ISE-TR-86-62

ON HUMAN-MACHINE INTERFACE FOR SYSTEM SAFETY : COMPARISON OF FAULT-WARNING AND SAFETY-ANNOUNCING CONFIGURATIONS

by

Toshiyuki INAGAKI

and

Yasuhiko IKEBE

December 26, 1986

INSTITUTE
OF
INFORMATION SCIENCES AND ELECTRONICS

UNIVERSITY OF TSUKUBA

ON HUMAN-MACHINE INTERFACE FOR SYSTEM SAFETY: COMPARISON OF FAULT-WARNING AND SAFETY-ANNOUNCING CONFIGURATIONS

Toshiyuki Inagaki and Yasuhiko Ikebe

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

Abstract - This paper discusses two configurations of human-machine interface: (1) conventional "fault-warning configuration" which gives a message of warning upon detecting plant failure and (2) "safety-announcing configuration", newly introduced in this paper, which can give a message of safety as well as a message of warning. These configurations are examined qualitatively and quantitatively to show that the safety-announcing configuration is superior to the fault-warning configuration in terms of avoiding catastrophes.

1. INTRODUCTION

A correct and immediate fault detection is vital for maintaining system safety. There exist many studies that deal with safeguarding functions such as fault detection sensors, warning systems, and protective systems; eg, [1-9]. Commonly considered in their models is a case in which a "warning" is given to the system operator when an unsafe phenomenon is detected in the plant that should be protected against a hazard. In other words, the operator regards the plant being safe as far as he receives no warning.

It would, however, be worth while considering a model in which a display device continues to show a "message of safety" stating that the "plant is currently safe" while an unsafe phenomenon is not detected in the plant.

A suggestive report is given in [10, pp 112-136] regarding an aircraft engine fire: Upon fire of a jet engine, the engine fire warning system in the cockpit gave no warning. An investigation after landing found that the fire warning system failed to work because the fire detection sensor at the engine was destroyed due to engine explosion that caused the fire.

Suppose the aircraft was equiped with a lamp that is on while the fire detection sensor sends a signal of "no fire at the engine". When the engine explosion destroyed the fire detection sensor, the "no fire" signal failed to be transmitted and the lamp would go off, which might suggest cockpit crews that "something is wrong" even though the fire warning system fails to give an actual alarm at that time.

This paper discusses two distinct configurations of human-machine interface: (1) conventional "fault-warning configuration" which gives a message of warning upon detecting plant failure, and (2) "safety-announcing configuration", newly introduced in this paper, which can give a message of safety as well as a message of warning. We examine these configurations qualitatively and quantitatively. A comparative study is made to show that the safety-announcing configuration is superior to the fault-warning configuration in terms of capability of avoiding hazards.

Some safety engineers have developed new sensors in various fields of applications [11]. The sensors are designed to announce the plant safety instead of giving a warning upon plant failure. Although developing new sensors is helpful for our purpose discussed here, it does not always follow that we assume the development of a new sensor itself. Conventional sensors can be used in implementing our safety-announcing system. The point lies in changing a strategy of treating sensor signals for showing a message of safety as well as a message of warning.

2. ASSUMPTIONS, NOTATION

Assumptions for all models

1. A system is comprised of three units: (a) sensor, (b) display, and (c) plant. The sensor monitors the plant state and transmits the state information to the display. The display shows on its screen the plant state information given by the sensor.

2. The plant has two states: (a) safe state S, in which the plant works properly, and (b) unsafe state U, in which an unsafe

phenomenon is occurring. When the plant becomes unsafe, an appropriate countermeasure such as an immediate plant shut-off is necessary to avoid a catastrophic accident.

3. The sensor has three states: (a) normal state NM, in which the sensor identifies the plant state correctly, (b) positively failed state PF, in which the sensor regards the plant being unsafe even though the plant is actually safe, and (c) negatively failed state NF, in which the sensor cannot detect any unsafe phenomenon occurring in the plant.

4. The display has two states: (a) normal state NM, in which the display shows correctly on its screen the plant state information given by the sensor, and (b) negatively failed state NF, in which the display fails to show the plant state information given by the sensor.

5. When the plant becomes unsafe, the sensor attached to the plant may be damaged by the unsafe phenomenon occurring in the plant. If the sensor is damaged, the sensor cannot inform the display that the plant has become unsafe, as is the case where we have no sensor in the system. As a matter of convenience, let us regard the "no sensor situation" as the forth state of the sensor, a damaged state D.

6. Units fail s-independently with the exception of cases in which the sensor is damaged due to the unsafe phenomenon occurring in the plant.

7. All units of a system are normal or safe at time 0.

8. Any state transition is irreversible: no intermittent failure is considered and every unit is non-repairable in a mission of duration T.

Notation

NM normal state (sensor, display)

NF negatively failed state (sensor, display)

PF positively failed state (sensor)

D damaged state (sensor)

S safe state (plant)

U unsafe state (plant)

a_{PF} Pr{next enters state PF | leaves state NM}

a_{NF} Pr{next enters state NF | leaves state NM}, $a_{PF} + a_{NF} = 1$

b_S Pr{sensor is damaged | plant becomes unsafe}

c_{PF} Pr{operator regards the plant unsafe upon disappearance of messages from the display screen | plant is safe}

c_{NF} Pr{operator regards the plant safe upon disappearance of messages from the display screen | plant is unsafe}

c_{OL} Pr{operator overlooks an unsafe phenomenon occurring in the plant under Policy II | plant is becoming unsafe}; Policy II is defined in the text

I_0 event that every unit in the system was up and new at the initial time (t=0)

E_i events of mode i (i = 1, 2, 3): definitions of the modes are given in the text

$w_i(t)$ unconditional intensity for E_i (i = 1, 2, 3); viz,

$$w_i(t) = \lim_{dt \to 0} \frac{1}{dt} \Pr\{E_i \text{ occurs in } (t, t+dt) \mid I_0\}$$

T duration of a mission; $0 \leq t \leq T$

$f(x)$, $F(x)$, $\overline{F}(x)$ pdf{X}, Cdf{X}, Sf{X}

f_Y, F_Y, $\overline{F}_Y$ pdf, Cdf, Sf of unit Y (Y = s for sensor, = d for display, = p for plant)

3. FAULT-WARNING AND SAFETY-ANNOUNCING

Two different configurations can be considered with three units defined above. One is a conventional "fault-warning configuration" and the other is a "safety-announcing configuration" which we will introduce in this paper. The distinction between these two configurations lies solely in a strategy of human-machine interface or a method of giving the plant state information on the screen of the display.

3.1 Fault-Warning Configuration

In the fault-warning configuration the state of the plant is shown on the display screen according to the following rules:

1. As far as the plant is regarded safe, no message is given on the screen.

2. When the display is announced by the sensor that an unsafe phenomenon is occurring in the plant, the display gives a "message of warning" on its screen.

Possible state transitions are depicted in Fig.1, where a system state is defined as an ordered triplet (sensor state, display state, plant state), such as (NM,NM,S) for state 1. The state of a single unit differs between system states connected by an arrow in Fig.1 with the exception of cases where the sensor is damaged when the plant becomes unsafe (see, for example, a transition from state 1 to state 8).

We can see the following five classes of system states:

Class 1. system is free from any failure: state 1

Class 2. system is safe just because the plant is safe; sensor/display subsystem can never generate a message of warning

even if the plant becomes unsafe: states 3, 4, 5, 6

Class 3. catastrophic accident is circumvented since the plant is shut off based on a correct message of warning appeared on the display screen when the plant becomes unsafe: state 7

Class 4. plant is unnecessarily shut off based on an erroneous message of warning: state 2

Class 5. catastrophic accident occurs, since no message of warning is given on the screen of the display when the plant becomes unsafe and thus the plant is not shut off: states 8, 9, 10, 11, 12, 13, 14, 15, 16

As can be seen in the above, safety of the system is diminished by "unrevealed faults" in the sensor/display subsystem and the possibility of sensor destruction upon plant failure.

3.2 Safety-Announcing Configuration

In the safety-announcing configuration the plant state is announced continuously in time on the screen of the display according to the following rules:

1. While the sensor regards the plant being safe, the display continues to show a "message of safety" on its screen.

2. When the sensor detects an unsafe phenomenon occurring in the plant, the "message of safety" that has been shown on the screen is immediately replaced by a "message of warning."

3. Any message that has been shown on the screen disappears immediately when the display fails or the sensor is damaged by an unsafe phenomenon occurring in the plant.

Possible state transitions are depicted in Fig.2. We have six classes of system states, where the first five classes represent

the same situations as classes 1 through 5 of the fault-warning configuration.

Class 1. System is free from any failure: state 1

Class 2. Message of safety on the screen happens to be correct because the plant is actually safe when the sensor is failed negatively: state 3

Class 3. Catastrophic accident is circumvented because of a correct message of warning: state 7

Class 4. Plant is shut off unnecessarily based on a erroneous message of warning: state 2

Class 5. Catastrophic accident occurs since no message of warning is given when the plant becomes unsafe: state 9

Class 6. Disappearance of messages from the screen of the display makes the operator recognize that some unit is wrong in the system: states 4, 5, 8, 10

The sixth and the last class of states includes the following two cases: (a) any message cannot be seen because of a display failure, (b) neither a message of safety nor a message of warning is sent by the sensor because the sensor is damaged by an unsafe phenomenon occurring in the plant. Without any introduction of an auxiliary method for identifying the system state, the operator cannot distinguish which of the above two cases he is facing with.

We consider the following two policies that become effective upon the disappearance of a message from the display screen:

Policy I: The operator shuts off the plant if no message can be seen on the screen.

Policy II: Under the situation where the display shows no message on its screen, the operator estimates the plant state by some means. If the operator thinks that the plant is unsafe, then he shuts off the plant. If the operator regards the plant being safe, then he leaves the plant as it is.

An interpretation of the above policies will be given for the case of an aircraft engine fire in the INTRODUCTION section. Suppose the display ceases to show any message regarding the state of an engine. Under Policy I, the captain shuts off the engine immediately. Under Policy II, the captain estimates the engine state based on instrument indications. He can ask some cabin crew to describe how the engine looks like through the window. Then the captain decides whether to shut off the engine or not.

The point is that safety of the safety-announcing configuration is policy-dependent. Under Policy I, states 4 and 5 in Class 6 represent cases where the plant is shut off unnecessarily, while states 8 and 10 correspond to cases where a catastrophic accident is circumvented by shutting off the engine which is becoming unsafe.

If we choose Policy II, on the other hand, system safety varies depending on what we expect on the operator. Consider the following simple situation:

1. Upon the message disappearance at time u, the operator decides whether to shut off the plant or not. He may fail to take the correct decision at that time.

2. Suppose the plant becomes unsafe at some time t in the interval (u,T] before a mission of duration T completes. The

unsafe phenomenon occurring at time t in the plant may not be recognized by the operator.

Fig.3 shows possible sequences of events in [u,T] for the above situation under Policy II.

4. PROBABILISTIC EVALUATION

To examine characteristics of the fault-warning configuration and the safety-announcing configuration, we will evaluate the unconditional intensities of the following three modes of events:

Mode 1: inappropriate abort of a mission, where the safe plant is shut off because of an erroneous message of warning,

Mode 2: successful prevention of a hazard, where the plant which is becoming unsafe is shut off properly based on a correct message of warning, and

Mode 3: catastrophic accident, which is an end of failure in shutting off the unsafe plant.

4.1 Fault-Warning Configuration

We have the following set of unconditinal intensities [12]:

(A) Mode 1: inappropriate mission abort

$$w_1(t) = a_{PF} f_S(t) \overline{F}_d(t) \overline{F}_P(t) \tag{1}$$

(B) Mode 2: hazard prevention

$$w_2(t) = (1-b_S) f_P(t) \overline{F}_S(t) \overline{F}_d(t) \tag{2}$$

(C) Mode 3: catastrophic accident

$$w_3(t) = f_P(t)\{a_{NF} F_S(t) + [b_S \overline{F}_d(t) + F_d(t)]\, \overline{F}_S(t) + a_{PF} \int_0^t f_S(x) F_d(x) dx\} \tag{3}$$

Intensities are not always uniquely represented. For example, in

(3), the integral term can be expressed as:

$$\int_0^t f_S(x)F_d(x)dx = \int_0^t [F_S(t) - F_S(u)]f_d(u)du$$
$$= F_S(t)F_d(t) - \int_0^t F_S(u)f_d(u)du \qquad (4)$$

where the first equality is justified by the following relation on the interchange of the order of integration:

$$\int_0^t [\int_0^x f_S(x)f_d(u)du]dx = \int_0^t [\int_u^t f_S(x)f_d(u)dx]du$$

We will use the right expression in the right place, especially in Section 4.4.

4.2 Safety-Announcing Configuration with Policy I

Assume we adopt Policy I for our safety-announcing configration. We have the following set of intensities:

(A) Mode 1: inappropriate mission abort

$$w_1(t) = \{a_{PF}f_S(t)\overline{F}_d(t) + [1 - a_{PF}F_S(t)]f_d(t)\}\ \overline{F}_P(t) \qquad (5)$$

(B) Mode 2: hazard prevention

$$w_2(t) = f_P(t)[\overline{F}_S(t) + b_S a_{NF}F_S(t)]\ \overline{F}_d(t) \qquad (6)$$

(C) Mode 3: catastrophic accident

$$w_3(t) = (1-b_S)a_{NF}F_S(t)\overline{F}_d(t)f_P(t) \qquad (7)$$

We note here $w_2(t)$ is increasing in b_S while $w_3(t)$ decreasing in b_S, which exhibits a distinctive feature of the safety-announcing configuration with Policy I: viz, the more easily damaged the sensor is upon plant failure, the more successfully we can avoid catastrophic accidents. This contrasts with the case of the fault-warning configuration in which the sensor must be guarded well against any damage possibly caused by plant failure in order to prevent a catastrophe. The above "paradox" for the safety-announcing configuration with Policy I can be interpreted as follows: When the sensor suffers from a damage

due to plant failure, every message disappears from the screen of the display. Thus we can suspect the plant failure even though a message of warning is not actually shown on the screen of the display. In other words, whether the sensor itself is damaged or not carries an important information regarding the plant state as well as the usual plant state information shown on the screen of the display.

4.3 Safety-Announcing Configuration with Policy II

Assume we take Policy II for our safety-announcing configuration. The intensities of our interest are:

(A) Mode 1: inappropriate mission abort

$$w_1(t) = \{a_{PF} f_s(t) \overline{F}_d(t) + c_{PF}[1 - a_{NF} F_s(t)] f_d(t)\} \overline{F}_p(t) \qquad (8)$$

(B) Mode 2: hazard prevention

$$w_2(t) = \{(1-b_s)\overline{F}_s(t) + b_s(1-c_{NF})[1 - a_{PF} F_s(t)]\} \overline{F}_d(t) f_p(t) + \\ + (1-c_{OL})(1-c_{PF}) f_p(t)[F_d(t) - a_{PF} \int_0^t F_s(u) f_d(u) du] \qquad (9)$$

(C) Mode 3: catastrophic accident

$$w_3(t) = \{(1-b_s) a_{NF} F_s(t) + b_s c_{NF}[1 - a_{PF} F_s(t)]\} \overline{F}_d(t) f_p(t) + \\ + c_{OL}(1-c_{PF}) f_p(t)[F_d(t) - a_{PF} \int_0^t F_s(u) f_d(u) du] \qquad (10)$$

4.4 Comparison

Suppose we are given the following set of units: (a) sensor with reliability characteristics described by a_{PF}, a_{NF} and $F_s(t)$, (b) display with $F_d(t)$, (c) plant with $F_p(t)$. Also assumed given is the probability b_s of sensor destruction upon plant failure, and a triplet (c_{PF}, c_{NF}, c_{OL}) which describes the operator characteristics. Our interest, in this setting, lies in examining the relation among three kinds of configurations discussed in the preceding sections.

To distinguish the configurations, we use symbols $w_1(t)$, $w_2(t)$, $w_3(t)$ for the fault-warning case, $w_1^{I}(t)$, $w_2^{I}(t)$, $w_3^{I}(t)$ for the safety-announcing case with Policy I, and $w_1^{II}(t)$, $w_2^{II}(t)$, $w_3^{II}(t)$ for the safety-announcing case with Policy II.

We have the following set of properties:

Property 1: $w_1(t) \leq w_1^{II}(t) \leq w_1^{I}(t)$ (11)

The left equality holds for $c_{PF} = 0$ and the right for $c_{PF} = 1$.

Proof: This result follows directly from (1), (5), and (8).

Property 2: $w_2(t) \leq \min \{w_2^{I}(t), w_2^{II}(t)\}$ (12)

Equality holds for $b_S = 0$ or $(1-c_{NF})b_S + (1-c_{OL})(1-c_{PF}) = 0$.

Proof: See appendix I.

Property 3: (a) Assume $b_S = 0$. Then we have:

$$w_2^{I}(t) \leq w_2^{II}(t) \tag{13}$$

Equality holds for $(1-c_{OL})(1-c_{PF}) = 0$.

(b) Assume $b_S \neq 0$. Then we have:

$$\begin{cases} w_2^{I}(t) > w_2^{II}(t) & \text{if } h > 0 \\ w_2^{I}(t) = w_2^{II}(t) & \text{if } h = 0 \\ w_2^{I}(t) < w_2^{II}(t) & \text{if } h < 0 \end{cases} \tag{14}$$

where

$$h = c_{NF}A - (1-c_{PF})(1-c_{OL})B \tag{15}$$

$$A = b_S \bar{F}_d(t)[\bar{F}_S(t) + a_{NF}F_S(t)], \quad 0 < A < 1 \tag{16}$$

$$B = \int_0^t [\bar{F}_S(u) + a_{NF}F_S(u)]\, f_d(u)du, \quad 0 < B < 1 \tag{17}$$

Proof: See appendix II.

Property 4: $w_3^{I}(t) \leq w_3^{II}(t) \leq w_3(t)$ (18)

The left equality holds for $b_S c_{NF} + c_{OL}(1-c_{PF}) = 0$. The right equality holds if $b_S(1-c_{NF}) = 0$ and $c_{OL}(1-c_{PF}) = 1$.

Proof: See appendix III.

To be brief, both of the safety-announcing configurations have a decided superiority to the conventional fault-warning configuration in preventing catastrophic accidents, although the latter suffers least from an inappropriate mission abort.

Becase of (13), in which the order relation between $w_2^{I}(t)$ and $w_2^{II}(t)$ varies accoding to circumstances, one may presume at first that the order relation between $w_3^{I}(t)$ and $w_3^{II}(t)$ is also indecisive. We have, however, the definite order relation between $w_3^{I}(t)$ and $w_3^{II}(t)$ as shown in Property 4. This is because the expected length of operation time in the safety-announcing configuration is greater under Policy II than under Policy I: viz, the safety-announcing configuration with Policy II is exposed more to possible plant failures than that with Policy I.

Remark. All the order relations given in Properties 1 through 4 hold for the expected numbers of the corresponding modes of events occurring during the interval [0,T].

APPENDIX I

We have:

$$w_2^{I}(t) - w_2(t) = b_s[\overline{F}_s(t) + a_{NF}F_s(t)]\,\overline{F}_d(t)f_p(t) \geq 0$$

Note:

$$F_d(t) - a_{PF}\int_0^t F_s(u)f_d(u)du = \int_0^t [\overline{F}_s(u) + a_{NF}F_s(u)]f_d(u)du \geq 0 \quad (A.1)$$

Then:

$$w_2^{II}(t) - w_2(t) = (1-c_{NF})[w_2^{I}(t) - w_2(t)] +$$
$$+ (1-c_{OL})(1-c_{PF})f_p(t)\int_0^t [\overline{F}_s(u) + a_{NF}F_s(u)]f_d(u)du \geq 0,$$

which proves Property 2.

APPENDIX II

Note:

$$w_2^{I}(t) - w_2^{II}(t) = f_p(t)\{c_{NF}b_s\bar{F}_d(t)[\bar{F}_s(t) + a_{NF}F_s(t)] - (1-c_{OL})(1-c_{PF})\int_0^t [\bar{F}_s(u) + a_{NF}F_s(u)]f_d(u)du\}$$

(a) Assume $b_s = 0$. Then:

$$w_2^{I}(t) - w_2^{II}(t) = -(1-c_{OL})(1-c_{PF})f_p(t)\int_0^t [\bar{F}_s(u)+a_{NF}F_s(u)]f_d(u)du \leq 0$$

(b) Assume $b_s \neq 0$. Then:

$$w_2^{I}(t) - w_2^{II}(t) = f_p(t)[c_{NF}A - (1-c_{OL})(1-c_{PF})B],$$

where A and B are defined by (16) and (17), respectively. Thus:

$$\mathrm{sgn}[w_2^{I}(t) - w_2^{II}(t)] = \mathrm{sgn}[c_{NF}A - (1-c_{OL})(1-c_{PF})B] = \mathrm{sgn}(h),$$

where sgn(x) denotes the sign of x, which proves Property 3.

APPENDIX III

Applying (A.1) to (9), we have $w_3^{I}(t) \leq w_3^{II}(t)$. The point for proving $w_3^{II}(t) \leq w_3(t)$ lies in applying (4) to (3). After some calculations, we obtain:

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

By applying (A.1), we have:

$$w_3(t) - w_3^{II}(t) = b_s(1-c_{NF})[\bar{F}_s(t) + a_{NF}F_s(t)]\,\bar{F}_d(t)f_p(t) + [1-c_{OL}(1-c_{PF})]f_p(t)\int_0^t [\bar{F}_s(u) + a_{NF}F_s(u)]f_d(u)du \geq 0,$$

which proves Property 4.

ACKNOWLEDGMENTS

The authors would like to acknowledge the support of The Ministry of Education, Science and Culture under Grant-in-Aid EYS 61750375.

REFERENCES

[1] J.M. Kontoleon, N. Kontoleon, N.G. Chrisochoides, "Optimum active-inactive times in supervised protective systems for nuclear reactors", Nuclear Science and Engineering, vol 55, 1974, pp 219-224.

[2] S.C. Chay, M. Mazumdar, "Determination of test intervals in certain repairable standby protective systems", IEEE Trans. Reliability, vol R-24, 1975 Aug, pp 201-205.

[3] H. Kumamoto, E.J. Henley, "Protective systems hazard analysis", Ind. Engr. Chem., vol 13, 1978, pp 274-276.

[4] I. Takami, T. Inagaki, K. Inoue, E. Sakino, "Optimal allocation of fault detectors", IEEE Trans. Reliability, vol R-27, 1978 Dec, pp 360-362.

[5] T. Inagaki, K. Inoue, H. Akashi, "Optimization of staggered inspection schedules for protective systems", IEEE Trans. Reliability, vol R-29, 1980 Jun, pp 170-173.

[6] C. Singh, A.D. Patton, "Protection system reliability modeling: unreadiness probability and mean duration of undetected faults", IEEE Trans. Reliability, vol R-29, 1980 Oct, pp339-340.

[7] K. Inoue, T. Kohda, H. Kumamoto, I. Takami, "Optimal structure of sensor systems with two failure modes", IEEE Trans. Reliability, vol R-31, 1982 Feb, pp 119-120.

[8] H. Kumamoto, H. Otsuka, K. Inoue, "Expected numbers of failures caused by protective systems", IEEE Trans. Reliability, vol R-31, 1982 Jun, pp 219-221.

[9] E.J. Henley, H. Kumamoto, Designing for Reliability and Safety Control, Prentice-Hall, 1985.

[10] T. Kato, T. Ueda, Messages from Airline Captains, Yuhikaku, 1986 (in Japanese).

[11] S. Kumekawa, K. Futsuhara, N. Sugimoto, Introduction to Safety Technology, Chu-Rou-Sai, 1986 (in Japanese).

[12] T. Inagaki, E.J. Henley, "Probabilistic evaluation of prime implicants and top-events for non-coherent systems", IEEE Trans. Reliability, vol R-29, 1980 Dec, pp 361-367.

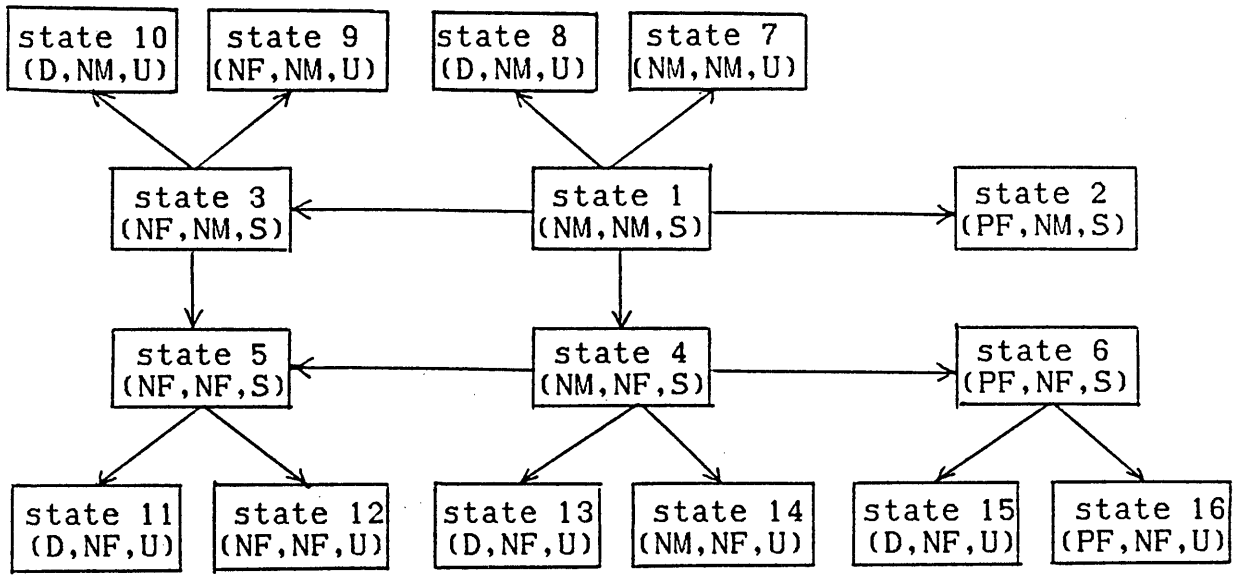

Fig. 1. State Transitions for Fault-Warning Configuration

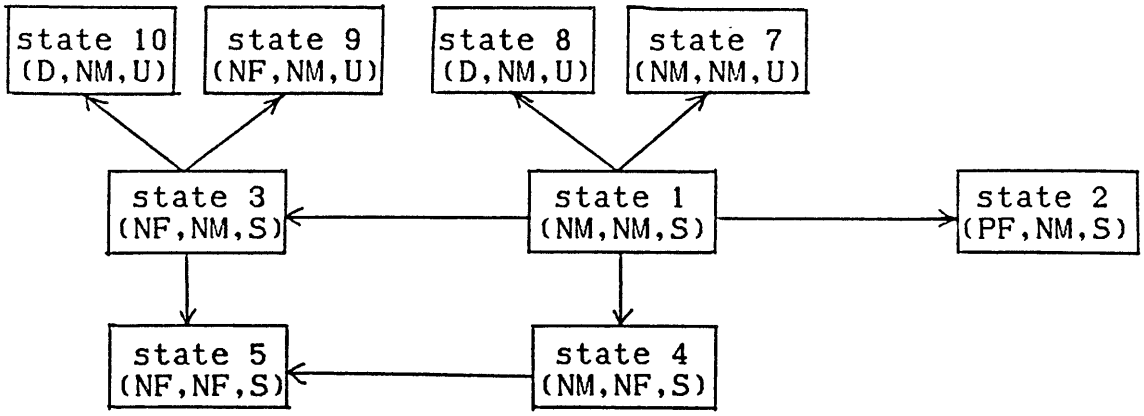

Fig. 2. State Transitions for Safety-Announcing Configuration (the same numbering is applied to states as Fig. 1)

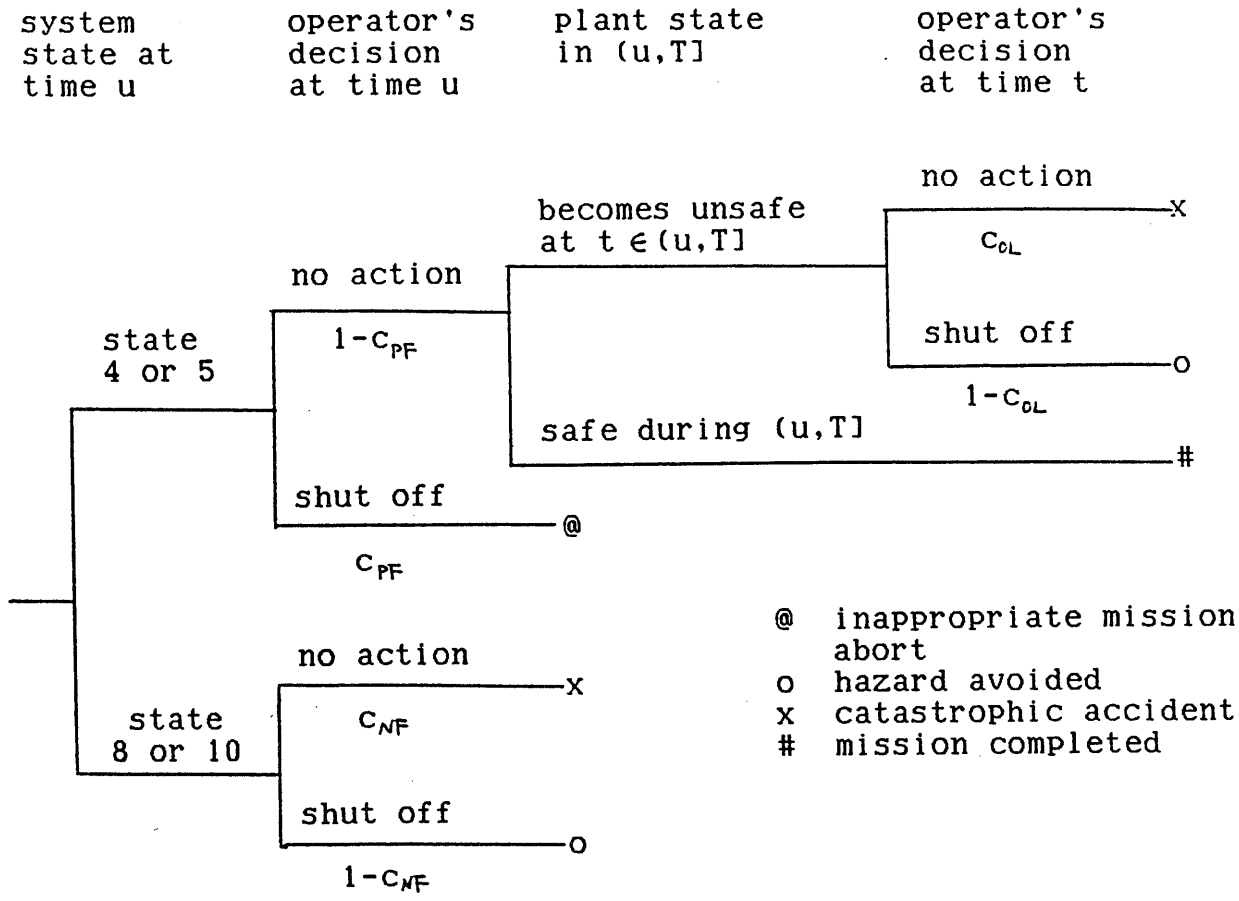

Fig. 3. Possible sequences of events in [u,T] under Policy II which becomes effective upon disappearence of messages at time u

INSTITUTE OF INFORMATION SCIENCES AND ELECTRONICS
UNIVERSITY OF TSUKUBA
SAKURA-MURA, NIIHARI-GUN, IBARAKI 305 JAPAN

REPORT DOCUMENTATION PAGE	REPORT NUMBER ISE-TR-86-62

TITLE

ON HUMAN-MACHINE INTERFACE FOR SYSTEM SAFETY: COMPARISON OF FAULT-WARNING AND SAFETY-ANNOUNCING CONFIGURATIONS

AUTHOR(S)

Toshiyuki Inagaki; Institute of Information Sciences and Electronics; University of Tsukuba; Ibaraki 305 JAPAN.

Yasuhiko Ikebe; Institute of Information Sciences and Electronics; University of Tsukuba; Ibaraki 305 JAPAN.

REPORT DATE	NUMBER OF PAGES
December 26, 1986	20
MAIN CATEGORY	CR CATEGORIES
Reliability theory	

KEY WORDS

Fault detection, Warning system, Human-machine interface

Abstract - This paper discusses two configurations for human-machine interface: (1) conventional "fault-warning configuration" which gives a message of warning upon detecting plant failure and (2) newly introduced "safety-announcing configuration" which can give a message of safety as well as a message of warning. These configurations are examined qualitatively and quantitatively to show that the safety-announcing configuration is more capable of avoiding catastophes than the fault-warning configuration.

SUPPLEMENTARY NOTES