ヒューマン・インターフェイスと安全制御方策の組合せを 考慮した警報システムの構成と確率的解析*

王 丹**・稲垣敏之***

Probabilistic Analysis of Alarm Subsystems with Different Types of Human Interface and Safety-Control Policies*

Dan WANG** and Toshiyuki INAGAKI***

This paper gives four types of alarm subsystem configurations which include fault-alerting and safety-presentation types, where two kinds of correspondence between sensor states and plant states are distinguished. For each configuration, we give a probabilistic analysis on fail-safe (FS) failures and fail-dangerous (FD) failures. We prove that we can have an optimal alarm subsystem which minimizes FS and FD failures probabilities simultaneously by choosing a human-machine interface configuration and an associated safety-control policy in an appropriate manner.

1. はじめに

原子力発電所や化学プラントに代表される巨大システムは、近年ますます大規模複雑化の様相を呈している。その結果、いったん事故が発生すると、プラント自体の損失だけでなく、周囲の社会環境に大きな被害をもたらす。

警報システムは、プラント異常の発生をオペレータに伝える重要な任務をもつ。しかし、警報システムの故障により、オペレータがプラントの状態を正しく認識できず、結局処置を誤って事故になるケースも少なくない。警報システムの様々な形態の故障可能性を前提としつつプラントの安全性を保つためには、警報システムの情報表示方式を含めたヒューマン・インターフェイスの適切な設計が重要な課題となる。

警報システムの情報表示方式は、「危険表示型」と「安全表示型」の二通りが考えられる^{1),2)}。危険表示型警報システムとは、プラント異常が検出された場合には、ベル等によって警報を出す、プラントが正常である間

は、いかなるメッセージも提示しない形態のものをいう。一方、安全表示型警報システムとは、プラント異常が検知されたときに警報を出すだけでなく、プラントが正常であると判断される間は、そのことを緑ランプ等によって表示する形態のものをいう。

危険表示型警報システムと安全表示型警報システムは動作原理が異なるため、故障モードも異なったものとなる。危険表示型警報システムの故障モードとしては、プラント正常時に警報を出す「誤報モード」と、プラント異常時に警報を出さない「欠報モード」がある。

安全表示型警報システムの故障モードは、やや複雑である。プラント正常時に、安全を示す緑ランプが消えるとともにベルによる警報が出る場合は、明らかに誤報モードである。しかし、緑ランプは消えたもののベルが鳴らない状況も起こりうる。この状況が誤報モードとなるか否かは、プラントに対してオペレータがどのような措置を施すかに依存する。すなわち、このときオペレータがプラントを停止すればプラント誤停止となるが、プラント運転を継続させれば、何ら損失は生じない。

同様のことは、プラント異常発生時についてもいえる。プラント異常発生時に緑ランプが消えず、ベルも鳴らない場合は明白な欠報モードであるが、これ以外にも欠報モードと同一視できる状況が存在する。例えば、緑ランプが消え、ベルが鳴らないときに、オペレータがプラントに対していかなる措置も施さない場合である。

* 原稿受付 1992. 7. 29

** 筑波大学 大学院 工学研究科 Graduate School of University of Tsukuba; Tennodai 1-1-1, Tsukuba-city, Ibaraki 305, JAPAN

*** 筑波大学 電子・情報工学系 Institute of Information Science and Electronics, University of Tsukuba; ditto.

Key Words: system safety, alarm system, human-machine interface, fail-safe failure, fail-dangerous failure.

このように、安全表示型警報システムでは、提示される情報間に不一致あるいは不整合がある場合、それが誤報モード、欠報モードに相当するか否かは、オペレータがプラントに対して何を行うかに依存して決まることになる。

本論文では、まず、センサ、リレー、緑ランプおよびベルを用いて、危険表示型警報システムと安全表示型警報システムが具体的に構成できることを明らかにする。ここで、プラント状態をモニタするセンサとして、動作原理の異なる2種類のセンサを考える。すなわち、プラントが安全状態にあることを、警報システムの低エネルギー状態に対応させるセンサ α と、警報システムの高エネルギー状態に対応させるセンサ β を考える。このとき、危険表示型警報システムと、安全表示型警報システムのいずれに対しても、各々2種類の構成が可能となり、結果的に4種類の警報システムが得られる。これらの4種類の警報システムの欠報モード故障、ならびに誤報モード故障発生確率の特性を評価し、各警報システム間の選好順序関係を明らかにする。さらに、上述の2種類のセンサのいずれを用いる場合でも、安全表示型警報システムは、欠報による事故発生可能性と誤報によるプラント誤停止の可能性を同時に最小にする意味において最適な警報システムとなりうることを証明する。

2. 警報システム

2.1 警報システムの構成

警報システムは一般に、プラントの状態を監視するセンサと、その情報をオペレータに提示するための情報処理・表示部から成る。警報システムとオペレータの間のインターフェイス、すなわちプラント状態の表示方式としては、危険表示型と安全表示型の二通りがある。危険表示型の警報システムでは、プラント異常が検出された場合に限って警報が出され、プラントが正常である間はいかなる情報も表示されない。一方、安全表示型の警報システムは、プラント異常時に警報を出す、プラントが正常であると判断される間も、「プラントは安全な状態にある」ことを、緑のランプ等によって表示する。

上述の二通りのインターフェイスをもつ警報システムは、例えばセンサ、リレー、ベル、緑ランプを用いて構成することができるが、警報システムのエネルギー状態とプラント状態の対応づけには、さらにつぎの二通りの方式が考えられる。

- (1) 警報システムの高エネルギー状態がプラントの危険状態に対応し、低エネルギー状態がプラントの安全状態に対応する。
- (2) 警報システムの高エネルギー状態がプラントの安

全状態に対応し、低エネルギー状態がプラントの危険状態に対応する。

このことから、危険表示型 (fault-alerting type)、安全表示型 (safety-presentation type) の各々に対して、2種類の警報システムを構成することが可能である。こうして得られる4種類の警報システムの構成方法をFig.1に示す。

警報システム1および3では、プラントが安全なときは抵抗が ∞ 、プラント異常発生に伴って抵抗が0に変化するセンサ α を用いている。これにより、プラントが安

(a) Alarm subsystem 1 (Fault-alerting type)

(b) Alarm subsystem 2 (Fault-alerting type)

(c) Alarm subsystem 3 (Safety-presentation type)

(d) Alarm subsystem 4 (Safety-presentation type)

Fig. 1 Alarm subsystems

E_1, E_2 : Electric power units, L : Lamp, B : Bell. The above diagrams show the operation of the plant in its safe state.

全な間は、コイルを通過する電流が0となり、リレーの中接点 r_0 は重力で下に落ちた状態（低エネルギー状態）に保持される。このとき、危険表示型警報システム1では、いかなる情報も表示されないが、安全表示型警報システム3では、リレーの下接点 r_2 を利用して緑ランプを点灯状態に保つことにより、プラント安全を表示する。

一方、プラントが異常になると、コイルに電流が流れ、リレーの中接点 r_0 が上に昇り（高エネルギー状態）、危険表示型警報システム1、安全表示型警報システム3のいずれもベル鳴動により、プラント異常の発生をオペレータに通報する。

警報システム2および4では、プラントが安全なときは抵抗が0、プラント異常発生に伴って抵抗が ∞ に変化するセンサ β を用いることによって、プラントが安全な間は、コイルに電流が流れ、リレーの中接点 r_0 が上に昇った状態（高エネルギー状態）に保持される。このとき危険表示型警報システム2では、オペレータにいかなる情報も表示されないが、安全表示型警報システム4では、リレーの上接点 r_1 を利用して緑ランプを点灯状態に保つことにより、プラント安全を表示する。

プラントが異常になると、コイルを通過する電流が0となり、リレーの中接点 r_0 は重力で下に落ち（低エネルギー状態）、危険表示型警報システム2、安全表示型警報システム4のいずれも、ベルでプラントが危険状態へ移行したことを通報する。

2.2 警報システム状態の分類

プラント、ベル、緑ランプの状態を、各々以下に定める2値状態変数 P, B, L で表現するものとする。

$$P = \begin{cases} 1, & \text{プラントは正常} \\ 0, & \text{プラントは異常} \end{cases}$$

$$B = \begin{cases} 1, & \text{ベルが鳴る} \\ 0, & \text{ベルが鳴らない} \end{cases}$$

$$L = \begin{cases} 1, & \text{緑ランプが点灯} \\ 0, & \text{緑ランプが消灯} \end{cases}$$

また簡単のため、警報システムの構成要素のうち、電源ならびにリレーは故障しないものと仮定する。このとき、危険表示型および安全表示型警報システムの各々がとりうる状態は、Fig.2 に示すように分類される。

故障状態としては、危険表示型警報システムでは、欠報 (FD: Fail-Dangerous failure) と誤報 (FS: Fail-Safe failure) の二通りが存在するのみであるが、安全表示型警報システムの場合は、自明な欠報モード、誤報モードのほかに、Fig.2 (b) において ω_1, ω_2 で示され

P		B		
1	0	0	1	0
NM	FS			
FD	NM			

P		B			L
1	0	0	1	0	0
NM	FS	ω_1			
FD	NM	ω_2			

(a) Fault-alerting type (b) Safety-presentation type

Fig. 2 Classification of states for the alarm subsystem

NM: Normal, FS: Fail-Safe failure,
FD: Fail-Dangerous failure

る故障モードがあることに注意する必要がある。ここに、 ω_1 は、プラントが安全な時、警報ベルは鳴らないが、緑ランプが消える状態であり、 ω_2 は、プラントが異常な時、警報ベルは鳴らないが、緑ランプが消える状態である。これらの状態 ω_1, ω_2 はいずれも、プラントが安全であるか危険であるか、明確に判定できない状況を表わす。

ω_1, ω_2 において何らかの損失が生ずるか否かは、オペレータの安全制御方策、すなわち、プラントに対してどのような措置を施すかに依存する。一般に、安全制御方策は、Fig.3 に示すように、「危険検知に基づく安全制御方策」（以後、FW (Fault-Warning) 型方策とよぶ）と「安全確認に基づく安全制御方策」（以後、SP (Safety-Preservation) 型方策とよぶ）に分類できる³⁾。前者は、プラントが危険であると判断された場合に限り、プラントを停止させる方策であり、後者は、プラントが安全であると判断されない限り、プラントを稼働させない方策である。たとえば、1986年1月のスペースシャトル・チャレンジャーの打ち上げに際しては、「安全が保証できないから、打ち上げを延期すべきだ」という意見 (SP 型方策) と、「危険だという確実な証拠がない限り、打ち上げを行う」との意見 (FW 型方策) との間で対立があったとされている。

状態 ω_1, ω_2 に対して FW 型方策を採用 (プラントを停止させない) のものとしよう。このとき、 ω_1 については損失は生じないが、 ω_2 の場合には、プラント事故を招くことになる。一方、状態 ω_1, ω_2 に対して SP 型方

	Plant state		
	safe	unknown	unsafe
FW policy	operative		stop
SP policy	operative	stop	

Fig. 3 Classification of safety-control policies

FW: Fault-Warning safety-control policy,
SP: Safety-Preservation safety-control policy

策を採用する（プラントを停止させる）と、 ω_1 についてはプラント誤停止を招くが、 ω_2 の場合にはプラント事故を回避することが可能となる。以後、SP 型安全制御方策を採用した安全表示型警報システム i ($i=3, 4$) を「安全表示型 SP 警報システム i 」、FW 型安全制御方策を採用した安全表示型警報システム i を「安全表示型 FW 警報システム i 」とよぶことにする。

3. 警報システムの確率的特性

警報システム構成要素のうち、ベル、ランプについては、正常と故障の2状態があり、センサ α, β は、正常、開モード故障（例えば断線故障）、閉モード故障（例えば短絡故障）の3状態があると仮定する。また、各構成要素の故障は統計的に独立であるとする。

3.1 危険表示型警報システム

危険表示型の警報システム 1（センサ α を使用）、2（センサ β を使用）では、Fig. 2 (a) に表わされるような欠報と誤報の2通りの故障モードが存在する。

時刻 t でプラント異常が発生したとき、危険表示型警報システム 1, 2 が警報を出さない事象を、それぞれ $G_1(t)$, $G_2(t)$ で表わす。事象 $G_1(t)$, $G_2(t)$ が生起するのは、センサがプラント異常を検知できなかった場合、あるいはベルが故障していた場合であることから、 $G_1(t)$, $G_2(t)$ の発生確率はつぎの各式で与えられる。

$$P\{G_1(t)\} = F_b(t) + \bar{F}_b(t) F_a(t) x_a \quad (1)$$

$$P\{G_2(t)\} = F_b(t) + \bar{F}_b(t) F_\beta(t) \bar{x}_\beta \quad (2)$$

ここで、 $F_b(t)$, $F_a(t)$, $F_\beta(t)$ はベル、センサ α , センサ β の寿命の分布関数を表わし、 $\bar{F}(t) \equiv 1 - F(t)$ とする。さらに、 $x \equiv P\{\text{センサが開モード故障} \mid \text{センサが故障}\}$ とする。センサが故障する場合には、その故障が開モード故障、閉モード故障のいずれであるか区別しなければならない。ここで定義した x は、センサが故障（すなわち正常状態から離脱）した場合、その遷移が開モード故障への遷移である条件つき確率である。また、 $\bar{x} \equiv 1 - x$ とすると、 $\bar{x}$ は、センサが故障するとき、それが閉モード故障である条件つき確率を表わす。なお、 x あるいは $\bar{x}$ の添字 α, β は、各々センサ α , センサ β に対応して定義されるものであることを表わす。

時刻 t でプラントが正常であるとき、危険表示型警報システム 1, 2 によって、微小区間 $\varepsilon \equiv (t, t + \Delta t)$ でプラント誤停止が発生する事象を、それぞれ $H_1(\varepsilon)$, $H_2(\varepsilon)$ で表わす。事象 $H_1(\varepsilon)$, $H_2(\varepsilon)$ が生起するのは、ベルが正常であり、かつセンサが微小区間 ε で誤報モード故障に陥るときであることから、 $H_1(\varepsilon)$, $H_2(\varepsilon)$ の発生確率はつぎの各式で与えられる。

$$P\{H_1(\varepsilon)\} = \bar{F}_b(t) \bar{x}_a f_a(t) \Delta t \quad (3)$$

$$P\{H_2(\varepsilon)\} = \bar{F}_b(t) x_\beta f_\beta(t) \Delta t \quad (4)$$

ここで、 $f_a(t)$, $f_\beta(t)$ はセンサ α , センサ β の寿命の密度関数を表わす。

3.2 安全表示型 SP 警報システム

安全表示型の警報システム 3（センサ α を使用）、4（センサ β を使用）において SP 型方策を採用すると、ベルが鳴るか否かに依らず、緑ランプが消えると直ちにプラントは停止される。

時刻 t でプラント異常が発生したとき、安全表示型 SP 警報システム 3, 4 が警報を出さない事象を、それぞれ $G_3(t; \text{SP})$, $G_4(t; \text{SP})$ で表わす。事象 $G_3(t; \text{SP})$, $G_4(t; \text{SP})$ が生起するのは、プラント異常時にセンサがすでに欠報モード故障状態（センサ α では開モード故障状態、センサ β では閉モード故障状態に対応）にあり、ランプが点灯している場合に限られることから、 $G_3(t; \text{SP})$, $G_4(t; \text{SP})$ の発生確率はつぎの各式で与えられる。

$$P\{G_3(t; \text{SP})\} = \bar{F}_L(t) F_a(t) x_a \quad (5)$$

$$P\{G_4(t; \text{SP})\} = \bar{F}_L(t) F_\beta(t) \bar{x}_\beta \quad (6)$$

ここで、 $\bar{F}_L(t)$ は、時刻 t までランプが正常である確率を表わす。

プラント正常時に、安全表示型 SP 警報システム 3, 4 において、微小区間 ε でプラント誤停止が発生する事象を、それぞれ $H_3(\varepsilon; \text{SP})$, $H_4(\varepsilon; \text{SP})$ で表わす。事象 $H_3(\varepsilon; \text{SP})$, $H_4(\varepsilon; \text{SP})$ が生起するのは、プラント正常時に微小区間 ε においてセンサ誤報モード故障（センサ α では閉モード故障状態、センサ β では開モード故障状態に対応）が発生するか、ランプが故障する場合である。よって、 $H_3(\varepsilon; \text{SP})$, $H_4(\varepsilon; \text{SP})$ の発生確率はつぎの各式で与えられる。

$$\begin{aligned} P\{H_3(\varepsilon; \text{SP})\} &= \bar{F}_L(t) \bar{x}_a f_a(t) \Delta t + [1 - F_a(t) \bar{x}_a] f_L(t) \Delta t \\ &\quad (7) \end{aligned}$$

$$\begin{aligned} P\{H_4(\varepsilon; \text{SP})\} &= \bar{F}_L(t) x_\beta f_\beta(t) \Delta t + [1 - F_\beta(t) x_\beta] f_L(t) \Delta t \\ &\quad (8) \end{aligned}$$

ここで、 $f_L(t)$ はランプの寿命の密度関数を表わす。

3.3 安全表示型 FW 警報システム

安全表示型の警報システム 3（センサ α を使用）、4（センサ β を使用）に対して FW 型方策を採用すると、ベルが鳴らない限り、プラントは停止させない。ただし、ランプが消えたが、ベルは鳴らないことも起こりうる。このとき、FW 型方策の意味を拡大解釈すれば、ベル

が鳴らない以上、オペレータは一切の行動を起こさないことになる。しかし、このようにすると、「安全表示型」インターフェイスの意義が失われ、危険表示型インターフェイスへ移行したのと等価となる。安全表示型インターフェイス採用の意義を考えると、ベルが鳴らず、ランプが消えた場合、オペレータは、FW 型方策のもとでプラント停止措置をとらないが、警報システムに不具合がないか点検を行うことができる。そこで、本論文ではこのような状況を考慮する。このとき、警報システム欠報、あるいはプラント誤停止の事象生起は、ランプが点灯している場合に限定して考察することになる。

時刻 t でプラント異常が発生したとき、安全表示型 FW 警報システム 3, 4 が警報を出さない事象を、それぞれ $G_3(t:FW)$, $G_4(t:FW)$ で表わす。事象 $G_3(t:FW)$, $G_4(t:FW)$ が生起するのは、プラント異常が発生したとき、ランプは点灯しているため、あたかもプラントは正常であるとオペレータには思わせるが、実は、センサがすでに欠報モードで故障しているか、ベルが故障している場合であることから、 $G_3(t:FW)$, $G_4(t:FW)$ の発生確率はつぎの各式で与えられる。

$$P\{G_3(t:FW)\} = \bar{F}_L(t)[F_a(t)x_a + \bar{F}_a(t)F_b(t)] \quad (9)$$

$$P\{G_4(t:FW)\} = \bar{F}_L(t)[F_\beta(t)\bar{x}_\beta + \bar{F}_\beta(t)F_b(t)] \quad (10)$$

ところで、(9), (10) 式は (5), (6) 式の結果を用いれば、つぎのように表現できる。

$$P\{G_3(t:FW)\} = P\{G_3(t:SP)\} + F_b(t)\bar{F}_L(t)\bar{F}_a(t) \quad (11)$$

$$P\{G_4(t:FW)\} = P\{G_4(t:SP)\} + F_b(t)\bar{F}_L(t)\bar{F}_\beta(t) \quad (12)$$

すなわち、(11), (12) 式から、センサ α, β のいずれを用いる場合でも、FW 型方策は SP 型方策より、欠報の可能性が増すことがわかる。

時刻 t でプラントが正常であるとき、安全表示型 FW 警報システム 3, 4 において、微小区間 ε でプラント誤停止が発生する事象を、それぞれ $H_3(\varepsilon:FW)$, $H_4(\varepsilon:FW)$ で表わす。事象 $H_3(\varepsilon:FW)$, $H_4(\varepsilon:FW)$ が生起するのは、プラント正常のとき微小区間 ε でベルが鳴る場合であり、安全表示型インターフェイスのもとでは、誤報モードはランプが点灯している場合に限定して考えてもよいことから、 $H_3(\varepsilon:FW)$, $H_4(\varepsilon:FW)$ の発生確率はつぎの各式で与えられる。

$$P\{H_3(\varepsilon:FW)\} = \bar{F}_L(t)\bar{F}_b(t)\bar{x}_a f_a(t) \Delta t \quad (13)$$

$$P\{H_4(\varepsilon:FW)\} = \bar{F}_L(t)\bar{F}_b(t)x_\beta f_\beta(t) \Delta t \quad (14)$$

ところで、(13), (14) 式は (3), (4) 式の結果を用い

ると、

$$P\{H_3(\varepsilon:FW)\} = \bar{F}_L(t)P\{H_1(\varepsilon)\} \leq P\{H_1(\varepsilon)\} \quad (15)$$

$$P\{H_4(\varepsilon:FW)\} = \bar{F}_L(t)P\{H_2(\varepsilon)\} \leq P\{H_2(\varepsilon)\} \quad (16)$$

を得る。このことはセンサ α, β のいずれを用いた場合でも、同種のセンサをもつ危険表示型警報システムと安全表示型警報システム間では、FW 型方策はプラント誤停止をもたらす可能性を増加させないことがわかる。

4. 警報システムの特性評価

4.1 欠報特性の比較

警報システムのインターフェイス方式（危険表示型、安全表示型）と、欠報モード故障発生との関係を調べる。

4.1.1 危険表示型警報システムと安全表示型 SP 警報システム

安全表示型警報システムでは、安全制御方策を区別する必要がある。そこで、まず、危険表示型警報システムと安全表示型 SP 警報システムとの欠報可能性の比較を行うためには、次式を定義する。

$$g_{ij} \equiv P\{G_i(t)\} - P\{G_j(t:SP)\}, \quad (17)$$

$$i \in \{1, 2\}, j \in \{3, 4\}$$

センサ α を用いる危険表示型警報システム 1 と安全表示型 SP 警報システム 3 の欠報モード発生特性については、(1), (5) 式より次式を得る。

$$g_{13} = F_b(t)[1 - F_a(t)x_a] + F_L(t)F_a(t)x_a \geq 0, \quad \forall t \in [0, \infty], \forall x_a \in [0, 1] \quad (18)$$

一方、センサ β を使用する危険表示型警報システム 2 と安全表示型 SP 警報システム 4 については、(2), (6) 式から、次式を得る。

$$g_{24} = F_b(t)[1 - F_\beta(t)\bar{x}_\beta] + F_L(t)F_\beta(t)\bar{x}_\beta \geq 0, \quad \forall t \in [0, \infty], \forall x_\beta \in [0, 1] \quad (19)$$

(18), (19) 式から、センサ α, β のいずれを用いた場合でも、安全表示型 SP 警報システムのほうが、危険表示型警報システムに比べて、任意の時刻 $t > 0$ において欠報モードの可能性が小さいことがわかる。

センサ α とセンサ β の故障発生に関する確率的特性が等しい、すなわち $F_a = F_\beta (= F_s)$, $x_a = x_\beta (= x)$ が仮定できる場合は、さらに詳細な解析が可能である。表記の簡単化のため、 $P\{G_3(t:SP)\}$, $P\{G_4(t:SP)\}$ をそれぞれ $P\{G_3(t)\}$, $P\{G_4(t)\}$ と書き、

$$g_{ij}^* \equiv P\{G_i(t)\} - P\{G_j(t)\}, \quad (20)$$

$$i, j \in \{1, \dots, 4\}$$

と定義すると、 $g_{13}^* = g_{13}$, $g_{24}^* = g_{24}$ が成立し、さらに

(1), (2), (5), (6) 式から, つぎの各式を得る.

$$g_{12}^* = \bar{F}_b(t) F_s(t) (2x-1) \quad (21)$$

$$g_{34}^* = \bar{F}_L(t) F_s(t) (2x-1) \quad (22)$$

$$g_{14}^* = F_s(t) [\bar{F}_L(t) + \bar{F}_b(t)] x + [F_b(t) - \bar{F}_L(t) F_s(t)] \quad (23)$$

$$g_{32}^* = F_s(t) [\bar{F}_L(t) + \bar{F}_b(t)] x - [F_b(t) + \bar{F}_b(t) F_s(t)] \quad (24)$$

ここで, g_{ij}^* を x についての関数 (線形関数) とみなし, g_{ij}^* を $g_{ij}^*(x)$ と書くことにすると, $g_{ij}^*(x) = 0$ を満たす x_{ij} について, 次式が成立する.

$$x_{14} < x_{12} = x_{34} (= 0.5) < x_{32} \quad (25)$$

ここで上式における不等式の部分は次式が成立することによる.

$$x_{32} - 0.5 = 0.5 - x_{14} = \frac{[F_s(t) F_L(t) + F_b(t) + \bar{F}_s(t) F_b(t)]}{2 F_s(t) [\bar{F}_b(t) + \bar{F}_L(t)]} \geq 0 \quad (26)$$

ところで, x は条件つき確率として定義されるものであることから, 区間 $[0, 1]$ が (25) 式に現われる x_{14} , x_{12} , x_{34} , x_{32} によってどのように分割されるかを調べる必要がある. ここで再び (26) 式より, x_{14} および x_{32} は数直線上で 0.5 を中心として対称の位置にあることがわかる. このことは, $x_{14} > 0$ と $x_{32} < 1$ が同値であること, すなわち, (a) $x_{14} > 0$ かつ $x_{32} < 1$ となる場合, (b) $x_{14} \leq 0$ かつ $x_{32} \geq 1$ となる場合の 2 通りがあることがわかる.

まず, $x_{14} > 0$ かつ $x_{32} < 1$ の場合, x_{14} , $x_{12} = x_{34} (= 0.5)$, x_{32} は区間 $[0, 1]$ を四つの区間に分割する. ここで, $g_{ij}^* \geq 0$, すなわち $P\{G_i(t)\} \geq P\{G_j(t)\}$ が成立することを記号的に「 $i > j$ 」で表わすと, $x \in [x_{14}, 0.5]$ については, (18), (19), (21)~(24) 式から各々 $1 > 3$, $2 > 4$, $1 > 4$, $2 > 3$, $2 > 1$, $4 > 3$ が成立し, これらに推移律を用いて次式を得る.

$$2 > 1 > 4 > 3 \quad (27)$$

他の区間 $[0, x_{14}]$, $[0.5, x_{32}]$, および $[x_{32}, 1]$ についても同様な解析が可能である. 結果を Fig. 4 (a) に示す.

また, $x_{14} \leq 0$ かつ $x_{32} \geq 1$ の場合についての同様な解析の結果を Fig. 4 (b) に示す.

Fig. 4 (a), (b) に示された $P\{G_i(t)\}$ ($i = 1, \dots, 4$) の順序関係から, つぎのことがわかる.

- (1) 欠報の可能性が最小のものは, 安全表示型 SP 警報システム (警報システム 3 あるいは 4) である. ただし, 直観的に成立が期待される命題「安全表

Fig. 4 Order relation on $P\{G_i(t)\}$ where $F_\alpha = F_\beta$, $x_\alpha = x_\beta (= x)$

示型 SP 警報システムは, いかなる危険表示型警報システムより欠報の可能性が小さい」は必ずしも真ではない. すなわち, Fig. 4 (a) の区間 (x_{14}, x_{32}) あるいは Fig. 4 (b) の区間 $(0, 1)$ では, 上の命題は成立するが, Fig. 4 (a) の区間 $[0, x_{14}]$ では, $P\{G_4(t)\} > P\{G_1(t)\}$ が成立し, 安全表示型 SP 警報システム 4 より危険表示型警報システム 1 のほうが欠報発生の可能性が小さい. また, Fig. 4 (a) の区間 $(x_{32}, 1]$ でも $P\{G_3(t)\} > P\{G_2(t)\}$ が成立し, 安全表示型 SP 警報システム 3 より危険表示型警報システム 2 のほうが欠報の可能性が小さい.

- (2) 一般には, 警報システムの高エネルギー状態でプラント危険を表わすより, 低エネルギー状態でプラント危険を表わすほうが, 欠報発生の可能性を小さくできると考えられる. しかし, いずれの方式を選択するかは, センサの開モード故障と閉モード故障の発生比率を決める x の値に応じて定めなければならない. たとえば, Fig. 4 (a) の区間 $[0, x_{14}]$ では, 警報システムの高エネルギー状態でプラント危険を表わす方式を採用する警報システム 1, 3 の方が, 低エネルギー状態でプラント危険を表わす方式に基づく警報システム 2, 4 より欠報の可能性が小さく, プラント事故を回避する観点からは優れている. しかし, $x \in (x_{32}, 1]$ のときは, これらの方式の優劣は逆になる.

4.1.2 危険表示型警報システムと安全表示型 FW 警報システム

危険表示型警報システムと, 安全表示型 FW 警報システムとの欠報可能性の比較を行うために, 次式を定義する.

$$e_{ij} \equiv P\{G_i(t)\} - P\{G_j(t; \text{FW})\}, \quad (28)$$

$$i \in \{1, 2\}, j \in \{3, 4\}$$

センサ α を用いる危険表示型警報システム 1 と安全表示型 FW 警報システム 3 の欠報モード発生特性の比較については, (1), (9) 式から, 次式を得る.

$$\begin{aligned}
e_{13} = & F_L(t)[F_a(t)x_a + \bar{F}_a(t)F_b(t)] \\
& + F_b(t)F_a(t)\bar{x}_a \geq 0, \quad (29) \\
& \forall t \in [0, \infty), \forall x_a \in [0, 1]
\end{aligned}$$

安全表示型警報システム3についてFW型方策を採用するとき、欠報の可能性がSP型方策の場合より増えることはすでに(11)式で示した。しかし(29)式から、それでもなお危険表示型警報システム1より欠報の可能性が小さいことがわかる。このことから、SP型方策、FW型方策の選択に依らず、任意の時刻 $t > 0$ において、安全表示型警報システム3は、危険表示型警報システム1より欠報の可能性が小さいことがわかる。

センサ β を使用する危険表示型警報システム2と安全表示型FW警報システム4についても同様のことが示される。すなわち、(2)、(10)式より

$$\begin{aligned}
e_{24} = & F_L(t)[F_\beta(t)\bar{x}_\beta + \bar{F}_\beta(t)F_b(t)] \\
& + F_b(t)F_\beta(t)x_\beta \geq 0, \quad (30) \\
& \forall t \in [0, \infty), \forall x_\beta \in [0, 1]
\end{aligned}$$

が得られ、(12)式の結果を合わせると、SP型方策、FW型方策の選択に依らず、任意の時刻 $t > 0$ において安全表示型警報システム4は、危険表示型警報システム2より欠報の可能性が小さいことがわかる。

4.2 プラント誤停止特性の比較

警報システムのインターフェイス方式(危険表示型、安全表示型)と、プラント誤停止発生との関係を調べる。

4.2.1 危険表示型警報システムと安全表示型SP警報システム

危険表示型警報システムと、安全表示型SP警報システムとのプラント誤停止をもたらす可能性の比較を行うために、次式を定義する。

$$h_{ij} \equiv \frac{P\{H_i(\epsilon)\} - P\{H_j(\epsilon : SP)\}}{\Delta t}, \quad (31)$$

$$i \in \{1, 2\}, j \in \{3, 4\}$$

センサ α を用いる危険表示型警報システム1と安全表示型SP警報システム3のプラント誤停止発生特性については、(3)、(7)式より次式を得る。

$$h_{13} = \{[F_L(t) - F_b(t)]f_a(t) + F_a(t)f_L(t)\}(1 - x_a) - f_L(t) \quad (32)$$

ここで

$$\begin{aligned}
h_{13}(x_a = 1) &= -f_L(t) < 0 \quad (33) \\
h_{13}(x_a = 0) &= [F_L(t) - F_b(t)]f_a(t) - \bar{F}_a(t)f_L(t) \quad (34)
\end{aligned}$$

に注意すると、 $h_{13}(x_a = 0) < 0$ のとき、任意の $x_a \in [0, 1]$ に対して、安全表示型SP警報システム3によるプラント誤停止が起こる可能性は危険表示型警報システ

ム1の場合より大きいことがわかる。

一方、 $h_{13}(x_a = 0) > 0$ のときは、 $h_{13}(x_a) = 0$ を満たす $x_{a0} \in (0, 1)$ が存在し、次式が成立する。

$$h_{13}(x_a) \begin{cases} > 0, \forall x_a \in [0, x_{a0}) \\ \leq 0, \forall x_a \in [x_{a0}, 1] \end{cases} \quad (35)$$

ここで注目すべきことは、 $h_{13}(x_a) > 0$ となりうる点である。すなわち、「安全表示型SP警報システムは、危険表示型警報システムより、プラント誤停止をもたらす可能性は大きい」という、直観から導かれる命題は必ずしも真でなく、 $x_a \in [0, x_{a0})$ については、安全表示型インターフェイスのほうが、危険表示型インターフェイスよりプラント誤停止の可能性が小さくなることがわかる。

同様に、センサ β を使用する危険表示型警報システム2と安全表示型SP警報システム4についても、(4)、(8)式より

$$h_{24}(x_\beta) = \{[F_L(t) - F_b(t)]f_\beta(t) + F_\beta(t)f_L(t)\}x_\beta - f_L(t) \quad (36)$$

が得られ、

$$\begin{aligned}
h_{24}(x_\beta = 0) &= -f_L(t) < 0 \quad (37) \\
h_{24}(x_\beta = 1) &= [F_L(t) - F_b(t)]f_\beta(t) - \bar{F}_\beta f_L(t) \quad (38)
\end{aligned}$$

に注意すれば、 $h_{24}(x_\beta = 1) < 0$ のとき、任意の $x_\beta \in [0, 1]$ に対して安全表示型SP警報システム4がプラント誤停止をもたらす可能性は、危険表示型警報システム2より大きいことがわかる。しかし、 $h_{24}(x_\beta = 1) > 0$ ならば、 $h_{24}(x_\beta) = 0$ を満たす x_β を $x_{\beta 0}$ と表わすとき、 $x_\beta \in (x_{\beta 0}, 1]$ について、安全表示型警報システム4は危険表示型警報システム2よりプラント誤停止をもたらす可能性が小さいことが示される。

4.2.2 危険表示型警報システムと安全表示型FW警報システム

センサ α, β のいずれを用いた場合でも同種のセンサを用いる限り、安全表示型FW警報システムは危険表示型警報システムより、プラント誤停止をもたらす可能性が小さいことはすでに(15)、(16)式で示した。

4.3 安全制御方策の選択

安全表示型警報システムにおける安全制御方策の選択が、プラント事故発生ならびにプラント誤停止の確率的特性へどのような影響を与えるかを調べる。記号 g_i, h_i ($i \in \{3, 4\}$)をつぎのように定める。

$$g_i \equiv P\{G_i(t : FW)\} - P\{G_i(t : SP)\} \quad (39)$$

$$h_i \equiv \frac{P\{H_i(\epsilon : FW)\} - P\{H_i(\epsilon : SP)\}}{\Delta t} \quad (40)$$

4.3.1 プラント事故発生

(11), (12) 式より任意の $x_a, x_\beta \in [0, 1], t > 0$ について, $g_3 > 0, g_4 > 0$ が成立し, 安全表示型警報システムのもとでは, SP 型方策は, FW 型方策に比べ, プラント事故を回避できる可能性が高いことがわかる。

4.3.2 プラント誤停止

(7), (8), (13), (14) 式より

$$\begin{aligned} h_3 &= -\bar{F}_L(t) F_b(t) \bar{x}_a f_a(t) \\ &\quad - [1 - F_a(t) \bar{x}_a] f_L(t) \leq 0, \end{aligned} \quad (41)$$

$$\forall t \in [0, \infty), \forall x_a \in [0, 1]$$

$$\begin{aligned} h_4 &= -\bar{F}_L(t) F_b(t) x_\beta f_\beta(t) \\ &\quad - [1 - F_\beta(t) x_\beta] f_L(t) \leq 0 \end{aligned} \quad (42)$$

$$\forall t \in [0, \infty), \forall x_\beta \in [0, 1]$$

を得ることから, 安全表示型警報システムに対しては, SP 型方策は, FW 方策に比べプラント誤停止をもたらす可能性が高いことがわかる。

5. 最適な警報システム

警報システムの欠報モード故障, 誤報モード故障によってもたらされる損失期待値を最小にする意味で最適な警報システムが存在することは, すでに知られている⁴⁻⁶⁾。これに対して本論文では, 単一の評価基準(すなわち, 損失期待値)のもとで警報システム最適性を議論するのではなく, 2 個の評価基準, すなわち欠報モードの可能性 $P\{G_i(t)\}$ とプラント誤停止の可能性 $P\{H_i(\varepsilon)\}$ をとりあげ, これらを同時に最小にする警報システムを, 最適警報システムとよぶことにする。

センサ α , センサ β のいずれを用いた場合でも, 同種類のセンサを使用する限り, 最適警報システムとなりうるものは安全表示型インターフェイスをもつものであることを以下で明らかにする。

5.1 危険表示型警報システムと安全表示型 SP 警報システム

安全制御方策を SP 型に固定して議論する。

センサ α を使用する場合, (18) 式から安全表示型 SP 警報システム 3 は危険表示型警報システム 1 より, 常に欠報の可能性が小さいことがわかる。また, (34), (35) 式は

$$[F_L(t) - F_b(t)] f_a(t) > \bar{F}_a(t) f_L(t) \quad (43)$$

が成立するとき, $x_a \in [0, x_{a0})$ を満たす x_a について安全表示型 SP 警報システム 3 は, 危険表示型警報システム 1 より, プラント誤停止の可能性が小さいことを示す。したがって, (43) 式は $x_a \in [0, x_{a0})$ を満たすセンサ α を用いた安全表示型 SP 警報システム 3 が最適な警

報システムとなるための必要十分条件であることがわかる。

センサ β を使用する場合も同様である。(19) 式から, 安全表示型 SP 警報システム 4 は危険表示型警報システム 2 より, 常に欠報の可能性が小さい。よって, (38) 式において,

$$[F_L(t) - F_b(t)] f_\beta(t) > \bar{F}_\beta f_L(t) \quad (44)$$

が成立するとき, $x_\beta \in (x_{\beta 0}, 1]$ を満たすセンサ β を用いた安全表示型 SP 警報システム 4 は, 最適な警報システムとなる。

5.2 危険表示型警報システムと安全表示型 FW 警報システム

安全制御方策を FW 型に固定して考えてみよう。

センサ α を使用する場合, (29) 式から, 安全表示型 FW 警報システム 3 は危険表示型警報システム 1 より常に欠報の可能性が小さい。しかるに, (15) 式より安全表示型 FW 警報システム 3 は危険表示型警報システム 1 より, 常にプラント誤停止の可能性が小さい。したがって, 任意の $x_a \in [0, 1], t > 0$ について, 安全表示型 FW 警報システム 3 は最適な警報システムとなる。

センサ β を使用する場合, (30) 式から, 安全表示型 FW 警報システム 4 は危険表示型警報システム 2 より常に欠報の可能性が小さく, (16) 式より, 安全表示型 FW 警報システム 4 は危険表示型警報システム 2 より, 常にプラント誤停止の可能性が小さいことが示される。したがって, 任意の $x_\beta \in [0, 1], t > 0$ に対して, 安全表示型 FW 警報システム 4 は最適な警報システムとなる。

6. むすび

本論文では, 危険表示型ならびに安全表示型の警報システムの構成例を示し, その各々に対して, 欠報ならびにプラント誤停止の確率的特性を評価した。さらに, 警報システムが表示する情報からは, プラントの状態を判断できなくなる場合がありうることを示し, 警報システム構造と安全制御方策との関連を明らかにした。また, プラント事故発生の可能性とプラント誤停止の可能性を表す 2 個の評価基準を同時に最小にするという意味において, 最適な警報システムが存在することを明らかにした。

謝辞 本論文に対して多くの貴重なご指摘をいただいたレフェリーに深く感謝いたします。

参 考 文 献

- 1) T. Inagaki and Y. Ikebe : A Mathematical Analysis of Human-Machine Interface Configurations for a Safety Monitoring System ; IEEE Trans. Reliability, Vol. 37, No. 1, pp. 35~40 (1988)
 - 2) 糸川ほか : 安全技術入門, 中央労働災害防止協会 (1986)
 - 3) T. Inagaki : Interdependence between Safety-Control Policy and Multiple-Sensor Schemes via Dempster-Shafer Theory ; IEEE Trans. Reliability, Vol. 40, No. 2, pp. 182~188 (1991)
 - 4) M. J. Phillips : k -out-of- n : G Systems Are Preferable ; IEEE Trans. Reliability, Vol. 29, No. 2, pp. 166~169 (1980)
 - 5) 井上, 幸田, 熊本, 高見 : 安全監視システムの最適論理構成 ; 計測自動制御学会論文集, Vol. 24, No. 2, pp. 142~154 (1985)
 - 6) 田中 : 安全監視と危険監視の最適組合せによる高信頼度安全監視システム ; 計測自動制御学会論文集, Vol. 28, No. 6, pp. 725~732 (1992)
-