Safety Documents of the National Institute
of Industrial Safety, NIIS–SD–NO.13 (1996)
U D C 62-521 : 62-783 : 621.3.07

3. 機械制御回路の安全化手法

—安全確認形の制御システム—

梅崎　重夫*, 杉本　旭*

3.1 はじめに

我国の労働災害防止対策では，機械の信頼性の向上や作業者の教育・訓練の強化によって災害発生件数の減少を図る場合も多い。これに対し，本章で提案する安全確認形の制御システム[1)~4)]では，機械は故障し作業者はミスを犯すことをまず認めた上で，仮にこれらが起きても，作業者に危害を及ぼさない構造を，システムの設計段階で構築しておくことを基本とする。これは，欧州規格に規定された設備安全対策の基本的考え方とも整合する。

安全確認形の制御システムの特徴は，制御に関連した災害を扱う際に顕著に表れる。たとえば工作機械による労働災害の中には，作業者が起動用の光線式センサを遮光したために機械が突然運転を開始して，被災するケースがある（**表1**の事例1参照)。このような災害は，我国では，作業者の不注意として片づけられる場合が多い。

また災害の中には，安全装置や安全スイッチ等の安全関連機器が故障したとか，作業者が意図的に安全関連機器を無効化したことが原因で発生する災害も多い（表1の事例2，事例3参照)。これらの災害の原因も，我国では，作業者が安全関連機器を有効に保持していなかったことが原因として，作業者側の問題として捉える場合が多い。

これに対し，本章で提案する安全確認形の対策では，災害の原因をインタロック機構等の設備対策の欠陥として捉える（表1参照)。このような対策に不可欠なのが，本章で述べるインタロック，フェールセーフ，タンパレジスト等の安全技術である。また，実際の回路設計にあたっては，非常停止回路，再起動防止回路，ガードインタロック回路，行き過ぎ防止回路，電磁リレーや電磁弁の周辺回路等を構成する際の安全化手法に関する知識も必要である。そこで，本章では，当研究所の最近の研究成果等を基に，これらの安全技術や安全化手法の概要を述べる。

*機械システム安全研究部　Mechanical and System Safety Research Division

3.2 本章で提案する設備対策の要点

3.2.1 安全確認形のインタロック機構

(1) インタロック機構の意義

工作機械等による労働災害は，作業者が機械の危険な可動部と接触することによって発生する場合が多い。このような災害を防止するには，まず，機械の危険な可動部の動作領域を固定ガード等で囲うことによって作業者と機械を空間的に分離することが基本となる。しかし，実際の作業では，両者の作業領域が重なるために，隔離によっては安全を確保できないことも多い。

このため，多くの機械では，機械の動作領域に人体が進入しそうになったことを検出する安全装置を設け，この装置からの情報に基づいて，機械の運転を許可したり，禁止したりする機構を設けている。以後，このような機構をインタロック機構と呼ぶ。

インタロック機構の役割は，作業者と機械の接点に介在して，機械の異常な動作（不意作動，暴走等）や作業者の異常な行動（誤操作，危険領域への進入等）が発生したときは直ちに機械を停止させて，作業者の安全を確保することにある。**図1**はインタロック機構の概念図である。この機構の特徴は次の2点に集約できる。

① 機械の運転が許可されるのは，安全装置からの情報に基づいてインタロック機構が安全を確認したときに限る。言い換えれば，仮に機械が異常な動作をしようとしたり，作業者が異常な行動をしたとしても，イ

表１　工作機械等の制御機構の不都合に起因して発生した災害の事例

	災害事例	原因及び対策
1	製品の搬送装置がトラブルを起こして自動停止したため，装置の横でトラブル処理作業を行っていたところ，装置に起動信号を与える赤外線センサを作業者が遮光したために，装置が自動的に起動して指を挟まれた。	この事例では，製品の到達を赤外線センサが検出して，機械を自動的に起動するように制御回路を構成していた。しかし，このような回路では，人体が赤外線センサを遮光すると機械が起動し，人体に危害を加える場合がある。そこで，このような装置では，人体が機械の可動範囲内に侵入したことを検出する安全装置を別途設け，この安全装置が人体を検出しているときは，起動信号が発生しても機械の起動を許可しないように回路を構成することが必要である。 このように，安全装置からの情報に基づいて機械の運転を許可したり禁止したりする仕組みをインタロック機構と呼ぶ。この機構は人間と機械が共同して行う作業には必須である。
2	梱包用プレス（古紙を圧縮して体積を減少させるためのプレス）の内部に蓄積したゴミを除去しようとして，作業者が圧縮室に侵入したときに，他の作業者が操作盤の起動ボタンを押したため，プレス機械のスライドが動き出し，被災者がスライドと圧縮室の壁の間に挟まれた。	このプレスには，圧縮室に出入りする扉にインタロック用のリミットスイッチが設けられていた。このスイッチでは，扉を閉じたとき，扉の動きに押されてスイッチは強制的にＯＮの状態となり操作回路が入る。一方，扉を開けたときは，スイッチ内部に設けられているバネの復帰作用によってスイッチはＯＦＦとなる。従って，起動ボタンを操作してもスライドは起動しないはずであるが，災害発生時には，スイッチを復帰させるバネが破損していたためスイッチがＯＦＦとならず，機械が起動してしまった。 このように，制御回路の中にはインタロック機構の故障によって機械が危険な動きをするものがある(これを危険側故障と言う)が，作業者の安全を確保するには，制御回路は，故障時に機械を必ず停止させる回路としなければならない。このように，故障時に安全側に固定する技術をフェールセーフ技術と言う。
3	自動機械を利用して製品を加工した後，排出する過程で，製品の送りに異常が生じて製品が正規の位置からずれたため，機械が自動的に停止した。このため，作業者が手を出して製品を正規の位置に戻す作業をしていたところ，すぐ横にあった他の搬送装置が不意に作動し，この装置に頭部を挟まれた。	この機械には，人体の侵入を防止するための固定ガードが設けられていたが，事故時は固定ガードは取り外されており，その開口部から容易に侵入できるようになっていた。また，この固定ガードには，ガードを取り外すと機械が起動しないようにインタロック用のリミットスイッチが設けられていたが，事故時にはリミットスイッチはガムテープによって意図的に固定されており，その結果，ガードを開いても機械が停止しないようになっていた。 このように，インタロック機構の中には容易に無効化できるものがあり，特に我国では，この意図的無効化によって災害に至る場合も多い。そこで，本安全資料では，インタロックやフェールセーフに加えてタンパレジスト対策（作業者によるインタロック機構等の意図的な無効化を防止する対策）も加えることにした。
4	この災害では，パレットに積み上げられた袋が荷崩れを起こし，これをワイヤ式の異常検出装置が検知して機械が自動停止したため，作業者がパレタイザの中に入って袋をパレットの上に戻す作業をしていたところ，ワイヤが正常な状態に戻った約３０秒後に，突然機械が起動し作業者が足を巻き込まれて重傷を負ったものである。 なお，パレタイザに対する起動命令は，プログラマブル・コントローラ（ＰＬＣ）から直接与えるようになっていた。	この災害の原因は，ワイヤが正常状態に復帰した３０秒後にパレタイザが自動起動するようＰＬＣにプログラムされていたことにある。従って，ワイヤが正常状態に復帰しても作業者が再起動操作をしなければ，パレタイザが自動起動することのないように再起動防止回路を組み込む必要がある。 特に，自動機械では，プログラムをユーザーが容易に変更できることから，簡単にプログラム変更を行いやすいが，自動機械と言えども，トラブル処理等の作業のときには人間が介在して作業を行うことがあるので，そのような作業も想定した上で，プログラムを組む必要がある。 なお，プログラマブルな電子制御装置(ＰＬＣ，ＭＰＵ等)によって制御される機械では，プログラムのバグ，電子制御装置の故障，ノイズの影響等が起こると，作業者の安全を確保できない場合がある。従って，電子制御装置を使用したシステムでは，安全を確認するセンサと，このセンサからの情報に基づいて電子制御装置からの命令に許可を与えるインタロック機構を別途設ける必要がある。

ンタロック機構が安全を確認しない限りは，機械の運転が許可されることはない。

② インタロック機構では，安全装置からの情報に基づいて災害の発生が予測されるときは，直ちに機械の運転を停止して，作業者の安全を確保する。この停止によって得られる安全を，筆者らは，無条件安全[1)]と呼んでいる。

(2) 危険検出形と安全確認形

インタロック機構には，危険検出形と安全確認形の2つの形態がある。このうち危険検出形とは，「危険」な状態を安全装置が検出したとき，直ちに機械を停止させる形態である。これに対し安全確認形とは，「安全」な状態にあることが安全装置からの情報に基づいて確認されているときに限り，機械の運転を許可する形態である。

両者の違いは，安全装置が故障したときに顕著に表れる（**表2**参照）。たとえば**表3**(a)に示す透過形の光線式安全装置（安全確認形の装置）では，投光器が故障して発光が停止すると，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。これに対し，**表3**(b)に示す反射形の光線式安全装置（危険検出形の装置）では，投光器が故障して発光が停止すると，危険領域内に作業者がいるにもかかわらず，この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という問題が生じる。従って，インタロック機構は，安全確認形の形態とする必要がある。

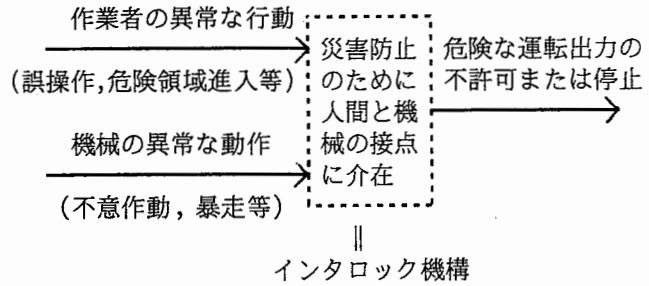


図1　インタロック機構の概念図

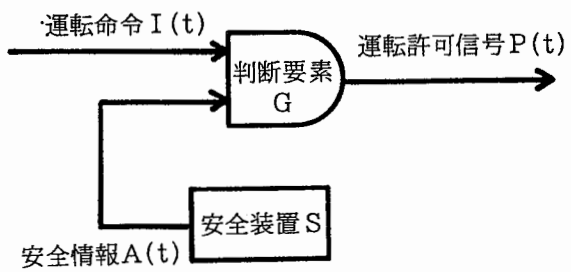


図2　インタロック機構の構成要素

(3) インタロック機構の基本構成要素

安全確認形のインタロック機構は，**図2**のような論理積演算要素を基本として構成される。

図で，I(t)は機械側に与えられる運転命令であり，作業者が起動装置を操作したときや制御装置から起動命令が発信されたときなどに「ON」となる。一方，A(t)は，安全装置Sが発信する情報であり，安全が確認できたとき（たとえば，危険領域に作業者がいないことが確認できたとき）に限って「ON」となる。以後このA(t)を安全情報と呼ぶ。

図の判断要素Gは，運転命令I(t)と安全情報A(t)の両方が「ON」の時だけ運転許可信号P(t)を「ON」とする機能を持つ。これを式で表すと次のようになる。

$$P(t) = I(t) \wedge A(t) \qquad (1)$$

(1)式で「∧」は，論理積演算（AND）を表している。ここで重要なのは，

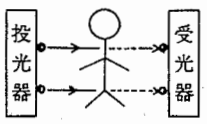
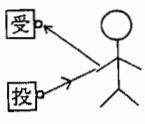
[A] 条件判断用の判断要素Gが故障しても，運転許可信号P(t)を出力しないことと，

[B] 安全装置Sが故障しても，安全情報A(t)を出力しないこと

表2　危険検出形と安全確認形

区　分	危険検出形	安全確認形
安全な状態	運転開始または運転継続	運転開始または運転継続
インタロック機構の故障		運転停止
危険な状態	運転停止	

表3　光線式安全装置の故障特性

区　分	(a) 透過形	(b) 反射形
装置の形態		
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。

である。言い換えれば，(1)式とともに，[A] 及び [B] の条件が満たされれば，仮に作業者が運転中の機械の動作領域に進入したり，作業者のミスや制御装置の故障によって運転命令 I (t)が誤って与えられても，これに起因して災害を生じることはない。これを技術的に達成するのがインタロック機構である。

実際のインタロック機構には，**表 4** に示すような種類のものがある。特に工作機械等では，ガードインタロックや，急停止，非常停止，再起動防止等のインタロック機構は必須であり，これらを機械の設計段階で確実に具備させることが安全確保の基本となる。

3.2.2 電子制御された機械でのインタロック機構

最近の工作機械は，プログラムを変更するだけで多様な作業に対応できる汎用機としての能力を備えている場合も多い。このような機械では，プログラムを適切に組むことにより，機械の運用効率を何倍にも上げて運転することも可能である。また，安全の条件についても，作業の切替毎にプログラム上で随時変更しながらインタロックを組むことができれば，機械の運用上都合が良い。このような理由から，最近，プログラ

表 4　工作機械等に用いるインタロック機構の例

区　分		内　容	関連記載箇所
1	ガードインタロック	機械の運転中に作業者が安全確保領域内へ進入することを防止する機構。機械が停止した後にガードのロック機構を解除し，作業者が安全確保領域内へ進入することを許可する方式と，ガードを開いたときに機械が急停止する方式の２つがある。	3.3.6節参照
2	ホールド停止監視	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，暴走が起きたとき直ちに機械を停止させる機構。	
3	再起動防止	急停止機構や非常停止機構の作動により機械が運転を停止したときや，停電後に機械への通電が復帰したときに，作業者等が再起動操作を行わなければ，再起動できないようにするための機構。	3.3.2節参照
4	急停止	機械側で何らかの異常を感知したときに機械の運転を停止させる機構。作業者等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。	3.3.9節参照 3.3.10節参照 3.3.11節参照
5	非常停止	作業者が何らかの異常を感知したときに機械の運転を停止させる機構。機械の運転中に人体に危害を加え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。	3.3.1節参照
6	行き過ぎ防止	機械があらかじめ設定した位置・角度等を越えて行き過ぎないように監視を行い，行き過ぎが起きたときは直ちに機械を停止させる機構。	3.3.7節参照
7	速度監視	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機構。	
8	操作監視	起動・切換等の操作が正しく行われているかを監視する機構。作業者の誤操作やスイッチの溶着等による不意作動等の防止を目的としている。	3.3.3節参照
9	ホールド・ツー・ラン	作業者が操作装置を押しているときに限って機械の危険な可動部が動作し，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機構。	

マブル・コントローラ（ＰＣ）やマイクロ・プロセッサ（ＭＰＵ）等を利用した電子制御装置が，機械の運用効率を高める制御だけでなく，安全の制御にも広く利用されるようになってきた。

しかし，プログラマブルな電子制御装置によって制御される機械では，プログラムのバグ（誤り），プログラマブルな電子制御装置の故障，ノイズの影響等によって，機械が暴走したり，不意作動を起こしたりする場合があり，直ちに重大な災害を引き起こしかねない。そこで，本安全資料では，プログラマブルな電子制御装置によって制御される機械は，いかに信頼性を向上させたとしても必ず誤るものであることを前提とした上で，仮にプログラムのバグ，電子制御装置の故障，ノイズの影響等によって電子制御装置の側から誤った運転命令が生じても，これに起因して機械の危険な動作を生じないシステムの構成について検討を行った。

いま，このシステムの構成を明確にするために，安全の条件を次の２つに区分して考える。

① 緊急安全条件

この条件を満たさないことによって直ちに災害を生じさせる可能性があるため，直ちに機械を停止させることが必要な安全の条件

② 支援安全条件

この条件を満たさなくとも直ちに災害を生じることはないが，そのまま放置すると緊急安全条件を満足できなくなるおそれがあるため，何らかの対策をとることが必要な安全の条件

上記のうち支援安全条件は，一般に緊急安全条件と比較して条件設定が複雑である等の理由から，プログラム上でインタロックを組んだ方がシステムの構成が単純になり，柔軟性に富んだ制御も可能になると考えられる。これに対し緊急安全条件では，機械を停止すべきときに停止できないという危険側の誤りを生じないことが何よりも重要であり，このためには適切な故障対策を講じたインタロック機構を必要とする。

以上のように，緊急安全条件と支援安全条件は，本来，その実現方法が明確に異なるという性質を持つ。しかし，従来の安全制御では上記２つの安全条件の差異が明確でない場合も多かったために，時として緊急安全条件に関する制御を電子制御装置に依存してしまったり，支援安全条件に対して必ずしも必要でないフェールセーフなインタロック機構を要求したりというような事態も生じていたと考えられる。

図３は，以上の議論に基づいて提案する安全制御システムの基本構成である。図で，$f_1, f_2, \cdots f_N$は機械の運用効率を向上させるための制御装置である。また，$a_1, a_2, \cdots a_N$は支援安全条件を確認するためのセンサであり，判定回路$g_1, g_2, \cdots\cdots$

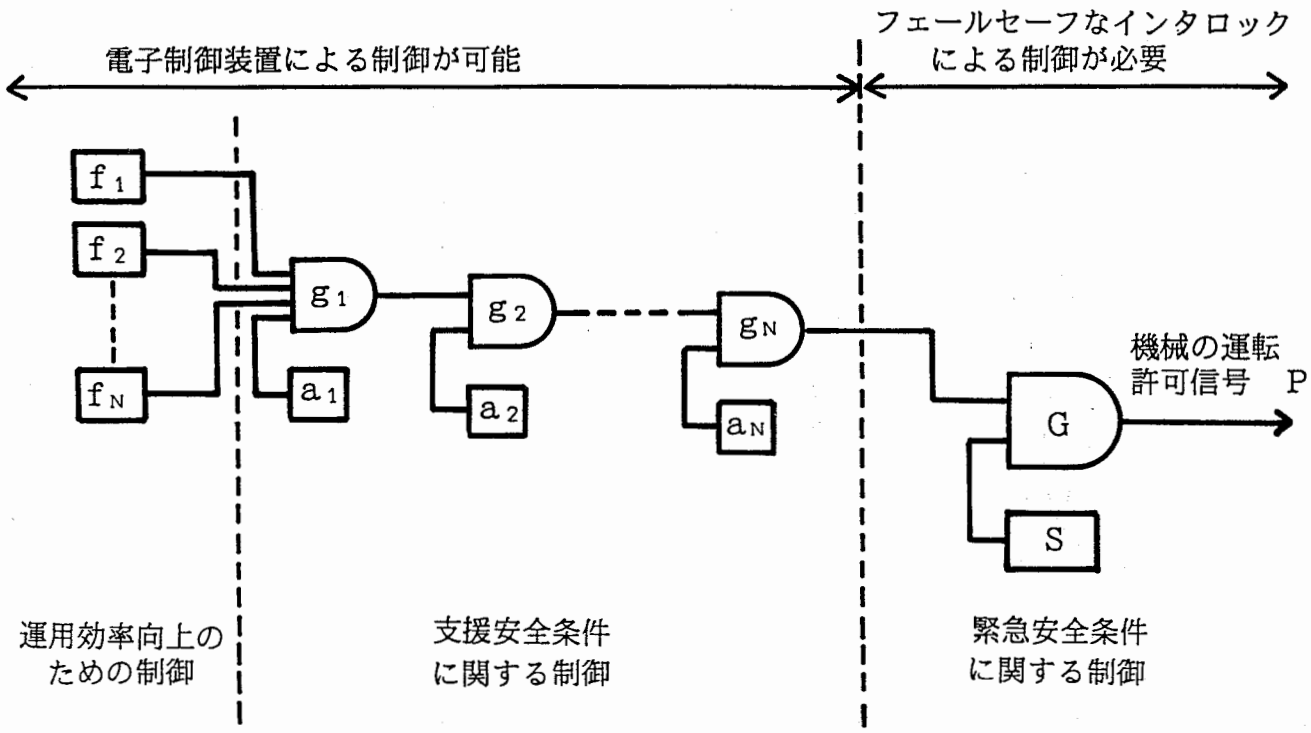


図３　階層化された安全制御システム

g_Nと共にインタロック機構を構成している。これらは，いづれもプログラマブルな電子制御装置を用いて実現することが可能である。しかし，これらの装置は，プログラムのバグ，コンピュータの故障，ノイズの影響等が起こると，作業者の安全を確保できない場合がある。そこで，これらとは別に，安全の条件を確認するためのセンサＳと，このセンサからの情報に基づいて機械の運転を許可するフェールセーフなインタロック機構Ｇによってシステムを構成するようにした。以後，この構成を階層化安全制御と呼ぶ。

3.2.3 安全確保のためのフェールセーフ

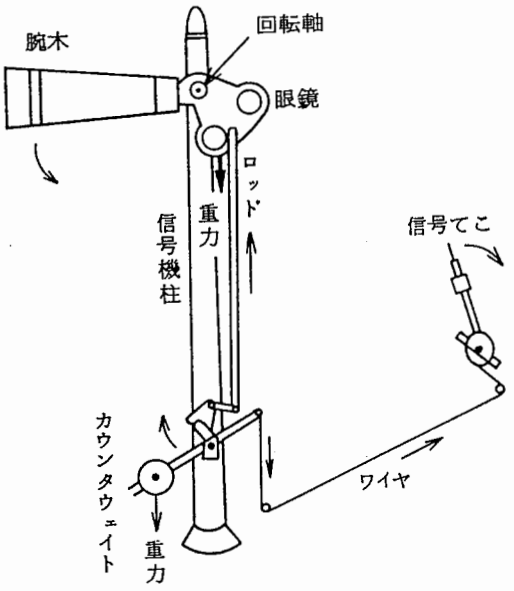
3.2.1節(3)の条件［A］，［B］は，仮に判断要素Ｇや安全装置Ｓが故障しても，誤って「ＯＮ」信号を出力してはならないことを意味している。この特性を実現するのがフェールセーフ技術であり，「故障が発生しても人命の損傷や重大な社会的混乱とはならないよう，（予め定められた）安全状態に固定し，故障の影響を限定する技術」と定義されている[5]。

この技術の歴史は，鉄道信号の分野で始まった。鉄道では，信号機の故障によって青であるべきときに赤になっても列車は停止するだけですむが，赤であるべきときに信号が青になれば重大な災害を招くおそれがある。従って，信号機が故障したときは常に赤が表示されなければならない。

図4は，かって使われていたフェールセーフな腕木式信号機である[6]。この信号機では，信号機柱に腕木を取り付け，腕木の角度で信号の状態を表示するもので，腕木の制御は信号てこによってワイヤを引いたり（列車がいないとき），緩めたり（列車が接近したとき）して行われる。腕木は水平のときが赤信号と定められているから，この機構をフェールセーフとするため，腕木より重い眼鏡と称するものを回転軸の反対側に取り付けてある。これにより，列車が接近して信号てこがワイヤを緩めたときだけでなく，万一，ワイヤが切れたり，ロッドが折れたような場合でも，眼鏡やカウンタウェイトの重力によって腕木が水平となり，安全側，すなわち赤信号を表示するようになっている。このように機械的機構のフェールセーフは，不滅の力である重力により安全側への移行を保証していることに特徴がある。

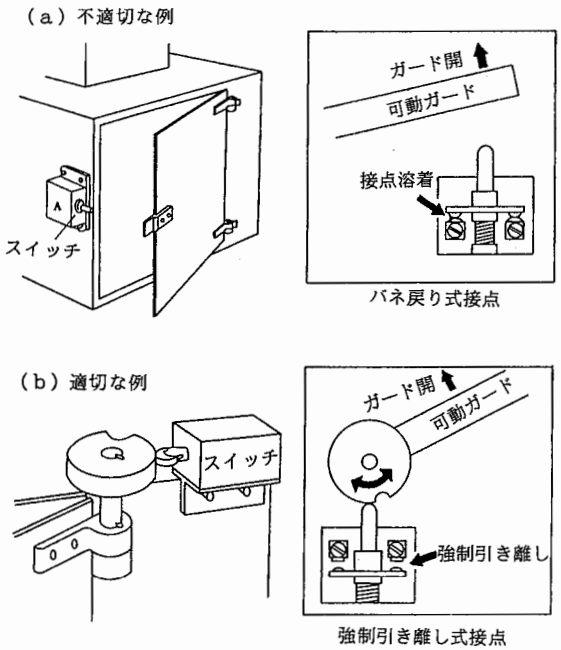
現在は，このような考え方が産業用の機械設備にも広く普及している。たとえば**図5**は，工作機械のインタロックガードを開いたとき電源が遮断されるように安全スイッチを設けた例であるが，このスイッチは，**図5(a)**のように使用されると，スイッチが接点溶着を起こしたり，バネが破損したり，摺動部が引っかかったりした場合は，接点が閉じたままになるおそれがあるため，ガードが開いているにもかかわらず機械が運転を開始してしまう。これは，接点がバネの力だけで開く構造となっているからである。

これに対し，**図5(b)**のようにガードの蝶番点にカムを取り付け，ガードを開いたときはカムの作用によっ



ワイヤの切断またはロッドの破損の場合には，眼鏡部の重量によって腕木が上がり，停止信号を示す。

図4　腕木式信号機の例(文献6より引用)



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。

図5　工作機械のインタロックガードの例

表5　ガードインタロックの故障解析

故障モード		図5(a)の安全スイッチ	図5(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

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，人間が危険行為（たとえばガードを開けるなど）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のである。**表5**に，ガードインタロックの故障解析結果を示す。

表6は，フェールセーフ化の一般的手法を分類したものである。

3.2.4 安全情報の伝達とユネイト性

前節で説明したインタロックガードでは，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共にクラッチが閉じて機械が運転を開始する。

この一連の過程では，安全情報の伝達要素であるスイッチ，リレー，クラッチ，ブレーキのいづれかに故障が生じたとき，誤って安全情報が伝達されてはならない。このためには，**図6**のように，安全情報の個々の伝達要素が故障したとき，必ず機械が停止側となることが必要である。以後，この関係をユネイトな情報伝達と呼ぶ。

表7に，ユネイトな情報伝達の真理値表を示す。ここで，情報伝達の一つの要素の入力をSi，出力をSoとし，入力ありをSi＝1，入力なしをSi＝0，出力ありをSo＝1，出力なしをSo＝0とすると，許容されない情報伝達は，「入力がない（Si＝0）にもかかわらず出力が発生する（So＝1）関係」に限られる。従って．ユネイトな情報伝達は，次式で表される。

$$Si \geqq So \qquad (2)$$

ユネイトな情報伝達を行うには，工学的な工夫が必要である。例えば，安全を伝える信号に「電流あり」を割り当てれば，電線等の故障時には「電流なし」となり，故障時に危険を示すこととなるのでユネイト性が成り立つ。また，安全を「磁力あり」に割り当てれば，コア故障時には「磁力なし」になるのでこれもユネイト性が得られる。ただし，これらの信号は，雑音で乱されるものであってはならない。

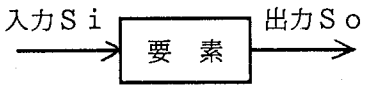
以上をまとめると，安全情報伝達の条件は次のようになる。

① 安全情報の伝達においては，安全をエネルギの高い側に，危険と故障をエネルギの低い側に割り当てる。

表7　ユネイトな情報伝達

Si	So	判　定
0	0	○（正常）
1	0	○（許容）
0	1	×（許容しない）
1	1	○（正常）

注）以上の関係を式で示すと，Si≧Soとなる。これをユネイトな関係と呼ぶ。



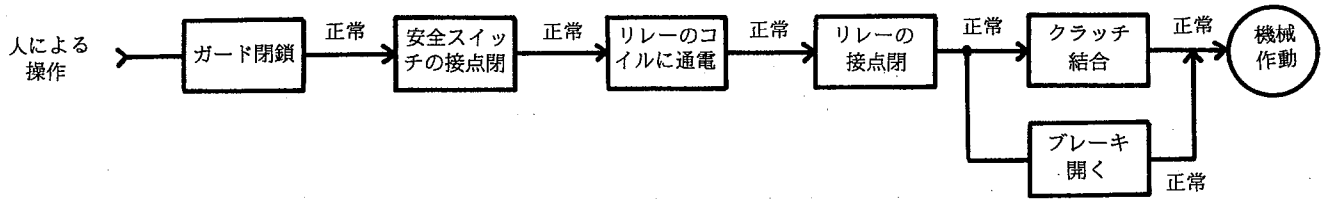


図6　情報伝達のユネイト性

表6　フェールセーフの一般的手法

手法の区分		手法の具体的内容	関連記載箇所
1	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，機械の危険な可動部がスイッチと接触するときの力などを直接利用して，スイッチのｂ接点を強制的に引き離し，機械を停止させる。	3.3.1節参照 3.3.6節参照 3.3.7節参照
2	ＯＦＦ確認	ボタンを押して接点を閉じる動作に続けて，そのボタンを離して接点を開く動作を行ったときに，初めて起動信号や始動信号を発生させる。	3.3.3節参照
3	相反モードによる監視	相反するモードのスイッチ（正モードと負モード）を２個設けて，ガードの開閉が正常であることを確認し，正常でないときは，次のサイクルの運転を開始させないか，または直ちに機械を停止させる。	3.3.6節参照
4	自己保持回路の利用	起動操作によって自己保持回路の保持を開始し，作業者が停止操作を行ったときや，安全装置が作動したときなどは，自己保持回路の保持を解除し，機械の再起動を防止する。	3.3.2節参照
5	発振回路の利用	入力のエネルギによって発振するように回路を構成しておき，故障時には発振が停止することを利用して回路の出力をＯＦＦとする。	3.3.8節参照
6	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共に，回路の出力をＯＦＦとする。	3.3.8節参照
7	電源枠外処理	安全情報を電源電圧より高い電圧に設定し，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。	3.3.8節参照
8	フェールセーフなチェック回路	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定期的にチェックする。	
9	バックチェック	ａ接点に溶着が生じたことを対となるｂ接点で検出して，直ちに機械を停止させるか，または次のサイクルの運転を開始させない。	3.3.9節参照
10	二重化不一致検出	接点や弁を二重化し，２つの動作が不一致のときは，接点や弁に溶着または固着が起きたとみなして，機械を停止させる。	3.3.9節参照 3.3.10節参照
11	非溶着	本質的に溶着しない接点を用いる。	3.3.9節参照
12	ノーマルクローズ形の利用	ノーマルクローズ形の弁やブレーキを利用することにより，故障時には流路の遮断や機械の停止が起こり，安全が確保される。	3.3.10節参照 3.3.11節参照
13	その他，非対称性を持つ物理特性の利用	たとえば，安全情報の生成が停止したときは，重力の作用によって機械的機構が自然に落下して安全を確保する方法や，過熱等が生じたとき，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などがある。	3.2.3節参照

② 安全情報は，周囲に存在するエネルギより高いエネルギレベルを持つようにする（ポテンシャル極大の条件と呼ばれる）。
③ 安全情報は，ユネイトに伝達しなければならない。

3.2.5 タンパレジスト設計

タンパレジスト設計とは，作業者が故意に安全装置やインタロック機構等の安全関連機器を無効化することができないように，覆い等を設けたり，特殊な工具でなければ取り外すことができないように工夫した設計を言う。特に，工作機械等の場合には，作業者がインタロック機構用の安全スイッチを意図的に無効化することを防止するための技術として有効である。具体的な対策例は，3.3.6節を参照されたい。

3.3 安全化手法の具体例

3.3.1 非常停止回路

非常停止ボタンは，作業者が機械を緊急に停止させたいときに操作するボタンであり，ボタンを押したにもかかわらず機械が停止しないという事態は絶対にあってはならない。

いま仮に非常停止ボタンに**図7(a)**のようなａ接点タイプのものを使用すると，接点に接触不良が起きたとき，機械が停止しないことがある。

これに対し，非常停止ボタンに**図7(b)**のような強制引き離し式のｂ接点タイプを使用すると，接点に接触不良が起きたときは，ｂ接点を介しての通電が停止するために機械は停止する。また，仮に接点溶着やバネの破損，摺動部の固着等が生じたときは，作業者が非常停止装置を操作したときに，接点が強制的に引き離されて機械が停止する。従って，非常停止ボタンには必ず図7(b)のようなｂ接点タイプのボタンを使用する必要がある。

また，非常停止用の装置の中には，コンベヤ等に適用するための緊急停止用のワイヤ（**参考資料1**のNo.20参照）があるが，この装置では，作業者がワイヤを操作したときだけでなく，ワイヤが切れたり，緩んだときにも，非常停止しなければならない。

なお，非常停止回路にプログラマブルな電子制御装置（プログラマブル・コントローラ，マイクロ・プロセッサ等）を介在させると，電子制御装置の暴走によって機械が止まらなくなることがある。そこで，非常停止回路はプログラマブルな電子制御装置を用いない回路とする必要がある。

3.3.2 再起動防止回路

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，作業者がトラブルを処理したところ，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8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言う。
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，および非常

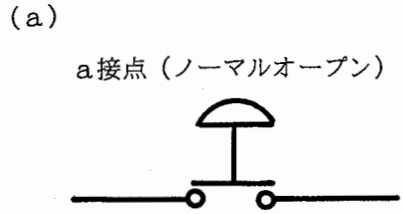


図7　非常停止ボタンの例

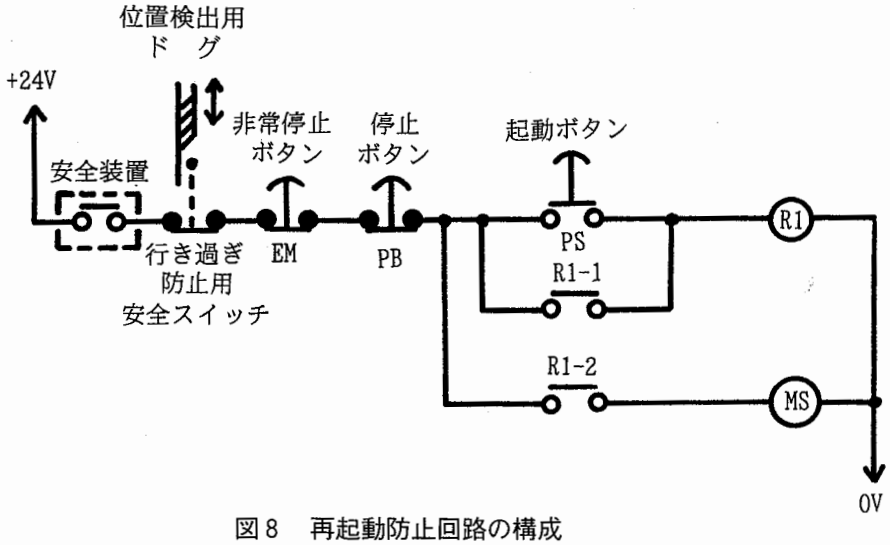


図８　再起動防止回路の構成

停止ボタンが操作されたときも，起動ボタンＰＳを押さない限り機械は再起動しない。

3.3.3 操作ボタンを利用した起動回路

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OFF確認と呼ばれる手法である。

図９は，ボイラの起動制御回路等に利用されているＯＦＦ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。

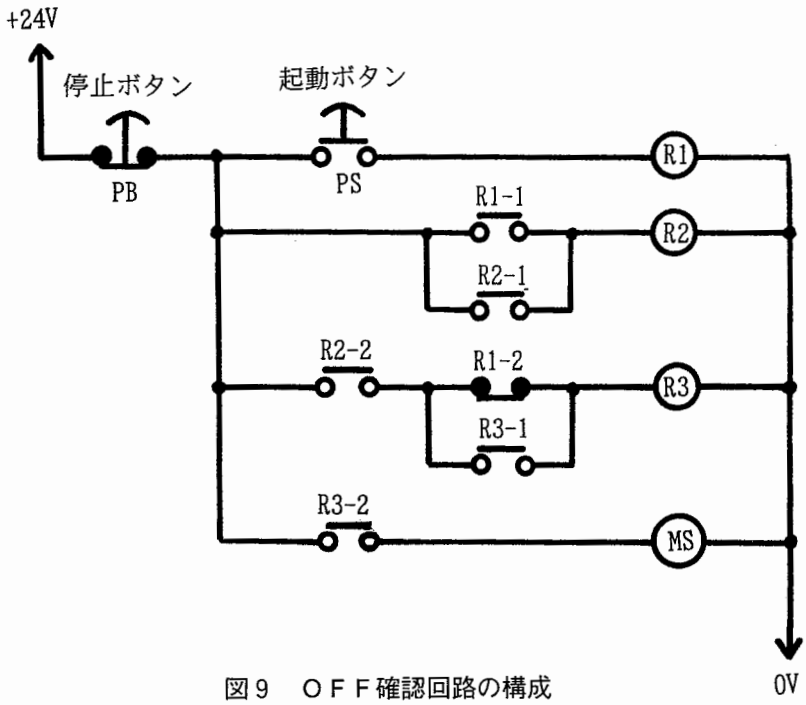


図９　ＯＦＦ確認回路の構成

⑥ 起動ボタンＰＳの接点が溶着したり，摺動部分が固着（引っかかり）したときは，接点（Ｒ１－２）が開いたままとなるため，Ｒ３は自己保持せず，機械は起動しない。

なお，ボイラで特にこの回路が重要であるのは，起動ボタンが接点溶着を起こすと，残留ガスのプレパージを行うことなくボイラが運転を開始する場合があり，残留ガスによる爆発が生じるおそれがあるためである。

3.3.4 非接触式センサを利用した起動回路

工作機械では，非接触式センサが製品の到着を検出して，機械を自動的に起動させる回路がある。たとえば，製品が所定の位置に到着したことを赤外線センサで検出し，搬送装置を自動的に起動させる回路などは，その典型的な例である。

このような回路では，一般にセンサは製品と人体を区別できないから，センサが製品の代わりに人体を検出すると，機械が不意に作動し，作業者が危害を受けることがある。そこで，このような回路では，製品を検出するためのセンサと，人体を検出するための安全装置を併設し，センサが人体を検出する前に必ず安全装置が人体を検出するように両者を配置して，上記のような災害を防止する。

なお，安全装置が人体を検出したときは，再起動防止回路の自己保持を解除し，その後作業者が再起動操作を行わなければ機械が起動しないように回路を構成する。

3.3.5 固定ガードのインタロック回路

機械作業では，段取り，保全，トラブル処理，清掃等の作業のために，固定ガードを頻繁に取り外すことがある。このような場合，固定ガードを取り外した箇所から他の作業者が機械の可動範囲内に進入すると，重大な災害を引き起こしかねない。

そこで，固定ガードを頻繁に取り外して作業を行うときは，当該作業時に機械が起動しないように，インタロック用の安全スイッチを設ける。また，固定ガードを取り外したときに再起動防止回路の自己保持を解除し，その後固定ガードが正常な状態に復帰し，かつ，再起動操作を行わなければ機械が起動しないように回路を構成する。

なお，インタロック用安全スイッチの具体例は，**参考資料１**を参照されたい。

3.3.6 可動ガードのインタロック回路

可動ガードのインタロック回路では，安全スイッチに**図５(a)**のようなバネ戻り式のものを使用すると，接点の溶着，バネの破損，摺動部の固着等が生じたときに，ガードを開いたにもかかわらず機械を停止できなくなることがある（**表５**の故障解析参照）。これに対し，**図５(b)**のような強制引き離し式のｂ接点では，表５に示すいづれの故障が生じた場合でも，機械を停止できる。従って，このような箇所には強制引き離し式のｂ接点を用いなければならない。

次に，この回路では，ガード開閉の正常性を確認するために，ガードが開いていることを確認するための安全スイッチと，ガードが閉じていることを確認するための安全スイッチの２種類を設けて，ガードの開閉状態の確認を行うことがある。**図10**は，そのための回路の一構成例であり，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印加される。

② ガードが開いているときは，スイッチS_1とS_2が閉じ，Ｒ２が自己保持する。

③ ガードを閉じると，スイッチS_3とS_4が閉じ，R_3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），（Ｒ３－３）が閉じて，機械が運転を始める。

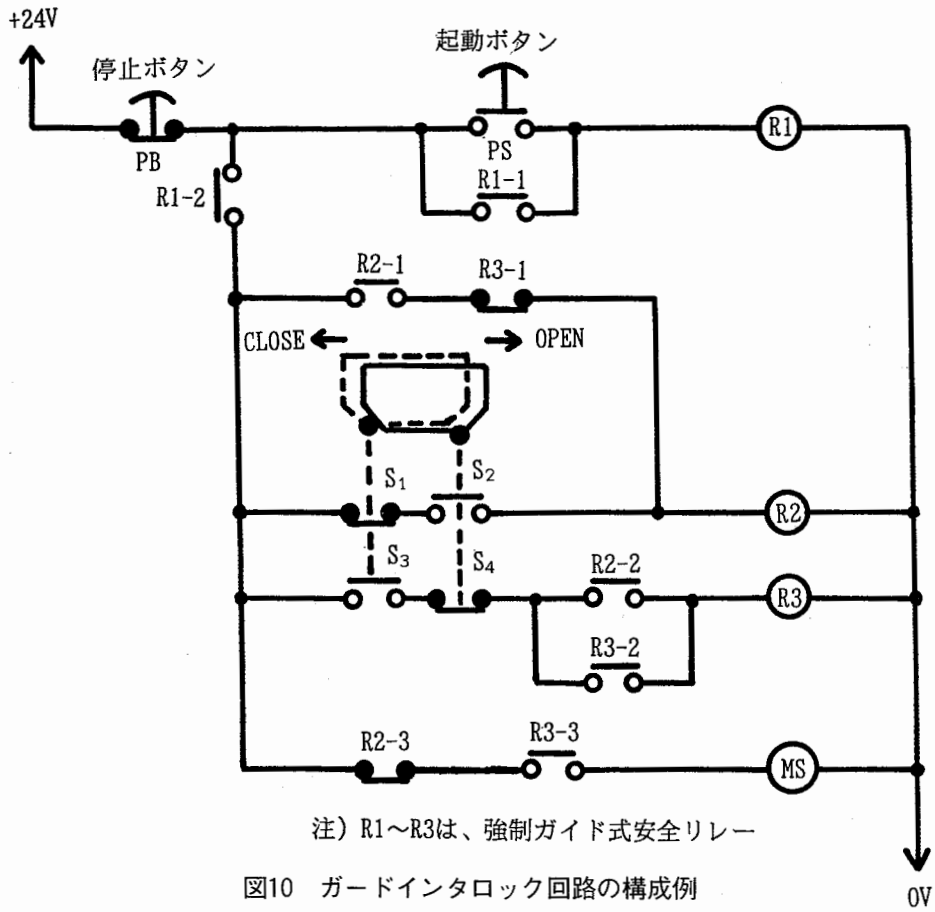
⑥ S_1に溶着が生じたときは，S_3が閉じないため，R_3は自己保持されない。S_2に溶着が生じたときは，S_4が開くために，R_3は自己保持されない。S_3に溶着が生じたときは，S_1が開くため，R_2は自己保持されない。S_4に溶着が生じたときは，S_2が閉じないため，R_2は自己保持されない。これらにより，機械は運転を開始しない。

⑦ S_1またはS_2に接触不良が生じたときは，Ｒ２が自己保持されない。S_3またはS_4に接触不良が生じたときは，Ｒ３が自己保持されない。これらにより，機械は運転を開始しない。

⑧ ⑥および⑦の故障は，少なくとも次にガードを閉じるときまでに検出され，そのとき機械は必ず停止する。

なお，S_1～S_4は，S_1が溶着したときは必ずS_3が開き，S_2が溶着したときは必ずS_4が開き，S_3が溶着したときは必ずS_1が開き，S_4が溶着したときは必ずS_2が開くという関係になければならない。このような構成の安全スイッチの具体例は，**参考資料１**を参照されたい。

次に，我国では，作業者が安全スイッチを意図的に無効化したために，止まるべき機械が止まらずに，災害となる例が非常に多い。このため，安全スイッチには，少なくとも次のような要件を満足するものを選定



注）R1～R3は、強制ガイド式安全リレー

図10　ガードインタロック回路の構成例

しなければならない（タンパレジスト設計）。

[A] バネ戻り式の安全スイッチを使用してはならない。これは，作業者がスイッチの位置を針金やガムテープ等で意図的に固定すると，ガードを開いたときに機械を停止できなくなるためである。

[B] 接点を磁石でON/OFFできるものは，作業者が磁石を用いてスイッチを意図的に無効化できるため，使用してはならない。

[C] 作業者による不意の接触や，意図的な無効化ができないように，覆い等が設けられたものを使用する。また，作業者が意図的に取り外すことができないように，特殊な工具（菊ねじ等）で取り付けることができるものを使用する。

なお，インタロック用安全スイッチの具体例は，**参考資料1**を参照されたい。

3.3.7 行き過ぎ防止用の回路

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言う。このような危険を防止するための回路が行き過ぎ防止用の回路であり，通常は**参考資料1** No.18のようなリミットスイッチを利用して機械の行き過ぎを検出している。しかし，このスイッチにａ接点タイプのものを使用すると，接点の接触不良が生じたとき機械を停止できなくなる場合がある。このため，行き過ぎ防止用のリミットスイッチは，機械の危険な可動部がリミットスイッチと直接接触したとき，ｂ接点を強制的に引き離す方式のもの（強制引き離し式のｂ接点タイプ）を使用することが必要である。

表8は，リミットスイッチにａ接点タイプのものと，強制引き離し式の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。

3.3.8 フェールセーフな論理回路

フェールセーフな論理回路とは，回路に故障が生じたときは，機械を必ず停止側とできるように，故障時に必ず信号出力をＯＦＦとできる回路のことを言う。この回路には，論理積演算，レベル検定，自己保持等の演算機能を持つものがある。また最近では，これらの回路をＩＣに実装したものも市販されている（**参考資料1** No.21参照）。

図11(a)は，フェールセーフＡＮＤゲートの回路構成である。この回路では，故障時に必ずＯＦＦ信号を

表8　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		バネ戻り式 a接点タイプ	強制引き離し式 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

出力するように，回路を一種の交流発振器（発振周波数は200kHZ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レベルの高い交流信号を生じないからである。

図でＯＳＣは交流発振部，ＡＭＰは増幅部，ＲＥＣは整流部である。ここで，ＯＳＣ部は，入力I_1またはI_2が印加されないとき，

Q_1：ＯＦＦ，Q_2：ＯＮ，Q_3：ＯＮ

の状態であり，入力I_1, I_2が共に印加されたとき，

Q_2：ＯＦＦ→Q_3：ＯＦＦ→Q_1：ＯＮ

→Q_2：ＯＮ→Q_3：ＯＮ→Q_1：ＯＦＦ

の順序で発振を開始し，**図11(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。

表9にフェールセーフＡＮＤゲートの故障解析結果を示す。表からも明かなように，この素子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。

3.3.9 電磁リレーの制御回路

電磁リレーでは，リレーのａ接点が閉じたときに機械を停止させ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場合がある。また，リレーの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場合がある。従って，電磁リレーでは，リレーのａ接点が閉じたときに，機械が作動するように回路を構成しなければならない。

また，このように回路を構成した場合でも，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，２つのａ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ように回路を構成する。**図12**はそのための回路の一構成例であり，次のような順序で動作する。

① 起動ボタンを押すと，接点（Ｒ１－１），（Ｒ２－１），（Ｒ１－２），（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 ②，③より，接点（Ｒ１－４），（Ｒ２－４），（Ｒ３－４）が閉じて，機械が運転を開始する。

⑤ Ｒ１，Ｒ２の接点のいづれかに溶着が生じたときは，接点（Ｒ１－１）または（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，Ｒ３は，ａ接点が溶着したとき，対となるｂ接点は必ず開いた状態に保持できる構造のもの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適用する（**参考資料１** No.16参照）。

[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，または，個々の接点が遮蔽室等に収納された構造であること。

[B] 万一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。

上記の要件を満足できるものを，強制ガイド式安全リレーと呼ぶ。

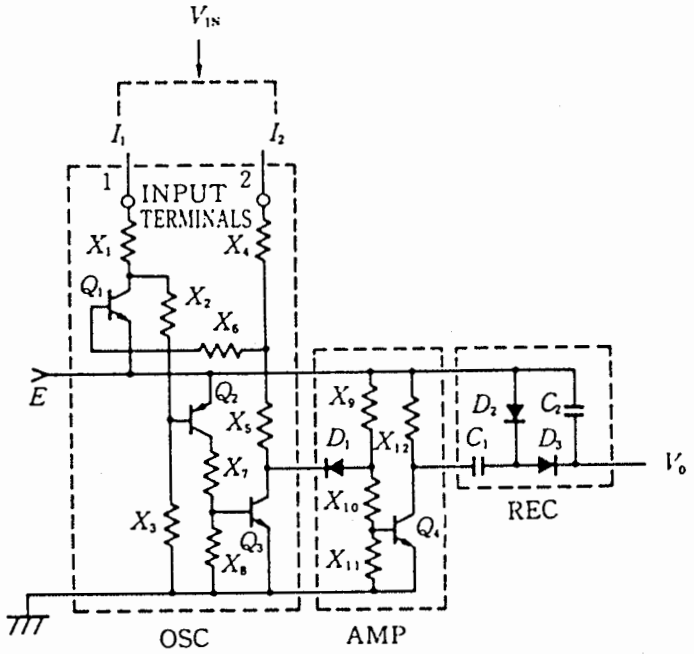
なお，最近，電磁リレーに接点溶着が生じたことを検出できるモニタ機構を持つリレーが，我国でも市販されるようになってきている（**参考資料１** No.17参照）。このリレーは，安全上特に問題となるメインコンタクタ（モータの駆動部分等に使われるリレー）部分の溶着対策に有効と考えられる。

また，安全リレーの中には，接点機構に使用する材質を吟味することによって，溶着が生じないように工夫したリレーもある（非溶着リレー）。たとえば，銀ー炭素接点の使用によって，接点が溶着しそうになると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。

3.3.10 電磁弁の制御回路

ノーマルオープン形の電磁弁では，ソレノイドに断

(a)



(b)

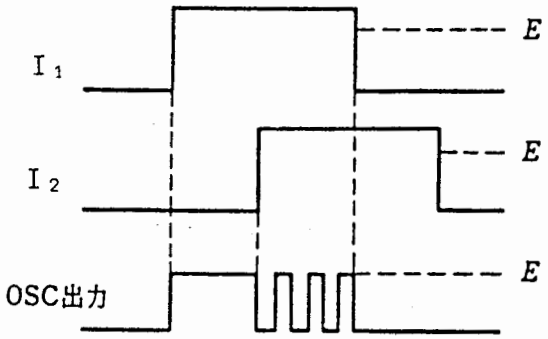
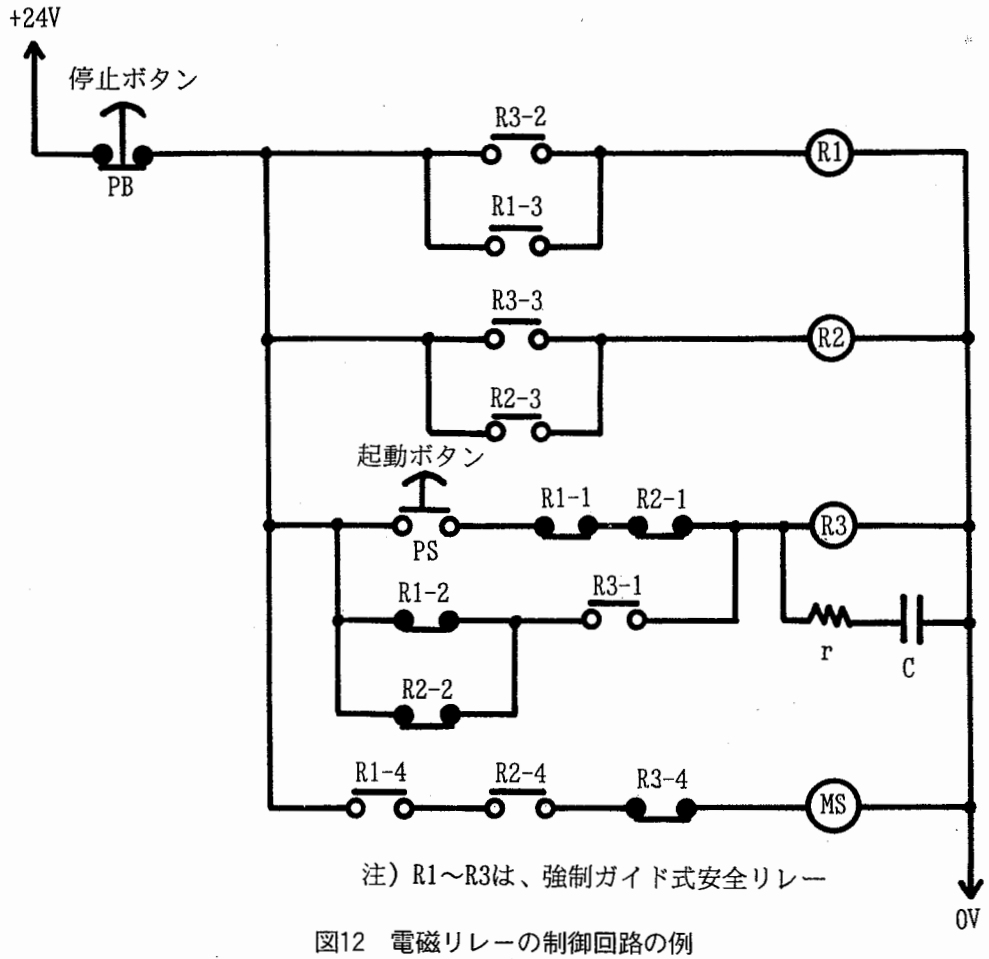


図11　フェールセーフなＡＮＤ回路

表９　フェールセーフＡＮＤゲートの故障解析

構成要素	記号	故障状態	結果
トランジスタ	Q_1 ～ Q_3	3端子間おのおの短絡・断線	演算発振器発振できず。
	Q_4	3端子間おのおの短絡・断線	発振出力なし、または出力低下。
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。



注）R1～R3は、強制ガイド式安全リレー

図12　電磁リレーの制御回路の例

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。従って，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形のものとする必要がある。なお，この場合，復帰を確実なものとするために，戻り方式は，油圧式にあってはバネリターン形，空気圧式にあってはプレッシャリターン形のものでなければならない。

次に，ノーマルクローズ形の電磁弁を選定した場合でも，仮に弁に異物等が挟まったり，弁座が固着したりすると，弁が開いたままとなり，機械を停止できなくなる場合がある。そこで，特に危険な機械に使われる電磁弁では，弁を二重化（複式電磁弁と言う）すると共に，2つの弁の動作をモニタ装置によって監視し，万一動作が不一致のときは，弁に開固着が起きたと見なして機械を停止させるように回路を構成する。参考**資料1** No.19にこの具体例を示す。

3.3.11 ブレーキの制御回路

正作動（ノーマルオープン）形のブレーキは，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。従って，機械の危険な可動部の停止用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負作動（ノーマルクローズ）形のものであることが望ましい。

3.4 おわりに

我国の労働災害防止対策では，機械の信頼性の向上や作業者の教育・訓練の強化によって，災害発生件数の減少を図る場合も多い。これに対し，本章で提案する安全確認形の制御システムでは，機械は故障し，作業者はミスを犯すことをまず認めた上で，仮にこれらが起きても，作業者に危害を及ぼさない構造を，システムの設計段階で構築しておくことを基本とする。このシステムの特徴は，次のように要約できる。

1）作業者の危険領域への進入や機械の異常動作等を前提とした安全装置を備えていること。

2）安全装置からの情報に基づいて，機械の異常な動作（不意作動，暴走等）や作業者の異常な行動（誤　操作，危険領域への進入等）が発生したときは，直　ちに機械を停止させて作業者の安全を確保する機構（インタロック機構）を備えていること。

3)　インタロック機構の故障時は，必ず安全側（機械を停止させる側）となること。この特性を実現するのがフェールセーフ技術である。
4)　安全装置が生成する情報（安全情報）は，安全をエネルギの高い側に，危険と故障をエネルギの低い側に割り当てていること。
5)　安全情報は，周囲に存在するエネルギより高いエネルギレベルを持つこと。
6)　安全情報はユネイトに伝達されること。
7)　作業者が安全スイッチ等を意図的に無効化できないように，覆いを設けたり，特殊な工具でなければ取り外せない設計（タンパレジスト設計）としていること。

本章では，工作機械等の安全確保のために特に重要な回路として，①非常停止回路，②再起動防止回路，③操作ボタンを使用した起動回路，④非接触式センサを利用した起動回路，⑤固定ガードのインタロック回路，⑥可動ガードのインタロック回路，⑦行き過ぎ防止用の回路，⑧フェールセーフな論理回路，⑨電磁リレーの制御回路，⑩電磁弁の制御回路，⑪ブレーキの制御回路等について述べた。

以上が本章の概要であるが，本章で述べた安全化手法は，あくまでも現段階で知られているいくつかの手法を例示したに過ぎないものであり，これ以外にも様々な方法が考えられる。この意味からも本章では，工作機械等の回路設計に携わる設計者や，フェールセーフの専門家の方々等からの率直な意見や批判を期待する。なお，本章で述べた以外の安全化手法は，今後機会を見つけて順次増補していきたいと考えている。

参考文献

1)　杉本・粂川他，安全確認形安全の基本構造，機論，54-505，C(1988)pp.2284-2292
2)　粂川・杉本・深谷・佐藤・江川・清水，安全制御における計測技術，産業安全研究所特別研究報告，RIIS-SRR-86,No.1(1986)pp.18-72
3)　粂川・杉本・深谷・江川・梅崎・池田・清水・田畠・富田，高齢者向けＭＥ機器の開発・改善に関する特別研究，産業安全研究所特別研究報告，RIIS-SRR-90(1990)pp.7-21
4)　杉本・梅崎・池田・粂川・深谷，安全制御システムの基本構成，産業安全研究所研究報告，NIIS-RR-95(1996)に掲載予定
5)　Ｊ．グレイ他，渡辺栄一訳，フォールト・トレラント・システム，マグロウヒル(1986)p.375
6)　近藤，本質安全化とフェールセーフ，安全，31－8(1980)p.43

（平成８年３月７日受理）

［補足］　インタロック機構の安全上の要件に関するチェックリストの例

（1）インタロック機構の設計原則

対象		チェック項目	判定	留意事項
1	インタロック機構	①　作業者の異常な行動（誤操作，危険領域への進入等）が起きても災害とならないように，適切なインタロック機構を設けているか。 ②　機械の異常な動作（不意作動，暴走等）が起きないように，適切なインタロック機構を設けているか。 ③　インタロック機構は，原則として，非対称誤り特性を持つように設計されているか。	YES　NO　不明　該当なし YES　NO　不明　該当なし YES　NO　不明　該当なし	・インタロック機構の具体例は，表４を参照のこと。 ・インタロック機構に非対称誤り特性を持たせるための手法は，表６を参照のこと。 ・インタロック，フェールセーフ，タンパレジスト等の技術の概要は，第3.2節を参照のこと。
2	安全情報	①　安全情報は，安全を通報する信号を高エネルギ状態に危険と故障を通報する信号を低エネルギ状態に対応させているか。 ②　安全情報はユネイトに伝達されているか（途中に，否定回路を含んでいないか）。 ③　安全情報には，電磁ノイズ等の影響を受けないように十分なエネルギを持たせているか。	YES　NO　不明　該当なし YES　NO　不明　該当なし YES　NO　不明　該当なし	・安全情報の伝達経路に否定回路を設けると，安全情報のユネイトな伝達を保証できなくなるため，設けてはならない。
3	プログラマブルな電子制御装置の使用	インタロック機構には，できる限りプログラマブルな電子制御装置（プログラマブル・コントローラ，マイクロ・プロセッサ等）を使用しないように努めているか。	YES　NO　不明　該当なし	・安全と関係しない機能的制御や支援安全条件に関連した制御には，プログラマブルな電子制御装置を使用しても差し支えない。

（2）インタロック機構で使用する部品類の選定

対象		チェック項目	判定	留意事項
1	安全スイッチ	①　スイッチには，強制引き離し式のｂ接点タイプを使用しているか。 ②　スイッチには，永久磁石によって接点をON/OFFできない構造のものを使用しているか。 ③　スイッチには，作業者による不意の接触や意図的な無効化ができないように，覆い等が設けられたものを使用しているか。	YES　NO　不明　該当なし YES　NO　不明　該当なし YES　NO　不明　該当なし	・ａ接点タイプのスイッチは，接点が接触不良を起こすと，機械を停止できなくなる場合があるため，使用してはならない。 ・バネ戻り式のスイッチは，接点溶着や，バネの破損，摺動部の固着等が生じたときや，作業者がスイッチの位置を意図的に固定したときは，機械を停止できなくなる場合があるため，使用してはならない。

（続き）

対象		チェック項目	判定	留意事項
1	安全スイッチ（続き）	④ 前項の覆いには，特殊な工具等を使用しなければ取り外せないものを使用しているか。 ⑤ 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か。	YES NO 不明 該当なし YES NO 不明 該当なし	・永久磁石によってスイッチの接点をON/OFFできるものは，作業者が磁石を用いてスイッチを意図的に無効化しとき機械を停止できなくなる場合があるため，使用してはならない。
2	非常停止装置	① 非常停止ボタンには，強制引き離し式のb接点タイプを使用しているか。 ② 非常停止用ボタンはプッシュロック式のものか。 ③ 緊急停止用ワイヤは，ワイヤが切れたときや緩んだとき，接点を強制的に引き離す構造か。	YES NO 不明 該当なし YES NO 不明 該当なし YES NO 不明 該当なし	・a接点タイプの非常停止ボタンは，接点に接触不良が生じたとき機械を停止できなくなることがあるため，使用してはならない。
3	安全プラグ	作業者が意図的に無効化できない構造のものか。	YES NO 不明 該当なし	・意図的に無効化できない構造とは，たとえば，プラグの電極間を故意に短絡できない構造などを言う。
4	電磁リレー	強制ガイド式安全リレーのように，安全性の高いものを使用しているか。	YES NO 不明 該当なし	・左記リレーを使用するのは，電磁リレーの接点溶着時に機械を停止できなくなる場合があるためである。
5	電磁弁	① ノーマルクローズ形のものを使用しているか。 ② 原則として，複式のものを使用しているか。 ③ 油圧式ではバネリターン形，空気圧式ではプレッシャリターン形のものを使用しているか。	YES NO 不明 該当なし YES NO 不明 該当なし YES NO 不明 該当なし	・ノーマルオープン形の電磁弁は，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場合があるために，使用してはならない。 ・複式でない電磁弁(シングル・ソレノイドバルブ)は，弁の開固着によって，機械を停止できなくなる場合がある。したがって，機械の不停止が重大な災害に至る可能性のある機械では，複式でない電磁弁は使用してはならない。
6	ブレーキ	負作動形のブレーキを使用するように努めているか。	YES NO 不明 該当なし	・正作動形のブレーキは，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場合があるために，できる限り使用しないことが望ましい。

（3）インタロック用回路の安全化

対象		チェック項目	判定	留意事項
1	起動回路	① 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，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，初めて起動信号を発生させているか。 ② センサが製品の到達を検出して自動的に起動信号を発信する回路では，このセンサ以外に人体の侵入を検出する安全装置を設けているか。	YES NO 不明 該当なし YES NO 不明 該当なし	・②の回路は，再起動防止機能を持つ必要がある。このためには，安全装置が人体を検出したとき，再起動防止回路の自己保持を解除し，その後作業者が再起動操作をしなければ機械を起動させない等の回路構成が考えられる。
2	再起動防止回路	再起動防止機能を持つように，自己保持回路で構成する等の措置を講じているか。	YES NO 不明 該当なし	・再起動防止機能を持たせるには，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，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，再起動を防止するなどの方法が考えられる。
3	ガードインタロック用の回路	① 段取り作業等のために固定ガードを頻繁に取り外す箇所には，インタロック用のスイッチを設けているか。 ② 可動ガードのインタロック用回路は，再起動防止機能を持つものか。	YES NO 不明 該当なし YES NO 不明 該当なし	・①の回路では，再起動防止機能を必要とする。 ・ロック機構なしの可動ガードには，ガードが開いていることを確認するａ接点タイプのスイッチと，ガードが閉じていることを確認するｂ接点タイプのスイッチを設け，ガード開閉の正常性を確認することが望ましい。 ・ロック機構付きの可動ガードには，機械の可動部が完全停止したことを確認するセンサやタイマを設け，これらからの信号に基づいてガードのロックを解除する。
4	論理回路	① 故障時には必ず出力がＯＦＦとなるように回路を構成しているか。 ② ＯＮディレー用の回路は，故障時に必ず出力がＯＦＦとなるか，または出力がＯＮとなるのが遅れるように回路を構成しているか。 ③ ＯＦＦディレー用の回路は，故障時に必ず出力がＯＦＦとなるか，または出力がＯＦＦとなるのが早まるように回路を構成しているか。	YES NO 不明 該当なし YES NO 不明 該当なし YES NO 不明 該当なし	・論理回路では，入出力信号と電源電圧が混触して，誤った安全信号を発生してはならない。このために，入出力信号を電源電圧より高い電圧とする(電源枠外処理)。 ・増幅用の回路では，通常，入力信号は微小であるためノイズと弁別することが難しい。そこで，入力を交流信号としてノイズとの弁別を行うことがある。

（続き）

対象		チェック項目	判定	留意事項
5	電磁リレーの周辺回路	① リレーのａ接点が閉じたとき機械が駆動するように回路を構成しているか。 ② 複数のリレーを使用する場合は，途中に否定回路を設けないように回路を構成しているか。 ③ 強制ガイド式安全リレーを使用した回路では，リレーの接点を二重化し，２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ようにモニタ回路を構成しているか。	YES NO 不明 該当なし YES NO 不明 該当なし YES NO 不明 該当なし	・リレーのａ接点が閉じたとき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場合があるため，このような構成としてはならない。 ・リレーのｂ接点が閉じたとき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場合があるため，このような構成としてはならない。 ・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構成しなければならない。これは，否定回路を設けてはならないことを意味する。
6	電磁弁の周辺回路	複式電磁弁を使用した回路では，２つの弁の動作が不一致のとき，弁に固着が起きたとみなして機械を停止させるようにモニタ回路を構成しているか。	YES NO 不明 該当なし	
7	機械の危険な可動部の駆動用回路	① 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供給を直接遮断するか，または，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，機械の危険な可動部を停止させているか。 ② 油空圧機器をアクチュエータとする機械では，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，機械の危険な可動部を停止させているか。 ③ 機械の危険な可動部をホールド停止状態とするときは不意作動による危険を防止するためにホールド停止監視機構を設け，万一不意作動が起きたとは，①，②等の遮断方法によって機械を停止させる構成としているか。	YES NO 不明 該当なし YES NO 不明 該当なし YES NO 不明 該当なし	

注）①安全化の原則的事項は，第３．２節を参照のこと。
②本チェックリストで述べた要件は，あくまでも例示である。