ISE-TR-88-75

PERFORMANCE ANALYSIS OF A SAFETY MONITORING SYSTEM UNDER HUMAN-MACHINE INTERFACE OF SAFETY-PRESENTATION TYPE

by

Toshiyuki INAGAKI

and

Yasuhiko IKEBE

July 2, 1988

INSTITUTE
OF
INFORMATION SCIENCES AND ELECTRONICS

UNIVERSITY OF TSUKUBA

PERFORMANCE ANALYSIS OF A SAFETY MONITORING SYSTEM UNDER HUMAN-MACHINE INTERFACE OF SAFETY-PRESENTATION TYPE

TOSHIYUKI INAGAKI and YASUHIKO IKEBE

Institute of Information Sciences and Electronics
University of Tsukuba, Tsukuba, Ibaraki 305 JAPAN

Abstract - This paper introduces a safety monitoring system equipped with a cold-standby console display under human-machine interface of safety-presentation type. We analyze probabilistically the performance of the safety monitoring system. A set of order relation is established for unconditional intensities of event modes of the safety monitoring system to show the effectiveness of equipping a standby redundant console display for acquiring plant safety under human-machine interface of safety-presentation type.

I. INTRODUCTION

A plant safety monitoring system has the key to plant safety as well as safety of plant personnel and the general public. There are plenty of studies that are pertinent to safety monitoring systems or protective systems; e.g. [1-8]. One of common assumptions in those studies is that a fault detection sensor can suffer from two modes of failure; (a) failure to generate an alarm upon plant failure and (b) generation of a spurious alarm when the plant is in its normal operating conditions.

Inagaki & Ikebe [10] have shown that the following third mode of sensor failure must be incorporated into our consideration; (c) sensor at the plant is damaged by the event which caused plant failure. The third mode of failure disables the sensor from detecting plant failure or generating an alarm signal. A real example of the third mode of sensor failure can be found in [11, pp. 112-136] concerning an accident of aircraft engine fire; when a jet engine got fire, the fire detection sensor at the engine could not send any alarm signal because the sensor was destroyed by the engine explosion that caused the fire.

We encounter here an issue of human-machine interface for a safety monitoring system in dealing with the third mode of sensor failure. We say that the safety monitoring system has human-machine interface of 'fault-warning type' if (1) an alarm is given to the operator when the failed condition of the plant is detected and (2) no actual message is given to the operator as far as the failed condition of the plant is not detected. Note that the fault-warning type interface fails to give an alarm upon plant failure if the plant failure caused the third mode of sensor failure.

The occurrence of the third mode of sensor failure can be detected if we adopt human-machine interface of 'safety-presentation type', in which (1) an alarm message is given to the operator when the failed condition of the plant is detected and (2) a safety message is given continuously to the operator while the failed condition of the plant is not detected. Inagaki & Ikebe [10] have proved that the human-machine interface of safety-presentation type is superior to the fault-warning type interface in the well-defined sense of avoiding catastrophic accidents of the plant. However it is also shown in [10] that the safety-presentation type interface is likely to cause unnecessary plant shutdowns, in which the plant is shut down even though it is actually in its normal operating

conditions.

This paper introduces a safety monitoring system which is equipped with a cold-standby console display, where a console display is used as a device to give the plant state information to the operator. We give a probabilistic analysis for the time-dependent behavior of the performance of the safety monitoring system under human-machine interface of safety-presentation type. We establish a set of order relation to show the effectiveness of equipping a standby redundant console display under the interface of safety-presentation type.

II. MODEL DESCRIPTION

Consider a safety monitoring system for a plant. The safety monitoring system consists of three units: sensor, console display, and operator. The sensor monitors the plant and transmits signals regarding the plant state to the console display. The operator shuts down the plant immediately when the console display tells the operator that the plant has failed.

We make the following assumptions.

Assumptions:

1. The plant has two states:

   a. Safe (S) state, in which the plant is in its normal operating condition.

   b. Unsafe (U) state, in which the plant is in its failed condition and must be shut down immediately.

We assume an arbitrary life distribution for the plant; let f_p and F_p denote the probability density function (pdf) and the cumulative distribution function (cdf) of the plant life, respectively.

2. The sensor has four states:

   a. Normal (NM) state, in which the sensor identifies the plant state correctly. No delay is assumed in the detection of the plant failure occurrence.

   b. Positively failed (PF) state, in which the sensor regards the safe plant as being (U).

   c. Negatively failed (NF) state, in which the sensor regards the unsafe plant as being (S).

d. Damaged (D) state, in which the sensor is destroyed when the plant goes from (S) to (U) and thus the sensor cannot transmit any signal to the console display.

The sensor has an arbitrary life distribution; we denote the pdf as f_s and the cdf as F_s. The state transition probabilities for the PF and NF failures of the sensor are defined as:

a_{PF} = Pr{next enters (PF) | leaves (NM)}

a_{NF} = Pr{next enters (NF) | leaves (NM)}

where $a_{PF} + a_{NF} = 1$. We also define the probability of sensor destruction upon plant failure as:

b_s = Pr{sensor enters (D) | plant goes from (S) to (U)}

3. The console display has two states:

a. Working (W) state, in which the console display correctly shows on its screen the plant state information given by the sensor. No delay is assumed in displaying the plant state information.

b. Failed (F) state, in which the console display fails to show any plant state information.

The console display has an arbitrary life distribution; let us denote the pdf as f_d and the cdf as F_d. We assume that f_d is unimodal or monotone for which $f_d(0) > 0$. This assumption is required for establishing Property 1 in Section VI.

4. The operator is free from any error in reading the information given on the console display. The operator shuts down the plant immediately when the console display tells that the plant went from (S) to (U).

5. The plant, the sensor, and the console display are up and new at the initial time $t = 0$ and fail independently with the exception of cases in which the sensor is destroyed when the plant goes from (S) to (U).

6. Any state transition is irreversible: neither intermittent failure nor maintenance action is considered.

III. HUMAN-MACHINE INTERFACE FOR A SAFETY-MONITORING SYSTEM

We say that a safety monitoring system has human-machine interface of "fault-warning type" if the plant state is shown on the console display according to the following rules:

1. No message is shown on the console display as far as the plant is regarded as being (S).

2. An "alarm message" is given on the console display immediately when the console display receives the sensor signal telling that the plant went from (S) to (U).

The major drawback of the fault-warning type interface is the following: The unsafe plant is not shut down if the sensor is damaged when the plant goes from (S) to (U); the operator is to regard the plant as being (S) because he is not given any "alarm message".

One of possibble solutions to resolve the drawback will be to replace the fault-warning type interface by the interface of "safety-presentation type". We say that a safety monitoring system has human-machine interface of safety-presentation type if the plant state is indicated on the console display according to the following rules:

1. The console display continues to show a "safety message" as far as the plant is regarded as being (S).

2. An alarm message replaces the safety message immediately when the plant failure is detected by the sensor.

If the plant failure causes sensor destruction under the interface of safety-presentation type, every message disappears from the console display and the operator can recognize that something became wrong with the plant or the safety monitoring system, even though no alarm is actually given.

It is shown in [10] , in terms of unconditional intensities [9], that the safety-presentation type interface is more capable than the fault-warning type in avoiding catastrophic accidents. However the safety-presentation type interface has a drawback that it is likely to cause unnecessary plant shutdowns.

IV. SAFETY-MONITORING SYSTEM WITH A STANDBY CONSOLE DISPLAY

This paper shows that equipping a cold-standby redundant console display enables to mitigate the proneness to unnecessary plant shutdowns of the safety-presentation type interface. We make the following assumptions.

Assumptions:

7. A safety monitoring system is equipped with a redundant console display which is in a cold-standby position while the primary console display is in use: the redundant console display is up and new at the initial time $t = 0$ and never fails while standing by.

8. When the primary console display ceases to show a message, the standby console display replaces the primary one immediately. The safety monitoring system is reconfigured so that sensor signals are transmitted to the newly activated console display (which we call hereafter the secondary console display). We assume that switching over to the secondary console display is instantaneous, and that the reconfiguration process is free from any errors.

9. The operator shuts down the plant immediately when the secondary console display ceases to show a message.

10. The secondary console display is assumed to have the same life distribution as the primary console display. (This assumption is introduced solely for simplicity of notation in the subsequent sections. Extension is straightforward to cases in which the primary and the secondary console displays have distinct life distributions.)

Let us define a system state as an ordered triplet (sensor state, console display state, plant state). The possible state transitions is depicted in Figure 1. We note here a distinctive feature of the safety monitoring system with a cold-standby redundant console display under safety-presentation type interface: The safety monitoring system can distinguish failure of the primary console display from plant failure accompanying the sensor destruction. If the message disappearence was due to failure of the primary console display, the lost message can be recovered immediately on the secondary console display. The lost message can never be recovered on the secondary console display, however, if the sensor was damaged when the plant went from (S) to (U).

V. PROBABILISTIC EVALUATION

Consider the following three modes of events:

(A) Mode 1: unnecessary plant shutdown, where the plant is shut down even though it is actually in its normal operating condition.

(B) Mode 2: successful prevention of an accident, where the plant is shut down immediately when the plant became unsafe.

(C) Mode 3: catastrophic accident, which results from failure in shutting down the plant which became unsafe.

For each of these three modes of events we quantify the unconditional intensities [9]. The unconditional intensity of events of mode i, denoted as $w_i(t)$ for i = 1,..., 3, is defined as follows:

$$w_i(t) = \lim_{h \to 0} \Pr\{\text{events of mode i occurs in } (t, t+h) \mid E_0\} / h \qquad (1)$$

where E_0 denotes the event that the plant and every unit of the safety monitoring system were up and new at the initial time t = 0.

We have the following set of unconditional intensities for the case in which a cold-standby redundant console display is provided for the safety monitoring system under safety-presentation type interface.

(A) Mode 1: unnecessary plant shutdown

$$w_1(t) = \{a_{PF} f_s(t) [\bar{F}_d(t) + \int_0^t f_d(u) \bar{F}_d(t-u)\, du] +$$

$$+ [\bar{F}_s(t) + a_{NF} F_s(t)] \int_0^t f_d(u) f_d(t-u)\, du\} \bar{F}_p(t) \qquad (2)$$

where $\bar{F}(t) = 1 - F(t)$.

(B) Mode 2: successful accident prevention

$$w_2(t) = [\bar{F}_s(t) + b_s a_{NF} F_s(t)] \{\bar{F}_d(t) + \int_0^t f_d(u) \bar{F}_d(t-u)\, du\} f_p(t) \qquad (3)$$

(C) Mode 3: catastrophic accident

$$w_3(t) = (1 - b_s) a_{NF} F_s(t) \{\bar{F}_d(t) + \int_0^t f_d(u) \bar{F}_d(t-u)\, du\} f_p(t) \qquad (4)$$

VI. COMPARISON

Let us compare the following two configurations for the safety monitoring system under safety-presentation type interface: (1) Safety monitoring system without any redundant console display and (2) Safety monitoring system equipped with a cold-standby console display. To avoid confusion, let the unconditional intensity of events of mode i be denoted as $w_i(t; 1D)$ for Case 1 and as $w_i(t; 2D)$ for Case 2, where '1D' or '2D' indicates the total number of displays in the safety monitoring system. The unconditional intensity $w_i(t; 2D)$ is exactly the $w_i(t)$ derived in Section V. Note that $w_i(t; 1D)$ is obtained by the following procedures:

a) Replace $\int_0^t f_d(u)\, f_d(t-u)\, du$ in $w_i(t; 2D)$ by $f_d(t)$.

b) Replace $[\overline{F}_d(t) + \int_0^t f_d(u)\, \overline{F}_d(t-u)\, du]$ in $w_i(t; 2D)$ by $\overline{F}_d(t)$.

Then we have:

$$w_1(t; 1D) = \{a_{PF}\, f_s(t)\, \overline{F}_d(t) + [\overline{F}_s(t) + a_{NF}\, F_s(t)]\ f_d(t)\}\, \overline{F}_p(t) \tag{5}$$

$$w_2(t; 1D) = [\overline{F}_s(t) + b_s\, a_{NF}\, F_s(t)]\, \overline{F}_d(t)\, f_p(t) \tag{6}$$

$$w_3(t; 1D) = (1 - b_s)\, a_{NF}\, F_s(t)\, \overline{F}_d(t)\, f_p(t) \tag{7}$$

We need the following lemma for examining the above mentioned two configurations.

Lemma: Let f be a pdf for a continuous nonnegative random variable. Assume f is unimodal or monotone for which $f(0) > 0$. Then there exists a nonnegative μ such that:

$$f(t) \le \int_0^t f(u)\, f(t-u)\, du \qquad \text{for all } t \in [\mu, \infty) \tag{8}$$

(Proof) Take an arbitrary t for which $f(t) \le f(0)$ holds. Then we have:

$$f(t) - \int_0^t f(u)\, f(t-u)\, du \le f(t)\, [1 - 2\, F(t/2)]$$

where we note:

$$\int_0^t f(u)\, f(t-u)\, du \ge 2 \int_0^{t/2} f(u)\, f(t)\, du = 2\, f(t)\, F(t/2)$$

Let t_1 and t_2 be defined by:

$$t_1 = \min \{t:\ f(0) \geq f(t)\}$$

$$t_2 = \min \{t:\ F(t/2) \geq 1/2\}$$

Such t_1 and t_2 exist because the pdf f has only a finite number of points of discontinuity and the cdf F is continuous and monotone. If we set μ as:

$$\mu = \max \{t_1, t_2\}$$

then (8) follows immediately. □

The following set of order relation holds for unconditional intensities of events of mode i for $i = 1,..., 3$.

Property 1: There exist μ_1 and μ_2 such that:

$$w_1(t; 1D) > w_1(t; 2D) \quad \text{for all } t \in [0, \mu_1] \tag{9}$$

$$w_1(t; 1D) = w_1(t; 2D) \quad \text{for some } t \in (\mu_1, \mu_2) \tag{10}$$

$$w_1(t; 1D) < w_1(t; 2D) \quad \text{for all } t \in [\mu_2, \infty) \tag{11}$$

(Proof) Let us define h as:

$$h(t) = w_1(t; 2D) - w_1(t; 1D)$$

Then we have:

$$h(0) = - f_d(0) < 0 \tag{12}$$

Since h is a continuous function of t, there exists $\mu_1 > 0$ such that:

$$h(t) < 0 \quad \text{for all } t \in [0, \mu_1],$$

implying (9).

There exists $\mu_2 > 0$, by Lemma, such that:

$$f_d(t) \leq \int_0^t f_d(u)\, f_d(t-u)\, du \qquad \text{for all } t \in [\mu_2, \infty)$$

Thus we have:

$$h(t) = a_{PF} f_s(t) \int_0^t f_d(u) \bar{F}_d(t-u)\, du] +$$

$$+ [\bar{F}_s(t) + a_{NF} F_s(t)] [\int_0^t f_d(u) f_d(t-u)\, du - f_d(t)] \bar{F}_p(t)$$

$$> [\bar{F}_s(t) + a_{NF} F_s(t)] [\int_0^t f_d(u) f_d(t-u)\, du - f_d(t)] \bar{F}_p(t) \geq 0$$

$$\text{for all } t \in [\mu_2, \infty) \tag{13}$$

which implies (11).

Because of continuity of h, we have (10) from (12) and (13). □

Property 2:

$$w_2(t; 1D) \leq w_2(t; 2D) \quad \text{for all } t \in [0, \infty) \tag{14}$$

The equality holds at the initial time t = 0.

(Proof) Since

$w_2(t; 2D) - w_2(t; 1D)$

$$= f_p(t) [\bar{F}_s(t) + b_s a_{NF} F_s(t)] \int_0^t f_d(u) \bar{F}_d(t-u)\, du \tag{15}$$

the result follows immediately. □

Property 3:

$$w_3(t; 1D) \leq w_3(t; 2D) \quad \text{for all } t \in [0, \infty) \tag{16}$$

The equality holds for $b_s = 1$ or at the initial time t = 0.

(Proof) We have:

$w_3(t; 2D) - w_3(t; 1D)$

$$= (1 - b_s) a_{NF} F_s(t) f_p(t) \int_0^t f_d(u) \bar{F}_d(t-u)\, du \tag{17}$$

which yields the result. □

At the first glance of (11) or (16), it might seem that equipping a standby redundant console display brings about undesirable characteristics on the safety-presentation type interface. However it should be noted that the 'undesirable' order relation (11) or (16) is just a reflection of the 'desirable' fact that the operation time of the plant becomes longer by equipping a standby redundant console display in the safety monitoring system: Once the plant was shutdown upon message disappearance from the console display, neither spurious plant shutdown nor catastrophic accident can occur after that. If the safety monitoring system has no redundant console display, the plant is shut down immediately upon the first message disappearance from the console display even though the message disappearance was due to display failure. The safety monitoring system with a standby redundant console display, on the other hand, enables the safe plant to continue its operation at that time, which yields the longer operation time of the plant.

VII. DISCUSSIONS

1. Let us extend our examination to incorporate the case of the usual interface of fault-warning type. Let $w_i(t; FW)$ denote the unconditional intensity of events of mode i under the fault-warning type interface. We do not have to imagine a case in which the safety monitoring system is equipped with a standby redundant console display; equipment of a standby redundant console display is meaningless under the fault-warning type interface. The intensities $w_i(t; FW)$ are given in [10] as:

$$w_1(t; FW) = a_{PF}\, f_s(t)\, \overline{F}_d(t)\, \overline{F}_p(t) \tag{18}$$

$$w_2(t; FW) = (1 - b_s)\, \overline{F}_s(t)\, \overline{F}_d(t)\, f_p(t) \tag{19}$$

$$w_3(t; FW) = \{a_{NF}\, F_s(t) + [b_s\, \overline{F}_d(t) + F_d(t)]\, \overline{F}_s(t) + + a_{PF} \int_0^t f_s(u)\, F_d(u)\, du\}\, f_p(t) \tag{20}$$

We have:

$$w_1(t; FW) \leq w_1(t; 2D) \} \text{ for all } t \in [0, \infty) \quad (21)$$

$$w_3(t; 2D) \leq w_3(t; FW) \quad \text{for all } t \in [0, \infty) \quad (22)$$

where (21) follows immediately from (2) and (18), while (22) is established from (4) and (20) by noting:

$$\overline{F}_d(t) + \int_0^t f_d(u)\, \overline{F}_d(t-u)\, du \leq 1$$

Combining with the order relation for $w_i(t; FW)$ and $w_i(t; 1D)$ given in [10], we obtain the following sets of properties:

Property 1a:

$$w_1(t; FW) \leq \min \{w_1(t; 1D), w_1(t; 2D)\} \quad \text{for all } t \in [0, \infty)$$

Property 2a:

$$w_2(t; FW) \leq w_2(t; 1D) \leq w_2(t; 2D) \quad \text{for all } t \in [0, \infty)$$

Property 3a:

$$w_3(t; 1D) \leq w_3(t; 2D) \leq w_3(t; FW) \quad \text{for all } t \in [0, \infty)$$

2. We have assumed so far that the operator shuts down the plant immediately when he no longer finds any message on the console display (Assumption 9), which we call Model 1. We can extend Model 1 to a more practical one, Model 2, in which the operator is given the right to decide whether to shut down the plant or not. More precisely, the operator diagnoses the plant without any use of the safety monitoring system when the secondary console display ceases to show any message. The plant is shut down if the operator judges the plant as being (U), while the operator leaves the plant as it is if he regards the plant as being (S). Inagaki & Ikebe [10] have shown that

$$w_1(t; 1D, \text{Model 2}) \leq w_1(t; 1D, \text{Model 1})$$

even though the operator may cause some error in judging the plant state under the safety-presentation type interface. We can prove the same order relation

$w_1(t; 2D, Model 2) \leq w_1(t; 2D, Model 1)$

for the current case in which the safety monitoring system has a standby redundant console display.

VIII. CONCLUSION

This paper has given a probabilistic analysis for a safety monitoring system under human-machine interface of safety-presentation type in which the system is equipped with a standby redundant console display. We have established a set of order relation among unconditional intensities $w_i(t; 1D)$, $w_i(t; 2D)$ and $w_i(t; FW)$ to show the significance of human-machine interface as well as the effectiveness of equipping a standby redundant console display for acquiring plant safety.

ACKNOWLEDGMENT

We would like to note here that discussion with Dr. Sadaaki Miyamoto, University of Tsukuba, was stimulative and useful in giving our proof of Lemma in Section VI.

REFERENCES

1. J.M. Kontoleon, N. Kontoleon, and N.G. Chrisochoides, Optimum active-inactive times in supervised protective systems for nuclear reactors, *Nuclear Science and Engineering*, 55, 219-224 (1974).
2. S.C. Chay and M. Mazumdar, Determination of test intervals in certain repairable standby protective systems, *IEEE Trans. Reliab.* R-24, 201-205 (1975).
3. H. Kumamoto and E.J. Henley, Protective system hazard analysis, *Ind. Engr. Chem.* 13, 274-276 (1978).
4. I. Takami, T. Inagaki, K. Inoue, and E. Sakino, Optimal allocation of fault detectors, *IEEE Trans. Reliab.* R-27, 360-362 (1978).

5. T. Inagaki, K. Inoue, and H. Akashi, Optimization of staggered inspection schedules for protective systems, *IEEE Trans. Reliab.* R-29, 170-173 (1980).
6. C. Singh and A.D. Patton, Protective system reliability modeling: unreadiness probability and mean duration of undetected faults,*IEEE Trans. Reliab.* R-29, 339-340 (1980).
7. K. Inoue, T. Kohda, H. Kumamoto, and I. Takami, Optimal structure of sensor systems with two failure modes, *IEEE Trans. Reliab.* R-31, 119-120 (1982).
8. H. Kumamoto, H. Otsuka, and K. Inoue, Expected numbers of failures caused by protective systems, *IEEE Trans. Reliab.* R-31, 219-221 (1982).
9. T. Inagaki and E.J. Henley, Probabilistic evaluation of prime implicants and top-events for non-coherent systems, *IEEE Trans. Reliab.* R-29, 361-367 (1980).
10. T. Inagaki and Y. Ikebe, A mathematical analysis of human-machine interface configurations for a safety monitoring system, *IEEE Trans. Reliab.* R-37, 35-40 (1988).
11. T. Kato and T. Ueda, *Messages from Airline Captains*, Yuhikaku, Tokyo, (1986) (in Japanese).

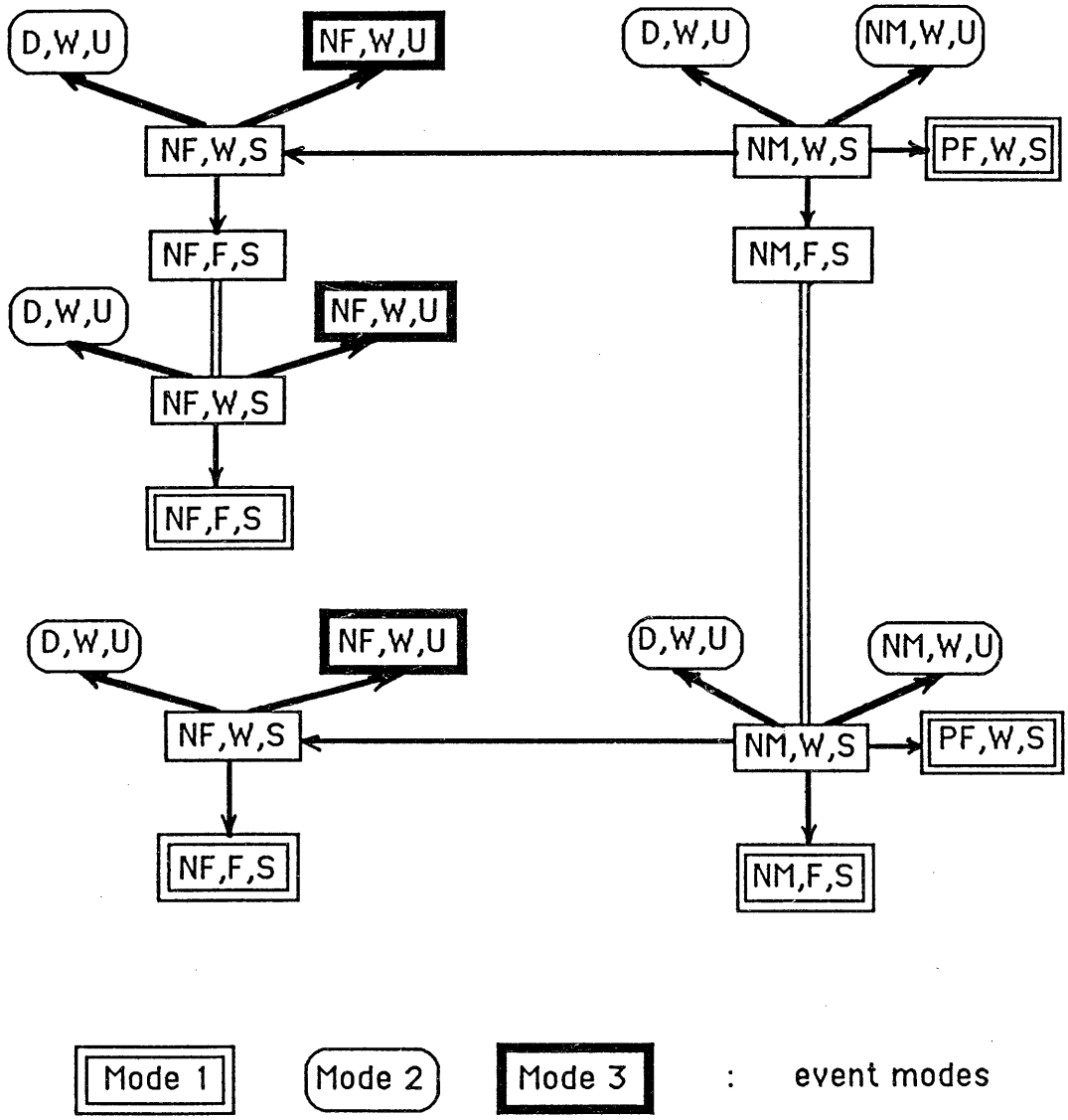

Figure 1. State transitions under safety-presentation type interface

INSTITUTE OF INFORMATION SCIENCES AND ELECTRONICS
UNIVERSITY OF TSUKUBA
TSUKUBA-SHI, IBARAKI 305 JAPAN

REPORT DOCUMENTATION PAGE	REPORT NUMBER ISE-TR-88-75

TITLE

PERFORMANCE ANALYSIS OF A SAFETY MONITORING SYSTEM UNDER HUMAN-MACHINE INTERFACE OF SAFETY-PRESENTATION TYPE

AUTHOR(S)

TOSHIYUKI INAGAKI and YASUHIKO IKEBE

Institute of Information Sciences and Electronics

University of Tsukuba, Tsukuba, Ibaraki 305 JAPAN

REPORT DATE	NUMBER OF PAGES
July 2, 1988	15
MAIN CATEGORY: Reliability theory	CR CATEGORIES

KEY WORDS

Safety monitoring system, Unconditional intensity, Human-machine interface

ABSTRACT

Abstract - This paper introduces a safety monitoring system equipped with a cold-standby console display under human-machine interface of safety-presentation type. We analyze probabilistically the performance of the safety monitoring system. A set of order relation is established for unconditional intensities of event modes of the safety monitoring system to show the effectiveness of equipping a standby redundant console display for acquiring plant safety under human-machine interface of safety-presentation type.

SUPPLEMENTARY NOTES