“フェールセーフ素子”について

日本信号㈱（安全技術応用研究会会員）
坂井正善・白井稔人

1．はじめに

平成10年7月労働省より発行された「工作機械等の制御機構のフェールセーフ化に関するガイドライン」（基発第464号）では，不具合を確実にチェックするための原則ならびにエネルギー発生方法の原則が示されている。また，接点を用いる場合の電気回路の設計原則と半導体を用いる場合の電子回路の設計原則が示されている。（文献[1]）。しかし，安全に関わる電子回路の設計原則は我が国では古くから研究されてきている（文献[2]）にも拘わらず，一般には知られていないようである。本文では，電力回路の基礎的設計原則とこの原則に基づいて構成された国際安全規格適合認証済みのデバイスを紹介する。

本文では，まず，2章で用語「フェールセーフ」の国際安全規格上の扱いを述べる。国際安全規格は，草案の段階で使用していた用語「フェールセーフ」を，発行の段階で全て削除した。3章で，冗長系を使用しない安全確保の基礎的技法を示し，4章で3章の技法に基づいて構成された自己診断機能付きデバイスを示す。

2．用語「フェールセーフ」

用語「フェールセーフ」は，システムを構成するコンポーネントに不具合が発生したとき，システムの出力が圧倒的割合で安全側に誤る非対称の誤り特性を本来意味する。圧倒的割合は，国（例

表1　国際安全規格で削除された用語「フェールセーフ」関連部分

規　格	草案段階	発行段階
IEC61508-4：1998 functional safety -safety-related system Part 4	1995年草案段階では，以下の定義あり。 フェールセーフ：規定される障害モードが圧倒的に安全な方向であるようなアイテムの設計特性	削除
IEC61496-1：1997 Safety of machinery- Electro-sensitive protective equipment Part 1	欧州規格草案(prEN50100-1:1993)段階では，タイプ4の実現手段として以下の注釈あり。 ダイナミックなフェールセーフ信号処理を用いたシングルチャンネル技法	下線部分は「不具合検出手段」に変更。
ISO12100-1:200X Safety of machinery- Basic concepts, general principles for design, Part 1	1992年TR段階では，以下の定義あり。 フェールセーフ条件(危険側不具合の最小化)：動力源あるいはコンポーネントの不具合発生状況で，安全機能がそのまま維持されることによって達成される理論的条件	削除(平11年度，機械安全分野の国際規格適正化調査研究成果報告書，日本機械工業連合会　より)
prENV50129：1997 Railway applications: Safety related electronic systems for signalling	フェールセーフ：障害発生時，製品が安全な状態に移行するか，あるいは，安全な状態に留まるように製品の設計に組み入れられる概念 フェールセーフ性：発生し得ると認識される全ての単一ハードウェア不具合発生下で，システムあるいはサブシステム，設備が安全であることを確実にする原則	

えば，米国や仏国）によっては絶対と錯誤される可能性がある。このため，PL（製造物責任）を考慮して，この用語の使用を避けるべきであるとする意見に従って，国際安全規格上では「フェールセーフ」は削除されてきている。国際規格上では，「フェールセーフ」の概念は危険側に誤る不具合を最小化する概念に置き換えられてきている。表1は，規格草案の段階で使用されていた“フェールセーフ”に関連する定義の例を示す。表1には，国際規格ではないが欧州鉄道規格で用いられている「フェールセーフ性」を一緒に示してある。

現在，IEC61508：functional safety ではSIL4，あるいは，ISO13849-1：safety of machinery safety-related parts of control system では安全性カテゴリー4，IEC61496-1：safety of machinery-Electro-sensitive protective equipment -General requirements and tests ではタイプ4として規定される安全性確保能力が国際安全規格上の最高のランク付けになっている。この最高のランク付けは，冗長構成によるシステムを含む。本文では，冗長構成の技法に関しては述べないが，冗長構成によるシステムは，システムを構成する複数のサブシステムに同時に不具合を生じる可能性がどの程度最小化されているかによってその安全性が評価される。表2は，規格で規定される最高の安全確保能力の例を示す。表2に示すように，欧州鉄道規格の付属書では，IEC61508で規定される4通りの安全確保レベル（SIL）に用語を割り当てている。最高レベルであるSIL4が“fail safe”に該当するとしている。

表2　国際安全規格類で規定される最高レベルの安全確保能力の例

規　格	最高レベル	要求事項の概要
IEC61508-2：1998 functional safety -safety-related system Part 2	SIL　4	マイクロプロセッサを使用しない安全関連保護システムに対する要求事項： ・オンラインの不具合検出能力の高いシステムの場合，単一の不具合発生下で安全機能が維持されること。不具合検出能力が高くない場合，2重の不具合発生下で安全機能が維持されること。 ・未検出の不具合は適切な周期で実施されるオフラインの点検で検出されること。
IEC61496-1：1997 Safety of machinery- Electro-sensitive protective equipment Part 1	Type　4	・能力喪失につながる単一の不具合によって出力 OFF 固定状態(ロックアウト条件)に移行すること。 ・危険側誤りとはならない未検出の単一の不具合は，他の不具合と組合せてテストされること(3 を越える不具合の蓄積に関しては，それらが互いに独立している場合に限り，テストする必要はない)
ISO13849-1：1999 Safety of machinery- Safety-related parts of Control systems, Part 1	カテゴリー4	・単一の不具合によって安全機能を喪失しないこと。 ・単一の不具合は，安全機能のデマンド発生前またはデマント発生時に検出されること。できない場合，不具合の蓄積によって安全機能を喪失しないこと。
ANSI/RIA R15.06 -1999: for Industrial Robot Systems Safety Requirements	Control reliable	・いかなる単一の不具合によってもロボットの停止を妨げてはならない。 ・単一の不具合は直ちに検出されることが望ましい。できない場合，次の安全機能のデマンドより前に検出されることが望ましい。
prENV50129：1997 Railway applications: Safety related electronic systems for signalling	IEC61508 と同じ SIL4：フェールセーフ SIL3：高インテグリティー(高程度の達成) SIL2：中インテグリティー(中程度の達成) SIL1：低インテグリティー(低い達成)	

表3　労働省ガイドラインで示される電子回路設計のための基礎的安全原則

方　法	意　味	設計上の要求事項
交流信号の利用	信号伝達手段に不具合が発生した場合，交流信号が伝達されなくなる現象を用いて出力発生をやめるようなチェック機能付きの出力信号発生方法	安全を示す入力信号を交流信号とし，この交流信号が伝達されるときあらかじめ準備したエネルギーを発生させること。
電源枠外処理の利用	電源枠内の交流信号を電源に重ね整流することによって電源より高い電位の信号を生成する信号処理。	電源線が出力信号線に直接接続されるような不具合を検出できること。このような場合，電源より高い電位は生じ得ない。
発信回路の利用	入力信号が回路動作の電源として与えられている場合に限り，回路が発振し交流信号が生成されるような信号処理。レベル検定回路やANDゲートを構成できる。	回路の発振動作によって回路の不具合がチェックされ，不具合発生によって発振動作が停止すること(交流信号の利用)。
単調な信号伝達	入力としてエネルギーが存在するときのみ出力にエネルギーを生成するような信号伝達によって，エネルギーを伝達できない不具合発生時に出力の発生をやめる信号の伝達方法。	不具合の発生を発見できてもエネルギーの発生をやめることができなければ安全を確保できないので，出力回路部は単調な信号伝達を満足すること。

3．ダイナミック信号処理

本章では，冗長構成によらない信号処理の技法（“フェールセーフ”信号処理の技法）を述べる。表3に，労働省ガイドラインで紹介される基礎的安全原則を示す。なお，欧州から提案されている電気接点利用の冗長構成の解説は，文献[3]を参照されたい。

3.1　交流信号の利用

市販の電磁リレーや半導体スイッチなどスイッチ素子は，ON側とOFF側いずれの側にも誤る素子である。安全側誤りはエネルギーを発生しない側であるから，スイッチ素子のOFF側不具合は安全側に，ON側不具合は危険側に誤りに各々相当する。このような市販のスイッチ素子を用いて，安全側に誤ることはあっても危険側に誤ることのないような特性を実現する方法として，交流信号は古くから利用されてきた。スイッチ素子に不具合を生じたときスイッチ素子の出力状態はON側かOFF側のいずれか一方に固定されてしまうので，交流信号は不具合の発生したスイッチ素子の出力には生じ得ない。図1(a)で示すようにスイッチ素子にON側の不具合が発生すると，入力信号に関係なくモータにエネルギーが供給されてしまう。図1(b)は交流信号を利用する場合の構成例を示す。半導体スイッチ素子は交流の入力信号に追従してON／OFFし，磁気結合を介してトランスの2次側に交流信号が発生する。交流信号は整流回路で平滑され直流モータにエネルギーが伝達される。半導体スイッチ素子にON側の不具合が発生すると，トランスの1次側に交流信号は生じないのでトランスの2次側にエネル

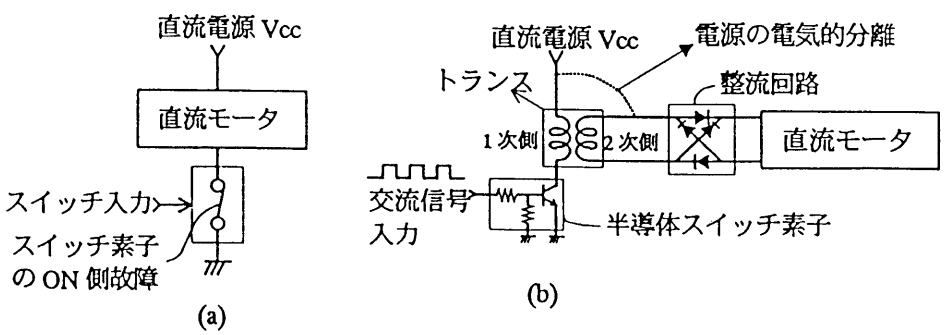


図1　交流信号の利用方法例

ギーは伝達され得ない。このような信号処理をダイナミック信号処理と呼ぶ。なお，図1(b)で，電源Vccと直流モータはトランスによって電気的に分離されている点に注意されたい。この電気的分離により電源Vccと負荷である直流モータが接続される事象が回避されている。トランスを使用しない電気的分離の技法は次節で述べる。

3.2 電源枠外処理と演算発信器

図2(a)は，電源枠内，すなわち，Vcc-0V間で変化する交流信号を電源電位Vccに重ね合わせることによって，電源枠外，すなわち，電源より高い電位の2 Vccと電源電位Vccの間で変化する交流信号に変換する信号処理を示す。この技法を利用することによって電源電位Vccより高い電位を有する直流信号を発生することができる。図2(b)は，具体的回路の構成例を示す。図2(b)の出力と電源Vccの間に負荷を接続すれば，出力に電源電位より高い出力信号が生じた場合に限り，エネルギーが負荷に供給される。このように，交流信号を用いて，電源より高い電位を発生するような処理を電源枠外処理と呼ぶ。

図2(c)に，電源枠外処理を用いた応用例として光結合素子を用いたAND回路を示す。電源枠内の交流の入力信号I1は，整流回路を経由して電源枠外の直流信号に変換される。この記号が生じている場合に限り，光結合素子PH1の発光素子にエネルギーが伝達される。電源枠内の交流の入力信号I2は，光結合素子PH 2を介して光結合素子PH 1の発光素子をON／OFFし，光結合素子PH 1の受光側には電源電位Vcc'の枠内で変化する交流信号Yが生成される。

図3に，ANDゲートの別の実現例を示す。電源枠外信号処理に基づく加算回路としきい値演算回路で構成される。電源枠内の交流信号I1が存在するとき，整流回路REC1の出力信号の電位は約2 Vccである。整流回路REC2はこの電位2 Vccに更に入力信号I2を重ね合わせ約3 Vccの出力を生成する。図3で示す加算回路の特徴は，整流回

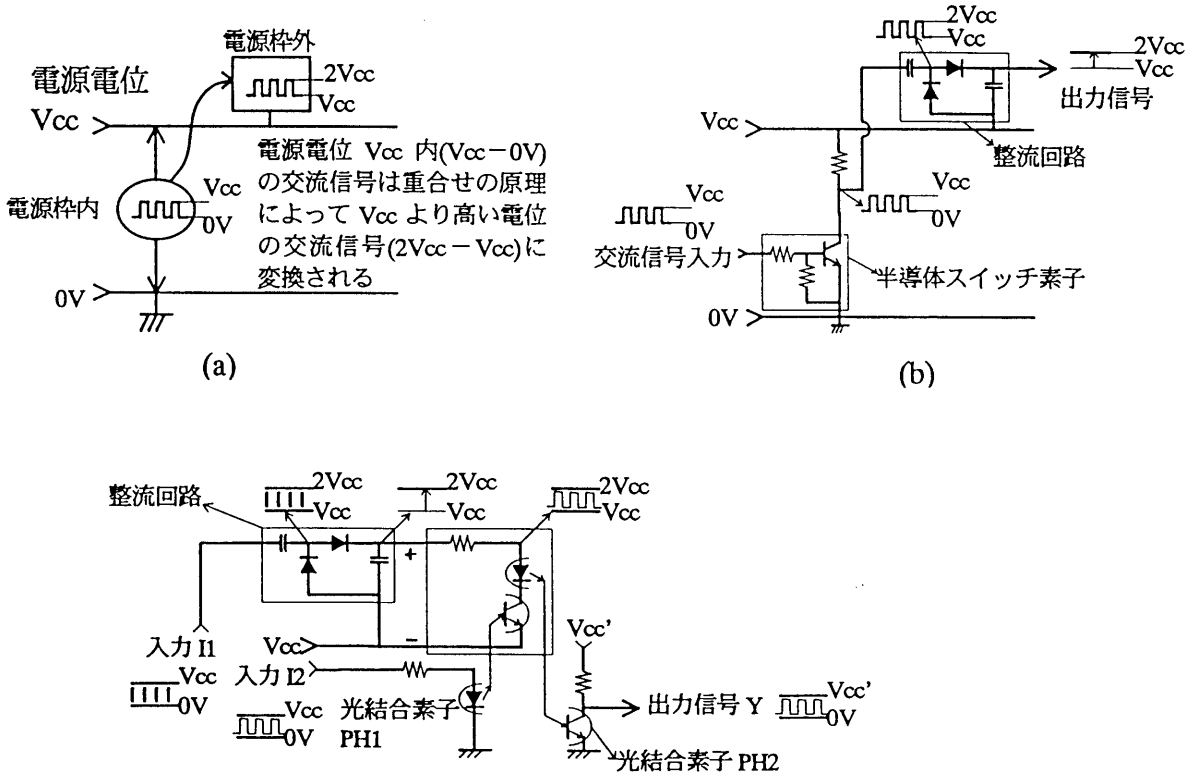


図2 電源枠外処理の構成例

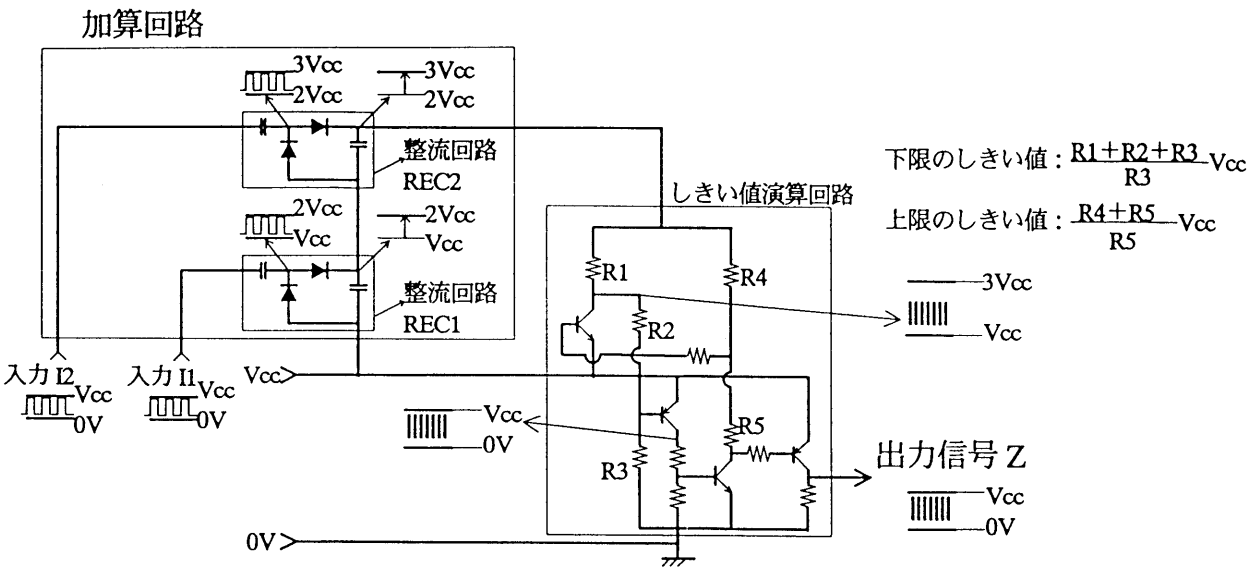


図3　電子回路設計の安全原則に基づくANDゲートの構成例

路に不具合が発生しり場合，出力信号の電位が低くなる側に誤る点である。図3で示すしきい値演算回路は，上限と下限のしきい値をもつしきい値演算回路である。しきい値演算回路に入力される電源枠外の直流信号電位が上限と下限の間に収まるとき，しきい値演算回路は発振し交流の出力信号Zを発生する。しきい値演算回路の動作（文献は［4］）は本文では詳述しないが，しきい値演算回路に不具合を生じたとき交流信号を出力しないような誤り特性を備える。

4．ダイナミック信号処理に基づくインタロックデバイス

3章で述べた基礎的安全原則に基づいて構成された2種類のデバイスの機能を図解する。

4.1　デバイスの機能

図4にデバイスの機能をブロック図で示す。2つのデバイスは，図3に示す加算回路としきい値演算回路をベースに構成されている。基本デバイスは，ON側不具合検出機能付き出力回路を2回路内蔵している。図5は，デバイスの部品配置を示す。

4.2　デバイスの応用例—非同期駆動を用いた出力回路—

図6に，基本デバイスを使用した安全性カテゴリー4（ISO13849-1）認証済みの出力回路（文献［5］）のブロック図を示す。図7は，認証済み回路の写真を示す。

5．おわりに

冗長構成を使用しない高安全な回路構成の技法を，労働省ガイドラインに関連付けて紹介した。ガイドラインで示される電子回路の設計原則は，“本質的フェールセーフ”として欧州及び我が国において高く評価されてきた技法である。

国際安全規格で示される安全の考え方は，リスクに見合った安全方策の実施である。リスクアセスメントを実施してリスクが高くないことを立証できた場合に限り，安全方策の安全性確保能力はそれなりでよい。しかし，米国ロボット安全規格で明確に規定されているように，リスクアセスメントを実施しないリスク不明の状況では，本文で紹介したような最高レベルの安全確保能力が制御システムに要求されることになる。

引用文献

［1］㈱日本労働安全衛生コンサルタント会編：“これからの安全技術－工作機械等のフェールセーフ

化に関するガイドラインの解説”，中央労働災害防止協会（1997-6）

2] 川西：“Fail Safe”，電気学会誌，Vol.191，No.4(1971-4)

3]例えば，安全技術応用研究会，電気担当者教育資料作成委員会：機械安全制御入門，SOSTAP (1999-4)

[4]例えば，安全技術応用研究会編，機械システム安全技術，日刊工業新聞（2000-4）

[5]坂井，高安全性インタロック装置の開発，平成11年全国産業安全衛生大会（1999－10）

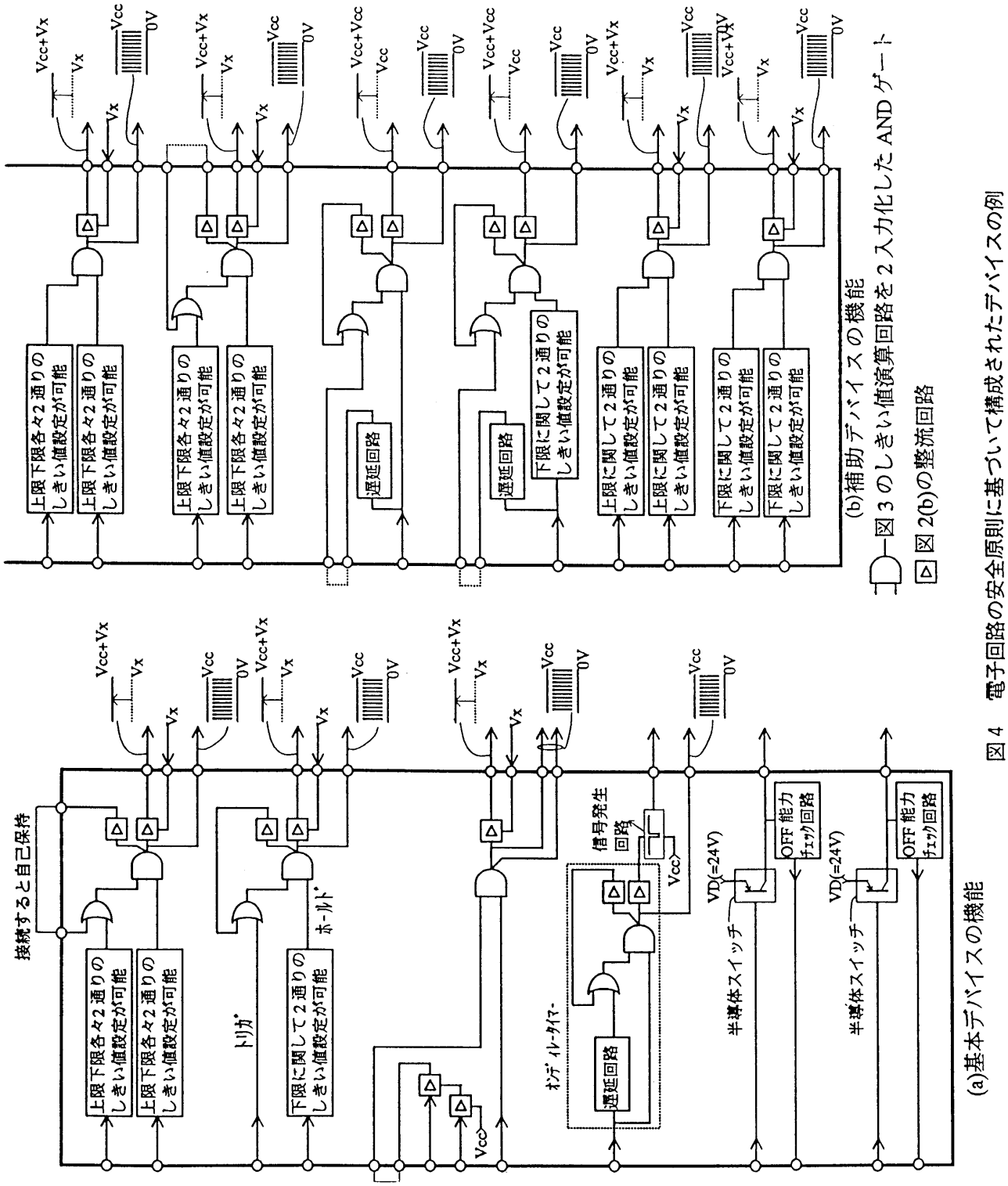
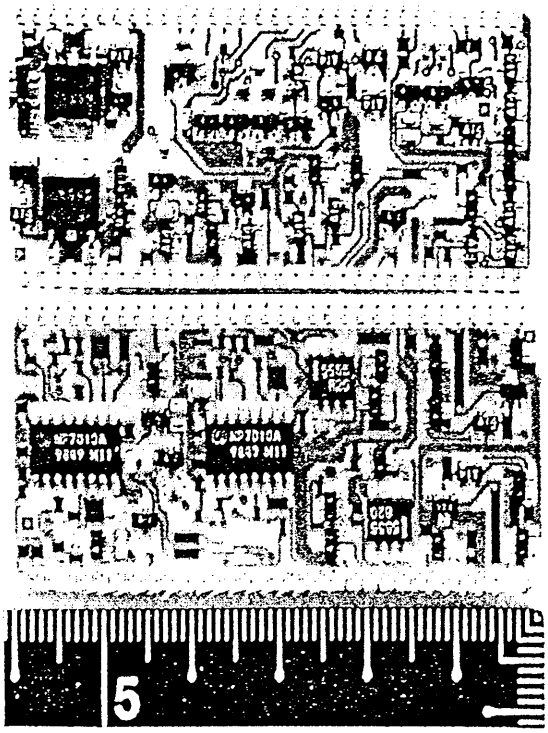
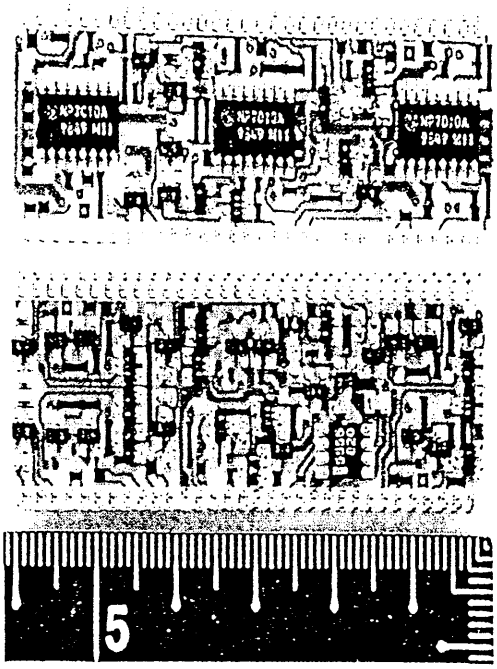


図4　電子回路の安全原則に基づいて構成されたデバイスの例



(a)基本デバイスの部品配置：
写真（上）は表面，写真（下）は裏面



(b)補助デバイスの部品配置：
写真（上）は表面，写真（下）は裏面

図5　デバイスの部品配置

図6は次頁に掲載してあります。

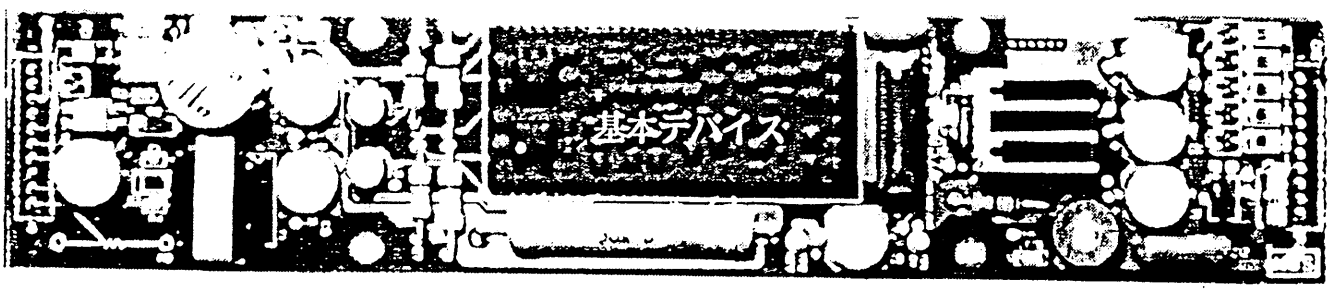


図7　基本デバイスを応用したカテゴリー4認証済み回路（TUV.ps 認証 No.U000436252001）の外観

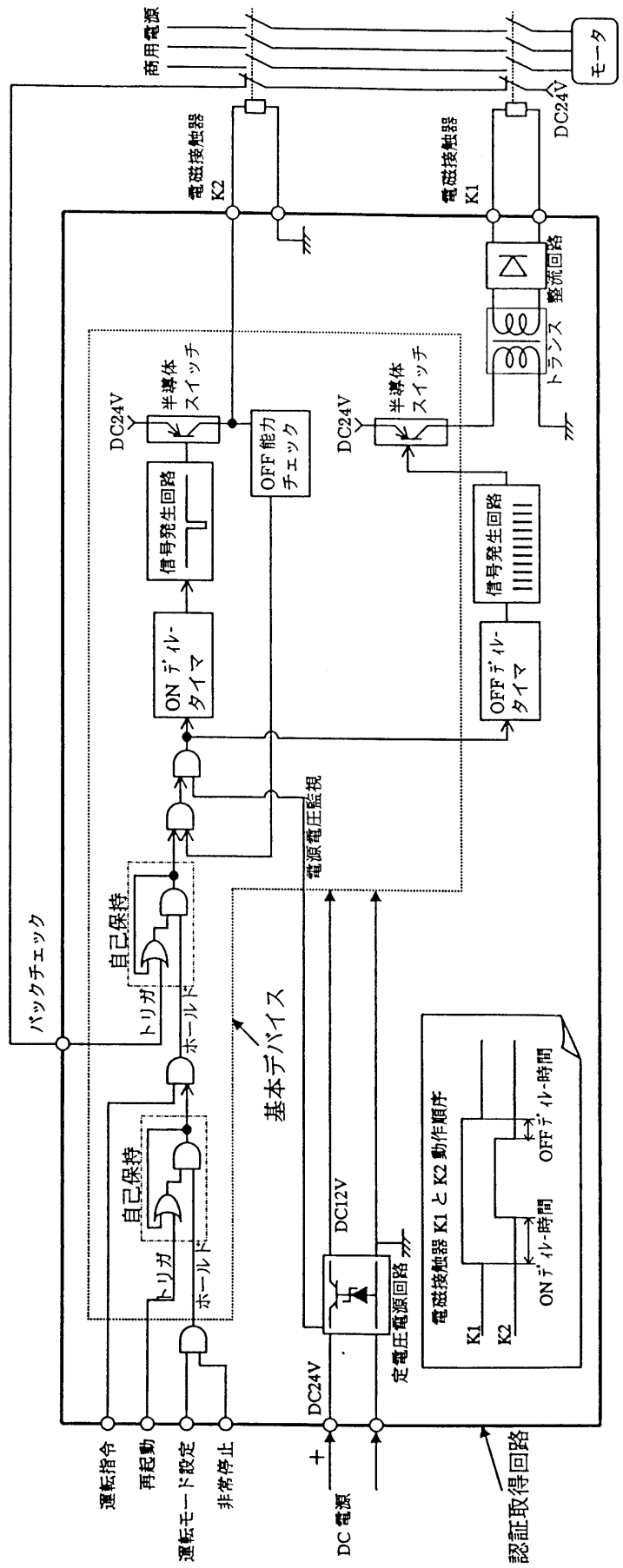


図6　基本デバイスを応用したカテゴリー4認証済み回路の機能概略：電磁接触器 K1 は無負荷で駆動され，回路に不具合を生じた場合，電磁接触器を駆動する出力信号は停止する。電磁接触器 K1 は非常用ブレーキに，電磁接触器 K2 は常用ブレーキに各々該当する。両者の組合せにより，K1 と K2 の ON／OFF の頻度によらずカテゴリー4の制御回路として利用することができる（詳細は IEC　44/278/NF(1999-11-26)，p47 参照）