Research Report of the Research Institute
of Industrial Safety, RISS-RR-88, 1988.
UDC 658.513.3 : 167/168

安全作業システムの原理とその論理的構造

杉本　旭*

Principle and Logic of Safety in Man-Machine System

by Noboru SUGIMOTO*

Abstract ; Despite the fact that reliability of processing machines has been increasing recently occupational accidents show a rising tendency in last few years. At the same time, a newly born machine based on Micro-electronics, like a robot, that triggered Technology Innovation, presented new safety problems which is difficult to be handled by means of a conventional safety technology. These call for a rapid shift from conventional to new safety technologies.

In this paper, an operation conducted between man and machine is comprehended as a man-machine system, and approached from the logical structure of the system.

Safety operation is defined as that both the matter of "existence of human" (H) and the matter of "existence of movable parts of machine" (M) cannot happen at the same time and space.

This definition leads to a principle of safety operation, namely, $H \wedge M = 0$.

In addition to that, the requirements of the system aiming at the safety operation are to meet the following principles of safety structure :

1) Permission of operation along with confirmation of safety,
2) Inhibition of error on hazardous side.

The logical system structure of safety is achieved by means of Interlock and Fail-Safe technology.

Key words ; Safety, Safety Engineering, Safety System, Man-machine System, Fail-Safe, Interlock

1. はじめに

近年，産業機械における信頼性は著しく向上している。同時に，職場での教育・訓練の重要性が叫ばれ，人間のミスに起因するトラブルを少なくする努力も大いになされている。しかしながら，今もって，多くの労働災害が発生しており，しかも，最近，災害の減少傾向にかげりを見せていることも事実である。併せて，産業用ロボットなど，いわゆるメカトロ機械の進展に伴い，これまでの安全技術では対応できない新しい安全問題も発生してきており，安全技術の抜本的見直しと，安全技術の新たな展開の必要性が叫ばれている。

これまで，安全に係わる論議は，主として信頼性を基調とし，しかも，機械側と人間側のそれぞれの立場から展開されてきた。このような形で安全の論議がなされる限り，直面する問題を解決してゆくには限界があると言わざるをえない。

機械はいつかは故障し，人間はミスを犯すものであるという事実を認め，人間機械システムの構造として安全を追及しない限りは，「人間のための安全」は達成されえない。また，機械側と人間側から個々に立場を主張していては，人間機械システムとしての正しい安

* 機械研究部　Mechanical Safety Research Division

全構造を論ずることはできない。

本論文では，プレス機械等の従来形機械だけでなく，産業用ロボットのような新しい技術を伴う機械にも広く適用できるように，これらの機械と人間によってなる作業システムを人間機械システムとして捉えてこれを定式化し，その安全に係わる基本原理と論理的構造とを明らかにする。そして，これによって得られる安全作業システムが，インターロック構造とフェールセーフという2つの技術により実現可能であることを示す。

2. 安全作業システムの定式化と安全作業の原理

プレス機械や産業用ロボット等の産業機械に係わる作業システムに，広く適用する安全作業システムの一つのモデルとして，次のような定式化を行なう。なお，ここでは，定常作業の場合のみを対象とし，定常作業以外，例えば故障のために機械を修理する場合等は考慮外とする。また，「事故の型」については，危険な可動部との接触による「切れ・こすれ」，「挟まれ・巻き込まれ」等，機械災害として現在最も多く発生しているものを想定して検討を進める。

まず，作業空間（作業をする場所）を定式化する。Fig. 1 のように作業空間は，人間空間，共同作業空間（S），及び機械空間の3つからなるとし，人間は1人とする。人間は人間空間と共同作業空間のみを動く。また，機械は固定部と可動部に分かれており，固定部は機械空間に固定されており，可動部は共同作業空間と機械空間のみを動くものとする。定常作業では，一人の人間と機械の可動部とが共同作業空間Sで交互に協調して作業を行なうものとする。時刻tに，共同作業空間Sに人間が居ることを論理変数 $H(t)$ を用いて，又，同様に，時刻tに共同作業空間Sに機械の可動部が在ることを論理変数 $M(t)$ を用いて表すことにする。すなわち，

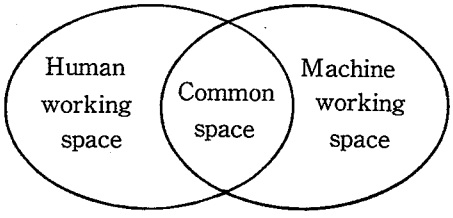

Fig. 1　Relations between the defined spaces in an operation system.
作業システムにおける空間の定義

$H(t)=1$ …時刻tに人間がSに居る，
$=0$ …時刻tに人間がSに居ない，
$M(t)=1$ …時刻tに機械の可動部がSに在る，
$=0$ …時刻tに機械の可動部がSにない，

とする。

人間機械システムにおける事故とは，許容値を超えてエネルギが，機械から人間に漏洩することであると見なされるが，これは人間と機械の可動部とが，物理的に同一時間に同一空間に存在する時に生ずる。従って，作業が安全に遂行されるためには，すべての時刻tにおいて，

$$H(t) \wedge M(t) = 0 \qquad (1)$$

が成立していることが条件となる。ここで，記号∧は論理積を表わしており，人と機械の可動部の位置関係に対して Table 1 で定義される。本論文では，以降(1)式を安全作業の原理と呼ぶことにする。すなわち，機械と人間とが，協調して作業を行ない，しかも，(1)式に示す安全作業の原理を満たしているためには，人間と機械の可動部とが時間的にずれて，交互に共同作業空間で作業をしなければならないことになる。

一般に，システムを安全な構造として求めるには，次の2つの基本的原理を満たさなければならない。本論文ではこれを安全の基本原理と呼ぶことにする。すなわち，

(i)　危険の可能性のある動作は，安全であることが確認されている時のみなされること，

(ii)　装置のいかなる故障も，危険の可能性のある動作を生じさせないこと。

作業システムが安全作業の原理を満足しつつ，上の2つの安全の基本原理をも満たす構造とするために，本論文では，次節以降に，インターロック及びフェールセーフという2つの技術を用いて，真の安全作業システムを実現する。

Table 1　Truth table of logical product (AND)
論理積（AND）真理値表

A	B	A∨B
1	1	1
1	0	0
0	1	0
0	0	0

3. インターロック

本論文で考察している安全作業システムにおける危険の可能性のある動作とは，$H(t)$及び$M(t)$，すなわち人間及び機械の可動部が，共同作業空間にあって実際の作業を行なうことである。一方，安全の確認は人間は人間空間に，機械の可動部は機械空間にそれぞれ明らかに存在することを確認することにより行なわれる。これらの確認信号をそれぞれ論理変数$H^c(t)$，$M^c(t)$を用いて表わすことにする。すなわち，

$H^c(t)=1$…時刻tに人間が人間空間に居ることが確認されている，

$=0$…時刻tに人間が人間空間に居ることが確認されていない，

$M^c(t)=1$…時刻tに機械の可動部が機械空間に在ることが確認されている，

$=0$…時刻tに機械の可動部が機械空間に在ることが確認されていない，

とする。

なお，$H(t)=0$は必ずしも$H^c(t)=1$を，また$M(t)=0$は必ずしも$M^c(t)=1$を意味していないことに注意されたい。何故ならば，現実には共同作業空間を離れて人間空間又は機械空間に戻って安全が確認されるまでには多少の時間がかかるからであり，$H(t)=0$かつ$H^c(t)=0$ということが，また$M(t)=0$かつ$M^c(t)=0$ということがあり得る。しかし，正常に動作している時には$H^c(t)=1$, $M^c(t)=1$であるのは，明らかに$H(t)=0$, $M(t)=0$の時のみであり，この条件による安全が確認される。今，否定を表わす論理演算を記号 $\bar{}$ で表わす（Table 2）とすると，上の事実は，

$$\left.\begin{aligned} H^c(t) &\leqq \bar{H}(t) \\ M^c(t) &\leqq \bar{M}(t) \end{aligned}\right\} \qquad (2)$$

が常に成立していることを主張している。

(2)式は，$H^c(t)=0$の時には$\bar{H}(t)=0$ということも1ということもあり得るが，$H^c(t)=1$の時には$\bar{H}(t)=1$，すなわち$H(t)=0$でなければならないことを主張している。同様に，$H(t)=0$，すなわち$\bar{H}(t)=1$の時には，$H^c(t)=0$の時には$H^c(t)=0$でなければならないことを主張している。$M^c(t)$についても同様である。なお，記号≦は，論理記号→と論理的には同じであるから，(2)式は$(H^c(t)\rightarrow\bar{H}(t))=1$, $(M^c(t)\rightarrow\bar{H}(t))=1$と表わしてもよい。

(2)式は，作業システムが安全であるための必要条件の一つであり，人間は一人しかいないこと，及び安全の確認信号$H^c(t)$，$M^c(t)$はSにおける存在信号$H(t)$, $M(t)$は，0であるべき時1には決して誤ってはならないことを意味している。

Table 2 Truth table of logical sum (OR)
論理和 (OR) 真理値表

A	B	A∧B
1	1	1
1	0	1
0	1	1
0	0	0

さて，安全の確認信号により安全が確認されてから，危険の可能性のある動作を行なうということは，$M^c(t)=1$の信号を得てから始めて$H(t)=1$となるべきこと，及び$H^c(t)=1$の信号を得てから始めて$M(t)=1$となるべきことを主張しており，これは同様に，

$$\left.\begin{aligned} H(t) &\leqq M^c(t) \\ M(t) &\leqq H^c(t) \end{aligned}\right\} \qquad (3\,a)$$

と表わすことができる。(3 a)式の条件を満たすように動作する機械構造を以降，ンターロック，すなわち(3 a)式の前半を人間側のインターロック，後半を機械側のインターロックと呼ぶこととする。

今，人間への作業命令及び機械への作業命令を，それぞれ論理変数$\hat{H}(t)$，$\hat{M}(t)$で表わすものとする。機械の作業命令$\hat{M}(t)$があった時，実際の機械可動部の作業$M(t)$は，人間が人間空間に退避して共同作業空間に居ない，即ち$H^c(t)=1$の時のみ1となり，それ以外は0でなければならず，機械側インターロックは，

$$M(t)=\hat{M}(t)\wedge H^c(t) \qquad (3\,b)$$

と記せる。また，人間の共同作業空間Sにおける実際の作業$H(t)$は，人間への作業命令$\hat{H}(t)$があった時，機械の可動部分がSに存在しないという確認ができた時，すなわち，$M^c(t)=1$の時のみ1であり，それ以外は0でなければならず，人間側インターロックは，

$$H(t)=\hat{H}(t)\wedge M^c(t) \qquad (3\,c)$$

と記される。以上のことは，次のようなフリップフロップ構造 (Fig. 2) を用いて模擬的に表現することができる。

なお，論理変数$M(t)$を混乱のない限り，機械の可動部がSに在ること，そのことを表す信号，及び可動部

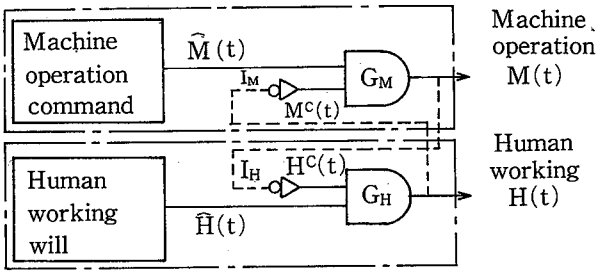

Fig. 2　Structure of a man-machine interlocking system.
人間機械システムのインターロック構造

に対するSでの実際の作業指示とに同一視して用いる。$H(t)$についても同様とする。

同図で記号 G_M 及び G_H はそれぞれ機械側及び人間側のインターロックを表現する論理積を表わしている。否定回路の記号 I_M, I_H の出力としてそれぞれ $M^c(t)$, $H^c(t)$が得られている，これは，それぞれセンサ等により，人間空間に人間が居ることを，及び機械空間内に機械の可動部が在ることを確認して得られる信号である。これらは，$M(t)$, $H(t)$の否定に相当しているが，前述した如く，(2)式を満足していなければならない。同図から分かるように，$\hat{M}(t)$と$\hat{H}(t)$とが同時に1になったときでさえ，$M(t)$と$H(t)$とは同時に1になることはなく，安全の基本原理(i)　及び安全作業の原理(1)式がインターロック構造により実現されていることが分かる。

4.　安全作業動作の論理的関係

Fig. 2 において，正常に動作している時，信号 $H(t)$, $H^c(t)$, $M(t)$, $M^c(t)$の関の関係について考察する。

まず，(2)式と(3)式から，

$$\left.\begin{aligned} H(t) \leqq M^c(t) \leqq \bar{M}(t) \\ M(t) \leqq H^c(t) \leqq \bar{H}(t) \end{aligned}\right\} \qquad (4)$$

を得る。(4)式を否定すると，

$$\left.\begin{aligned} M(t) \leqq \bar{M}^c(t) \leqq \bar{H}(t) \\ H(t) \leqq \bar{H}^c(t) \leqq \bar{M}(t) \end{aligned}\right\} \qquad (5)$$

を得る。(4)式と(5)式から，

$$\left.\begin{aligned} H(t) \leqq M^c(t) \leqq \bar{M}(t) \\ H(t) \leqq \bar{H}^c(t) \leqq \bar{M}(t) \end{aligned}\right\} \qquad (6a)$$

$$\left.\begin{aligned} M(t) \leqq H^c(t) \leqq \bar{H}(t) \\ M(t) \leqq \bar{M}^c(t) \leqq \bar{H}(t) \end{aligned}\right\} \qquad (6b)$$

を得る。

$H(t)$, $H^c(t)$, $M(t)$, $M^c(t)$の間には(6 a)式と(6 b)式の関係が常に成立していることが示された。(6 a)または(6 b)式から，$H(t) \leqq \bar{M}(t)$, $M(t) \leqq \bar{H}(t)$となって，これにより必然的に，(1)式の示す安全作業の原理が満たされる。すなわち，インターロック構造により安全作業の原理が成り立っていることが示される。

Fig. 3 に，(6 a)式の論理関係を示す。論理変数 $H(t)$, $H^c(t)$, $M(t)$, $M^c(t)$は，それぞれ0と1とをとるから，すべての組み合わせは $2^4=16$ 通りあるが，(6 a)式を満たすためには，Fig. 3 に示す通り，6通りの組み合わせしか許されない。すなわち Table 3 で示される6通りであって，Table 3 の①～⑥は Fig. 3 における①～⑥に対応している。

ここで，

①…人間が共同作業空間で作業をしている，
②…機械の可動部が共同作業空間で作業している，
③…人間は共同作業空間を離れているが，これが未確認であり，機械の可動部は機械空間にある，
④…機械の可動部は共同作業空間を離れているが，それが未確認であり，人間は人間空間にいる，
⑤…人間と機械の可動部は，それぞれ人間空間，機械空間にいる，
⑥…人間は共同作業空間と人間空間との，機械の可動部は共同作業空間と機械空間との間を移動中，

を意味している。

通常，作業は Fig. 3 において A で示されるルート，

Table 3　Logical relations of possible signal of safety operation system.
安全作業システムで許される信号の論理的関係

	ステップ					
	①	②	③	④	⑤	⑥
$H(t)$	1	0	0	0	0	0
$H^c(t)$	0	1	0	1	1	0
$M(t)$	0	1	0	0	0	0
$M^c(t)$	1	0	1	0	1	0

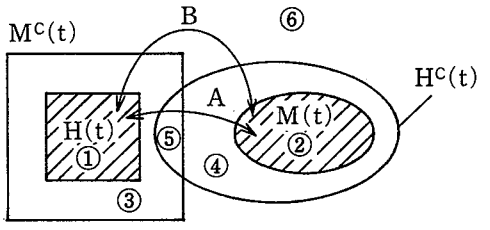

Fig. 3　Logical relations among H(t), $H^c(t)$, M(t), and $M^c(t)$.
H(t), $H^c(t)$, M(t), $M^c(t)$の論理的関係

すなわち，

①⇔③⇔⑤⇔④⇔②

又は，Bで示されるルート，すなわち，

①⇔③⇔⑥⇔④⇔②

により行なわれる。

さて，⑥の状態は，例えば，人間が共同空間を離れて人間空間に到着したという確認信号を得る前に，機械の可動部が機械空間を離れているが，それが未確認であることを表わしており，これは必ずしも望ましい状態ではない。これをなくすためには，人間（機械の可動部）が人間空間（機械空間）に到着したという確認を得てから機械（人間）は機械空間（人間空間）から離れることにすれば良い。これは，

$$H^c(t) \vee M^c(t) = 1 \qquad (7)$$

が成り立つことを，また，論理的には同じことではあるが，

$$\left.\begin{aligned} \bar{H}^c(t) &\leqq M^c(t) \\ \bar{M}^c(t) &\leqq H^c(t) \end{aligned}\right\} \qquad (8)$$

が成立することを要求している。ここで，記号∨は論理和を表わしており，人間と機械の可動部の位置関係に対してTable 4で定義される。以降，(7)式又は(8)式を安全確認の原理と呼ぶことにする。(6 a)，(6 b)式と(8)式から，直ちに，

$$H(t) \leqq \bar{H}^c(t) \leqq M^c(t) \leqq \bar{M}(t) \qquad (9)$$

または，

$$M(t) \leqq \bar{M}^c(t) \leqq H^c(t) \leqq \bar{H}(t) \qquad (10)$$

が導かれる。(9)式が成立するためには，Fig. 3で⑥の領域が消えて，許される場合はTable 3の①～⑤の5通りとなり，作業のルートはAのみとなる。すなわち，時刻を$t_1 < t_2 < t_3 < t_4 < t_5 < t_6 < t_7 < \cdots < t_{10}$とすると，作業は，例えば，Fig. 4のような時系列として進行することになる。同図で，T_M及びT_Hは機械及び人間が作業を要する時間を表わしている。同図から，常に(9)式が満たされていることが分かる。(9)式より，必然的に安全作業の原理(1)式，及び，安全確認の原理(7)式が導かれる。この意味からも，(9)式が各論理変数の間の関係を表す最も基本的な論理関係といえる。

なお，Fig. 4は，時間遅れを考慮して描いてあるので，時間遅れを無視して議論した(3 b)式及び(3 c)式とは必ずしも一致しない（勿論(3 b)式及び(3 c)式に時間遅れも考慮すれば一致する）。

Table 4
Truth table of negation (NOT).
否定（NOT）真理値表

A	$\bar{A}$
1	0
0	1

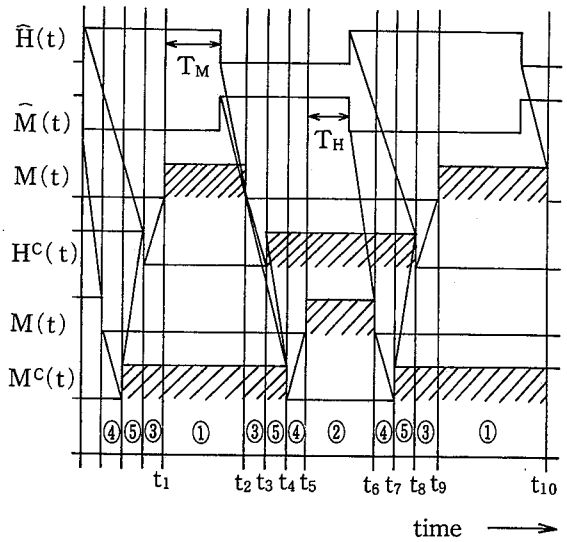

Fig. 4 Operational timing chart of Safety-Operation System
安全作業システムおける作業流れ(タイムダイアグラム)

5. インターロックの構成条件—フェールセーフ—

フェールセーフ（Fail-Safe）という概念は，元々は装置が故障しても安全であるという考え方に基づいており，鉄道信号の分野で古くから導入されてきた。論理装置にフェールセーフの考え方を導入したフェールセーフ論理回路が，電子回路として土屋[1]らにより実現されている。これには，2値（1,0）を用いるものと，3値（1,1/2,0）を用いるものとがあるが，ここでは，2値のフェールセーフ論理回路を例にして説明する。2値のフェールセーフ論理回路では，信号には真理値1と記される信号（これを危険側信号と呼ぶ場合もあるが，安全であるときに具体的制御の許可を与える信号であることから，本論文では安全信号と呼ぶことにする）と，真理値0と記される信号（これを安全側信号と呼ぶ場合もあるが，危険であるときに具体的制御の停止を与える信号であることから，本論文では危険信号と呼ぶことにする）との2種類がある。フェールセーフ

論理回路とは，回路内のいかなる故障に対しても，常に正しい信号を出力するか，または誤る場合には危険信号を出力するように構成されている回路をいう。すなわち，0であるべき時，決して1には誤らない論理回路をいう。このように構成するには，向殿ら[2]が提案しているように，安全信号に高エネルギー状態を対応させる必要がある。回路内に故障が生ずると，高エネルギー状態を保持できないように構成しておけば，回路内に故障が生じて誤る場合には常に安全側(0：危険信号）となる。すなわち，他からエネルギーを受ける事なしに低エネルギー状態が高エネルギー状態になることは物理的にありえないという事実から，危険信号が故障により誤って安全信号となることはないという非対称誤りの出力特性（これをフェールセーフの原理と呼ぶことにする）を実現することができる。

安全作業システムにおいては，$M(t)$，および$H(t)$が安全信号となる。よって，Fig. 2における論理積演算要素（ゲート）G_M及びG_Hは0であるべき時1に誤ってはならない。すなわち，G_M，G_Hはフェールセーフ論理回路，すなわち非対称誤りの出力特性を持つ論理回路で構成されていなければならない。また，$H^c(t)$，$M^c(t)$の信号も，0であるべき時1へ誤ると，$M(t)$及び$H(t)$をそれぞれ0であるべき時1としてしまうから，これらも誤って安全信号を発生してはならない。よって，$H^c(t)$，$M^c(t)$もフェールセーフの条件を満たしていなければならない。このように構成すれば，いかなる故障に対しても安全の基本原理(ii)及ぶ(2)式を満足することになる。なお，$H^c(t)$，$M^c(t)$の信号は，$H(t)$，$M(t)$の信号から，否定回路を用いて構成してはならないが，それはフェールセーフな否定回路であっても駄目である。何故ならば，$H(t)$ $\{M(t)\}$がフェールセーフな故障により誤って0になったとすると，否定回路が正しく動作することにより$H^c(t)$ $\{M^c(t)\}$は安全信号1となってしまい，本来0であるべき時1となり結果的にフェールセーフの条件を満足しないことになるからである。すなわち，否定回路を含む$\bar{H}(t)$，$\bar{M}(t)$は(2)式を満たし得ないからである。Fig. 2で$H(t)\{M(t)\}$と否定回路I_H（I_M）とが点線で結ばれているのはこのことを意味している。よって，信号$H^c(t)$は，例えば人間が人間空間に居る時に押しボタンを押して高エネルギー状態の信号を出力させ，人間が人間空間を離れたり又はその装置が故障したりした時には低エネルギー状態になるよう，直接，このセンサをフェールセーフの原理に従って構成しなければならない。$M^c(t)$についても同様である。なお，共同作業空間Sに人間が居ないということを，フェールセーフの原理に従って直接検出しても良い。この場合には，人間と機械の可動部の動特性を考慮して，共同作業空間の周辺に余裕を持たせた領域に例えば光センサを設置し，人間のいない時にはエネルギーを受けて高エネルギー状態とし，人間が入ると光を遮ってエネルギー零の状態として機械の運転を停止させることが考えられる。

G_H，I_H，I_Gをフェールセーフに構成しておけば，正常に動作している時は勿論のこと，故障が生じても安全の基本原理(ii)および(2)式が実現されており，常に安全であることになる。

以上により，フェールセーフなインターロック構造を用いることにより，安全の基本原理(i)，(ii)，さらに(2)，(3)式が，従って安全作業の原理(1)式がいかなる故障に対しても成立していることになる。

6. 誤り動作に関する考察

ここで本論文で定式化した安全作業システムにおける故障等による誤り動作について考察する。

一般に，人間側作業に関して，

$$H(t)=Hs(t)\vee Hf(t)$$

と置ける。ここで，

$Hs(t)$…正しい動作として人間が時刻tに共同作業空間に居ること，

$Hf(t)$…誤った動作として人間が時刻tに共同作業空間に居ること，

を表わす論理変数とする。ただし，$Hs(t)\wedge Hf(t)=0$である。同様に，機械側の作業に関して，

$$M(t)=Ms(t)\vee Mf(t)$$

と置ける。ここで，

$Ms(t)$…正しい動作として機械の可動部が時刻tに共同作業空間に居ること，

$Mf(t)$…誤った動作として機械の可動部が時刻tに共同作業空間に居ること，

を表わす論理変数とする。ただし，$Ms(t)\wedge Mf(t)=0$である。上式より

$$\begin{aligned}&H(t)\wedge M(t)=\\&\{Hs(t)\wedge Ms(t)\}\vee\{Hs(t)\wedge Mf(t)\}\\&\vee\{Hf(t)\wedge Ms(t)\}\vee\{Hf(t)\wedge Mf(t)\}\end{aligned}\qquad(11)$$

となる。安全作業の原理(1)式が成り立つように，作業システムが設計されているならば，

$$Hs(t) \wedge Ms(t) = 0$$

が成立しているはずである。よって，もし誤り動作が生じた場合にも安全作業の原理が成立しているためには，

$$\{Hs(t) \wedge Mf(t)\} \vee \{Hf(t) \wedge Ms(t)\} \vee \{Hf(t) \wedge Mf(t)\} = 0 \quad (12)$$

でなければならない。人間側と機械側の両方がフェールセーフに実現されているならば，いかなる故障に対しても $Mf(t)$ 及び $Hf(t)$ という誤りはないはずであるから，(12)式は常に成立している。一方，フェールセーフ構成でない場合を考えてみる。ただし，人間側及び機械側共にインターロック構造を有するものとする。いま，一方が危険側の誤りを犯したとする。すなわち，例えば Fig. 2 でゲート G_H が 0 であるべき時 1 を出力したとする。この時，$Hf(t)=1$ となり，人間が共同作業空間に入ろうとする。しかし，他方のインターロックを構成しているゲート G_M が正常であるから，$H^c(t)=0$ という信号から，$M(t)=0$ となり，(12)式は成立し安全作業の原理は保持される。ただし，この場合は強制的停止状態である。他方，$Mf(t)$ が 1 となった場合も同様である。フェールセーフでない場合は両方とも同時に誤動作して $Mf(t)=1$, $Hf(t)=1$ となった時に，安全作業の原理がくずれ，危険な事態が発生する。

これまでの論議では，人間側と機械側とを対等に取り扱ってきた。しかし，現実には機械側はインターロック構造にでき，しかもそれをフェールセーフに構成できるが，人間側のインターロックに対応するゲート G_H は人間の判断に任されているので，一般にフェールセーフにもできないし，又，インターロック構造をとることもできない。

そこで，機械側のみフェールセーフなインターロックの構造をとるとする。この場合には，$Mf(t)=0$ となるので，$Hf(t) \wedge Ms(t)$ という項のみが危険を表わすことになる。ところが，機械側のインターロックが正常に働いていれば前述のように $Mf(t)=Ms(t)=0$, すなわち $Mf(t)$ $\{Ms(t)\}$ 作業指示と解釈すると，強制的停止が働いていることに相当し，安全が確保される。また，機械側が故障した場合には，フェールセーフの構成がとられているから $Ms(t)=0$ となり，やはり同様に安全が保証されることになる。

以上のように，機械側が完全にフェールセーフ化されていて，インターロック構造になっていれば，構成要素の故障及び人間の危険側の誤り動作に対しても強制的停止となり，常に安全であるということができる。

7. 今後の課題

本論文によって，安全作業システムの論理構造が明らかになったが，残された問題がいくつかある。これらの今後の課題について述べる。

（1） 機械側にとっての安全信号 $M(t)$ が 1 から0に変化する場合には，次の 2 通りの場合がある。1 つは，機械の可動部による作業が終わって，作業命令 $\hat{M}(t)$ が 1 から 0 となった時であり，これは正常な作業の一部である。他の 1 つは，$\hat{M}(t)$ は 1 であるのに，誤動作が原因で $M(t)$ が 1 から 0 になる時である。これには，(i)インターロックを実現しているフェールセーフなゲート G_M の故障で G_M の出力を 1 にすべき時に 0 に誤った場合，(ii)人間が人間空間に居ることを検出するフェールセーフなセンサ I_H が故障して，I_H の出力を 1 にすべき時に 0 に誤った場合，及び(iii)人間が人間空間に留まるべき時誤って人間空間を離れた時（これは，人間側のインターロックが有効となっていないことに相当する）の 3 つの場合である。これらは，機械の可動部が作業中であるにもかかわらず，$M(t)=0$，即ち「共同作業空間から出ろ」という機械側への命令に相当し，生産側に与える犠牲が大きい場合も出てくる。従来，このような場合，強制的停止状態をとる方法が取られてきた。しかし，この誤り動作による強制的停止状態は極めて異常な状態であり，正常作業における 1 → 0 の停止とは区別されるべきものであり，安全の確認がなされる条件のもとで，段階的に運転の継続の許可を与える新しいインターロックの構造も検討すべきである。

（2） 本論文で考察した安全作業システムのモデルでは，人間は一人とした。しかし現実の問題として，一人が共同作業空間で作業中に，他の一人が人間空間に侵入するという事態が発生する可能性は少なくない。このような場合，$H^c(t)=1$ となって機械の可動部も共同作業空間に入ることになり，安全作業の原理かが破られることになる。人間が二人以上いることを考慮すると，5 節で述べたように，人間が共同作業空間に居ないということを検出するフェールセーフなセンサが必要となり，本論文で考察した信号 $H^c(t)$ が，人間が人間空間内にいるときに 1 を出すフェールセーフなセンサであったのとは逆の特性となる。このように，各種の状態に適用できる個々のフェールセーフなセンサを開発する必要がある。

8. 終わりに

本論文では，安全作業システムの定式化と，それを実現する二つの技術，すなわち，インターロック構造とフェールセーフについて述べ，また各信号間の論理関係を明らかにした。更に，機械側がフェールセーフなインターロック構造になっていれば，常に安全であることを示し，工学的には安全制御に人間の判断の要素を含まないことを示した。

安全の観点から人間機械システムを論ずる場合，これまで人間側からのアプローチとしてフールプルーフ，そして機械側からのアプローチとしてフェールセーフが個々に提案されてきた。本論文では，インターロックという概念を導入することにより，人間の行動にミスを許し，また機械の故障を生じてもなお安全が保持される安全作業システムを提案している。これは，安全の観点からこれまでなされなかった安全構造へのアプローチである。これらの成果は更に具体的適用を目指すことにするが，安全は単一の工学を超えた討議が必要である。専門工学の境界を超えて広く検討を望む。

謝　辞

本論文はすでに発表した論文（杉本旭，蓮原弘一，向殿政男，“安全作業システムの原理とその論理的構造”，電気学会論文誌　D-107-9，1092-1098（昭和62-9））に手を加え，解説を補って当研究所の産業安全研究所研究報告としてここに報告するものである。産業安全に係わる分野の多くの方々に参考になれば幸いである。

最後に，当研究所の研究報告とすることを快く御了承いただいた，共同研究者の蓮原弘一（日本信号株式会社），向殿政男（明治大学）両氏に謝意を表する。また，本研究をまとめるに当たり御尽力いただいた東京工業大学の芳司俊郎君に紙面を借りて感謝の意を表する。

（昭和63年4月4日受付）

参考文献

1）土屋，フェイルセイフ論理方式の研究，電気試験所研究報告，No. 695（昭44-1）

2）向殿，C-型 Fail Safe 論理の数学的構造について，信学論，52-C，812（昭44-12）