Design Method of Plant Alarm Systems on the Basis of Two-Layer Cause-Effect Model

Kazuhiro Takeda[1], Annuar H. B. M. Aimi[1], Takashi Hamaguchi[2], Masaru Noda[3] and Naoki Kimura[4]

1 Department of Materials Science and Chemical Engineering, Shizuoka University, 3-5-1 Johoku, Naka-ku, Hamamatsu-shi, Shizuoka 432-8561 Japan
2 Graduate School of Engineering, Nagoya Institute of Technology, Gokiso-cho, Showa-ku, Nagoya-shi, Aichi 466-8555 Japan
3 Graduate School of Information Science, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma-shi, Nara 630-0192 Japan
4 Department of Chemical Engineering, Kyushu University, 744 Motooka, Nishi-ku, Fukuoka 819-0395 Japan
tktaked@ipc.shizuoka.ac.jp, hamachan@nitech.ac.jp, noda@is.naist.jp, nkimura@chem-eng.kyushu-u.ac.jp

Abstract. In the recent years, there has been an increase in the number of accidents involving chemical and industrial plants. In most of the cases, the inadequate performance of alarm system has become a significant cause of industrial incidents and serious accidents. In general, alarm systems design can be divided into two processes, which are selecting alarm source signal and determining alarm limit. Authors have proposed the alarm source signal selection method. In this paper, we would like to focus on how to determine alarm limit using statistical method and evaluate this alarm design method through study case.

Keywords: Plant Alarm System, Two-Layer Cause-Effect Model, Alarm Limit

1 Introduction

In the recent years, there has been an increase in the number of accidents involving chemical and industrial plants. In most of the cases, the inadequate performance of alarm system has become a significant cause of industrial incidents and serious accidents.

A poorly designed alarm may cause the event of a small incident turning into a more serious incident which led to major accident. For example, the Three Mile Island accident [1] that occurs in 1979 in Pennsylvania was a minor event that turns into major accident resulted from operator's confusion due to an alarm flood—too many alarms were activated at the same time on the operator's screen in the operator room at the time of the incident. From this incident, we can learn that alarm which was supposed to guide the operator on how to respond to upset in plant did not serve its purpose, backfired and caused confusion to the operator, which led to injury, loss of life, equipment and property damage, fines and harm to company reputation.

Therefore, in order to prevent such accident, better design of alarm is needed to detect fault or abnormality in plant, alert, inform and guide [2] [3] the operator during plant upset. In general, alarm systems design can be divided into two processes, which are selecting alarm source signal [4] [5] and determining alarm limit. In this paper, we would like to focus on how to determine alarm limit using statistical method and evaluate this alarm design method through study case.

Liu and Noda (2009) [6] proposed a human-model-based evaluation in which alarm limits are defined as 2% margin from a variable normal fluctuation range. According to Brooks, Thorpe and Wilson (2004) [7] there has been no general method available to calculate values for alarm limits either in single-or multi-variable cases and this is the root cause of the poor performance of alarm systems today and hence of the low regard in which operators hold them. According to Izadi et al. (2009) [8] alarm limits that are set close to instrument limits are used to protect the equipment and avoid hazardous situations. Alarm limits that are set at a certain confidence range are meant to keep the operation at normal and often optimal conditions.

2 Selection of Alarm Source Signals

Takeda et al. (2010) [4] [5] proposed an alarm source signal selection method based on a two-layer cause-effect model. The model represents the cause and effect relationships between the deviations of state variables, such as process variables and manipulated variables, from normal fluctuation ranges. It is represented by a directed graph, where two types of nodes are defined.

$i+$: Upward deviation of state variable i from normal fluctuation range
$i-$: Downward deviation of state variable i from normal fluctuation range

In the two-layer cause-effect model shown in Fig. 1, a single direction arrow links the deviation of a state variable and its affected state variable. The letters F and L indicate flow rate sensor and valve positions, respectively.

An evaluation method for plant alarm system derives the sets of the state variables with the direction of their deviation from the normal fluctuation range. The derived sets are theoretically guaranteed to be able to qualitatively distinguish all assumed malfunctions in a plant when alarm limits are adequately set to those state variables. In this study, to evaluate distinguishability of the derived sets, alarm limits are determined by statistical information.

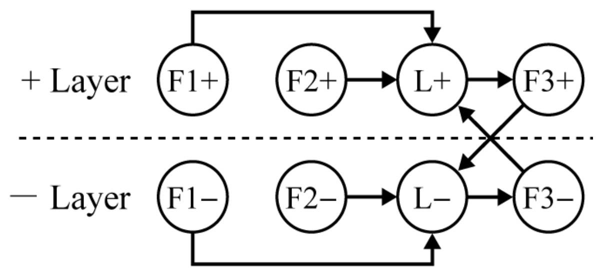

Fig. 1. Example of two-layer cause-effect model.

3 Alarm Limit Setting and Assumption of Abnormal State

3.1 Measured Value with Noise

In any chemical plant, data measured from instrument usually contains noise. The measured value is expressed by Eq. (1).

$$Xo = X + N \tag{1}$$

Where X is true value, N is noise and Xo is measured value. In this paper, it is assumed the noise as normal random noise. Using normal distribution theory in statistic, abnormal state data distribution is assumed to be a deviation of mean from the normal steady state data distribution. But, the variance of the abnormal state data distribution is assumed to be equal to that of the normal steady state data distribution (Fig. 2).

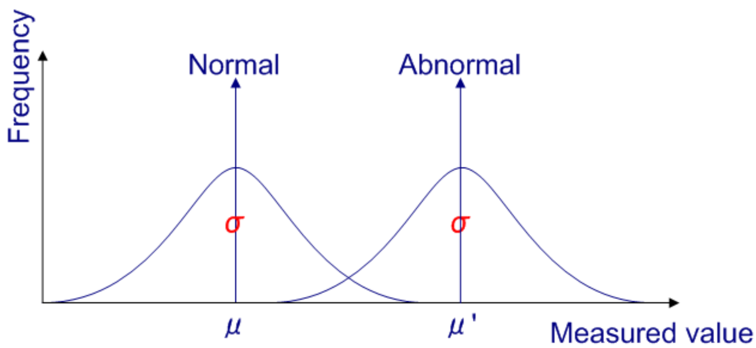

Fig. 2. Distributions with equal variance but difference means.

3.2 Alarm Limit Setting

To detect the abnormal high (or low) state, the high (or low) alarm limit is set. When measured value exceeds the high (or low) alarm limit, the alarm is woken up to inform operators that the plant is in abnormal state. The operators will diagnose the cause of the abnormal state and take countermeasure. The alarm limit should be determined not to generate undesired alarm. The undesired alarm means alarm generation in normal steady state, or missed alarm generation in abnormal state. The former is called false alarm, and the later is called missed alarm [8]. The undesired alarm constraint is usually expressed the number of times per month or day. From the number of alarm source signals in the plant and the sampling period of the alarm source signals, the concept of probability distribution and critical region is used to determine alarm limit. For a probability distribution, outside region of a value is called critical region. When there is one critical region at one side of a probability distribution, test using the region is called one-tail test. When there are two critical regions at both sides of a probability distribution, test using the two regions is called two-tail test.

Assume that there are N_a alarms in a plant, and these alarm source signals are sampled per S_p minute. All sampled values in a month at the plant are $60 \cdot 24 \cdot 30 \cdot N_a$ / S_p=43,200 N_a / S_p samples. Assume that false alarm should be under S_f times per month, and then each alarm source signal's critical region for one-tail test should be under S_f / (43,200 N_a / S_p). Alarm limit is determined to meet the critical region. Assume D_f as distance between the mean of normal steady state and alarm limit.

3.3 Abnormal State Data Distribution Model

On the other hand, assume that missed alarm should be under S_m times per month, and then each alarm source signal's critical region for one-tail test of abnormal state should be under S_m / (43,200 N_a / S_p). The mean of abnormal state should differ from alarm limits to meet the critical region. Assume D_m as distance between the mean of abnormal state and alarm limit. Then, to meet false alarm constraint and missed alarm constraint, the distance D_a between the mean of normal steady state and that of abnormal state should be over $D_f + D_m$.

3.4 Example

For example, assume that data distribution is normal distribution, N_a is 100, S_p is 1 minute, S_f is 3 times per month, and S_m is 5 times per day. It is assumed that S_f and S_m are desired for operators. During long normal state, operators may a few false alarms for a month. In abnormal state, operators may not allow missed alarm for short time. All sampled values in a month at the plant are 4.3e6 samples. The critical region for false alarm is 6.9e-7. Then D_f becomes about 5σ of the distribution as shown in Fig. 3. All sampled values in a day at the plant are 1.4e5 samples. The critical region for missed alarm is 3.5e-5. Then D_m becomes about 4σ of the distribution, and D_a becomes about 9σ.

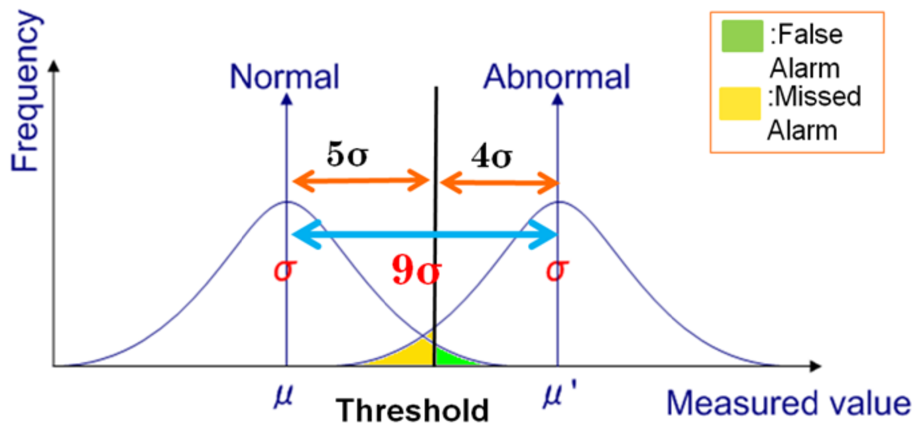

Fig. 3. Alarm limit and critical region.

4 Case Study

4.1 Example Plant and Plant Alarm System

The proposed plant alarm selections and limit settings are demonstrated through a case study that uses the two-tank system in Fig. 4 as an example plant. Product is fed to Tank 1 and transferred to Tank 2. A certain amount of the product is recycled to Tank 1 from Tank 2. The letters P, F, L, and V in Fig. 4 indicate pressure, flow rate and liquid level sensors, and valve positions, respectively. Each sensor's sampling period is 1 minute. There were 10 sensors. Variables to be set as alarms were 20.

In this example plant, five types of malfunctions are assumed to be distinguishable from the operation of the plant alarm system.

- Mal-1: High feed pressure
- Mal-2: Low feed pressure
- Mal-3: Blockage in recycle pipe
- Mal-4: Wrong valve operation of V4 open
- Mal-5: Wrong valve operation of V4 close

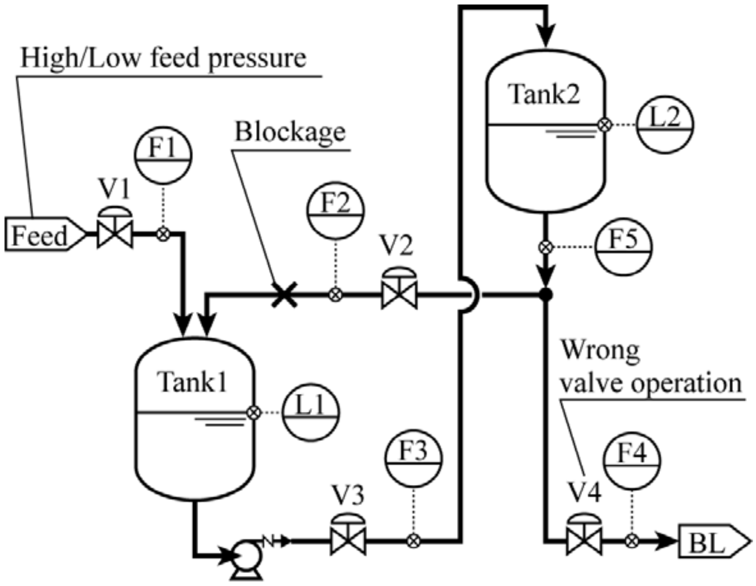

Fig. 4. Example plant of two-tank system.

For each malfunction, normal steady state was sampled for 10 minutes, and abnormal state was sampled for 590 minutes with normal distribution noise. Fig. 5 shows the two-layer cause-effect model of the example plant. To distinguish the above 5 malfunctions, 688 types of alarm source signals sets were selected by using of proposed algorithm. For demonstration, a set of all alarms from 10 source signals (F1+, F1-, F2+, F2-, F3+, F3-, F4+, F4-, L1+, L1-, L2+, L2-, V1+, V1-, V2+, V2-, V3+, V3-, V4+, V4-) and a minimum set of 6 alarms from 3 source signals (F1+, F1-, F4+, F4-, V4+, V4-) were selected among these sets. The limits for these alarms were set to submit following constraints.

- False alarm should be under 3 times per month.
- Missed alarm should be under 5 times per day.

To meet the above constraints, the limits were 5σ of the measured noise and the averages of assumed abnormal state were distanced 9σ from the average of steady state. These limits were decided by using above mentioned abnormal state data distribution model based on normal distribution. When the value of a state variable exceeded the corresponding alarm limit, the corresponding alarm was generated. Candidates of causes of alarms were estimated based on two-layer cause-effect model. The estimation is called fault diagnosis.

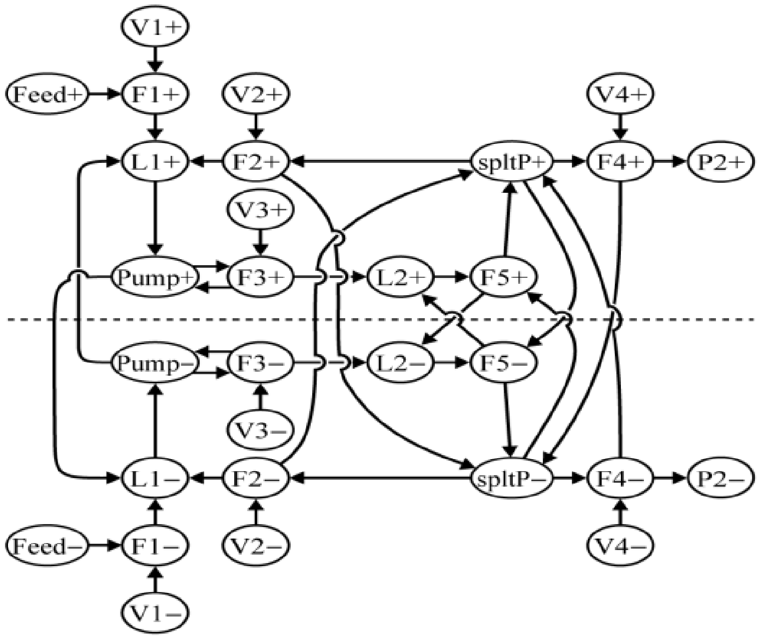

Fig. 5. Two-layer cause-effect model of example plant.

5 Results and discussion

The case for a set of all alarms is called case 1, and the case for a minimum set of 6 alarms is called case 2. Tables 1 and 2 show simulation results for each case, respectively. In these tables, FD means fault diagnosis.

5.1 Results for Generated Alarms

For each case, false alarm is not generated because of short steady state. For the beginning of abnormal state of Mal-3, missed alarm was generated because of process dynamics. Generated alarms were met assumed false alarm and missed alarm constraint. First alarms are summarized for each case. For case 1, Mal-4 and Mal-5 had 3 first alarms. For case 2, Mal-4 and Mal-5 had 2 first alarms. The other experiments had only 1 first alarm. Total number of alarms of case 2 was about 1/3 of that of case 1. For example, 3,258 alarms were generated from 10 source signals for Mal-1, whereas 1,061 alarms were generated from 3 source signals. By alarm selection, many waste alarms were eliminated. First alarm is very important information to aware operators as early as possible. Except Mal-3, first alarm time was 11 minutes for case 1 and 2. These results means that case 2 didn't exclude important alarms except Mal-3.

5.2 Results for Fault Diagnosis

Fault diagnosis results for generated alarms were almost identified the occurred malfunctions. Candidates of Tables 1 and 2 mean candidates of cause of abnormal state. The candidates were selected from assumed malfunctions using consistency among malfunctions and alarms. For example, 590 identified fault diagnosis were equal to 590 sampling for the abnormal state of almost experimental. Exceptionally, for first 9 alarms of Mal-3 of case 1, it was impossible to diagnose fault of candidates using generated alarms. The first 9 alarms were inconsistent because of process dynamics. Thus, more alarm variables led more difficulty of adequate alarm limit setting. For case 2, all selected alarms were consistent. Especially, for Mal-3, first FD of case 2 was earlier than that of case 1. For Mal-4 of case 1 and 2, incorrect 9 alarms were generated by process simulator problem, then it was impossible to diagnose fault of candidates using these alarms. These results show that diagnostic distinguishability by alarm selection was almost equal to that by all alarm source signals.

Table 1. Simulation result for a set of all alarms.

	First alarm		Total Alarm		First FD		Total FD	
Malfunctions	Source signals	Time [min]	Source signals	Counts	Candidates	Time [min]	Identified	Impossible
Mal−1	F1+	11	F1+, F2+, F3+, F4+, L1+, L2+	3258	P1[+]	11	590	
Mal−2	F1−	11	F2−, F2−, F3−, F4−, L1−, L2−	3272	P1[−]	11	590	
Mal−3	F2−	11	F2−, F3−, F4+, L1−, L2+	2909	F2[−]	20	581	9
Mal−4	F4+, V4+, L2−	11	F2−, F3−, F4+, F4−, L1−, L2−, V4+	3460	V4[+]	11	581	9
Mal−5	F4−, V4−, L2+	11	F2+, F3+, F4−, L1+, L2+, V4−	3469	V4[−]	11	590	

Table 2. Simulation result for a minimum set of 6 alarms.

	First alarm		Total Alarm		First FD		Total FD	
Malfunctions	Source signals	Time [min]	Source signals	Counts	Candidates	Time [min]	Identified	Impossible
Mal−1	F1+	11	F1+, F4+	1061	P1[+]	11	590	
Mal−2	F1−	11	F1−, F4−	1064	P1[−]	11	590	
Mal−3	F4+	18	F4+	583	F2[−]	18	583	
Mal−4	F4+, V4+	11	F4+,F4−,V4+	1180	V4[+]	11	581	9
Mal−5	F4−, V4−	11	F4−, V4−	1180	V4[−]	11	590	

6 Conclusion

Using two-layer cause-effect model, alarm source signals were selected from available alarm source signals to distinguish assumed fault origins. To evaluate the selected alarm source signals, numerical experiments were performed. To generate alarms, the limit for each alarm source signal is determined to meet constraints about false alarm and missed alarm. The experimental results show that many waste alarms were eliminated, and diagnostic performance by alarm selection was almost equal to that by all alarm source signals.

References

1. Rubinstein, E. and Mason, J.F.:An analysis of Three Mile Island. The accident that shouldn't have happened. The technical blow-by-blow, IEEE Spectrum, pp.33–42, November (1979)
2. Hollifield, B., Habibi, E.: The Alarm Management Handbook, PAS (2006)
3. Engineering Equipment and Materials Users' Association (EEMUA); ALARM SYSTEMS - A Guide to Design, Management and Procurement Publication No.191 2nd Edition, EEMUA, London (2007)
4. Takeda, K., Hamaguchi, T., Noda, M., Kimura, N. and Itoh, T.:Plant Alarm Signal Selection on the Basis of Two-Layers Cause-Effect Model, Kagaku Kougaku Ronbunshu, Vol. 36, No. 6, pp.582–588 (2010)
5. Takeda, K., Hamaguchi, T., Noda, M., Kimura, N. and Itoh, T.:Use of Two-Layer Cause-Effect Model to Select Source of Signal in Plant Alarm System, LNAI, Vol. 6277, pp.381–388 (2010)
6. Liu, X., Noda, M., Nishitani, H.:Evaluation of plant alarm systems by behavior using a virtual subject, Journal of Computers and chemical engineering, Vol.34, pp.374–386 (2010)
7. Brooks, R., Thorpe, R., Wilson,J.:A new method for defining and managing process alarms and for correcting process operation when an alarm occurs, Journal of Hazardous Materials, Vol. 115, pp.169–174 (2004)
8. Izadi, I., Shah, S.L., Shook, D.S. and Chen,T.:An Introduction to Alarm Analysis and Design, International Federation of Automatic Control, pp.645–650 (2009)