A Method of Designing Plant Alarm System Based on First Alarm Alternative Signals for Each Assumed Plant Malfunction

K. Takeda, T. Hamaguchi, N. Kimura, and M. Noda

Faculty of Engineering, Shizuoka University, 3-5-1 Johoku Hamamatsu, 432-8561, Japan
Graduate School of Engineering, Nagoya Institute of Technology, Gokiso Showa-ku Nagoya, 466-8555, Japan
Faculty of Engineering, Kyushu University, 744 Motooka Fukuoka, 819-0395, Japan
Department of Chemical Engineering, Fukuoka University, 8-19-1 Nanakuma, Jonan-ku, Fukuoka, 814-0180, Japan

*Corresponding Author’s E-mail: tktaked@ipc.shizuoka.ac.jp

Abstract

When a chemical plant is abnormal state, an alarm system must provide useful information to operators as the second layer of independent protection layer. Therefore, a method of designing plant alarm system is important for plant safety. Because the plant is modified in the plant lifecycle, the alarm system for the plant should be properly managed through the plant lifecycle. To manage the changes, the design rationales of alarm system should be explained explicitly. This paper investigates logical and systematic alarm system design method that explicitly explain design rationales from know-why information for proper management of change through the plant lifecycle. In the method, the modules proposed by Hamaguchi et al. (2011) to assign fault origin to be distinguished are extended. Using modules to investigate the sets of alarm sensors and the alarm threshold setting, an alarm system design method is proposed. Using the two types of modules and the set of fault origins to be distinguished by alarm system, we try to explicitly explain the design rationales of the alarm system.

Keywords: First Alarm; Plant Alarm System Design; Cause-Effect Model; Alarm Management; Plant Alarm Malfunction.

1. Introduction

For a chemical plant safety, independent protection layer (called IPL) has been proposed (CCPS, 2001). When the plant is abnormal state, an alarm system must provide useful information to operators as the second layer of IPL. Because the modification of the plant is happened in the plant lifecycle, the alarm system for the plant should be properly managed through the plant lifecycle. A framework to manage the alarm system lifecycle has been proposed (ISA, 2009). If the alarm system was designed without enough assessment using design rationales, the alarm system may not properly work as a part of IPL when the plant is abnormal state. Then, the alarm system cannot prevent the plant from accidents or disasters.
Although many papers have proposed alarm system design method, there is no systematic design method to explicitly provide whole design rationales. Hence, the useful design method has been required for this problem.

2. Alarm System Design Problem

To support safe operation, an alarm system is required to early detect an abnormal state of a plant and alert to operators. An objective alarm system should distinguish significant fault origins at objective early abnormal state. For example, the operators assumes that the fault origins of abnormal state may be a leakage from the pipe or a decrease of source pressure. If the real fault origin is a leakage from the pipe, to open a valve as the countermeasure for a decrease of source pressure will be lead a disaster. To implement a suitable countermeasure, these fault origins should be distinguished by the alarm system. In this paper, a set of fault origins to be distinguished by the alarm system is called C. The alarm system design problem consists of following sub problems.

Sub problem 1: Selection of the set C.
Sub problem 2: Selection of the set of alarm sensors to distinguish the set C.
Sub problem 3: Setting of the thresholds of the alarm sensors to alert.

Takeda et al. (2010) assume that the thresholds of the alarm sensors are properly set and the status (normal or abnormal) of process variables can be observed. They have proposed design method to search the sets of alarm sensors to logically distinguish the set C using abnormal status patterns of the sets of alarm sensors, a CE (cause-effect) model and the rule of propagation of fault on the model. Abnormal status pattern contains abnormal status of one or more alarm sensors. The CE model represents cause-effect relationships between process variables. They assume that the order of detection time of abnormal status of alarm sensors is unreliable. Therefore, the method may reject the set of alarm sensors which is able to distinguish the set C using the order of detection time of abnormal status of alarm sensors.

Kato et al. (2011) have proposed design method to reject the set of alarm sensors which cannot distinguish the set C even if the detection order is available. However, the thresholds are hard to set to satisfy the detection order of all alarm sensors as correct fault propagation paths.

At the alarm system design, if a set of alarm sensors cannot be found to distinguish the set C, then decision making will be needed whether adding sensors or using other method to distinguish the set C. The proposed methods cannot provide the design rationales for the decision making at the alarm system design, although the methods present the results of distinguishability of the set C.

To provide the design rationales, Hamaguchi et al. (2011) have proposed a module using the CE model and allocation of sensors to assign at most one fault origin of the set C. They also assume that the detection order of alarm sensors is unreliable. Therefore, a loop of the CE model becomes one module, even if the loop contains one or more alarm sensors.

This paper investigates logical and systematic alarm system design method that explicitly explain design rationales from know-why information for proper management of change through the plant lifecycle. Approaches of modules using the CE model and allocation of sensors proposed by Hamaguchi et al. (2011) are useful to explicitly explain design rationales. In this paper, the modules proposed by Hamaguchi et al. (2011) to assign fault origin to be distinguished are extended. Using modules to
investigate the sets of alarm sensors and the alarm threshold setting, an alarm system design method is proposed. Using the two types of modules and the set of fault origins to be distinguished by alarm system, we try to explicitly explain the design rationales of the alarm system. This paper assumes following conditions for alarm system design.

1) Operation states of objective plant can be estimated. Cause-effect relationships between process variables in the operation states can be represented as a CE (Cause-Effect) model, which is constructed by nodes and arcs.
2) Only one of the fault origins to be distinguished by the alarm system can be occurred simultaneously. A set of fault origins to be distinguished is obtained by use of process hazard analysis such as HAZOP (Hazard and operability) study.
3) The fault origins to be distinguished can be assigned one by one to pairs of nodes and their signs of the CE model. The nodes represent process variables. One fault origin can be assigned to one pair at most, because the fault origins cannot be distinguished when two or more fault origins are assigned to a pair.
4) Abnormal status of upper node can propagate to lower nodes only by path of CE model. Only the propagated nodes are abnormal status. The other nodes, that are not propagated, should not be abnormal status.
5) At alarm system design, known existing sensors are initially available to the set of alarm sensors.
6) When the set C cannot be distinguished by any sets of existing sensors, an approach to add new sensors is conceivable. But the approach is out of scope of this paper.

3. Explicit Design Rationales Using Modules to Assign Fault Origins of the set C

3.1. CE model
An example plant and a CE model corresponding to the example plant are shown in Figure 1(a) and Figure 1(b). Nodes of the CE model represent process variables, and arcs represent cause and effect relationships between nodes. The arcs are solid for positive influences and broken for negative influences. Sensor nodes to be available for the set of alarm sensors are double circles in this paper.
A general CE model can be constructed from combinations of four basic components (straight, combine, branch and strongly connected) as shown in Figure 2. This paper investigates design method of modules to assign fault origin of the set C using the basic components. The modules consist of measured primitive group units and unmeasured primitive group units.

![Figure 1. Example plant and CE model.](image-url)
3.2. Basic Design Method of Modules to Assign Fault Origins of the set C

In this paper, a measured primitive group unit means upstream nodes from a sensor node before another sensor node or to an uppermost node. In case of a sensor node and an uppermost node, the node is a measured primitive group unit. Unmeasured primitive group unit means upstream nodes from a lowermost unmeasured node before a sensor node or to an uppermost node. In each measured primitive group unit, fault propagation can be detected, but which node occurs fault cannot be distinguished. Thus, one fault origin at most to be distinguished should be assigned to the measured primitive group unit. In an unmeasured primitive group unit, fault propagation cannot be detected, because the unmeasured primitive group unit is lowermost and has no sensor node. Thus, no fault origin to be distinguished should be assigned to the unmeasured primitive group unit. This information is design rationales for above mentioned sub problem 1 and 2.

Design example of the modules to assign fault origin of the set C for a straight component is demonstrated in Figure 3. Sensor nodes are 3 and 5. The measured primitive group units are \{1,2,3\} and \{4,5\}. The unmeasured primitive group unit is \{6\}. For the measured primitive group unit \{1,2,3\}, when the sensor node 3 detects abnormal status, the node 1, 2 or 3 may be fault origin. But which node is fault origin cannot be distinguished. Thus, either of 1, 2 or 3 may be assigned a fault origin to be distinguished. For the measured primitive group unit \{4,5\}, the node 4 or 5 may be fault origin when the sensor node 3 represents normal state and the sensor node 5 detects abnormal status. But which node is fault origin cannot be distinguished. Thus, either of 4 or 5 may be assigned a fault origin to be distinguished. A fault occurred in unmeasured primitive group unit \{6\} cannot be detected. Thus, the node in the unmeasured group unit should not be assigned any fault origins to be distinguished.

The design method for the straight components can be easy to extend for the combine component or the branch component with measured junction node. For the branch component with unmeasured junction node, the measured and unmeasured primitive group units are needed to extend in following section.
3.3. Extension for the Branch Component with Unmeasured Junction Node

Definition of the unmeasured primitive group unit is extended that the unit means upstream nodes from a lowermost unmeasured node before a sensor node, to an uppermost node or before an unmeasured junction node. When two or more measured primitive group units share the nodes as shown in Figure 4, the nodes in the units are divided into shared nodes and unshared nodes. The junction node M has three output branches. Left branch is unmeasured primitive group unit. The other branches are part of respective measured primitive group unit. The nodes in the branches are the unshared nodes. The upper nodes from the junction node M are shared with two measured primitive group units and the shared nodes. One fault origin at most to be distinguished may be assigned to the unshared nodes of the measured primitive group unit.

Assignment a fault origin to the shared node means assignment the fault origin to all measured primitive group units sharing the node. Thus, one fault origin at most to be distinguished may be assign to whole of the measured primitive group units with the shared nodes.

![Figure 4. Extension for the branch component with unmeasured junction node.](image)

3.4. Modularize of Strongly Connected Component Using Merged Measured Primitive Group Unit

A CE model with straight and strongly connected components is shown in Figure 5(a). The nodes 2, 4 and 5 are sensor nodes. The CE model is divided into three measured primitive group units \{1,2\}, \{3,4\}, and \{5\}. The unit \{1, 2\} connects to the unit \{3,4\}, the unit \{3,4\} connects to the unit \{5\}, and the unit \{5\} connects to the unit \{1,2\}. The connections are based on the arcs. An alarm system design procedure is that the CE model is convert to the modules to assign fault origin of the set C and fault origins to be distinguished is assigned.

If there are units unassigned the fault origins to be distinguished in lower stream from an assigned unit, the units are merged into a measured group unit. The merging procedure is continuing until there is no unassigned unit. In Figure 5(b), it is assumed that the fault origins to be distinguished are assigned to the node 1 and 5 as f1 and f5 respectively. The unit \{3,4\} isn’t assigned the fault origins. The unit \{1,2\} and \{3,4\} are merged into a measured group unit \{1,2,3,4\}. The unit \{5\} is a measured group unit \{5\}. It is assumed that the first detected alarm sensor is identified after fault propagation is widely spread.

The alarm sensors in each measured group unit are first alarm alternative signals to distinguish the fault origin in the unit. Thresholds of any first alarm alternative signals of the unit are set to detect abnormal state earlier than the alarm sensors of the other units.
The measured primitive group unit is a module to explicitly describe the condition that a fault origin at most to be distinguished in the unit can be distinguished. On the other hand, the measured group unit is a module to investigate the sets of alarm sensors and the alarm threshold setting after assignment of the fault origins to be distinguished. Using the measured group units, the strongly connected components are modularized. In Figure 5(b), the node 2 or 4 suffices to be detected earlier than the node 5 when the fault f1 occurred. The node 5 suffices to be detected earlier than the nodes 2 and 4 when the fault f5 occurred. The threshold setting for the detection is easier than that the order of detection time of all alarm sensors follows the order of fault propagation on the CE model. The progress and results information is design rationales for above mentioned sub problem 3.

![Figure 5. Measured group units for strongly connected component.](image)

4. Conclusion

This paper investigated logical and systematic alarm system design method that explicitly explains design rationales from know-why information for proper management of change through the plant lifecycle. In the method, the modules proposed by Hamaguchi et al. (2011) to assign fault origin to be distinguished were extended to modularize the branch and strongly connected components. The modules are constructed using the nodes connections and allocation of sensors of CE model. Using the modules to investigate the sets of alarm sensors and the alarm threshold setting after assignment of the fault origins to be distinguished, an alarm system design method was proposed to moderate the requirement about the order of detection time proposed by Kato et al. (2011). Using the two types of modules and the set of fault origins to be distinguished by alarm system, we tried to explicitly explain the design rationales of the alarm system.

References

CCPS, 2001, Layer of Protection Analysis, New York; American Institute of Chemical Engineers, Center For Chemical Process Safety