Trans. of the Society of Instrument and Control Engineers
Vol.E-1, No.1, 13/19 (2001)

Optimal Logical Structure of Safety Monitoring Systems with Two Failure Modes[†]

Takehisa KOHDA[*], Koichi INOUE[*],
Hiromitsu KUMAMOTO[**] and Isao TAKAMI[***]

The optimal logical structure is developed for safety monitoring systems, which have two types of contradictory failures; a failed-dangerous failure and a failed-safe failure. The optimal structure that minimizes an expected damage caused by two types of contradictory failures is analytically shown to be $k*$-out-of-n:G system among all coherent structures composed of n identical components. A simple formula to find the optimal $k*$ is obtained. We discuss how the optimal $k*$ varies depending on two failure probabilities of sensor, the plant failure probability, and damages caused by two types of contradictory failures of the safety monitoring system. Illustrative examples are given.

Key Words: failed-dangerous failure, expected damage, k-out-of-n:G system, coherent structure

1. Introduction

The main object of the safety monitoring system such as automatic fire alarm systems is to prevent accidents and disasters by detecting the abnormality as early as possible, issuing an alarm, and then taking appropriate protective actions. The first requirement for the safety monitoring system is to make alarms certainly in case of abnormality.

Next, consider the case where the monitored system is normal. In this case, a false alarm actuates unnecessary protective actions to cause undesired effects such as the plant shut-down or loss of operation. Further, if this kind of situation occurs many times like a story of "wolf and boy" written by Aesop, the trust on alarms will be decreased and the function of safety monitoring systems will be lost. In a modernized high-rise building, about 2000 - 3000 fire sensors are allocated, and too frequent occurrence of false alarms causes a serious problem. The simple idea does not hold that a false alarm does not matter because it is a kind of fail-safe. The second requirement for the safety monitoring system is to issue alarms only in case of the abnormality.

Table 1 Failed-dangerous rate and failed-safe rate

Item	Failed-dangerous rate (faults/year)	Failed-safe rate (spurious-faults/year)
Process connection	0.15	0.21
Diff. pressure transmitter	0.14	0.31
Signal line interface	0.007	0.03
Pressure switch	0.03	0.10
Channel wiring and relay to logic	0.02	0.02
Totals	0.347	0.67

Consider the reliability of a sensor used in safety protective systems for process plants. **Table 1** [1)] shows the failed-dangerous failure rate, failure rate of not issuing an alarm under an abnormal system condition, and the failed-safe rate, failure rate of issuing an alarm under a normal system condition.

It is clearly shown in Table 1 that sensor reliability is far below 0.999, and both failed-dangerous rate and failed-safe rate are higher than expected. In this way, the safety monitoring system composed of a single sensor has the limitation in its reliability. Therefore, more than two sensors must be combined to develop a more reliable safety monitoring system. Further, both failed-safe failure and failed-dangerous failure must be considered.

[†] This paper was presented at the 23-rd Joint Symposium on Automatic Control (1980·11).

[*] Faculty of Engineering, Kyoto University, Yoshida-Honmachi Sakyo-ku, Kyoto; Graduate School of Engineering, Kyoto University, Yoshida-Honmachi Sakyo-ku, Kyoto

[**] Faculty of Engineering, Kyoto University, Yoshida-Honmachi Sakyo-ku, Kyoto (Currently, Graduate School of Information, Kyoto University, Yoshida-Honmachi Sakyo-ku, Kyoto)

[***] Takasago Institute, Mitsubishi Heavy Industry Ltd., 2-1-1 Shinhama Araicho, Takasago (Currently, Nagoya Institute, Mitsubishi Heavy Industry Ltd., 1 Azatakamichi Iwatukacho, Nakamura-ku, Nagoya)

In the design of safety monitoring systems such as automatic fire-alarm systems, the following two types of failure must be considered:

[1] failed-dangerous failure: failure to issue alarms in case of emergency,

[2] failed-safe failure: to issue alarms in case of normality.

Inoue, Kohda, & Kumamoto [2] applied fault-tree analysis to reliability evaluation of safety monitoring systems with two types of failure, and obtained a systematic derivation of fault trees for failed-dangerous and failed-safe failure, and evaluated various types of logical structures based on their qualitative and quantitative analyses.

Relay devices in electric circuits and valves also have two types of contradictory failure shown above, and the optimal redundancy allocation of these devices has been studied. Moore & Shannon [3] studied that of hammock and bridge structures, Barlow, Hunter & Proschan [4] studied that of series-parallel structures, Meisel [5] studied that of k-out-of-n:G systems. Nakagawa & Hattori [6] and Phillips [7] discussed mixed structure of series and parallel redundancy. Kaufmann, Grochiko & Cruon [8] considered that among all coherent systems composed of 3 components. Phillips [9] proved that the optimal structure maximizing its reliability is among k-out-of-n:G systems considering all coherent structures, however he did not obtain the optimal one explicitly.

This paper obtains the logical structure that minimizes the expected loss caused by failed-dangerous and failed-safe failure of a safety monitoring system. It is proved that the optimal structure among all coherent safety monitoring systems composed of n identical sensors is $k*$-out-of-n:G system(1). A simple formula to obtain the optimal $k*$ is also given. Further, it is discussed how the optimal $k*$ changes depending on failed-dangerous or failed-safe failure probability of a sensor, failure probability of the plant to be monitored, and the loss caused by failed-dangerous and failed-safe failure of the safety monitoring system. Finally, both the optimal logical structure that maximizes the normal operational probability of the safety monitoring system and the optimal structure that minimizes the construction cost plus the expected loss of the safety monitoring system are also obtained.

Chapter 2 discusses failed-dangerous and failed-safe failure probabilities of the safety monitoring system, and chapter 3 obtains the optimal logical structure.

2. Failed-Dangerous Failure Probability Q_{1S} & Failed-Safe Failure Probability Q_{2S}

Define 0-1 variable x_i expressing state of i-th sensor of the safety monitoring system as:

$$x_i \equiv \begin{cases} 1, & \text{if } i\text{-th sensor issues an alarm signal} \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

The state of a safety monitoring system composed of n sensors is determined completely by the state of the sensors. Thus, the state of the safety monitoring system is represented as follows in terms of function $\phi(\underline{x})$ of state vector $\underline{x} \equiv (x_1, x_2, \cdots, x_n)$:

$$\phi(\underline{x}) \equiv \begin{cases} 1, & \text{if the safety monitoring system} \\ & \text{issues an alarm} \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

where function $\phi(\underline{x})$ is called a structure function of the safety monitoring system.

Let P_i denote a minimal path set(2) of structure function $\phi(\underline{x})$, and let K_j denote a minimal cut set(3). Using minimal path sets and minimal cut sets, structure function $\phi(\underline{x})$ is represented as follows:

$$\phi(\underline{x}) = \coprod_{i=1}^{p} \prod_{j \in P_i} x_j = \prod_{j=1}^{k} \coprod_{i \in K_j} x_i \tag{3}$$

where p and k denote number of minimal path sets and minimal cut sets, respectively, and $\coprod_i x_i \equiv 1 - \prod_i (1 - x_i)$.

The plant state monitored by the safety monitoring system is either abnormal or normal. Let A denote an event that the plant state is abnormal, and then $\overline{A}$ denotes the opposite event that the plant state is normal. The overall states composed of the plant state and the safety monitoring system are represented as:

1) $\phi(\underline{x}) = 1$ and A
2) $\phi(\underline{x}) = 1$ and $\overline{A}$
3) $\phi(\underline{x}) = 0$ and A
4) $\phi(\underline{x}) = 0$ and $\overline{A}$

States 1) and 4) shows normal operations of the safety monitoring system. These states mean that the safety monitoring system issues an alarm in case of the plant abnormality and does not in case of the plant normality. State 2) indicates that the safety monitoring system issues an alarm when the plant is normal, and is called failed-safe state of the safety monitoring system. State 3) shows that the safety monitoring system fails to issue an alarm when the plant is abnormal, and corresponds

[1] safety monitoring system which issues a system alarm if more than $k*$ of n sensors issue alarm signals

[2] See Appendix A.

[3] See Appendix A.

to the failed-dangerous state of the safety monitoring system. Failure of the safety monitoring system at states 2) and 3) are failed-safe failure and failed-dangerous failure, respectively. The loss is caused in the overall system at states 2) and 3).

Similarly to the case of the safety monitoring system, the overall states composed of i-th sensor state and the plant state are represented as:
1') $x_i = 1$ and A
2') $x_i = 1$ and $\overline{A}$
3') $x_i = 0$ and A
4') $x_i = 0$ and $\overline{A}$
States 1') and 4') indicate the normal operation of i-th sensor, state 2') indicates its failed-safe state and state 3') indicates its failed-dangerous state. Failures of i-th sensor at states 2') and 3') are called its failed-dangerous and failed-safe failure, respectively.

Let binary variable y_i denote the state of i-th sensor under the abnormal condition of the plant as follows:

$$y_i \equiv \begin{cases} 1, & \text{if } x_i = 0 \mid A \\ 0, & \text{if } x_i = 1 \mid A \end{cases} \qquad (4)$$

where $B \mid A$ denotes the occurrence of event B under the occurrence of event A.

Let binary function $\phi'(\underline{y})$ of sensor state vector $\underline{y} \equiv (y_1, y_2, \cdots, y_n)$ denote the state of the safety monitoring system under the abnormal condition of the plant as follows:

$$\phi'(\underline{y}) \equiv \begin{cases} 1, & \text{if } \phi(\underline{x}) = 0 \mid A \\ 0, & \text{if } \phi(\underline{x}) = 1 \mid A \end{cases} \qquad (5)$$

The safety monitoring system gets failed-dangerous if all the sensors get failed-dangerous at least for one minimal cut set of structure function $\phi(\underline{x})$. Thus, binary function $\phi'(\underline{y})$ can be represented as:

$$\phi'(\underline{y}) = \coprod_{j=1}^{k} \prod_{i \in K_j} y_i = 1 - \prod_{j=1}^{k} \coprod_{i \in K_j} (1 - y_i) \qquad (6)$$

Binary function $\phi'(\underline{y})$ is equal to the dual structure function[10)] of $\phi(\underline{y})$, $\phi^D(\underline{y}) \equiv 1 - \phi(\underline{1-y})$. Here, subscript D means "dual", and $\underline{1-y} \equiv (1 - y_1, 1 - y_2, \cdots, 1 - y_n)$.

Next, let binary variable z_i denote the state of i-th sensor under the normal condition of the plant as follows:

$$z_i \equiv \begin{cases} 1, & \text{if } x_i = 1 \mid \overline{A} \\ 0, & \text{if } x_i = 0 \mid \overline{A} \end{cases} \qquad (7)$$

Let binary function $\phi''(\underline{z})$ of sensor state vector $\underline{z} \equiv (z_1, z_2, \cdots, z_n)$ denote the state of the safety monitoring system under the normal condition of the plant as follows:

$$\phi''(\underline{y}) \equiv \begin{cases} 1, & \text{if } \phi(\underline{x}) = 1 \mid \overline{A} \\ 0, & \text{if } \phi(\underline{x}) = 0 \mid \overline{A} \end{cases} \qquad (8)$$

The safety monitoring system gets failed-safe if all the sensors get failed-safe at least for one minimal path set of structure function $\phi(\underline{x})$. Thus, binary function $\phi''(\underline{z})$ can be represented as:

$$\phi''(\underline{z}) = \coprod_{i=1}^{p} \prod_{j \in P_i} z_j \qquad (9)$$

Binary function $\phi''(\underline{y})$ is equal to the structure function $\phi(\underline{z})$.

Reliability function $h(\underline{p})$ of the safety monitoring system, failed-dangerous failure probability q_{1i} and failed-safe failure probability q_{2i} of i-th sensor are defined as follows:

$$h(\underline{p}) \equiv \Pr\{\phi(\underline{x}) = 1\} \qquad (10)$$

$$q_{1i} \equiv \Pr\{y_i = 1\} = \Pr\{x_i = 0 \mid A\} \qquad (11)$$

$$q_{2i} \equiv \Pr\{z_i = 1\} = \Pr\{x_i = 1 \mid \overline{A}\} \qquad (12)$$

where $\underline{p} \equiv (p_1, p_2, \cdots, p_n)$, $p_i \equiv \Pr\{x_i = 1\}$, $\Pr\{A\}$ denotes the occurrence probability of event A and Pr $\{B \mid A\}$ denotes the conditional probability of the occurrence of event B under the occurrence of event A.

Similarly, failed-dangerous failure probability Q_{1S} and failed-safe failure probability Q_{2S} of of the safety monitoring system are defined as follows:

$$Q_{1S} \equiv \Pr\{\phi'(\underline{y}) = 1\} = \Pr\{\phi(\underline{x}) = 0 \mid A\} \qquad (13)$$

$$Q_{2S} \equiv \Pr\{\phi''(\underline{z}) = 1\} = \Pr\{\phi(\underline{x}) = 1 \mid \overline{A}\} \qquad (14)$$

Substituting eq. (6) into eq. (13) and eq. (9) into eq. (14), and using q_{1i} and q_{2i} defined as eqs. (11) & (12), Q_{1S} and Q_{2S} can be represented as follows:

$$Q_{1S} = 1 - h(\underline{1 - q_1}) \qquad (15)$$

$$Q_{2S} = h(\underline{q2}) \qquad (16)$$

where $\underline{1 - q_1} \equiv (1 - q_{11}, 1 - q_{12}, \cdots, 1 - q_{1n})$ and $\underline{q_2} \equiv (q_{21}, q_{22}, \cdots, q_{2n})$.

For the following discussion, these assumptions are made:

Assumption 1. Failure of each sensor occurs statistically independently.

Assumption 2. The sum of failed-dangerous failure probability and failed-safe failure probability of each sensor is less than 1. That is, $q_{1i} + q_{2i} < 1$ for any i.

Assumption 3. The safety monitoring system is coherent[(4)].

[(4)] See Appendix A.

Assumption 4. Logic circuits combining sensor inputs to make an alarm are perfect. In other words, logic circuits do not fail during the mission.

3. Optimal System

Consider the optimal logical structure of the safety monitoring system composed of n identical sensors.

The failed-dangerous failure of the safety monitoring system causes loss to the plant under its abnormal condition, while the failed-safe failure causes loss to the plant under its normal condition. Let P denote the occurrence probability of an abnormality at the plant monitored by the safety monitoring system, let C_{1S} denote loss caused by the failed-dangerous failure of the safety monitoring system, and let C_{2S} denote loss caused by the failed-safe failure. The expected loss, I_S, caused by two types of contradictory failure of the safety monitoring system can be represented as:

$$I_S = C_{1S} P Q_{1S} + C_{2S}(1-P) Q_{2S} \tag{17}$$

The following theorem holds for the safety monitoring system composed of n identical sensors that minimizes the expected loss caused by two types of failure.

Theorem 1. Let q_1 and q_2 denote failed-dangerous failure probability and failed-safe failure probability of a sensor. Among all the safety monitoring systems with coherent structure composed of n identical sensors, the optima system that minimizes the expected loss, I_S represented as eq. (17), caused by two types of failure is $k*$-out-of-n:G system. The optimal $k*$ can be determined as:

1) $k* = n$, if $C_{1S}P(1-q_1)^n \le C_{2S}(1-P){q_2}^n$

2) $k* = 1$, if $C_{1S}P(1-q_1){q_1}^{n-1} \ge C_{2S}(1-P)q_2(1-q_2)^{n-1}$

3) $k* = \left[\dfrac{\ln\frac{C_{2S}(1-P)}{C_{1S}P} + n\ln\frac{1-q_2}{q_1}}{\ln\frac{1-q_1}{q_1}\frac{1-q_2}{q_2}}\right]$, otherwise

Here, $[x]$ denotes a minimal integer greater than x. If x is an integer, $[x]$ is equal to either x or $x+1$. That is, $(x+1)$-out-of-n:G system and x-out-of-n:G system has the same minimal value I_S. $\ln a$ denotes a natural logarithm of a.

Proof. For a coherent safety monitoring system composed of n identical sensors, its reliability function h can be expressed as:[10)]

$$h = \sum_{i=0}^{n} A_i p^i (1-p)^{n-i} \tag{18}$$

where $p \equiv \Pr\{x_i = 1\}$ and A_i denotes the number of cases such that the system issues an alarm with i sensor alarms. Since the number of ways in selecting i items from n items is $\binom{n}{i}$, $0 \le A_i \le \binom{n}{i}$. From Assumption 3, $A_n = 1$ and $A_0 = 0$.

Since Q_{1S} and Q_{2S} are represented in terms of q_1 and q_2 as eqs. (15) & (16), I_S can be represented as follows using eq. (18):

$$I_S = C_{1S}P - \sum_{i=0}^{n} A_i\{C_{1S}P(1-q_1)^i {q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i}\} \tag{19}$$

Examining whether $C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i} > 0$, the following properties hold from Assumption 2: $q_1 + q_2 < 1$.

1) If $C_{1S}P(1-q_1)^n \le C_{2S}(1-P){q_2}^n$, $C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i} < 0$ for $i < n$.

2) If $C_{1S}P(1-q_1){q_1}^{n-1} \ge C_{2S}(1-P)q_2(1-q_2)^{n-1}$, $C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i} \ge 0$ for $i \ge 1$.

3) Otherwise, k exists such that $0 < k < n$ & $C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i} = 0$, and for $i \ge k$, $C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i} \ge 0$.

To summarize the above discussion, the following inequality holds:

$$I_S \ge C_{1S}P - \sum_{i=k^*}^{n} A_i\{C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i}\} \tag{20}$$

In eq. (20), the equality holds if $A_i = 0$ for $i < k^*$.

Since $0 \le A_i \le \binom{n}{i}$, the following inequality holds.

$$\begin{aligned} C_{1S}P - \sum_{i=k^*}^{n} & A_i\{C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i}\} \\ \ge C_{1S}P - \sum_{i=k^*}^{n} & \binom{n}{i}\{C_{1S}P(1-q_1)^i{q_1}^{n-i} - C_{2S}(1-P){q_2}^i(1-q_2)^{n-i}\} \end{aligned} \tag{21}$$

The equality in eq. (21) holds if $A_i = \binom{n}{i}$ for $i \ge k^*$.

Thus, if $A_i = \binom{n}{i}$ for $i \ge k^*$ and $A_i = 0$ for $i < k^*$, the safety monitoring system takes the minimal of I_S, and has the following reliability function:

$$h = \sum_{i=k^*}^{n} \binom{n}{i} p^i (1-p)^{n-i} \tag{22}$$

That is, the optimal reliability function reduces to be that of k^*-out-of-n:G system.

Table 2 Optimal structures of example 1

n	Optimal structure	I_S
2	1-out-of-2:G	19.600
3	2-out-of-3:G	9.770
4	3-out-of-4:G	5.188
5	3-out-of-5:G	1.926

Example 1. Assume that C_{1S}, C_{2S}, P, q_1, and q_2 take the following values:

$$C_{1S} = 1 \times 10^4,\ C_{2S} = 1 \times 10^2,\ P = 0.1$$

$$q_1 = 0.05,\ q_2 = 0.10$$

In this case, the optimal system can be obtained as shown in **Table 2** according to `Theorem 1`. As n increases, the expected loss I_S decreases.

Consider how the optimal k^* varies depending on the value of q_1, q_2, P, or C_{1S}/C_{2S}. Define k as:

$$k* \equiv \left[\frac{\ln \frac{C_{2S}(1-P)}{C_{1S}P} + n \ln \frac{1-q_2}{q_1}}{\ln \frac{1-q_1}{q_1} \frac{1-q_2}{q_2}} \right] \tag{23}$$

Understanding how k changes depending on each parameter, the change of the optimal value k^* can be also understood. Partial derivatives of k with respect to each parameter; q_1, q_2, P, or $\frac{C_{1S}}{C_{2S}}$ gives:

$$\frac{\partial k}{\partial q_1} \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2} = \frac{k}{1-q_1} - \frac{n-k}{q_1} \tag{24}$$

$$\frac{\partial k}{\partial q_2} \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2} = \frac{k}{q_2} - \frac{n-k}{1-q_2} \tag{25}$$

$$\frac{\partial k}{\partial P} = -\frac{1}{P(1-P) \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2}} \tag{26}$$

$$\frac{\partial k}{\partial \left(\frac{C_{1S}}{C_{2S}}\right)} = -\frac{1}{\left(\frac{C_{1S}}{C_{2S}}\right) \ln \frac{(1-q_1)(1-q_2)}{q_1 q_2}} \tag{27}$$

Eqs. (24) & (25) show that k does not increase monotonically as q_1 or q_2 increases. That is, The variation of k with respect to q_1 or q_2 depends on the other parameters. However, if q_1 or q_2 is sufficiently smaller than 1, $\partial k/\partial q_1 < 0$ or $\partial k/\partial q_2 > 0$. Thus, since failed-dangerous failure and failed-safe failure probabilities of sensors used in practical situations are sufficiently smaller than 1, the optimal k^* approaches to 1 as the failed-dangerous failure increases, and the optimal k^* approaches n as the failed-safe failure probability increases.

In eq. (26), since $0 < P < 1$ and $q_1+q_2 < 1$, $\partial k/\partial P < 0$. That is, k decreases as P increases. Thus, the optimal k^* approaches 1 as the abnormality occurrence probability gets larger, which means that the system become more resistive to the failed-dangerous failure.

In eq. (27), since $C_{1S} > 0$, $C_{2S} > 0$ and $q_1 + q_2 < 1$, $\partial k/\partial(C_{1S}/C_{2S}) < 0$. That is, k decreases as C_{1S}/C_{2S} increases. Thus, the optimal k^* approaches 1 making the safety monitoring system more resistive to the failed-dangerous failure as the loss caused by the failed-dangerous failure gets larger. On the contrary, as the loss caused by the failed-safe failure gets larger, the optimal k^* approaches n making the safety monitoring system more resistive to the failed-safe failure.

These results show that the property of the optimal k^* is consistent with the property of k-out-of-n:G system that as k approaches n, the failed-dangerous failure probability gets larger while the failed-safe failure probability gets smaller.

`Theorem 1` shows that whatever value parameters C_{1S}, C_{2S}, and P of the expected loss may take, that is, whatever the ratio of Q_1S to Q_2S may be, the optimal system is k^*-out-of-n:G system. This is the more explicit expression of Phillips's result[9].

Reliability of the safety monitoring system can be defined as:

$$R \equiv 1 - PQ_{1S} - (1-P)Q_{2S} \tag{28}$$

This represents the probability of normal operation of the safety monitoring system without failed-dangerous and failed-safe failure. The optimal system that maximizes the reliability among all the coherent safety monitoring systems can be obtained from `Theorem 1` by setting $C_{1S} = C_{2S} = 1$.

It is clear from `Theorem 1` that the expected loss caused by two types of failure decreases monotonically as the number of sensors increases. On the other hand, the construction cost of a safety monitoring system gets higher as the number of sensors increases. Therefore, the expected loss I_S must be balanced with the system construction cost. Now, consider the objective function $I_S{}'$ which sums the expected loss I_S and the construction cost of the safety monitoring system.

$$I_S{}' = C_{1S}PQ_{1S} + C_{2S}(1-P)Q_{2S} + c_s n \tag{29}$$

where c_s denotes the cost of a sensor. The optimal system that minimizes objective function $I_S{}'$ can be obtained by determining only the number of sensors, n, using the result of `Theorem 1`.

Example 2. Assume that C_{1S}, C_{2S}, P, q_1, q_2, and c_s take the following values:

$$C_{1S} = 1 \times 10^4,\ C_{2S} = 1 \times 10^2,\ P = 0.1$$

$$q_1 = 0.05,\ q_2 = 0.15,\ c_s = 10$$

Under this condition, **Table 3** shows the searching process of the optimal system that minimizes $I_S{}'$. The optimal system is 2-out-of-3:G system with $I_S{}' = 42.717$

Table 3 Searching process of example 2

n	Optimal structure	I_S	$I_S{}'$
1	1-out-of-1:G	63.500	73.500
2	1-out-of-2:G	27.475	47.475
3	2-out-of-3:G	12.717	42.717*
4	2-out-of-4:G	10.388	50.388
5	3-out-of-5:G	3.553	53.553

* Optimal solution of example 2

4. Conclusions

This paper proves analytically that the optimal logical structure that minimizes the expected loss caused by failed-dangerous and failed-safe failure is k^*-out-of-n:G system among all coherent safety monitoring systems composed of n identical sensors. Further, a simple formula that determines the optimal k^* is given, and how the optimal k^* changes depending on parameters is investigated.

Though this paper discussed on the safety monitoring system composed of identical sensors with the same type, various types of sensors are used in practical situations. Thus, the problem to determine the optimal logical structure for the safety monitoring system composed of various types of sensors will be our future problem.

Lastly, we would deeply appreciate Dr. Yoichi Ogawara and Mr. Etsushi Sakino, Takasago Laboratory, Mitsubishi Heavy Industry, Ltd., for their helpful discussion and suggestions.

References

1) B. Sayers: Safety and Risk in a Chemical Plant (A Case Study), 1979 Proceedings Annual Reliability and Maintainability,
Washington DC, 174/180 (1979)
2) K. Inoue, T. Kohda, and H.Kumamoto: Analysis of Failed-dangerous and Failed-safe Failure of Sensor Systems Using FTA, Journal of Safety Engineers, 19-5, 272/278 (1980) (in Japanese)
3) E.F. Moore and C.E. Shannon: Reliable Circuits Using Less Reliable Relays, J. Franklin Institute, 262, 191/208 (Sept. Oct. 1956)
4) R.E. Barlow, L.C. Hunter and F. Proschan: Optimum Redundancy When Components Are Subject to Two Kinds of Failure, SIAM, 11-1, 64/73 (1963)
5) W.S. Meisel: Reliability in Digital Systems with Asymmetric Failure Modes, IEEE Trans. on Reliability, R-18-2, 74/75 (1969)
6) Y. Nakagawa and Y. Hattori: Reliability of All Possible Series-Parallel Redundant Strutures of M i.i.d. Units with Two Failure Modes, IEEE Trans. on Reliability, R-29-4, 320/323 (1980)
7) M.J. Phillips: The Reliability of Two Terminal Parallel-Series Networks Subject to Two Kinds of Failure, Microelectronics and Reliab., 15, 535/549 (1976)
8) A. Kaufmann, D. Grouchko and R. Cruon: Mathematical Models for the Study of the Reliability of Systems, Academic Press, New York (1977)
9) M.J.Phillips: k-out-of-n:G Systems Are Preferable, IEEE Trans. on Reliability, R-29-2, 166/169 (1980)
10) R.E. Barlow and F. Proschan: Statistical Theory of Reliability and Life Testing, Holt, Rinehart and Winston, New York (1975)

Appendix A.

1. The safety monitoring system is coherent if its structure function $\phi(\underline{x})$ satisfies the following conditions:
(1) Each sensor is relevant to $\phi(\underline{x})$.
(2) Function $\phi(\underline{x})$ is non-decreasing with respect to each variable x_i.
Condition (1) means that the system has no sensors irrelevant to issuing alarms, in other words, unnecessary and meaningless sensors, and is self-evident. Condition (2) represents a natural requirement that the issue of an alarm signal in some sensor (represented as x_i changing from 0 to 1 for some i) cannot prevent the safety monitoring from issuing an alarm (represented as $\phi(\underline{x})$ changing from 1 to 0). Any ordinary logical structure composed of only AND and OR logical gates is a coherent structure.
2. For a vector x such that $\phi(\underline{x}) = 1$, a path set is defined as $C_1(\underline{x}) \equiv \{i \mid x_i = 1\}$ and vector $\underline{x}$ is called a path vector. If $\underline{x}_p$ is a path vector and $\phi(\underline{y}) = 0$ for any $\underline{y}$ such that $\underline{y} < \underline{x}_p$, $\underline{x}_p$ is a minimal path vector. In this case, the corresponding path set $C_1(\underline{x}_p)$ is called a minimal path set. On the contrary, for a vector x such that $\phi(\underline{x}) = 0$, a cut set is defined as $C_0(\underline{x}) \equiv \{i \mid x_i = 0\}$ and vector $\underline{x}$ is called a cut vector. If $\underline{x}_c$ is a cut vector and $\phi(\underline{z}) = 1$ for any $\underline{z}$ such that $\underline{z} > \underline{x}_c$, $\underline{x}_c$ is a minimal cut vector. In this case, the corresponding cut set $C_0(\underline{x}_c)$ is called a minimal cut set. To summarize the above discussion simply, a minimal path set is a minimal combination of sensors whose alarm signals can make the safety monitoring system issue an alarm, a minimal cut set is a minimal combination of sensors whose failure to issue alarm signals can prevent the safety monitoring system from issuing an alarm.

Takehisa Kohda (Member)

He received his B.Eng, M.Eng. Dr.Eng. degrees all in Precision Mechanics from Kyoto University in 1978, 1980, and 1983, respectively. Prior to joining Kyoto University in 1988, he worked with National Mechanical Engineering Laboratory, Japan, from 1983 to 1988. He is now an Associate Professor in the Department of Aeronautics and Astronautics, Kyoto University. Since 1999, he has been an Associate Editor of IEEE Transactions on Reliability. His interests lie in the systems safety and reliability, risk analysis, systems analysis, and so on.

Koichi Inoue (Member)

Dr. Inoue received his B.Eng., M.Eng. and Dr.Eng. degrees all in Applied Mathematics and Physics from Kyoto University in 1963, 1965 and 1968, respectively. Dr. Inoue served from 1969 to 1986 as an Associate Professor to the Department of Precision Mechanics, Kyoto University, Kyoto, and since 1986 he has been a Professor with the Department of Aeronautics & Astronautics, Kyoto University, where he has taught, performed and directed research on Control and Systems Engineering as well as Reliability and Safety Engineering. He is presently the Vice-President of Technical Operations, IEEE Reliability Society and the President of Human Interface Society. He received Outstanding Paper Awards five times from the Society of Instrument and Control Engineers (3 times), the Institute of Systems, Control and Information Engineers and Japan Society for Safety Engineering for his contributions in control and systems engineering. He is a recipient of the IEEE Third Millennium Medal. His fields of interest include systems reliability and safety, system optimization, risk analysis, human interface, neural networks, and UAV control.

Hiromitsu Kumamoto (Member)

He received B.S., M.S., and Dr. Eng. Degrees from Kyoto University in 1969, 71, and 76, respectively. He is now a professor of Dept. of Systems Science, Graduate School of Informatics, Kyoto University. He coauthored with Prof. Henley at University of Houston four books: Reliability Engineering and Risk Assessment (Prentice-Hall, 1981), Designing for Reliability and Safety Control (Prentice-Hall, 1986), Probabilistic Risk Assessment (IEEE Press, 1992; reprinted version of the 1981 book), Probabilistic Risk Assessment and Management for Scientists and Engineers (IEEE Press, 1996). His current research fields include human-machine problems in intelligent transport systems. He is a member of IEEE.

Isao Takami (Member)

He received the B.S., M.S., and Dr.Eng. degrees in applied mathematics and physics from Kyoto University in 1972, 1974, and 1986. He has belonged to Mitsubishi Heavy Industries, Ltd. His research interest includes safety and reliability of large scaled plants. He is a member of ISCIE, HIS, and SICE.

Rewrited from T.SICE, Vol.17, No.9, 908/913 (1981)