Human Model-Based Dynamic Evaluation for Alarm System in Chemical Plant

Xiwei Liu, Masaru Noda, Hirokazu Nishitani, Nara Institute of Science and Technology, Ikoma, Japan

Abstract

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 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 operator as a virtual subject to supervise the plant system. The operator model automatically produces a track of fault detection and identification (FDI) in an emergency after a malfunction occurs. By analyzing the FDI tracks for an alarm system, we can evaluate the effectiveness of the alarm system. Case study shows the usefulness of the model-based dynamic evaluation method.

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

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 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:

- Each alarm should alert, inform, and guide.
- Every alarm should have a defined response.
- Adequate time should be allowed for the operator to carry out his defined response.
- 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 are a time-consuming and costly process. A promising solution to this problem is a human model-based evaluation approach.

The purpose of this study is to construct an operator model for evaluating an alarm system under a set of assumed malfunctions. We focus on the evaluation of alarm settings by analyzing the fault detection and identification (FDI) behaviors based on the operator model. In other words, the operator model is used as a virtual subject.

Operator Model

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.

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.

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.

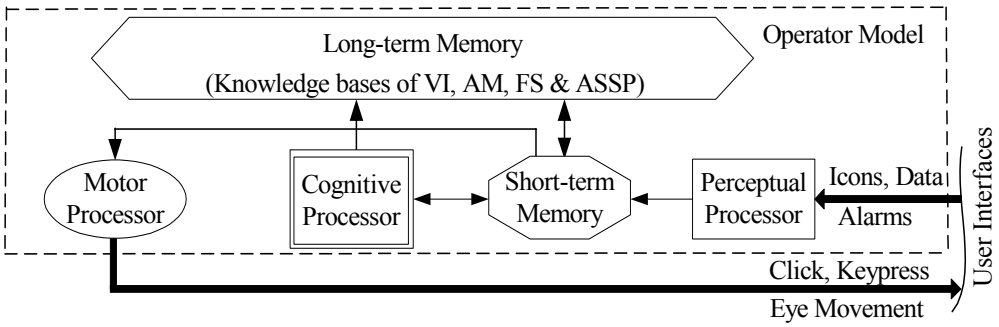

Fig. 1 Structure of operator model

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 simulation, the virtual subject consults the table to find the position of a relevant graphic item.

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

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.

Table 2 Example of AM-KB converting alarm status to symptom

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

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.

The relations between failure causes and symptoms after enough time for propagation can be represented as a matrix form according to the results of cause-effect analysis for all assumed malfunctions. For instance, Table 3 shows the matrix, where F_m is mth failure cause and S_n is nth symptom; FL_m is the number of all symptoms for the mth failure cause, 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. In the matrix, a row corresponds to a symptom and a column corresponds to a failure cause. If a failure cause F_m can cause a symptom S_n, the element in the nth row and 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.

The matrix is also illustrated by a bipartite graph shown in Fig. 2. 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. 2. Dotted lines in Fig. 2 also indicate these connections, but the other ends of the 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)

$$AS_{m,n} = \frac{\frac{w_{m,n}}{SL_n}}{\sum_{k \in A_m} \frac{w_{m,k}}{SL_k}}, \tag{1}$$

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.

$w_{m,n}$ for every symptom is defined by the model designer according to questionnaires of expert plant operators, which is important to distinguish similar failure causes. Obviously, the matrix of cause-effect relation decides *AS* value of every pair of failure cause and symptom. The matrix is embedded in the operator model as a part of FS-KB.

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	

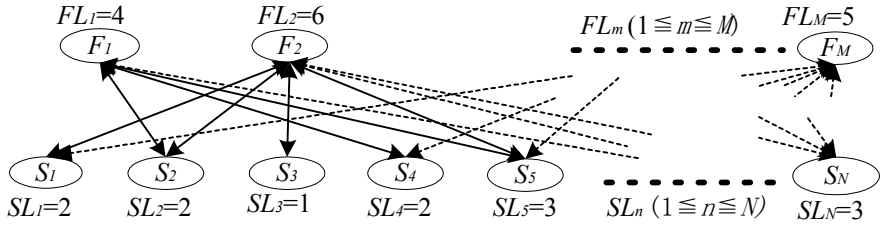

Fig. 2 Failure-symptom links

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 the earliest alarm. The outline of the procedure is shown in Fig. 3.

(1) Based on AM-KB, interpret the newly detected alarm as the *n*th 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, return to the first step.
(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 and F_m has been rejected by the failure to verify $S_{n'}$, 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 returned to the first step and the set of possible causes of failure is modified by taking into account the corresponding symptom of the new alarm. 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 returned to the first step and the set of possible causes is updated as mentioned above. A number of confirmation rounds may be generated in an FDI process. The dash-lined area in Fig. 3 shows a confirmation round.

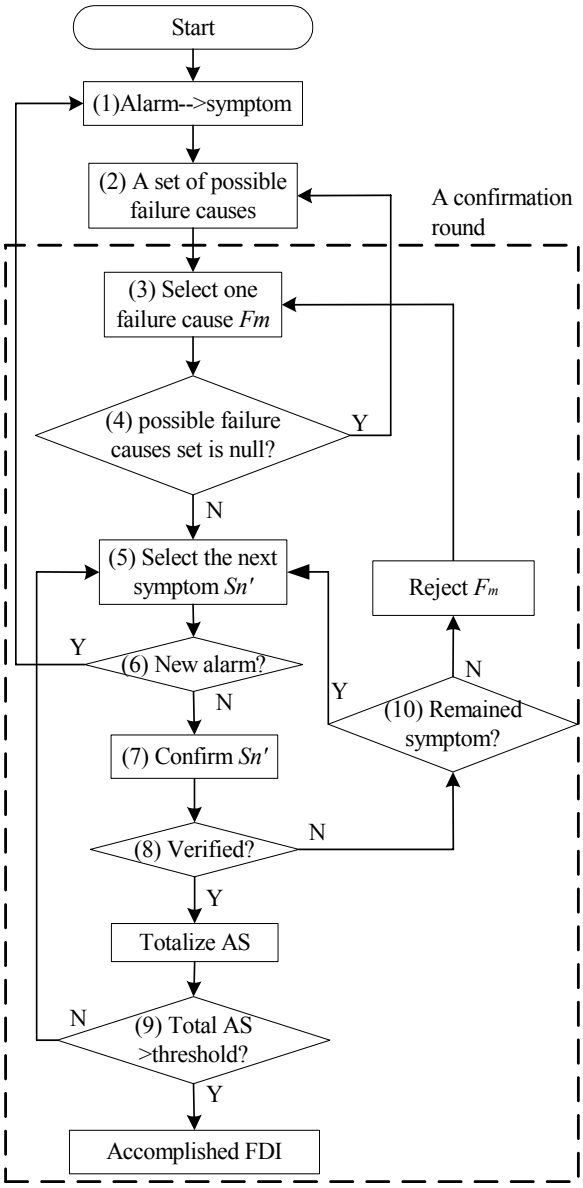

Fig. 3 Abnormal state supervising procedure (ASSP)

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 4 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, i.e. 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.

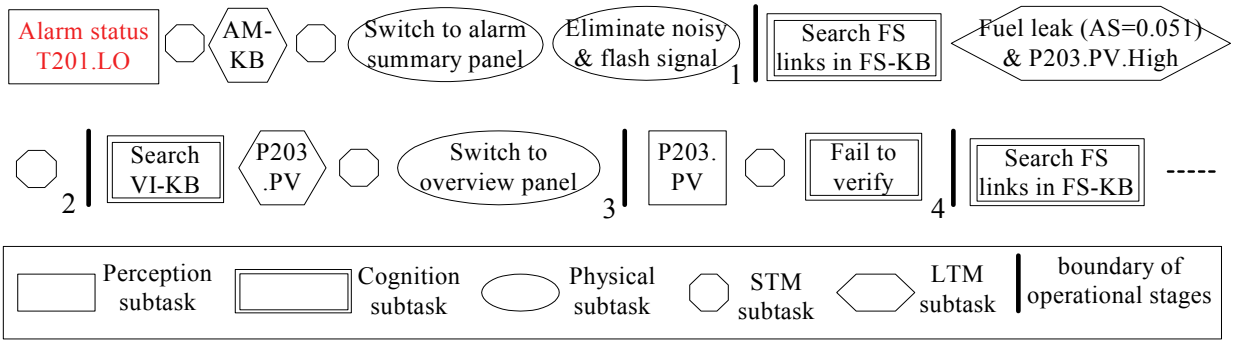

Fig. 4 FDI track generation after an alarm

Alarm System Evaluation Procedure

EEMUA guidance [3] stipulates the number of alarms displayed in 10 minutes following a major plant upset as a criterion of the acceptability of an alarm system. If the number of alarms in 10 minutes is under 10, the alarm system may be manageable for an operator. If it is 20~100, the operator may feel difficulty in handling these alarms. The worse 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 appearance should be less than 10 per minute. 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 failure cause, 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.

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 of the FDI process is also an important criterion. It is estimated in every operational stage and affected by the number of operational stages. The total elapsed time 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 for various situations to evaluate an alarm system.

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

(1) Total elapsed time.
(2) Time from the beginning of malfunction to the earliest alarm.
(3) Elapsed time of the FDI process after the earliest alarm.
(4) Number of operational stages.
(5) Association by tag and status of the earliest alarm.

(6) Number of alarms during the FDI process.
(7) Total length of eye movements in the FDI process.

This research mainly concerns the evaluation of alarm settings, which has been introduced with AM-KB. Figure 5 shows an example of how to configure effective alarm limits [3]. 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 under the normal state. When the plant becomes the upset state from the normal state, HI or LO alarms let the operator know of abnormal situations. 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 shut down (ESD) system will be activated.

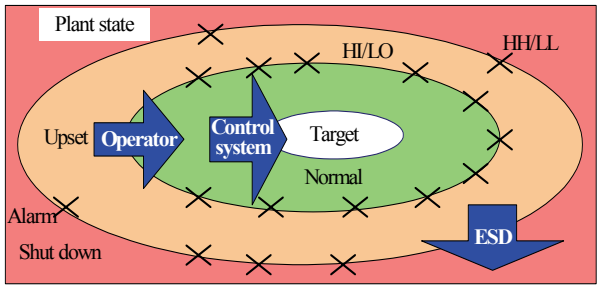

Fig. 5 Effective alarm settings

In practice, the three boundaries in Fig. 5 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 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 be continued throughout a plant life to confirm that good performance is maintained.

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

(1) List up all available 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.
(3) Through FDI simulations by using the operator model, obtain the resulting FDI track and evaluation criterion 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.

To construct a sufficient FS-KB is an important work for the dynamic evaluation. Here, an illustrative example shows the cause-effect analysis in case of fuel leak malfunction. Before evaluation, the cause-effect analysis for eleven malfunctions should be done for FS-KB construction.

Based on the cause-effect procedure, we drew failure propagation chains after a fuel leak, as shown in Fig. 6. Lines with double arrows mean the relation of material and energy balances, and lines with an arrow indicate the function of control loops. A thick-lined rectangle means a symptom whose corresponding variable has alarm limits, and a thin-lined rectangle means a symptom whose corresponding variable does not have an alarm limit. A rectangle with a dot line means a symptom whose corresponding variable is unavailable on existing user panels. Fuel leaks affect the air component (A201.PV and A202.PV) in the furnace and the drum's condition (P202.PV and T203.PV). Steam condition (P201.PV and T201.PV) varies, and this changes the air draft state (P203.PV) and fuel oil supply (F202.MV). Table 4 shows part of FS-KB for the FDI process. In the fuel leak column (Mal-7) in Table 4, elements corresponding to the 15 available symptoms are set to 1.

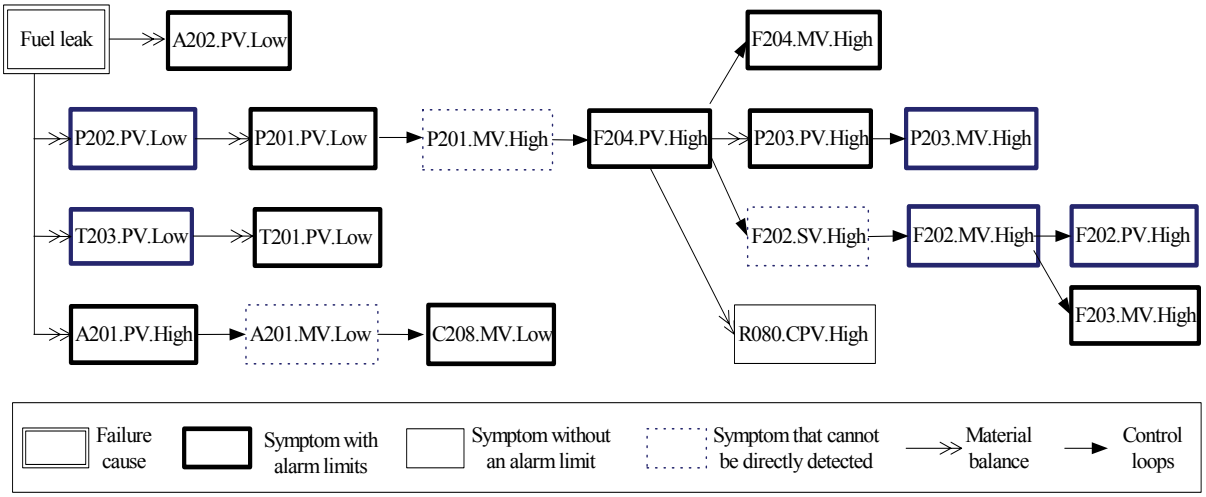

Fig. 6 Cause-effect analysis for fuel leak

Table 4 Part of FS-KB

Failure cause / Symptom	Mal-1	Mal-2	Mal-3	Mal-4	Mal-5	Mal-6	Mal-7	Mal-8	Mal-9	Mal-10	Mal-11	*SL*
FOP1.Icon.Flash	1	0	0	0	0	0	0	0	0	0	0	1
Burner1.Fire.No	0	1	0	0	0	0	0	0	0	0	0	1
FDF.Icon.Flash	0	0	1	0	0	0	0	0	0	0	0	1
F202.PV.HIGH	0	1	0	0	0	1	1	0	0	0	0	3
A201.PV.HIGH	1	1	0	0	1	0	1	0	0	0	0	4
R080.CPV.HIGH	0	1	0	0	0	1	1	0	0	1	0	4
F202.MV.HIGH	1	1	0	0	1	0	1	0	0	0	0	4
F204.PV.HIGH	0	1	0	0	0	1	1	0	0	1	0	4
C208.MV.LOW	1	1	0	0	1	0	1	0	0	0	0	4
P203.PV.HIGH	0	0	0	1	0	1	1	0	1	1	0	5
P203.MV.HIGH	0	0	0	1	0	1	1	0	1	1	0	5
F203.MV.HIGH	1	1	0	0	1	1	1	0	0	0	0	5
T201.PV.LOW	1	1	1	0	1	0	1	0	0	0	0	5
T203.PV.LOW	1	1	1	0	1	0	1	0	0	0	0	5
A202.PV.LOW	1	1	0	0	1	0	1	0	0	1	0	5
P201.PV.LOW	1	1	1	0	1	0	1	1	0	0	0	6
P202.PV.LOW	1	1	1	0	1	0	1	1	0	0	0	6
F204.MV.HIGH	0	1	1	1	0	1	1	0	0	1	0	6
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
FL	18	18	18	9	19	16	15	10	5	8	6	

Case Study

Objective Plant System

A process flow diagram of the objective boiler plant simulator is shown in Fig. 7. Tags of continuous process variables in the simulator are listed in Table 5. As a target state, the simulated boiler plant produces 80 ton per hour of superheated steam at 485ºC. In normal situations, the demand load of the simulated boiler plant randomly changes from 77.9 to 82.4 t/h, which determines the

normal ranges of all variables in the plant. Table 6 shows the normal fluctuation of PV and MV values. The operator model reads real-time process and alarm information by using object linking and embedding for process control (OPC) connection to a process computer. The user interface system of the boiler plant includes the following panels: overview, operational, engineering, trend, and alarm summary, etc. Figure 8 shows the overview panel as an example.

Alarm messages can be displayed on several user interfaces, as shown in Fig. 9. A message window, which is always on top of the monitoring screen, can show the latest alarm. The five latest alarms are listed in the process alarm window, which can be summoned from the message window. On the alarm summary panel, we can check the 200 latest alarms. Figure 10 shows the tuning panel through which alarm limits can be directly modified.

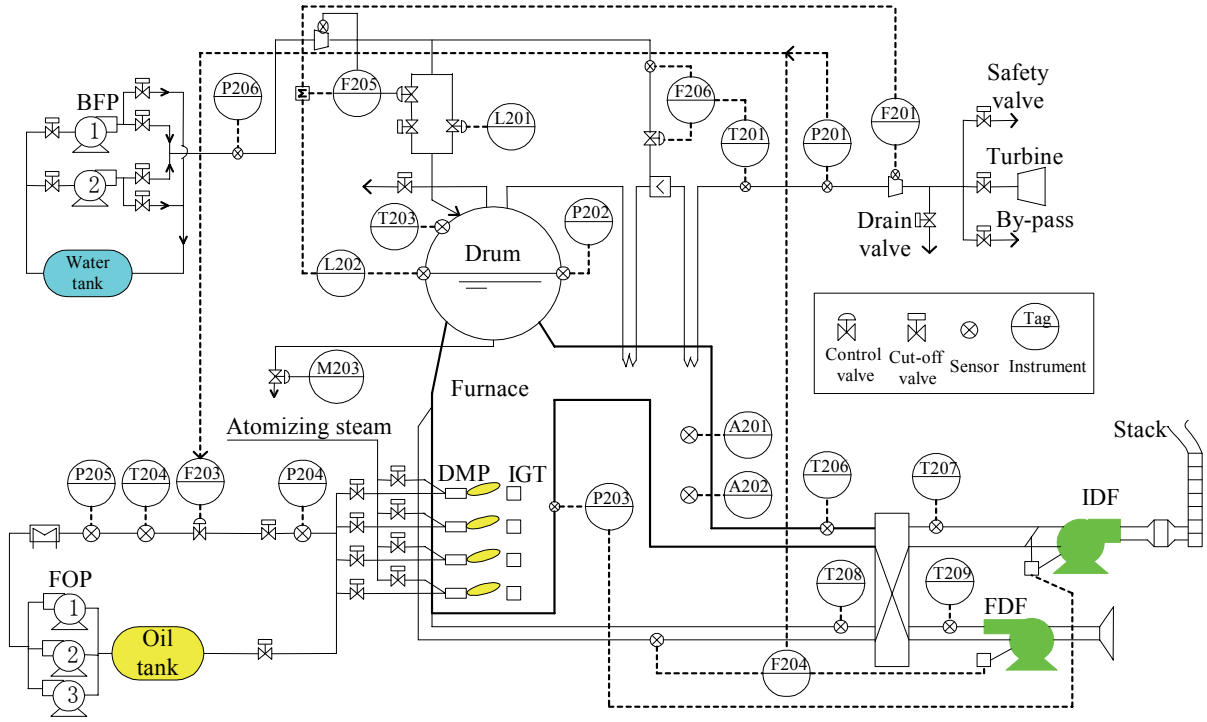

Fig. 7 Process flow diagram of a boiler plant simulator

In the actual alarm system of the simulator denoted as alarm system α, 21 continuous process variables with 123 alarm limits are shown in Table 7. The settings of alarm system α were designed by the boiler plant simulator's manufacturer. Most alarm limits in Table 7 cannot be violated because they are set at their extreme values. Tags with possibly violated alarm limits in the simulation are indicated in bold. There are only 12 process variables with 28 possibly violated alarm limits in alarm system α.

We assume the following eleven malfunctions in the boiler plant:

Mal-1: Indicated by FOP1 failure. A fuel pump (FOP1) failure decreases fuel oil flow rate (F202) and burner-head pressure (P204). The FOP1 icon flashes in red, so this malfunction is easy to identify.

Mal-2: Indicated by burner extinction. Extinction of all burners decreases the pressure (P201) and flow rate (F201) of the main steam. After this malfunction, the icons of the burner's fire disappear.

Mal-3: Indicated by FDF degradation. A forced draft fan (FDF) degrades, which reduces air intake (F204) and pressure in the furnace. Air/fuel ratio control correspondingly decreases the fuel oil flow rate. The FDF icon flashes after this malfunction.

Mal-4: Indicated by IDF trip. An induced draft fan (IDF) trip reduces air exhaust and increases furnace pressure. The IDF icon flashes in this case.

Mal-5: Indicated by oil heater failure. It causes a drop of oil temperature (T204), and then the oil flow rate decreases due to viscosity (R034) increase.
Mal-6: Indicated by P204 sensor failure. Burner-head pressure sensor (P204.PV) failure forces the measured variable to remain at a low value. This fully opens a control valve of the fuel flow rate. Then the fuel oil flow rate increases out of control.
Mal-7: Indicated by a fuel leak. It actually decreases the oil flow rate to burners and causes a state where the heat is insufficient to produce the desired steam flow rate.
Mal-8: Indicated by BFP1 trip. A water-feeding pump (BFP1) trip interrupts the water supply to the drum and the desuperheater, which may explode the water tube. This malfunction can be detected by BFP1's flashing icon.
Mal-9: Indicated by a water leak. Water tube leak increases furnace pressure (P203). Water flow rate (F205) slightly decreases.
Mal-10: Indicated by O2 sensor failure. Oxygen sensor (A201.PV) clings to a small value that causes an increase of the air/fuel ratio.
Mal-11: Indicated by turbine trip. This drastic malfunction causes sharp changes of many variables.

Four malfunctions were abandoned in the evaluation scenarios even though operator model can identify all eleven malfunctions based on corresponding symptoms. Mal-8, which presents a direct alarm of a BFP1 trip, is unsuitable for this study because fault identification is not needed in this case. Since Mals-9 and -10 can only cause such slight fluctuation that an abnormality cannot appear for a long time, they should be identified with some monitoring tactics other than an alarm system. If we do not filter repeating alarms, Mal-11 always causes alarm flooding which is not the focus of our current interest.

Table 5 Tags in boiler plant simulator

Tag	Description	Tag	Description
A201	Oxygen concentration	P201	Main steam pressure
A202	CO concentration	P202	Drum press indicator
C208	O_2 and CO analyzer selector	P203	Furnace pressure
F201	Main steam flow rate	P204	Burner-head pressure
F202	Fuel flow rate	P205	Fuel pump outlet pressure
F203	Fuel auto selector	P206	BFP outlet pressure
F204	Air flow rate	R080*	Wind speed
F205	Drum feedwater flow rate	R034*	Fuel oil viscosity
F206	Desuperheater spray flow rate	T201	Main steam temperature (for control)
L201	Drum water level control (for a small valve)	T202	Main steam temperature (for measurement)
L202	Drum water level control (for a large valve)	T203	Drum water temperature indicator
M203	Drum blow valve control	T204	Fuel temperature

*R080 and R034 are not measurement points

Table 6 Normal fluctuation of PV and MV values

Tag	Low PV value	High PV value	Low MV value	High MV value
A201	2.61%	2.78%	49.1%	49.9%
A202	23.5 ppm	25.7 ppm	0%	0%
C208	-	-	49.1%	49.9%
F201	77.9 t/h	82.4 t/h	-	-
F202	6.78 t/h	7.23 t/h	51.1%	53.7%
F203	51.1%	53.7%	51.1%	53.7%
F204	67.9%	71.9%	47.7%	55.5%
F205	75.59 t/h	81.11 t/h	42.9%	44.74%
F206	1.68 t/h	1.88 t/h	40.61%	43.49%
L201	-1.63 mm	1.12 mm	0%	0%
L202	-1.63 mm	1.12 mm	75.9 t/h	81.44 t/h
P201	79.3 Kg/cm^2	80.6 Kg/cm^2	67.9%	72.3%
P202	83.3 Kg/cm^2	84.6 Kg/cm^2	-	-
P203	-14.9 mmH_2O	-5.76 mmH_2O	66.1%	72.9%
P204	3.75 Kg/cm^2	4.1 Kg/cm^2	0%	0%
P205	12.6 Kg/cm^2	12.9 Kg/cm^2	-	-
P206	96.7 Kg/cm^2	97.2 Kg/cm^2	-	-
T201	480.4℃	489.8℃	1.67 t/h	1.88 t/h
T202	480.4℃	489.8℃	-	-
T203	297.9℃	298.8℃	-	-
T204	89.1℃	90℃	-	-

-: unavailable item.

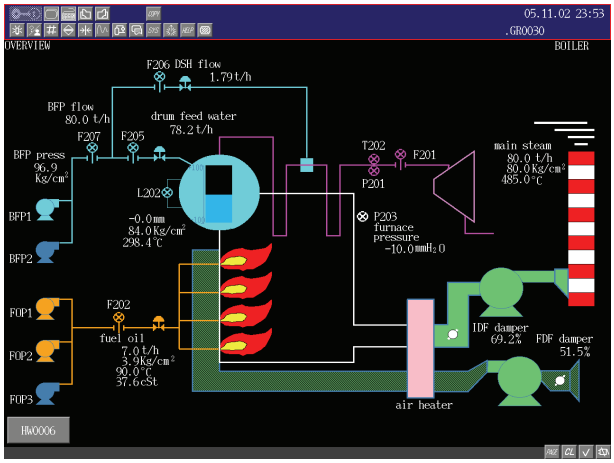

Fig. 8 Overview panel

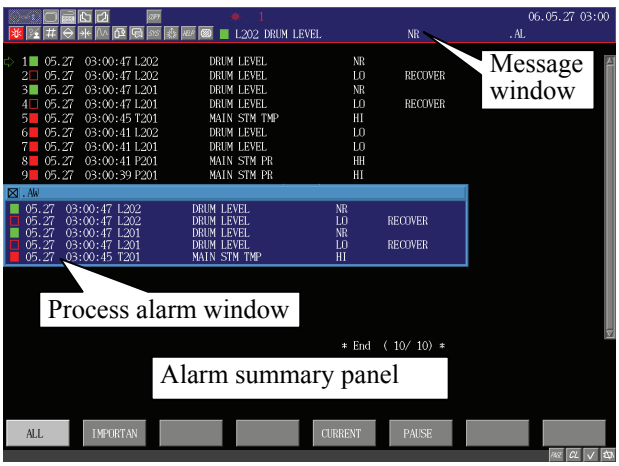

Fig. 9 User interfaces for alarm message

Fig. 10 Tuning panel to modify alarm limits

Table 7 Settings of alarm limits in a boiler plant simulator (alarm system α)

Tag \ Limit	HH	PH	PL	LL	VL	Unit 1	MH	ML	Unit 2
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	%
F203	-	-	-	-	-		100	**40**	%
F204	100	100	**25**	**20**	100	t/h	100	0	%
F205	100	**90**	0	0	100	t/h	100	0	%
F206	10	10	0	0	10	t/h	100	0	%
L201	100	**50**	**-50**	-100	200	mm	100	0	%
L202	**95**	**50**	**-50**	**-95**	200	mm	100	0	t/h
P201	**90**	**85**	**75**	**70**	100	Kg/cm^2	100	0	%
P202	100	100	0	0	100	Kg/cm^2	-	-	-
P203	100	**50**	**-50**	-100	200	mmH_2O	100	0	%
P204	15	15	**2.2**	**2**	15	Kg/cm^2	100	0	%
P205	15	15	0	0	15	Kg/cm^2	-	-	-
P206	100	100	0	0	100	Kg/cm^2	-	-	-
T201	**520**	**500**	**480**	**470**	300	ºC	10	0	t/h
T202	600	600	0	0	600	ºC	-	-	-
T203	400	400	0	0	400	ºC	-	-	-
T204	100	100	0	0	100	ºC	-	-	-

Unit 1: unit of HH, PH, PL, LL, and VL; Unit 2: unit of MH and ML;
Bold: tags with alarm limits that may be violated.

Evaluation of Alarm System α

A failure cause is identified when its total *AS* value exceeds a threshold, defined as 0.6. After a fuel leak is caused in alarm system α, the alarm statuses that appeared during the FDI process are listed in Table 8. Figure 11 is the resulting FDI track, and the thick vertical bars indicate operational stages with their sequence numbers. The track was generated based on the proposed ASSP in the operator model. Figure 12 shows a screenshot of the evaluation process. An eye movement trajectory is displayed on the graphic panel. In this research, the trajectory of gaze points is drawn by line segments.

Figure 11 shows the following process: Through AM-KB, an alarm message for T201.LO was interpreted as symptom T201.PV.Low, which is connected with the following failure causes: FOP1 failure (Mal-1), burner extinction (Mal-2), FDF degradation (Mal-3), oil heater failure (Mal-5), and fuel leak (Mal-7). The corresponding *AS* values of the links between symptom T201.PV.Low and the above five failure causes were 0.010, 0.010, 0.010, 0.015, and 0.051, respectively. Based on the ASSP, the operator model started to identify the failure cause from the fuel leak. Comparing the Mal-2 column with Mal-7 in Table 4, it found that most Mal-7 symptoms are also Mal-2 symptoms and that P203.PV.High is an important symptom to distinguish Mal-7 from Mal-2. The symptom, P203.PV.High, was given a high weight, so it began symptom confirmation from P203.PV.High. Most weights for symptoms are set as 1, except some symptoms have definite relation with a failure cause. Failure cause can be quickly identified if these symptoms are early verified. Soon after the malfunction, only a few variables became out of normal ranges. At the 13th operational stage, a new alarm was issued, and ASSP was returned to its first step. This is called an FDI round.

In the second round, P203.PV.High was not verified again. Based on ASSP, even if P203.PV.High was not verified, the next symptom for Mal-7, F202.PV.High was sequentially confirmed. Symptoms FOP1.Icon.Flash, Burner1.Fire.No, and FDF.Icon.Flash have the highest weight to calculate the total *AS* values for Mals-1, -2, and -3, respectively; so these malfunctions can be easily rejected in the FDI process. In the Mal-7 column of Table 4, except symptoms T201.PV.Low, C208.MV.Low, and P201.PV.Low that were shown by alarms, symptoms F202.PV.High, F202.MV.High, A201.PV.High, F204.PV.High, T203.PV.Low, and F203.MV.High were sequentially verified for Mal-7. Since several variables were not abnormal before FDI was accomplished, some corresponding Mal-7 symptoms were not successfully verified. Finally, 48.7 seconds after the earliest alarm, the true failure cause was identified when the total *AS* value of the fuel leak became larger than 0.6. Figure 13 shows the changes in the total *AS* value after Mal-7.

Table 9 shows the evaluation results of alarm system α under seven malfunctions. Alarm T201.LO appears four times as the earliest alarm, which gives the complexity of FDI. On the other hand, the earliest alarms of Mals-4, and -6 appear 60 seconds later after the malfunctions occurred, which makes it difficult to cope with these failures. Generally, the evaluation result mainly shows two weak points of alarm system α: the earliest alarms appear too late for some malfunctions and the Mal-7 FDI costs too many operational stages and has a long distance of eye movement.

Table 8 Alarms after fuel leak in alarm system α

No.	Time after fuel leak [s]	Alarm status
1	15	T201.LO
2	20	C208.MLO
3	45	P201.LO

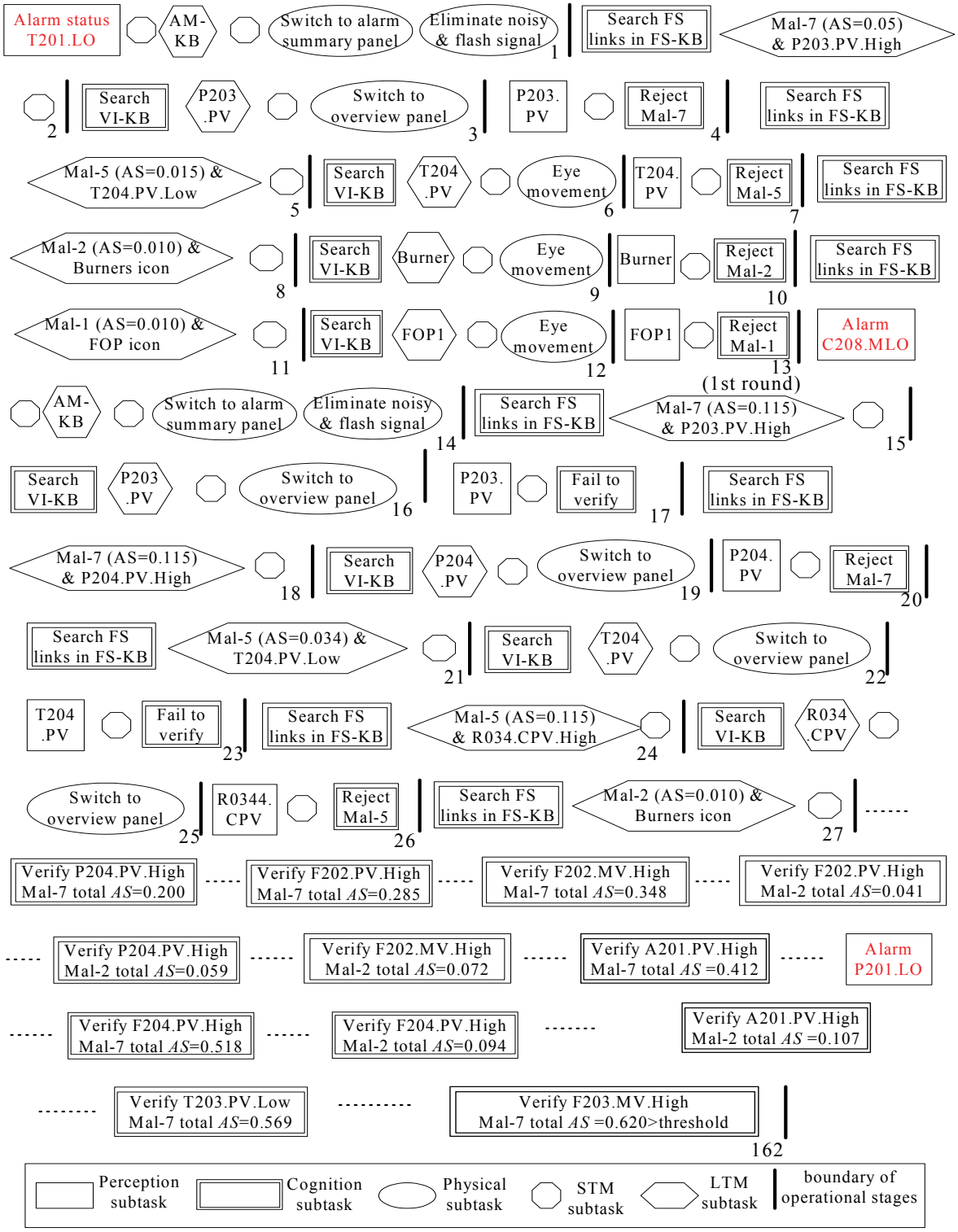

Fig. 11 FDI track of fuel leak under alarm system α

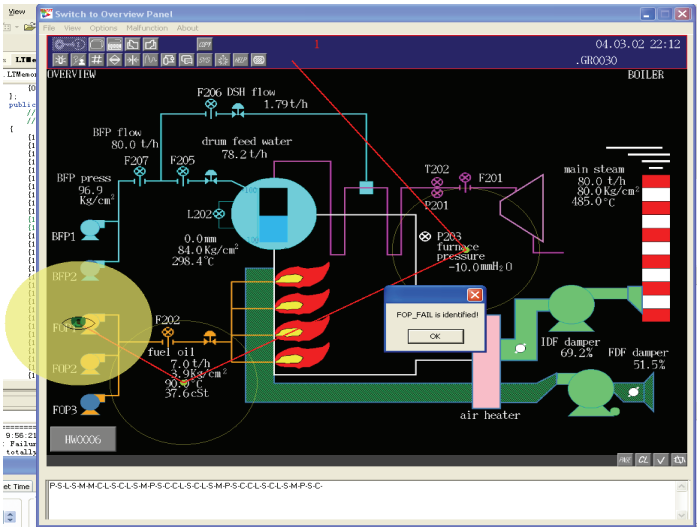

Fig. 12 Screenshot of evaluation program

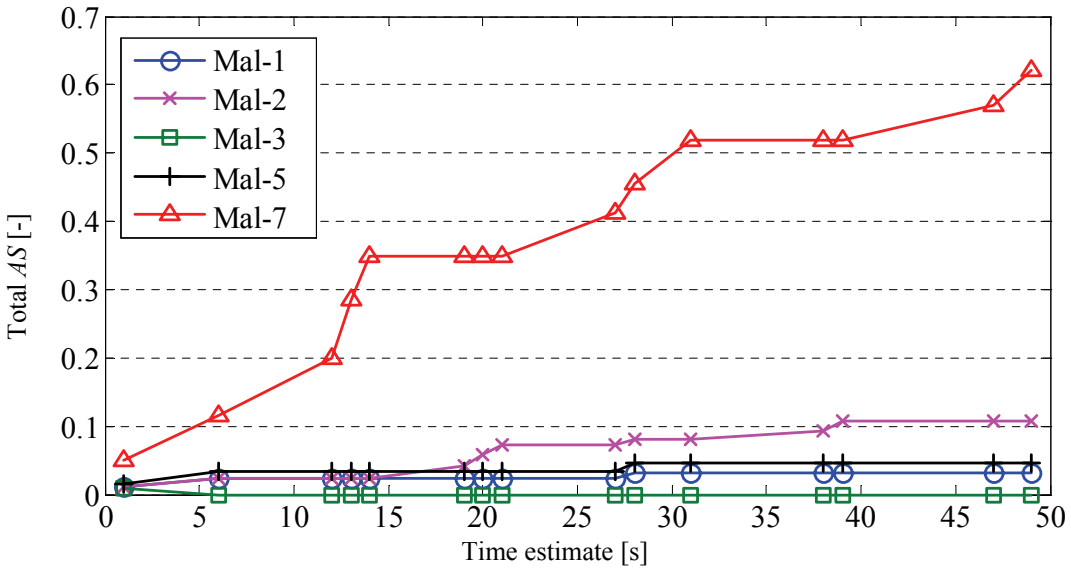

Fig. 13 Changes in total AS values for alarm system **α**

Table 9 Evaluation results of alarm system α

Criteria \ Malfunction	Mal-1	Mal-2	Mal-3	Mal-4	Mal-5	Mal-6	Mal-7	Total
Total elapsed time [s]	30.6	17.3	7.8	72	53.4	103	66.5	350.6
Earliest alarm appearance [s]	26.3	13.7	5.4	65.7	50.2	96.2	17.8	275.3
Elapsed time for FDI [s]	4.3	3.6	2.4	6.3	3.2	6.8	48.7	75.3
Number of operational stages	13	10	4	16	7	16	162	228
Earliest alarm	T201.LO	T201.LO	F203.MLO	P203.HI	T201.LO	A201.LO	T201.LO	
Number of alarms during FDI	1	1	1	1	1	1	3	9
Eye movement distance [cm]	61.6	47.6	30	120.9	37.1	76.3	848.2	1221.7

We collected the measured data of the 29 variables that have alarm limits and obtained their normal ranges. Accordingly, we tightly redefined the PH, PL, and VL values. A margin was defined as 2% of a variable's measurement range. As shown in Fig. 14, PH value is defined as the maximum value of a variable in normal fluctuation plus the margin; PL value is set to the minimum value of the variable in normal fluctuation minus the margin; VL is set to the value of the maximum rate of change plus a small value. The redefined alarm system issued a lot of alarms after a malfunction. After adjusting these alarm limits, an optimum solution (alarm system β) was obtained based on the evaluation.

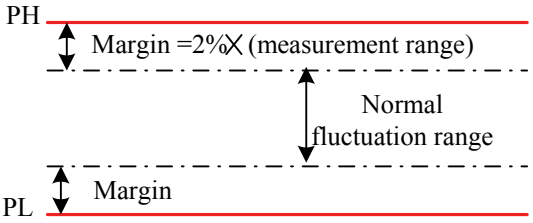

Fig. 14 Setting of PH and PL

Evaluation of Alarm system β

Table 10 shows the alarm settings of alarm system β. Figure 15 illustrates the changes in total *AS* values after a fuel leak under alarm system β. Comparing with Fig. 13, we see that alarm system β effectively helps distinguish failure causes and shortens the time to accomplish the FDI process. Table 11 lists the three alarms after a fuel leak by using alarm system β. These alarm messages supplied useful information to identify the failure cause.

Table 10 Settings of alarm system β

Limit / Tag	HH	PH	PL	LL	VL	Unit 1	MH	ML	Unit 2
A201	10	10	**2.41**	**0.5**	10	%	100	0	%
A202	**275**	**35.7**	0	0	500	ppm	100	0	%
C208	-	-	-	-	-	-	**60**	**40**	%
F201	100	**84.4**	**75.9**	0	100	t/h	-	-	-
F202	10	**7.43**	**6.58**	0	10	t/h	100	0	%
F203	-	-	-	-	-		100	**40**	%
F204	100	100	**25**	**20**	100	t/h	100	0	%
F205	100	**83.1**	0	0	100	t/h	100	0	%
F206	10	**2.08**	0	0	10	t/h	100	0	%
L201	100	**50**	**-50**	-100	200	mm	100	0	%
L202	**95**	**5.01**	**-5.3**	**-95**	200	mm	100	0	t/h
P201	**90**	**82.6**	**75**	**70**	100	Kg/cm^2	100	0	%
P202	100	**86.6**	0	0	100	Kg/cm^2	-	-	-
P203	100	**9.76**	**-18.9**	-100	200	Kg/cm^2	100	0	%
P204	15	15	**2.2**	**2**	15	Kg/cm^2	100	0	%
P205	15	**13.3**	0	0	15	Kg/cm^2	-	-	-
P206	100	**99.2**	**94.7**	0	100	Kg/cm^2	-	-	-
T201	**520**	**496**	**470**	**465**	300	ºC	10	0	t/h
T202	600	600	0	0	600	ºC	-	-	-
T203	400	**307**	0	0	400	ºC	-	-	-
T204	100	**92**	**87.1**	0	100	ºC	-	-	-

Characters in shading: modified items from alarm system α

We evaluated alarm systems for seven malfunctions (Mal-1 ~ Mal-7) and repeated the evaluations for an optimum solution. Table 12 shows evaluation results of alarm system β. Most of earliest alarms are presented faster than system α. Even early alarms are helpful to detect abnormalities. Since FDI needs to confirm a certain number of symptoms, it costed the operator model more time to verify additional symptoms after these alarms, for example, the cases of Mals-5 and -6. The corresponding earliest alarms for the seven malfunctions are F202.LO, P203.LO, F203.MLO, P203.HI, T204.LO, F202.HI, and C208.MLO, respectively, which effectively warn of the typical abnormalities of the corresponding malfunctions. Generally, alarm system β decreases the number of operational stages, the total length of eye movement, and the elapsed time for FDI of seven malfunctions. The number of alarms during FDI is basically acceptable. Alarm system β is not an optimum solution for some malfunctions, but it is important to evaluate the alarm system as a whole.

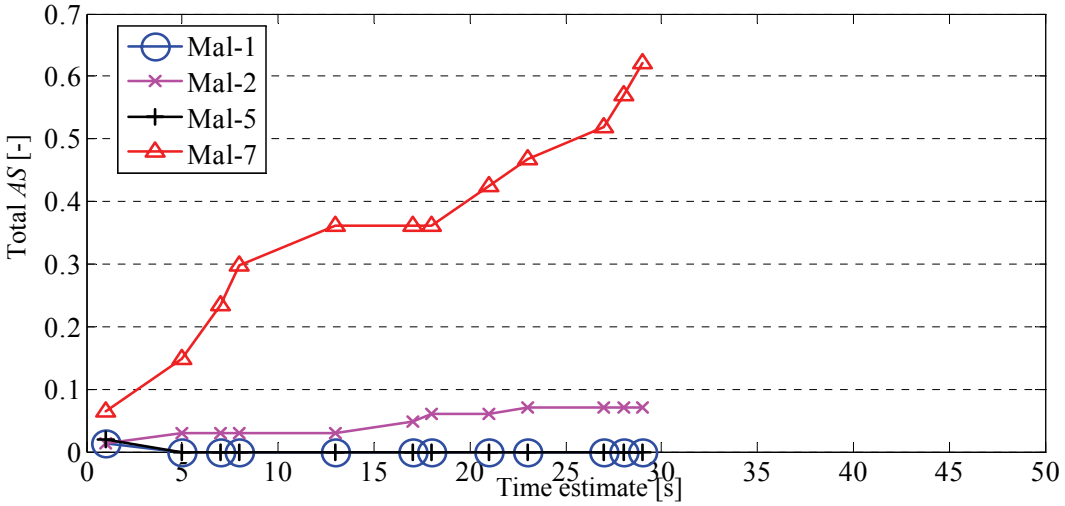

Fig. 15 Changes in total *AS* values for alarm system β

Table 11 Alarms after fuel leak for alarm system β

No.	Time after fuel leak [s]	Alarm
1	23	C208.MLO
2	29	F202.HI
3	45	P201.LO

Table 12 Evaluation results of alarm system β

Criterion \ Malfunction	Mal-1	Mal-2	Mal-3	Mal-4	Mal-5	Mal-6	Mal-7	Total
Total elapsed time [s]	12.5	6	7.7	18.1	15.8	66.8	52.8	179.7
Earliest alarm appearance [s]	9.4	2.9	5.1	12.1	13.3	53.8	24	120.6
Elapsed time for FDI [s]	3.1	3.1	2.6	6.0	2.5	13.0	28.8	59.1
Number of operational stages	7	7	4	16	4	36	83	157
Earliest alarm	F202.LO	P203.LO	F203.MLO	P203.HI	T204.LO	F202.HI	C208.MLO	
Number of alarms during FDI	1	1	1	1	1	2	3	10
Eye movement distance [cm]	32.0	34.8	30.0	120.9	24.9	144.2	383.3	770.1

Conclusion

A quantitative evaluation approach based on an operator model was proposed for evaluating alarm systems during emergencies. Through this model-based method, we located the weak points of alarm systems and improved them. We examined the effectiveness of this approach through a case study of a boiler plant. The presented method can be used to support alarm system design and evaluation. We are going to establish a practical evaluation method.

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).