○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の策定について

(平成１０年７月２８日)

(基発第４６４号)

(都道府県労働基準局長あて労働省労働基準局長通達)

機械設備による労働災害については、従来からその防止対策を重点的に推進してきたところであるが、その休業 4 日以上の被災者数は、年間 5 万人近くに達し、労働災害全体の 3 割以上と最も大きな要因の一つを占めている。このうち、製造業についてみれば、機械設備によるはさまれ、巻き込まれ等の災害が 5 割近くを占めている。また、平成 7 年における製造業を対象とした労働災害原因要素の分析によれば、工作機械等による休業 4 日以上の災害のうち、機械設備側に適切な対策が施されていれば未然に防止することができたと考えられる災害が全体の約 6 割にも上っている。

また、工作機械等の産業用機械については、ME 化・自動化が進められており、その制御機構はますます複雑となり、高度化してきている。これに伴って制御機構の不備に基づく労働災害の発生も少なくない。

さらに、国際的にも、フェールセーフの考え方を取り入れた機械設備の安全設計等の規格化が進められている状況にある。

このような状況を踏まえ、また、フェールセーフ化の技術指針を策定することにより、機械設備の本質安全化を促進することとした第 9 次の労働災害防止計画に沿って、今般、工作機械等の本質安全化を促進するため、別添のとおり、「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」を取りまとめたところである。ついては、各局において、管内における工作機械等の製造事業場に対しては開発、設計及び製造時に、また使用事業場に対しては設備導入等の際の安全審査時に、それぞれ本ガイドラインが活用されるよう周知徹底を図り、これら機械設備による労働災害の防止対策の推進に積極的に取り組まれたい。

なお、本件に関して、関係事業者団体に対し別紙のとおり要請を行ったので了知されたい。

別添

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

1　総則

(1)　趣旨

このガイドラインは、工作機械、成形機及びこれらの設備と一体となって使用される搬出入装置(以下「工作機械等」という。)の制御機構を対象に、フェールセーフ化の原則、一般的方法、具体的方法等を取りまとめたものである。制御機構の開発、設計、製造及び改造等に携わる者は、これらの原則や手法を十分参考にした上で、当該機構の設計、製造及び改造等を行うことが望ましい。

(2)　フェールセーフ技術の意義

機械の本質安全化を図るには、機械は故障し、作業者は誤りを犯すことをまず認めた上で、仮にこれらが発生しても作業者の安全が確保される構造を、機械設備の設計、製造及び改造等の段階で、構築しておく必要がある。このために安全確認システムが設置されるが、安全確認システムが故障すると、作業者の安全が確保されず、労働災害が発生することがあるため、安全確認システムでは、故障時、必ず安全側(労働災害を発生させない形で機械を停止させる側)となる特性が求められる。本ガイドラインで示すフェールセーフ技術は、この特性の実現を目的とした技術である。

(3)　本ガイドラインで記載していない手法の取扱い

本ガイドラインで示すフェールセーフ化の手法は、上記の特性を実現するための主要な手法を示したものであり、同等以上のフェールセーフ性を有する他の手法を排除する趣旨ではない。この場合に、当該手法のフェールセーフ性を事前に十分確認しておくことが必要である。

2　定義

(1)　安全情報

安全装置等により安全が確認されているときに限り生成される情報をいう。

(2)　インターロック

安全情報に基づき、機械の可動部の動作を許可したり、禁止したりする仕組みをいう。

(3)　フェールセーフ

システム又はこれを構成する要素が故障しても、これに起因して労働災害が発生することのないように、あらかじめ定められた安全側の状態に固定し、故障の影響を限定することにより、作業者の安全を確保する仕組みをいう。

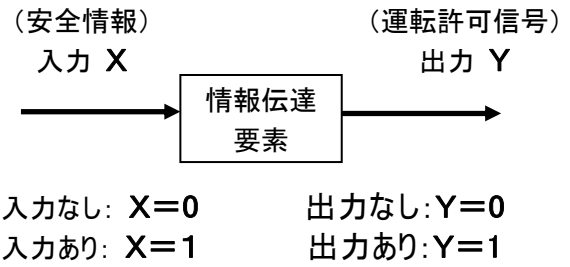
(4)　非対称誤り特性

システム又はこれを構成する要素が故障しても、安全側に誤る故障の頻度が危険側に誤る故障の頻度よりも著しく高い特性又は安全側にしか故障しない特性をいう。

(5)　ユネイトな情報伝達

システムに安全情報が入力されない限り誤って運転許可信号を発生することのない情報伝達の形態をいう。

表 1 ユネイトな情報伝達要素による情報伝達の形態			
	X	Y	判定
①	0	0	○ （正常）
②	1	0	○ （許容される故障）
③	0	1	× （許容されない故障）
④	1	1	○ （正常）



(ユネイトな情報伝達とは、表１において③の場合が許されない情報伝達の形態をいう。)

3　フェールセーフ化の原則

(1)　フェールセーフ化の対象とする制御機構は、原則として、表 2 に示す制御機構とする。ただし、故障によって労働災害が発生するおそれのない場合は、この限りではない。

(2)　表 2 の制御機構は、原則として、非対称誤り特性を持つように設計するものとする。

(3)　表 2 の制御機構にプログラム可能な電子制御装置(プログラマブルコントローラ)を用いるときは、非対称誤り特性を有するものを使用するように努めるものとする。

(4)　安全情報は高エネルギー状態に、危険及び故障を通報するための信号は低エネルギー状態に対応させ、危険や故障を誤って安全と通報しないようにするものとする。

(5)　安全情報は、ユネイトに伝達するようにするものとする。

(6)　予測される最大の環境ノイズに対する耐性を確保するため、安全情報には十分なエネルギーを持たせるものとする。

表　2

	制御機構の区分	内容
1	再起動防止回路	急停止機構等の作動によって機械が停止したときや、停電後に機械への通電が復帰したときに、作業者が再起動操作を行わなければ、機械を再び起動できないようにする回路。
2	ガード用のインタロックの回路	機械の可動中に作業者が危険領域内へ侵入するのを防止する回路。機械が停止した後にガードのロック機構を解除し、作業者が危険領域内へ進入するのを許可する方式と、ガードを開いたときに機械が急停止する方式の二種類がある。
3	急停止用の回路	機械側で何らかの異常を感知したときに、直ちに機械の運転を停止させる回路、作業者がガードを開いたとき、安全装置が作動したとき、機械が何らかの故障や

		異常を起こしたときなどに作動する。
4	非常停止用の回路	作業者が何らかの異常を感知したときに直ちに機械の運転を停止させる回路。機械の運転中に労働災害が発生しかねない不測の事態が起きたときや、機械に異常が生じたとき、作業中にトラブルが発生したときなどに作動させる。
5	行き過ぎ防止用の回路	機械があらかじめ設定した位置・角度等を超えて行き過ぎないように監視を行い、行き過ぎが生じたときは直ちに機械を停止させる回路。
6	操作監視用の回路	作業者が正しい操作をしたときに限り、起動信号を発生させる回路。
7	ホールド停止監視用の回路	ホールド停止状態にある機械が故障や電磁ノイズ等の影響によって暴走しないように監視を行い、暴走が起きたときに直ちに機械を停止させる回路。
8	速度監視用の回路	機械を低速状態で運転するときに、故障や電磁ノイズ等の影響によって機械があらかじめ定めた速度を超えて暴走しないように監視を行い、暴走が起きたときは直ちに機械を停止させる回路。
9	ホールド・ツー・ランの回路	作業者が操作装置を押しているときに限って機械が運転を開始し、操作装置から手指等を離したときは直ちに機械を停止させる回路。

4　フェールセーフ化の一般的方法

表 2 の制御機構には、一般的には、次のような方法によりフェールセーフ化を行うものとする。ただし、故障によって労働災害が発生するおそれのない場合は、この限りではない。

イ　オフ確認

ボタンを押して接点を閉じる動作に続けて、ボタンを離して接点を開く動作を行ったときに初めて起動信号又は始動信号を発生させる方法

ロ　再起動防止

起動操作によって自己保持回路が作動して自己保持を開始し、作業者が停止操作を行ったとき又は安全装置が作動したとき等には自己保持を解除し、機械の再起動を防止する方法

ハ　ノーマルクローズ型の利用

ノーマルクローズ型の弁又はブレーキによって、故障時には、労働災害を発生させない形で機械を停止させる方法

ニ　強制引き離し

作業者が非常停止装置を操作するときの力、作業者が可動ガードを開くときの力、機械の可動部がスイッチと接触するときの力等を直接利用して、ノーマルクローズ型スイッチの接点を強制的に引き離し、労働災害を発生させない形で機械を停止させる方法

ホ　相反モードによる監視の利用

相反するモード(正モードと負モード)のスイッチを二個設けて、ガード開閉の正常性を監視し、正常でないときは労働災害を発生させない形で機械を停止させる方法

ヘ　発振回路の利用

入力によって発振するように回路を構成し、故障時には発振が停止することを利用して故障を検出するとともに、回路の出力をオフとする方法

ト　交流信号の利用

安全情報を交流信号として伝達し、故障時には直流出力が生じることを利用して故障を検出するとともに、回路の出力をオフとする方法

チ　電源枠外処理

安全情報を電源電圧より高い電圧に設定することにより、信号線と電源線の混触による誤った安全情報の伝達を防止する方法

リ　フェールセーフなチェック回路の利用

フェールセーフなチェック回路によって、制御機構を構成する非フェールセーフな安全装置や部品類に故障が生じていないかを常時チェックする方法

ヌ　二重化不一致検出

接点又は弁を二重化し、二つの動作が不一致のときは、接点又は弁に溶着又は固着が起きたとみなして、労働災害を発生させない形で機械を停止させる方法

ル　バックチェック

通電時に閉じる接点(以下「a 接点」という。）に溶着が生じたとき、対となる通電時に開く接点（以下「b 接点」という。）によってこれを検出し、直ちに機械を停止させる又は次のサイクルの運転を開始させない方法

ヲ　非溶着

本質的に溶着しない接点を用いる方法

ワ　その他非対称誤り特性を持つ物理特性の利用

安全情報の生成が停止したとき、重力の作用によって機械的機構が自然に落下し、安全を確保する方法及び加熱等が生じたとき、温度センサ固有の物理特性に基づいてセンサの抵抗値等が増大し、機械への通電を遮断する方法等

5　フェールセーフ化の具体的方法

表 2 の制御機構にフェールセーフ化を行う際に用いる部品額については、部品額ごとに 5—1 の要件を満たすものとし、その設計については、回路ごとに 5—2 の事項に留意するものとする。

5—1　部品類の要件

(1)　ガード用のインターロック回路の安全スイッチ

イ　原則として、強制引き離し式のノーマルクローズ型スイッチであること。ただし、非接触式の安全スイッチ等で、フェールセーフなチェック回路によって、常時故障検出を行っているものはこの限りではない。

ロ　接点溶着、ばねの破損若しくは摺動部の固着等が生じたとき又は作業者がスイッチの位置を意図的に固定したときに、機械を停止できなくなることを防止するため、ノーマルオープ

ン型(バネ戻り式)でないこと。

ハ　作業者が磁石を用いて安全スイッチを意図的に無効化したとき、機械を停止できなくなることを防止するため、接点を磁石でオン・オフできないこと。

ニ　作業者による不意の接触及び意図的な無効化を防止するため、覆い等が設けられたものであって、覆いは特殊な工具等を使用しなければ取り外せないものであること。

(2)　行き過ぎ防止用のリミットスイッチ

イ　原則として、強制引き離し式のノーマルクローズ型であること。

ロ　接点の接触不良が生じたとき機械を停止できなくなることを防止するため、ノーマルオープン型でないこと。

ハ　行き過ぎ防止用リミットスイッチを駆動するドグは、作業者が容易に取り外せない構造であること。

(3)　非常停止用装置

イ　非常停止ボタンは強制引き離し式のノーマルクローズ型であること。

ロ　接点の溶触不良が生じたとき機械を停止できなくなることを防止するため、ノーマルオープン型でないこと。

ハ　非常停止用ワイヤロープは、ワイヤロープが切れたとき又は緩んだときに、接点が強制的に引き離される構造であること。

(4)　安全プラグ

プラグの電極間を故意に短絡して無効化することを防止するため、覆い等が設けられたものであること。

(5)　電磁リレー

原則として、強制ガイド式安全リレー、非溶着リレー又はこれと同等以上の安全性を持つものであること。

(6)　電磁弁

イ　複式であることが望ましいこと。

ロ　ノーマルクローズ型であること。油圧式についてはスプリングリターン型、空気圧式についてはプレッシャーリターン型であること。

ハ　ソレノイドの断線故障によって弁が常時開状態となり、機械を停止できなくなることを防止するため、ノーマルオープン型でないこと。

(7)　ブレーキ

イ　ノーマルクローズブレーキ、複式ブレーキ又はこれと同等以上の安全性をもつものであることが望ましいこと。

ロ　ブレーキ作動用励磁コイル等の断線によってブレーキが作動しなくなり、機械を停止できなくなることを防止するため、ノーマルオープン型でないことが望ましいこと。

5―2　　回路のフェールセーフ化対策

(1)　再起動防止回路

原則として、自己保持回路として構成されており、起動時に自己保持回路の保持を開始し、停電時、トラブル発生時、安全装置の作動時及び非常停止装置の操作時等には、自己保持回路の保持を解除して再起動を防止するものであること。

(2)　ガード用のインターロック回路

イ　固定ガード用のインターロック回路では、原則として、固定ガードの取り外しによって再起動防止回路の自己保持を解除し、その後固定カードが正常な状態に復帰し、かつ、作業者が再起動操作を行わなければ機械が再起動しない機能を有するものであること。

ロ　可動ガード用のインターロック回路では、原則として、可動ガードを開くことによって再起動防止回路の自己保持を解除し、その後可動ガードを閉じ、かつ、作業者が再起動操作を行わなければ機械を再起動しないものであること。

(3)　操作監視用の回路

作業者の押しボタン操作によって起動信号を発生させる回路では、起動ボタンを押して接点を閉じる動作に続けて、起動ボタンを離して接点を開く動作を行ったときに初めて起動信号を発生させることが望ましいこと。

(4)　論理回路

イ　故障時には必ず出力がオフとなるように構成されているものであること。

ロ　入出力信号は、原則として、電源電圧より高いこと。

ハ　オンディレー用の回路では、故障時には必ず出力がオフとなるか、又は出力がオンとなるのが遅れる側となるものであること。

ニ　オフディレー用の回路では、故障時は必ず出力がオフとなるか、又は出力がオフとなるのか早まる側となるものであること。

(5)　電磁リレーの制御回路

イ　電磁リレーの制御回路では、a 接点が閉じたとき、機械が駆動するように回路が構成されていること。電磁リレーには、原則として、強制ガイド式安全リレー、非溶着リレー又はこれと同等以上の安全性を有するものを使用すること。

ロ　強制ガイド式安全リレーを使用した回路については、リレーの接点を二重化し、二つの接点の動作が不一致のときは接点に溶着が起きたとみなして、機械を停止させるものであること。

ハ　a 接点が閉じたときに機械が停止するように回路を構成すると、接点の接触不良によって機械を停止できなくなるため、このような回路を構成してはならないものであること。

ニ　b 接点が閉じたときに機械が作動するように回路を構成すると、励磁コイル等の断線によって b 接点が閉じたままとなり、機械を停止できなくなるため、このような回路を構成してはならないものであること。

ホ　複数のリレーを使用する場合は、安全情報がユネイトに伝達するように、途中に否定回路を設けてはならない。

(6)　電磁弁の制御回路

複式電磁弁を使用した回路では、弁の開閉状態を直接的に検出する手段を設け、二つの弁の動作が不一致のときは、弁に開固着が起きたとみなして機械を停止させるものであること。

(7)　可動部の駆動回路

イ　電動機をアクチュエータとする機械では、電動機へのエネルギー供給を直接遮断するか、又は電動機を制御するリレーの励磁コイルへの通電を直接遮断することによって、機械の可動部を停止させるものであること。

ロ　油空圧機器をアクチュエータとする機械については、油空圧機器を制御する電磁弁のソレノイドへの通電を直接遮断することによって、機械の可動部を停止させるものであること。

6　フェールセーフ化に準ずる方法

フェールセーフ化された制御機構は、故障によってシステムが停止するため、その実用性を十分なものにするには、必要に応じ、高信頼化等の手法の採用によって稼働率の低下を防ぐ必要がある。このような手法には、部品の高信頼化のほかに次のようなものがある。

イ　質の異なるものの二重系

通信における有線ケーブルと無線のように、同じ機能であっても質の異なるものによる二重の系を使用する方法

ロ　マスク

制御機構を構成する要素に全く同じものを二つ以上設け、そのうちのいくつかに故障が生じても他が正常ならば、その故障をマスク(遮断)して外に出さない方法

ハ　デュアル

制御機構を構成する要素に全く同じものを二つ設け、お互いに出力をチェックし合い、故障した方がわかる場合は切り替える方法

ニ　デュープレクス

制御機構を構成する要素に正と副の二つを設け、正に障害が発生した場合は副に切替える方法

ホ　三重多数決

単一誤りを訂正し、どれが誤ったかを知るために制御機構を構成する要素に全く同じものを三つ設け、これらの多数決で出力する方法

(以上)

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の運用上の留意事項について

改正履歴　　平 10.7.28

事務連絡
平成 10 年 7 月 28 日

標記については、平成 10 年 7 月 28 日付け基発第 464 号をもって通達されたところであるが、運用上の留意事項を別添のとおりとりまとめたので、了知の上、関係者に対する指導に遺憾のないようにされたい。

なお、別紙 1 及び別紙 2 により関係団体あて通知したので了知されたい。

「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」の運用上の留意事項

「1　総則」について

(1) 趣旨

ガイドラインで対象とする工作機械とは、JIS B0105 に定める旋盤、ボール盤、中ぐり盤、フライス盤、平削り盤、形削り盤、立削り盤、ブローチ盤、金切り盤・切断機、研削盤、表面仕上盤、歯切り盤、歯車研削盤、歯車仕上盤、特殊工作機械及びその他の工作機械をいう。

ガイドラインで対象とする成形機とは、射出成形機（労働安全衛生規則第 147 条）、圧縮成形機、 押出し成形機等をいう。

「これらの設備と一体となって使用される搬出入装置」には、製品の自動供給装置、自動排出装置、コンベヤ、ストッカ、フィーダ等が含まれる。

また、「一体」とは、次のような場合が該当する。

[1] 複数の機械の可動部の運転領域が重なる場合

[2] 複数の機械の制御系の間で情報のやり取りがある場合

ガイドラインの主な対象は工作機械であるが、制御回路の不都合に起因して発生する労働災害は、工作機械や成形機と一体となって使用される搬出入装置において多く発生していることから、ガイドラインでは、これらの機械を包括的に工作機械等としてとらえたものである。

ガイドラインは、制御機構のフェールセーフ化に関する原則や手法について示したものであるが、一部、高信頼化設計とタンパレジスト設計（作業者による意図的な安全スイッチ等の無効化を防止するための設計）についても示している。

高信頼化設計について示しているのは、フェールセーフな制御機構の信頼性が低いと機械が停止する頻度が高くなり、実用上問題が起こるためである。

また、タンパレジスト設計について述べているのは、我が国では、安全関連機器の無効化によって災害に至る場合が多いためである。

「開発、設計、製造及び改造等に携わる者」とは、ガイドラインが工作機械等の設計者や製

造者だけでなく、すでに購入した工作機械等の制御機構を改造する生産技術者や安全担当者も対象とする趣旨である。

(2) フェールセーフ技術の意義

安全確認システムとは、安全が確認されているときに限り機械の運転を許可する制御システムであり、次の機能をすべて持つものである。

[1] 安全か否かを判断するために、あらかじめ定めた安全の条件（例えば、作業者が機械の可動範囲内に侵入していない、機械が暴走していないなど）が満足されているかどうかを機械側で確認する機能

[2] 安全の条件を満足しているときに限り、機械の運転を許可する機能

[3] 安全の条件が満足できなくなったときは、機械の運転を開始させないか又は直ちに機械の運転を停止させて、作業者の安全を確保する機能

例えば、産業用ロボットの可動範囲内に「人がいない」かどうかを安全装置によって常時確認し、可動範囲内に「人がいない」ことが確認できるときに限りロボットの運転を許可し、可動範囲内に「人がいない」ことが確認できなくなったときは、直ちにロボットの運転を停止するシステムなどは、安全確認システムの典型的な例である。

図１は、ロボットを例とする安全確認システムの例である。

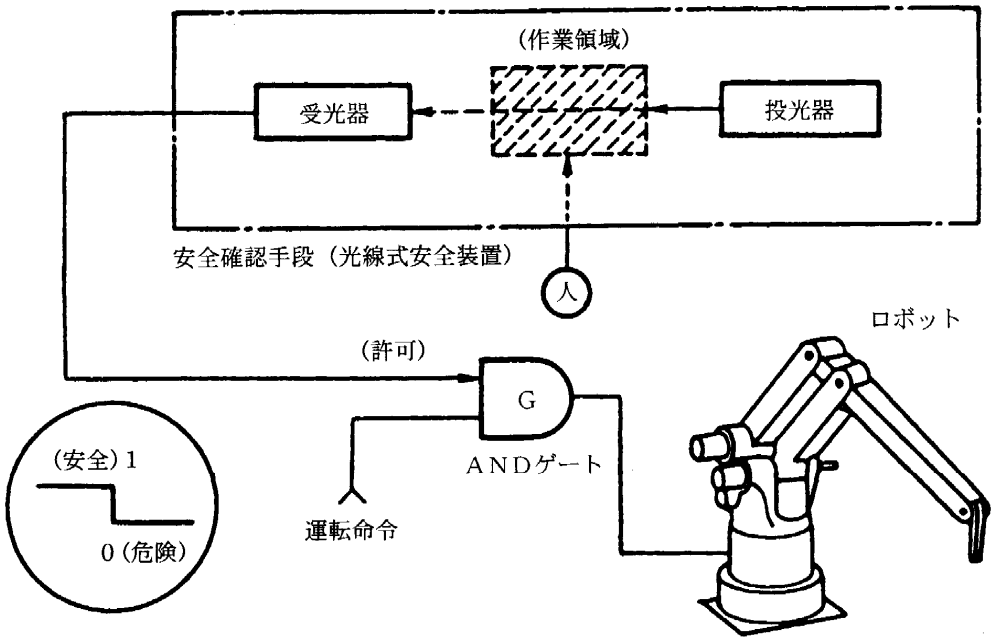


図１　ロボットを例とする安全確認システムの例

図２は、インターロックガードを開いたときに電源が遮断されるように安全スイッチを設けた例であるが、このスイッチは、図２(a)のように使用されると、接点が接点溶着を起こしたり、バネが破損したり、摺動部が引っかかったりした場合は、接点が閉じたままになるおそれがあるため、

ガードが開いているにもかかわらず機械が運転を開始してしまう。これは、接点がバネの力だけで開く構造となっているからである。

注）スイッチには、作業者による意図的な無効化を防ぐために、覆いを設ける必要がある。

これに対し、図２(b)のようにガードの蝶番点にカムを取り付け、ガードが開いたときはカムの作用によって接点を直接切り離す構造とすれば、仮に接点溶着やバネの破損、摺動部の引っかかり等が生じていても、接点は切れ、機械は停止する。

これは、人間がガードを開ける等の危険行為を行うときの力を直接利用して接点を強制的に引き離し、フェールセーフを保証しているものである。表１は、図２のインターロックガードの故障解析結果である。

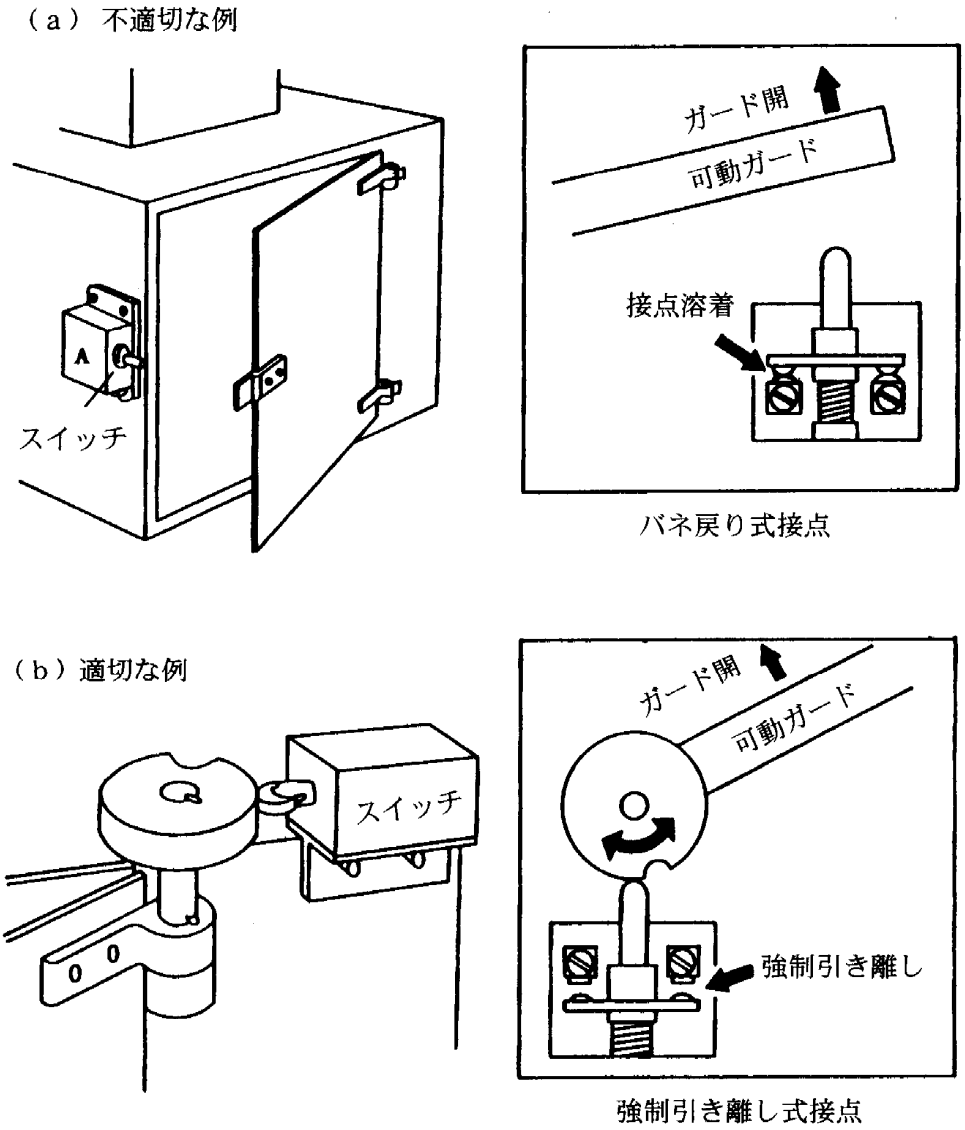


図２　インターロックガードの例

表１ インターロックガードの故障解析結果

故障モード		図2(a)の安全スイッチ	図2(b)の安全スイッチ
電気系	断線	機械停止	機械停止
	接触不良	機械停止	機械停止
	溶着	機械停止せず	機械停止
機械系	摺動部固着	機械停止せず	機械停止
	バネの折れ	機械停止せず	機械停止
	バネのヘタリ	機械停止せず	機械停止

(3) ガイドラインで記載していない手法の扱いについて

ガイドラインでは、工作機械等のフェールセーフ化に関する主要な手法を示しているが、今後、これと同等以上のフェールセーフ性を持つ他の手法が開発される可能性がある。

新しく開発された手法は、安全技術の高度化を図る意味からも積極的に採用すべきと考えられるが、同時に、これらの手法の採用にあたっては、そのフェールセーフ性を事前に十分確認しておく必要がある。

新しく開発された手法のフェールセーフ性を事前に確認するには、例えば FMEA（Failure Mode Effect Analysis）などを用いる方法が有効と考えられる。

「２ 定義」について

(1) 安全情報

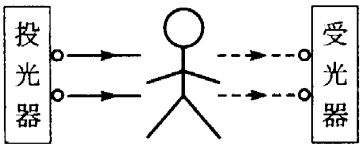
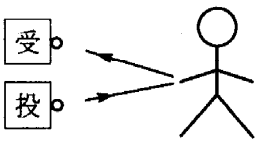
「安全装置等」には、光線式安全装置、両手操作式安全装置、ガード式安全装置等だけでなく、インターロックガードの安全スイッチやリミットスイッチ、電磁リレー、電磁弁等の部品類も含めるものとする。

「安全の確認」とは、作業者が機械の可動範囲内に侵入していない、機械が暴走していない等の確認などをいうものである。

「安全情報」は、安全側を高エネルギー状態、危険及び故障側を低エネルギー状態に対応させるものとする。これは、例えば、表 2(a)に示す透過型の光線式安全装置は、安全を意味する信号を高い電圧（オン信号)に対応させているため、故障によって信号がオフになると、これは危険とみなされて機械は停止する（安全確認型）が、表 2(b)に示す反射型の光線式安全装置は、安全を意味する信号を低い電圧（オフ信号）に、危険を意味する信号を高い電圧（オン信号）に対応させている（危険検出型）ため、故障によって信号がオフになると、安全だからオフ信号となっているのか、故障してオフ信号となっているのか区別がつかないためである。

表２の趣旨は、反射型の光線式安全装置を問題とすることではなく、安全装置に関する信号処理のあり方を問題とするものである。

表２　透過型光線式センサの故障特性

区　　分	(a)　透過型	(b)　反射型
装置の形態		
受光器出力	オン：「人間がいない」(安全) オフ：「人間がいる」(危険) オン（安全） オフ（危険）　オフ（危険）	オン：「人間がいる」(危険) オフ：「人間がいない」(安全) オン（危険） オフ（安全）　オフ（安全）
投光器が故障したときの挙動	作業者が光線を遮光したのと同じ状態となるため、機械は停止し、作業者の安全が確保できる。	危険領域内に作業者がいるにもかかわらず、作業者からの反射光を検出できなくなるため、機械を停止できなくなる。

(2) 非対称誤り特性

「安全側」とは、機械が停止する側をいう。また、「安全側の状態に固定する」とは、機械を停止したり、作業を中止したりすることをいう。

「安全側に誤る故障」とは、機械が停止する側の故障をいう。これに対し、「危険側に誤る故障」は、機械が停止できなくなる側の故障である。

(3) ユネイトな情報伝達

図２のインターロックガードでは、ガードの閉鎖が直ちに機械の運転につながるわけではなく、次に示すように、途中にいくつかのステップが存在する。

[1] ガードの閉鎖によって安全スイッチの接点が閉じる。

[2] この接点を通って電磁リレーのコイルに電流が流れる。

[3] この電流によってコイルに吸引力が発生し、その力によってリレーの接点が閉じる。

[4] このリレー接点を通ってブレーキの励磁コイルに電流が流れ、ブレーキを開放するとともにクラッチが閉じて機械が運転を開始する。

以上の過程で特に重要なことは、安全情報の伝達要素であるスイッチ又はリレーに故障が生じたとき、各々の伝達要素が誤って安全情報を生成してはならないことである。これは、誤って安全情報が生成すると、実際は安全でないのに機械の運転が許可されるという事態が生じるためである。

このような特性を実現するためには、安全情報の伝達要素が故障したとき、必ず安全情報の生成を停止するように各伝達要素を構成しなければならない。この関係を示したのが図３である。

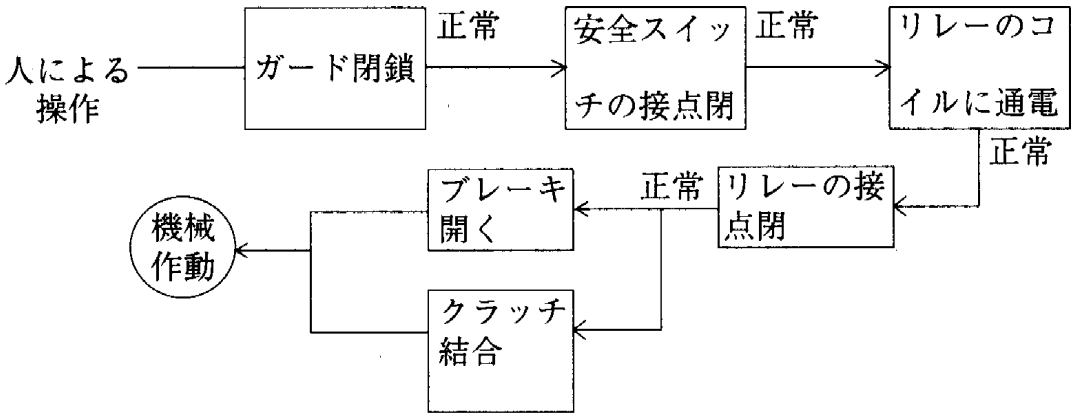


図３　インターロックガードでのユネイトな情報伝達

「３　フェールセーフ化の原則」について

(1)「フェールセーフ化の対象とする制御機構」とは、安全確認システム又はその一部であり、ガイドラインでは、通常の場合に安全確認システム又はその一部として扱われる回路をガイドラインの表２に列挙したものである。なお、フェールセーフ化の対象はガイドラインの表２に限定されるものではなく、これら以外でも安全確認システム又はその一部に該当するものがあれば、フェールセーフ化の対象となるので留意する必要がある。

「故障によって労働災害が発生するおそれのない場合」には、次のような場合がある。

[1] 機械の全周囲が固定ガードで完全に防護されているシステムに、再起動防止回路や急停止用の回路を適用する場合

この場合、回路に故障が起こって機械が止まらなくなったり、機械が不意作動を起こしたりしても、固定ガードがあるために作業者が機械と接触することはないため、必ずしも回路のフェールセーフ化を図る必要はない。

[2] 危険領域全体を監視するエリアセンサが設けられているシステムに操作監視用の回路を適用する場合

この場合、作業者が誤って起動ボタンを押しても、他の作業者が危険領域に存在している限りは機械が起動しないため、必ずしも操作監視用回路のフェールセーフ化を図る必要はない。

(2)「プログラム可能な電子制御装置」について、非対称誤り特性を有するものを使用するように努めるのは、非対称誤り特性を有しないプログラム可能な電子制御装置を使用すると、装置の暴走によって機械が止まらなくなったり、不意作動したりすることがあるためである。

(3)「安全情報は、ユネイトに伝達されなければならない」について、安全情報をユネイトに伝達するためには、少なくとも次の要件を満足しなければならない。

[1] 安全情報の伝達要素の中に、否定回路を設けてはならない。

[2] 安全情報は、周囲に存在する電磁ノイズ等のエネルギーレベルよりも十分高いエネルギーを持つこと。

[1]の否定回路とは、表３のようにシステムの入力と出力が論理的に逆転する回路をいう。図４は、電磁リレーを用いた否定回路の典型的な例である。なお、例示した回路では、電磁リレ

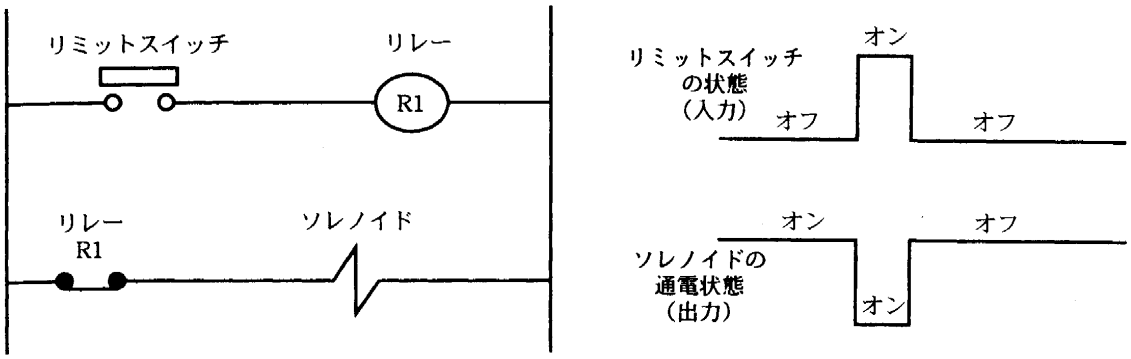
ーの励磁コイルに断線故障が起こると、機械を停止できなくなるという問題点がある。したがって、フェールセーフな回路には、否定回路を設けてはならない。

リミットスイッチがオンのときソレノイドはオフ、リミットスイッチがオフのときソレノイドはオンとなる。このような回路を否定回路という。

表 3　否定回路の真理値表

X	Y
0	1
1	0

入出力ありを１、なしを０としている。



リミットスイッチがオンのときソレノイドはオフ。リミットスイッチがオフのときソレノイドはオンとなる。このような回路を否定回路という。

図 4　否定回路の典型的な例

(4) 「環境ノイズに対する耐性の確保」とは、通常の電磁ノイズ対策や機械的ノイズ対策（振動等）を実施することである。

(5) 「行き過ぎ防止用の回路」とは、通常、限界位置検出回路と呼ばれているものである。

(6) 「ホールド停止監視用の回路」には、例えば、機械の可動部を駆動するモータ電流を監視し、この電流値が定められた範囲を超えたときは直ちに機械を停止させる回路が該当する。

(7) 「速度監視用の回路」は、通常、手動モードで機械を低速運転させるときに、機械が暴走するのを監視するために使用する。

(8) 「ホールド・ツー・ラン」は、我が国では、寸動と呼ばれていることがしばしばあるが、ここでは、寸動は次のいずれかに該当するものとし、ホールド・ツー・ランとは分けて定義する。

[1] 押しボタン等を押し続けても機械が一定距離又は一定角度以上動作しない方式

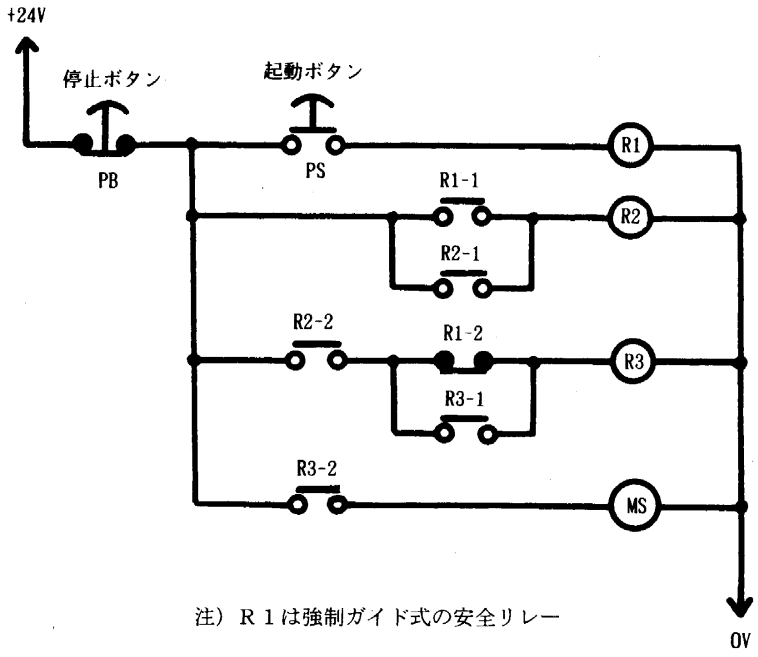
[2] 押しボタン等を押し続けても機械が一定時間以上動作しない方式

「４　フェールセーフ化の一般的方法」について

「労働災害が発生しない形で機械を停止させる」方法には、機械の特性によって、安全を確認できないときは直ちに機械を停止させる方法と、次のサイクルの運転を開始させないことで機械を停止させる方法がある。

イ　オフ確認

通常の起動回路では、作業者が起動ボタンを押すとボタンの接点が閉じて機械が起動するようになっている。しかし、この構成では、起動ボタンの接点が溶着すると、メインスイッチを入れただけで機械が不意に起動し危険である。そこで、起動操作時には、起動ボタンの接点が溶着していないことを確認した上で起動信号を発生するように回路を構成する。これがオフ確認と呼ばれる手法である。



注）Ｒ１は強制ガイド式の安全リレー

図5.1　オフ確認回路の例

図 5.1 はボイラーの起動制御回路等に利用されているオフ確認回路である。この回路は次のような手順で動作する。

[1] 起動ボタン PS を押すとリレーR1 が励磁される。

[2] 接点（R1—1）が閉じ、リレーR2 が励磁される。これにより、接点（R2—1）が閉じ、R2 が自己保持する。

[3] [2]により、接点（R2—2）が閉じるが、起動ボタンの操作中は接点（R1—2）が開いているため、R3 は励磁されない。

[4] 起動ボタン PS を離すと、接点（R1—2）が閉じ、R3 が自己保持する。

[5] 接点（R3—2）が閉じ、機械が運転を始める。

[6] 起動ボタンＰＳの接点が溶着、摺動部が固着していたりしたときは、接点（R1—2）が開いたままとなるために、Ｒ３は自己保持せず、機械は起動しない。

この回路は、リレー接点（R3—2）の溶着や停止ボタン PB の接点の溶着が起こると、機械を停止できなくなるという欠点を持っている。したがって、この回路は厳密な意味でのフェールセーフ回路とはいえないが、ここではオフ確認の意味を分かりやすく説明する必要があるために、この回路を記載した。

なお、フェールセーフ化対策のためには、少なくとも溶着が問題となる接点を二重化し、二重化された接点の挙動が一致しないときは、機械の運転を許可しない構成とする必要がある。(このような回路の基本構成については、図 5.7 を参照)

ロ　再起動防止

工作機械等による労働災害の中には、製品の位置ずれ等をセンサが検出して機械が自動停止したために、作業者が位置ずれを処理したところ、機械が不意に作動して被災したり、停電後に機械への通電が復帰したときに、機械が不意に作動し被災するという災害がある。

このような災害を防止するには、何らかの理由によって機械が停止した後は、作業者が再び起動操作をしなければ機械が再起動しないように回路を構成する必要がある。このための回路が再起動防止回路であり、通常は、再起動防止回路を自己保持回路として構成し、起動操作によって自己保持回路の保持を開始し、停電時、トラブル発生時、安全装置の作動時、非常停止装置の作動時等には、自己保持回路の保持を解除することによって機械の不意作動を防止する。

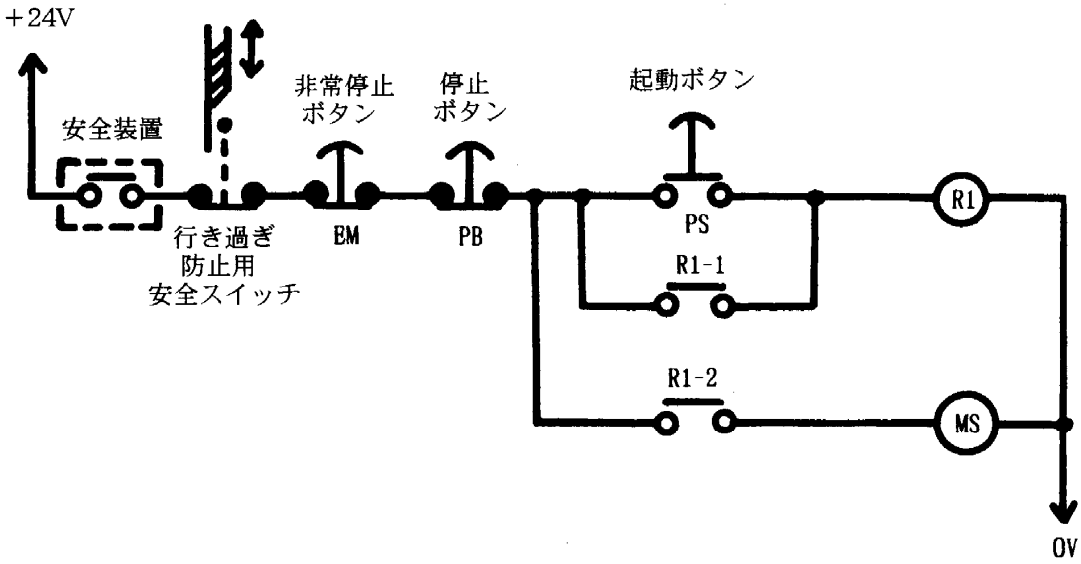


図5.2　再起動防止回路の例

図 5.2 は、この回路の基本構成図であり、次のような順序で動作する。

[1] 起動ボタンＰＳを押すと、リレーＲ１が励磁されて接点（R1—1）が閉じる。この結果、ボタンを離してもリレーR1 は励磁されたままとなる。これをリレーの自己保持という。

[2] 接点（R1—2）が閉じることにより、メインコンタクタ MS が励磁され、機械が運転を始める。

[3] 停止ボタン PB を押すと、リレーR1 が無励磁となり、接点（R1—2）が開いて機械が停止す

る。

[4] その後、停止ボタン PB を離すと、ボタン PB は復帰位置に戻るが、既に R1 が無励磁となっているので、起動ボタン PS を押さない限り、機械は再起動しない。

[5] 安全装置が作動したとき、位置検出用ドグが行き過ぎ防止用安全スイッチと接触したとき及び非常停止装置が操作されたときは、起動ボタン PS を押さない限り機械は再起動しない。

この回路は、リレー接点（R1—2）の溶着、行き過ぎ防止用安全スイッチの接点の溶着、停止ボタンＰＢの接点の溶着又は非常停止ボタンＥＭの接点の溶着が起こると、機械を停止できなくなるという欠点を持っている。また、起動ボタンＰＳの接点の溶着が起こると、電源を投入しただけで機械が突然作動を開始してしまう。したがって、この回路は厳密な意味のフェールセーフ回路とはいえないが、ここでは再起動防止の意味を分かりやすく説明する必要があるために、この回路を記載した。

なお、フェールセーフ化対策のためには、少なくとも溶着が問題となる接点を二重化し、二重化された接点の挙動が一致しないときは、機械の運転を許可しない構成とする必要がある。（このような回路の基本構成については、図 5.7 を参照）

ハ　ノーマルクローズ型の利用

ノーマルクローズ型の利用とは、この型の弁やブレーキを採用することによって、故障時には流路の遮断や機械の停止がおこり、安全が確保される方法のことである。

例えば、ノーマルオープン型の電磁弁は、ソレノイドに断線故障が起こると、弁が常に開いた状態となり、機械を停止できなくなる場合がある。したがって、機械の駆動回路に使用する電磁弁は、ソレノイドに通電がなくなることにより弁が閉じるノーマルクローズ型のものとする必要がある。

また、ノーマルオープン（正作動）型のブレーキは、ブレーキの励磁コイルに断線故障が起こると、ブレーキが作動しなくなり、機械を停止できなくなる場合がある。したがって、機械の可動部の停止に使用するブレーキは、励磁コイルに通電がなくなることによりブレーキが閉じるノーマルクローズ負作動）型のものとする必要がある。

ニ　強制引き離し

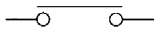
強制引き離しについては、ガード式インターロック及び行き過ぎ防止用リミットスイッチに用いられる。

強制引き離し式のガード式インターロックについては、図２を参照すること。

また、行き過ぎ防止用リミットスイッチに関して、行き過ぎによる危険とは、機械の危険な可動部が行き過ぎて人体と直接接触したり、行き過ぎにより機械の他の部分を破壊し、その部分が人体に向けて落下するなどの危険をいう。

いま、このスイッチにノーマルオープン型（a 接点タイプ図 5.3(a)参照）のリミットスイッチを使用すると、接点の接触不良が生じたときに機械を停止できなくなるおそれがある。このため、行き過ぎ防止用のリミットスイッチは、機械の可動部がリミットスイッチと直接接触したときに接点を強制的に引き離すノーマルクローズ型（b 接点タイプ図 5.3(b)参照）のものを使用する必要がある。

(a)
ノーマルオープン型（a 接点タイプ）



通常は接点が開いており、ボタンを押すことによって、接点が閉じる構成のスイッチ。通常は白丸で表す。

(b)
ノーマルクローズ型（b 接点タイプ）

通常は接点が閉じており、ボタンを押すことによって、接点が開く構成のスイッチ。通常は黒丸で表す。

図5.3　ノーマルオープン型スイッチとノーマルクローズ型スイッチ

表 4.1 は、リミットスイッチに a 接点タイプのものと、b 接点タイプのものを使用したときの故障解析結果である。

表 4.1　行き過ぎ防止用リミットスイッチの故障解析

故障モード		a接点タイプ	b接点タイプ
電気系	断線	機械停止せず	機械停止
	接触不良	機械停止せず	機械停止
	溶着	機械停止	機械停止
機械系	摺動部固着	不定	機械停止
	バネの折れ	不定	機械停止
	バネのヘタリ	不定	機械停止

ホ　相反モードによる監視の利用

機械のインターロック用ガードでは、ガードが開いていることを確認するためのリミットスイッチ（直接作動によってスイッチがオフする方式、すなわち正モードスイッチ）と、ガードが閉じていることを確認するためのリミットスイッチ（直接作動によってスイッチがオンする方式、すなわち負モードスイッチ）の二種類を設けて、ガードの開閉状態の正常確認を行うことがある。正負の異なるモードのスイッチを使用してガードの開閉の正常性を確認することから、これを相反モードによる監視という。

図 5.4 はそのための回路の構成例であり、次のような順序で動作する。

[1] 起動ボタン PS を押すと、リレーR1 が自己保持し、接点（R1—2）が閉じて、制御回路側に電圧 が加えられる。

[2] ガードが開いているときは、スイッチＳ１及びＳ２が閉じ、R2 が自己保持する。

[3] ガードを閉じると、スイッチＳ３及びＳ４が閉じ、R3 が自己保持する。

[4] 接点（R3—1）が開き、R2 の自己保持が解除される。

[5] 以上のように、R2 自己保持→R3 自己保持→R2 自己保持解除という順序を経たときに限り、接点（R2—3）及び（R3—3）が閉じて、機械が運転を開始する。

[6] S１に溶着が生じたときは、S３が閉じないため、R3 は自己保持されない。S２に溶着が生じたときは、S４が開くために、R3 は自己保持されない。S３に溶着が生じたときは、S１が開くため、R2 は自己保持されない。S４に溶着が生じたときは、S２が閉じないため、R2 は自己保持されない。これらにより、機械は運転を開始しない。

[7] S１又はS２に接触不良が生じたときは、R2 は自己保持されない。S３又はS４に接触不良が生じたときは、R3 は自己保持されない。これらにより、機械は運転を開始しない。

[8] [6]及び[7]の故障は、少なくとも次にガードが閉じるときまでに検出され、そのとき機械は停止したままとなる。

なお、S１からS４は、S１が溶着したときはS３が開き、S２が溶着したときはS４が開き、S３が溶着したときはS１が開き、S４が溶着したときはS２が開く構造でなければならない。

この回路は、停止ボタン PB の接点溶着が起こると、機械を停止できなくなる。また、起動ボタン PS の接点溶着が起こると、電源を投入しただけで機械が突然作動を開始してしまう。したがって、この回路は厳密な意味のフェールセーフ回路とはいえないが、ここでは相反モードによる監視の意味を分かりやすく説明するために、この回路を記載した。

なお、フェールセーフ化対策のためには、少なくとも溶着が問題となる接点を二重化し、二重化された接点の動作が一致しないときは、機械の運転を許可しない構成とする必要がある。(このような回路の基本構成については、図 5.7 を参照)

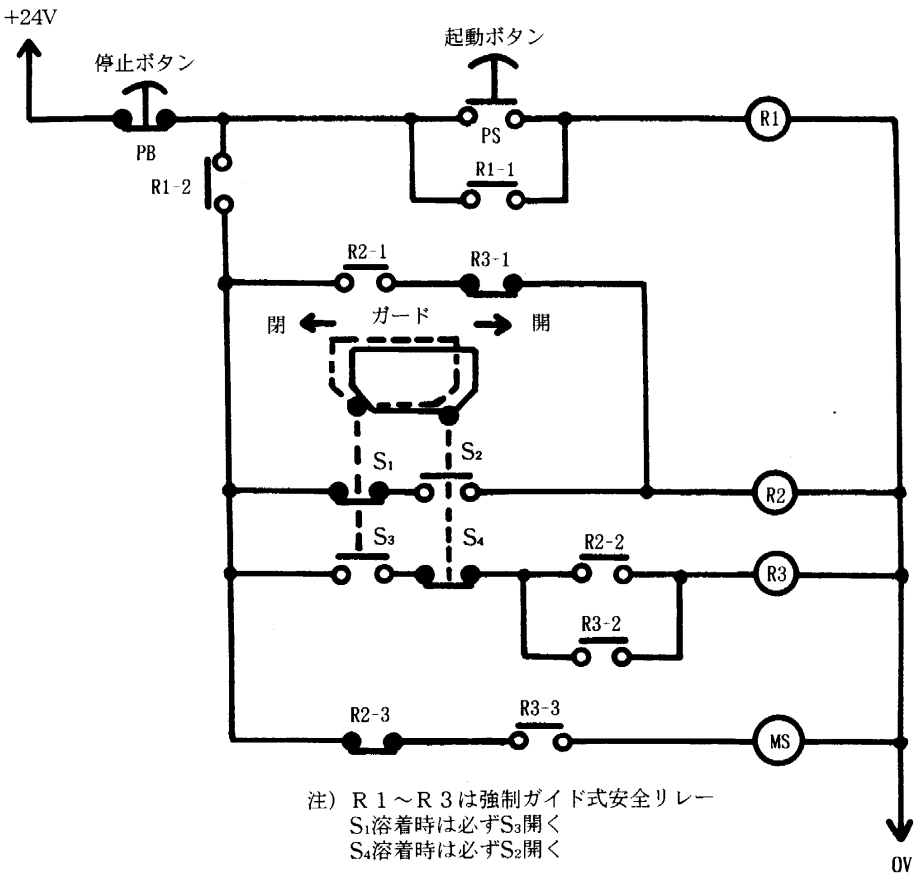


図5.4　相反モードによる監視の例

へ　発振回路の利用

発振回路及び交流信号を利用する回路では、回路を一種の交流発振器（発振周波数は 200 kHz 程度）として構成している。ここで交流発振を利用するのは、発振による信号は直流信号に比べて高いエネルギー消費を必要とし、かつ、通常は発振回路の故障によりエネルギーレベルの高い交流信号を生じないためである。

図 5.5(a)は、交流発振器を使用したフェールセーフな AND 回路である。図で OSC は交流発振部、AMP は増幅部、REC は整流部を意味する。ここで、OSC 部は、入力Ｉ1 又はＩ2 がないとき、

Q1：オフ、Q2：オン、Q3：オン

の状態であり、入力Ｉ1 及びＩ2 の同時に入力があったとき、

Q2：オフ→Q3：オフ→Q1：オン→Q2：オン→Q3：オン→Q1：オフ

の順序で発振を開始し、図 5.5(b)のような OSC 出力を生じる。この OSC 出力を増幅部で増幅し、電源との混触により誤って出力を生じないよう整流部で倍電圧整流した後、最終的な出力とする。

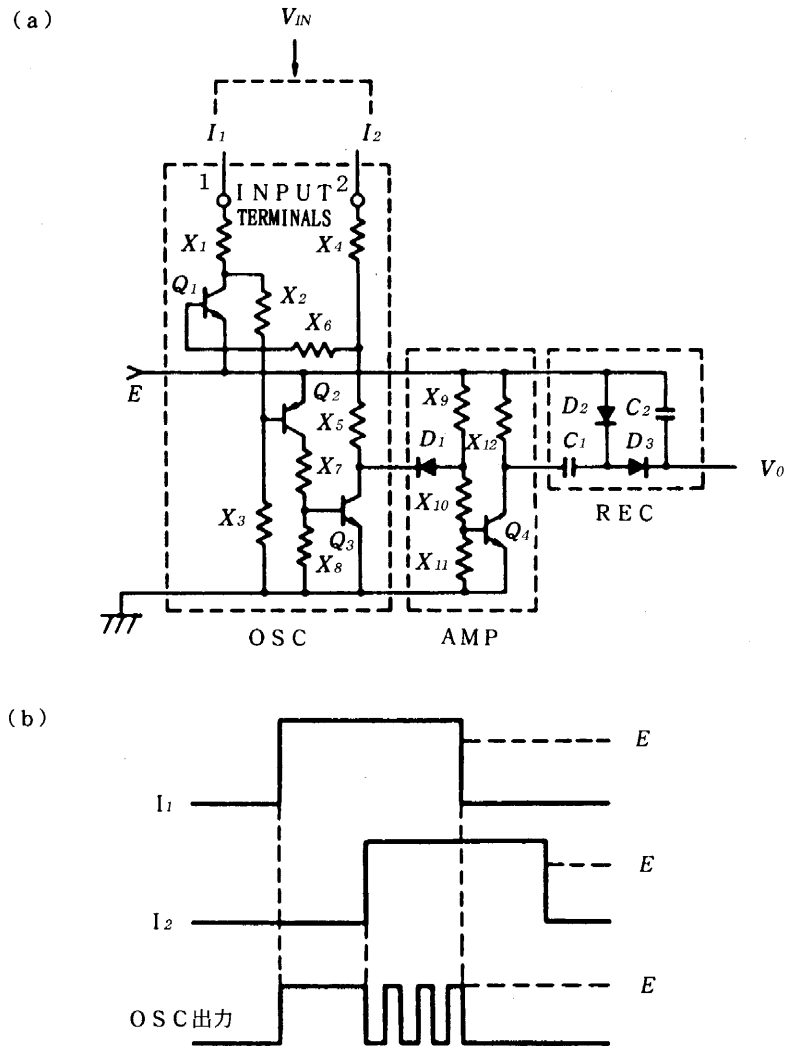


図5.5　フェールセーフなAND回路の例

表 4.2 にフェールセーフな AND 回路（図 5.5 の回路）の故障解析結果を示す。表からも明らかなように、この回路は故障時に誤って出力を生じないことが保証されている。

表 4.2　フェールセーフな AND 回路の故障解析

構成要素	記号	故障状態	故障解析
トランジスタ	Q_1 ～Q_3	3 端子間各々の短絡又は断線	演算発振器発振できず
	Q_4	3 端子間各々の短絡又は断線	発振出力なし又は出力低下
ダイオード	D_1	短絡	発振出力なし
		断線	発振出力なし
抵抗	X_1 ～X_8	断線	演算発振器発振できず
	X_9 ～X_{12}	断線	発振出力なし

ト　交流信号の利用

へと同様の趣旨である。

チ　電源枠外処理

電源枠外処理とは、安全情報を電源電圧より高い電圧に設定することにより、信号線と電源線の混触による誤った安全情報の伝達を防止する方法のことである。

例えば、図 5.5(a)の回路では、電源電圧 E に対して、安全情報 V0 をこれより高く設定すれば、仮に電源線が混触しても、これに起因して誤った安全情報が発生することはない。

リ　フェールセーフなチェック回路

「安全装置や部品類」とは、アナログ信号処理を行うものをいう。

センサに危険検出型のものを使用すると、センサが故障したとき危険を検出できなくなることがある。そこで、センサの入力側に常時検査信号（交流信号）を与え、センサが故障したとき検査信号は出力しなくなる（すなわち直流出力となる。）ようにして、センサが故障したか否かを常時確認できるようにシステムを構成する。このような原理によってセンサの正常性を確認するのがフェールセーフなチェック回路である。

図 5.6 は、危険検出型のセンサを対象にしたフェールセーフなチェック回路の構成図である。これは、次のような順序で動作する。

[1] センサ PS に情報 a（危険情報）が入力する。なお、センサ PS が危険検出型であることから、情報 a は危険側をオン信号、安全側をオフ信号としている。

[2] パルス信号発生器（PG）により、センサ PS の入力側に検査信号 b を入力する。

[3] [1]と[2]の結果、センサ PS の入力信号は d=a+b となる。これを論理的に否定した e=d がセンサ PS の出力信号である。

[4] センサ PS の検査結果は、自己保持回路（SH）に記憶され、検査パルス b の一サイクルが終了するごとに信号 c でリセットされる。

[5] 危険が検出された場合、信号 a がオンとなるため、信号 e はオフとなる。この結果、信号 h はオフとなり、機械の運転は許可されない。

[6] センサＰＳ が故障した場合､センサ出力信号eは直流となるから信号hはオフとなり、機械の運転は許可されない。

[7] パルス発生器、AND 回路、自己保持回路をフェールセーフな回路構成とすれば、これらが故障した場合でも信号 h はオフとなり、機械の運転は許可されない。

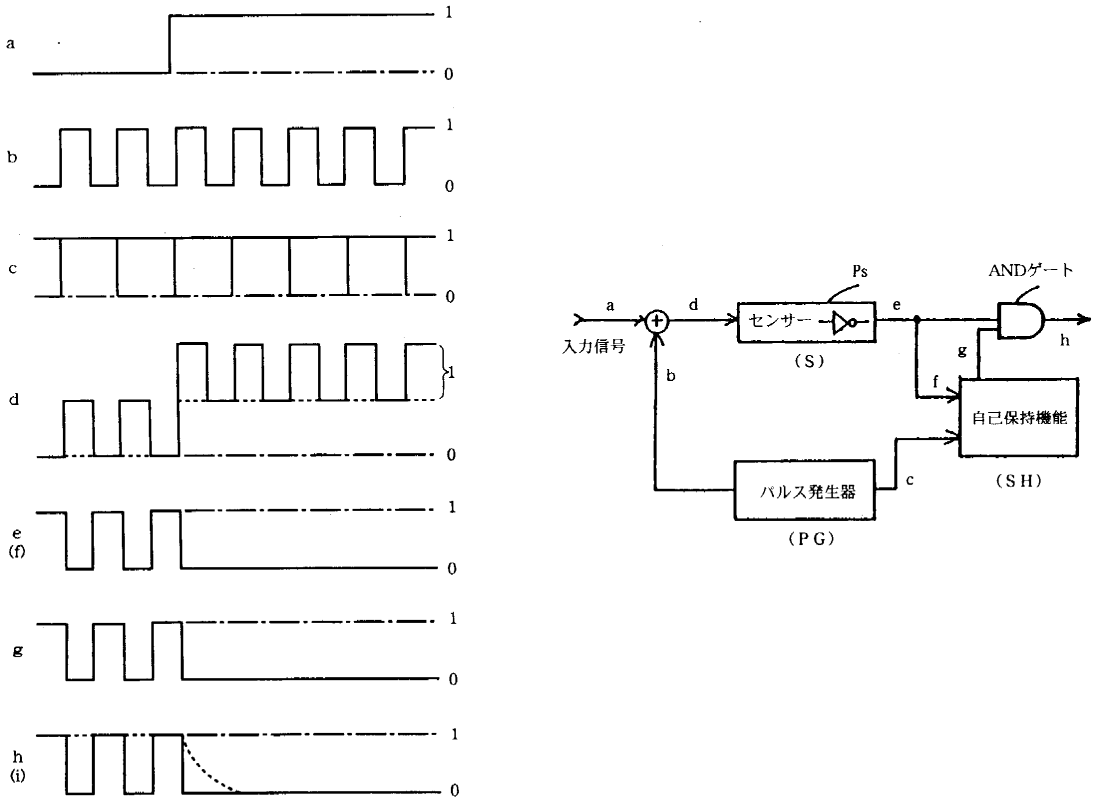


図5.6　フェールセーフなチェック回路の例

ヌ　二重化不一致検出

電磁リレーでは、a 接点に溶着が起こると、機械を停止できなくなる場合がある。そこで、リレーの a 接点を二重化し、二つの a 接点の動作が不一致の時は、接点に溶着が起きたとみなして機械を停止させるように回路を構成する。これが、二重化不一致検出回路である。

図 5.7 は二重化不一致検出回路の構成例であり、次のような順序で作動する。

[1] 起動ボタン PS を押すと、接点（R1—1）、(R2—1)、(R1—2）及び（R2—2）が閉じているため、R3 が自己保持する。

[2] 接点（R3—2）と（R3—3）が閉じ、R1 と R2 が自己保持する。

[3] 接点（R1—2）と（R2—2）が開き、R3 の自己保持は解除される（コンデンサによって R3 の解除は遅延する。)。

[4] [2]及び[3]より、接点（R1—4)、(R2—4）及び（R3—4）が閉じて、機械が運転を開始する。

[5] R1、R2 の接点のいずれかに溶着が生じたときは、接点（R1—1）又は（R2—1）が閉じないため、[1]のステップで R3 が自己保持せず、次のステップに進まない。また、R3 の接点に溶着が生じたときは、（R3—4）が閉じないため、機械は運転を開始しない。

なお、[5]が確実に実行されるためには、リレーR1、R2 及び R3 は、a 接点が溶着したとき、対となる b 接点は開いた状態に保持できる構造でなければならない。そこで、実際の回路では、次のような構造を持つリレーを使用する。

[A] a 接点と b 接点の極間短絡を防止するために、a 接点と b 接点の間は遮蔽板によって遮蔽されているか、又は、個々の接点が遮蔽室に収納された構造であること。

[B] a 接点が溶着したときは、対となる b 接点を開いた状態に保持できるように、強制ガイドを持つこと。

[C] [B]のとき、 b 接点の接点間ギャップは、0.5mm 以上を確保できること。

上記の条件を満足できるものを、強制ガイド式安全リレーという。

この回路は、停止ボタン PB の接点の溶着が起こると機械を停止できなくなる。また、起動ボタン PS の接点溶着が起こると、電源を投入しただけで機械が突然作動を開始してしまう。したがって、この回路は厳密な意味のフェールセーフ回路とはいえないが、ここでは二重化不一致検出による監視の意味を分かりやすく説明するために、この回路を記載した。

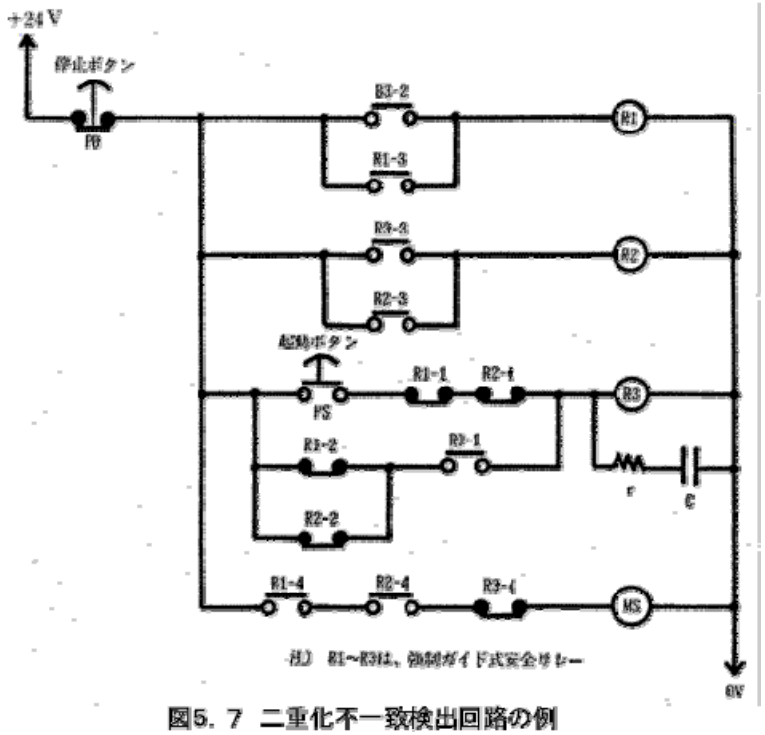


図5. 7 二重化不一致検出回路の例

ル　バックチェック

バックチェックとは、電磁リレーの a 接点に溶着が起きたことを対となる b 接点で検出し、直ちに機械を停止させるか、又は、次のサイクルの運転を開始させない方法のことである。b 接点をバック接点とも呼ぶことから、このような名称がつけられた。具体的なバックチェッ

ク接点の例としては、次のものがある。

[1] 図 5.1 の接点（R1—2）

[2] 図 5.4 の接点（R3—1）、（R2—3）、Ｓ１及びS4

[3] 図 5.7 の接点（R1—1）、（R2—1）、（R1—2）、（R2—2）及び（R3—4）

ヲ　非溶着

電磁リレーの中には、接点機構に使用する材質を適切に選定することによって、溶着が生じないように工夫したリレーもある。これを非溶着リレーと呼ぶ。例えば、銀—炭素接点の使用によって、接点が溶着しそうになると接点材料の破壊により開離する構造のリレーなどは、これに該当する。

「５フェールセーフ化の具体的方法」について

5－1　部品類の要件

「ばねリターン型」の電磁弁とは、ばねの復帰力を利用して弁を閉じる構造のものをいう。

「プレッシャーリターン型」の電磁弁とは、常時加えられている圧力（通常は油圧又は空気圧）を復帰力に利用し、弁を閉じる構造のものをいう。

「複式ブレーキ」とは、ブレーキに主ブレーキと補助ブレーキの両方を設けたもの及び冗長化したブレーキをいう。

5－2　回路のフェールセーフ化対策

操作監視用回路の具体例を、図 5.1 に示す。

再起動防止回路の具体例を、図 5.2 に示す。

ガイドライン 5(5)の「否定回路」には、例えば、図４のような回路が該当する。

「６　フェールセーフ化に準ずる方法」について

フェールセーフ化された制御機構は、故障によってシステムが停止するため、その実用性を十分なものにするには、必要に応じ、高信頼化等の手法の採用によって稼働率の低下を防ぐ必要がある。一般に、装置を高信頼に構成する方法として、次の二つの考え方があるが、ガイドラインに例を挙げたものは、次の(2)の冗長系による高信頼化の代表的な例である。

(1) 部品の高信頼化による方法（フォールト・アボイダンス）

部品の信頼度そのものを高くして、装置を構成する部品を故障しないようにする方法である。従来の一般的な方法で、品質管理（QC）手法に基づき高信頼度の部品を作るものである。

(2) 冗長化による高信頼化の方法（フォールト・トレランス）

部品に故障が発生することを認めるが、他の系でこれをカバーして、外から見る限り障害のないようにする方法である。基本的には多重系を構成するものである。

参考資料 災害事例＜略＞

別紙 1

事務連絡
平成 10 年 7 月 28 日

社団法人日本自動車工業会会長
社団法人日本電機工業会会長
社団法人機械工業連合会会長
社団法人日本ロボット工業会会長
中央労働災害防止協会会長
社団法人労働安全衛生コンサルタント会会長 殿

労働省労働基準局
安全衛生部安全課長

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の運用上の留意事項について

標記については、平成 10 年 7 月 28 日付け基発第 464 号の 2 をもって通達されたところですが、運用上の留意事項を別添＜略＞のとおりとりまとめましたので、了知の上、貴会傘下会員に対し周知されるようお願いします。

別紙２

事務連絡
平成 10 年 7 月 28 日

社団法人日本産業機械工業会会長
社団法人日本工作機械工業会会長 殿

労働省労働基準局
安全衛生部安全課長

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の運用上の留意事項について

標記については、平成 10 年 7 月 28 日付け基発第 464 号の 3 をもって通達されたところですが、運用上の留意事項を別添＜略＞のとおりとりまとめましたので、了知の上、貴会傘下会員に対し周知されるようお願いします。