窓特性をもつフェイルセーフ論理素子を使った インタロックシステムの一構成法

正 員 蓬 原 弘 一 (日本信号)

正 員 向 殿 政 男 (明治大)

1. はじめに

機械間で衝突の起こる危険がある場合、これを防ぐために通常インタロックを設ける必要がある。鉄道信号システム⁽¹⁾やプレス機械制御⁽²⁾では古くからこのインタロックが利用され、安全を確保するための重要な機器構成技術とされてきた。しかし、インタロックの考え方や具体的構成法について、現在までのところ統一的な考察は行われていない。

インタロックは「誤動作を防止するために、複数の機器間に機械的あるいは電氣的連絡を設けること⁽³⁾」、あるいは「関連のある機器の間に電氣的または機械的連絡を設け、相手方の機器が正常な状態にあるときのみ操作が行われる機器構成⁽⁴⁾」と定義されている。一方、インタロック自身を電子回路を用いて実現する場合、電子回路の故障により、通常必らずしも安全を確保できないときがある。本論文では、単に誤動作を防止するために機器間に連絡を設けて安全を確保する従来のインタロックの定義に加えて、安全機構自身が故障したときにも、常に安全側になるように構成されているフェイルセーフなインタロックについて述べる。

このため、次章でまずフェイルセーフシステムとインタロックシステムについて考察する。次に、フェイルセーフなインタロックを構成するために必要な基本要素を示す。すなわち、基本要素としてフェイルセーフな AND ゲートと否定演算機能を有するフェイルセーフなセンサとが必要なことを示す。ところが、2 値

の否定演算は原理的にフェイルセーフに実現できない。このため、第3章でアナログ信号に対してしきい値演算を行って否定の信号を抽出するフェイルセーフな演算素子（ウィンドウ・コンパレータ）を提案する。第4章では、フェイルセーフなウィンドウ・コンパレータの構成法と実現例を示し、これを用いてフェイルセーフな AND ゲートも実現できることを示す。また、フェイルセーフなウィンドウ・コンパレータ自身も、出力を出す条件として自ら回路を検査して結果を生成するフェイルセーフなインタロックの構造となっていることを示す。

2. インタロックシステム

まず、対象とするフェイルセーフシステムを示し、ここで必要とするインタロックの構成条件と基本要素を明らかにする。

〈2・1〉 対象とするシステムのモデル いま、独立する二つの入力信号 $x_a, x_b \in \{1, 0\}$ に対して処理 $h_a(x_a), h_b(x_b)$ を行って各々 2 値出力 $f_a, f_b \in \{1, 0\}$ を生成する二つの機械（装置） N_a, N_b を考える（図 1(a)）。この機械 N_a, N_b は 2 値の出力 $f_a=1$ または $f_b=1$ のエネルギーによって機械可動部を動かし、危険作業（衝突を伴う作業）を作業領域 C で行うものとする。具体的には、例えば 2 台のロボットが各々アームを動かして共通の作業台にワークを搬入して戻る作業、あるいは列車を交互に共通の制御領域（閉そく区間）に進入させて退出させるまでの作業などに相当する。

二つの機械 N_a, N_b の可動部が交互に衝突しないで作業を行うためには、各々の作業出力 $f_a=1$ または $f_b=1$ は相手方の作業が終ってから発生しなければならない。このため、二つの機械間に順序付けのための連絡⁽³⁾（インタロック）を設ける必要が生じる⁽⁵⁾。図 1(b)はこのインタロックを備えた機械システムの構

A Method for Constructing Interlock System Using Fail-Safe Logic Device with Window Characteristics. By Koichi Futsuhara, Member (Nippon Signal Co.) & Masao Mukaidono, Member (Meiji Univ.).

蓬原弘一：正員，日本信号（株）研究開発部

向殿政男：正員，明治大学工学部電子通信学科

図 1 インタロックシステムのモデル
Fig. 1. Interlock system model.

成のモデルを示す。図 1(b)で、機械 N_a は入力信号 x_a に処理 h_a を施した結果を x_{ba} が 1 のときのみ f_a として出力し〔図 1(b)ではこれを AND ゲート G_a で表す〕、機械 N_b は入力信号 x_b に処理 h_b を施した結果を x_{ab} が 1 のときのみ f_b として出力する。ここに、 $x_{ab} \in \{1, 0\}$ は機械 N_a から N_b に伝達される機械 N_a の作業終了信号、 $x_{ba} \in \{1, 0\}$ は機械 N_b から N_a に伝達される機械 N_b の作業終了信号で、1 は作業終了を 0 は作業未終了を意味するものとする。こうすると x_{ab} は出力 f_a が 0 になったとき 1 を発生し、 x_{ba} は出力 f_b が 0 になったとき 1 を発生しなければならない。また、出力 $f_a=1$ と $f_b=1$ は現実には危険を伴う作業を行う出力状態であるから、0 であるべきとき、1 に誤ってはならない。これは後述するように、1 をエネルギーの高い状態に対応させ、故障は必ずエネルギーが低くなるという物理事象を利用して初めて実現される。よって $f_a=1$ と $f_b=1$ は、論理レベルとして高エネルギー状態、 $f_a=0$ と $f_b=0$ は低エネルギー状態（または零）でなければならない。また、 x_{ab}, x_{ba} も同様に、 $x_{ab}=1, x_{ba}=1$ を高エネルギー状態の論理レベル、 $x_{ab}=0, x_{ba}=0$ を低エネルギー状態の論理レベルとする論理変数でなければならない。

さて、上記のインタロックがフェイルセーフである、すなわちインタロックのために導入した機器自身が故障しても機械 N_a, N_b の可動部が誤って衝突しないためには、次の二つの条件を必要とする（衝突回避条件）。

(i) 機械 N_a, N_b の出力は、それぞれ $f_b=1$ のとき $f_a=1$ を、または $f_a=1$ のとき $f_b=1$ を誤って生成しないこと。

(ii) 作業終了を意味する信号 x_{ab}, x_{ba} は、それぞれ $x_{ab}=0$ であるべきとき $x_{ab}=1$ に、また $x_{ba}=0$ であるべきとき $x_{ba}=1$ に誤ってはならないこと。

ここで、フェイルセーフ処理を厳密に定義しよう。入力信号 x に対して信号処理 $h(x)$ を行う一般的処理機械 N の動作状態を論理変数 $N^* \in \{1, 0\}$ で表し、1 を正常動作状態、0 を故障状態とすると、機械 N の出力 f が次式で表される処理をフェイルセーフな処理と定義する⁽⁶⁾。

$$f = h(x) \cdot N^* \dots\dots\dots (1)$$

(以後、処理機械（システム）またはこの構成要素の動作状態を表す論理変数に * 印を付し、正常時を 1、故障時を 0 とおく)

上述の衝突回避条件 (i) は信号 x_{ab}, x_{ba} に誤りがないものとすれば、フェイルセーフな信号処理として出力 f_a, f_b が次式で出力されればよい。

$$f_a = h_a(x_a) \cdot x_{ba} \cdot G_a^* \dots\dots\dots (2)$$

$$f_b = h_b(x_b) \cdot x_{ab} \cdot G_b^* \dots\dots\dots (3)$$

よって故障時出力 0 であるべきとき、誤って 1 を発生しないようなフェイルセーフな AND ゲートを必要とすることがわかる。

さて、一方作業終了信号 x_{ab}, x_{ba} は各々対応する機械出力 f_a, f_b が 0（例えば出力電流零）になったとき 1 にならなければならない、すなわち否定演算が必要となる。

一般に x_{ab}, x_{ba} を得るには、例えば f_b, f_a をセンサで検出する必要がある。ところが、 $f_b=1, f_a=1$ であることをセンサで検出してから、否定演算を施したのでは、センサおよび否定回路がともにフェイルセーフであっても衝突回避条件 (ii) は実現できない。なぜならば、センサの処理回路と否定演算回路の動作状態を各々 $S^*, N_0^* \in \{1, 0\}$ とすれば、例えば x_{ab} は

$$x_{ab} = \overline{f_a} \cdot S^* \cdot N_0^* = (\overline{f_a} \vee \overline{S^*}) \cdot N_0^* \dots\dots\dots (4)$$

となる。よって、センサが故障して 0 になると $f_a=1$ のとき、否定演算回路に誤りがなければ、 $x_{ab}=1$ となって条件 (ii) は満足されない（このことについては、第 3 章で詳述する）。以上により、フェイルセーフなインタロックを実現するためには、フェイルセーフな AND ゲートと共に、否定機能を含んだフェイルセーフなセンサも必要であることがわかる。

〈2・2〉 フェイルセーフインタロックの構成方法

フェイルセーフなインタロックであるためには、前述のとおり衝突回避条件として信号 $x_{ab} \in \{1, 0\}$ および $x_{ba} \in \{1, 0\}$ をフェイルセーフに抽出することが必要である。

従来、構成容易なインタロックの方法として、作業終了信号 x_{ab}, x_{ba} は可動部の状態を表す論理変数として、出力 $\bar{f}_a, \bar{f}_b$ を直接検出する代わりに、危険な可動部が作業領域 C で作業を終了して確かに元（作業領域 C の外であるので C^c で表す）に戻ったことを検出して得ているのが通例である。この信号発生の実確な方法として、直接センサで戻りの可動部を検知し、この出力信号を衝突回避条件 $x_{ab}, x_{ba} \in \{1, 0\}$ としている。このときセンサの出力信号 x_{ab}, x_{ba} （第一のセンサ出力と呼ぶことにする）は次の特性をもたねばならない。

(1) 論理値 1, 0 は可動部の状態を検知して次のように表す。

- 1……作業領域 C^c に可動部が存在する
- 0……作業領域 C^c に可動部が存在しない

(2) センサは故障時 1 側出力の誤りが許されない。

一方、 x_{ab}, x_{ba} を得るもう一つの方法として、作業領域 C に衝突回避のためのセンサを設け、相手方可動部が存在しないことを直接検出して衝突回避を行うことが考えられる。この出力信号（衝突回避条件）を前述の方法と区別するために $x'_{ab}, x'_{ba} \in \{1, 0\}$ と記すことにする。この場合の相手方可動部が、作業領域 C に存在しないことを検知するセンサの出力信号 x'_{ab}, x'_{ba} （第二のセンサ出力と呼ぶことにする）は、次の特性をもたねばならない。

(1) 論理値 1, 0 は可動部の状態を検知して次のように表す。

- 1……作業領域 C に可動部が存在しない
- 0……作業領域 C に可動部が存在する

(2) センサは故障時 1 側出力の誤りが許されない。

上記二とおりの検出方法には根本的相違がある。それは機械 N_a, N_b とは別に、機械 N_a, N_b と同様の可動部をもつ第三の機械 N_c が存在し、この可動部が誤って作業領域 C または C^c に進入することがある（雑音が存在すると考えることができる）場合である。上述の第一のセンサ出力 x_{ab}, x_{ba} は、検知対象となる機械 N_a, N_b の代わりに、機械 N_c の可動部が検知されても論理値 1 を生じる。例えば、検知対象となる機械 N_a の可動部が作業領域外 C^c に存在するときを $\bar{f}_a \in \{1, 0\}$ （可動部は領域 C^c または C のいずれかに存在するものとし、機械 N_a の可動部が作業領域 C に存在しないときを $\bar{f}_a = 1$ とする）で表せば、センサが正常動作状態にあるときのセンサの出力特性は次の論理式で表すことができる。

$$x_{ab} \geq \bar{f}_a \quad \dots\dots\dots (5)$$

すなわち、 $\bar{f}_a = 1$ でも $x_{ab} = 1$ ということがあり得る。

一方、第二のセンサ出力 x'_{ab}, x'_{ba} は検知対象となる機械 N_a, N_b の可動部の代わりに、機械 N_c の可動部が検知されても論理値 0 となる。例えば、同様に対象とする機械 N_a の可動部の作業領域 C における不在を $\bar{f}_a$ とすれば、センサが正常動作状態にあるときのセンサの出力特性は次の論理式で表すことができる。

$$x'_{ab} \leq \bar{f}_a \quad \dots\dots\dots (6)$$

(6) 式は「状態 $\bar{f}_a = 1$ に対して検知出力 x'_{ab} は論理値 0 に誤ることはあっても、 $\bar{f}_a = 0$ のとき論理値 1 に誤らない」というフェイルセーフ論理演算の基礎的条件⁽⁷⁾を満たしている。しかし、(5) 式における状態 $\bar{f}_a$ とその検知出力信号 x_{ab} の関係は、このフェイルセーフ論理の基礎的条件を満たしていない。なお、この場合、(5) 式または (6) 式で出力信号が示されるセンサは、単に機械 N_a の可動部を検知するだけでなく、各々領域 C^c または C の作業環境を監視していることになる。

いま、作業領域 C および作業領域外 C^c の環境状態が正常でない（機械 N_a, N_b 以外のものが存在する）ことを表す論理変数を $D^*, D_c^* \in \{1, 0\}$ で表し、作業環境に検知誤りを起こす対象物（一種の雑音とも解釈できる）が浸入しているときを 1、浸入していないときを 0 とする。信号 x_{ab}, x'_{ab} を出力するフェイルセーフなセンサの動作状態を各々 S_a^*, S_b^* とおくと、(5)、(6) 式に対応するセンサ出力 x_{ab}, x'_{ab} は次式となる。

$$x_{ab} = (\bar{f}_a \vee D_c^*) \cdot S_a^* \quad \dots\dots\dots (7)$$

$$x'_{ab} = \bar{f}_a \cdot \bar{D}_c^* \cdot S_b^* \quad \dots\dots\dots (8)$$

(7) 式は作業環境が正常でないときには誤り出力 $x_{ab} = 1$ となり、フェイルセーフにシステムを構成することができないことを意味している。これに対して (8) 式は作業環境が正常でない場合でも、このとき $x'_{ab} = 0$ の誤りとなり、センサがフェイルセーフ構成であれば、フェイルセーフなシステムを構成できることを意味している。

〈2・3〉 インタロックの基本構成 以上の例では、図 1(b) における信号 x_{ab}, x_{ba} と x'_{ab}, x'_{ba} とは異なった機構で与えられるが、出力 f_a, f_b の否定を直接センサで検出する場合も含めて、これらの信号はいずれも作業領域 C の安全状態を 1、危険状態を 0 としている。すなわち、出力発生の許可信号 $I_s \in \{1, 0\}$ を安全状態を示すとき 1、危険状態を示すとき 0 をとる論理変数とすると、インタロックは結局図 2 のように表現することができる。

図2 インタロックの基本構成
Fig. 2. Basic construction of interlock system.

図2は機械の出力命令 $\hat{M} \in \{1, 0\}$ の出力 $f \in \{1, 0\}$ がセンサ S で与えられる許可信号 $I_s \in \{1, 0\}$ に基づいて発生する構成である。この構成をインタロックの基本構成と呼ぶことにする。ANDゲート G は図1(b)のゲート G_a, G_b 、機械の命令 $\hat{M}$ は処理 $h_a(x_a), h_b(x_b)$ の出力信号、 I_s は(7)式または(8)式で与えられる出力信号に対応している。図1(b)で処理 $h_a(x_a), h_b(x_b)$ の入力信号 x_a, x_b に誤りが起こると出力 f_a, f_b に誤り出力が生じる。しかし、インタロック(許可信号 $I_s=1$)によって作業領域 C の安全が保証されるので、たとえ誤り出力 f_a, f_b が生じても機械 N_a, N_b の可動部間の衝突は起こらない。

以上により、図2で示すフェイルセーフインタロックの基本構成は、前述したようにセンサが(8)式に基づき、以下の特性をもたなければならない。

(1) 命令 $\hat{M}$ には誤りが許されるがセンサ S による許可信号 I_s には、 $I_s=0$ であるべきとき $I_s=1$ の誤りが許されない(フェイルセーフセンサ)。

(2) ANDゲート G には $f=0$ であるべきとき、 $f=1$ となる誤りの出力が許されない(フェイルセーフANDゲート)。

なお、センサ S が(8)式に基づく場合、機械(N_a, N_b)は出力 f を発生してよいか否かセンサ S で自ら作業領域(C)を検査し、検査結果としての許可信号 $I_s (=1)$ が発生するときのみ、出力 $f (=1)$ を生じるインタロックで、これを自己確認形インタロックと呼ぶことにする。もし、センサ S が(7)式に基づくならば、自ら検査を行う構造にならず、相手方機械に依存して一方的に許可信号が与えられる構成となり、このインタロックを相互インタロックと呼ぶことにする。

3. フェイルセーフセンサ

フェイルセーフなインタロックシステムは前述したように、自己確認形インタロックに基づかなければならない。この場合のセンサ出力 $I_s \in \{1, 0\}$ の一般的発生方法を考察する。

いま、許可信号 I_s の論理レベルとして1を高エネルギー状態、0を低エネルギー状態(零)とし、センサ S の入力信号を $e \in \{1, 0\}$ とおく。入力信号 e の1は危険発生を0は安全状態を意味するものとすれば、

表1 センサの出力特性
Table 1. Sensor output property.

e	I_s
0	1
1	0

図3 否定機能をもつセンサの構成方法
Fig. 3. Construction method of sensor including NOT operation.

表1で示すように、センサ S は否定演算機能を含まねばならない。図3(a), (b)はこのセンサの構成例を示す。 $u(e), u(\bar{e})$ は否定演算機能を含まないセンサ機能、NOTは否定演算機能を表すものとする。(a)図はセンサで信号 e を抽出して後に否定演算を行っており、センサの処理機能 $u(e)$ の回路の動作状態を u^* 、否定演算回路の動作状態を N_0^* とすれば前述したように[(4式)], 出力信号 I_s は次式で表される(「は否定記号)。

$$I_s = (u(e) \cdot u^*) \cdot N_0^* = (\bar{e} \vee u^*) \cdot N_0^* \cdots (9)$$

ここに、 u^* は処理 $u(e)$ を行う回路の正常状態の否定を表す。(9)式はこの否定出力により、センサが故障すると否定回路が正常であれば $I_s=1$ の誤りを起こし、フェイルセーフ構成とはならないことを意味している。

(b)図はまず否定演算を行って後、この出力信号 $\bar{e}$ が処理回路(u)に入力されており、処理 $u(\bar{e})$ の回路の動作状態を u^* とおくと、出力信号 I_s は次式で表される。

$$I_s = u(\bar{e} \cdot N_0^*) \cdot u^* = \bar{e} \cdot N_0^* \cdot u^* \cdots (10)$$

(10)式はセンサが $\bar{e}$ を直接抽出できる場合に相当しており、この場合にはセンサをフェイルセーフに構成できれば、フェイルセーフなインタロックを構成することができる。

一般にはセンサの入力信号 e は2値信号でなくアナログ信号である。センサはこれを2値信号に変換する役目も担わなければならない。

アナログ信号から図3(b)に対応する否定出力を直

接抽出するには、センサはあるしきい値 (e_t とおく) をもち、この機能は次のように表すことができる。

$$u(\bar{e}) = 1 \cdots \cdots e \leq e_t \text{ のとき} \\ 0 \cdots \cdots e > e_t \text{ のとき}$$

しかし、アナログ信号の発生や伝達回路に故障が生じると $e=0$ が起こる。これらの故障は図 3(b)における否定回路の故障に相当し、この場合には $\bar{e} \cdot N^* = 0$ でなければならないが、上の定義では $u(\bar{e})=1$ となってしまう、フェイルセーフの条件[(1)式]を満足しない。よって、もう一つのしきい値 $e_0 (e_0 < e_t)$ を定め、論理値 1 のレベルを e_0 と e_t の間に設定して、上述のセンサ機能は次のように表されねばならない。

$$u(\bar{e}) = 1 \cdots \cdots e_0 \leq e \leq e_t \text{ のとき} \\ 0 \cdots \cdots e > e_t, \text{ または } e < e_0 \text{ のとき}$$

以上により、フェイルセーフインタロックのセンサには、次章で述べるようなしきい値をもつフェイルセーフなウィンドウ・コンパレータが必然的に必要となる。

4. 入力に窓をもつフェイルセーフ論理素子

〈4・1〉 ウィンドウ・コンパレータの定義 ウィンドウ・コンパレータ (以下、WC と略記) は、入力レベル x に対して二つの異なるしきい値 $V_H, V_S (V_H > V_S)$ をもち、この二つのしきい値間の内側と外側で異なる論理値の 2 値出力 $F(x) \in \{1, 0\}$ を発生するものとする。すなわち、次式で定義される。

$$F(x) = \begin{cases} 1, & V_H \geq x \geq V_S \\ 0, & x > V_H, \text{ または } x < V_S \end{cases} \cdots \cdots (11)$$

また、上記の WC の動作状態を Q^* とすると、動作状態を含む出力関数 $H(x) \in \{1, 0\}$ が次式で表される WC をフェイルセーフなウィンドウ・コンパレータと呼ぶ。

$$H(x) = F(x) \cdot Q^* \cdots \cdots (12)$$

ここに、二つのしきい値の間隔 $V_H - V_S$ を WC の窓と呼ぶ。そして、(12)式はフェイルセーフな WC として故障時出力が $H(x)=0$ となるべきことを意味する。

図 4 ウィンドウ・コンパレータの構成方法
Fig. 4. Basic construction of window-comparator.

〈4・2〉 フェイルセーフ・ウィンドウ・コンパレータの実現方法 図 4(a) は WC を実現するための基本構成図である。同図で S_1, S_2 は各々しきい値 $V_H, V_S (V_H > V_S)$ をもつレベルコンパレータ。 S_3 は AND ゲートである。同図の構成はフェイルセーフな特性をもつ WC として、入力信号 x に対して出力関数 $H(x)$ が次式で与えられねばならない。

$$H(x) = (F_H(x) \cdot S_1^*) \cdot (F_S(x) \cdot S_2^*) \cdot S_3^* \cdots \cdots (13)$$

$$F_H(x) = 1, x \leq V_H, \quad F_S(x) = 1, x \geq V_S \\ 0, x > V_H \quad \quad \quad 0, x < V_S$$

ここに、 S_1^*, S_2^*, S_3^* はコンパレータおよび AND ゲートの動作状態を表す。

図 4(b) は (13) 式の入力特性を示し、縦軸は入力レベル x である。しきい値演算 $F_H(x)=1$ と $F_S(x)=1$ の重なる部分 (斜線の重なる部分) が WC の窓 W で、この範囲で $H(x)=1$ を生ずる。

図 4(a) を構成する三つの要素が故障時出力 $H(x)=0$ を生成すれば、フェイルセーフな WC が実現する。

〈4・3〉 具体的フェイルセーフ・ウィンドウ・コンパレータ 図 2 で示すインタロックが自己確認形インタロックを構成するとき、信号 $\hat{M}$ は出力 $f(=1)$ として発生されるべきか否かが検査され、この結果で許されるときのみ出力 $f(=1)$ として生成される。この自

図 5 自己確認形インタロックによる
フェイルセーフ回路
Fig. 5. Fail-safe circuit expressed by self-confirm type interlock.

己確認形インタロックの構成を電子回路に適用してみる。

図5(a)は2値入力信号 i を増幅して出力信号 $j \in \{1, 0\}$ (1を高レベルとする) を生成する直流増幅器である。出力信号 j は、増幅器 B が1に固定故障すると0であるべきとき1に誤ってしまう。同図(b)では、入力信号 $i \in \{1, 0\}$ が高周波信号 m の包絡線に変換されて増幅器 B に入力され、入力信号 i に対応する出力信号 $j \in \{1, 0\}$ は整流されて包絡線検波器 ED の出力として生成される。ここで、増幅器 B が故障で1(高レベル)側に固定されても0(低レベル)に固定されても、包絡線検波器 ED の出力信号は $j=0$ となる。これは、図の入力側破線で示す入力信号 $i=1$ を高周波信号(検査信号) m の包絡線として入力することによって、増幅器 B の出力信号が $i=1$ 側にも $i=0$ 側にもなり得ることを確認しつつ正常時の出力 $j=1$ が生じていると考えられる。すなわち、検査信号を2値信号 $m \in \{1, 0\}$ として、検査信号が出力されるべきときを1、出力されないときを0とすると出力信号 j は $j=i \cdot m$ で表せる。

図5(c)は入力信号 x_1, x_2 が2段のトランジスタ増幅器の電源として入力されるANDゲートで、外部に検査信号発生器 PG を備えている。演算出力 $x_1 \cdot x_2$ はこの検査信号の包絡線として発生する。包絡線検波器 ED と検査信号発生器 PG を含む $x_1 \cdot x_2$ のANDゲートの動作状態 $Q^* \in \{1, 0\}$ は検査信号が出力されるべきとき1、故障で出力されないとき0となる。(c)図の回路は構成要素に故障が起こると出力信号 $j=1$ が発生しない特性をもち、 $j=x_1 \cdot x_2 \cdot Q^*$ で表せる。この演算結果は $f(x)=x_1 \cdot x_2$ とおくと(d)図に示すように、故

障しない仮想ゲート G' を用いてインタロックの構成で表示できる。

図6(a)はフェイルセーフなWCの具体的回路構成図で、図5(c)の外部検査信号発生器の代わりに、入力信号があるときのみ発振して検査を行い、この検査信号の包絡線として出力信号が発生する構成としている。入力端子1および2に電圧が印加されないとき、トランジスタ Q_2 がON状態であり発振しない。入力端子1, 2に所定の入力電圧が印加されると、 $Q_2 \text{ OFF} \rightarrow Q_3 \text{ OFF} \rightarrow Q_1 \text{ ON} \rightarrow Q_2 \text{ ON} \rightarrow Q_3 \text{ ON} \rightarrow Q_1 \text{ OFF} \rightarrow Q_2 \text{ OFF} \rightarrow \dots$ の過程で発振を開始する。この発振が起こる条件は入力端子1の入力電圧を V_a 、入力端子2の入力電圧を V_b とおくと次式で与えられる。

$$V_a > (R_1 + R_2 + R_3)E/R_3 (\cong V_S) \quad \dots\dots\dots (14)$$

$$E < V_b < (R_4 + R_5)E/R_5 (\cong V_H) \quad \dots\dots\dots (15)$$

そして入力端子1, 2を共通接続し、このときの入力電圧を x とすると入力 x が次の範囲(窓 $V_H - V_S$)で発振するWCとなる。

$$(R_1 + R_2 + R_3)E/R_3 < x < (R_4 + R_5)E/R_5 \quad \dots\dots\dots (16)$$

図6(a)でトランジスタ Q_1 は、入力電圧が $(R_4 + R_5)E/R_5$ より高くなると常時ON状態(スイッチングの動作が不可能)となって、窓の上限($\cong V_H$)を与える。トランジスタ Q_2 は発振のための増幅機能をもつと共に、入力電圧が $(R_1 + R_2 + R_3)E/R_3$ より低くなると常時ON状態となって、窓の下限($\cong V_S$)を与える。トランジスタ Q_3 は入力端子2の入力信号をスイッチしてトランジスタ Q_1 に与えるためのインバータである。従って、このしきい値演算回路は二つの入

図6 フェイルセーフ・ウィンドウ・コンパレータの回路構成
Fig. 6. Fail-safe window-comparator circuit construction.

力端子に(14), (15)式の条件を満たす入力電圧が印加されるときのみ発振して出力を生じ, 図 4(a)の構成を満たす。

図 6(b)は, (a)図の WC をトランジスタ Q_4 によるスイッチ回路 (インバータ) を介して縦続接続し, 抵抗 R_9 を介して正帰還して発振器を構成した 2 入力 WC (二つの入力端子が各々窓をもち, ともに窓を満たす入力があるときのみ出力 1 を生成する WC) である。この回路は 2 入力の AND ゲートを特別な場合として含む (すなわち, フェイルセーフ AND ゲートとして利用できる)。同様に, (a)図の帰還 (R_6) を含まない回路を複数縦続接続して帰還発振器を構成すれば, 多入力の WC が実現する。この多入力 WC は, 入力端子ごとに異なる窓でしきい値が設定できるので, 多線系・多値入力信号に対して入力端子ごとに異なる値の論理積演算が行える。

図 4(a)の基本構成図で示した WC は入力レベルに対して二つのしきい値機能 (S_1, S_2) をもつと共に, この二つの機能の出力信号を論理積 (S_3) として生成し, 故障時出力を生じない特性をもつ必要がある。

図 6(a), (b)の回路は入力信号 X に対して(16)式, すなわち抵抗器で定まる窓をもつ。抵抗器 (炭素皮膜抵抗器) の抵抗値変動は極小であるが, 過電力強制劣化試験を行うと約 +10% の変化後断線に至る⁽⁸⁾ので, 窓変動はこれを配慮すれば十分である[(16)式にかかわる抵抗器が断線したら回路は発振できない]。

また, 図 6(a), (b)の回路は入力端子 1, 2 または I_1, I_2 の入力信号の論理積として出力信号が発生する。論理積演算機能がフェイルセーフである[(1)式

を満たす)ためには, (i)故障時自ら出力信号 1 を発生しないと同時に, (ii)論理積入力のすべてが入力されない[(1)式の $h(x)$ が満たされない]のに出力信号 1 を生じないことが必要である。同図の発振器は構成するトランジスタの一つにベース・コレクタ間の短絡故障が生じて (入力信号が直接出力信号として現れても) 正の帰還が達成されず, 発振が起らない。しかし, 複数 (偶数) のトランジスタでこの故障が起ると, (例えば, 故障したトランジスタに入力信号がないのに) 発振を起こす⁽⁹⁾危険が生じる。このため, 二つ以上のトランジスタの入出力間に短絡故障が生じて発振が起らないように, トランジスタ増幅回路の間でレベル変換を行っている。

図 6 に示した WC の発振過程を図 7 に示す。図 7(a), (b)は各々図 6(a), (b)に対応し, 回路を構成するトランジスタを図に合せて横軸に並べ, 縦軸は各トランジスタのスイッチング時のコレクタ電位を示す (E は電源電位, v は電源電位より高い入力電圧で生ずるコレクタ電位)。矢印は順次 ON/OFF されるトランジスタの順序を示す。図 7 で, トランジスタ Q_4, Q_5 間を省いて, トランジスタどうしの出力電位が電源電位より高い電位 (電源枠外電位)⁽⁶⁾と低い電位 (電源枠内電位)⁽⁶⁾間でレベル変換される。すなわち, 例えば図 6(a)でトランジスタ Q_1 の出力信号 (コレクタ電位) は ON, OFF のいずれの状態も電源枠外電位であるが, この出力信号はトランジスタ Q_2 によって ON, OFF のいずれの状態も電源枠内電位となる出力信号 (Q_2 のコレクタ電位) に変換される。また, トランジスタ Q_1 が電源枠外電位の出力信号で変

図 7 ウィンドウ・コンパレータの発振過程
Fig. 7. Oscillation process of fail-safe window-comparator.

化できるように、トランジスタ Q_2 の出力信号はトランジスタ Q_3 によって、電源枠外電位 (Q_3 の OFF 時の出力電位) に変換される。ここに、電源枠内電位で出力信号が変化する (すなわち、電源 E から電力を供給されている) トランジスタ Q_2 は発振を起こすために主として電力増幅の役目を担い、トランジスタ Q_1 は Q_3 による電源枠外電位の出力信号を検出すると共に、出力信号が電源枠外電位でありながら、電源枠内で動作するトランジスタ Q_2 をスイッチする役目をしている。このレベル変換を行うことによって、図の回路は構成されるトランジスタで万一ベース・コレクタ間に短絡故障が起こって、トランジスタの入力電圧が直接出力側に伝達されても、入力信号が印加されない限り発振できない構造となっている。すなわち、例えば図 6(b) でトランジスタ Q_1 (または Q_4) のベースには、前段のトランジスタ Q_6, Q_7 (または Q_2, Q_3) にいかなる故障状態が起こっても、入力端子 I_2 (または I_1) に入力信号が印加されない限り電源枠外電位の入力電位は発生しない。また、トランジスタ Q_1 と Q_2 または Q_1 と Q_7 に同時に故障が起こった場合、あるいはトランジスタ Q_4, Q_5 で同時に故障が起こった場合、トランジスタ Q_2 または Q_6 の入力条件、すなわち(14)式の発振条件が満たされないが、たとえ仮にこの発振条件が成立したとしても入力端子 I_1, I_2 の両方とも入力信号が印加されない限り、図 6(b) の回路は発振できない。

従って、図 6(b) は故障時、少なくとも二つの入力端子に発振条件を満たす入力信号がともに入力されない限り、発振の出力信号が発生しないフェイルセーフな特性をもつ。たとえ複数の要素 (トランジスタおよび抵抗) で故障が同時に起こってもこの特性は変らない。

5. 終りに

機械間で衝突を防止するためのフェイルセーフなインタロックは、相手方出力が発生していないことを直

接センサで検知し、この検知出力がないとき自出力を発生する自己確認形インタロックでなければならないことを示した。ここで用いられるセンサは検知の出力信号を発生すると同時に、否定演算機能を有していなければならない。このためのしきい値演算素子として、アナログ信号から 2 値の否定演算出力信号を生成するフェイルセーフなウィンドウ・コンパレータを提案し、具体的回路の構成方法と実現例を示した。またこれにより、フェイルセーフな AND ゲートも実現できる。ここに示したフェイルセーフなウィンドウ・コンパレータ自身は自己確認形インタロックの構造で実現されており (なお、既に著者らが提案している人間機械システムにおけるインタロック⁽¹⁰⁾も自己確認形インタロックに相当している)、内部の発振過程に電源電位の上下でレベル変換が行われるために、構成要素に多重故障が発生しても出力を生じない特性をもつ。このしきい値演算素子は既に鉄道信号システムにおいて実用に供されている⁽¹¹⁾⁽¹²⁾。

(昭和 62 年 12 月 23 日 受付, 同 64 年 1 月 6 日 再受付)

文 献

- (1) R. Mathon: "Computers Replacing Safety Relays in Railway Signaling", IFAC Int. Conf. Digital Compt. Appl. to Process Control, A5-3 (1977)
- (2) JIS B 0111-1981: プレス機械用語 (5018)
- (3) 機械用語辞典, p. 201 (昭 47) コロナ社
- (4) 電気辞典, p. 66 (昭 28) (財) 商工会館出版部
- (5) JIS B 0134-1979: 産業用ロボット用語 (5013)
- (6) 蓬原・向殿: 「レール短絡を使った列車検知用フェイルセーフセンサの特性と構造」, 電学論 C, **107**, 955 (昭 62-10)
- (7) 川西: 「Fail-Safe」, 電学誌, **91**, 21 (昭 46-4)
- (8) 蓬原・池田・黒後: 「カーボン抵抗器の劣化特性に関する考察」, 第 6 回日本ロボット学会学術講演会予稿集, p. 2609 (昭 63)
- (9) 土屋: 「フェイルセーフ論理方式の研究」, 電気試験所報告, No. 695, p. 10 (昭 44-1)
- (10) 蓬原・杉本・向殿: 「安全作業におけるインタロックの構造と実現」, 電学論 D, **107**, 1099 (昭 62-9)
- (11) K. Futsuhara & M. Mukaidono: "Realization of Fail-Safe Train Wheel Sensor Using Electromagnetic Induction", *IEEE Trans. Instrum. Meas.*, **38**, No. 2 (1989)
- (12) 旧国鉄仕様書: 踏切障害物検知, JRS 22521-4 A-13 BR 3 E (昭 58-6)