Safety Science 82 (2016) 432–444

Contents lists available at ScienceDirect

Safety Science

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

A two-level intelligent alarm management framework for process safety

Jinqiu Hu *, Yan Yi

College of Mechanical and Transportation Engineering, Laboratory of Oil and Gas Production Safety and Accident Prevention and Control, China University of Petroleum, Beijing 102249, China

ARTICLE INFO

Article history:
Received 20 December 2014
Received in revised form 27 August 2015
Accepted 15 October 2015
Available online 13 November 2015

Keywords:
Alarm management
Petrochemical process
Alarm filtering
Root-cause diagnosis

ABSTRACT

Alarm management, which alerts process operators to deviations of variables from designed limits, has been a key safety issue in a petrochemical plant. Petrochemical processes frequently operate upon a multitude of steady states, transitions and states in abnormal events. Some single-fault scenarios producing similar symptoms usually cause false alarms, while fault propagation scenarios produce alarm floods which will overwhelm critical alarms. A two-level intelligent alarm management framework (IAMF) is proposed considering fault interdependence in plant operation, including alarm filtering first and root-cause diagnosis second. The two-level IAMF with different strategies are applicable to various hazard scenarios involving multi-fault with similar symptoms and propagation scenarios. Two cases are studied applying the IAMF to FCCU, in which the root causes of alarm floods can be identified. Redundant alarms, false alarms and alarm failures cut down effectively, thus ensuring the safety of the petrochemical process and reducing economic losses caused by improper alarms.

1. Introduction

Complex systems widely used in the process industry pose considerable challenges to their proper design, control, safety and management for smooth operation over their life cycles. Modern chemical plants consist of a large number of integrated and interlinked units. Their scale, nonlinearities, interconnectedness, and interactions with humans and the environment can make these complex systems fragile, when the cumulative effects of multiple abnormalities propagate in numerous ways to cause systemic failures (Zhang and Hu, 2013). Abnormal situations may result in process variables deviating from their designed ranges and potential undesired outcomes, even serious consequence, such as considerable economic impacts on plant profitability due to unacceptable product quality, plant shutdown, or even loss of lives.

Alarming is a critical function of the industrial automation in abnormal situation management for safe operation. In the cases of the explosion in the BP Texas City refinery, "13/11" Jilin petrochemical explosion, "16/7" Dalian oil pipeline explosion, and "11/6" Penglai 19-3 oil spill (these numbers indicate the date when these accidents happened), investigations of these disasters have shown that poor design of the alarm system led the process from potential hazards to catastrophic failures. As process units are highly interlinked, deviations due to an abnormal situation could propagate through various process units and numerous variables, leading to many alarms occurring at the same time.

Out of all the alarms, only one or two are root alarms. In other words, most of them are merely "effect" or "phantom" alarms (Leung and Romagnoli, 1999). "Effect" alarms are caused by the interactions between process variables. Abnormality in one variable can propagate, causing abnormality of another variable downstream. "Phantom" alarms are "effect" alarms that occur some time after the "root" alarms with a time delay. An abnormality in one variable may take minutes, or even hours, to propagate to another downstream variable. This delay-effect propagation will continue even after the upstream variable has been restored to its normal operating range. Alarm filtering and fault diagnosis are tasks of interpreting alarms from the control systems. They involve filtering all the effect alarms, locating the root alarms and thus identifying the root cause of the abnormality.

The operators have to pay close attention to the barrage of alarms, quickly and accurately identify the root cause of the abnormal situation, and take corrective actions according to the root cause and bring the process back under control (Adhitya et al., 2014). Process modeling and fault detection are important for solving the pressing problem of alarm flooding (Pasman and Rogers, 2014). In order to make reasonable maintenance decisions, one would like to know the cause of the abnormal situation. Due to process disturbances propagating through a plant, the cause can be quite distant from the position where the alarm is set off.

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

http://dx.doi.org/10.1016/j.ssci.2015.10.005
0925-7535/

One of the important challenges in effective real-time process alarm management is to implement intelligent systems that can assist process operators in making supervisory control decisions, instead of simply sounding an alarm when process variables go out of range (Gupta et al., 2013). According to Leveson (2015), there are always warning signs before a major accident. That is, most major accidents have multiple precursors and cues. Thus, there is a need to develop a reliable alarm management system that enables the operators to quickly and correctly diagnose the root causes of the abnormal situation and take suitable corrective actions.

In this paper, with the goal of avoiding the progression of the process to emergency shutdown, a two-level intelligent alarm management framework (IAMF) has been developed with alarm filtering and root cause diagnosis of the abnormal situation. The latter is the major function which will help operators to fully understand the causality via the actual hidden state of the process and the phenomena that occur at various locations, identify the causes that lead to the abnormal situations, and take all possible safety measures to cope with the situation. The application of the strategy is demonstrated with two case studies on the FCCU system. The results from case studies demonstrate the effectiveness of the strategies of IAMF for the safe and stable operation of a plant.

The rest of the paper is organized as follows. Section 2 presents a review of alarm management systems with alarm filtering and fault diagnosis in petrochemical plants. In Section 3, the first level of alarm management (alarm filtering) is illustrated with detailed calculation algorithms and workflows in order to help effective operation in practice. In Section 4, the second-level of alarm management (root-cause diagnosis) is presented. Then two hazard scenarios are developed in case studies in Section 5, and IAMF is applied to demonstrate its effectiveness. A comparison with traditional alarm system in DCS is also presented followed by conclusions with suggestions on future work in Section 6.

2. Literature review

An alarm system is critical to safety management in the process industry by preventing an abnormal situation from escalating and minimizing frequencies of activating safety instrumented system (SIS), such as a trip or an emergency shutdown device (ESD). As sustainable development is pursued by modern process industries, the demand for a more advanced, safe and effective alarm management system is desired. Modern chemical processes are usually equipped with distributed control systems (DCSs) to ensure safe operation and high product quality. Typically within a DCS, an alarm system is installed and maintained, in which high/low and/or high–high/low–low alarms are often configured for important process variables so that operators can maintain variables within their defined operating limits, i.e., alarm thresholds, to optimize operation performance. When a variable deviates from the limit, an alarm is set off and the operators are notified that an abnormal event would happen. Generally, alarm thresholds are carefully determined during the operation of plants. Unreasonably assigned thresholds may result in frequent false alarms or alarm failures.

On the other hand, due to the material, energy and information flow in a plant, single disturbance can cause multiple alarms, and the alarm messages may overload the operator by presenting many redundant alarms, which is called "alarm flooding". In such situations, the operator may fail to keep the plant within safe operation limits and find the root cause of the disturbance.

So alarm management in a plant has been a key safety issue because of disasters caused by false alarms and alarm failures or even alarm flooding which cause critical alarms overwhelmed. This is the strategy and situation of the traditional alarm management systems, where alarm thresholds are designed for a single steady operation state. When a petrochemical plant is in an abnormal state, an alarm system must provide useful information to operators. Unfortunately in complex hazard scenarios, multiple faults, cascading faults and fault propagating phenomenon exist. In such situations false alarms and alarm failures or even alarm floods make it hard for operators to detect the main causes of the abnormal events and fail to handle the root cause in time.

Therefore, alarm management has recently attracted a lot of attention among researchers to improve the alarm accuracy. The main points in the alarm management can be classified as two levels (as Fig. 1). The first and direct level is alarm filtering, which is the most basic and used to reduce false alarms, without missing any true alarm. The second and indirect level is root-cause diagnosis, which is more important and imperative because a trivial fault could propagate to cause costly damages to the entire system. The root cause deduced at the second level can be usually considered as the initial event, while in the safety management background, the root cause usually refers to social and cultural problem. Therefore in this paper, the root cause is identified as the initial event in the abnormal situation.

For the alarm management mission at the first-level (alarm filtering), there exist lots of related studies across the world. Zhu et al. (2014) proposes a strategy to control alarm floods for chemical process transitions. In this strategy, the artificial immune system-based fault diagnosis (AISFD) method and a Bayesian-estimation-based dynamic alarm management (BEDAM) method are integrated to generate useful alarms in fault situations. Brooks et al. (2004) proposes a new mathematical treatment of alarms that considers them as multi-variable interactions between process variables to calculate values for alarm limits. It helps to reduce substantial false alarms, and integrates alarm management, process control and product quality control into a single mathematical framework. Chao and Liu (2004) proposes an alarm management framework for automated network fault identification, in which the concepts of redundant/ringleader alarms and innocent network elements are also introduced into the framework to obtain an effective diagnosis. Chang et al. (2011) addresses two main issues related to an alarm system: the reliability and the prioritization of the alarms. A multi-alert voting system based on sensor redundancy approach is proposed to improve the reliability. A quantitative risk-based alarm management approach is proposed to address the flooding issue. Yang et al. (2012) points out the problem of multivariate alarm analysis and rationalization is complex and important in the area of smart alarm management due to the interrelationships between variables. His work focuses on the technique of capturing and visualizing the correlation information to reduce the influence of missed, false, and chattering alarms. Schleburg et al. (2013) argues that if alarms are related to one another, those alarms should be grouped and presented as one alarm problem. In this way, an approach to reduce the number of alerts is presented to the operator, and a software prototype is developed to perform this reduction automatically.

Therefore alarm filtering is becoming more and more difficult for operators due to the complexity of process schematics and the interaction between various upstream and downstream variables (Leung and Romagnoli, 1999). There are three categories of problems to be handled, i.e. (1) false alarms due to sensor malfunction, signal transmission problem, or control logic errors; (2) alarm failures due to physical problems of condition monitoring system; (3) redundant alarms due to the interaction between various variables related to the same abnormal event. Existing studies have developed alarm systems successfully conquering one or two alarm filtering problems, but failed to address the three issues systematically. Another phenomenon that attracts more and more