Journal of Loss Prevention in the Process Industries 33 (2015) 279–288

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Integrating probabilistic signed digraph and reliability analysis for alarm signal optimization in chemical plant

Di Peng [a], Xiangbai Gu [a, b], Yuan Xu [a], Qunxiong Zhu [a, *]

[a] College of Information Science & Technology, Beijing University of Chemical Technology, Beijing 100029, China
[b] Sinopec Engineering (Group) Co., Ltd., Beijing 100101, China

A R T I C L E I N F O

Article history:
Received 24 July 2014
Accepted 4 January 2015
Available online 6 January 2015

Keywords:
Alarm system
Probabilistic signed digraph
Reliability
ROC analysis
TE process

A B S T R A C T

The alarm system given in industrial plants are massive and complex. Under such condition, critical alarms are overwhelmed by false and unnecessary alarms and thus result in severe safety issues. To address the problem, this paper proposes a probabilistic signed digraph (PSDG) based alarm signal selection method that requires achieving maximal system reliability. In this method, a PSDG model is firstly constructed to visualize the causal relations between process variables. Then the criteria of observability and identifiability are imposed to determine the candidate alarm variables that can qualitatively distinguish all assumed faults. Instead of selecting the minimum number of combinations of candidate variables, the alarm variables are optimized by a reliability formulation that takes into account the missed alarm and false alarm probabilities of the system; this formulation is solved by the receiver operating characteristic (ROC) graph. Finally, the developed methodology is illustrated using a Tennessee Eastman process.

1. Introduction

The growth of industrial scale and the sophistication of plant monitoring systems increase the monitoring workload for each plant operator, which contributes to the complexity of fault detection and the increased probability of human error. In the plant alarm system, if a variable moves beyond the predefined operating limit, an alarm is triggered with sounds and lights, and the operators are notified that there might be a fault happening. However, unnecessary alarms may be assigned because there isn't an effective method for plant alarm system design, and these redundant alarms result in a flood of alarms in a short time. As defined by ISA (International Society of Automation) (International Society of Automation (ISA), 2009), an alarm flood is a condition during which the alarm rate is greater than that the operator can effectively manage, typically 10 or more alarms per 10 min period. In the alarm flood, operators either turn off or ignore some alarms. The worst case is that crucial alarms are overwhelmed and false judgments or operations are made. Consequently, it is necessary and urgent to design an effective alarm management strategy that assists operators to quickly identify the cause of faults.

In recent years, alarm management has attracted increasing attention by researchers and industrial companies. Both EEMUA (Engineering Equipment and Materials Users' Association) (Engineering Equipment and Materials Users' Association (EEMUA), 2007) in Europe and ISA in USA published standards about alarm management. These standards provide guidance to help users design, implement and maintain a well performing alarm system. The alarm system design contains adjustment of threshold of monitoring ranges and selection of alarm variables. For setting the alarm limits, optimal filter, time delay and deadband (Izadi et al., 2009; Adnan et al., 2011, 2013; Cheng et al., 2013a) were the three common methods. Besides, Yang et al. (Yang et al., 2012) adjusted the alarm limit by analyzing the correlation between process variables and alarm variables. Zhu et al. (Zhu et al., 2014) developed a dynamic alarm limit, which was especially suitable for process transitions such as feedstock, throughput, or product grade changes and maintenance operations. For selecting the alarm signals, some approaches, such as fuzzy clustering (Zhu and Geng, 2005; Geng et al., 2005), multivariate statistics (Chen, 2010), pattern matching (Cheng et al., 2013b) and Bayesian analysis (Pariyani et al., 2012), were proposed to improve process safety and product quality. Furthermore, two alarm data visualization tools, high density alarm plot (HDAP) and alarm similarity color map

* Corresponding author.
E-mail address: zhuqx@mail.buct.edu.cn (Q. Zhu).

http://dx.doi.org/10.1016/j.jlp.2015.01.005

(ASCM), were presented to evaluate the integrated performance of alarm system (Kondaveeti et al., 2010). However, all above-mentioned alarm selection methods use the data driven approach, and cannot explain the underlying relationship between the selected alarm signals and the other alarm signals.

As the process industrial system is complex with nonlinear properties, some cause-effect models, instead of mathematical models, are being used in the alarm system analysis. The cause-effect model (such as signed digraph, SDG) represents the causal relationship between variables and shows the abnormality propagation process. Luo et al. (Luo et al., 2007) firstly combined the abnormality propagation diagram with the alarm system design. This method selected the alarm source variables that are the nearest neighbor distance from listed faults. Takeda et al. (Takeda et al., 2010a, 2010b) proposed an alarm signal selection method using a two-layer cause-effect model. The method evaluated the sets of alarm source variables by reachability matrix and the signs that upper or lower the monitoring range, and ensured that the finally derived sets of candidate alarms could qualitatively identify all assumed faults. Even though the above methods reduce the number of alarms and improve the fault resolution, they ignore the reliability of the selected alarm signals.

In engineering practice, alarms might be faulty. For example, an alarm may be raised even if the variable behaves normally, which is called a false alarm; or no alarm may be raised when the variable behaves abnormally, which is called a missed alarm. Therefore, some redundant alarm variables should be allowed in case of failures. In order to describe the reliability of the system, the missed alarm and the false alarm probability of the system are defined in this paper. According to the reliability analysis, if the number of alarm signals increases, the potential for nuisance alarms or alarm flood become higher and higher, resulting in a high false alarm probability and a low missed alarm probability. On the contrary, if the number of alarm signals decreases, the false alarm probability might decrease with larger missed alarm probability. Therefore, missed alarm and false alarm are two aspects of reliability, and a receiver operating characteristic graph is used in this research to make a trade-off between them. Finally, the Tennessee Eastman process is applied to reveal the advantages of this alarm signal selection method.

2. Cause-effect representation

The probabilistic signed digraph (PSDG), as a development of the traditional SDG, is presented to represent cause-and-effect relationship between state variables. In the SDG model, a variable node denotes a process variable, a reason node denotes an abnormal reason that will cause variation of its adjacent variable nodes, and a directed edge denotes a direct causal relationship between them. The states of variable nodes in SDG include '0', '+' and '−', representing the normal state, higher than normal state and lower than normal state, respectively. The signs of directed edges include '+' and '−', representing the cause node and effect node change in the same direction or in the opposite direction. The SDG model can be constructed from a topology of the plant piping and the material and energy balance of the plant (Maurya et al., 2003a, 2003b, 2006). Along with SDG model, operators can easily find how a fault is propagated in the system.

Nevertheless, traditional SDG cannot describe the probability of the causal influence between variables. Because there are self-regulatory and control actions in the target system, some influences from one node to another node would be broken even though there is causal connection between them. To this end, PSDG model is developed on the basis of SDG model by introducing the probabilistic information of the nodes and directed edges. The PSDG model has been proposed in our previous work (Peng et al., 2014), and its definition is reviewed briefly here.

Definition 2.1. A PSDG model $\gamma = (G,\varphi,P)$ is composed by a directed graph G, a function φ and a probability distribution P.

The directed graph G is defined as $G = (V,R,E)$, where $V = \{x_{j_1}, x_{j_2}, \cdots, x_{j_N}\}$ is a variable node set, $R = \{x_{i_1}, x_{i_2}, \cdots, x_{i_M}\}$ is a reason node set and $E = \{e_{lk}\}$ (where $l, k = i_1, i_2, \ldots, i_M, j_1, j_2, \ldots j_N$) is a directed edge set. The function is defined as $\varphi : E \rightarrow \{+,-\}$, and $\varphi(e_{lk})$ is the sign of directed edge e_{lk}.

The probability distribution P is defined as $P{:}R,E \rightarrow [0,1]$, where $f_i = P(x_i)$ indicates the occurrence probability of fault reason x_i ($x_i \in R$), and $p_{j_{K-1}j_K} = P(e_{j_{K-1}j_K})$ indicates the propagation probability from the cause node $x_{j_{K-1}}$ failure to effect node x_{j_K} failure ($e_{j_{K-1}j_K} \in E$).

Fig. 1 is an illustration of a PSDG model. In Fig. 1, the circle nodes, rectangle nodes, directed solid lines and directed dotted lines denote process variables, fault reasons, positive directed edges and negative directed edges, respectively. It should be noted that every reason node is considered as a root node, which has at least one connection to the corresponding effect nodes and no connection to a cause node.

3. Selection criteria of candidate alarm sets

To assist plant operators quickly diagnose faults and plan countermeasures, the criteria of observability (detecting all faults) and identifiability (distinguishing the exact fault) are discussed in this section. Under these two criteria, the selected alarm signals can statistically identify all assumed faults.

3.1. Obesrvability of all assumed faults

When a fault occurs, the alarm will be measured not only by the adjacent variables directly but also by the influenced variables due to the propagation between process variables. Based on the definition of PSDG model, the reachability from a reason node to a variable node p_{ij} (where $i \in \{i_1, i_2, \ldots, i_M\}, j \in \{j_1, j_2, \ldots, j_M\}$) can be calculated as follows:

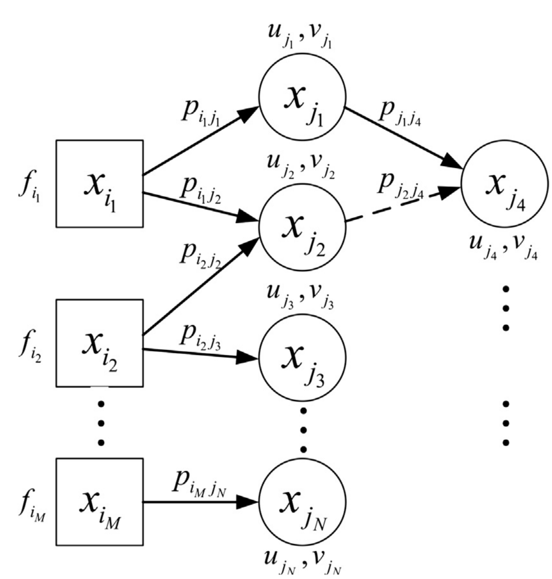

Fig. 1. An illustration of the PSDG model.