Model-based Dynamic Evaluation to Support the Design of Alarm Systems

Part 1: Development of Virtual Subject

Xiwei Liu, Hiroaki Kosaka, Masaru Noda, and Hirokazu Nishitani
Nara Institute of Science and Technology

In this paper, we propose an operator model to detect and identify causes of failure in an emergency, based on which an alarm system in a process system can be evaluated and improved. The operator model is a human processor model that includes a perceptual processor, short-term and long-term memories, a cognitive processor, and a motor processor. Knowledge bases for variable information, failure-symptom relation, and alarm management, as well as an abnormal state supervising procedure, are constructed. Since the knowledge bases are built based on general knowledge of a plant system, the model is easily augmented. Consequently, the operator model substitutes for an ideal operator as a virtual subject to supervise the plant system. The operator model automatically produces the track of fault detection and identification (FDI) in an emergency after a malfunction occurs. By analyzing the FDI track for an alarm system, we can evaluate the effectiveness of the system.

(Keywords: alarm system, fault detection and identification, operator model, model-based evaluation)

1. Introduction

Industrial processes are becoming increasingly complex while being manipulated by fewer operators. At the same time, companies are demanding high standards of safety, reliability, quality, and efficiency. Many aspects such as instrumentation, control strategies, user interfaces, and human factors are involved in meeting these demands. In industrial processes, a human supervisory control system consists of human operators, user interfaces, and a process control system, whereas in a distributed control system, a single operator might manipulate a chemical plant through a set of user interfaces on a cathode-ray tube (CRT) monitor. All information about related equipment and process variables are collected and displayed on user panels through the CRT monitor. Although measuring and control technology has become highly advanced, somewhat ironically it has greatly increased human operators' workloads.

A user interface in plant operations may bottleneck human performance of plant operations, especially in an emergency. An alarm system is an essential part of a user interface system because it provides vital support to plant operations by warning operators of situations that need their attention. Statistics [(1)] show that in Japan's chemical plants there were typically 200 alarms per day per operator in 2005, which indicates that alarms are very common in plant operations. Therefore, the design of an effective alarm system is a key issue in meeting expected demands.

A poorly designed alarm system causes nuisance alarms, standing alarms, and alarm flooding, and it can even result in incidents or accidents. For example, the explosion and fires at the Texaco Refinery in Milford Haven, UK, in 1994 resulted in plant damage costing

nearly US$72 million and significant production losses. The operators failed to prevent this accident partly because of a deficient alarm system, which forced the operators to respond to one alarm every 2-3 seconds (20-30 alarms/min) in 5 hours and finally led to the accident [2][3].

The Engineering Equipment and Materials Users Association (EEMUA) issued a comprehensive guideline for designing, implementing, evaluating, improving, and buying alarm systems [3]. It lists four key design principles of alarm systems:

(1) Each alarm should alert, inform, and guide.
(2) Every alarm should have a defined response.
(3) Adequate time should be allowed for the operator to carry out his defined response.
(4) Alarm system should be explicitly designed to take account of human limitations.

These principles mean that it is impossible to design an alarm system without direct or indirect participation of operators. To investigate various situations, however, a great number of subjects are required in the human subject-based experiments, which is a time-consuming and costly process. A promising solution to this problem is the human model-based evaluation approach.

The purpose of this study is to construct an operator model, which will be used as a virtual subject in order to evaluate alarm settings of an alarm system by analyzing its fault detection and identification (FDI) behavior.

2. Operator Model

2-1 Previous studies

In 1983, Card *et al.* proposed a model human processor (MHP) [4] as a conceptual framework. It is a metaphor for a human operator as an information processing system, which typically consists of a perceptual processor, short-term and long-term memories, a cognitive processor, and a motor processor. To apply the MHP to an operator model workable on PCs, relevant knowledge bases and procedures should be embedded in the model.

As a pioneering study, Takano *et al.* presented an operator behavior model for a nuclear power plant [5], which contains large knowledge bases to simulate the teamwork of three operators in a control room. It is a comprehensive model for simulation of teamwork in plant operations and investigation of human errors in the team's decision-making process. Also based on the MHP, Jin *et al.* developed an operator model for a boiler plant [6] to investigate cognitive errors. In this model, some parameters are tuned in a heuristic way to generate human errors that might occur when dealing with abnormal situations.

2-2 Operator model of alarm system evaluation

The MHP framework explicitly describes human's perception, cognition, execution, and memory. It is easy to customize and extend for various applications.

Referring to the MHP, we built the operator model shown in Fig. 1 for alarm system evaluation. In every scenario under abnormal situations, the operator model's main tasks are monitoring graphic panels with alarm messages and identifying causes of failure. The perceptual processor focuses on a certain few items or areas that are determined by the operator model's knowledge bases. After capturing a target item, the perceptual processor directly stores it into the short-term memory (STM).

A set of three knowledge bases (KBs) for variable information (VI), alarm management (AM), and failure-symptom relation (FS) is built based on general knowledge about the objective plant system and stored in the long-term memory (LTM). VI-KB is a mapping of all related user panels in an operator's memory when a process is normal and stable. AM-KB is applied to convert an alarm status of the plant monitoring system to a symptom. FS-KB contains all of the assumed failures with these symptoms as a bipartite graph.

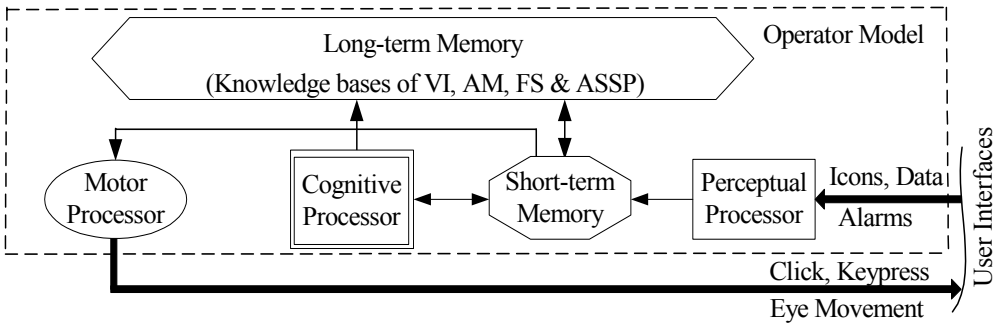

Fig. 1 Structure of operator model

As well as the three knowledge bases, an abnormal state supervising procedure (ASSP) is implemented in the operator model. Through the STM, the cognitive processor sends commands to the motor processor to move a gaze point or to push a button to confirm the status of the associated variables. The motor processor executes commands from the cognitive processor.

2-3 Construction of the three knowledge bases

Variable information knowledge base (VI-KB)

VI-KB includes the color, position, and normal range of each process or control variable on the user panels. It is stored as a table; for example, Table 1 shows a part of VI-KB for a user panel for a boiler plant. In a simulation, the virtual subject consults the table to find the position of a relevant graphic item.

Alarm management knowledge base (AM-KB)

In the plant monitoring system, the following alarm limits are used: high (PH), low (PL), high-high, low-low, and rate-of-change (VL) alarms for process variables (PV), and high (MH) and low (ML) alarms for manipulated variables (MV). If these alarm limits are exceeded, their corresponding alarm statuses become HI, LO, HH, LL, VEL+ or VEL-, MHI, and MLO, respectively.

Once a malfunction occurs, some process variables change outside of their normal ranges and even violate alarm limits. These changes are considered symptoms of malfunctions and are denoted as “xxx.High” or “xxx.Low” according to the tendency of the change. AM-KB in the operator model has rules, each of which converts an alarm status of the plant monitoring system to a symptom. An example is shown in Table 2.

Failure-symptom relation knowledge base (FS-KB)

FS-KB is built based on a general cause-effect analysis as follows:

(1) Supposing a malfunction occurs, analyze the stationary effects of failure propagation based on the physical or logical relations between process variables, which are usually obtained in the process flow sheets and control loop diagrams.

(1') If a plant simulator is available, cause a malfunction and record the response data for all process and manipulated variables. The response data are helpful for revising the results obtained in the first step.

(2) Draw failure propagation chains from cause to effect.

(3) Except for a root failure cause, all of the nodes in the obtained chains are classified into symptoms.

(4) Repeat steps (1)-(3) for other assumed malfunctions as failure causes.

For example, Figure 2 depicts the result of the cause-effect analysis for a fuel leak in a boiler plant. This diagram is generally used to represent propagation of influences. Lines with double arrows represent the relation of material and energy balances, and lines with a single arrow indicate the function of control loops. A thick-lined rectangle denotes a symptom whose corresponding variable has alarm limits, and a thin-lined

Table 1 Example of VI-KB for a user panel

Process variable	Color	Shape	Coordinates [pixel]		Normal operating condition	
			X	Y	Low value	High value
F201.PV	White	data	1107	346	76.9 t/h	83.4 t/h
F202.PV	White	data	202	666	6.7 t/h	7.3 t/h
F204.MV	White	data	1182	768	46.7%	56.5%
F205.PV	Cyan	icon	307	300	74.6 t/h	82.1 t/h
F206.PV	Cyan	icon	349	162	1.58 t/h	1.98 t/h
P201.PV	White	data	1120	369	78.3 Kg/cm^2	81.6 Kg/cm^2
P201.PV	Magenta	icon	777	390	78.3 Kg/cm^2	81.6 Kg/cm^2
P202.PV	White	data	322	507	82.3 Kg/cm^2	85.6 Kg/cm^2
P203.PV	White	data	837	513	-16.9 mmH_2O	-3.8 mmH_2O
P203.MV	White	data	1045	741	65.1%	73.9%
P204.PV	White	data	304	804	3.6 Kg/cm^2	4.25 Kg/cm^2
P206.PV	White	data	79	366	95.7 Kg/cm^2	98.2 Kg/cm^2
T201.PV	White	data	1090	396	477.4 ºC	492.8 ºC
T202.PV	Magenta	icon	778	331	477.4 ºC	492.8 ºC
T203.PV	White	data	291	535	293.9 ºC	302.8 ºC
T204.PV	White	data	274	828	88.1 ºC	91 ºC

Table 2 Example of conversion rule from alarm status of the monitoring system to symptom in AM-KB

Alarm status	HI, VEL+, MHI, HH	LO, VEL-, MLO, LL
Symptom	.High	.Low

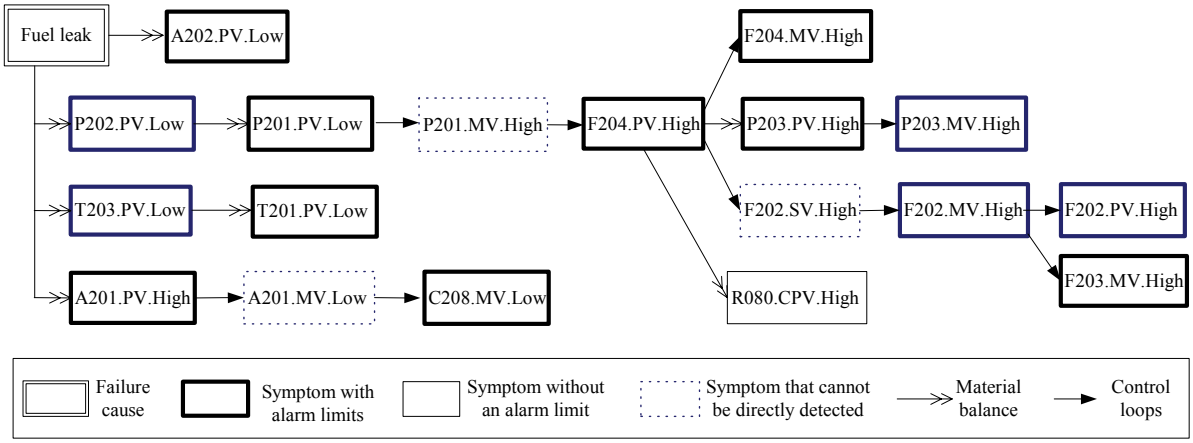

Fig. 2 Cause-effect analysis for fuel leak

rectangle means a symptom whose corresponding variable does not have an alarm limit. A rectangle with a dotted line is a symptom whose corresponding variable is unavailable on the existing user panels. Figure 2 shows that fifteen symptoms can be directly checked and three symptoms cannot be directly detected on these user panels.

The relations between failure causes and symptoms after sufficient time for propagation for all assumed malfunctions can be simply represented as a matrix form according to the results of cause-effect analysis. In the matrix, a row corresponds to a symptom and a column corresponds to a cause of failure. For instance, Table 3 shows the matrix, where F_m is the mth failure cause and S_n is the nth symptom; FL_m is the number of all symptoms for the mth cause of failure, and SL_n is the number of all causes related to the nth symptom. *FL* and *SL* values reflect the complexity of cause and effect, respectively. If a cause of failure F_m can cause a symptom S_n, the element in the nth row and the mth column is set to 1. Obviously, the total value in the nth row is SL_n, and the total value in the mth column is FL_m. Even when a set of assumed malfunctions is added, the matrix is easily modified.

The matrix is also illustrated by a bipartite graph shown in Fig. 3. The graph has two layers. The upper layer shows all causes of failure and the lower one shows all symptoms. An element 1 of the matrix in Table 3 is shown by a solid line between related cause of failure and symptom in Fig. 3. Dotted lines in Fig. 3 also indicate these connections, but the other ends of the

Table 3 Matrix of cause-effect relation

	F_1	F_2	.....	F_m	.....	F_M	*SL* value
S_1	0	1	.....	1	.....	0	SL_1
S_2	1	1	.....	0	.....	0	SL_2
⋮	⋮	⋮	⋱	⋮	⋱	⋮	⋮
S_n	1	0	.....	1	.....	1	SL_n
⋮	⋮	⋮	⋱	⋮	⋱	⋮	⋮
S_N	0	1	.....	1	.....	1	SL_N
FL value	FL_1	FL_2	.....	FL_m	.....	FL_M	

dotted lines are omitted due to space limitation. FL_m is the number of links connected with F_m and SL_n is the number of links connected with S_n. We define the association strength $AS_{m,n}$ of an FS link between F_m and S_n in a systematic way as follows: for any (m, n)

$$AS_{m,n} = \frac{\dfrac{w_{m,n}}{SL_n}}{\displaystyle\sum_{k \in A_m} \frac{w_{m,k}}{SL_k}} , \qquad (1)$$

where $w_{m,n}$ indicates a weight of the F_m-S_n link, and A_m is a set of indices of all symptoms connected with F_m. In other words, $AS_{m,n}$ is a contribution ratio of S_n to cause of failure F_m. For any cause, the total *AS* of all links in set A_m is normalized to 1.0, but the value becomes 1.0 after complete propagation. Calculation of *AS* by Eq. (1) enables a simple construction of FS-KB.

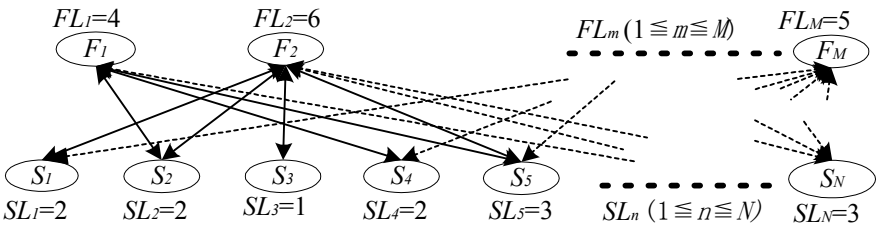

Fig. 3 Failure-symptom links

2-4 Abnormal state supervising procedure (ASSP)

A human operator can employ various tactics to identify the cause of a failure in an emergency. We assume the following procedure is activated after detecting an alarm. The outline of the procedure is shown in Fig. 4.

(1) Based on AM-KB, interpret the newly detected alarm as the nth symptom S_n and acknowledge the alarm.

(2) Based on FS-KB, assume that the causes of failure that connect to all alarmed symptoms are a set of possible ones, and reject others without a connection to S_n.

(3) Select one cause of failure F_m whose AS value $AS_{m,n}$ is the largest among those of the possible causes.

(4) If all possible causes of failure are rejected, return to step (2) to start a new round of confirmation.

(5) Select the next symptom $S_{n'}$ whose AS value is the largest among those of all unconfirmed symptoms that connect to F_m.

(6) If a new alarm is detected, restart the procedure.

(7) Confirm $S_{n'}$ by checking the trend data of its corresponding process variable $Tag_{n'}$ on a graphic panel.

(8) If the value of $Tag_{n'}$ changes outside of its normal range and accords with $S_{n'}$, add the $AS_{m,n'}$ of the link between $S_{n'}$ and F_m to the total AS value, otherwise go to step (10).

(9) When the total AS value becomes larger than the specified threshold, the FDI process is accomplished.

(10) If a symptom that connects to F_m remains, go to step (5). Otherwise, reject F_m from the set of possible causes of failure and return to step (3).

This ASSP can cope with multiple alarms. When a new alarm is issued, the ASSP is restarted and the set of possible causes of failure is modified by taking into account the corresponding symptom of the new alarm.

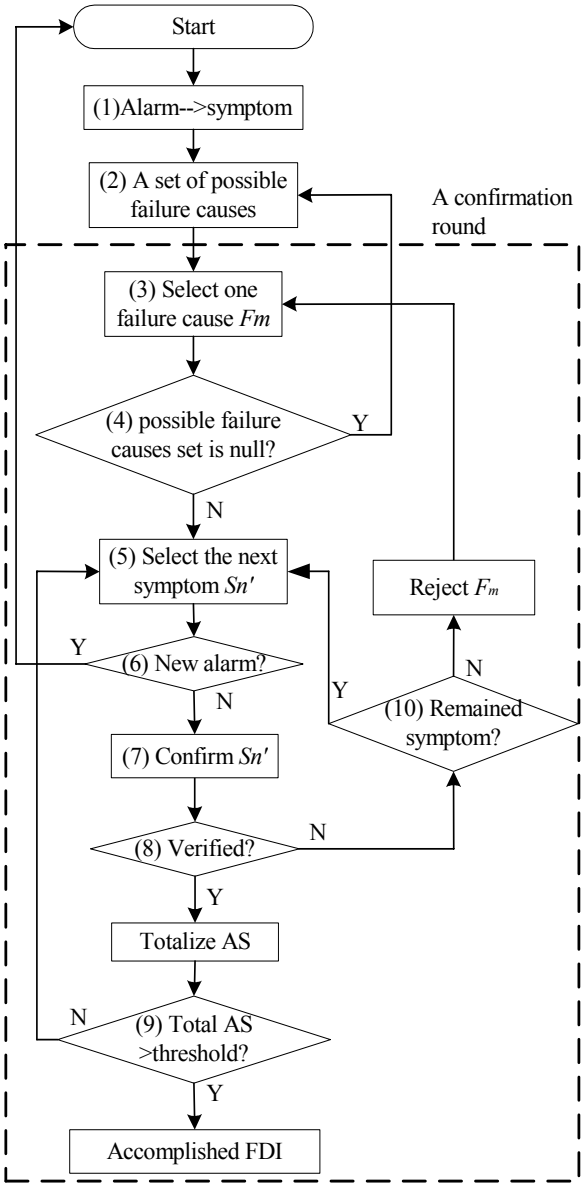

Fig. 4 Abnormal state supervising procedure (ASSP)

Symptoms converted from alarms remove the irrelevant failure causes from the set of possible causes of failure and then these removed causes will not be checked again during the entire FDI process. After checking all symptoms for a cause of failure, if its total AS value is less than the threshold, the cause of failure is temporarily rejected in that confirmation round, but it is not removed from the set of possible cause of failure and will be considered again in the next round. If failed confirmations temporarily reject all possible causes of

failure, ASSP is restarted and the set of possible causes is updated as mentioned above. The restarting ASSP generates a number of confirmation rounds. The dash-lined area in Fig. 4 shows a confirmation round.

2-5 FDI track generation

Human behaviors in the FDI process are classified into physical and mental subtasks. The latter includes perception, cognition, STM, and LTM activities, respective examples of which are reading an alarm message, remembering a previous alarm, searching for a symptom in the KB, and rejecting a cause of failure. An FDI track is an information flow diagram composed of these subtasks. In this study, the FDI track from detecting an alarm to successfully identifying a cause of failure is generated automatically based on the proposed ASSP of the operator model.

Even a simple operation may include a lot of subtasks. This makes the human behavior analysis very troublesome. However, according to the structure of the operator model shown in Fig. 1, we can define a part of the subtask sequence as an operational stage. Every operational stage has at least one STM subtask, which may follow after a perception, cognition, or LTM subtask. Therefore, an operational stage is processed in the order of perception, cognition, LTM, and physical subtask, but it may not include all types of subtasks.

Figure 5 shows an example of the generation of an FDI track after an alarm of low temperature (T201.LO). The first subtask is a perception subtask, through which the virtual subject captures the alarm message. Then, the STM subtask is performed to store the alarm information. Through AM-KB, the alarm information is converted to a symptom T201.PV.Low and stored in the STM. The following physical subtasks are performed to acknowledge the alarm, and the first operational stage ends at the vertical bar with a sequence number. Sequentially, the cognitive processor searches FS-KB in the LTM for a set of possible causes of failure. The cause of failure with the maximum *AS* value, that is, fuel leak, and its corresponding symptom, P203.PV.High, are selected and stored into the STM. This is the second stage. The cognitive processor searches VI-KB in the LTM for the information of P203.PV and then stores in the STM. According to the position information of P203.PV, the virtual subject switches to the overview panel from the alarm summary panel. The third operational stage is accomplished here. From the overview panel, P203.PV is captured by the perceptual processor and then stored into the STM. The cognitive processor fails to verify P203.PV.High. After the fourth operational stage, the FDI process continues until the total *AS* value is larger than the specified threshold.

3. Alarm System Evaluation

3-1 Evaluation criteria

EEMUA guidelines [3] stipulate the number of alarms

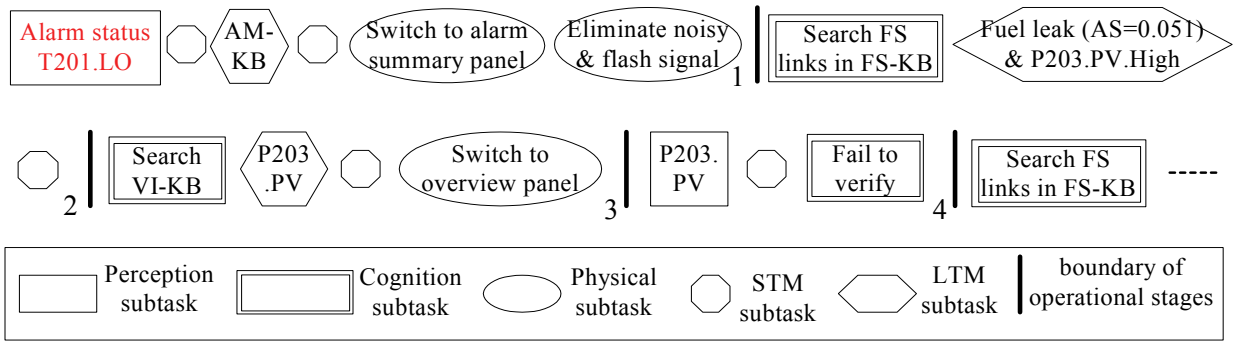

Fig. 5 FDI track generation after an alarm

displayed in the ten minutes following a major plant upset as a criterion of the acceptability of an alarm system. If the number of alarms in ten minutes is less than ten, the alarm system may be manageable for an operator, whereas if it is 20~100, the operator may feel difficulty in handling these alarms. The worst condition is when it exceeds 100, which leads to the operators abandoning use of the alarm system. Here, we count the number of alarms during FDI. Because the FDI process is commonly accomplished in a minute, the average rate of alarm occurrence should be less than ten per minute.

The number of operational stages indicates the difficulty of an FDI. This is not a criterion for evaluating an alarm system but it can be used to compare two systems. We also focus on the total length of eye movement. This indicates the effort of a physical subtask, which can be decreased by an efficient alarm system. The elapsed time for the entire FDI process by the operator model is also an important criterion. The time is estimated in every operational stage and affected by the number of operational stages. The elapsed time for an evaluation scenario is a sum of the earliest alarm appearance time and the elapsed time for the FDI, which reflects the general performance of the alarm system. In this study, we consider all of these criteria to evaluate an alarm system under various situations.

By analyzing the FDI track, we can evaluate an alarm system with the following criteria:

(1) Tag and status of the earliest alarm.
(2) Time from the beginning of malfunction to the earliest alarm.
(3) Number of alarms during the FDI process.
(4) Number of operational stages.
(5) Total length of eye movements.
(6) Elapsed time of the entire FDI process.
(7) Elapsed time for an evaluation scenario.

The earliest alarm is an important clue guiding the FDI process. If the first symptom converted from the earliest alarm has a close relation to the true cause of failure, it can shorten the time of the FDI process. To detect abnormality earlier, the earliest alarm should appear in a timely manner without introducing a nuisance alarm.

3-2 Improvement of alarm settings

Figure 6 shows an example of how to configure effective alarm limits [3]. The four zones in the figure indicate four types of plant states: target, normal, upset, and shutdown states. A control system commonly works to restrict all variables within the target operating condition. When the plant enters the upset state from the normal one, HI or LO alarms notify the operator of an abnormal situation under the normal state. High-high (HH) or low-low (LL) alarms are provided to inform the operator of critical situations. If the operator fails to recover the plant to the normal state, an emergency shutdown (ESD) system will be activated.

In practice, the three boundaries in Fig. 6 may be vague, and the choice of alarm settings is complicated. Inadequate alarm settings can cause standing, fleeting, nuisance, and repeating alarms, and these may result in alarm flooding. To avoid these problems, the amplitude and duration of acceptable fluctuations should be determined based on the analysis of a certain number of assumed malfunctions. In order to ensure that an alarm system is usable and effective under all operation conditions, its performance should be assessed during design and commissioning. Regular auditing should also be conducted throughout a plant's life to confirm that good performance is maintained.

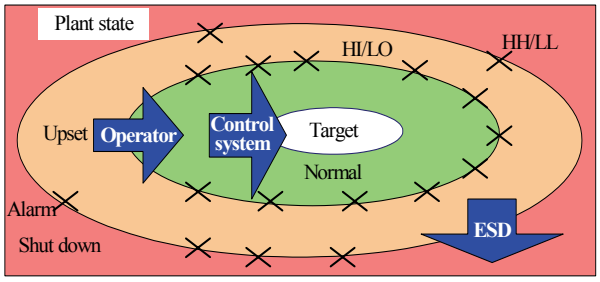

Fig. 6 Effective alarm settings

Table 4 Example of alarm settings in a boiler plant

Tag \ Limit	HH	PH	PL	LL	VL	Unit1	MH	ML	Unit2
A201	10	10	1.5	0.5	10	%	100	0	%
A202	275	150	0	0	500	ppm	100	0	%
C208	-	-	-	-	-	-	60	40	%
F201	100	100	0	0	100	t/h	-	-	-
F202	10	10	0	0	10	t/h	100	0	%
L201	100	50	-50	-100	200	mm	100	0	%
P201	90	85	75	70	100	Kg/cm^2	100	0	%
T201	520	500	480	470	300	℃	10	0	t/h

Unit1: unit of HH, PH, PL, and LL; unit of VL is unit1/s; Unit2: unit of MH and ML; -: unavailable item

This research mainly concerns the evaluation of alarm settings, which has been introduced with AM-KB. Table 4 is an example of the alarm settings in a boiler plant.

4. Procedure of Model-based Evaluation for Alarm System

By using the operator model as a virtual subject, we can evaluate an alarm system through the following procedure.

(1) List all possible malfunctions in an objective plant.

(2) Build VI-KB, FS-KB, and AM-KB based on process and control-system design information, cause-effect analyses, operational experience, and expert reviews of the objective plant system.

(3) Through FDI simulations by using the operator model, obtain the resulting FDI track and evaluation criteria for each malfunction.

(4) Evaluate the alarm system and modify alarm settings if necessary.

(5) Repeat steps (1)-(4) until an acceptable result is obtained.

5. Conclusion

To evaluate alarm systems, an operator model was developed based on the structure of Card's MHP. We embedded simple knowledge bases of plant operations into the LTM and made the operator model as a virtual subject to mimic the FDI behaviors of an ideal human operator. The knowledge bases are built based on general knowledge, and these knowledge bases are easily modified for additional malfunctions. These features are useful for practical applications. In the next paper, we will apply this approach to evaluate the existing alarm system of a boiler plant simulator.

References

(1) Plant Operation Section, System, Information Simulation Division, Society of Chemical Engineers, Japan: Report on Plant Operations and Technology Transfer (2005).

(2) Nochur, A., Vedam, H., and Koene, J.: Alarm performance metrics; On-Line Fault Detection and Supervision in the Chemical Process Industries, 2001 (Chemfas-4): A Processing Volume from the 4th IFAC Workshop, Jejudo Island, Korea, 7-8 June 2001 (Stephanopoulos, G. *et al.* Ed.), Cambridge, UK, Elsevier Science, pp. 203-208 (2001).

(3) The Engineering Equipment and Materials Users Association (EEMUA): Alarm Systems, a Guide to Design, Management and Procurement,

Publication No. 191, EEMUA, London (1999).

(4) Card, S. K., Moran, T. P., and Newell, A.: The Psychology of Human-Computer Interaction, Lawrence Erlbaum Associates, London (1983).

(5) Takano, K., Sasou, K., Yoshimura, S., Iwai, S., and Sekimoto, Y.: Behavior simulation of operation team in nuclear power plant —Development of an individual operator model, Research Report of Central Research Institute of the Electric Power Industry, S93001 (1994).

(6) Jin, Y., Yamashita, Y., and Nishitani, H.: Study on plant operator's recognition errors in fault diagnosis using cognitive information processing model, *Journal of the Society for Industrial Plant Human Factors of Japan*, Vol. 9, No. 1, pp. 27-37 (2004).