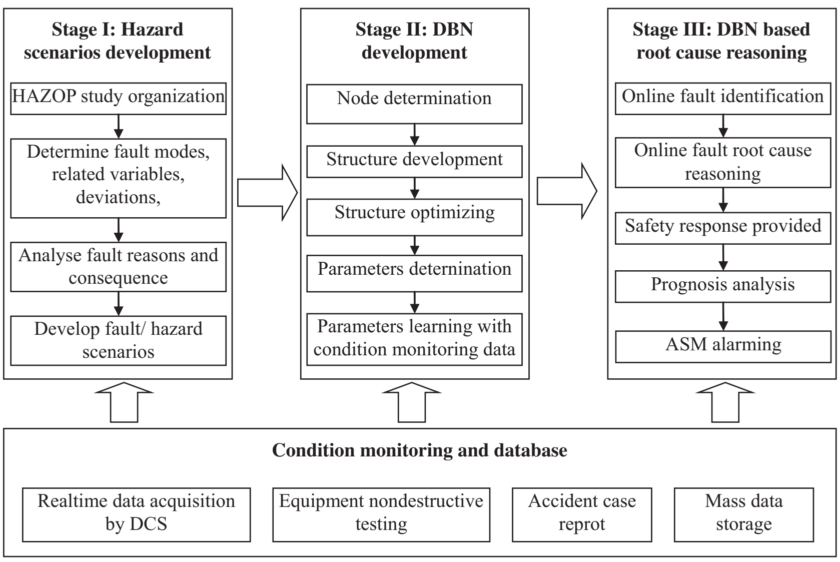

Fig. 1 – DBN-based framework for fault propagation behavior study and root cause reasoning.

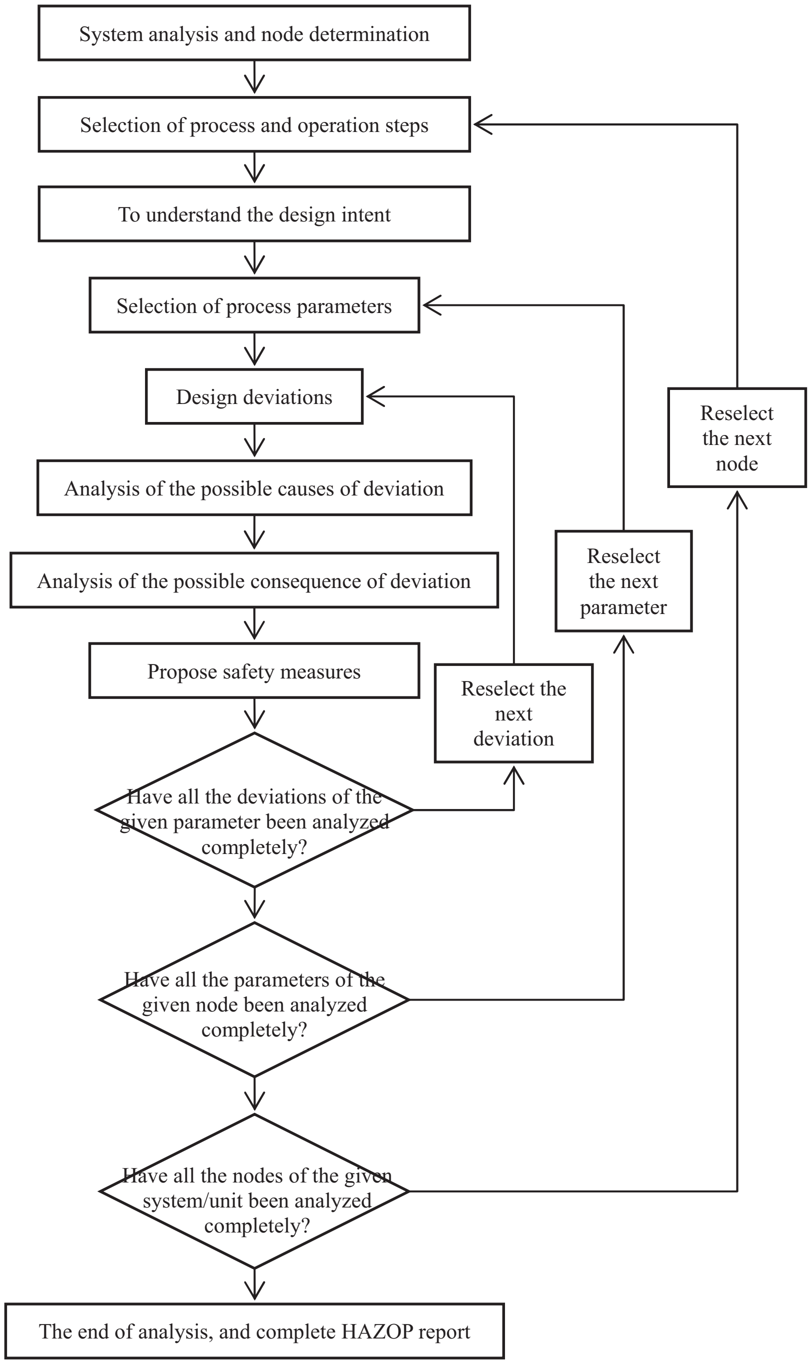

Fig. 2 – Process of the hazard scenarios development by HAZOP.

development in process industry. Once the hazards and problems are identified, possible safety measures and contingency plan can be proposed to avoid these hazards and problems. For a more detailed presentation of the HAZOP advantage and application, see, e.g., Kletz (1999a,b).

The process of the hazard scenarios development by HAZOP can be presented as Fig. 2. The plant P&ID is divided into sections or nodes and then each section is further studied by brainstorming method. Usually nodes are equipment items. Once a node is chosen, each line of the node is analyzed applying certain deviations. These deviations result from the combination of a 'guide word' with a 'property' of the line, i.e., "*GuideWord + Property = Deviation*". GuideWords are described in *IEC61882*, which includes but not limited that *NONE*, *MORE OF*, *LESS OF*, *PART OF*, *MORE THAN*, *OTHER THAN*, *REVERSE*, etc. Properties or parameters are *flow*, *temperature*, *composition*, etc. The detailed steps in stage I are generally conducted as follows:

(1) Compose a concise and detailed description of the process and explain its design intent. Break it down into functional blocks or process sections.
(2) For each node of the system, the process variable(s) should be described, which identifies design intent. Select one guideword to combine with the parameter as a deviation.
(3) Systematically question every node to discover how deviations from the design intention can occur and estimate whether these deviations can give rise to hazards. To those meaningful deviations, analyze its possible causes, negative consequences after its occurrence, and propose appropriate suggestions.

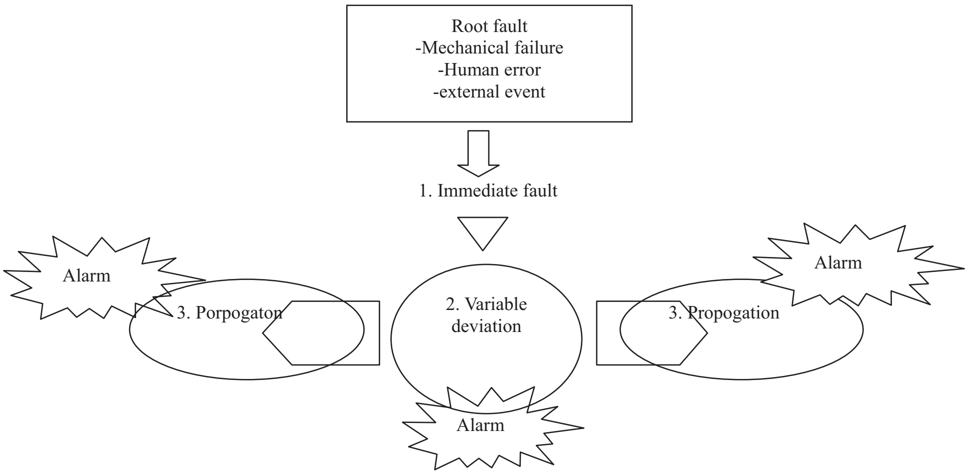

Fig. 3 – schematic diagram of fault propagation path.

(4) Repeat step (3) till all the possible deviations of this parameter are finished.
(5) Select the next parameter. Repeat steps (2)–(4) till all the possible deviations of all parameters of this node are finished.
(6) Select the next node of the system, repeat step (2)–(5) till all the nodes of the whole system are finished.
(7) Develop hazard scenarios. The previous nodes' possible consequences should be linked to the subsequent nodes' possible reasons, which will develop a hazard propagation path (HPP). Analyzing node by node in HAZOP results, the hazard scenarios can be developed successfully as various abnormal event chains or fault chains.
(8) Risk evaluation according to each hazard scenario (optional choice).
(9) Repeat above analysis steps until all hazards are reduced to a risk value below the safety threshold.
(10) Record the results. Follow up action items.

Therefore HAZOP analysis is also a high completeness bidirectional analysis method. In each analysis step, bidirectional analysis is used to identify hazard scenarios (accident chains) consisting of each deviation's causes and consequences. Reasons which could cause the abnormal event are identified by reverse analysis and the negative consequences are also predicted by forward analysis along accident chains according to each deviation of process parameters.

Based on HAZOP study, the previous nodes' possible consequences may have relation to the subsequent nodes' possible reasons. The hazard scenarios can be developed in this way successfully, which are very important for the work of the DBN development in the later stage. By the hazard scenarios development, it is able to find causes far from the node of the deviation. Hence it provides a convenient approach to build a DBN model for root cause reasoning and consequence prediction.

During the development of the hazard scenarios development process, the fault modes, internal variables, exogenous factors, the fault cause, and effect relationships (which can be considered as qualitative fault propagation behaviors) are determined. The outputs of stage I will be used as the input of stage II (DBN model development).

4.2. *Stage II: DBN development*

After hazard scenarios development by HAZOP study, the fault propagation path and the relationship of deviation and fault modes are revealed in detail. In this stage, DBN is used to develop a probability-based knowledge representation of the fault propagation behavior.

By analyzing historical accident cases, sometimes the reasons causing abnormal events are multi-level, including root causes, remote causes, and indirect and direct causes. The fault propagation path is shown in Fig. 3. The propagation behaviors are described as following: root cause → indirect cause → immediate cause → variable deviation → deviation propagation → alarm (or accident).

Condition monitoring system usually only provides alarms of various deviations without any diagnosis function. Therefore in practice, when the operator meets a large amount of alarms of deviations, they even do not know how to handle them, and what the real problems are. In fact when accident happens, large amount of alarms may come from only a few hidden problems, such as equipment failure or fault, misoperation, etc.

The effective representation of fault propagation knowledge is an important issue in artificial intelligence area, because it determines how easily dataset characteristics can be comprehended. DBNs aid the comprehension of causal relations between random variables using a graphical structure. Therefore it is developed to help to provide the reasons of each abnormal situation level telling operators why the abnormal events or accidents happen, and where the root causes exist, even providing appropriate safety measures or emergency plans in time. All these analysis work should be carried out online and in a timely manner, since the abnormal event should be handled as soon as possible, otherwise it may lead to serious problem or catastrophe causing more losses. In order to make the established DBN model reflect the fault propagation process in a more accurately and comprehensively way, several developing steps are provided as follows.

Step 1: to determine the model nodes.

Nodes in DBN Model are determined corresponding to the nodes analyzed in HAZOP. Among all the HAZOP nodes, those state variables that need to be observed are considered as static nodes in DBN model. Static nodes' values can be acquired by condition monitoring system such as distributed control systems (DCS). Their states can be described by HAZOP guidewords.

Another kind of nodes in DBN model named as dynamic nodes, which are related to the hidden states of the system, representing different fault modes (such as the fault condition of oil pump, corrosion condition of equipment, etc.). The status of these hidden nodes should be calculated by reasoning algorithm given the current the states of static nodes in DBN model.

Step 2: DBN structure development

DBN structure development aims to figure out a proper DAG, and confirm the association relationship between nodes. Every variable in hazard scenario is represented by a DBN node. Then the network structure can be developed by creating the directed edges from the node corresponding to fault cause to the node representing its consequence. The intervention of priori knowledge obtained from stage I can help to determine the BN structure design effectively. In some literatures, FTA or bow-tie diagram can be used to map into Bayesian network (Wu et al., 2015; Khakzad et al., 2013). Here in this paper the correlation between the parameters is clarified by HAZOP study before FTA or bow-tie diagram can be omitted (if time and budget are enough, it would be better to carry out a FTA or bow-tie for deep analysis).

Step 3: DBN structure optimization

Learning BN structure from the data has been proven to be an NP-hard problem. Robinson (1977) showed that the number $r(n)$ of possible structures for Bayesian network having n nodes is given by the recurrence formula:

$$r(n) = \sum_{i=1}^{n} (-1)^{i+1} \frac{n!}{i!\,(n-i)!} 2^{i(n-1)} r(n-i) \tag{3}$$

Searching for the best structure is necessary but difficult because the search space increases exponentially with the number of variables. Fortunately in stage I, by HAZOP study the interdependency among variables can be determined in general, and we can use such information to build several basic DBN structures, so the search space can be largely reduced. However an observed fault may have more than one possible cause. Therefore usually more than one available DBN model can be developed according to the results of HAZOP studies, and not all alternative models are appropriate. The HAZOP study in stage I generally relies on brainstorming, and may not be complete with causal paths starting in one of the first HAZOP nodes and propagating further down. So there is a multiple of possible BNs relating HAZOP deviations with background causes, since there is a little ambiguity about the mechanism of interfering variables. In this paper, K2 algorithm (Cooper and Hersovits, 1992) is introduced to pick up the optimal DBN structure to guarantee the accuracy and effectiveness of the root cause reasoning. The selected DBN is based on the most likely BN structure that fits historical time-series sequences of observations of faults developing.

The K2 algorithm proceeds as follows: an initial ordering of the nodes is assumed first, which can be based on prior expert knowledge from HAZOP study in stage I. Let D be a database of cases, Z be the set of variables represented by D, and B_{si} and B_{sj} be two belief-network structures containing exactly those variables that are in Z. By computing such ratios for pairs of Bayes network structures as Eq. (4), a set of structures can be ranked by their posterior probabilities. Then the optimal DBN structure with the highest score will be chosen.

$$\frac{P(B_{si}|D)}{P(B_{sj}|D)} = \frac{\frac{P(B_{si},D)}{P(D)}}{\frac{P(B_{sj},D)}{P(D)}} = \frac{P(B_{si},D)}{P(B_{sj},D)}. \tag{4}$$

Cooper (Cooper and Hersovits, 1992) presented a method for calculating $P(B_s, D)$ based on four assumptions, which also conform to the features of the process plant system. Assumption 1: the database variables Z are discrete. Assumption 2: cases occur independently, given a belief-network model. Assumption 3: there are no cases that have variables with missing values. Assumption 4: the density function $f(B_p|B_s)$ is uniform, where B_p is a vector whose values denote the conditional-probability assignments associated with structure B_s, and f is the conditional-probability density function over B_p given B_s.

In his paper, the $P(B_s, D)$ can be computed as Eq. (5), letting B represents an arbitrary Bayes network structure containing just the variables in D. In Eq. (5), let Z be a set of n discrete variables, where a variable x_i in Z has r_i possible value assignments: $(v_{i1}, \ldots, v_{ir_i})$; D be a database of m cases, where each case contains a value assignment for each variable in Z. Each variable x_i in B_s has a set of parents, which is represented with a list of variables π_i. Let w_{ij} denote the jth unique instantiation of π_i relative to D. Suppose there are q_i unique instantiations of π_i. Define N_{ijk} to be the number of cases in D in which variable x_i has the value v_{ik} and π_i is instantiated as w_{ij}. For a more detailed presentation of the K2 algorithm, such as its heuristic method and some applications, please see Cooper and Hersovits (1992).

$$P(B_s, D) = P(B_s) \prod_{i=1}^{n} \prod_{j=1}^{q_i} \frac{(r_i - 1)!}{(N_{ij} + r_i - 1)!} \prod_{k=1}^{r_i} N_{ijk}! \tag{5}$$

where $N_{ij} = \sum_{k=1}^{r_i} N_{ijk}$.

Bayesian scoring criteria (BIC) is selected as the scoring function to find the model structure with the highest score. BIC value is defined as Eq. (6), where L is the maximum likelihood estimation, d is the number of parameters, N represents the number of the data, and $\hat{\theta}$ is the maximum likelihood parameter estimation.

$$\log\ P\left(L|\hat{\theta}\right) - 0.5d\ \log N \tag{6}$$

Step 4: to determine conditional probability

Conditional probability tables (CPT) should be determined to present the quantitative causal relationship between nodes with uncertainty under the established DBN structure, which belongs to parameter learning problem. CPT can be determined by learning the parameters from the database such as historical data from long time condition monitoring. Several learning algorithms, e.g., maximum a posterior (MAP) for complete data (Yang et al., 2012) and expectation-maximization (EM) for incomplete data, can be used in this step.

4.3. *Stage III: DBN based root cause reasoning*

The key issue of fault root cause reasoning by DBN Model is to obtain the probability $P(X^T|Y^T)$, where Y^T is the observation set of variables within a limited time-series, and X^T is the hidden variable set, which should be estimated on the basis of the observed value of Y^T. Bayesian inference algorithm includes forward–backward (FB) smoothing algorithm, decomposition tree algorithm, differential algorithm, approximate reasoning algorithm and so on. In this paper FB algorithm is used for forward and backward inference calculation to search the fault root cause and consequences. It includes two steps as follows:

(1) Fault root cause inference:

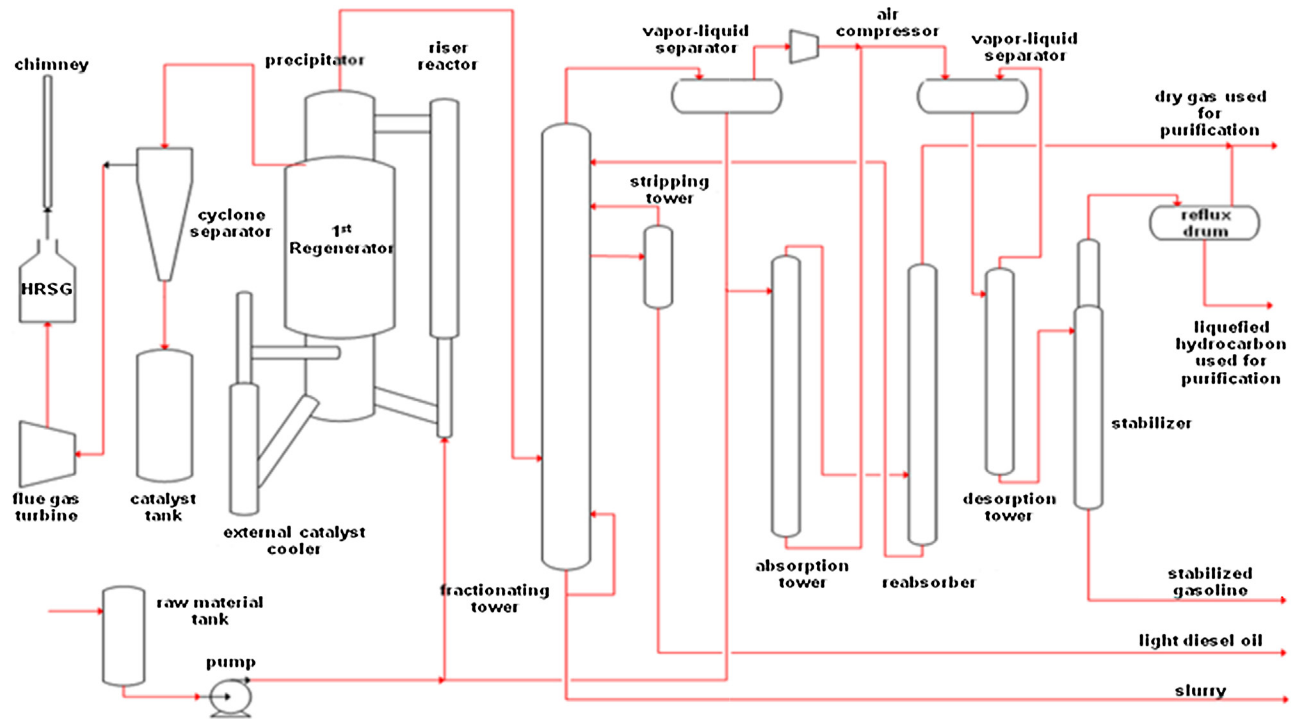

Fig. 4 – Overview of the FCCU.

The forward recursive calculation is applied to compute $\alpha_t(i)$ as Eq. (7), where $\alpha_t(i)$ indicates the state probability, that $X_t = i$ at moment t, and it meet the given observable sequence $(y_1, y_2, \ldots, y_t)$ before moment t.

$$\alpha_t(i) = P(X_t = i|y_{1:t}) = P(y_t|X_t)\left[\sum x_{t-1} P(X_t|x_{t-1}) P(x_{t-1}|y_{1:t-1})\right]. \quad (7)$$

(2) Consequence prediction:

The backward recursive calculation is applied to compute $\beta_t(i)$ as Eq. (8).

$$\beta_t(i) = P\left(y_{t+1}|Y_0^t\right) = \frac{\sum_{x_{t+1}} \alpha_{t+1}(x_{t+1})}{\sum_{x_t} \alpha_t(x_t)} = \frac{\sum_{x_{t+1}} P(X_{t+1} = i|y_{1:t+1})}{\sum_{x_t} P(X_t = i|y_{1:t})} \quad (8)$$

where, $\beta_t(i)$ represents the probability of the observable sequence at moment $t+1$, and by recursive computation, the probability that the observable sequence is in keeping with $(y_{t+1}, y_{t+2}, \ldots, y_T)$ after moment t can be calculated.

The above method of DBN based framework will be applied in a case study of FCCU to validate its effectiveness. The following case study will include several steps:

(1) alternative DBN models are established according to the HAZOP analysis results of FCCU;
(2) DBN structures are learned and trained with the help of historical data, then the optimal one is selected by scoring mechanism;
(3) the developed optimal DBN is applied for fault root cause reasoning and early warning information can be provided.

5. Case study

In modern refinery, fluid catalytic cracking (FCC) is an important oil refinery process, which converts heavy petroleum fractions into a series of more valuable products such as gasoline, diesel fuel and light gases. A common fluid catalytic cracking unit (FCCU) consists of reaction regeneration unit, fractionation unit, and absorption-stabilization unit, etc. The typical production process is illustrated in Fig. 4. Reaction regeneration unit is used for the regeneration and recycling of the catalyst, which can be considered as the key equipment in FCC process. The interaction between feedstock used and reaction environments, such as temperature, catalyst circulation rate, air flow and pressure, has a combined effect on the final product quality and safety. Such highly complex, nonlinear dynamics, constrained variables and cross-coupling interaction system brought engineers a great deal of risk. In this section, an abnormal event case, i.e., alarming caused by low regenerator temperature, is considered to validate the proposed approach, and analyze its application effectiveness.

5.1. *Stage I: hazard scenarios development*

The FCCU reactor–regenerator which processes mixtures of fresh, recycle and residual oil using regenerator and riser. A typical FCC unit process flow diagram is illustrated in Fig. 5. From a system point of view, FCCU reactor–regenerator can be considered as a high dimensional, highly nonlinear, interconnected, complex system (Jia et al., 2003). The preheated hot feedstock from atmospheric distillation unit is mixed with recycle oil from fractionator bottom. The mixture is vaporized once in contact with the hot regenerated catalyst from the regenerator and injected into the bottom of the riser reactor. Catalytic cracking reactions take place in the lower area of the riser. Spent catalyst is discharged into the bottom of the reactor after separation from oil vapor, then enters the stripping section to be further stripped from product vapors by hot steam. The flow of catalyst from reactor to the regenerator is controlled by a slide valve present in the standpipe connecting the regenerator and the reactor. This slide valve is used to control the catalyst bed level in the reactor. Regenerated catalyst flows to the riser through a slide valve located in the standpipe connecting the regenerator and the riser. This valve is used to control the heat supply to the riser by regulating the catalyst

Table 1 – HAZOP results of the reaction regeneration (partial results).

Node	Deviation	Possible reasons	Possible consequences	Safety measures
Node 7: air pipeline of the main air blower	Flow of the air for regeneration + LOW	1. The main fan shutdown; 2. anti surge valve is opened; 3. the main fan entrance filter net has adsorbate; 4. filter is sucked into the pipeline, causing the primary air flow get down; 5. the flow control valve has fault.	1. The oxygen content in flue gas decreased; 2. the amount of carbon in the regenerated catalyst increased; 3. the activity of the catalyst decreased, get black, seriously causing carbon accumulation accidents.	1. When the main air is interrupted, carry out the emergency shutdown procedure; 2. regularly check whether the filtering net entrance have dopant; 3. if there exist serious mechanical noises, start the emergency shutdown procedure as soon as possible;
	Flow of the air for regeneration + MORE	1. Air compressor failed, causing air supply broken off.	1. Energy consumption will increase, and energy will be wasted; 2. secondary combustion will be initiated.	1. Start standby supercharger timely to recover the air supply, meanwhile contact instrument engineer and mechanical repair engineer to repair the supercharger fault.

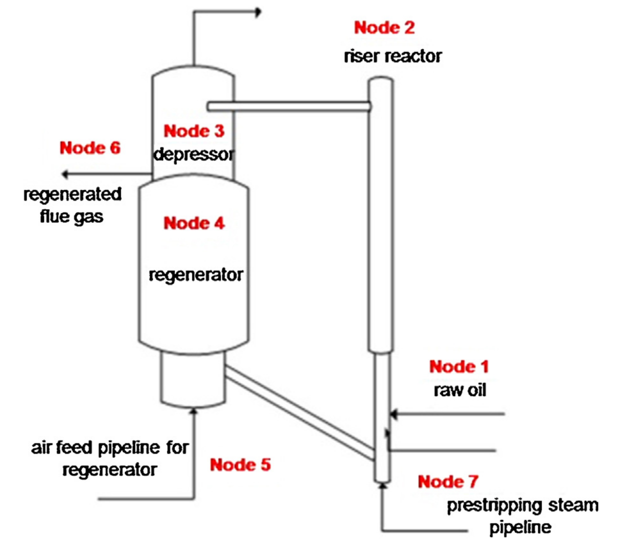

Fig. 5 – overview of the configuration of the reactor–regenerator unit.

flow rate to maintain the riser temperature at a desired level and therefore the product composition.

HAZOP study of the reactor–regenerator system was carried out, by breaking it down into functional nodes shown in Fig. 5. Seven nodes was divided, and each node was analyzed applying certain deviations, such as "*Flow of the air for regeneration + LOW*", "*Flow of the air for regeneration + MORE*", etc. The HAZOP study results were shown in Table 1 (partial results for demonstration). Related hazard scenarios were developed by the way that the previous nodes' possible consequences were linked to the subsequent nodes' possible reasons as fault chains. One of the hazard scenarios of the reactor–regenerator system was shown in Fig. 6 as an example.

5.2. *Stage II: DBN development*

According to the HAZOP study results, the related parameters which can reflect the safety condition of the unit were selected, and the information of the dynamic and static nodes used in DBN model of the reaction regeneration part were show in Tables 2 and 3. There were four dynamic nodes and six static nodes in the DBN model of the selected unit.

Several DBN models can be developed, and the K2 algorithm was used to evaluate each model structure and help to select the optimal one based on the historical data of the system. The structure with highest score can be considered as the optimal one. Therefore during the optimazation step, a group of historical data containing fault states was obtained. At first 1000 samples were used. Then in every calculation cycle, more 1000 samples were added in the calculation process until the total amount of the data arrived 100, 000 samples. The K2 algorithm was then used to evaluate the rationality of each DBN structure, computing each BIC value respectively. Fig. 7 shows the change of the BIC value of the optimal DBN structure which got the highest score as training data increases.

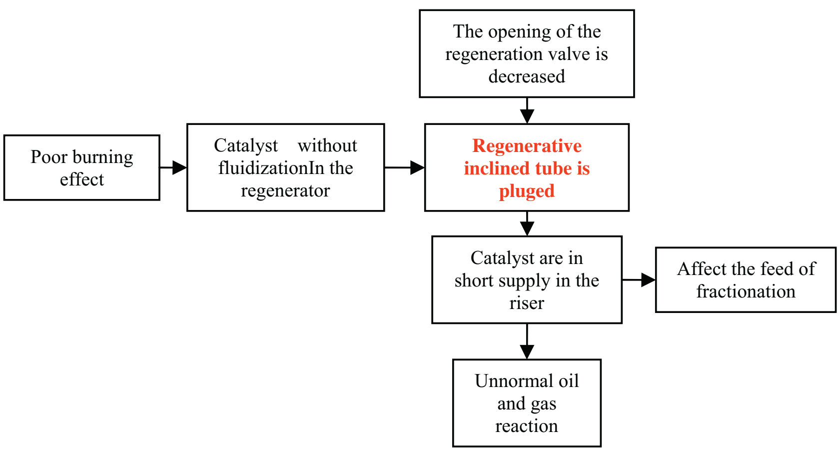

Fig. 6 – Developed hazard scenario of reactor–regenerator system (partial results).

Table 2 – The information of the dynamic nodes in the DBN model of the reaction regeneration part.

Unit	Dynamic node	Node ID	State set
Regeneration part	1. Regenerator	D1_1	{1.normal, 2.incrustation, 3.leakage, 4.failure}
	2. Slide valve at the output of the regeneration	D1_2	{1.normal, 2.large opening, 3.small opening}
	3. Slide valve at the input of the regeneration	D1_3	{1.normal, 2.large opening, 3.small opening}
	4. Main air blower	D1_4	{1.normal, 2.fault}

Table 3 – The information of the static nodes in the DBN model of the reaction regeneration part.

Unit	Static node	Node ID	State set	Safety range	State threshold
Regeneration part	1. Regenerator reserves	S1_1	{1.normal, 2.more, 3.less}	(6,54)	{(6,54); ≥54; ≤6}
	2. Regenerator temperature	S1_2	{1.normal, 2.more, 3.less}	(80,720)	{(80,720); ≥720; ≤80}
	3. Regenerator pressure	S1_3	{1.normal, 2.more, 3.less}	(0.1,0.4)	{(0.1,0.4); ≥0.4; ≤0.1}
	4. Pressure difference of the slide valves at the output of the regeneration	S1_4	{1.normal, 2. more, 3.less}	(8,72)	{(8,72); ≥72; ≤8}
	5. Pressure difference of the slide valves at the input of the regeneration	S1_5	{1.normal, 2.more, 3.less}	(10,80)	{(10,80); ≥80; ≤10}
	6. Flow of the main air blower	S1_6	{1.normal, 2.less}	>6000	{6000; ≤6000}

It indicated that with the increasing amount of training data, the BIC value of the given model tended to be stabilized and constant. The DBN structure which got the highest score was show in Fig. 8.

The CPTs of the nodes in DBN model contained two parameters that were state transition probability density distribution $P_r(x_{t+1}|x_t)$ and observational variable probability density distribution $P_r(y_t|x_t)$. The parameters should be trained taking advantage of the historical data and also the expert prior knowledge if necessary. When the failure data was limited, the prior knowledge was primarily used for parameter learning; while the condition monitoring and failure data were accumulated for a long time, the parameter learning could be updated by data-driven method.

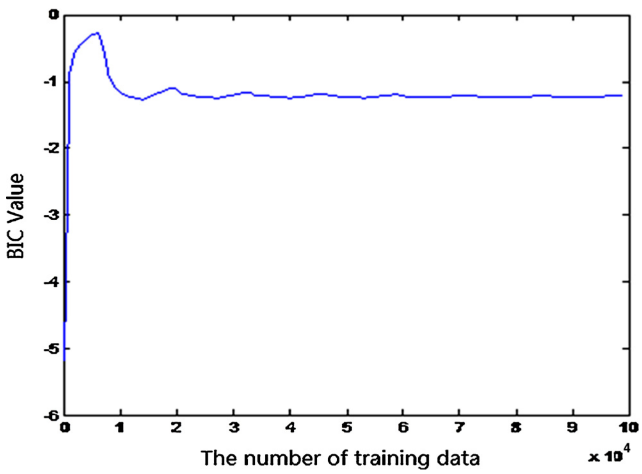

Fig. 7 – BIC values of the optimal DBN structure.

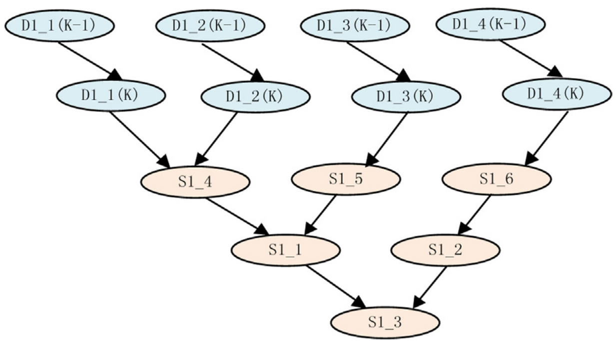

Fig. 8 – The optimal DBN structure with highest score.

5.3. *Stage III: DBN based root cause reasoning*

Before the abnormal event occurred, each parameters (observable nodes) of the regeneration part were all in normal states. By the inference of the DBN model, the hidden nodes D1_1 (regenerator), D1_2 (slide valve at the output of the regeneration), D1_3 (slide valve at the input of the regeneration), and D1_4 (main air blower) were in "normal" states. Fig. 9 shows the inference results of each hidden nodes before the abnormal event occurred (the numbers on the abscissa axis indicated the state numbers in Tables 2 and 3).

At a certain moment, low level alarms about the temperature of the regenerator and the flow of the main air blower arose, while other parameters were still in normal states. By the inference of the DBN model, the state of the node D1_4 changed, and the fault probability was calculated as 90%,

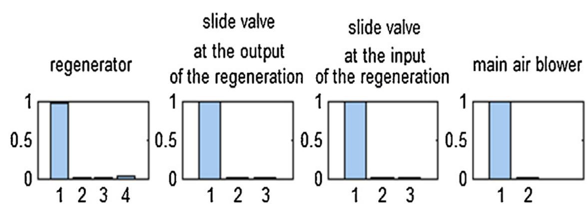

Fig. 9 – The reasoning results of each hidden nodes (normal condition).

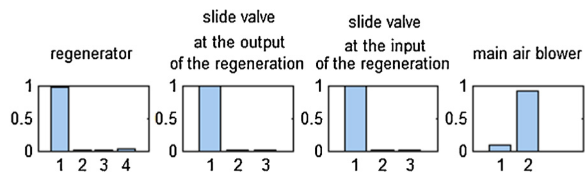

Fig. 10 – The reasoning results of each hidden nodes (fault condition).

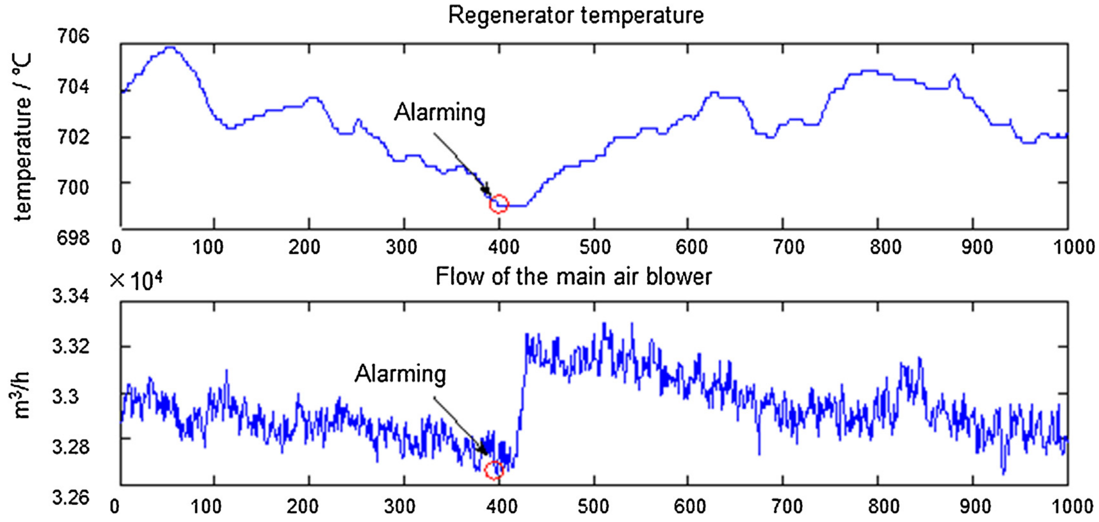

Fig. 11 – The historical data corresponding to the regenerator temperature (above) and the flow of the main air blower (below).

while the states of other nodes did not change obviously. Fig. 10 shows that the reasoning results of each hidden nodes after alarming arose.

Conclusions can be get from the reasoning results that: (1) the main air blower failed, which further caused the flow of the main air blower of the regenerator decreased; (2) the opening degree of the valve on the pipeline of the main air blower may get decreased because of failure, which made the flow of the main air blower of the regenerator decreased. Safety measures which have been analyzed in Table 1 can be provided to the field operators to quickly carry out effective actions preventing future accident happen.

Fig. 11 shows the historical condition monitoring data corresponding to the regenerator temperature and the flow of the main air blower within a short range around the alarming moment. After abnormal event happened, according to the information provided by the DBN model, the opening degree of the valve on the main air pipeline was adjusted larger. Then the flow of the main air blower increased immediately, and the regenerator temperature was also increased accordingly. In this way two parameters fell back to normal states. In the case study, the effectiveness and rationality of the proposed method are validated.

6. Conclusion

This paper focuses on the area of abnormal situation management which should be enhanced from Bhopal tragedy. According to the strong interdependencies between various facilities and components in the process facilities, which usually cause cascading faults or accidents, a DBN based framework for fault propagation behavior study and root cause reasoning is proposed and illustrated in detail.

In order to build the model which is able to systematically, accurately and entirely reflects the interdependency between process parameters of the facilities, HAZOP study is carried out to develop hazard scenarios firstly. All the possible deviations and their corresponding potential fault causes and consequences are analyzed carefully. Then DBN is used to build the fault causal relationships. Finally by the inference mechanism of DBN, the most possible root cause(s) can be accurately found out online with advised safety responses when the condition monitoring system discovers an abnormal event.

The application of the proposed method has been illustrated on the FCCU. The overall risk of the abnormal event can be reduced for the operator by providing them clear diagnosis information and helping them to take effective corrective actions.

Acknowledgments

The project is supported by the Natural Science Foundation of China (Grant No. 51104168), the Excellent Doctoral Dissertation Supervisor Project of Beijing (Grant YB20111141401), the Program for New Century Excellent Talents in University (No. NCET-12-0972), the Beijing Natural Science Foundation (3132027) and also supported by Science Foundation of China University of Petroleum (No. YJRC-2013-35).

References

Bisarya, R.K., Puri Swaraj, 2005. The Bhopal gas tragedy—a perspective. J. Loss Prevent. Process Ind. 18 (4–6), 209–212.

Codetta-Raiteri, D., Bobbio, A., Montani, S., Portinale, L., 2012. A dynamic Bayesian network based framework to evaluate cascading effects in a power grid. Eng. Appl. Artif. Intel. 25 (4), 683–697.

Cooper, G., Hersovits, E., 1992. A Bayesian method for the induction of probabilistic networks from data. Mach. Learn. 9, 309–347.

Honeywell, 1995. The Abnormal Situation Management Joint Research and Development Consortium. http://www.iac.honeywell.com/Pub/Absitmang

Hu, J., Zhang, L., Ma, L., Liang, W., 2011. An integrated safety prognosis model for complex system based on dynamic Bayesian network and ant colony algorithm. Expert Syst. Appl. 38, 1431–1446.

Hu, J., Zhang, L., Liang, W., 2012. Opportunistic predictive maintenance for complex multi-component systems based on DBN-HAZOP model. Process Saf. Environ. Prot. 90 (5), 376–388.

Jia, C., Rohani, S., Jutan, A., 2003. FCC unit modeling, identification and model predictive control, a simulation study. Chem. Eng. Process: Process Intensif. 42 (4), 311–325.

Khakzad, N., Khan, F., Amyotte, P., 2013. Dynamic safety analysis of process systems by mapping bow-tie into Bayesian network. Process Saf. Environ. Prot. 91 (1–2), 46–53.

Kletz, T.A., 1999a. Hazop and Hazan – Identifying and Assessing Process Industry Hazards, 4th edition. Institution of Chemical Engineers, Rugby, UK [Chapters 3–6].

Kletz, T.A., 1999b. The origins and history of loss prevention. Process Saf. Environ. Prot. 77 (3), 109–116.
Leveson, N., 2015. A systems approach to risk management through leading safety indicators. Reliab. Eng. Syst. Saf. 136, 17–34.
Mannan, M.S., West, H.H., Krishna, K., et al., 2005. The legacy of Bhopal: the impact over the last 20 years and future direction. J. Loss Prevent. Process Ind. 18 (4–6), 218–224.
Murphy, K., (Ph.D. thesis) 2002. Dynamic Bayesian Networks: Representation, Inference and Learning. University of California, Berkeley.
Ramírez, P., Utne, I., 2015. Use of dynamic Bayesian networks for life extension assessment of ageing systems. Reliab. Eng. Syst. Saf. 133, 119–136.
Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Saf. Sci. 27 (2–3), 183–213.
Robinson, R.W., 1977. Counting unlabeled acyclic digraphs. Comb. Math. 622, 28–43.
Vedam, H., Dash, S., Venkatasubramanian, V., 1999. An intelligent operator decision support system for abnormal situation management. Comput. Chem. Eng. 23 (1), S577–S580.
Venkatasubramanian, V., Rengaswamy, R., Yin, K., et al., 2003a. A review of process fault detection and diagnosis: Part I: quantitative model-based methods. Comput. Chem. Eng. 27 (3), 293–311.
Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., 2003b. A review of process fault detection and diagnosis: Part II: qualitative models and search strategies. Comput. Chem. Eng. 27 (3), 313–326.
Venkatasubramanian, V., Rengaswamy, R., Kavuri, S.N., et al., 2003c. A review of process fault detection and diagnosis: Part III: process history based methods. Comput. Chem. Eng. 27 (3), 327–346.
Wu, X., Liu, H., Zhang, L., Skibniewski, M., Deng, Q., Teng, J., 2015. A dynamic Bayesian network based approach to safety decision support in tunnel construction. Reliab. Eng. Syst. Saf. 134, 157–168.
Yang, A., Lu, M., 2000. A formulation of the collaboration mechanism for integrated abnormal situation management. Comput. Chem. Eng. 24 (2–7), 539–544.
Yang, J., Zhang, X., Suo, H., Lu, L., Zhang, J., Yan, Y., 2012. Maximum a posteriori linear regression for language recognition. Expert Syst. Appl. 39 (4), 4287–4291.
Zhang, L., Hu, J., 2013. Safety prognostic technology in complex petroleum engineering systems: progress, challenges and emerging trends. Pet. Sci. 10 (4), 486–493.