Research Reports of the Research Institute
of Industrial Safety, RIIS-SRR-90, 1990

2. 安全の基本原理と安全制御技術

杉本 旭*, 深谷 潔*

2. Safety Control Technology Based on the Principles of Safety

by Noboru SUGIMOTO* and Kiyoshi FUKAYA*

Abstract: On the basis of probability, in which accidents are recognized as an unavoidable happening, 'safety' cannot be logically discussed and developed. In this report, logical safety is approached.

As safety goes with the information indicating the 'safety', the condition for constructing any reasonable safety operation system is that the information (safety information) must be transmitted 'unate'. This means that the extraction of safety information demands the introduction of the threshold logic into the operational space. In this report, the safety condition is logically defined in an operation requiring safety, and the definition of 'safety control system' is presented on the basis of the condition securing the safe operation.

In the defined safety control system, interlocking as a fundamental element is logically developed under an energy transmitting model of interlocking. The model defines the condition of output signal in the interlocking. The interlocking indicates the truth that a practical safety system composes a phased structure, consists of a system in which safety information is transmitted 'unate', and a system in which the safety information is not necessarily transmitted.

Key Words: Safety, Safety System, Safety Control, Safety Control System, Interlocking, Fail-Safe, Energy Transmitting

2.1 はじめに

ここで安全の基本について考える前に，これまで安全について論理的な考察がなされないままに，多くの主観的な安全が語られ，安全対策を講じようとする側の人達をいかに混迷させてきたかについて触れておきたい。危険は必ず事故にいたってはじめて分かる宿命を持つが，人間は長い歴史をもって，すでに多くの事故や災害を経験し，安全が危険とは同時に起こりえないものとして論理的に創造しうることを知っている。すなわち，本来，人間は多くの経験を基に危険を確認し，いまだ起こっていない危険を予測して安全を確保しようとする特性を持っている。しかも，この特性，すなわち，帰納・演繹として人間の持つ基本的認識形式は科学そのものであり，これに従えば，「安全」は科学に基づく学問として成立するはずである。もし，論理的展開ができないならば勉強不足の誹りを免れえない。

科学として「安全」を追求する場合，まず先に「危険」が確認され（帰納論的），「安全」は「危険」の否定として演繹化の過程を伴うが，「安全」のこれまでの論理性欠如の理由，いい換えれば，科学として「安全」が成立しなかった最大の理由は，その否定の概念

*機械研究部，Mechanical Safety Research Division

が演繹された「安全」を導出していないことである。すなわち，事故の発生の可能性を確率で示し，発生確率が大きいときを「危険」，そして発生確率が小さいときを「安全」と定義しても，「危険」の否定としての演繹化された「安全」とは決してなりえない。

人間はすでにエネルギと共に危険（事故発生）の能力をも獲得した。このことは確率論によって扱われる以前に事実である。人間はこの危険なエネルギを出力する前に危険でないことを確認し，事故が確率的に生じない事実に基づいて制御されねばならない。すなわち，確率的に生ずる危険に対して，確率的に生じない状態を構成する秩序系として演繹されるとき，科学としての「安全」を生ずるということである。ただし，危険でないことの予測が「安全です」という情報に基づくことから，安全は情報として生ずる特性を持っている。したがって，安全工学は情報の発生形態と処理形態の両方から論じられるべきで，信頼度の数値評価だけで論じられるべきではない。

人間と機械の間で安全な作業が実行されるシステムが基本的には安全を論理的に追及する対象である。これまで，この安全作業システムの構成条件として機械側の危険なエネルギはいつでも出力できるわけではなく，安全を示す情報（安全情報）に基づくべきものであることとし，これが基本的にはフェールセーフとインタロックという 2 つの技術によって達成できることが，すでに著者らによって示された[1)]。ここでは，具体的作業システムにおける安全情報の抽出から安全確保のための制御まで一貫した論理的考察を行う。このため，まず本章第 2.2 節で，安全を必要とする作業系の安全状態を論理的に定め，ここで安全作業が行われるための条件に基づいてエネルギ出力を制御するシステムを安全制御系として定義する。次に，第 2.3 節では，上で定義した安全制御で必要とする基本要素としてインタロックを示し，このインタロックの論理展開に出力発生のためのエネルギを導入する。この結果，安全制御系の構成条件をエネルギ伝達系として実用的モデルで表現できることを示す。すなわち，実用的な制御系は，安全情報が故障時伝達されない特性（論理的にはユネイトな伝達と呼ばれる）を持つ系（安全装置）と，必ずしも制御情報がユネイトに伝達されない系の階層構造で表現できることを示す。第 2.4 節では，機械系を含む安全情報伝達手段と安全情報抽出手段に関して情報伝達および抽出に関する論理的考察を行い，異常時を含むこれらの手段のエネルギ伝達特性が共に上に示したインタロックモデルを使って論理的に表現できることを示す。

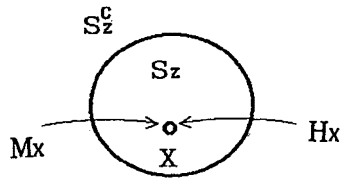


Fig. 2.1　Hazard area and safety area.
危険領域と安全領域

2.2　安全作業の論理的考察と安全制御

Fig. 2.1 において，機械の可動部が作業する領域を Sz とし，これを危険領域と定め，それ以外の領域を安全領域 Sz^c とする。いま，作業領域 Sz 内に点 X をとり，点 X に作業者が存在することを Hx，機械の可動部（例えばロボットのアーム）が存在することを Mx で表す。ただし，存在するときを論理値 1，存在しないときを論理値 0 とする 2 値変数とする。事故は両者が同時に点 X に存在するときに起こるから，これは $Hx \cdot Mx = 1$ と表せる。また，両者の存在を時間の関数として $Hx(t)$, $Mx(t)$ で表すと，安全作業は人間と機械可動部が交代に作業すること，すなわち，次式が常に成立していなければならない。

$$Hx(t) \cdot Mx(t) = 0 \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}1)$$

すなわち，空間の状況として，安全状態を 0，事故状態を 1 とする 2 値の論理変数 Dx で表せば，空間の状態 Dx は次式で表すことができる。

$$Dx = Hx(t) \cdot Mx(t) \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}2)$$

少なくとも式 (2-1) の条件を満たしつつ作業が行われるためには，機械側の作業は人間が存在しないこと $\overline{Hx}$ を，また人間の側の作業は機械の可動部が存在しないこと $\overline{Mx}$ を安全条件とすればよい。よって相互の具体的作業条件が次の 2 つの式で示される。

$$\overline{Hx} \cdot Mx = 1 \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}3)$$

$$Hx \cdot \overline{Mx} = 1 \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}4)$$

ここに $\overline{Hx}$, $\overline{Mx}$ はおのおの 2 値で表される作業 Hx, Mx の否定を示す論理変数である。

式 (2-3) は機械側の作業条件を $C_M(t) \in \{1, 0\}$ で表し，機械側可動部が作業領域に進入しているとき

を1，していないときを0で表すものとすると，式(2-3)に対応する機械側の操作の結果として，C_Mは次式となる。

$$C_M = \overline{H}x \cdot Mx \cdots\cdots (2\text{-}5)$$

もし，人間側の行動を制御系出力とみなして，人間の行動の結果を$C_H \in \{1,0\}$で表し，式(2-5)と同様に表現するならば，式(2-4)に対応する制御系出力の結果として$C_H = Hx \cdot \overline{M}x$で表すことができる。ここに，危険を伴う作業が安全の条件に基づいて行われる機械操作，すなわち，式(2-5)の出力状態を生成する操作を安全制御と呼ぶものとする。制御とは，「ある目的に適合するように対象となっているものに所要の操作を加えること」と定義される。ここでは，式(2-2)で示される空間の状態を安全($Dx = 0$)に保つために，式(2-5)の論理式に基づいて行われる制御を安全制御と定義する。

また，式(2-3)，(2-4)は点Xに人間も機械の可動部も存在しない場合があるから，厳密には，少なくとも作業Mxは$\overline{H}x = 0$のとき$Mx = 1$（またはHxは$\overline{M}x = 0$のとき，$Hx = 1$）であってはならない関係として次式で表せる。

$$\overline{H}x \geqq Mx \cdots\cdots (2\text{-}6)$$

$$\overline{M}x \geqq Hx \cdots\cdots (2\text{-}7)$$

例えば，式(2-6)は，人がいなければ($\overline{H}x = 1$)必ずしも機械出力を生ずるとは限らない($Mx = 1,\ 0$)が，機械出力を生ずる場合は($Mx = 1$)必ず人はいないことが保証されねばならない($\overline{H}x = 1$)関係を示している。これは$\overline{H}x = 0$のとき$Mx = 1$には決して誤ってはならないことを意味し，このような論理的関係をユネイトな関係と呼ぶ。そして，上の2つのユネイトな関係は作業空間Szのすべての点で成立する。

Fig. 2.2に前述の条件(2-3)，(2-4)を満足する人間機械系のモデルを示す。同図で$\widehat{H}x(t)$は人間の作業意志を，$\widehat{M}x(t)$は機械側の作業命令を示す。G_Hは人間側のインタロックを実現する論理積演算要素である。これは機械の可動部がSzに存在しないこと$\overline{M}x(t)$をセンサ（例えば目I_H）で検出し，このセンサ出力と作業意志$\widehat{H}x(t)$に対して式(2-4)に対応する演算を行っている。この出力信号は人間の作業を示す条件を与えている。また，G_Mは機械側インタロックの論理積演算要素である。これは，人間がSzにいないこと$\overline{H}x(t)$をセンサI_Mで検出し，センサ出力と作業命令$\widehat{M}x(t)$に対して式(2-3)に対応する演算を行っている。すなわち，おのおの$\overline{H}x(t)\cdot\widehat{M}x(t) = Mx(t)$，$\widehat{H}x(t)\cdot\overline{M}x(t) = Hx(t)$の論理処理を行っている。そして，運転出力$Mx(t)$によって，機械側可動部が$Sz$に進入することになる。

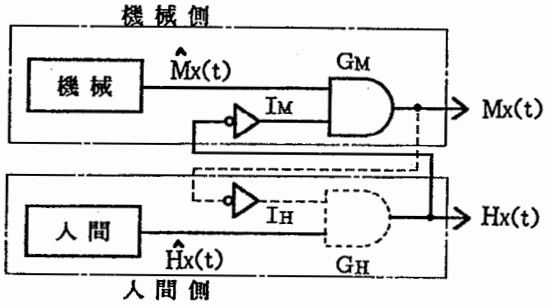


Fig. 2.2　Operation model of man-machine system.
人間機械系の作業モデル

ここで，Fig. 2.2のシステムは少なくとも人間がいないとき作業$Mx(t)$が実行され，また，少なくとも機械側作業$Mx(t)$が出力されていないとき，人間側の作業$Hx(t)$が実行される。したがって，センサI_MおよびI_Hにはおのおの誤って機械側作業命令$\widehat{M}x(t)$，および人間の作業意志を許可する誤り（すなわち，センサ出力が論理値1となる誤り）が許されない。また論理積要素G_M，G_HもおのおのセンサI_M，I_Hから許可の情報がないのに誤って（勝手に），作業出力$Mx(t)$または人間の作業$Hx(t)$を発生しない特性を持たねばならない。一方，センサI_M, I_Hおよび論理積演算要素G_M, G_Hが上の特性を持てば，例え機械側作業命令$\widehat{M}x(t)$または人間の作業意志が誤って発生しても，センサI_MまたはI_Hが危険を示すとき出力$Mx(t) = 1$または$Hx(t) = 1$は発生しない。さらに，センサI_MまたはI_Hが許可するとき，例え誤りの出力$Mx(t)$, $Hx(t)$が生じてもかまわない。すなわち，安全状態がセンサから示されているとき，誤りの出力$Mx(t) = 1$（または$Hx(t) = 1$）を許すシステムである。ここで，センサI_M, I_Hと論理積演算要素G_M, G_Hには論理値1側の誤りが許されない。すなわち，フェールセーフな特性が要求される。したがって，物理的にセンサや論理積演算要素はフェールセーフに構成できるが，現実にはセンサI_Hと論理積演算要素G_Hは人間の判断によるものであるから，上述のフェールセールな特性を有しない。

従来，ヒューマン・ファクタに基づく人間側インタ

ロックを安全条件とするシステムがややもすると安易に採用されてきている。しかし，論理的にはこれは誤りで，安全作業システムは以下の条件を不可欠とする。

(1) 人間がいない（一般には危険状態でない）ときのみ機械側は危険作業$Mx(t)$を実行できる。

(2) 機械側は誤って危険作業$Mx(t)$を行ってはならない。すなわちフェールセーフであること。

2.3 インタロックモデル

Fig. 2.2 の人間機械システムは，相互に機械側または人間側作業出力がないことを検出するセンサと，このセンサ出力の許可に基づき作業実行の出力を発生する判断要素としての論理積演算要素とから構成される。さらに，機械側作業条件について考えると，一般的には機械側作業命令$\widehat{M}x(t)$自体も人間（またはソフト）によって与えられ，これは誤りを含むと考えねばならない。したがって，安全作業の条件は少なくとも人間（危険）が存在するとき機械側は作業しない（人間がいないとき機械側誤りを許す）構成としてFig. 2.3 の基本インタロックで表すことができる。

Fig. 2.3 で，L は安全を示す情報である（安全を1，危険を 0 とする）。Fig. 2.3 の構成で入力情報LとセンサSの出力I_Sと論理積演算要素G の実行出力Mx の間には，少なくとも$L=0$ の時$I_S=1$, または$I_S=0$ の時$Mx=1$ の発生を許さない関係として次の（ユネイトな）関係が成立しなければならない。

$$L \geqq I_S \geqq Mx \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}8)$$

一方，命令$\widehat{M}x$ と実行出力Mx の間には必ずしもユネイトな関係，すなわち，$\widehat{M}x \geqq Mx$ が要求されていない。しかし，一般的には論理積演算要素G はフェールセーフな特性で実現すればよく，センサと論理積演算要素G の動作状態を 2 値の論理変数S^*, G^*で表せば，実行出力Mx は次式で示されるフェールセーフシステムであればよい（S^*, G^*は正常時を 1，故障時を 0 とし，以降 $*$ 印は共通して動作状態を意味するものとする）。

$$Mx = L \cdot \widehat{M}x \cdot S^* \cdot G^* \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}9)$$

式 (2-9) はフェールセーフシステムとして，論理積演算要素および，センサが正常，すなわち，$G^*=S^*=1$ の時のみ演算出力$Mx = L \cdot \widehat{M}x$ が発生するという情報の論理的関係を意味する。そして，$\widehat{M}x$ には 1 にも

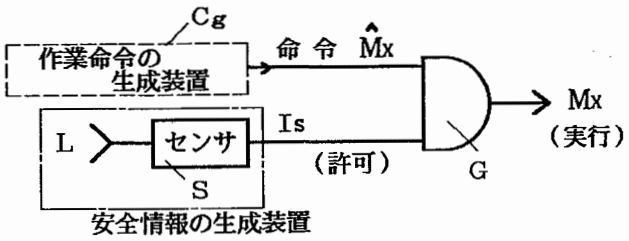


Fig. 2.3　Structure of interlocking.
基本インタロックの構成

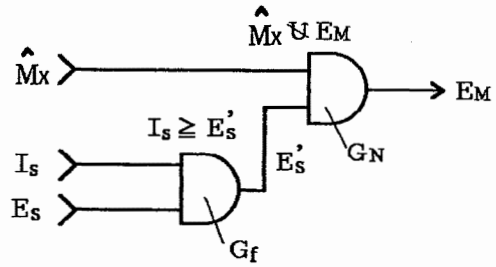


Fig. 2.4　Interlocking with consideration of power supply.
エネルギ供給を考慮した基本インタロック

0 にも誤りが許されるが，命令$\widehat{M}x$ に許可を与える情報$I_S = L \cdot S^*$には$I_S=1$ の側の誤りが許されない。

式 (2-9) は，作業実行出力Mx の論理的発生条件を示すが，このエネルギがどこで発生するか明らかにしていない。現実に，Fig. 2.3 のインタロックにおける実行出力Mx にはエネルギを伴う。Fig. 2.4 は実行のためのエネルギ供給を含む基本インタロックを示す。ここに，機械的出力エネルギの供給の有無とこの論理的出力条件をおのおの論理変数E_S, $E_M \in \{1,0\}$（1：有り，0：無し）で表せば，実際の論理出力E_Mは，外部から供給されるエネルギが許可なく出力されることだけは許されない論理的構成として，次式で与えられる（$\vee$は論理和記号）。

$$E_M = E'_S \cdot (\widehat{M}x \cdot G^*_N \vee \overline{G}^*_N \cdot Mx') \cdots\cdots (2\text{-}10)$$

ただし，$E'_S = E_S \cdot I_S \cdot G^*_f$である。Fig. 2.4 は式 (2-10) をインタロックモデルで表しており，G_fは論理積$E_S \cdot I_S$を行うための論理積要素，G_Nは論理積$E_S \cdot I_S$の演算結果(E'_S) と命令$\widehat{M}x$ の論理積演算を行うための論理積要素である。さらに，G^*_f, $G^*_N \in \{1,0\}$ はおのおの論理積演算要素G_f, G_Nの動作状態を表す論理変数，$\overline{G}^*_N$は動作状態の否定を表す論理変数，$Mx' \in \{1,0\}$ は論理積演算要素G_Nの故障時（$G^*_N=0$, $\overline{G}^*_N=1$ の時）の出力状態をあらわす。

式 (2-10) は論理積演算要素G_fとG_Nが正常($G_f^*=1$, $G_N^*=1$) の時$E_M=E_S\cdot I_S\cdot \widehat{M}x$ の論理出力となり，論理積演算要素G_Nだけが故障した時，$E_M=E_S\cdot I_S\cdot Mx' \triangleq Mx'$として$E_S\cdot I_S$に無関係に出力が定まることを意味している。Fig. 2.4 のインタロックモデルで作業命令 $\widehat{M}x$ と出力状態 E_M の間には必ずしもユネイトな論理的関係を有する必要がなく ($\widehat{M}x \Psi E_M$で表す[1])，論理積演算要素 G_N は故障時の出力状態が $E_M=0$ となるフェールセーフな特性を有する必要がない。しかし，論理積演算要素 G_f は許可 $I_S=1$ がない限り外部エネルギ E_S を供給することは決してしないばかりでなく，論理積演算要素自ら故障で出力 $E_S'=1$ を発生してはならない特性，すなわちフェールセーフな特性を有しなければならない。ここに，出力エネルギ E_S' は，外来する雑音に対しても許可 $I_S=1$ を与える条件 $L=1$ がない限り発生してはならないことを意味する。そして，Fig. 2.3 に示す安全情報発生源を含む論理積演算要素 G_f は設備としてのいわゆる安全装置と呼ぶことができ，例えば，プレーカやプレス機械におけるオーバーラン監視装置，あるいは光線式安全装置が該当する。また，Fig. 2.4 のモデルで示される実用システムは，論理積演算要素 G_N を用いて制御を行う命令発生源が例えばファジー制御，フェールソフト等の機能を持つコントローラでよく，これは，正常時論理積演算要素 G_f を用いて高度な制御を行いつつ，異常時論理積演算要素 G_N によって安全が保証される階層構成系を意味している。

2.4 インタロックにおける情報の処理形態

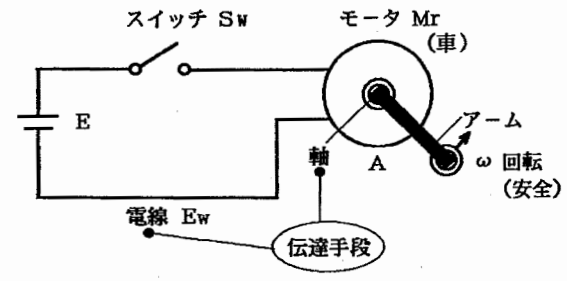
2.4.1 フェールセーフ・システム

Fig. 2.4 の基本インタロックは，$I_S \geqq Mx$ としてユネイトに情報が伝達される系と，作業命令発生から具体的作業実行のシステム発生まで命令が必ずしもユネイトに伝達されない系 ($\widehat{M}x \Psi Mx$, すなわち出力に$Mx=1$ の危険側誤りを含む系) とから構成される。情報がユネイトに伝達される系は，出力の誤り (すなわち，出力非遮断の誤り) を許さない系として，後述するように外部 (環境) エネルギより高いエネルギレベルで伝達される一方，出力非遮断の誤りを許す系は雑音や故障によって外部エネルギが直接出力されてよく，通常，電位 (通常の電子回路やマイクロプロセッサは故障時電源電位の誤り出力を発生する) や力，圧力 (例えば圧力伝達系は伝達系の一部に外力が印加されると誤りの出力を発生する) を使って，情報 (信号) が伝達されている系である。

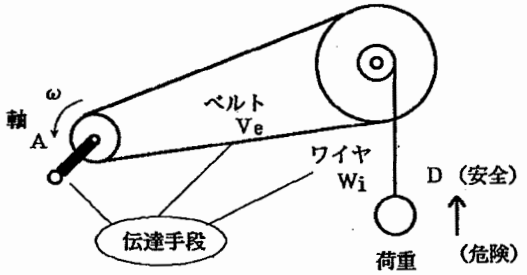
エネルギによってユネイトに情報が伝達される系は原因と結果が時間軸上で決定される。すなわち，決定論として定まる系である。このようにマクロ的決定論で定まる物理系は熱力学系であり，特に，システムを閉鎖的 (断熱的) にした場合，熱力学第 2 法則 (エントロピ増大側) が適用される。式 (2-10) の$E_S\cdot I_S$で示される情報伝達系は$S^*=G^*=1$ の時のみ情報が伝達されるフェールセーフ・システムとして故障時出力エネルギが低下する。すなわち，エントロピ増大則にしたがう構造で実現され，確率的にエネルギを発生する (エントロピ低下の) 構造，すなわち，上述の出力非遮断の誤りを許す系の構造とは区別される。例えば，雑音による誤り防止を行ったとしても，このフィルタが故障した時出力低下に陥る，すなわちエントロピ増大則が適用されねばならない。逆に，式 (2-10) の$E_S\cdot I_S=1$ は，エントロピ最小の条件として出力されねばならない[2]。マイクロ・エレクトロニクス化する現代情報処理技術は素子を装着する基板の単位面積当たりの消費電力を制限することによって高密度実装を実現せざるをえない。このため演算要素は必然的に高入力抵抗となり，雑音による誤りが生じやすくなり，エントロピ最小条件を満たすことがむずかしくなってきている。産業用ロボット工業会による調査の結果はまさにこの事実を証明している[3]。

2.4.2 エネルギ伝達系の論理的構造

次に，エネルギによってユネイトに情報が伝達される系を Fig. 2.5 の運転機械の例を用いて考察する。Fig. 2.5 はスイッチSwを閉成することによってモータを回転させ，この回転出力で揚上機を上下させる制御モデルを示す。Fig. 2.6 は Fig. 2.5 における制御情報の流れ図で，各ブロックは操作のための要素を示す。図を構成するエネルギ伝達要素は壊れた時エネルギを伝達しない特性 (非対称故障特性) を持つ。すなわち，電線やモータ，軸，ベルト，ワイヤロープは壊れた時制御情報を伝達できず，また，壊れることによって逆にエネルギを伝達する構造では製作されない。よく電気系で用いられるサイリスタやトランジスタ等の半導体を使った伝達要素は，壊れた時制御出力を発生してしまう (対称故障特性) 場合があり，Fig. 2.4 における出力非遮断の誤りを許す系で利用されるべき要素である。Fig. 2.5 でスイッチSwによって与えられる入力 (制御) 信号を$\widehat{M}x\cdot I_S \in \{1,0\}$



(a) 回転運動の伝達



(b) 動力の伝達

Fig. 2.5　Transmission of information and energy.
情報とエネルギの伝達

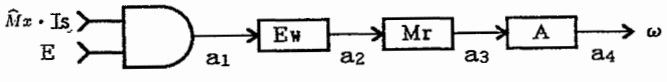
式 (2-11) は，出力状態$D=1$を生成するエネルギが安全制御系として安全情報I_Sを担っていることを示す。

いま，Fig. 2.5 における操作系全体を出力状態Dを生成する要素とし，この動作状態を論理変数$D^* \in \{1,0\}$ で表せば，式 (2-11) は次式で表される。

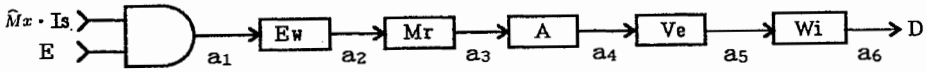
$$D = (\widehat{M}x \cdot I_S) \cdot D^* \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}12)$$

ここに，$D^* = E^* \cdot Ew^* \cdot Mr^* \cdot A^* \cdot Ve^* \cdot Wi^*$

であり，各要素のいずれが故障した時もベルト揚上機の上昇エネルギは伝達されない特性を示す。すなわち，Fig. 2.5 を構成する各要素が非対称故障の特性を持ち，情報伝達がユネイトになされるために，全体もまた非対称故障の特性を持つことを示している。これは，各要素で伝達される情報（エネルギ）の入出力をai $(i=1\sim6)$ で表し (Fig. 2.6(b))，各要素について番号の小なる側を入力，大なる側を出力として各要素の動作状態を式 (2-12) と同様の方法で$K^* \in \{1,0\}$



(a) 回転運動（情報）の伝達



(b) 動力（情報）の伝達

Fig. 2.6　Block diagram of energy transmission.
エネルギ伝達の流れ図

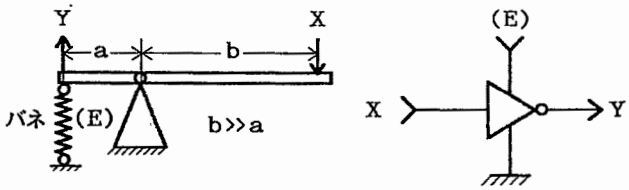
で表し，ベルト揚上機の移動出力を上昇状態を 1，下降した状態を 0 とする論理変数Dで表すものとする。ここに$\widehat{M}x \in \{1,0\}$ は制御命令としての入力情報，$I_S \in \{1,0\}$ は安全であるという許可を与える情報（安全情報）である。$\widehat{M}x \cdot I_S$ は安全であるという条件に基づく入力情報を示すので，この値が 1 であることは，制御出力$D=1$の発生の許可を意味する。ここで，電線Ew, モータMr, 軸A, ベルトVe, ワイヤロープWi, 電源Eの動作状態をおのおの 2 値の論理変数Ew^*, Mr^*, A^*, Ve^*, Wi^*, $E^* \in \{1,0\}$ で表すと，出力状態Dは次式で表される。

$$D = (\widehat{M}x \cdot I_S) \cdot Ew^* \cdot Mr^* \cdot A^* \cdot Ve^* \cdot Wi^* \cdot E^* \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}11)$$

として代表させれば，各要素の入出力関係は，次式で表されることになる。

$$aj = ai \cdot K^*,\ i<j \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}13)$$

換言すると，ここに示される制御情報の伝達は，すべ



（a）機械的差動構造　　（b）電気的差動構造

Fig. 2.7　Differential mechanism.
差動構造

ての要素の情報伝達が故障に関してユネイトな関係で伝達され，機械的差動構造（例えばFig. 2.7(a)，電気的には同図 (b) で表現される）による否定演算構造を安易に採っていないことによる。これらの伝達系は，Fig. 2.8 で示すように，情報伝達系として出力を正常時のみ出力する仮想ゲートG'で表現できる。

2.4.3　具体的センサ構成

次に安全を示す情報（安全情報）の抽出手段について安全情報の発生する作業空間を含むセンサ構成の論理的考察を行う。

2.4.3.1　情報の処理形態

安全を確保すべき対象（作業空間）の状態を安全状態と危険状態の 2 つに分けることができるものとする。この分割は，安全状態から危険状態までの状態の変化に対して，安全を示す状態として十分余裕を持つしきい値を設けることによって行うことができるものとし[1)]，定義される安全状態を 1，危険状態を 0 とする 2 値の論理変数$L \in \{1,0\}$ で表すものとする。そして，この情報抽出のための物理的手段（センサ）のあり方をまず定める。ここに，物理的手段とは，一つの空間の安全状態を抽出するための音，光，磁気，電気接点等であって，安全情報$L=1$ をセンサ出力$I_S=1$ として生成するセンサである。安全情報$L=1$ の抽出方法には，安全状態（すなわち，L）を直接抽出する方法と危険発生（$\overline{L}$, すなわちL の否定）を抽出する方法の 2 通りが考えられる。

いま，センサ出力$I_S \in \{1,0\}$ の論理的エネルギレベルに対して，高エネルギ状態を論理値 1，低エネルギ状態を 0 と定め，入力信号を$\overline{L} \in \{1,0\}$ とおく。入力信号$\overline{L}=1$ は危険発生を，$\overline{L}=0$ は安全状態を意味するから，Table 2.1 の真理値表で示すように，センサが上に定めた 2 値出力Is を生成するには，否定演算機能が不可欠となる。Fig. 2.9(a), (b) はこのセンサの基礎的構成法を示し，$u(\overline{L})$ は否定演算を含まないセンサとしての処理機能，NOT は否定演算機能を表す。

同図 (a) はセンサで信号$\overline{L}$を抽出した後否定演算を行っており，センサ機能$u(\overline{L})$ と否定演算機能 NOT の動作状態をそれぞれu^*, $No^* \in \{1,0\}$ とすれば，出力I_Sは次の論理式で表される。

$$I_S=\overline{(u(\overline{L})\cdot u^*)}\cdot No^*=(L\vee \overline{u}^*)\cdot No^* \cdot (2\text{-}14)$$

ここに，$\overline{u}^*$はセンサ機能$u(\overline{L})$ の故障時の出力状態の否定を表す。式 (2-14) は，この否定によりセンサが故障して$u(\overline{L})\cdot u^*=0$ が生じ，しかも否定機能が正常であれば（例え入力情報が$\overline{L}=1$（危険）であっても），$I_S=1$ となる誤りが起こることを意味する。この危険側誤りが生じないためには，センサの機能は$u(\overline{L})\cdot u^*=0$ の誤りが生じない特性を有する必要がある。しかし，機械的には接点の接触不良や接点磨耗は不可避であるし，電気的には，構成されるセンサに対して，出力エネルギ零の故障を認めない構成は不可能（電源が切れると必ず起きる）である。したがって，論理的に $L \geqq I_S$ は満たされない。図 (b) は，まず否定演算を行って後この出力情報 $\overline{\overline{L}}=L$ が処理機能$u(L)$ によって処理されて出力I_Sを生じており，処理機能の動作情報を上と同様にu^*とおけば，出力I_Sは次の論理式で表せる。

$$I_S=u(\overline{L}\cdot No^*)\cdot u^*=L\cdot No^*\cdot u^* \cdots\cdots (2\text{-}15)$$

式 (2-15) すなわち，Fig. 2.9(b) で入力情報$\overline{L}$の否定は直接安全情報 L の抽出$u(L)$ を意味しており，論理的には$L \geqq I_S$を満たす。すなわち，センサは安全情報$L=1$ を直接抽出して$I_S=1$（高エネルギレベル）

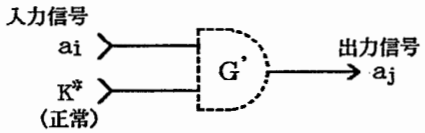


Fig. 2.8　Imaginary gate.
仮想ゲート

Table 2.1　Generation of negative information. (Truth table)
否定情報の生成（真理値表）

$\overline{L}$	I_S
0	1
1	0

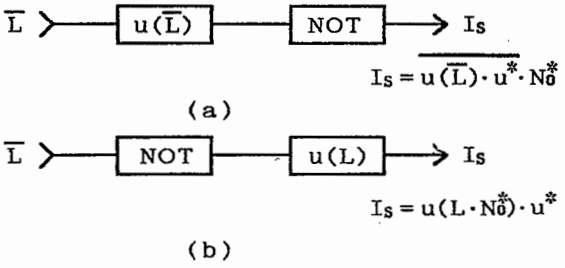


Fig. 2.9　Generation of negative information.
否定情報の生成

を生成しなければならない。例えば，機械的接点を使って直接出力I_Sを得る場合，あるいは電気的センサとして接点出力を与える場合，ノーマルクローズド・タイプ（通常時閉型）でなければならないことを意味する。

2.4.3.2　センサ構造

センサは検出対象となる被検出物体の持つ磁気や温度，光等のエネルギが直接トランスジューサの出力となる直動変換型センサと，情報を抽出するためにあらかじめエネルギを幅射し，トランスジューサは検出すべき情報をこの幅射エネルギの変調信号（ON/OFFのスイッチ信号を含む）として抽出する変調変換型センサとに分けることができる[4]. 前者は，例えば炎の持つエネルギを直接電流に変換する熱電対や人体の持つ赤外線を検出する赤外線センサ，騒音を検出するマイクロフォン，押す動作で作動するスイッチ等である。このセンサはトランスジューサにエネルギが供給される時が安全を示し，かつ，エネルギの供給を受けるトランスジューサが出力として論理値 1 (I_S=1) に誤らない時のみ，$L \geqq I_S$ の論理的関係を満たす(例えばガスの安全供給設備は炎がある時を安全状態とし，かつ熱電対が故障した時出力電流を生じない特性を持つ[5])。しかし，例えば作業空間にいる人の発生する赤外線エネルギを用いてトランスジューサ出力(論理値 1）を得る場合，人間の存在は危険発生を意味し，センサ出力として安全を示す出力$I_S=1$を発生させるには，トランスジューサと出力$I_S=1$の間に否定演算が必要となり，式 (2-14) で示したように，ユネイトなセンサ構成とはならない。一方，作業空間にエネルギビームを幅射し，空間が安全状態にある時のみ，この幅射エネルギを抽出する変調変換型センサの構成とするならば，抽出される人間の不在／存在（すなわち安全情報 L）とセンサ出力（トランスジューサ出力）の間にはユネイトな関係が成立する。

Fig. 2.10 でεi は作業空間Szに幅射される。例えば音あるいは光のエネルギビームである。ε_{01}とε_{02}は作業空間を経由して出力される音あるいは光の出力エネルギで，出力ε_{01}は作業空間Szに人間が進入した時反射して生じ（人間がいない時生じない），出力ε_{02}は人間がいない($L=1$) 時出力される（人間がいると遮断されて生じない）。図で，出力ε_{01}は，人間の前方でエネルギビームεi を遮断する障害物（Sb で示す）が存在すると発生できないが，人間と同じ位置に障害物が進入すると人間でないのにε_{01}は生じる。したがって，作業空間に異常が生じた場合，出力ε_{01}は発生しない場合と発生してしまう場合とが存在する。一方，出力ε_{02}は障害物Sb がエネルギビームεi の進行軸上いずれの位置であっても生じない特性を持つ。

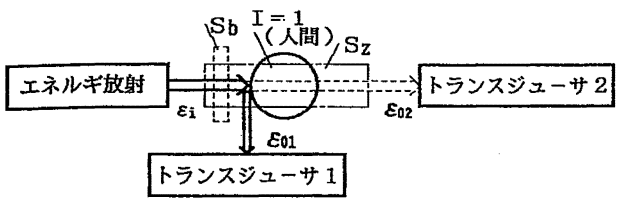


Fig. 2.10　Confirmation of space normality.
空間の正常性確認

いま，作業空間に障害物が存在する時を異常とみなし，正常時を 1 異常時を 0 とする 2 値の論理変数Sz^*で表し，空間に入力されるエネルギεi と，空間から出力されるエネルギε_{01}，ε_{02}を（存在を 1，不在を 0 とする）論理変数をそれぞれEi, E_{01}, E_{02}とおく（トランスジューサの出力側から見てしきい値を与えれば，2 値情報として捉えることができる)。そして，異常時における出力エネルギの誤り出力状態を 2 値の論理変数$E'_{02} \in \{1,0\}$ で表せば，論理出力E_{01}, E_{02}は次式で与えられる。

$$E_{01} = \overline{L} \cdot Sz^* \cdot Ei \cdot \vee Sz^* \cdot E'_{02} \quad \cdots\cdots\cdots (2\text{-}16)$$

$$E_{02} = L \cdot Sz^* \cdot Ei \quad \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}17)$$

式 (2-16) は，抽出される情報$\overline{L}$からセンサ出力I_Sを得るには否定演算を必要とする（ユネイトでない）ばかりでなく，出力変数E_{01}の誤り方が定まらないことを意味する。式 (2-17) は常に$L \geqq E_{02}$, $Ei \geqq E_{02}$ (エネルギの幅射源の動作状態を$Ei^* \in \{1,0\}$（正常時を 1，故障時を 0）とすると$E_{02} = L \cdot Sz^* \cdot Ei^*$) が成立し，エネルギ幅射源の故障時だけでなく，人間の検知も作業空間の異常として捉えられていることを意味する。すなわち，正確に表現するならば，次式で表される。

$$E_{02} = Sz^* \cdot Ei^* \quad \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}18)$$

ここに，幅射されるエネルギの論理値Ei と受信されるエネルギの論理値E_{02}は Fig. 2.4 において外部から供給されるエネルギEs と安全情報I_Sの許可に基づく論理積出力Es'におのおの対応し，安全を示す入力情報L は，Fig. 2.4 における許可I_Sに対応する。すなわち，Fig. 2.10 において発生されるエネルギεi

と空間Szに生ずる安全情報（人間の不在）はインタロック (Fig. 2.11(a)) を構成し，式 (2-18) で示されるように安全を示す状態($Sr^* = 1$) と幅射エネルギ($E_i^* = 1$) の論理積がトランスジューサで受信されるエネルギ($E_{02} = 1$) である。換言すると，式 (2-18) は，式 (2-10) における$Es' = Es \cdot I_S$である。ここに，Fig. 2.10 における障害物Sbと人間は空間Szにおいて安全($E_{02}=1$) を確保するための一種の雑音である。

次に，直動型トランスジューサにおける安全情報の抽出形態について考察する。いま，作業空間Szの外Sz^cには作業者が 1 人だけ存在し，また，人間と同様の赤外線を発生する物体（雑音）は存在しないものと仮定する。この場合，人間（赤外線）が作業空間の外Sz^cに到着した時が空間Szの安全状態である。そして，人間の赤外線エネルギの発生を$Ei = 1$ とおくと，空間Sz^cにおける人間の存在，すなわち安全状態$L = 1$ は$Ei = 1$ の時発生し，$L = Ei$ である。すなわち，このトランスジューサで受信されるエネルギ (論理値) をE_{01}とおくと，$E_{01} = L \cdot Ei$ である。もし，空間Sz^cに他の作業者が進入する場合があるとすれば，これを空間Sz^cの異常（論理値 0）とみなして空間Sz^cの状態を$Sz^{c*} \in \{1, 0\}$ とおけば，受信されるエネルギの論理値E_{01}は次式で表される。

$$E_{01} = L \cdot Ei \cdot Sz^{c*} \vee \overline{S}z^{c*}$$
$$= Ei \cdot Sz^{c*} \vee \overline{S}z^{c*} \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}19)$$

式 (2-19) は空間が正常($Sz^c = 1$) である時のみ安全情報$E_{01} = 1$ をエネルギの受信$Ei = 1$ として生成されることを意味し，これは，Fig. 2.11(b) のインタロックモデルで表現される。

空間Sz^cにおけるセンサを Fig. 2.10 におけるトランスジューサ 1 による受信方法とすれば，上の直動型センサと同様の効果が得られる。この場合，空間Sz^cに備えられたエネルギビームの幅射空間に人間が到着した時受信エネルギε_{01}が発生する。したがって式 (2-19) に対応する受信されるエネルギの論理値E_{01}は次式で表される。

$$E_{01} = L \cdot Ei^* \cdot Sz^{c*} \vee \overline{S}z^{c} \cdots\cdots\cdots\cdots (2\text{-}20)$$

式 (2-20) では，エネルギビームの幅射源が正常($Ei^* = 1$) である時，必ずエネルギビームは発生するものとしている($Ei^* = Ei$)。すなわち，この場合は，図 Fig. 2.11(c) のインタロックモデルで表現でき，同図 (b) は同図 (c) の特別な場合であることが分かる。

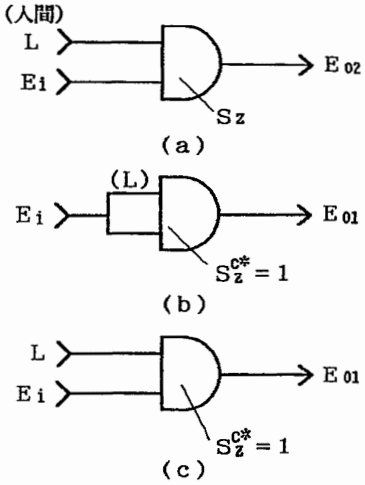


Fig. 2.11 Sensor for generating safety information.
安全情報生成のためのセンサ

(b) は同図 (c) の特別な場合であることが分かる。

Fig. 2.11(a), (b) は安全情報抽出センサに関して次のことを示している。

(1) 安全情報($L = 1$) によってエネルギが受信される($E_{02} = 1$, または$E_{01} = 1$) 構造で実現される。

(2) 安全を確保すべき空間(Sz) で安全を直接抽出すれば，空間の異常($Sz^* = 0$) が安全側検知情報($E_{02} = 0$) となり，フェールセーフな検知空間が実現する。

(3) 安全を確保すべき空間(Sz) で安全を直接抽出せず，間接的に外の空間(Sz^c) で安全を抽出しようとすると，空間を正常($Sz^{c*} = 1$) に保つ必要が生じ，フェールセーフな検知空間が得られない。

ここに，フェールセーフな空間とは空間が検知対象外のものによって乱された場合に，危険を示す検知情報が発生する空間を示す。

2.5 インタロックの運用

一般に 2 値の信号を伝達する要素 F の入力をSi, Si'.., 出力をSo, 信号処理をf, 要素Fの正常性を示す論理変数をF^*(正常を 1，異常を 0）とすると，出力So は次式で表される。(Fig. 2.12 参照)

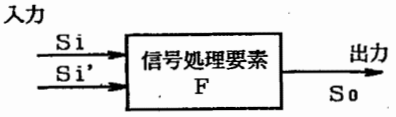


Fig. 2.12 Signal Processing unit.
信号処理要素

$$So = f(Si, Si'..) \cdot F^* \vee fe \cdot F^* \cdots\cdots\cdots (2\text{-}21)$$

ただし，fe は要素Fが異常時の出力を示す。この式で，例えば，Fが 2 入力の論理積処理であれば，それはゲートとみなすことができ，1 入力のバッファ処理の場合は，増幅器等の信号伝達要素とみなせる。また，入力をアナログ量と考えても，(2-21) 式は成り立つが，この場合センサとみなせる。また，So を仕事出力の状態を示すものと考えれば，アクチュエータを示すものとみることもできる。すなわち，この式は，作業システムの要素を一般化したものとみなせる。

この式で$fe \neq 0$ であれば異常時に出力$So = 1$ となることがあり，$fe = 0$ であれば，異常時には出力$So = 0$ となる。前章で述べたように，安全システムにおいて，その要素は危険側（1 側）誤りが許されない。すなわち，異常時の出力は 0 でなくてはならない。これは，(2-21) 式でいうと，$fe = 0$ でなくてはならないことを意味する。安全システムでは，信号伝達要素はフェールセーフ，すなわち，

$$So = f(Si, Si'..) \cdot F^*$$

あるいは，

$$fe = 0$$

でなくてはならない。安全システムでは，さらに，入力に含まれる 0 側誤りを 1 側誤りに変換しないために，fが入力の否定を含まない，すなわち，増加関数であることが必要である。

本節においては，これを実現するための，技術的手段の基本原理について述べる。

(1)　アクティブな信号伝達

フェールセーフな構造の実現方法について，前述したことの要点のみを整理すると，次の 3 つがフェールセーフを実現するための基礎条件となる。

① 安全情報はエネルギとして伝達される。

② 安全情報は，周囲に存在する雑音や電源に誤って混触しても，安全情報を生成しない特性，すなわち，周囲に存在するエネルギレベルより高いエネルギで伝達される。これをポテンシャル極大の条件という。

③ 安全情報は，非対称の誤り特性を持つ情報伝達要素によって，ユネイトな関係で伝達される。

前述の Fig. 2.5, Fig. 2.6 のシステムを構成する要素のように安全のエネルギを伝達する要素は，故障時“0” を出力する特性を有しており，これは非対称誤りの出力特性と呼ばれる。そして，正常時，各要素は入力が安全である時，出力もまた “1” を生じ，また，故障によって，出力は決して “1” とはならない関係を持つ。これは安全情報のユネイト性と呼ばれる。

(2)　セルフチェック

フェールセーフな信号処理システムにおいては，入力信号は「安全」を示す信号と，システムが正常であることを示す「動作確認」の信号が共に高エネルギ状態で伝達される。この 2 つの信号は，エネルギレベルが閾値（処理部）で弁別され，2 値の情報で表されるものとすると，両信号の論理積（あるいは重畳信号）として，高エネルギ状態で出力される。このことは，システムの入出力信号の関係において，ユネイト性が保証されなくてはならないことを意味する。

Fig. 2.13 で伝達される信号が安全情報として有意性を持つためには，ハードウェアは雑音より高いエネルギ状態にあるしきい値を持ち，なおかつ，この機構が正常に働いているかどうか確認する構造を必要とする。

前述したように，安全状態の持つエネルギを用いると，以上のことが自然に実現できる。しかし，多くの場合，センサ出力を仕事出力と結ぶ過程でエネルギの増幅が行われる。このような場合に，故障によって電源のエネルギが直接出力される可能性もあるので，安全を伝える “1” が誤りでないことを証明すること，すなわち，“0” となりうることを示すことが必要とな

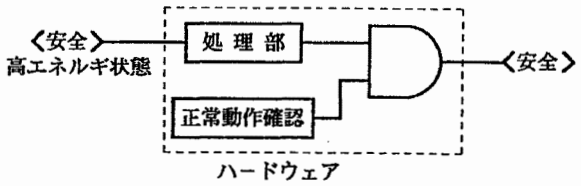


Fig. 2.13　Fail-safe structure of signal processing.
信号処理のフェールセーフ構造

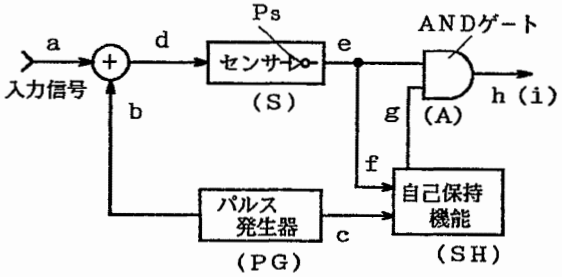


Fig. 2.14　Basic structure of self-checking.
セルフチェックの基本構成

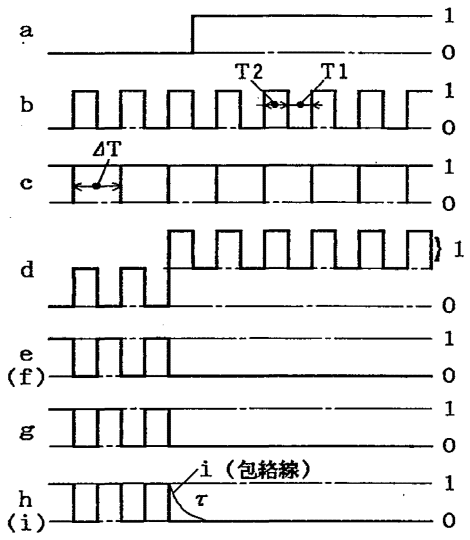


Fig. 2.15 Self-checking system.
セルフチェック・システム

る。すなわち，信号源（安全状態）以外のエネルギ源を用いる場合は，積極的な正常動作確認構造を必要とする。

ここでは，フェールセーフな信号処理の原理が説明しやすいように，1入力1出力系のセンサの動作確認作業を扱う。

危険検出型のハードウェアは故障すると危険を通報できない。そのため，通常，始業点検や定期点検において動作確認が行われる。Fig. 2.14 は否定演算$f(a)$を行うセンサS(例えば火災センサ,「火災がない＝安全」を検出する）の動作確認を自動的に行う場合の機能をブロック図で示している。また，Fig. 2.15 は動作を説明するタイミングチャートである。

このセンサシステムの入力信号aは0を安全，1を危険とする2値論理である。センサ部Sは，入力信号dの否定演算を行い出力信号eを発生する。信号eのままでは，(1) で述べた非対称性が得られない。そのために，PG, SH等を用いる。

パルス発生器PGは，センサSの機能確認を行うためのテストパルス信号発生器である。自己保持回路SHはセンサSの出力信号に含まれる機能確認信号fをセット入力とし，パルス発生器PGの出力信号cをリセット信号として，センサが正常動作状態にあることを記憶する機能である。AND ゲート A は，自己保持機能SHの出力信号$g(=1)$がある時のみ，センサ出力eを出力信号hとして発生する。すなわち，図の構成はセンサSの機能確認を行って，この結果を自己保持で記憶し，センサSが正常状態にある時のみ入力信号aに対するセンサ出力を AND ゲートAから出力する構成である。次に図の動作を説明する。

センサSの入力信号dは，入力信号aにテスト信号bが重畳したもの$(d = a + b)$となる。一方，自己保持機能SHのリセットの信号cはパルス発生器PGの出力信号bの立ち上がり成分を負信号とする波形である$(c = db/dt(> 0))$. テスト信号bの周期は，入力信号aの変化より十分短い周期となるようにする。各ブロックの出力信号b, c, e, f, g, hは2値である。信号dは$a = 1, b = 1$の時センサSは非線形領域にあり，タイムチャートに示すように，センサsの出力換算値として$d = 1$の論理値とする。

入力信号$a = 0$の時，センサSには入力信号bだけが入力され，出力信号$e = 1$の立ち上がり成分$f = de/dt(> 0)$で自己保持機能がセットされ，パルス発生器の出力信号$c = 0$でリセットされる。このため，自己保持機能SHの出力信号gとセンサ出力eとは同相となり，AND ゲートAにはパルス信号発生器の出力周波数のパルス信号hが生じる。

入力信号が$a = 1$となると，入力信号dは連続的に$d = 1$となり，したがってセンサの出力信号は$e = 0$となって，自己保持機能SHにも AND ゲートAにも出力信号が発生せず$h = 0$となる。いま，出力信号hのパルス信号を整流して，改めてこれを$h = 1$の論理積で表すものとすれば，Fig. 2.14 のシステムは安全$a = 0$に対してセンサの正常時のみ出力信号$h = 1$を生じ，危険$a = 1$または，センサの故障時，出力信号$h = 0$を生じる（非対称誤り特性の実現)。そして，自己保持機能SHと AND ゲート A が故障で誤って出力信号$g = 1$または$h = 1$を発生しない特性，すなわち，非対称誤り特性を有するならば，Fig. 2.14 の構成は入力信号aに対して非対称誤り特性を持つフェールセーフなハードウェアとなる。なお，センサSは対称誤り特性でよく，また，以上の議論は必ずしも否定演算機能を有するものには限らず適用される。

次に，検査信号が高周波である場合，自己保持回路SHと AND ゲート A は，包絡線検波器で代行できる。この場合の自己保持機能のリセットは平滑の時定数である。Fig. 2.16 にこの構成を示す。同図の構成は，従来から行われてきたフェールセーフな信号処理の手法である。一般には，信号dは入力信号aが小さい時検査信号の変調信号として発生し，入力信号aが大きい時には，Fig. 2.14 で示したように検査信号の

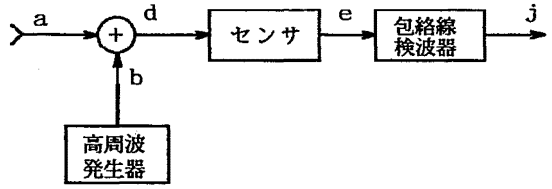


Fig. 2.16 Fail-safe signal processing.
フェールセーフな信号処理

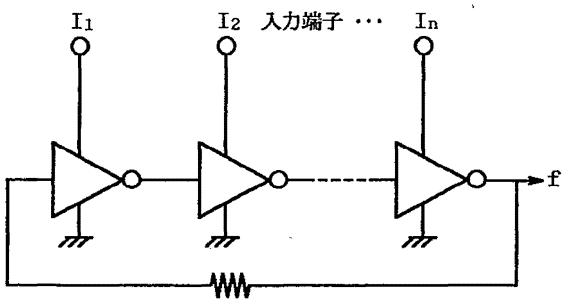


Fig. 2.17 Logical product operational oscillation.
論理積演算発振器

スイッチ信号（重畳信号）として発生する。

Fig. 2.13 で示される正常動作確認構造は，システム自体の監視を行ういわゆるインタロックである。具体例として，フェールセーフ論理演算用として，提案されている演算発信器を Fig. 2.17 に示す。これは，すべての入力がある時のみ帰還発信し，交流出力信号を発生するので，発信によって，回路自体が確認動作機能を有する構造となっている。

(3) インタロックと安全の予測

(a) 予測の構造

前の節では，災害が発生しない論理的条件として，(2-1) 式をあげ，そのための安全制御の方式を明らかにした。すなわち，

$$Hx(t) \cdot Mx(t) = 0 \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}1)$$

$$Mx(t) = \overline{H}x(t) \cdot \widehat{M}x(t) \cdots\cdots\cdots\cdots\cdots (2\text{-}22)$$

$$Hx(t) = \widehat{H}x(t) \cdot \overline{M}x(t) \cdots\cdots\cdots\cdots\cdots (2\text{-}23)$$

である。この (2-22) 式を実行する場合に発生する問題点について以下に検討する。

現実の機械においては，$Mx=1$ の状態から $Mx=0$ の状態への変化およびその逆の変化を行わせるために有限の時間がかかる。安全確認型のインタロック構造において，この時間遅れの効果等を明確にするため

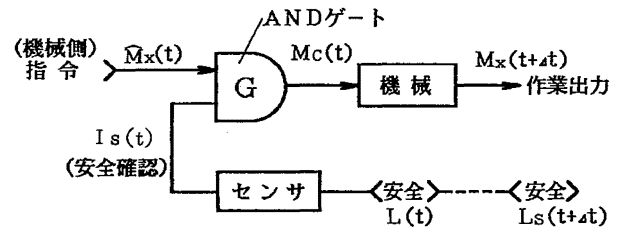


Fig. 2.18 Safety confirmation system which includes time delay.
時間遅れを含んだ安全確認システム

に，Fig. 2.3 をより詳細にしたものが，Fig. 2.18 のシステムである。図において，Mx は機械出力，Mc は機械に対する動作制御信号，Is はセンサの出力で動作指令 $\widehat{M}x$ に対する動作許可（それぞれ，ありが 1，なしが 0 を示す），L は安全状態を示すものである。Fig. 2.3 と異なるのは，機械の時間遅れを示すために，Mx を Mx と Mc に分けたことである。また，(2-22) 式の $\overline{H}x$ に対応する安全を示す論理変数も，安全センサの検知対象の状態を示す論理変数 L とシステムの安全状態 Ls を示す論理変数（それぞれ，安全が 1，危険が 0 を示す）に分けたが，これについては，後述する。

この図において，(2-6), (2-22) 式に対応するものとして，

$$Mx(t) \leqq L(t) \cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}6')$$

$$Mc(t+\delta t) = \widehat{M}x(t) \cdot Is(t) \cdots\cdots\cdots (2\text{-}22')$$

が得られる。(2-6′) 式は安全の条件を示し，(2-22′) 式は制御方式を示すものとなる。$Mc \neq Mx$, $Is \neq L$ であるため，(2-22′) 式は安全を保証するものではなくなっている。

これらの変数の時間遅れの関係を Fig. 2.19 のタイムチャートおよび以下の式に示す。Fig. 2.19 のタイムチャートに見られるように，制御信号 Mc に対して，機械の動作出力 Mx は，立ち上がり，立ち下がりにそれぞれ時間遅れ $\Delta t'$, Δt を生じる。すなわち，Fig. 2.19 の時間範囲において，

$$Mc(t) = Mx(t+\Delta t') \quad t \in (I, II, III)$$

$$Mc(t) = Mx(t+\Delta t) \quad t \in (III, IV, V) \cdots (2\text{-}24)$$

である。一般には，$L \rightarrow Is \rightarrow Mc$ の信号伝達でも遅れが存在する。センサ，ゲートにおける信号の遅れ

は，それぞれ

$$I_S(t+\delta t_1) = L(t)$$

$$Mc(t+\delta t_2) = I_S(t)$$

(ただし，$\widehat{M}x = 1$ の時)

となる。これらの遅れは，最後の$Mc \rightarrow Mx$ の遅れに較べて無視できることが多い。また，その遅れをΔt 等に繰り入れてと考えることができる。

立ち上がり，(Fig. 2.19 の時間範囲 II，“1” を伝達する過程) においては，$L \rightarrow Mx(L \geqq Mx)$ の順に遅れるので，$Mx = 1$ となる時には，すでに$L = 1$ となっている。すなわち，安全の条件 (2-6′) 式を満たすので，立ち上がりの遅れは安全上問題はない。

しかし，立ち下がり (Fig. 2.19 の時間範囲 IV，“0” を伝達する過程) においては，$L \rightarrow Is \rightarrow Mc \rightarrow Mx(L \leqq Is \leqq Mc \leqq Mx)$ の遅れがある場合，Mx が 0 となる以前に，L が 0 となり，(2-6′) 式を満たさない，そのため，安全確認においては，Fig. 2.19 に示すように，少なくとも遅れ分$(\Delta t + \delta t_1 + \delta t_2)$ だけは，事前の予測を必要とする。現実には，未来から信号をうることは不可能であるため，未来の安全状態Ls をユネイトに伝えることを証明できる検知対象を用いれば，安全情報L をうることができる。ここに，Fig. 2.3 の安全状態L が，論理的安全状態を示すLs と，物理的測定の対象と成りうる安全状態L に分けて考える必要がでてくる。また，これに伴い (2-6′) 式は，

$$Mx(t) \leqq Ls(t) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}6'')$$

となる。これらの論理変数の関係を図的に示すと，

$$\begin{array}{l} \quad\quad\quad\quad -\!-\!-\!-\!-\!\rightarrow t\ (\text{時間}) \\ L \rightarrow Is \rightarrow Mc \rightarrow Mx \\ \quad\quad\quad\quad \leftarrow (\text{予測}) - Ls \end{array}$$

となる。これを式で示すと

$$L(t) \leqq Ls(t+\Delta t) \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2\text{-}25)$$

となる。Fig. 2.19 の場合には，$\delta t = 0$ とすると，

$$L(t) = Is(t) = Mc(t)$$

であるから，(2-24) 式により

$$L(t) = Mx(t+\Delta t)$$

$$Mx(t) \leqq Ls(t)$$

となり，安全の条件 (2-6″) 式を満たす。なお，安全情報が 1 の時に，動作指令$\widehat{M}$が 0 になって停止する場合は，(2-25) 式の等号が不等号 <にかわるだけであり，正常停止なので当然 (2-6″) 式を満たす。

(b)　予測空間の生成

次にこの予測を実現するための手段について，人間が機械の運動する領域x_0，すなわち，可動範囲x_0の周りで動き回るという場合を例に考察する。説明を簡単にするために，機械はx_0から出ないが，人間がこの領域に侵入するものとする。また，機械が停止するまでにΔt かかり，人間の最高移動速度はv_0 とする。Fig. 2.20 から明らかなように，人間が時刻t にx_1 にいれば，$t + \Delta t$ には空間α(安全領域x_1から$v_0 \cdot \Delta t$ 以内の範囲の領域) の範囲にいることが予測できる。同様に，時刻 t に空間β(可動範囲Xから$v_0 \cdot \Delta t$ 以内の範囲の領域) の範囲に人間がいなければ，人間が$t + \Delta t$ にx_0にいないことが予測できる。逆に，人間がt に空間βにいれば，可動範囲x_0に入る可能性がある (ただし，空間βにいても，$t + \Delta t$ にx_0にいるとは限らない)。したがって，安全であることを意味する事象，すなわち，x_0に人間がいないということを論

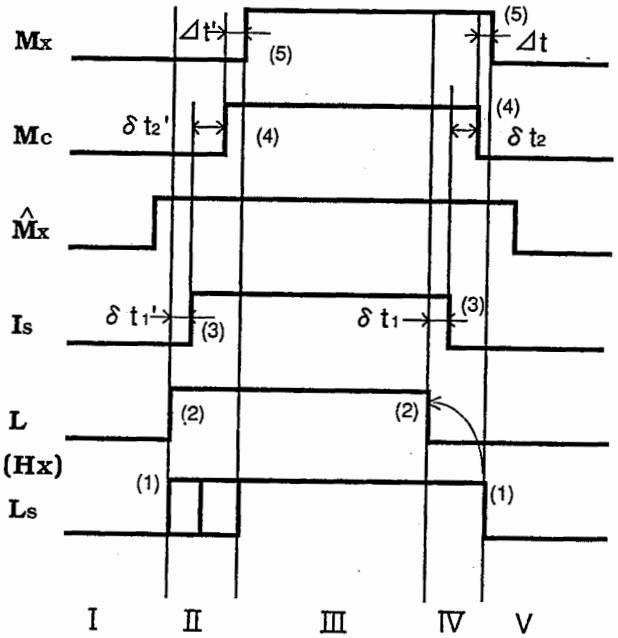


Fig. 2.19　Time-chart of safety information transmission.
安全情報伝達のタイムチャート

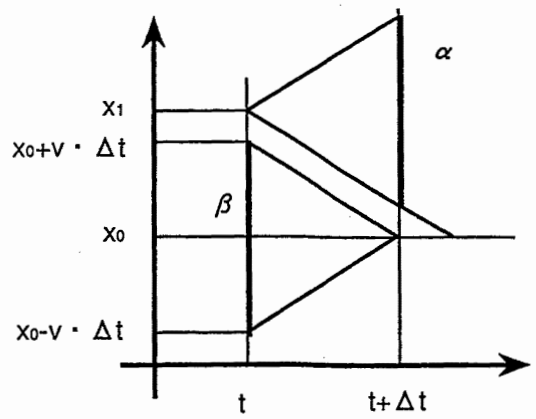


Fig. 2.20　Prediction by using space.
空間による予測

理変数$Ls(\overline{H}x_0, t+\Delta t)$で示し，物理的に検出できる状態として，空間$\beta$に人がいないということを論理変数$L(\overline{H}\beta, t)$で示せば，

$$L(\overline{H}\beta, t) \leqq Ls(\overline{H}x_0, t+\Delta t)$$

$$\beta = \{x | d(x, x_0) \leqq v_0 \cdot \Delta t\} \quad \cdots\cdots\cdots\cdots (2\text{-}26)$$

である。ただし，$d(x, y)$はxとyの距離を示す。

一般に，危険空間x_0が状態変数xの領域として与えられ，エネルギ消散時間Δtと，xの変化率の上限v_0が与えられれば，x_0のまわりに設けた予測空間βを見ることで，安全の予測ができる。すなわち，xがx_0にいないということは，xがβにいないというユネイトな関係を構成できる。

なお，xとしては位置に限ったことではなく，温度や圧力等についても，温度空間，圧力空間というものを考えれば同様のことがいえる。

(4)　検知空間の構成

前節においては，機械の存在領域は固定した点として説明したが，一般的には，機械の可動部は移動する領域となる。この領域を空間Xとする。また，この可動部が完全に停止するまでの時間をΔt_Bとする。この場合，時刻tにおいて機械のエネルギが停止しても，$t \sim t+\Delta t_B$の間は機械は運転を継続するから，その間に人間が空間Xに侵入すると重大な災害となりかねない。

このようなことが起こらないということを予測するためには，前節で示したように空間Xを含むある空間 Hz 内に人間がいないということを確認しなければならない。この場合には，この空間は，空間Xの外側に幅$b = (V_H + V_M)\Delta t_B$の空間$B$とすると，$X$と$B$の合併集合 $\mathrm{Hz} = X \cup B$となる。以後，この空間を「危険空間」と呼ぶ，なお，V_H, V_Mはおのおの人間または可動部の最大移動速度である。

危険空間 Hz に人間がいなければ，災害が起きることはない。これを確認するために，Fig. 2.21 に示すように，空間 Hz の周辺に監視空間S_Rを設ける。

実際の安全センサの構成では，Fig. 2.22 のようにプロジェクタより監視空間S_Rに向けてエネルギを放射し，空間S_Rより広い領域に人間の侵入を検知するための空間Sを生成する（すなわち，$S \supset S_R$）。以後，これを「検知空間」と呼ぶ，この空間Sの状態変化は，Fig. 2.22 のようにトランスジューサで検知し，信号判定回路で増幅を行った後，レベル検定回路で判定基準と比較してセンサ出力を生成する。

監視空間，検知空間というものを考える意味は 2 つある。センサを理想化して考えれば，監視空間，検知空間というものは，空間 Hz の外周の幅のない線に集約できる。しかし，現実のセンサでは，Fig. 2.22 に示すように検知空間というものがある拡がりを持っている。この状態を示すために，検知空間というものを考える必要がある。

また，危険空間 Hz に人間がいないということを確認するためには，必ずしも Hz を監視する必要がない。はじめに Hz に人間がいないということが確認さ

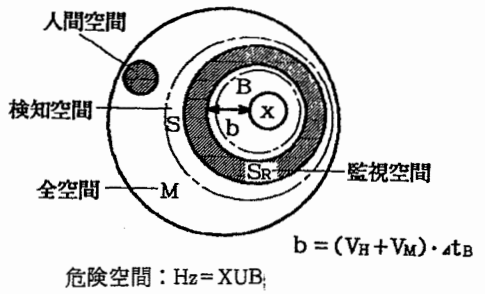


Fig. 2.21　Detection space and monitoring space.
検知空間と監視空間

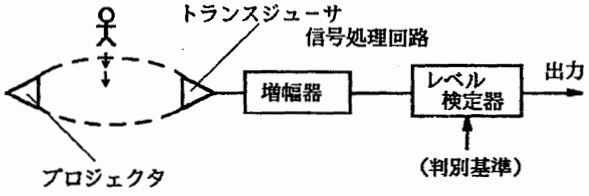


Fig. 2.22　Basic structure of safety sensor.
安全センサの基本構成

れているという条件があれば，監視空間 S_R に人間がいないということは，危険空間 Hz に人間がいないということを包含する。現実には，センサの能力による制約から，後者の方が容易であり，このことを示すため監視空間というものを考えている。

2.6 おわりに

安全作業システムの条件を，安全を抽出してこの情報に基づいてユネイトな論理構成でエネルギを供給する系と，作業命令に対してこのエネルギを必ずしもユネイトに伝達しない系との論理積モデルで示した。次に，ユネイトにエネルギ伝達が行われる機械的系の例を示し，この系は同様のモデルで表現でき，安全条件を正常条件に置換した仮想ゲートモデルで示した。そして，安全の情報を抽出する方法も抽出すべき空間に発生するエネルギを抽出することによって安全を示す情報が得られ，これは，安全情報とこれを抽出するためのエネルギの論理積モデルで表されることを示し，確実に安全が確保されるセンサ構成として，フェールセーフ空間を定義した。

（平成 2 年 11 月 30 日受理）

参考文献

1) 杉本，粂川他 6 名：安全確認型安全の基本構造，機論，54–505, C(1988) pp.2284–2292
2) 粂川，蓬原，杉本：安全技術入門，(1986), 237, 中災防
3) 向殿，杉本他 2 名：産業用ロボットおよびメカトロ機器のノイズによるトラブルについて，第 6 回日本ロボット学会学術講演会，(1988–10) pp.375–378
4) 岡村，寺尾：岩波講座，基礎工学 II（測定論），(1969) 岩波書店
5) 蓬原，杉本，向殿：フェールセーフ技術，安全，38–10 (1987) pp.18–22