Abstract

Support is required for operator activity in the correcting abnormalities in chemical plants. A plant alarm system must provide useful information to operators as the third layer of the Independent Protection Layers. Therefore, a method for designing a plant alarm system is important for plant safety. Because plants are modified throughout their plant lifecycles, any alarm systems need to be properly managed throughout the plant lifecycles. To manage the changes, the design rationale of the alarm system should be explained explicitly. Takeda et al. (2013) [3] proposed a logical and systematic alarm system design method that explicitly explains design rationales from know-why information for appropriate management of change throughout the plant lifecycle. For the combined or branched component of a cause-effect (CE) model, multiple alternative modules have been proposed. We propose a method of generating alternative modules for a plant alarm system based on first-out alarm alternative signals for the combined or branched component of a CE model.

1. Introduction

In most chemical plants, a distributed control system (DCS) is installed to keep the process variables stable. In these plants, the main role of the operators is to supervise plant operations by using process alarms, both normal and abnormal. The DCS is an effective means of decreasing the operator’s load of normal operation, and the number of operators has recently decreased due to the introduction of advanced control systems. Although the frequency of accidents is very low, the load of an operator in an abnormal state has become
heavier. When critical alarms are generated, operators face difficult tasks including complex decision making for detection, diagnosis, assessment of urgency, and countermeasure planning. In abnormal states, the DCS is not effective because of its lack of diagnosis systems or decision-support systems to prevent accidents or disasters. Therefore, a plant alarm system is very important to support safe operation. The Independent Protection Layers (IPLs) has been proposed (CCPS, 2001) [1]. When the plant is in an abnormal state, an alarm system consisting of critical alarms must provide useful information to operators as the third layer of the IPLs. Because plant modifications occur in the plant lifecycle, the plant alarm system needs to be properly managed throughout plant lifecycle. A framework and first-out alarm to manage the alarm system lifecycle has been proposed (ISA, 2009) [2]. The first-out alarm is defined as an alarm determined (i.e., by first-out logic) to be the first, in a multiple-alarm scenario. If an alarm system has been designed without sufficient assessment using design rationales, the alarm system may not properly work as a part of the IPLs when the plant is in an abnormal state. This is obviously problematic because it means that the alarm system cannot prevent accidents or disasters from occurring in the plant.

Although many researchers have proposed methods for designing alarm systems, there are few systematic design methods that explicitly provide entire design rationales. A useful design method is required.

2. Alarm System Design Problem

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

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

In this paper, we assume the following six conditions for alarm system design.

1) Operation modes of plant can be estimated, such as steady state, start up, Shutdown, or abnormal state operation. Cause-effect relationships between state variables such as process variables and manipulated variables in the operation modes can be represented by a cause-effect (CE) model constructed of nodes and arcs.

2) Only one of the fault origins to be distinguished by the alarm system can occur simultaneously. The set of fault origins to be distinguished is obtained by use of process hazard analysis such as a hazard and operability study (HAZOP).

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 state variables. One fault origin can be assigned to one pair at most, since the fault origins cannot be distinguished when two or more fault origins are assigned to a pair.

4) Abnormal status of the upper node, such as high, low, and no level, can propagate to lower nodes only by the path of the CE model. Only the propagated nodes have an abnormal status. The other nodes, which are not propagated, should not have an abnormal status.

5) At the alarm system design, known existing sensors are initially available as the set of alarm sensors.
6) When set C cannot be distinguished by any sets of existing sensors, an approach to add new sensors is conceivable. However, such an approach is outside the scope of this paper.

An example CE model to demonstrate the alarm system design problem is shown in Figure 1. Nodes of the CE model represent state variables and the arcs represent cause and effect relationships between nodes. The arcs are solid for positive influences and broken for negative influences. Sensor nodes available for the set of alarm sensors are represented by double circles. An abnormal status pattern contains the abnormal status of one or more alarm sensors. In this example, the fault origins to be distinguished are nodes f1 and f5. Nodes 4 and 6 are sensor nodes and nodes f1, 2, 3, and f5 are unmeasured nodes.

For example, assume that sensor node 4 is normal and sensor node 6 is abnormal. If transient fault propagation is assumed, nodes f1 and f5 are candidate fault origins in this fault propagation state. The fault origins cannot be distinguished. On the other hand, if the fault propagation is assumed to be widely spread, the candidate fault origin is node f5. Node f1 is not a candidate in this fault propagation state. The alarm system should be able to distinguish set C in any fault propagation state. Therefore, a systematic method is required to logically design an alarm system that can distinguish set C in any fault propagation state.

![Fig. 1. Example CE model to explain the alarm system design problem.](image-url)

Takeda et al. (2010) [3] assume that the thresholds of the alarm sensors are properly set and the status (normal or abnormal) of state variables can be observed. They have proposed a design method that searches sets of alarm sensors to logically distinguish set C using abnormal status patterns of the sets of alarm sensors, a CE model, and the rule of propagation of fault on the model. They assume that the order of detection time of the abnormal status of alarm sensors is unreliable. Therefore, the method may unintentionally reject the set of alarm sensors that is able to distinguish set C.

Kato et al. (2011) [4] proposed a design method that rejects the set of alarm sensors that cannot distinguish set C even if the detection order is available. However, the thresholds are difficult 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 that can distinguish set C is not found, a decision must be made about whether to add sensors or to use another method to distinguish set C. The methods above cannot provide any design rationale for decision making at the alarm system design, although they can present the results of the distinguishability of set C.

To provide design rationale, Hamaguchi et al. (2011) [5] proposed a module using the CE model and allocation of sensors to assign at most one fault origin of 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.
Takeda et al. (2013) [6] extended the module and proposed a logical and systematic alarm system design method that explicitly explains the design rationale from know-why information for the proper management of changes throughout a plant lifecycle. Using the two types of modules and the set of fault origins to be distinguished by the alarm system, they try to explicitly explain the design rationale of the alarm system. For a combined or branched component of a CE model, multiple alternative modules may be proposed. Therefore, proper modules among the alternatives need to be fully selected.

In this paper, we propose a method of generating full alternative proper modules for the combined or branched component of a CE model for designing an alarm system that can distinguish set C.

3. Explicit Design Rationale Using Modules to Assign Fault Origins of Set C

3.1. Basic Components of CE model

A general CE model can be constructed from combinations of four basic components (straight, combined, branched, and strongly connected), as shown in Figure 2. In this study, we propose how to design modules that can assign the fault origin of set C using the basic components. The modules consist of measured primitive group units and unmeasured primitive group units.

![Figure 2. Basic components.](image)

3.2. Basic Method of Proposed Alarm System Design based on a CE Model and Modules

In this paper, a measured primitive group unit means upstream nodes from a sensor node prior to another sensor node or to an uppermost node.

In the case an uppermost node is a sensor node, then the upper most node is a measured primitive group unit. Unmeasured primitive group unit means upstream nodes from a lowermost unmeasured node prior to a sensor node or to an uppermost node. In each measured primitive group unit, fault propagation can be detected, but which node causes the 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 needs to be assigned to the unmeasured primitive group unit. This information functions as the design rationale for sub problems 1 and 2 (mentioned above).
A design example of the modules to assign the fault origin of set C for a straight component is shown in Figure 3.

Step 1: A CE model is generated for a plant. Available sensor nodes for the alarm system are 2, 4, and 5.

Step 2: The measured primitive group units enclosed by solid lines are \{1, 2\}, \{3, 4\}, and \{5\}. The unmeasured primitive group unit enclosed by a broken line is \{6\}.

Step 3: For the measured primitive group unit \{1, 2\}, when sensor node 2 detects an abnormal status, node 1 or 2 is the fault origin. However, which node is the fault origin cannot be distinguished. Thus, either 1 or 2 can be assigned the fault origin to be distinguished. For the measured primitive group unit \{3, 4\}, node 3 or 4 is the fault origin when sensor node 2 represents a normal state and sensor node 4 detects an abnormal status. However, which node is the fault origin cannot be distinguished. Thus, either 3 or 4 can be assigned the fault origin to be distinguished. For the measured primitive group unit \{5\}, node 5 is the fault origin when sensor nodes 2 and 4 represent a normal state and sensor node 5 detects an abnormal status. Any fault that occurs in the 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. In this case, nodes 1 and 5 (named f1 and f5) are assigned each fault origin to be distinguished.

Step 4: If there are any units that are unassigned to fault origins to be distinguished in the lower stream from an assigned unit, the units are merged into a measured group unit. The merging procedure is continued until there are no unassigned units left. For fault origin f1, sensor nodes 2 and 4 can be used. These nodes can be detected earlier than node 5 when fault origin f1 occurs, and node 5 can be detected earlier than nodes 2 and 4 when fault origin f5 occurs. The threshold setting for detection is easier than when the order of detection time of all alarm sensors follows the order of fault propagation in the CE model. The progress and results information functions as the design rationale for sub problem 3 (mentioned above).

3.3. Extension for the Branched Component

The above steps can be easily extended for the branched component with a measured junction node, as shown in Figure 4.
For the branched component with an unmeasured junction node, the process is a little more complicated, but the measured and unmeasured primitive group units can be extended as follows.

When two or more measured primitive group units share nodes, as shown in Figure 5, the nodes in the units are divided into shared nodes and unshared nodes. Junction node 2 has two output branches, \{3, 4\} and \{5, 6\}, that are part of respective measured primitive group units. The nodes in the branches are the unshared nodes. The upper nodes from junction node 2 are shared with two measured primitive group units and the shared nodes. One fault origin at most to be distinguished can be assigned to the unshared nodes of the measured primitive group unit.

Assigning a fault origin to the shared nodes means assigning a fault origin to all measured primitive group units sharing the node. Thus, one fault origin at most to be distinguished can be assigned to the whole of a measured primitive group unit with shared nodes.
3.4. Extension for Combined Component

For a combined component, the measured primitive group units and the measured group units with the junction node can be generated by the above steps, as shown in Figure 6.

![Diagram showing the extension for combined component](image)

**Fig. 6. Unique measured group units.**

When multiple measured primitive group units with fault origins exist in the upper stream of the junction node, as shown at step 3 in Figure 7, the corresponding measured group units cannot be unique by the structure of the CE model, as shown at steps 4(a)–(b). Although properly measured group units should be selected from among the multiple patterns of measured group units to design an alarm system, the selection process, which ideally should use qualitative and/or quantitative information, is outside the scope of this paper.

![Diagram showing multiple patterns of measured group units](image)

**Fig. 7. Multiple patterns of measured group units.**
4. Conclusion

In this paper, we specified one of the problems in alarm system design: the need for a systematic method to logically design an alarm system that can distinguish set C in any fault propagation state. We proposed measured group units for the combined or branched component of a CE model to distinguish set C in any fault propagation state. For the branched component, a method of generating measured group units for the straight component can be easily extended. For the combined component, when multiple measured primitive group units with fault origins exist in the upper stream of the junction node, the corresponding measured group units cannot be unique by structure of the CE model. Properly measured group units should be selected using qualitative and/or quantitative information from the multiple patterns of measured group units in the design of an alarm system. A method of selecting the proper measured group units will be required.

Acknowledgements

This work was supported by JSPS KAKENHI Grant Number 24310119.

References

[1] CCPS, 2001, Layer of Protection Analysis, New York; American Institute of Chemical Engineers, Center For Chemical Process Safety
[2] ISA, 2009, Management of Alarm Systems for the Process Industries, North Carolina
[3] Takeda K., Hamaguchi T. and Noda M., 2010, Plant Alarm System Design based on Cause-Effect Model, Kagaku Kogaku Ronbunshu, 36, 2, 136—142
[4] Kato M., Takeda K., Noda M., Kikuchi Y. and Hirao M., 2011, “Design Method of Alarm System for Identifying Possible Malfunctions in a Plant Based on Cause-Effect Model,” 11th Int. Sympo. PSE
[5] Hamaguchi T., Takeda K., Noda M. and Kimura N., 2011, “A Method of Designing Plant Alarm Systems with Hierarchical Cause-Effect Model,” 11th Int. Sympo. PSE
[6] Takeda K., Hamaguchi T., Kimura N. and Noda M., 2013, “A Method of Designing Plant Alarm System Based on First Alarm Alternative Signals for Each Assumed Plant Malfunction,” 6th Int. Conf. PSE