A Method for Generation and Check of Alarm Configurations Using Cause-Effect Matrices for Plant Alarm System Design

Takashi Hamaguchi[1(✉)], B. Mondori[1], Kazuhiro Takeda[2],
Naoki Kimura[3], and Masaru Noda[4]

[1] Graduate School of Engineering, Nagoya Institute of Technology,
Nagoya, Japan
hamachan@nitech.ac.jp
[2] Graduate School of Engineering, Shizuoka University, Shizuoka, Japan
tktaked@ipc.shizuoka.ac.jp
[3] Faculty of Engineering, Kyushu University, Fukuoka, Japan
nkimura@chem-eng.kyushu-u.ac.jp
[4] Department of Chemical Engineering, Fukuoka University, Fukuoka, Japan
mnoda@fukuoka-u.ac.jp

Abstract. An alarm system must provide useful information to operators as the third layer of an independent protection layer when a chemical plant is at abnormal situation. Therefore, a design method of a plant alarm system is important for plant safety. Because the plant is maintained in the plant lifecycle, the alarm system for the plant should be properly managed through the plant lifecycle. To manage changes, the design rationales of the alarm system should be explained explicitly. This paper investigates a logical and systematic alarm system design method that explicitly explains the design rationales from know-why information for proper management of changes through the plant lifecycle. In this paper, we propose a method for generation and check of alarm configurations using cause-effect matrices for plant alarm system design. The matrices are based on a cause-effect model and used for generation and check of alarm configurations.

Keywords: Plant alarm system design · Cause-effect matrices · Alarm management

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 situation 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 situations, 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.

2   Alarm Management Lifecycle

To support the safety of plant operations, the Independent Protection Layers has been proposed (CCPS, 2001) [1]. When the plant is in an abnormal situation, an alarm system consisting of critical alarms must provide useful information to operators. Because plant modifications occur in the plant lifecycle, the plant alarm system needs to be properly managed throughout plant lifecycle. A framework and first alarm to manage the alarm system lifecycle had been proposed (ISA, 2009) [2] and the revised illustration has been proposed in IEC 62682 (IEC, 2014) [3]. The alarm management lifecycle in IEC 62682 with our focused area in this paper is shown in Fig. 1.
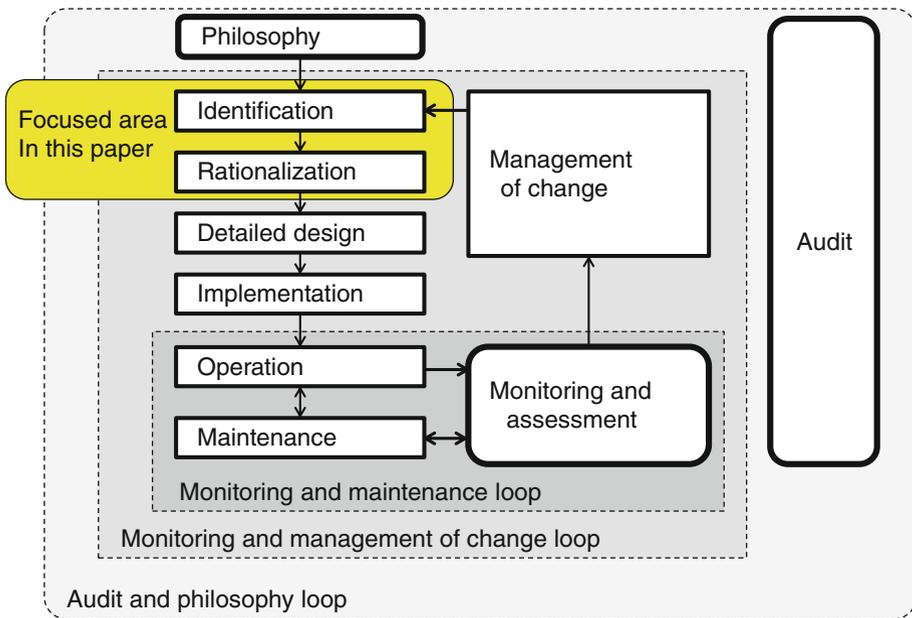

Fig. 1. Alarm management lifecycle in IEC 62682

3   Alarm System Design Using CE Matrices

3.1   CE Model

Operation modes of plant can be estimated, such as steady state, start up, shut-down, or abnormal situation 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. A CE model of example plant is shown in Fig. 2.
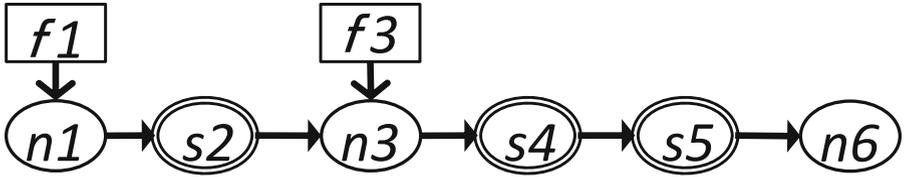

Fig. 2 CE model of example plant

The CE model is a diagram for the propagation of abnormalities that shows the propagation process for abnormalities after a fault has occurred. The CE model is based on the material and energy balances of the plant that could be constructed from the plant topology. The nodes in the model represent state variables in the plant. The arcs represent the directed influence between variables. Takeda et al. [4], Kato et al. [5], and Hamaguchi et al. [6] proposed some logical and systematic alarm system design based on CE model.

Let S be a set of all measured variables of state variables and s be the element of S. Double line nodes represent measured variables. Let N be a set of all unmeasured variables of state variables and n be the element of N. Single line nodes represent unmeasured variables. Let F be a set of all fault origins variable to be distinguished by alarm system and f be the element of F. Rectangle represent fault origins variables to be distinguished by alarm system.

3.2 CE Matrices

In this paper, we convert the CE model to CE matrices to generate the pairings between the fault origins variables F and measured variables S as alarm state triggers and check the qualitative adequacy as the alarm configurations by computer, automatically. The CE matrices have elements 0 or 1. Column variables and row variables correspond causes and effects, respectively. When the (i, j) element of the CE matrices are 1, the j-th column variable affects the i-th row variable.

3.3 CE Matrix G

A CE matrix G explains the plant model. The CE matrix G has rows and columns corresponding to the measured variables S, unmeasured variables N, and fault origins variables F.

The CE matrix G of the CE model in Fig. 2 is shown in Table 1. The "1" at the $(4, 7)$ element of Table 1 shows that the fault origins variable, $f1$, affects the unmeasured variable, $n1$.

Table 1. CE matrix G of the Plant

	Causes	S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
Effects	G	$s2$	$s4$	$s5$	$n1$	$n3$	$n6$	$f1$	$f3$
S:	$s2$	0	0	0	1	0	0	0	0
	$s4$	0	0	0	0	1	0	0	0
	$s5$	0	1	0	0	0	0	0	0
N:	$n1$	0	0	0	0	0	0	1	0
	$n3$	1	0	0	0	0	0	0	1
	$n6$	0	0	1	0	0	0	0	0
F:	$f1$	0	0	0	0	0	0	0	0
	$f3$	0	0	0	0	0	0	0	0

3.4   CE Matrix A

An alarm configuration 1 is shown in Fig. 3. The fault origin variables $f1$ and $f3$ are paired $s2$ and $s4$, respectively.
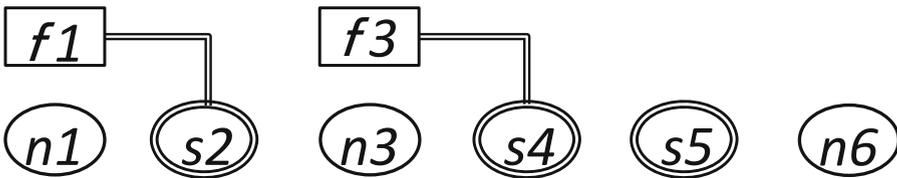

Fig. 3. Alarm configuration 1

A CE matrix A explains the alarm configurations. This CE matrix A can be generated automatically from unit matrix. Because each column variable of this CE matrix A always has only one "1". The CE matrix A can be generated easily to apply substitution of unit matrix.

The CE matrix A_1 of the alarm configuration 1 in Fig. 1 is shown in Table 2. The "1" at the (7, 1) element of Table 2 shows that the measured variable, s2, is used as an alarm sensor for the fault origins variable, $f1$.

3.5   CE Matrix GA

A CE model of the example plant with alarm configuration 1 is shown in Fig. 4. The propagations from alarm sensors, $s2$ and $s3$, are modified by alarm configuration1.

The alarm loop model GA_1, which explains the effect of the subset of C under the alarm configurations 1, is calculated by the Boolean multiplication of two matrices, G and A_1. The CE matrix GA_1 of the alarm loop model with alarm configuration 1 in Fig. 4 is shown in Table 3.

Table 2. CE matrix A_1 as alarm configuration 1

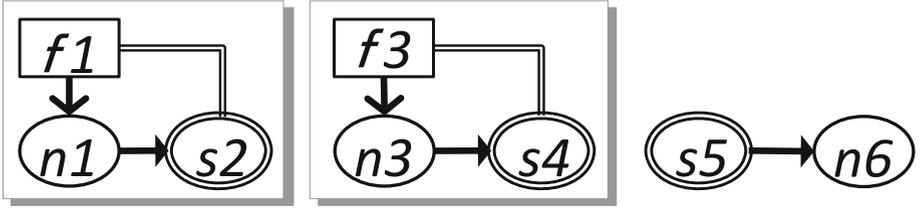| Causes		S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
Effects	A_1	s2	s4	s5	n1	n3	n6	f1	f3
S:	s2	0	0	0	0	0	0	0	0
	s4	0	0	0	0	0	0	0	0
	s5	0	0	1	0	0	0	0	0
N:	n1	0	0	0	1	0	0	0	0
	n3	0	0	0	0	1	0	0	0
	n6	0	0	0	0	0	1	0	0
F:	f1	1	0	0	0	0	0	1	0
	f3	0	1	0	0	0	0	0	1

Fig. 4. CE model of an example plant with alarm configuration 1

Table 3. CE matrix GA_1 of the alarm loop model with alarm configuration A_1

Causes		S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
Effects	GA_1	s2	s4	s5	n1	n3	n6	f1	f3
S:	s2	0	0	0	1	0	0	0	0
	s4	0	0	0	0	1	0	0	0
	s5	0	0	0	0	0	0	0	0
N:	n1	1	0	0	0	0	0	1	0
	n3	0	1	0	0	0	0	0	1
	n6	0	0	1	0	0	0	0	0
F:	f1	0	0	0	0	0	0	0	0
	f3	0	0	0	0	0	0	0	0

3.6 CE Matrix R

A reachability matrix R is defined by using GA as followed

$$R = \sum_{k=1}^{\infty} (GA)^k$$

If dimension of GA is n, the reachabity matrix R is defined as followed.

$$R = \sum_{k=1}^{n-1} (GA)^k$$

Using this method, result of the reachability matrix R_1 by GA_1 indicate the effect between variables under alarm configuration 1. The effect of fault origin $f1$ arrives at the alarm variables $s2$ and the alarm loop can work. The effect of fault origin $f3$ arrives at the alarm variables $s4$ and the alarm loop can work, too. The reachability matrix R_1 is shown in Table 4.

Table 4. Reachability matrix R_1 by GA_1

Effects \ Causes	R_1	S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
		$s2$	$s4$	$s5$	$n1$	$n3$	$n6$	$f1$	$f3$
S:	$s2$	1	0	0	1	0	0	1	0
	$s4$	0	1	0	0	1	0	0	1
	$s5$	0	0	0	0	0	0	0	0
N:	$n1$	1	0	0	1	0	0	1	0
	$n3$	0	1	0	0	1	0	0	1
	$n6$	0	0	1	0	0	0	0	0
F:	$f1$	0	0	0	0	0	0	0	0
	$f3$	0	0	0	0	0	0	0	0

3.7 Bad Alarm Configuration

Here, a bad alarm configuration 2 is explained. The alarm configuration 2 is shown in Fig. 5. The fault origin variables $f1$ and $f3$ are paired $s5$ and $s4$, respectively.
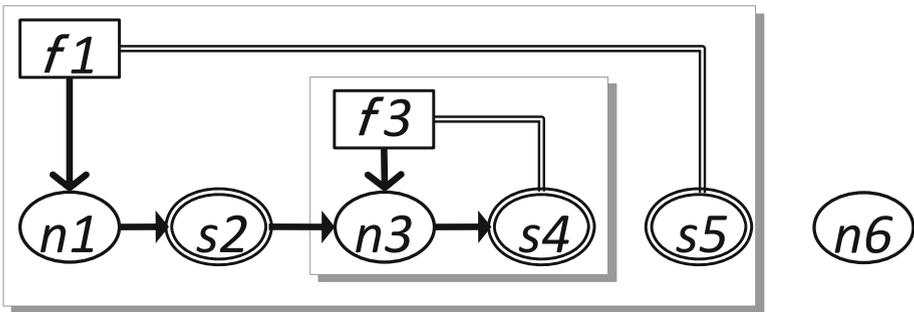

Fig. 5. A CE model of an example plant with alarm configuration 1

The CE matrix A_2 of the alarm configuration 2 in Fig. 5 is shown in Table 5.
The CE matrix GA_2 of the alarm loop model with alarm configuration 2 is shown in Table 6.

Table 5. CE matrix A_2 as alarm configuration 2

Causes	S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
A_2	s2	s4	s5	n1	n3	n6	f1	f3
s2	1	0	0	0	0	0	0	0
s4	0	0	0	0	0	0	0	0
s5	0	0	0	0	0	0	0	0
n1	0	0	0	1	0	0	0	0
n3	0	0	0	0	1	0	0	0
n6	0	0	0	0	0	1	0	0
f1	0	0	1	0	0	0	1	0
f3	0	1	0	0	0	0	0	1

Effects — S:, N:, F: (row groups)

Table 6. CE matrix GA_2 of alarm loop model with alarm configuration A_2

Causes	S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
GA_2	s2	s4	s5	n1	n3	n6	f1	f3
s2	0	0	0	1	0	0	0	0
s4	0	0	0	0	1	0	0	0
s5	0	0	0	0	0	0	0	0
n1	0	0	1	0	0	0	1	0
n3	1	1	0	0	0	0	0	1
n6	0	0	0	0	0	0	0	0
f1	0	0	0	0	0	0	0	0
f3	0	0	0	0	0	0	0	0

Effects — S:, N:, F: (row groups)

The reachability matrix R_1 by GA_2 is shown in Table 7. The effect of fault origin $f3$ arrives at the alarm variables $s4$ and the alarm loop can work. But, the effect of fault origin $f1$ doesn't arrive at the alarm variables $s5$. Therefore, the alarm configuration 2 is judged to a bad configuration.

Table 7. Reachability matrix R_2 of the Plant GA_2

Causes	S: Measured variables			N:Unmeasured variables			F:Fault origins variables	
R_2	s2	s4	s5	n1	n3	n6	f1	f3
s2	1	0	1	1	0	0	1	0
s4	1	1	1	1	1	0	1	1
s5	0	0	0	0	0	0	0	0
n1	0	0	1	0	0	0	1	0
n3	1	1	1	1	1	0	1	1
n6	0	0	0	0	0	0	0	0
f1	0	0	0	0	0	0	0	0
f3	0	0	0	0	0	0	0	0

Effects — S:, N:, F: (row groups)

4   Summary

In this paper, we propose a method for generation and check of alarm configurations using cause-effect matrices for plant alarm system design. The matrices are based on a CE model and used for generation and check of alarm configurations. The design algorithm can be the first step to bridge the discontinuity of plant alarm system design and alarm management.

References

1. CCPS, Layer of Protection Analysis, New York, American Institute of Chemical Engineers, Center for Chemical Process Safety (2001)
2. ISA, Management of Alarm Systems for the Process Industries, North Carolina (2009)
3. IEC, 62682 ed.01: Management of Alarm Systems for the Process Industries (2014)
4. Takeda, K., Hamaguchi, T., Noda, M.: Plant alarm system design based on cause-effect model. Kagaku Kogaku Ronbunshu **36**(2), 136–142 (2010)
5. Kato, M., Takeda, K., Noda, M., Kikuchi, Y., Hirao, M.: Design Method of Alarm System for Identifying Possible Malfunctions in a Plant Based on Cause-Effect Model. In: 11th International Symposium on PSE (2011)
6. Hamaguchi, T., Takeda, K., Noda, M., Kimura, N.: A Method of Designing Plant Alarm Systems with Hierarchical Cause-Effect Model. In: 11th International Symposium on PSE (2011)