

Research Reports of the Research Institute  
of Industrial Safety, RIIS-RR-92, 1993  
UDC 658.513.3:614.82

安全の論理に基づく制御の構成論理  
—安全制御系における安全情報のエネルギー伝達—

杉本 旭\*, 池田博康\*

Safety Control Theory Based on the Logic of Safety  
— Energy Transmission of Safety Information —

by Noboru SUGIMOTO\* and Hiroyasu IKEDA\*

**Abstract;** Safety control system, which is defined as the machine operation controlled according to safety confirmation information, is explained as an interlocking model that is so functioned that energy output from machine is permitted only while the information (safety information) reports safety. The information transmission properties presented in this model are applied on all devices in the interlocking system, consistent from the sensor for producing safety information to devices for transmitting/outputting energy. Small energy level of signal signifying safety is normally produced in a pickup element in the sensor. Enormous power made by amplifying the energy of the safety signal is supplied to the machine to conduct its powerful operation.

This paper discusses on the condition of energy transmission process in which energy is produced in safety sensor as a signal indicating safety and is amplified in the interlocking system up to the sufficient level to do machine duty. Firstly, in this paper, clarified is the characteristics of information to be provided with the information processing means in the interlocking system. Secondly, a logical fail-safe model is proposed for clarifying the production condition of the safety information. Lastly, this fail-safe transmission of information energy can be applied on not only electrically but mechanically processed safety information.

**Keywords;** Mechatronics, Robotics, Safety system, Safety control, Safety control system, Interlocking, Fail-safe.

## 1. 緒 言

著者らは先に、危険を伴う作業が安全の条件に基づいて行われる機械的操作を安全制御<sup>1)</sup>として定義し、この制御系の基本構成を安全を示す情報（安全情報）の許可に基づいてエネルギーが出力されるインタロックモデルで示した<sup>2)</sup>。そして、このモデルで示される情報の伝達特性は安全の情報を抽出するセンサシステムからこの情報が直接伝達されるエネルギー

伝達系まで共通して適用できることを示した<sup>3)</sup>。

通常安全を示す情報はセンサ入力として小さなエネルギーで生成される。一方、この情報に基づいて実行される危険作業に大出力エネルギー発生のための増幅が不可欠となる。本論文では、安全の情報が抽出されて、現実に危険作業が実行されるまでのインタロックシステムにおけるエネルギー増幅過程の特性を論ずる。即ち、第2章で、まず、安全情報の生成からこの情報に基づいて出力エネルギーが発生するまでの処理系の有すべき特性を示し、第3章で、外部に

\*機械研究部 Mechanical Safety Research Division

エネルギー源を有する簡単な作業機械における安全情報の生成条件を論理式モデルで示す。そして第4章でこのモデルを利用して具体的フェールセーフ演算系の構成原理を、また第5章ではフェールセーフな情報の伝達が電氣的、機械的に共通の処理形態で行われることを明らかにする。

## 2. 安全確認と出力エネルギーの発生過程

### 2.1 安全確認過程

安全 (Safety) は危険 (The Hazard) の反対の概念として把握される。即ち、安全は、まず先に危険が認識され、これを予測して回避する過程で生じる概念であって、次の2つの原則に基づいて確認される。

- i. 安全 (無事故) と危険 (事故) とは同一の場所と同時に発生しない。
- ii. 危険 (事故) は予測することができるが、この予測には誤りが存在し、この誤り (即ち、不安) を危険と見なすことによって安全を確保することができる。

上の原則 i は真の安全 (無事故) と危険 (事故) は否定の関係にあることを意味する。しかし、我々が予測する安全は、原則 i における危険 (事故) の反対としての安全 (無事故) でなく、少なくとも事故に至らないための安全である。従って安全を 1、危険を 0 とし、原則 i で与えられる安全と原則 ii で予測される安全を各々2値の論理変数  $Sc(t)$ ,  $Se(t) \in \{1, 0\}$  で表せば、2つの安全  $Sc(t)$ ,  $Se(t)$  の間には、少なくとも真に危険 ( $Sc(t) = 0$ ) であるとき誤って安全 ( $Se(t) = 1$ ) が予測されることだけは許されない論理的關係として次式が成立しなければならない。

$$\forall t, Sc(t) \geq Se(t) \quad (1)$$

### 2.2 安全確認に基づく出力エネルギーの発生過程

危険を伴う作業で出力される力学的エネルギーは安全であるとき発生し、危険であるときこのエネルギーは出力されない。従って、安全状態における出力エネルギーを  $u$ 、危険な状態におけるエネルギーを  $u'$  とおけば次の不等式が成立する。

$$u > u' \quad (2)$$

式 (2) で示されるエネルギー  $u$ ,  $u'$  の誤り特性を現状の作業機械や輸送機械で考えると、次の通りである。

Table 1 ユネイトな関係 ( $Sc(t) \geq U$ )

| $Sc(t)$ | $U$ |
|---------|-----|
| 1       | 1   |
| 1       | 0   |
| 0       | 0   |

$u$ : 通常、列車や車やロボットの可動部のように出力状態  $u$  が  $u'$  に誤ることが許される。しかし、上空の航空機や急停止を許されない列車や、ワークを落下することの許されないロボット可動部には出力状態  $u'$  への誤りも許されない。従って原則として出力状態  $u$  には誤りが許されない。

$u'$ : 出力状態  $u'$  であるべきとき出力状態  $u$  の誤りは許されないが、通常出力  $u'$  が発生しない側は許される。

上述の出力エネルギーを論理変数  $U$  で表し、エネルギー  $u$  のレベルを 1,  $u'$  のレベルを 0 とおくと、この出力  $U = 1$  は安全確認に基づいて出力されるエネルギーであって、この場合の安全確認は式 (1) における予測された安全  $Se(t) = 1$  である。従って、安全確認から出力エネルギー  $U$  の発生までこの安全確認信号を伝達して出力エネルギーを発生する手段  $F$  が必要となる。ここでは、この手段  $F$  を情報伝達手段と呼ぶことにする。この手段  $F$  の機能を論理変数  $F(Se)$  で表し、 $F(Se) = 1$  を安全を示す情報が伝達されるとき、 $F(Se) = 0$  を安全でないことを示す情報が伝達されているときとすれば、安全確認に基づく出力エネルギー  $U$  の発生は次式で示される。

$$Sc(t) \geq F(Se) \geq U \quad (3)$$

式 (3) は安全  $Sc(t)$  の予測とこれに基づく出力エネルギー  $U$  の発生の間には機能  $F(Se)$  が存在することを意味し、 $Sc(t) \geq U$  は、Table 1 で示すように、安全でない ( $Sc(t) = 0$ ) のに危険作業実行のエネルギー  $U = 1$  が発生してはならないこと (ユネイト) を示す。

式 (3) において、情報伝達機能  $F(Se)$  には情報  $Sc(t)$  が伝達されないときが物理的に必ず存在する。例えば、安全を示す情報  $Sc(t) = 1$  として物理的センサによって抽出されるエネルギーは通常微小であって、一方危険を伴う出力エネルギー  $U$  は大きい。したがって機械  $F(Se)$  は増幅機能を伴い、この増幅には

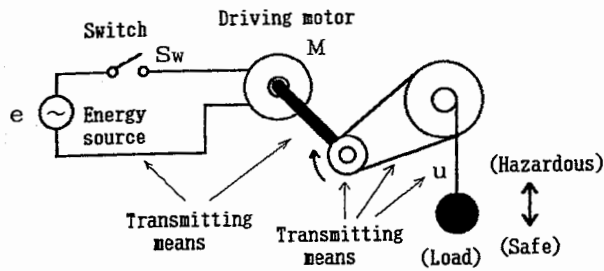


Fig. 1 Control model of load lifting machine  
荷揚げ機械の制御モデル

後述するように別途電氣的あるいは機械的的外部エネルギーを必要とし、もしこの外部エネルギーが供給されないとき出力エネルギー $U$ は発生しない。即ち、情報伝達機能 $F(Se)$ には誤りが存在し、手段 $F(Se)$ の動作状態を論理変数 $F^*$ で表し、正常なときを1、故障時を0とくと、式(3)の論理式で示される機能 $F(Se)$ は次式で表されねばならない(以降、動作状態を表す論理変数に\*印を付し、正常状態を1、故障状態を0とする)。

$$U = F(Se) \cdot F^* \quad (4)$$

式(4)は機能 $F(Se)$ が正常である( $F^* = 1$ )とき $U = F(Se)$ の出力が発生し、故障時は $U = 0$ であることを意味する。ここに、式(3)で示されるエネルギー伝達手段をフェールセーフなエネルギー伝達手段と呼ぶことにする。

式(3)で示される情報伝達手段は安全を示す情報 $Sc(t)$ を抽出する手段と、抽出された情報を伝達する手段と、式(4)に基づいて出力エネルギーを生成する手段(出力エネルギー生成手段)の外に現実には、危険( $Sc(t) = 0$ )時、すでに出力されたエネルギー $u$ ( $U = 1$ )が慣性を持つために強制的にこれを遮断する手段(強制的遮断手段)を必要とする場合が存在する。出力エネルギー生成手段は、式(4)に基づく出力エネルギー $U = 1$ が入力エネルギー遮断によって $U = 0$ となったとき、生成手段に蓄積されたエネルギーが消費される、即ち、エントロピ増大側にしたがって熱消散される過程を持つ。一方、強制的遮断手段は上の過程(応答)では不十分な(間に合わない)ためにもつ機構例えばブレーキ機構である。本論文で対象とするエネルギー伝達手段は抽出される安全情報を伝達し、これを出力エネルギーとして生成する手段であるとし、この出力エネルギー生成手段は危険時出力エネルギーを強制的

に遮断する手段を含む場合もあるものとする。そして、このエネルギー伝達手段は出力エネルギーに $U = 0$ の誤りを含むものとする。

### 3. 安全確認形エネルギー伝達系の論理モデル

#### 3.1 簡単な作業機械におけるエネルギー伝達の論理構成

危険を伴う操作が安全の条件に基づいて加えられる制御を安全制御と定義し、安全の条件に基づいて外部から供給されるエネルギーによって伝達されるエネルギー伝達系について簡単な作業機械を用いて考察する。

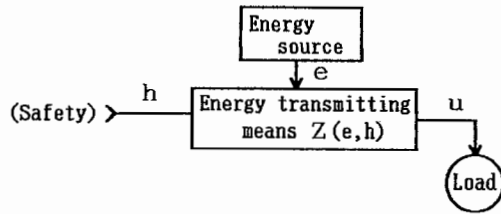
Fig. 1はスイッチ $Sw$ を投入すると電源からモータにエネルギー $e$ が供給され、この回転出力がプーリに伝達されて荷が上昇する簡単な荷揚げ機械の制御系である。この操作は当然上昇した荷の下に人が来ないという安全の条件(エネルギー $h$ で表す)に基づいてスイッチ $Sw$ が投入されるべきであり、スイッチや電線、モータ、軸、ベルト、ワイヤ等で構成されるエネルギー伝達手段を $Z(e, h)$ で表せば、荷揚げ機械の出力エネルギー $u$ の発生はFig. 2(a)のブロック図で表すことができる。Fig. 2(a)のエネルギー伝達手段は構成する電線やモータ、軸、ベルト、ワイヤ等の要素は故障した(切断された)ときエネルギーが伝達されない特性を持つ。従って、入出力エネルギー $e, u$ を2値の論理変数 $E, U \in \{1, 0\}$ で表し、エネルギーが発生しているときを1、発生していないときを0とし、エネルギー伝達手段 $Z(e, h)$ の動作状態を2値の論理変数(状態変数) $Z^* \in \{1, 0\}$ で表すものとすれば、入力エネルギー $e$ と出力エネルギー $u$ の間には次の論理式が成立する。

$$U = Z^* \cdot E \quad (5)$$

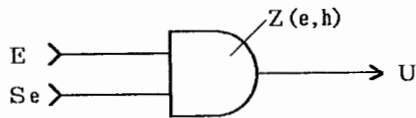
式(5)は入力エネルギーが供給されて( $E = 1$ )、エネルギー伝達手段が正常であるとき( $Z^* = 1$ )のみ、出力エネルギーが発生することを意味する。ここに、 $E \in \{1, 0\}$ はエネルギー供給源の故障状態に1対1で対応すると考えてよいから、エネルギー供給源の動作状態を $E^*$ で表せば、式(5)は次式で表せる。

$$U = Z^* \cdot E^* \quad (6)$$

式(6)はエネルギー $u$ の供給が供給源( $E^*$ )と伝達手段( $Z^*$ )に依存することを意味し、このエネルギー供給



(a) Energy-transmitting system for load lifting machine of Fig. 1  
荷揚げ制御 (図 1) のエネルギー伝達系



(b) Logic representation of energy transmission  
安全制御系におけるエネルギー伝達

Fig. 2 Energy-transmission in safety control  
安全制御系におけるエネルギー伝達

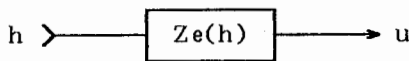


Fig. 3 Energy-transmitting system with internal energy source  
エネルギー供給源を装置内に持つエネルギー伝達系

は、安全の条件が満たされているときのみ行われて、安全でないとき出力エネルギー供給されない。従って、出力エネルギー  $u$  の発生する環境が安全な状況と危険な状況の 2 つに分けることができるものとし、この環境の状態を 2 値の論理変数  $Se \in \{1, 0\}$  で表し、安全状態を 1、危険状態を 0 とおくと、式 (6) は次式で表現されねばならない。

$$U = Se \cdot E^* \cdot Z^* \quad (7)$$

式 (7) は安全な状況 ( $Se = 1$ ) であって、エネルギー伝達系と供給系が正常な状態 ( $Z^* = 1, E^* = 1$ ) であるときのみ、出力エネルギー ( $U = 1$ ) が生成されることを意味し、出力エネルギー  $u$  の発生が安全情報  $Se$  を伴っていることを示す。

式 (7) は Fig. 2(a) のエネルギー伝達手段  $Z(e, h)$  が論理積  $Se \cdot E^*$  を行う論理積要素であることを示し、Fig. 2(b) で表されることを意味する (論理値として  $E^* = E$  であるから、 $Se \cdot E$  で表現している)。

いまここで、Fig. 2(a) のエネルギー伝達系は動力源を内部に持つものとし、Fig. 3 で示すように、安全

の条件  $h$  に対して出力  $u$  を発生する機能 ( $Ze(h)$ ) で表す) をもつ装置であるとする。この時、この装置の動作状態を  $Ze^* \in \{1, 0\}$  で表すと、この装置は動力源が故障したとき、このエネルギーを伝達する系が故障したときに関して、例えば  $Z^* = E^* \cdot Ze^* = 0$  (装置は故障時自ら内部にもつエネルギーを出力  $u$  として発生しない) が保証されねばならない。論理的には次式で表されねばならない。

$$U = Se \cdot Ze^* \quad (8)$$

式 (8) は、一般的装置に拡大して考える場合、エネルギー供給の形態が明確でなく、極めて煩雑となる (特に装置に電子回路が含まれる場合、この電源の供給形態は極めて多様である)。また、安全条件を  $Se$  とエネルギー供給  $E$  の論理関係が明確に表現されていない。このため、ここではエネルギー供給源とエネルギー伝達手段  $Z(e, h)$  は別系として式 (7) を定めている。

### 3.2 外部にエネルギー供給源を持つエネルギー伝達系

式 (7) は Fig. 2(b) で示したように、外部からのエネルギー供給を論理変数  $E$  (即ち情報) として扱っている。出力の発生をとくに次のように論理積で表すものとする。

$$U = Se \odot E \quad (9)$$

このとき、条件  $Se$  と  $E$  の間には次の 2 つの論理関係が成立しなければならない。

$$\text{条件 (1): } Se \geq U, \quad E \geq U \quad (10)$$

即ち、 $Se = 0$ 、又は  $E = 0$  であるとき  $U = 1$  を生じてはならない。

条件 (2): 式 (9) で示される論理積演算は、たとえこの演算を行う要素が故障状態にあっても、いずれか一方の論理値 1 の条件だけで出力  $U = 1$  を生じてはならない。この特性を持つ論理積をフェールセーフな論理積と呼ぶことにし、式 (9) で示すように論理積記号  $\odot$  で表現するものとする。

ここで  $\odot$  印で表される論理積  $A \odot B$  の意味を明確にしておく。

式 (4) で定義されるフェールセーフなエネルギー伝達は、エネルギー伝達手段  $F(Se)$  が故障した ( $F^* = 0$ ) とき  $U = 0$  を生じる特性を求めている。論理積  $A \odot B$

で定義されるフェールセーフ演算は、この演算要素の動作状態を  $F^* \in \{1, 0\}$  で表し、演算出力  $F(A, B)$  を  $F(A, B) = (A \odot B) \cdot F^*$  で表すとき、単に演算要素が故障 ( $F^* = 0$ ) したとき演算出力  $F(A, B) = 0$  を生じるだけでなく、さらに、故障があっても論理積  $A \cdot B$  が成立しないのに出力  $F(A, B) = 1$  を生じない (即ち、演算入力  $A, B$  のいずれか一方だけで出力が発生しない) 特性を持つことが要請されることを意味する。

上の条件 (1) の  $Se \geq U$  は Fig. 2(b) で安全情報  $Se = 0$  であるとき誤って Fig. 1 のスイッチ  $Sw$  を閉じてしまうことがないこと (ユネイト) を意味している。また、条件 (2) は「スイッチ  $Sw$  の電極間が溶着して、 $Se = 0$  であるにもかかわらず、 $E = 1$  時 (エネルギー供給源が正常 ( $E^* = 1$ ) であれば)  $U = 1$  が生じてしまう」か、あるいは、「 $E = 0$  のと (エネルギー供給源が故障している ( $E^* = 0$ )) であるとき  $Se = 0$  であるにもかかわらず人が別途エネルギー供給源を持ってきて  $U = 1$  を生ぜしめる」という事象が起こってはならないということの意味している。

外部のエネルギーを用いて安全情報に基づく制御が行われるエネルギー伝達系において、上の条件 (1)(2) が満たされるときフェールセーフであると呼び、上の条件 (1) または (2) のいずれかが満たされなときフェールセーフでないと呼ぶことにする。

Fig. 2(a) では、実際には安全の予測即ち安全情報の抽出は人によって行われる。この場合、人はたとえば目で小さなエネルギーとして抽出される安全情報  $Se$  をスイッチを開閉できるエネルギーに増幅していることになる。本来、抽出される安全情報  $Se$  と人の持つエネルギー発生源 (これを  $E_m$  とおけば) との間には、式 (7) に対応するスイッチ開閉の出力エネルギーが発生しなければならない。しかし、人は、誤りを含む。エネルギー発生源を含む人の機能を Fig. 3 に対応して  $Z_m(h)$  とおき、人が正常であるときを 1、正常でないときを 0 とする論理変数  $Z_m^*$  で表し、正常でないときの人の行動はスイッチを閉じる場合と閉じない場合が存在し、これをエネルギー供給あり (1)、なし (0) として論理変数  $E_m \in \{1, 0\}$  (人は 1 人とする) で表せば、人のスイッチ作業  $H_m$  は次式で表される。

$$H_m = Se \cdot Z_m^* \vee E_m \cdot \bar{Z}_m^* \quad (11)$$

式 (11) は人が正常 ( $Z_m^* = 1, \bar{Z}_m^* = 0$ ) であるとき、 $H_m = Se$  であり、人が正常でない ( $Z_m^* =$

0,  $\bar{Z}_m^* = 1$ ) 時、 $H_m = E$  であることを示す。

安全情報を外部エネルギーを用いてフェールセーフに伝達する系は式 (7) (Fig. 2(b)) で表すことができ、これを外部エネルギー ( $E$ ) をもつ増幅器として次式で表現するものとする。

$$U = E^*(Se) \quad (12)$$

式 (12) は外部エネルギー  $E$  をもつエネルギー伝達系によって安全情報  $Se$  が伝達されることを意味する。

#### 4. 外部エネルギーを用いる安全情報の伝達 (演算) 系

##### 4.1 フェールセーフ論理演算

ここで、 $n$  個の安全情報  $Se_i (i = 1, 2, \dots, n)$  を伝達する  $n$  個の出力  $U_i = E_i^*(Se_i) (i = 1, 2, \dots, n)$  を生ずる要素からなるエネルギー伝達系に関し、論理積および論理和による出力  $U_0$  を次式で定義する。

$$U_0 = E_1^*(Se_1) \odot E_2^*(Se_2) \odot \dots \odot E_n^*(Se_n) \quad (13)$$

$$U_0 = E_1^*(Se_1) \bigvee E_2^*(Se_2) \bigvee \dots \bigvee E_n^*(Se_n) \quad (14)$$

式 (13) は式 (9) の条件 (1)(2) と同様に定義される  $n$  個のフェールセーフな論理積を表し、式 (14) の記号  $\bigvee$  は論理和を表し、この論理和は  $n$  個の出力の中で、 $U_i = E_i^*(Se_i)$ ,  $i = 1, 2, \dots, n$  を出力する要素が故障するか又は  $Se_i = 0$  (安全でない) によって  $U_i = 0$  となっていない出力のみが伝達されることを意味する。

一般的エネルギー伝達系では複数のエネルギー供給源が利用される。たとえば各々異なる電源を有する複数の電磁リレーによって、複数の安全情報が伝達される場合である。この場合、電磁リレーはコイルを励磁する小さな電流を大きな接点電流に変換する増幅機能を含む。

式 (13) は、たとえば電磁リレーを使ったエネルギー伝達系 ( $n = 4$ ) として Fig. 4 で示すことができる。Fig. 4 で  $Se_1, Se_2$  は外部より接点で与えられる安全情報、 $E_1, E_2, E_3$  は外部より与えられるエネルギーとしての電源、 $CR_1, CR_2$  は電磁コイルと機械的接点で構成される電磁リレー、 $M$  はリレー接点による論理演算の結果  $U$  で駆動されるモータである。Fig. 4

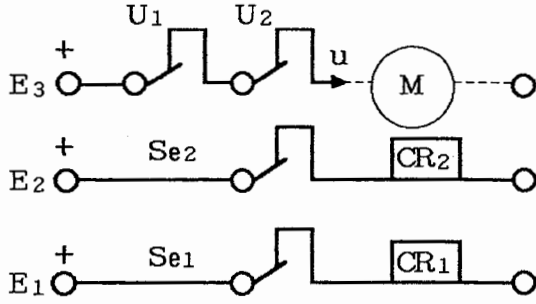


Fig. 4 Energy transmission by logic product  
論理積によるエネルギー伝達

は、接点入力  $Se_1$  と  $Se_2$  に対するリレー出力  $U_1, U_2$  の論理積出力  $U_1 \cdot U_2$  で、モータ  $M$  の駆動エネルギー（電流） $U$  が出力される。ここに、 $Se_1, Se_2, E_1, E_2, E_3, U_1, U_2$  は 2 値の論理変数として扱えるものとする。電磁リレーは後述するようなフェールセーフな構成であるとし、また接点は溶着しないものとする。と Fig. 4 は次式で与えられる。

$$U = \{(Se_1 \odot E_1 \cdot Z_1^*) \odot (Se_2 \odot E_2 \cdot Z_2^*)\} \odot E_3 \cdot Z_3^* \quad \therefore U = U_0 \odot E_3 \quad (15)$$

但し、

$$U_0 = (Se_1 \odot E_1 \cdot Z_1^*) \odot (Se_2 \odot E_2 \cdot Z_2^*) \odot E_3 \cdot Z_3^* \quad (16)$$

ここに  $Z_1^*, Z_2^*, Z_3^*$  は電線コイルと機械的接点（即ちリレー）で構成されるエネルギー伝達手段の動作状態、 $Z_3^*$  は出力  $U$  の発生する電線の動作状態を表す 2 値の論理変数である。

いま、Fig. 4 で、電源  $E_1, E_2$  が共通 ( $E_1 = E_2$ ) であるものとする。と、式 (16) は次の式 (17) で表現できる。

$$\begin{aligned} U_0 &= (Se_1 \cdot Z_1^*) \odot (Se_2 \cdot Z_2^*) \odot E_1 \cdot Z_3^* \\ &= Se_1 \odot Se_2 \odot E_1 \cdot Z_1^* \cdot Z_2^* \cdot Z_3^* \\ &= Se_1 \odot Se_2 \odot E_1 \cdot Z_{12}^* \cdot Z_3^* \\ &= E_1^* (Se_1 \odot Se_2) \end{aligned} \quad (17)$$

ここに、 $Z_{12}^* = Z_1 \cdot Z_2^*$  で、リレー  $CR_1$  と  $CR_2$  で構成されるエネルギー伝達系全体の動作状態を示し、 $CR_1$  系と  $CR_2$  系のいずれかが故障しても出力  $U_0$  が生じないことを意味する。また、 $(Se_1 \cdot Z_1^*) \odot (Se_2 \cdot Z_2^*) \odot E_1$

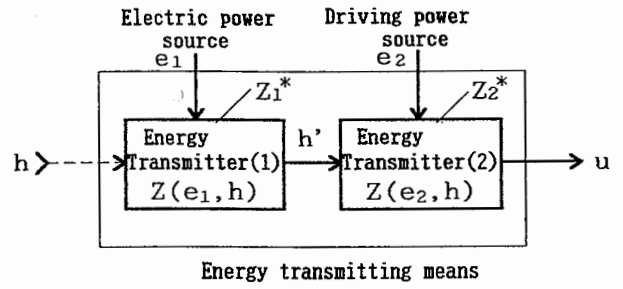


Fig. 5 Safety control system using sensor  
センサを用いた安全制御系

において、たとえば  $(Se_1 \cdot Z_2^*) \odot E_1$  は  $Z_2^* = 1, Z_2^* = 0$  が情報として生成され、 $Z_2^* \odot E_1$  としてフェールセーフな論理積演算でなければならないことを意味する。

式 (17) は共通のエネルギー源をもつ複数のエネルギー伝達系において、各々が式 (17) を満たすならば、入力  $Se_i$  に対するフェールセーフな論理演算を  $f(Se_i)$  とおき、この演算装置の動作状態を  $f^* \in \{1, 0\}$ 、電源を  $E$  とすれば、この時の出力は次式で与えられることになることを意味する。

$$\begin{aligned} U_0 &= f(Se_i) \odot E \cdot f^* \\ &= E^* (f(Se_i)) \end{aligned} \quad (18)$$

#### 4.2 外部エネルギーを用いるフェールセーフ論理演算の具体例

次に、異なる供給源を用いて、安全情報  $Se$  が順次伝達されるエネルギー伝達系について考察する。

Fig. 5 は安全を示す情報（エネルギー） $h$  を物理的に抽出して増幅出力  $h'$  を生成するセンサ（エネルギー伝達手段  $Z(e_1, h)$ ）と、この出力エネルギー  $h'$  が発生しているときのみ機械的出力エネルギー  $u$  を生成する手段  $Z(e_2, h')$  とから構成される一般的処理装置を示す。図で  $e_1$  はセンサ  $Z(e_1, h)$  の電源、 $e_2$  はエネルギー伝達手段  $Z(e_2, h')$  の動力源である。 $h_1, e_1, e_2, u$  を前述と同様に論理変数  $Se, E_1, E_2, U \in \{1, 0\}$  で表し、伝達手段  $Z(e_1, h), Z(e_2, h')$  の動作状態を  $Z_1^*, Z_2^* \in \{1, 0\}$  で表せば、出力は次の論理式で定まる。

$$\begin{aligned} U &= (Se \odot E_1 \cdot Z_1^*) \odot E_2 \cdot Z_2^* \\ &= E_2^* \{E_1^* (Se)\} \end{aligned} \quad (19)$$

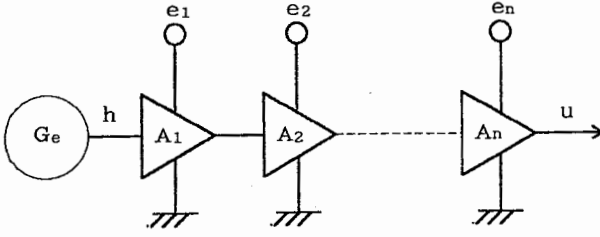


Fig. 6 Fail-safe AND circuit  
フェールセーフ論理積回路

即ち, Fig. 5 に示す安全装置は手段  $Z(e_1, h)$ ,  $Z(e_2, h')$  のいずれが故障しても出力  $U = 1$  を生じてはならないばかりでなく, 故障によって,  $Se = 0$  であるにもかかわらず, 外部エネルギー  $E_1 = 1$ ,  $E_2 = 1$  のいずれも  $U = 1$  として生成されてはならないことを示している。

著者らは増幅器 (光結合増幅器を含む) を従属接続し, この増幅器が正常であることを検査して出力を発生するフェールセーフな論理積回路を開発している (演算発信器と呼ばれる<sup>4,5)</sup>). Fig. 6 はこの構成原理を示し,  $A_1, A_2, \dots, A_n$  は増幅器,  $Ge$  は増幅器  $A_1, A_2, \dots, A_n$  の動作状態  $A_1^*, A_2^*, \dots, A_n^* \in \{1, 0\}$  を検査する検査信号発生器 (交流信号発生器),  $e_1, e_2, \dots, e_n$  は増幅器  $A_1, A_2, \dots, A_n$  の電源で, ここでは論理演算の入力信号である。即ち, 入力信号  $e_1, e_2, \dots, e_n$  のすべてがあるときのみ出力  $u$  が生成される。検査信号  $h$  が出力  $u$  として生成されるとき増幅器  $A_1, A_2, \dots, A_n$  は正常であることを意味し, 増幅器のいずれか 1 つでも故障して出力エネルギー  $u$  を発生することがないので, この信号  $h$  に対する出力  $u$  の発生は (入力信号  $e_1, e_2, \dots, e_n$  が安全を示す情報であれば, この論理積出力として) 安全を意味する。ここで, 検査信号  $h$  及び入力信号  $e_1, e_2, \dots, e_n$  と出力  $u$  を各々論理変数  $Se, E_1, E_2, \dots, E_n, U \in \{1, 0\}$  とおくと,

$$U = (Se \odot E_1 \cdot A_1^*) \odot E_2 \cdot A_2^* \odot \dots \odot E_n \cdot A_n^* \quad (20)$$

である。即ち, 検査信号発生器  $Ge$  が故障したとき検査信号  $h$  は生成されないから, 検査信号発生器の動作状態を  $Ge^* \in \{1, 0\}$  とおけば,  $Ge^* = Se$  であり, 電源入力  $E_1, E_2, \dots, E_n$  を論理入力とすると, Fig. 6 の増幅器はフェールセーフな論理回路として次式で

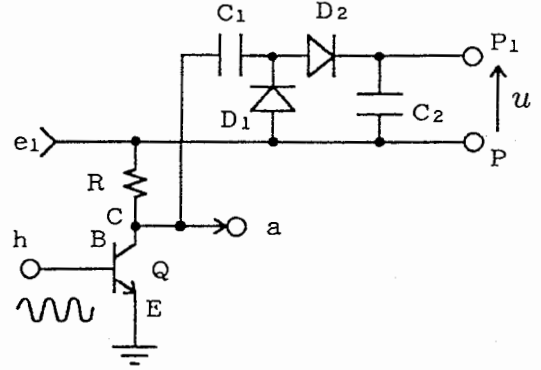


Fig. 7 Realization of  $V = Se \odot E_1 \cdot Z^*$  in electronic circuit  
電子回路における  $V = Se \odot E_1 \cdot Z^*$  の実現

表される。

$$U = E_1 \odot E_2 \odot \dots \odot E_n \cdot A_z^* \quad (21)$$

但し,

$$A_z^* = Ge^* \cdot A_1^* \cdot A_2^* \cdot \dots \cdot A_n^*$$

ここに  $A_z^*$  は検査信号発生器  $Ge$ , 及び増幅器のいずれが故障しても  $A_z^* = 0$  となることを示す。

## 5. 出力生成要素

式 (7) で示される安全情報  $Se$  に対応する出力エネルギー  $U$  は,  $Se = 0$  のとき外部エネルギー  $E$  が  $U = 1$  として生成されない構成が要求される。通常, 情報  $Se$  は物理的にはセンサ入力として小さなエネルギーで発生するので, Fig. 4, 5 で示すように, 増幅によるエネルギー伝達過程が存在し, このエネルギー伝達には電磁リレーや電子回路が利用される。

### 5.1 電子回路によるユニタなエネルギー伝達

通常, 電子回路による出力は, 故障時増幅のための電源が直接出力されるか, 又は出力零となる特性 (対称誤り特性) を持つ。Fig. 7 の抵抗  $R$  とトランジスタ  $Q$  で構成される増幅回路は, トランジスタ  $Q$  のコレクタ  $C$  が断線すると, たとえベース ( $B$ ) 側に入力電圧 ( $h = 1$ ) が印加されていなくても電源  $e_1$  が端子  $a$  に出力され, また, コレクタ  $C$  とエミッタ  $E$  が短絡すると出力は零レベルとなる (即ち, 対称誤り特性を示す)。このため, 例えば Fig. 6 における出力信号 (エネルギー)  $u$  のように, トランジスタのベース側に入力される信号  $h$  は交流信号安全情報には交流信号があるときを 1, ないときを 0 とする), この増幅

された出力信号（改めて  $u$  とおく）はコンデンサ  $C_1$ ,  $C_2$  とダイオード  $D_1$ ,  $D_2$  で構成される倍電圧電流回路を用いて外部から供給される電源  $e_1$  に重畳して出力される。端子  $P_1$ ,  $P_2$  の出力  $u$  は、安全情報  $h$ （交流）があるとき発生し、ないとき発生しない。このように、増幅された出力エネルギーを増幅のために供給された電源  $e_1$  に重畳して出力することによって、電源を含む外部環境の出力レベルより高いレベルで出力  $u$  が発生し、出力端子  $P_1$  には図の回路を構成する要素にいかなる故障があっても、入力  $h$  がないのに電源  $e_1$  より高レベルの出力が生成され得ない構成としている（電源枠外処理と呼ぶ<sup>6)</sup>）。即ち、入力  $h$ （交流） $\in \{1, 0\}$  を論理変数  $Se$  で表し、図の回路の動作状態と電源  $e_1$  と出力  $u$  を論理変数  $Z^*, E^*, U \in \{1, 0\}$  に置き換えれば、出力  $U$  は式 (7) で表せる。

## 5.2 出力遮断の論理（ブレーキ系）

Fig. 2(a) あるいは Fig. 4, Fig. 7 で示したエネルギー伝達系は、入力情報  $h$  又は外部から供給されるエネルギーが消滅したとき、出力  $u$  がエントロピ増大則にしたがって（即ち、熱となって）消費される系である。しかし、現実の出力エネルギーの遮断では、この熱消散では間に合わない場合が存在し、強制的遮断を伴う。

いま、機械の駆動エネルギーを  $\psi$ 、この駆動エネルギーによって実際に出力される機械出力を  $\omega$ 、機械出力  $\omega$  を強制的に停止するためのエネルギーを  $\chi$  とおく。ここに、 $\chi > \psi$  であるが、 $\omega$  と  $\chi$  の大小関係は運転時の蓄積エネルギーを含む出力エネルギー  $\omega$  と強制停止時のエネルギー消散を配慮した停止エネルギー  $\chi$  を考えねばならず、ここでは単純に  $\chi > \omega$  とおく。また、運転—停止の間の過渡状態が存在するが、ここでは運転、停止の論理的条件を考察するので無視する。出力エネルギー  $\omega$  の投入及び遮断を論理的に考察するために、上の夫々のエネルギーの有無を 1 と 0 とする 2 値の論理変数で表すものとし、上のエネルギー  $\psi$ ,  $\omega$ ,  $\chi$  に対応する論理変数を夫々  $Y$ ,  $Z$ ,  $X$  とおく。 $Z = 1$  は運転中、 $Z = 0$  は停止状態である。この時、 $Y$ ,  $X$ ,  $Z$  の間には少なくとも Table 2 で示す論理的関係が成立する。Table 2 で  $X = 1$ ,  $Y = 1$  は停止エネルギーと駆動エネルギーが同時に印加された状態でこの時の  $Z = 0$  は制動エネルギーあり ( $X = 1$ ) を優先させて停止状態とすべきことを意味している。通常  $\chi > \psi$  を与えるエネルギー  $\chi$  は大きなエネルギーとなる（たとえば非常停

Table 2 Logic relation for output interruption  
出力遮断の論理的関係

| $X$ | $Y$ | $Z$ |
|-----|-----|-----|
| 0   | 0   | 0   |
| 1   | 0   | 0   |
| 0   | 1   | 1   |
| 1   | 1   | 0   |

Table 3 Condition  $Z$  of machine operation  
機械の運転  $Z$  の条件 ( $Z = Se \cdot Y$ )

| $Se \backslash Y$ | 1 | 0 |
|-------------------|---|---|
| 1                 | 1 | 0 |
| 0                 | 0 | 0 |

止手段として) ので、通常このとき駆動エネルギーを遮断 ( $\psi = 0$ ) とする。この場合  $X = 1$ ,  $Y = 1$  は誤り状態と解釈される。 $X = 0$ ,  $Y = 0$  の状態は俗に言うブラの状態であり、何らかの誤りによって外部エネルギー（一種のノイズ）が印加されると  $Z = 1$  を生じやすい。このため、 $X = 0$ ,  $Y = 0$  の状態を避けて停止時は  $X = 1$ ,  $Y = 0$  の状態に保たれる。したがって、機械の運転は通常 Table 3 に点線を囲った部分の論理構成となる。

$X = 1$ ,  $Y = 0$  の停止状態から、 $X = 0$ ,  $Y = 1$  の運転状態に入る、あるいは運転状態  $X = 0$ ,  $Y = 1$  から停止状態  $X = 1$ ,  $Y = 0$  に戻るには、( $X = 1$ ,  $Y = 0$ )  $\rightarrow$  ( $X = 0$ ,  $Y = 0$ )  $\rightarrow$  ( $X = 0$ ,  $Y = 1$ ) の過程を経なければならない。停止状態  $X = 1$ ,  $Y = 0$  と運転状態  $X = 0$ ,  $Y = 1$  の間には  $X = 1 \rightarrow X = 0$  と  $Y = 0 \rightarrow Y = 1$  の相互に論理的否定のエネルギー伝達を必要とし、 $Y \geq Z$  であるが  $X \geq Z$  でない<sup>7)</sup>。表で常に  $X = 0$  とする条件で駆動側  $Y$  を許可 ( $Se$ ) に基づく出力 ( $U$ ) とすれば熱消散系となる。ブレーキ系として駆動側  $Y$  を別途与えるものとし、停止側  $X$  を許可  $Se$  に基づいて供給すれば、ノーマル・オープンブレーキ系となる。この場合、入力許可  $Se$  と停止のためのエネルギー  $\chi$  の間には論理的否定が必要で（即ち  $X = \bar{Se}$ ）、ユニタリなエネルギー伝達とならない（フェールセーフとならない）。このため、たとえば Fig. 7 に示すようなノーマル・クローズタイプのブレーキ構造とする。

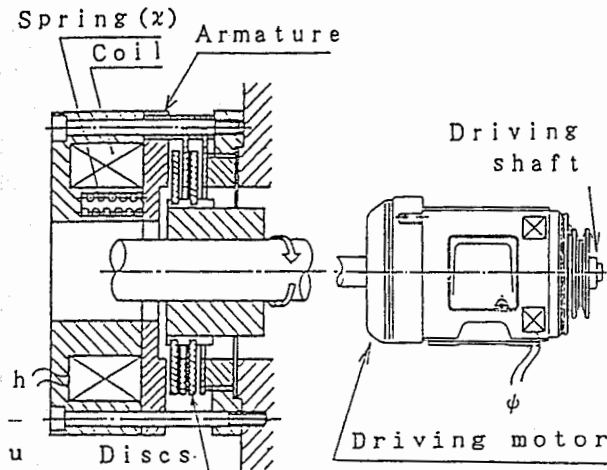


Fig. 8 Electromagnetic brake (normally closed)  
電磁ブレーキ（ノーマル・クローズ形）

Fig. 8 は常時バネ（このエネルギーを $\chi$ とおく）によってブレーキが閉成され、モータはブレーキ開放のためのエネルギー $u$ が供給されているときのみ、駆動エネルギー $\psi$ によって回転出力 $\omega$ を発生する構成である。論理値  $X = 0$  の状態はブレーキ開放エネルギー $u$ が停止時バネの持つエネルギー $\chi$ に重畳することによって実現し、論理的に  $Y \geq Z$  であると共により、ブレーキ開放エネルギーの有無を 1 と 0 とする論理変数  $Se$  で表せば、 $Se \geq Z$  となる。ここにバネエネルギー $\chi$ はエネルギー出力として消滅しない ( $\chi \neq 0$ ) 構造が要求される。Table 3 は停止入力  $Sec$  と駆動入力  $Y$  の論理的関係を示す真理値表で、 $Se = Y = 1$  の時のみ出力  $Z$  を生じ次式となる。

$$Z = Se \cdot Y \quad (22)$$

ここに、停止入力  $Se$  は運転許可の情報に基づき、 $Y$  は運転命令に基づくから、Fig. 8 はインタロックを構成していることになる。

### 5.3 電磁リレー

エネルギー遮断のために大きなエネルギーを得るためには、増幅機能をもつ要素が不可欠となる。Fig. 9 は小さな入力によって大出力（電流） $u$  を遮断するための電磁リレーを示す。入力エネルギー $h$ と出力エネルギー $u$ の間には論理的に  $Se \geq U$  の関係が維持されねばならない。Fig. 8 と同様に接点を確実に OFF 状態に保つためのバネエネルギー $\chi$  (Table 3 における  $X = 1$  に相当) が必要で、このバネは故障しない

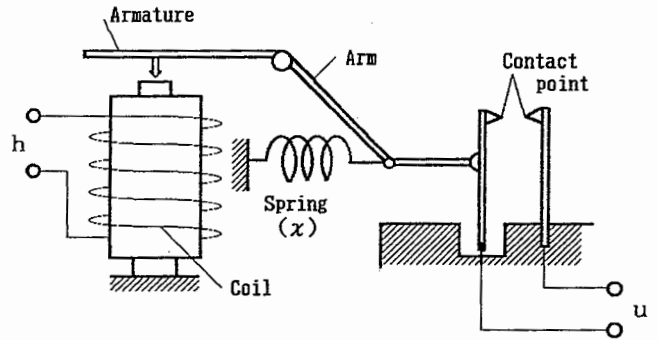


Fig. 9 Electromagnetic relay  
電磁リレー

( $X \neq 0$ ) ことを条件とする。このため、出力電流 ( $u$ ) はバネを流れる構成とすれば、バネが折れたとき出力電流  $u$  は発生しない構成となる。そして、バネのエネルギーに重畳して電磁コイルから接点を ON 状態にするためのエネルギーが供給される。

## 6. 結 言

安全確認過程としての安全の原理を示し、ここで必然的に不可欠となる安全情報伝達のユニタ性を機械系を含む増幅過程の論理として明らかにした。即ち、センサによって抽出される安全情報（安全を示す情報）は、安全であるときのみ出力されるエネルギーとして増幅される必要があり、この増幅には外部からエネルギーが別途供給されねばならず、このためのエネルギーと抽出される安全情報の論理的関係を論理積モデルで示した。そして、このモデルは具体的フェールセーフ演算処理に適用できることを示した。また、フェールセーフな出力エネルギー発生手段は、外部から供給されるエネルギーに安全情報が重畳されることによって、上述の論理積モデルが実現されることを示した。

### 謝 辞

本論文では、すでに日本機械学会論文集（C 編）56 巻 530 号（1990 年 10 月）及び JSME International Journal に掲載した「安全制御系における安全情報のエネルギー伝達 (Energy for Safety Information Transmitted in Safety Control System)」基本とし、新しい知見を加えて当研究所報告としてまとめたものである。なお、まとめるに当たり、共著者であ

る日本信号の蓬原弘一氏から快く承諾をいただいた。  
心からの謝意を表する。

(平成 5 年 6 月 1 日受理)

#### 参 考 文 献

- 1) 杉本, 蓬原, 向殿, 制御としての安全 (安全制御) に関する一考察, 日本ロボット学会第 5 回学術講演会予稿集 2601 (昭 63-10), pp. 359-362.
- 2) 蓬原, 杉本, 向殿, フェールセーフ技術, 日本ロボット学会第 6 回学術講演会予稿集 1301 (昭 62-11).
- 3) 蓬原, 杉本, 安全確認作業システムの論理的考察, 機構論投稿中 (平元-10) .
- 4) 土屋, フェイルセーフ論理方式の研究, 電気試験所研究報告 No. 695 (昭 41-1), pp. 19.
- 5) 蓬原, 杉本, 向殿, 事故防止の考え方と安全装置の試作, 電子情報通信学会報告 EMCJ89-55 (平元-11).
- 6) 蓬原, 向殿, レール短絡を使った列車検知用フェールセーフセンサの特性と構造, 電学論 C, Vol. 7, No. 10 (昭 63), pp. 995.
- 7) 杉本, 蓬原他, 安全確認型安全の基本構造, 機構論 505-C (昭 63-6).