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

表1

	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）

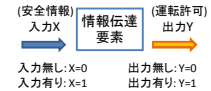


表1の解説

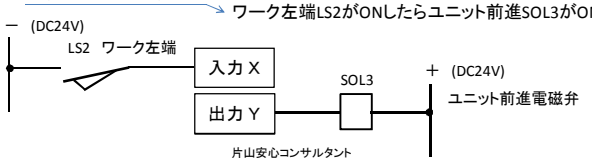
① 入力Xがゼロ=OFFなら出力Yはゼロ=OFFになる正常状態です。

② 入力Xが1=ONで、出力Yはゼロ=OFFは、出力が無いのは許容される故障です。

③ 入力Xがゼロ=OFFで、出力Yは1=ON、誤った出力は許容されない故障です。

④ 入力Xが1=ONなら出力Yは1=ONになる正常状態です。

ワーク左端LS2がONしたらユニット前進SOL3がONする。



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

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しまう。稼働率の低下を防ぐために、必要に応じて、部品の高信頼化のほかに次のものがある。

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。部品ではモータ駆動と電子回路によるタイマー　(両方又は片方の信号で動作する)
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

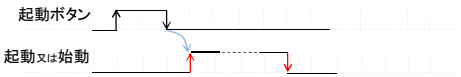
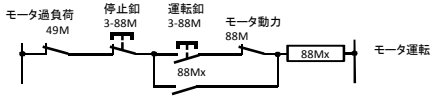
工作機械等の制御機構のフェールセーフ化に関するガイドラインから、制御機能について　1/2

制御機能の区分	内 容	身近な物での具体例
再起動防止回路	急停止機構等の作動によって機械の停止後に、停電後に機械への通電が復帰した時に、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。	電源OFFや非常用停止で運転指示の自己保持回路を切る
ガード用のインターロック回路	機械の運転中に作業者が危険領域内への侵入を防止する回路。 ①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の侵入を許可する方式と、 ② 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。	・動作停止後カバーが開くのは、洗濯機の蓋 ・電子レンジの外へマイクロ波が漏れると加熱を止めるのは、電子レンジの扉
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。 ①作業者がガードを開いた時、 ②安全装置が作動した時、 ③機械が何らかの故障や異常を起こした時	ファンヒータが停止する。 ・地震の震動、転倒 ・フィルタ目詰り
非常停止用の回路	作業者が何らかの異常で釦を押すなどの操作をして直ちに機械の運転を停止させる回路。 ①ケガ、災害が発生しかねない事態が起きた時、 ②機械に異常が生じた時、 ③作業中にトラブルが発生した時など	バイクのキルスイッチ 機械の非常停止釦、非常停止ワイヤー、非常停止ガード、他

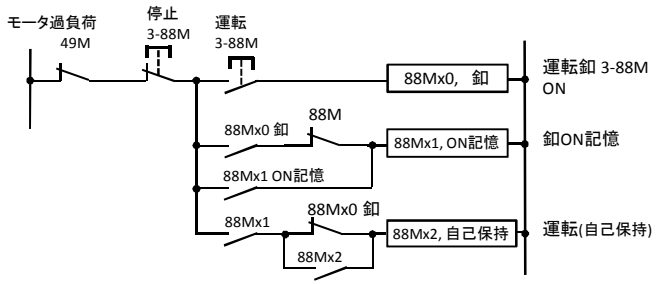
工作機械等の制御機構のフェールセーフ化に関するガイドラインから、制御機能について　2/2

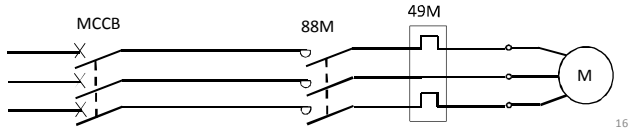
制御機能の区分	内 容	身近な物での具体例
行き過ぎ防止用の回路	機械があらかじめ設定した位置・角度等を超えて行き過ぎないように監視を行い、行き過ぎが生じたときは直ちに機械を停止させる回路	クレーンで、アーム角度を降ろし過ぎる
操作監視用の回路	作業者が正しい操作をしたときに限り、起動信号を発生させる回路	原位置でないと起動できない。他に、ぶつけない様に釦の押す順序が有る
ホールド停止監視用の回路	ホールド停止状態にある機械が故障や電磁ノイズ等の影響によって暴走しないよう監視を行い、暴走が起きた時に直ちに機械を停止させる回路	旋盤のクラッチノイズでロボットが誤起動した時、アームの角度検知で動力を切りアームを停止させる
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、暴走が起きた時は直ちに機械を停止させる回路	モータに有る位置検出器と機械のボールネジにもパルスコーダを直結する
ホールド・ツー・ランの回路 Hold to run	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	台所にあるミキサーは、ボタンを押している時だけ回転する

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から、フェールセーフ化　1/5

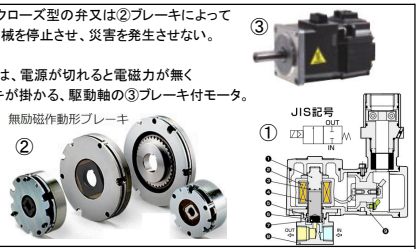
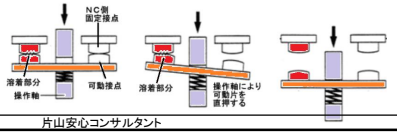
イ	オフ確認	ボタンを押して接点を閉じる動作に続けて、ボタンを離して接点を開く動作を行ったときに初めて起動信号又は始動信号を発生させる方法  その他に、動作OFF信号を条件に入れた起動回路 a. 動力開閉器のOFF確認：b接点に通が有り溶着していない事を確認する b. 検知のOFF確認：　自動運転において原位置が下降位置である時、上昇指示を行う際に下降端がON、上昇端はOFFしているのが正常で、上昇指示をONする条件に下降端ON（原位置）と上昇端OFF（検知のOFFチェック）を入れる。
ロ	再起動防止	起動操作によって自己保持回路が作動して自己保持を開始し、作業者が停止操作を行った時、又は安全装置が作動した時には自己保持を解除し、機械の再起動を防止する方法 具体的には、自己保持回路 

参考　起動ボタンのオフ確認回路

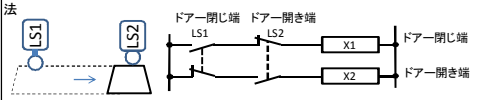
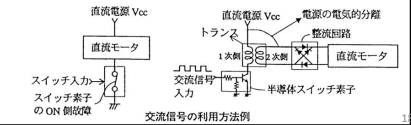




工作機械等の制御機構のフェールセーフ化に関するガイドラインから、フェールセーフ化　2/5

ハ	ノーマルクローズ型の利用	①ノーマルクローズ型の弁又は②ブレーキによって故障時に機械を停止させ、災害を発生させない。 具体的には、電源が切れると電磁力が無くなりブレーキが掛かる、駆動軸の③ブレーキ付モータ。 
ニ	強制引き離し	作業者が　①非常停止装置を操作するときの力、 ②作業者が可動ガードを開くときの力、 ③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機械を停止させる。 

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から、フェールセーフ化　3/5

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 次ページ資料「3.3.8 フェールセーフな論理回路」を参照する。
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 交流信号処理（直流信号の電圧レベルで信号の有無を判断せず、交流信号で信号の有無を表現する） 

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。

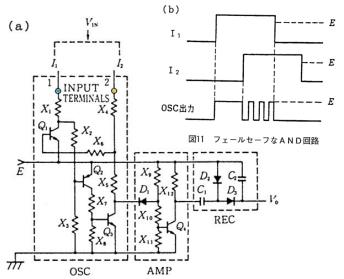


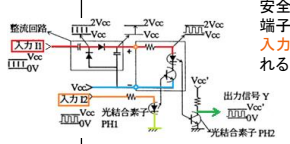
図11　フェールセーフなＡＮＤ回路

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。
		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_{11}	断線	演算発振器発振できず。
		断線	発振出力なし。

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から、フェールセーフ化　4/5

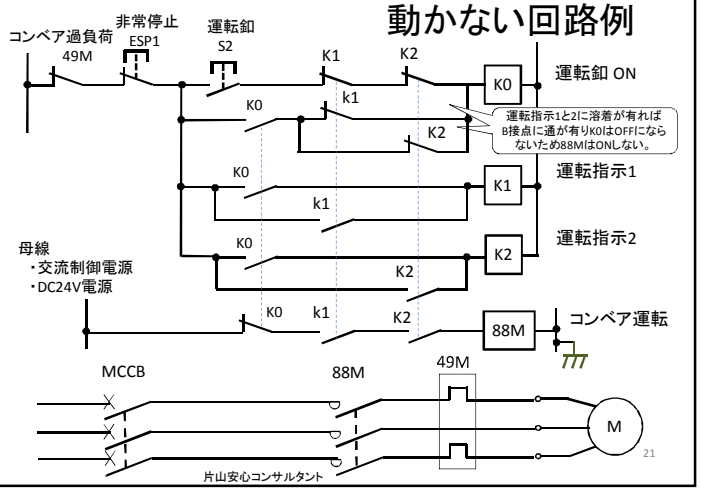
チ	電源　枠外処理	安全情報を電源電圧より高い電圧に設定することにより、信号線と電源線の混触による誤った安全情報の伝達を防止する方法 枠外電源処理（昇圧回路を用いて供給電源より高い電圧で信号処理をする技術）
リ	フェールセーフチェック回路の利用	フェールセーフなチェック回路によって、制御機構を構成する非フェールセーフな安全装置や部品類に故障が生じていないかを常時チェックする方法 次ページ「監視機能により安全機能の喪失は動かない回路例」を参照する



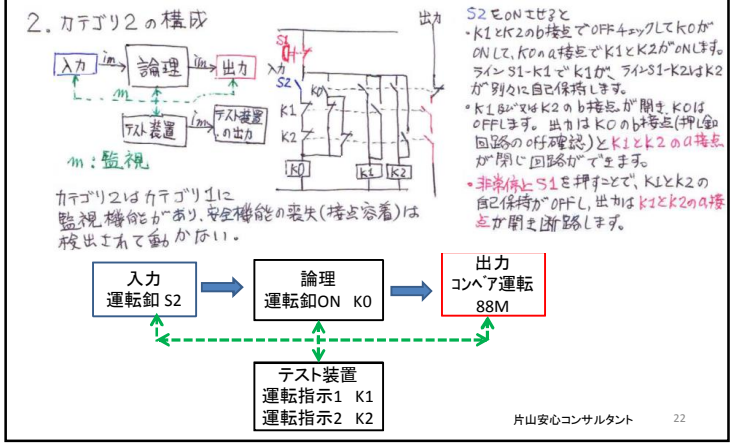
安全信号が入力I1に入り、端子＋に2Vcc，端子−はVccとなり、その電位差はVccとなる。入力I2がONに成ればANDで出力Yがonされる。

入力I1が電源Vccと混触した場合、カプラの電位が0Vとなり、カプラPH2はONしない。

参考　監視機能により安全機能の喪失は動かない回路例

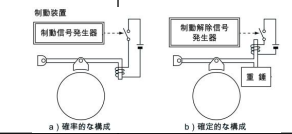


参考　監視機能により安全機能の喪失は動かない回路例の解説



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から、フェールセーフ化　5/5

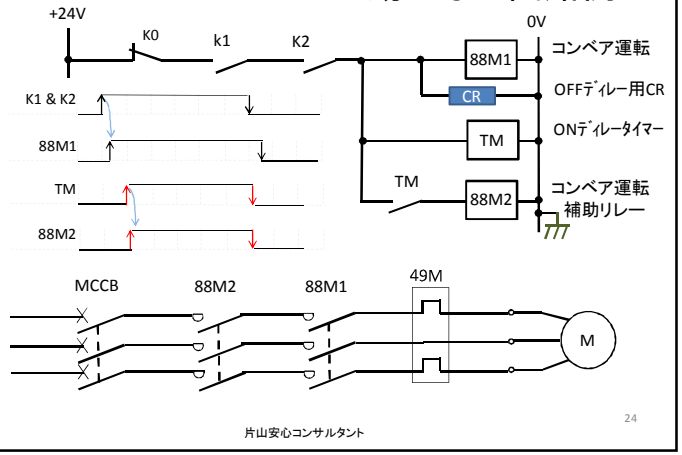
ヌ	二重化不一致検出	接点又は弁を二重化し、二つの動作が不一致のときは、接点又は弁に溶着又は固着が起きたとみなして、労働災害を発生させない形で機械を停止させる方法
ル	バックチェック	a接点に溶着が生じたとき、対となるb接点によってこれを検出し、直ちに機械を停止させる及び又は次のサイクルの運転を開始させない方法 例、ﾏｸﾞﾈｯﾄｽｲｯﾁがONの状態からOFFに変わった時、a接点が切れb接点はON(電気が通る)するが、a接点が溶着すればb接点はOFF(電気が通らない)のままとなりa接点の溶着が判る。
ヲ	非溶着	本質的に溶着しない接点を用いる方法 具体的には、溶着するに等しいエネルギーを与えると、接点が破壊する。
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、①重力の作用によって機械的機構が自然に落下して(くさびが入り固定される、鉄道の腕木式信号機)安全を確保する方法及び②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(サーミスタ)の抵抗値等が増大し機械への通電を減流・遮断する方法、他



a)確率的な構成:電源×スイッチ×配線×ソレノイド=制動力
正常に機能する時は1、故障は0とすると、
断線故障は　1×1×0×1=0になり制動できない。

b)確定的な構成:電源×スイッチ×配線×ソレノイド=解除力
正常に機能しないとブレーキが解除できないので、
断線故障は　1×1×0×1=0になり制動のままになる。

参考　接点の2重化による不一致は動かない回路例



セーフティユニットの内部回路例

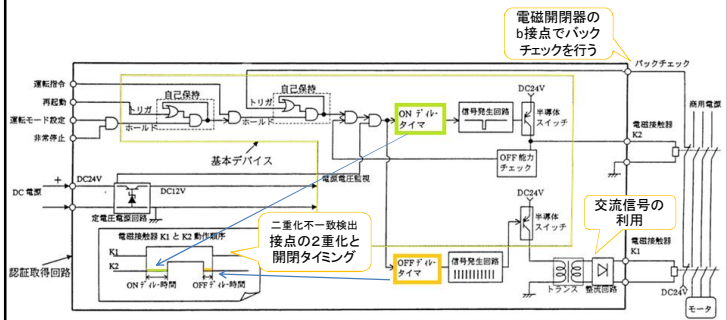


図6　基本デバイスを応用したカテゴリー4認証済み回路の機能概略：電磁接触器 K1 は無負荷で駆動され、回路に不具合を生じた場合、電磁接触器を駆動する出力信号は停止する。電磁接触器 K1 は非常用ブレーキに、電磁接触器 K2 は常用ブレーキに各々該当する。両者の組合せにより、K1 と K2 の ON／OFF の頻度によらずカテゴリー4 の制御回路として利用することができる（詳細は IEC　44/278/NF(1999-11-26)，p47 参照）

“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