Research Reports of the National Institute
of Industrial Safety, NIIS-RR-95 (1996)
UDC 161.2:164.01:62-783:621.3.07:681.586

安全制御システムの基本構成
—安全制御の原理とフェールセーフシステムの構成方法—

杉本　旭*, 梅崎　重夫*, 池田　博康*, 粂川　壮一*, 深谷　潔*

Fundamental Structure of Safety Control System
— Principles of Safety Control and Configulation Method for Fail-safe System —

by Noboru SUGIMOTO*, Sigeo UMEZAKI*, Hiroyasu IKEDA*,
Soichi KUMEKAWA* and Kiyosi FUKAYA*

Abstract: Recently, the reliability of industrial machines has been remarkably improved. In reality, however, there still have been a large number of accidents caused by industrial machines mostly due to failures in safety securing means. On the other hand, the evolution of mechatronic machines has brought new safety problems, such as the runaway of machines caused by electromagnetic noises. Therefore, the safety securing means of a machine should be so fail-safe as to exactly prevent any accident by stopping the machine in case of machine failure.

In view of the above consideration, this paper describes a theory of securing safety for such a system that enable men and machines to cooperate to work each other, and examines the validity of the system configulation theory proposed for a fail-safe system to achieve such a system.

Chapter 2 treats the safety promotion process through many experiences of accident. Such a conventional safety system that people accept the occurrence of a hazardous failure owing to the probablistic reason are discussed. This study is based on the concept of fail-safe that never accepts the failures of hazardous side.

In chapter 3, such logically unate relation that outputs energy only when safety is confirmed is discussed. Energy used for the industrial purpose is basically different from the energy that causes natural desaster. Industrial energy should be normally controlled and any disastor should be avoided in deterministic (not probablistic) manner by means of fail-safe control technology. The reason for deterministic safety based on logically unate relation is explained by a thermodynamic model.

A logical structure of safety securing system is discussed in chapter 4. An accident is analysed, and the accident process is expressed by binary logic. The safety defined as the denial of accident can be indicated as a confirmation of safety by means of safety signal. Such uncertain condition that safety is not confirmed should be judged as hazardous for a reason that safety must be guaranteed by all means. This truth is concluded as the "principle of safety confirmation".

In Chapter 5, an evaluation of safety is newly proposed, and in chapter 6, a model of the safety man-machine operation system attained through formulation is actually applied to the working site where men and machines are collaborating each other, and the validity of such model is demonstrated.

Keywords; Safety, Safety control, Fail-safe, Inherent safety, Fool-proof, Interlock, Logically unate relation, Safety confirmation, Safety principle

*機械システム安全研究部 Mechanical and System Safety Research Division

1. 緒　言

もともと，誰も危険な状況に近づかなければ事故とはならないはずである。事故は，人と他の物体との間でのエネルギーの移動によって生じ，典型的には衝突と見ることができる。よって，両者が十分離れた関係にあれば安全が確保されることになる。

しかし，現実には人は単に危険に近づかないという方法だけでは生活することは不可能である。このことは，文化的な生活を行うために，航空機や自動車に乗って旅行をしたり，危険な機械や物質を扱っていることを考えれば明らかである。すなわち，人と機械とが互いに関連を持ちつつ高度な文明を作り出そうとする現代では，事故がいつ起こるか分からない高エネルギー状態で人は行動せざるを得ず，しかもこの不安は拡大される傾向にある。

一方，事故に対する責任が厳しく問われるようになっているにも拘わらず，事故が繰り返されており，現状の安全対策に対する抜本的な見直しが求められている。

これまで，安全対策は確率論に基づく効果が求められてきた。しかし，事故というものは，一つ一つ回避しなければならず，しかも，その回避には失敗が決して許されないはずである。しかし，現実には事故回避（制御）には誤りが含まれ，この誤りに対する安全がフェールセーフによって確保されなければ，従来通り，安全対策は確率論的効果を示すにすぎない。

本研究では，これまでの安全対策を見直す上で，フェールセーフの導入が不可欠であるものとし，まず第2章で，危険の認識に始まり，安全が確保されるまでの過程を論理的に検討し，安全確保におけるフェールセーフの立場を明らかにする。

ところで，フェールセーフシステムでは，エネルギー（仕事出力）が出力されるときは，少なくとも安全でなければならない。このとき,「安全」と「エネルギー」との間に論理的にユネイトな関係があると言われる[1),2),3)]。第3章では安全に係わるエネルギーの一般的特性について検討を加える。そのため，自然に蓄積されて災害（自然災害）を生ずるエネルギーは，ユネイトな論理的関係が実現できないことをまず示し，次いで，工学で扱うエネルギーは，システムの故障によってエネルギーを消散する熱力学的特性を利用することによってユネイトな論理的関係が実現できることを示す。

さらに第4章では，ユネイトな論理的関係によりフェールセーフを実現するための基礎となる安全確保の原理を示す。ここに，この原理を事故の回避操作に適用し，フェールセーフの条件で事故回避操作を行ってできる限り機械の稼働状態を維持するための機械の運転システムについて検討を加える。

第5章では，安全性の評価方法について述べ，さらに第6章では，ユネイトな論理的関係が人と機械の共同作業において成立することを示し，その実現方法について述べる。なお，すでに著者等は危険性を伴う行為（危険行為）であれば予め安全の確認に基づいて実行しなければならないものとし，その構成を安全確認システムと呼び，これまでにいくつかの提案[4),5)]を行ってきた。第4章で論ずる安全システムの構成原理は，事故の回避が現実に安全確認システムを運用する上で不可欠であることから，これを考慮に入れた作業システムを構成するための基本的な原理としてここに改めて提案する。

2. 事故に基づく安全の認識過程

ここに，事故，危険状態（事故の予測状態），対策なしをそれぞれ2値の論理変数 A_{CC}，H_{az}，$\overline{M_{\mathrm{es}}}$で表し，それぞれ事故が発生するとき，危険状態であるとき，対策なしのときを論理値1に定めるものとする。対策が講じられていないとき危険状態となって事故が起こるから，次式が成立する。

$$A_{cc} = H_{\mathrm{az}} \cdot \overline{M_{\mathrm{es}}} \tag{1}$$

ここに，記号 “—” は論理否定を，また記号 “・” は論理積を示す。安全対策を講ずるには事故の発生機構を解明する必要がある。そのため，例えば，化学物質の発火危険性，食品添加物等の毒性，新材料の破断強度など，危険性を予め評価するための研究分野，あるいは事故の発生機構を解明する研究分野が存在する。

さらに，事故でないこと（否定）が安全を意味するから，式 (1) にド・モルガンの公式を適用すれば次式が得られる。

$$\overline{A_{\mathrm{CC}}} = H_{\mathrm{az}} \vee M_{\mathrm{es}} \tag{2}$$

ここに，記号 “∨” は論理和を示す。式 (2) によれば，危険 H_{az}が存在するかぎり，これを明らかにして事故を回避するための対策が必要であることが分かる。すなわち，$M_{\mathrm{es}} = 1$ であれば危険状態であっても事故は発生しない。

一方，危険な状態となったとき，たまたま安全装置が故障していたために事故となる場合が少なくない。このような事故は，危険状態 ($H_{\mathrm{az}} = 1$) のとき，安全装置が故障し，しかも，それが危険側の故障であった場合に起こる。いま，安全装置の故障発生と故障が危険側であることをそれぞれ論理変数 E_{rr}，H_{side}で表し，故障発生と危険側故障を論理値1で表すものとすると，事故 (A_{CC}) は次式で表せる。

$$A_{CC} = M_{es} = E_{rr} \cdot H_{side} \tag{3}$$

ここで式 (3) を否定し，さらにド・モルガンの公式を適用すると，安全 A_{CC}は次式で示される。

$$\overline{A_{CC}} = \overline{E_{rr}} \vee \overline{H_{side}} \tag{4}$$

式 (4) は，安全対策 M_{es}が故障しない ($\overline{E_{rr}} = 1$) か，または故障が安全側 ($\overline{H_{side}} = 1$) であれば事故にならないことを意味している。式 (4) を高信頼化技術とフェールセーフの観点で見れば，安全は，高い信頼性を得るか，または安全側に故障するように機械を構成するかのいずれかによって実現できることを意味する[6]。

機械は必ず故障し，しかもいつ故障するか分からない。特に，安全対策（安全装置）に生ずる故障は，他の一般的故障とは当然区別されなければならない。安全側の故障とは，究極的には機械を停止することである。今後，適切な安全対策を講じていくためには，そのために設置した安全装置が故障したとき機械を停止するフェールセーフ ($\overline{H_{side}} = 1$) が不可欠である。

3. 安全確認の形態

3.1 自然災害とエネルギー

自然界では，長時間をかけて大きなエネルギーが局所的に蓄積される場合がある。地震，雪崩，落雷，暴風雨，山火事など多くの自然災害は，蓄積エネルギーが短時間に放出されたために人に被害を与えるものだと言える。蓄積されたエネルギーは周囲に拡散しようとするが，この拡散を阻止しようとする力が局所的に存在するとき，これが原因となってエネルギー蓄積が起こるという見方もできる。ここでは，災害の特性をまずエネルギーとの関係で論理的に考察する。

蓄積エネルギーがある限界を超えると，一挙に放出されるものとし（しきい値特性），この放出エネルギーの有無を 2 値の論理変数 U_H（放出しているときを論理値 1，放出していないときを 0）で，蓄積エネルギーの有無を E（蓄積ありを 1，なしを 0）で表すものとする。また，エネルギーの放出を阻止する作用を論理変数 E^*で表し，その作用が正常であるとき（すなわち阻止する能力を有するとき）を論理値 1，正常でないときを論理値 0 で表すものとすれば，エネルギーが放出されていない状態$\overline{U_H}$は，もともと蓄積エネルギーがないかまたはそれがあっても放出を阻止しているかのいずれかの関係として，次式で与えられる。

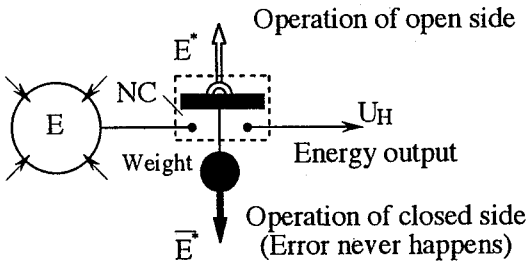
$$\overline{U_H} = \overline{E} \vee E \cdot (E^* \cdot \overline{E^*} \cdot \xi_f') \tag{5}$$

式 (5) は，エネルギー放出を阻止できない状況を含んでいる。すなわち，式 (5) のξ_f'は，放出を阻止する作用を失った場合（すなわち$\overline{E^*} = 1$）のエネルギーの放出を示す論理変数である（放出しないときを論理値 1 で表す）。解放されたエネルギーは周辺に拡散するから，自然界では明らかに$\xi_f' = 0$である。式 (5) に，ド・モルガンの定理を適用して整理すると次式が得られる。

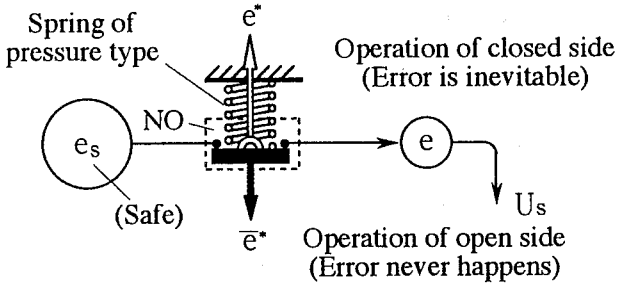
$$U_H = E \cdot \overline{E^*} \cdot \overline{\xi_f'} \tag{5'}$$

蓄積エネルギーの放出を阻止する力はいつか失われるのであるから，エネルギー蓄積が生ずるところでは，自然災害は避けられないと言わざるを得ない。しかも，それがいつ起こるかについて確定することは大変難しい（すなわち，$E^* = 1 \rightarrow 0$ は時間的に確率分布で与えられる）。自然災害の特性は，**Fig. 1(a)** の論理ゲートで表すことができる。この場合，通常時閉（ノーマルクローズ）型の重力リレーのモデルで表しており，エネルギーの放出を阻止する力が失われることがあっても，放出しようとする力の方は決して失われないことを示している。例えば，地震災害の場合，強固な岩盤は地震の発生を抑えるが，蓄積エネルギーが大きくなる可能性がある。そのためかえって大型の地震が発生する場合がある。また，地震の発生時刻を正確に予測することは難しいことから，長期間地震がないからといっても必ずしも安心できない。

一方，人工のシステムにおいても同様の状況がある。



(a) Natural disasters modeled by gravity relay



(b) Energy transmission by electromagnetic relay (Normal open type)

Fig. 1 Energy accumulation and transmission.
エネルギー蓄積と伝達手段

例えば，航空機の飛行状態では位置エネルギーが蓄積される。この場合，操作の失敗やエンジンの不調で（$E^* = 1 \rightarrow 0$）高度の維持ができなくなり（ξ_f'$= 0$），ついに位置エネルギーを一挙に放出する。これが墜落事故である。このように，エネルギーの蓄積状態を維持する操作は，本来誤りが許されない。逆の見方からは，このようなシステムでは，事故は有限の確率で起こることを認めざるを得ないため，人の訓練，システムの高信頼化，また災害による損失を可能なかぎり小さくするための対策が強く求められる。フェールセーフシステムは，このような危険側の故障や操作ミスが必然的に含まれるシステムとは明確に区別して扱われる[6]。

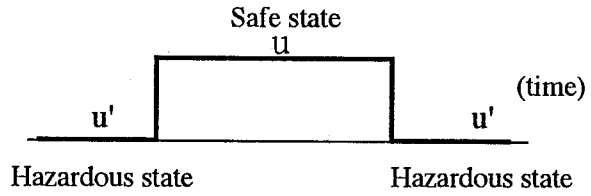
3.2 工学で扱われるエネルギー

3.2.1 安全確認のエネルギー形態

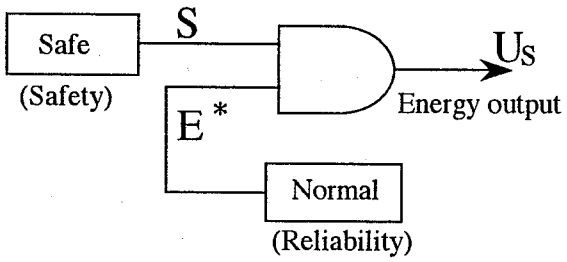
自然災害においては，エネルギーの蓄積状態を制御することはもちろんのこと，それを正確に予測することは難しい。しかし，工学的に利用するエネルギーは人によって制御される。ただし，第2章で述べたように，その制御はいつでも成功するとは限らず，事故が起こる可能性がある。本項では，機械的操作をエネルギーの制御とみなし，その制御の誤りに対して事故防止を実現するためのフェールセーフについて論ずる。

危険を伴う移動体や作業機械（人を含む）のエネルギーは事故を生じないという予測（安全の確認）に基づいて出力される。したがって，安全状態の出力エネルギーを u，危険状態の出力エネルギーを u' とすれば，次の不等式が成立する[7]。

$$u > u' \tag{6}$$



(a) Energy output in safe state



(b) Interlock model based on Uneit-logical relation

Fig. 2　Condition of output energy.
出力エネルギーの条件

式 (6) は時間軸上のエネルギーレベルとして **Fig. 2(a)** で表すことができる。そして，エネルギー u は少なくとも誤って発生されてはならない。すなわち，出力エネルギーは，出力 u' であるべきときに出力 u が発生してはならないが，出力 u であるべきとき出力 u' となることは許される。例えば，列車やロボット等において，止まるべき時に動いてはならないが，動くべき時に止まることは許される。一方，すでに述べたように，航空機が一度高エネルギー状態として空に上がった場合，あるいは列車や車でも急停止が許されない状態など，必ずしも出力レベル u' となることが許されない場合が存在するが，これに対しては別の議論が必要である。

3.2.2 フェールセーフとエネルギーの条件

事故を許容しない式 (6) によれば，もともと危険状態で大きなエネルギーは出力されない。エネルギーの出力状態を U_S で表し（出力時を論理値1で表す），安全を示す論理変数を S（安全を論理値1，安全でないを0）とすると，式 (6) の関係は，次の論理的関係に書き改められる。

$$S \geqq U_S \tag{7}$$

ここに論理記号 $\geqq$ はユネイトな関係[2]（正の単調な関係）を示す。すなわち，式 (7) の関係は，2つの論理値が $1 > 0$ であるものとして，**Table 1** の真理値表で示される。

式 (7) において両辺が一致しない状況，すなわち安全であっても必ずしもエネルギー出力しない状況は，例えば，安全を確認するセンサが故障で「安全」と判断できないという場合である。たとえ安全であったとしてもそれが確認できない場合があり，このときはエネルギー出力を停止すべきことから，式 (7) のユネイトな関係は，**Fig. 2(b)** のようなインターロックモデルで示される[9]。このように，現に安全であるばかりで

Table 1　Logically Uneit relation　$(S \geqq U_S)$
ユネイトな論理的関係

S	U_S
1	1
1	0
0	0
0	1

This combination is prohibitted.

なく，安全であることがセンサ等（後で示すように，式(19)の安全情報 Sc）を用いて確認されなければ，本当の「安全」とはならない。

フェールセーフにおけるエネルギーの扱いが自然災害の場合のエネルギーと根本的に異なることを示すために，ここで改めて，安全であるとき蓄積されるエネルギーを式(6)と同様に Eとし，また正常時を E^*とすれば，蓄積エネルギー Eは次式で表せる。

$$E = S \cdot E^* \vee \overline{E^*} \cdot \xi_S' \tag{8}$$

ここにξ_S'は，故障時（$\overline{E^*} = 1$）のエネルギー蓄積状態を示している（エネルギーを蓄積するときを論理値1，蓄積しないときを論理値0）。故障時のエネルギーEは消散されるときに限り，$\xi_S' = 0$である。この条件が満たされれば，蓄積エネルギー Eをエネルギー源とするあらゆる出力エネルギー U_Sは次の論理不等式で示される。

$$S \geqq E \geqq U_S \tag{9}$$

出力エネルギー $U_S = 1$は安全である時のみ生じ，一方 $U_S = 0$には，危険な場合ばかりでなく故障で出力できない場合も含まれる。式(4)で定義したフェールセーフ（$\overline{H_{\text{side}}} = 1$）は，危険側の故障を含まない条件で式(6)（$u > u'$）を実現する。ただし，これはあくまでも$\xi_S' = 0$であることが前提である。そこで，改めて$\xi_S' = 0$の条件について次に考える。

3.2.3 ユネイトな論理的関係

本来，安全確保は，例えば安全手段の故障を認めながらも，その故障で事故を生じることはないというように確定論に基づく。すなわち，安全手段による安全であるという判断で機械の運転を実行するシステムでは安全という判断には確率論が適用されない。式(7)で示されるユネイトな論理的関係（論理不等式）は，確定論による安全を扱う数学的手段であるばかりでなく，その実現のための構造を規定している点に注目すべきである。そこで，次にユネイトな論理的関係を実現する一般的構造について検討を加える。

熱力学によれば，熱力学的孤立状態は，エントロピー極大状態として決定される。この場合，故障によってエネルギーを遮断するものとすれば，無効エネルギーの蓄積状態（消散状態と呼ぶ）として予見できる。この場合，故障によって定まる状態は，次式のような熱力学的過程として記述できる。

$$e = e_S \cdot e^* \vee \overline{e^*} \cdot \xi_S' \tag{10}$$

論理変数 e，e_Sはそれぞれ，蓄積エネルギー，外部のエネルギー源であり，e^*は正常時の操作，ξ_S'は蓄積エネルギー eの消散状態を示す。ただし，これらは2値の正の論理変数で表している。

正常操作（$e^* = 1$）によってエネルギー源 e_Sからエネルギーが流入し，故障時（$\overline{e^*} = 1$）に流入を遮断する熱力学的過程（式(10)）は，**Fig. 1(b)** のようなエネルギー源 e_Sを持つゲートの特性で表現できる。この場合，通常時開型（ノーマルオープンタイプ）の電磁リレーモデルで表しており，正常時には接点を閉じる操作を行い，故障時は閉じる操作を止めることで接点が開く構造である。故障時のエネルギー蓄積状態は $e = 0$であるから，式(10)は，単純に次式で示される。

$$e = e_S \cdot e^* \tag{11}$$

このように，ユネイトな論理関係は，基本的にはエネルギー伝達過程における熱力学の特性を用いて実現されている。また，これは次のような安全の生成及び出力過程にも適用される。

(a) 直動型センサ

Fig. 1(b) で，安全なとき e_Sを生成し，安全でないときこれを生成しないとすれば，エネルギー eは安全かつ故障なしのときのみ蓄積される。すなわち，$S \geqq e$であると共に $e^* \geqq e$である。このセンサ構成は，一般に直動型センサと呼ばれ，安全を示すエネルギーを直接生成するセンサ，例えば，温度を検出する熱伝対，速度を検出するタコジェネレータである。

(b) 変調変換型センサ

さらに，**Fig. 1(b)** の e^*の操作を安全なときに行い，安全でないとき操作をやめる方法は，安全であることをエネルギー e_Sを利用して伝えることから変調変換型センサと呼ばれる。この場合，$S(= e^*) \geqq e$であるとともに $e_S \geqq e$である。**Fig. 1(b)** の電磁リレーはバネに機械的エネルギーを蓄積するが，このバネのエネルギーが安全 Sを示し，接点を閉じる。また，安全でないときまたは故障のときにはバネのエネルギーを消散して接点を開き，$e = 0$を実現している。

(c) 動力遮断系

機械的出力 U_Sを実行すれば，運動エネルギーまたは位置エネルギーが蓄積される。すなわち，機械的出力も式(10)の熱力学的過程の一般的特性に従うと考えなければならない。この機械的エネルギーの蓄積過程は，同様の手順によって次式のように書ける。

$$E_B = U_E \cdot E_B{}^* \vee \overline{E_B{}^*} \cdot \xi_{BS}' \tag{12}$$

ここに，E_Bは機械の運動（または位置）エネルギーの蓄積，$E_B{}^*$は機械出力の蓄積系までの伝達，ξ_{BS}'はエネルギー遮断時（$\overline{E_B{}^*} = 1$）のエネルギー蓄積状態を示す論理変数であり，全て2値の正論理で表している。

熱力学的孤立状態では機械的エネルギーも例外なく $\xi_{BS}' = 0$ である。これは，例えば電源を落とせばいつかは必ず運動を停止することから明らかであるが，一般に，危険回避のための機械停止は緊急を要すため，運動エネルギーを積極的に消散させる目的で摩擦ブレーキが使用される。式 (12) のエネルギー伝達手段 $E_B{}^*$ の最も分かりやすい例として，クラッチ/ブレーキシステムがある。これはクラッチとブレーキが互いに否定の関係で構成される。$E_B{}^* = 1$ はクラッチ作動して運転し，危険なとき $\overline{E_B{}^*} = 1$ でブレーキを作動することによって緊急停止を実現している。

以上述べたように，正常を条件とする出力のユネイトな論理的関係が，実は，厳密には故障時には決して出力を生じない構造を求めており，この構造は，**Fig. 1(b)** のように，2つの蓄積エネルギーの伝達系において，故障時伝達されないばかりでなくすでに蓄積されたエネルギーを必ず消散するという熱力学的過程そのものを利用する以外には実現できないといえる。

4. 安全制御の構成論理

4.1 危険回避制御

「安全 (Safety)」は，事故を予測して回避する過程で生ずる概念であると考えられる。通常，人は，事故の予測を行って「危険」と判断するとき，それまで行っていた行動（危険行為）とは別に事故の回避行動（改めて危険回避と呼ぶ）をとる。ただし，危険回避は，単に緊急を要するばかりでなく，少なくとも事故の直前までには回避を成功していなければならないという時間的制約（時間条件）があることは言うまでもない。

Fig. 3(a) に危険回避の過程を示す。時間軸上で（未来に向かって）行動するとき，将来定まる状況は事故か事故でないかのいずれかでしかない。そこで，「事故」を事故（論理値 1）と事故でない (0) の2値とする論理変数 $Hd(t) \in \{1,0\}$ で表し，事故の発生時刻 t_0 までの区間 ($\overline{Hd}(t) = 1$) では事故を生じない（真の安全または真の安全区間と呼ぶ）とする。

危険回避には時間を要し，しかも，少なくとも事故の直前までには回避を完了するためには，人は，通常，t_0 より十分手前に時刻 t_s を定め，時刻 t_s を過ぎたら「危険」と見なし危険回避の行動を開始する **Fig. 3(a)** の斜線の方法をとる。ここで，危険を2値の論理変数 $Hs(t) \in \{1,0\}$ で表し，危険であるときを 1，危険でないときを 0 とすれば，時刻 t_s 以降の状態は，危険回避の操作が求められる不安区間 $Ax(t) \in \{1,0\}$（事故の不安を 1，不安なしを 0）と，その後の事故 $Hd(t)$ に分けられる。すなわち危険 $Hs(t)$ は次式で構成される。

$$Hs(t) = Ax(t) \vee Hd(t) \tag{13}$$

さらに危険回避の実行を2値の論理変数 $w_K(t)$ で表し，実行を 1，実行しないを 0 で示すと，危険回避 $w_K(t)$ は，危険であるという判断 $Hs(t_s) = 1$ で開始され，不安区間 $Ax(t)$ で $Hd(t) = 1$ を予測し，その回避のための操作を行うことになる。危険回避 $w_k(t)$ は，不安区間 $Ax(t)$ に対して，少なくとも遅くなること（すなわち事故）があってはならない関係として次式の条件で実行される。

$$Hd(t)(= Ax(t)) \geqq w_k(t) \quad (t = t_s \sim t_0) \tag{14}$$

危険回避 $w_k(t)$ は，例えば，鉄道信号では前方の踏切への接近の判断（$Hs(t_s) = 1$）の下に踏切警報機が人や車の排除を行う操作に相当し，ボイラでは温度や圧力に対する「危険」の判断で燃料供給を停止または減少させて，温度や圧力を下げる操作に相当する。

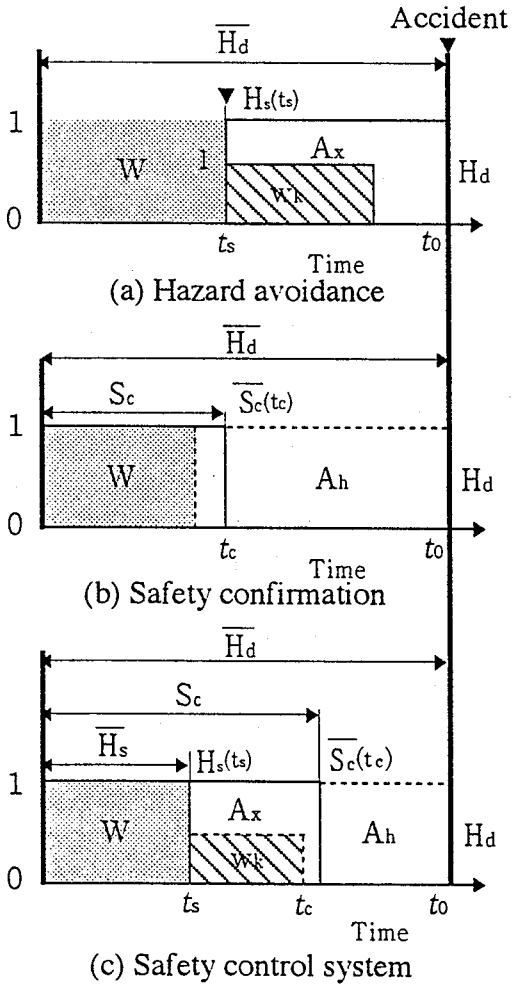


Fig. 3　Safety control system based on accident prediction.
事故の予測に基づく安全制御システム

Table 2 は式 (14) の論理的関係を表す真理値表である。危険の回避は一般に緊急を要し，間に合わないで事故となる場合が多い。さらに，危険であるという判断には，もともと危険を認識できない誤りも起こり得る。その場合には，危険回避を行わないまま危険行為が実行されてしまう。また，もともと，制御による目的の達成は確率的であり，必ず達成されるとは限らない。すなわち，式 (14) の論理不等式は，一方的な要求を示しているだけであって，ユネイトな論理的関係で実現されることを意味していない。よって，危険回避のためには，失敗を考慮してフェールセーフを実現しなければならないことが分かる。

4.2 安全確認に基づく機械の運転

一方，人は通常安全であるとき行動し，安全でないとき行動を控えることによって事故を避けるもう一つの行動様式を持っている。この安全確認に基づく人の行動は **Fig. 3(b)** のように表すことができる。この行動様式は，行動を停止することによって事故防止を実現しようとする点で，前項の制御による危険回避とは根本的に異なる。

Fig. 3(b) のように，事故が生ずるまでは明らかに安全である（真の安全：$\overline{Hd}(t)=1$）が，事故の直前で行動（危険行為）を停止しようとしても間に合わない。そこで，人は，改めて明らかに安全であると考える時刻 t_c を定め，ここを過ぎたら「安全でない」と見なして危険行為を停止するようにしている。この場合，安全であるという判断（以降，単に安全と呼ぶ）を 2 値の論理変数 $Sc(t)$ で表し，安全であるときを 1，安全でないときを 0 とすれば，$\overline{Sc}(t)$ は次式で定義される。

$$\overline{Sc}(t) = Ah(t) \vee Hd(t) \tag{15}$$

ここに 2 値の論理変数 $Ah(t)$ は，事故ではないが安全であることが必ずしも認められない区間として，もう一つの不安を示す。この区間では行動停止が求められることから，ここでは制止（区間）と呼ぶことにし，制止状態を論理値 1，制止でない状態を 0 とする。式 (6) で，安全であるときに危険行為を実行し，少なくとも安全でないときは危険行為を実行しない（停止する）という関係は，危険行為を論理変数 $W(t)$（実行を 1，実行しないを 0）で表せば，次の論理不等式で表される。

$$Sc(t) \geqq W(t) \tag{16}$$

ここで記号 "$\geqq$" は，$Sc(t)=1$ のときは $W(t)$ は 1，0 のいずれでもよいが，$Sc(t)=0$ ときは必ず $W(t)=0$ でなければならない関係として，ユネイトな論理的関係を表し，安全でないときの危険行為の停止は，遅くなる側の誤りは許されないことを意味している。

さらに，安全 $Sc(t)$ はド・モルガンの公式を式 (15) に適用すれば次式で得られる。

$$Sc(t) = Ah(t) \cdot Hd(t) \tag{17}$$

制止区間 $Ah(t)$ はいわゆるブレーキの区間であり，この区間で確実な機械停止を完了するための制動機構が実現されれば次式が得られる。

$$Hd(t) \geqq Sc(t) \tag{18}$$

式 (18) は，安全でない $(Hd(t)=0)$ のに誤って安全 $(Sc(t)=1)$ と判断することだけは許されない論理的関係（ユネイト）として安全の原理[11]（または，安全確認の原理[12]）を示す。また，その真理値表を **Table 3** に示す。ここに，故障時には少なくとも安全という判断を生じない式 (18) の構成は，式 (4) のフェールセーフのもう一つの表現である[6]。

通常，式 (18) の安全 $Sc(t)$ は，安全確認を示す情報（安全情報[12]）として具体的に示される。また，この安全情報 $Sc(t)$ はセンサによって小さなエネルギーで生成され，よって危険行為を実行するためのエネルギーは，

Table 2 Logical relation of hazard avoidance.
危険回避の論理的関係

$\overline{Hd}$	Ax	wk	State of hazard avoidance operation
1	1	1	Hazard recognition and avoidance
1	1	0	Failure in hazard avoidance
1	0	0	Hazardless state
			Failure in recognizing hazard
0	0(1)	0(1)	Accident occurs (1 : no use)

Table 3 Logical relation of princeple of safety ($\overline{Hd} \geqq S_c$).
安全の原理の論理的関係

$\overline{Hd}(t)$	$Sc(t)$	States of safety recognition
1	1	Recognize $\overline{Hd}(t)=1$ as safe.
1	0	Recognize $\overline{Hd}(t)=1$ as unsafe.
0	0	Recognize $\overline{Hd}(t)=0$ as unsafe.
※0	1	Recognize $\overline{Hd}(t)=0$ as safe.

※ Condition "$\overline{Hd} \geqq S_c$" is unsatisfied.

安全情報のエネルギーを増幅（ユネイトな論理的関係を維持）して利用される[7]。この場合，危険行為 $W(t)$ は，安全でないとき（$Sc(t)=0$）は勿論のこと，安全情報 $Sc(t)$ をエネルギーとして伝達（増幅）する過程で故障（式 (17) の $Ah(t)=0$）が発生しても，信号のエネルギーが出力されない側の特性（この故障は安全側故障[12]と呼ばれ，第5章で改めて論ずる）だけが許される。すなわち，式 (18) の安全確認過程では，安全状態 $\overline{Hd}(t)$ が安全情報 $Sc(t)$ として伝達されるが，そのためのセンサ（安全確認手段）の機能を $f(\overline{Hd}) \in 1,0$ で表し，$Hd(t)=1,0$ のときをそれぞれ論理値 1，0 とし，さらに機能 $f(\overline{Hd})$ の動作状態を論理変数 $F^* \in \{1,0\}$ として，正常状態を 1，故障状態を 0 で表せば，式 (17) は一般的に次式で表せる。

$$Sc(t) = \overline{Hd} \cdot F^* \vee \overline{F^*} \cdot \phi d' \tag{19}$$

ただし，ここに2値の論理変数 $\phi d'$ は故障時（$\overline{F^*}=1$）の出力状態であり，出力ありを 1，なしを 0 で表す。式 (18) のユネイトな論理的関係が維持されるには $\phi d'=0$ でなければならない。故障時に $Sc(t)=0$ なる特性は，故障時にエネルギーを出力しない構造として実現される[11]。すでにユネイトな論理的関係（3.2.3 節）で論じたように，安全なとき（$Sc(t)=1$）をエネルギーありとし，安全でないとき（$Sc(t)=0$）は故障時と同じくエネルギーなしとし，エネルギーありに対して安全確認を行えば，故障により誤って安全と判断しない安全の原理（式 (18)）が満たされる。

さらに，式 (16) のエネルギーの出力過程では，出力手段を $E(Sc) \in \{1,0\}$（$Sc(t)=1$ のとき $E(Sc)=1$）とし，$E(Sc)$ の動作状態を改めて $E^* \in \{1,0\}$ で表し，正常状態を 1，故障状態を 0 とおくと，式 (16) の $W(t)$ の実行は次式で表される。

$$W(t) = Sc \cdot E^* \vee \overline{F^*} \cdot \phi e' \tag{20}$$

ここに $\phi e'$ は，故障状態での手段 $E(Sc)$ の出力エネルギーを表す2値の論理変数であり，エネルギー出力ありを 1，なしを 0 としている。式 (20) が式 (16) の関係となるためには，$\phi e'=0$ でなければならない。

一方，手段E（Sc）は，一般に安全情報 $Sc(t)$ を大きなエネルギーに増幅する機能を含んでいる。式 (20) の $\phi e'=0$ は，現実には，故障時（$E^*=1$）に増幅のためのエネルギー源の遮断を求めている。さらに現実的な問題として，すでに式 (12) で示したように，機械的出力をいったん行えば，運動エネルギーが蓄積される。従って，運転中に安全でない状態（$Sc(t)=0$）または故障（$\overline{E^*}=1$）が生じても運動は持続されてしまうと考えるのが妥当である。そのため，$\phi e'=0$ とするには運動エネルギーを消散して機械を停止するための制動機構（ブレーキ）が $Sc(t)=0$ または $E^*=1$ によって起動され，かつ，式 (15) の少なくとも区間 $Ah(t)$ の中で運動エネルギーの消散を完了しなければならない。そのためには，一般にバネリターン型の摩擦ブレーキが利用され[7),13)]，停止時間との関係で区間 $Ah(t)$ が定まると考えてもよい。ここに式 (16)，(18) に基づく機械の運転システムを安全確認システムと呼ぶことにする。

4.3 安全確認に基づく危険回避

すでに述べたように，式 (14) の「危険」という判断で開始される危険回避はあくまでも成功が確率に依存する。それは，危険回避には時間条件が明らかに存在し，いつでも速やかに危険回避を完了できるとは限らないからである。これに対して，式 (16)，(18) のエネルギー遮断（式 (8) の $\overline{E^*} \cdot \xi_S'=0$ には蓄積エネルギーの消散の特性を伴うことはすでに述べた。）による機械停止で実現される事故防止は，有効エネルギーを持たない状態を安全状態とする点で明らかに確定性がある。

しかし，危険回避が必要ないわけではない。これまで，危険回避と停止による事故回避とは区別して検討してきた。実は，人は危険回避をできるだけ行って，どうしても回避できないとき行動を停止するようにしている。そこで，危険回避を積極的に行って安全確認システムの運用をより効率的に行うためのシステムについて改めて検討する。

式 (13) に戻って検討すれば，「危険」の判断 $Hs(t_s)=1$ によって定まる未来の状態は次の3つの区間で表すことができる。

$$Hs(t) = Ax(t) \vee Ah(t) \vee Hd(t) \tag{21}$$

区間 $Ax(t)$ で回避行動を実行するためには，明らかにエネルギーが必要であるが，制止区間 $Ah(t)$ におけるシステムはエネルギーが遮断されている。すなわち，$Ax(t)$ を $Ah(t)$ と同時刻に実行するよう計画しても無意味である。よって次式が成立する。

$$Ah(t) \cdot Ax(t) = 0 \tag{22}$$

従って，式 (21) より $Hs(t)$ は次式のように，互いに共通部分を持たない2つの区間から構成される。

$$Hs(t) = Ax(t) \vee Sc(t) \tag{23}$$

式 (23) の関係を **Fig. 3(c)** に示す。危険の判断 $Hs(t_s)=1$ によって生ずる不安 $Ax(t)$ は，未来の時刻 t_c における $Sc(t_c)=0$ の予測を示し，併せてこれを回避する区間（時間）を規定している。従って，この場合の危険回避 $w_k(t)$ は，不安区間 $Ax(t)$ において $Sc(t_c)=0$

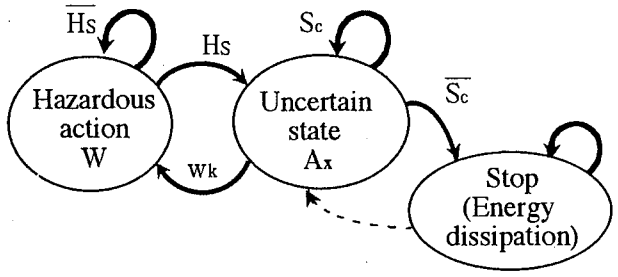


Fig. 4 State transition of safety control system.
安全制御システムの状態遷移図

とならないための操作として次式の条件で実行される。

$$Sc(t) \geqq Ax(t) \geqq w_k(t) \quad (t = t_s \sim t_c) \tag{24}$$

ただし，この場合，$Sc(t_c) = 0$ は式 (16)，(18) による機械の運転停止を意味するから，誤りが許される（ユネイトであることは必ずしも要求されない）。式 (14) における危険回避の目的が式 (24) では明らかに変化していることは特に注意に値する。すなわち，式 (24) は早期に危険回避行動を開始して安全確認を先んじて行うことによって，システムの運転停止をできるだけ回避しようとしている。

さらに，ド・モルガンの公式を用いて式 (23) の否定をとると，次式となる。

$$\overline{Hs}(t) = \overline{Ax}(t) \cdot Sc(t) \tag{25}$$

これにより $\overline{Ax}(t)$ が 1，0 のいずれの場合も明らかに次式が成り立つ。

$$Sc(t) \geqq \overline{Hs}(t) \tag{26}$$

これまで，一般に安全と危険という言葉が曖昧に使用されてきた。本章では，「危険でない」と「安全である」という言葉を区別して扱っている。「危険」はあくまでも危険であるという判断に基づく危険回避（制御）に関連し，一方「安全」は危険行為を許可する目的で，確認すべき状態としての安全を意味する。「危険」と「安全」とは互いに否定の関係として捉えられてきたが，必ずしも論理的否定関係にあるわけではないというのが筆者らの考え方である。式 (26) は，危険であるという判断と安全でないという判断には，時間的な前後関係が存在することを示している。**Fig. 4** は，3 つの制御状態の関係を示す状態遷移図である。すなわち，「危険」という判断でその回避を先んじて行い，それが成功しないとき「安全でない」という判断で運転が停止される関係を意味している。式 (26) は，生産性（稼働率）と安全性（事故防止）の両方を考慮すべき現実の運転システムを論じる上で基礎となる重要な式なので，改めて安全システムの構成原理と呼ぶことにする。

5. 安全確認に対する誤り特性

安全を確認して危険行為を許可する構成と，危険を判断して事故回避の操作を行う構成が，論理的に式 (26) によって与えられることをすでに示した。安全の確認は，一般にセンサによって情報を生成して行う。ここでは，安全確認を行うためのセンサの基本特性を，特に誤り特性の観点から考察する。

事故 $Hd(t) = 1$ と事故でない $Hd(t) = 0$ の設定には誤りがないものとし，式 (19) の特性で示されるセンサを安全 $(Sc = 1)$ と安全でない $(Sc = 0)$ とに分けて考えるものとする。

通常，情報がエネルギーで伝達される系は，故障時にこのエネルギーが伝達されない系として構成することは可能であるが，逆に，故障時にエネルギーを伝達する系を構成することは不可能である。すなわち，式 (19) によるセンサは故障時 $(\overline{F^*} = 1)$ における出力状態を $\phi d' = 0$ として設定できる。センサだけでなく，このように故障時における論理値を 0 として設定できる情報伝達手段をフェールセーフな伝達手段[12]と呼ぶことにする。

式 (15) で示されるセンサがフェールセーフであるとき，センサの特性は次の論理式で示される。

$$Sc = \overline{Hd} \cdot F^* \tag{27}$$

一方，安全でないという判断を行うセンサを Hd を検出するものとする（すなわち，$\overline{Sc} = Hd$）。ここで式 (19) の Sc，$\overline{Hd}$，F^*，$\phi d'$ に関し，論理値 1 側と 0 側の状態を表す論理変数として以下のように定める。

Sc^1，$\overline{Hd}^1$：安全のとき 1，安全でないとき 0
Sc^0，$\overline{Hd}^0$：安全のとき 0，安全でないとき 1
F^{*1}：センサが正常のとき 1，正常でないとき 0
F^{*0}：センサが正常のとき 0，正常でないとき 1
$\phi d'^1$：センサ $f(\overline{Hd})$ の出力状態が安全を示すとき 1，安全でないを示すとき 0
$\phi d'^0$：センサ $f(\overline{Hd})$ の出力状態が安全を示すとき 0，安全でないを示すとき 1

フェールセーフな安全確認手段において 1 側出力の発生と 0 側出力の発生は，上に定めた論理変数を用いて式 (27) と式 (19) から，次のように表される。

$$Sc^1 = \overline{Hd}^1 \cdot F^{*1} \tag{28}$$

$$Sc^0 (= Hs) = \overline{Hd}^0 \cdot F^{*1} \vee F^{*0} \cdot \phi d'^0 \tag{29}$$

式 (28) は，安全 $Sc^1 = 1$ の出力がセンサに依存せず安全状態 $\overline{Hd} = 1$ の設定だけで決定されることを意味す

る。式 (29) の出力 $Sc^0 = 1$ は，センサの故障 $F^{*0} = 1$ における $\phi d'^0 = 1$ に依存する。すなわち，危険状態 $\overline{Hd} = 1$ が直前に存在していたとしても，危険状態は必ずしも認識できない場合がある。ここに，$Sc^0 = 1$ (式 (19) における 0 側出力) がセンサの故障 (故障確率) に依存することは重要な意味を持つ。すなわち，フェールセーフなセンサ (一般に安全確認手段) では，安全であるという判断 ($Sc = 1$) はセンサの構造で決定され，一方，危険の通報はセンサの故障率に依存して，確率的であるということである。危険検出の誤りによる事故の回避のために，式 (26) は，別途フェールセーフな安全確認を必要とすることを主張している。

このように，安全確認手段の出力状態が安全 (論理値 1) と安全でない (論理値 0) とによって故障に対する誤り状態が異なる特性は，非対称故障特性[11]と呼ばれる。式 (19) において，手段 $f(\overline{Hd})$ が故障したとき出力状態 $\phi d' = 1$ の存在する手段，すなわちフェールセーフでない手段では $Sc^1(= 1)$ は次式で表され，確率的である。

$$Sc^1 = \overline{Hd} \cdot F^{*1} \vee F^{*0} \cdot \phi d'^1 \qquad (30)$$

そして，この場合，手段 $f(\overline{Hd})$ の論理値 1 側と 0 側の誤り状態は式 (29), (30) から分かるように対称である。このように論理値 1 側と 0 側の誤り状態が対称に現われる特性は，対称故障特性[11]と呼ばれる。

一般的電子回路 (コンピュータを含む) で実現される安全確認手段は，この対称故障の出力特性を持っている。しかし，例えば小電流を開閉する電磁リレーは，接点溶着がなく非対称故障特性を持つ。ここで，式 (27) で示される論理値 1 側の誤りがない安全確認手段の出力を理想として，式 (15) で示される一般的安全確認手段に対する安全性評価指標として，非対称故障率 η を次式で定義する。

$$\eta = \frac{\text{危険側故障発生確率}}{\text{全故障発生確率} - \text{危険側故障発生確率}} \qquad (31)$$

式 (31) で，危険側故障発生確率とは，安全確認手段の故障により誤って安全 (論理値 1) という信号を出力する確率で，式 (30) の $\phi'^1 = 1$ による $Sc^1 = 1$ の発生確率を意味する。全故障発生確率は，安全確認手段の故障確率であり，したがって，分母は安全側に故障する確率であると考えることができる。ただし，式 (31) は，対称であるとき $\eta = 1$ としている点で，これまで提案された非対称故障率[11]とは異なる点に注意を要する。

6. 人間機械系における安全作業

6.1 安全作業の論理構成

さらにここでは，人と機械とが共同作業を行う場合の安全の条件が，同様にユネイトな論理的関係で表されることを示す。

作業空間を 3 つに分けて考える。**Fig. 5** に示すように安全空間 S と危険空間 H の 2 つの空間を 1 人の作業者が移動するものとする。但し，作業者は 2 つの空間 S と H にまたがって存在し得ないものとする。空間 U は空間 S でも空間 H でもない不安空間を示す。ここで，**Fig. 5** の危険空間 H において，作業者と機械が衝突すること (事故) なしに作業を行うための条件について考える。

危険空間 H で作業者と機械が衝突しないということは，両者が同時に危険空間 H に存在しないということである。すなわち，機械が危険空間 H で作業するときを mh として次のように表すとき，安全の条件は次式で示される。

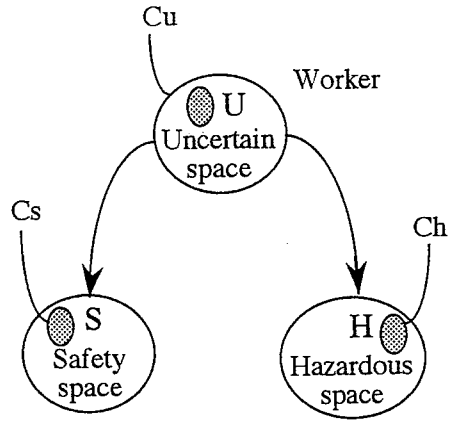


Fig. 5　Human operation in safe space and hazardous spase.
安全空間と危険空間における人の作業

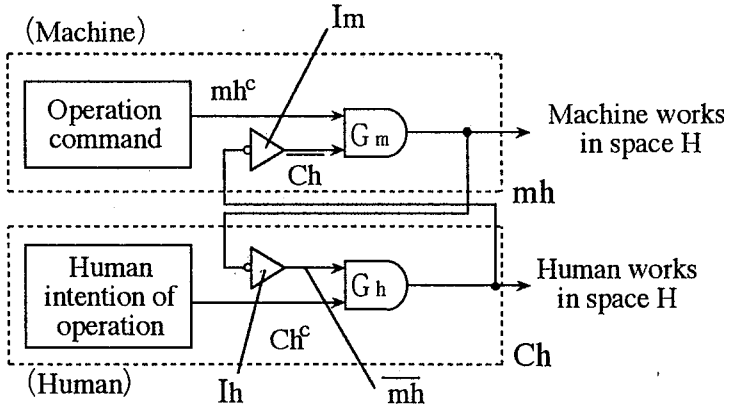


Fig. 6　Two kinds of interlocking in man-machine system.
人間機械系における 2 つのインターロック

$$Ch \cdot mh = 0 \tag{32}$$

ただし，論理変数は次のような意味を持つ。

$Cs = 1$…安全空間 S に作業者がいる
　　0…安全空間 S に作業者がいない
$Ch = 1$…危険空間 H に作業者がいる
　　0…危険空間 H に作業者がいない
$mh = 1$…危険空間 H で機械が作業をしている
　　0…危険空間 H で機械が作業をしていない

式 (32) は，a) 作業者が危険空間 Hで作業を行っている $(Ch = 1)$ ときは，この空間 Hで機械は作業をしていない $(mh = 0)$ か，b) 機械が危険空間 Hで作業を行っている $(mh = 1)$ ときは，この空間 Hに作業者はいない $(Ch = 0)$，あるいは，c) 機械は作業しない $(mh = 0)$ で作業者もいない $(Ch = 0)$，これら 3 つ状態のいずれかであれば安全が確保できることを意味している。

式 (32) が満たされるような作業システムは次のようになる。作業者は機械が作業を行っていないとき（すなわち，$\overline{mh} = 1$ のとき）作業を行えばよく，これは次式で示される。

$$Ch \cdot mh = 1$$

しかし，機械が作業を行っていないからといって，必ずしも作業者は危険空間 Hで作業を行う必要はないから，厳密には，$mh \geqq Ch$ と表現できる。このことは，空間 Hに機械がいない状態 mh と作業者の作業の実行 Ch の間にはユネイトな関係が成立することを意味する。さらに，このユネイトな関係は，Ch^Cを人間の作業の意志とすれば，次式で表せる。

$$Ch = mh \cdot Ch^C \tag{33}$$

また，機械は作業者が危険空間 H に存在しないとき（すなわち，$\overline{Ch} = 1$ のとき）作業を行えばよく，これは次式で示される。

$$mh \cdot \overline{Ch} = 1$$

これは，厳密にはユネイトな関係$\overline{Ch} \geqq mh$ で示され，よって，次式が成立する。

$$mh = \overline{Ch} \cdot mh^C \tag{34}$$

ここに，mh^Cは機械の動作指令である。式 (33) は人間側インターロック，式 (34) は機械側インターロックと呼ばれる[12]。式 (33)，(34) は，未来に起こる事故 $(mh \cdot Ch = 1)$ がない条件で，それぞれ仕事 Ch，mh を行う構造である。

Fig. 6 は式 (33)，(34) で示されるインターロックをフリップフロップモデルで示している。**Fig. 6** において否定演算記号で示される Im，Ih は機械側と人間側に備えられるセンサを意味し，Ih は，例えば作業者の目である。AND ゲート Gm は式 (34) に基づいて作業者が危険空間 Hに存在しない条件で機械側命令を伝達するための判断要素，Gh は式 (33) に基づいて機械が危険空間 Hで作業していない条件で作業者が空間 Hに進入するための判断要素である。例えば，プレス機械では，作業者の手がボルスタ（危険空間）上にないことが光線式センサで示され，さらに，運転ボタン ON によって明らかに手が安全な空間に戻ったことが示されて初めて機械（スライド）が降下する。この場合，**Fig. 6** の Im は光線式センサ出力であって，人間の手がないという判断結果を示すから，故障で誤って手があるにもかかわらず，手がないと判断することだけは許されないフェールセーフな特性が求められる。

6.2 安全監視のためのセンサ[14),15)]

ある空間が安全であるためには，その空間が安全情報生成のためのエネルギー源の役割をなしている。例えば，家庭の湯沸し器の安全システムなどに利用される熱電対は，炎があることを安全状態とし，蓄熱状態（炎）から安全情報を得るセンサである。このように，検出対象の持つ磁気や熱，光等のエネルギーが直接トランスデューサの出力となるセンサは，3.2.3 節で述べた直動型センサである[10]。**Fig. 1(b)** に示したように，空間の安全状態がエネルギーの蓄積状態として与えられる例はむしろ希である。これに対して，情報を抽出するために予

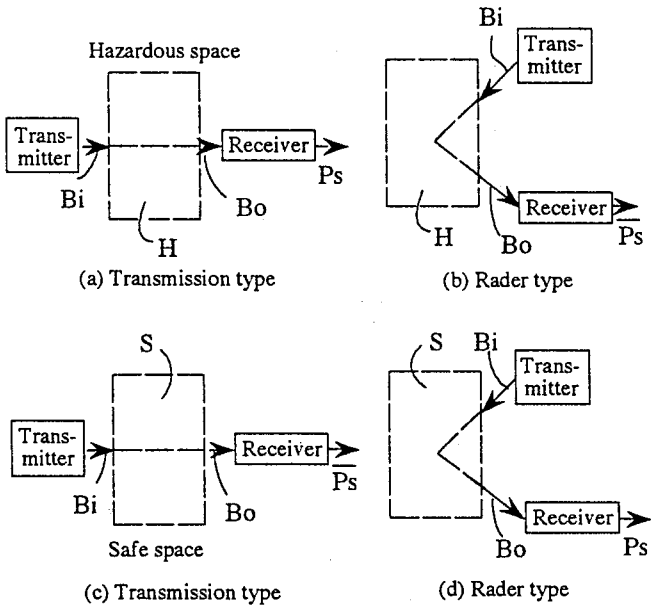


Fig. 7　Observation of work space by photo-electric sensor.
光センサによる空間監視の方法

めエネルギーを輻射し，トランスデューサは検出すべき情報をこの輻射エネルギーの変調信号（on/off のスイッチ信号を含む）として生成するセンサ構成はすでに述べた変調変換型である[10]。

さらに，変調変換型のセンサにおける情報の生成方法には，エネルギービーム透過型とレーダ型とがある。**Fig. 7(a)** 及び (c) は光センサを用いたエネルギービーム透過型センサを示す。空間 Hもしくは Sに光ビーム Bi が入射され，この透過光 Bo が受光器で受信される。同図 (b)，(d) は光センサを用いたレーダ型センサを示す。空間 Hもしくは Sに光ビーム Bi が入射され，反射光 Bo が受光器で受信される。ここで，Hは危険空間を，Sは安全空間を意味し，Ps はセンサの出力信号を表す。ただし，$Ps=1$ のとき「安全」，$Ps=0$ のとき「安全でない」の判断結果を示す。また，$\overline{Ps}$は Ps の否定信号を示す。**Fig. 7** で空間 H もしくは S から受信される光ビーム Bo に着目し，空間を監視するためのセンサ構成の特性を考察する（受光器は常に正常に動作して光ビーム Bo が受信されれば必ず出力信号 Ps もしくは$\overline{Ps}$を生成するものと仮定する）。まず，**Fig. 7(a)**，**(b)** で危険空間 Hにおける作業者の存在を検出する場合を考える。同図 (a) では光ビーム Bo が受信されないときは，$Ps=0$（危険）を示すことができる。この事象を論理的に表現すれば次のようになる。受光器で受信される光ビーム Bo を 2 値の論理変数として扱って，1 を光ビームあり（$Ps=1$ あるいは$\overline{Ps}=0$ を出力する），0 を光ビームなし（$Ps=0$ あるいは$\overline{Ps}=1$ を出力する）とすれば，空間 Hにおける作業者の存在に対して，次式が成立する。ただし，Ch は危険空間 Hに人がいることを示し，1 のとき存在，0 のとき不在を示す。

$$\overline{Ch} \geqq Bo \tag{35}$$

Table 4 に式 (35) の真理値表を示す。すなわち，作業者がいないときに ($Ch=1$) 安全でないことを示す信号 $Bo=0$ を生じてもよいが，作業者が空間 H にいるときに ($\overline{Ch}=0$) 誤って安全を示す信号 $Bo=1$ を生じるようなことがない特性として，ユネイトな論理的関係を示している。

式 (35) の場合，空間のエネルギー蓄積状態は予めエネルギービーム Bi で作られる。これは，人がいない（安全）ことで危険空間に流入するエネルギーのエネルギー源と見なすことができ，したがって，出力 Bo のエネルギー蓄積状態を改めて Bo で表すと，式 (10) の一般的特性によって次式が成立している。

$$Bo = Bi \cdot (\overline{Ch} \cdot e^{*}) \vee \overline{e^{*}} \cdot \xi_{S}' \tag{35'}$$

ここに，安全を示す空間のエネルギー ($Bi \cdot \overline{Ch}$) が正常に生成されるとき $Bo=1$ であり，故障は光エネルギー遮断状態となり，$\xi_S'=0$ である。

一方，**Fig. 7(b)** では投光器が故障した場合や，光ビーム Bi が障害物で遮られてしまった場合には，たとえ空間 Hに作業者がいても反射光 Bo を生じない。すなわち，論理的には **Table 5** で示すように，空間 Hにおける作業者の存在 Ch と受信される信号 Bo の間に，$Ch=1$，$\overline{Bo}=1$ を生じるような組み合わせが存在することになる。よって，信号 $Ps=1$ を与えるセンサは，エネルギービーム透過型センサでなければならないと考える。

Fig. 7(c)，**(d)** は同図 (a)，(b) の空間を安全空間 S に置き換えた場合である。同図 (c) では，作業者が空間 Sに存在しない場合でも，光ビーム Bi が障害物で遮られると作業者の存在を示す信号 $Bo=0$ が生じる。一方，同図 (d) では作業者が空間 Sに存在するにもかかわらず光ビーム Bi が障害物で遮られて不在を示す信号 $Bo=0$ が生じることはあっても，作業者が空間 S に存在しないときに反射光 $Bo=1$ を生じることがない。したがって，同図 (d) では，Cs を，安全空間に人がいることを示すものとし，存在を 1，不在を 0 で表すものとすると，式 (35) と同様に空間 Sにおける作業者の存在／不在（Cs）に対して次式が成立する（同図 (c) ではこの不等式が成立しない）。

Table 4　Trueth value (1).
真理値表 (1)　($\overline{Ch} \geqq Bo$)

$\overline{Ch}$	Bo
1 (Absent)	1 (Safe)
1 (Absent)	0 (Hazardous)
0 (Present)	0 (Hazardous)

Table 5　Trueth value (2).
真理値表 (2)　($Ch \geqq \overline{Bo}$)

Ch	$\overline{Bo}$
1 (Present)	0 (Hazardous)
※1 (Present)	1 (safe)
0 (Absent)	0 (Hazardous)
0 (Absent)	1 (Safe)

※ danger side of errors

$$Cs \geqq Bo \tag{36}$$

式(36)のエネルギー蓄積状態は，人が安全空間に入ったときのみ作られ，このエネルギーは，反射型の光センサによって生成される。よって，変数を式(35')と同様の定義で用いると，式(36)で示されるユネイトな論理的関係は次式となる。

$$Bo = Bi \cdot (Cs \cdot e^*) \vee \overline{e^*} \cdot \xi_S' \tag{36'}$$

入力の光ビームの正常性を $e*$に含めるとすれば，式(36')は次式となる。

$$Bo = Cs \cdot e^* \tag{37}$$

このように非対称特性の観点から，危険空間を監視するセンサは，式(35)に基づく構成でなければならない。一方，運転スイッチONの信号は，作業者の存在がエネルギービームとして発生する構成（式(36)に基づく信号）でなければならず，接点であればA接点（作業者が押したときに電極が閉じる接点）でなければならない。

7. 結　言

これまで，人は，多くの経験から事故を予測して回避する方法を発展させてきた。しかし，この方法は，予測の失敗または回避の失敗がそのまま事故につながるという致命的な欠点をはらんでおり，現に，このような失敗で多くの事故がすでに経験されてきている。

安全について，これまで論理的な考察が十分になされないまま主観的に語られてきている。すでに，人は多くの事故を経験して，行動様式（システム）の中で安全を実現してきている。すなわち，帰納・演繹としての人の持つ基本的認識形式（科学）がとられてきており，「安全」が学問として成立するはずである。

事故の経験は許容できない。事故を生じないための安全は論理的に証明せざるを得ない。ただし，失敗（機械の故障や人間のミス）を認めた上で事故防止を果たすには，常時安全が確認されなければならない。したがって，安全工学は安全を示す情報の生成から機械的操作（すなわち制御）に至るまでの一貫した論議が必要であって，信頼度の数値評価だけで論じられるべきではない。このことを論理的に示したのが本論文である。

エネルギーを持つ系（機械系）と人とが安全な共同作業を行う場合の構成条件として，安全を示す情報（安全情報）の生成からそれがエネルギーを伴って出力されるまで，一貫してユネイトに伝達されねばならない。ただし，ここで「ユネイト」の用語を用いるとかえって混乱をまねくおそれがある。しかし，確認（確定論）に基づく安全が，信頼性（確率論）に基づくこれまでの安全とは根本的に異なることを明らかにする必要があり，そのための表現方法として，論理数学で使用される「ユネイト」が内容を最も端的に表すと判断し，本報では，敢えて翻訳せず，ユネイトをそのまま用いることにした。

安全情報の生成から機械のエネルギー出力に至るユネイトな伝達過程（安全確認の原理）をまず論理的に明らかにし，ここに，ユネイトな論理的関係として求められる0側誤り特性が，現実には故障時に出力を生じない構造とすべきこと，また，この構造は，故障によって熱力学系の孤立で定まるエネルギーの消散過程を利用する以外には実現できないことを示した。このように，本報によって，ユネイトな論理的関係が安全システムの構成条件の基礎を与えるばかりでなく，その実現方法が明かとなったと考える。

安全は多様であると言われる。本論文では，例として制御に基づく安全に限定して論じている。安全が多様であるとすれば，多様な安全に対して幾つかの基礎的な原理が示されなければならない。本報では，その原理の一つとして式(18)を示した。この原理が広く一般的な安全に適用できることを今後も示して行きたい。

参考文献

1) 向殿，C型 Fail-safe 論理の数学的構造について，信学論，Vol. 52-C, (1969) 883-889.
2) H. Mine, Y. koga: Basic Properties and a Construction Method for Fail-safe Logical Systems, IEEE Trans. on Electronic Computers, Vol. EC-16, No.3 (1967).
3) 土屋，フェールセーフ論理方式の研究，電気試験所研究報告，No.695 (1961).
4) 産業安全研究所特別研究報告：機械の安全化のための計測技術に関する特別研究，RIIS-SRR-86(1986).
5) 杉本，粂川，他，安全確認型安全の基本構造ー安全確認構造の条件についてー，機論(C)，Vol. 54, No. 505 (1988) 2248-2292.
6) 杉本，蓬原，フェールセーフ技術とフォールトトレランス，第19回FTC研究会資料集 (1991) 1-12.
7) 杉本，蓬原，安全制御系における安全情報のエネルギー伝達，機論(C)，Vol. 56, No. 530 (1990) 2653-2665.
8) 杉本，蓬原，安全立証の基本的考え方，信学会，安全確保時限研究会報告 S-93-1 (1993) 1-6.
9) 杉本，蓬原，ロボットにおける安全確認システムの構成，情報処理，29-2 (1988).
10) 岡村，寺尾，岩波講座基礎工学II（測定論），岩波書店 (1969).

11) 杉本，蓬原，安全の原理，機論 (C)，Vol. 56, No. 530 (1990) 2601-2609.
12) 杉本，蓬原，向殿，安全作業システムの原理とその論理的構造，電学論 D，Vol. 107, No. 9 (1987).
13) 蓬原，杉本，安全確認作業システムの論理的考察，機論 (C)，Vol. 56 , No. 529 (1990) 2378-2385.
14) 蓬原，杉本，向殿，安全制御のためのセンサ構成，第1回ロボットセンサシンポジウム，(1988) 127-132.
15) 浅田，蓬原，竹村，向殿，杉本，プレス機械の安全制御用光センサデバイスの開発，平2電学産業応用部門 (1990) 158.

(平成8年5月10日受理)