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、故障の環境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

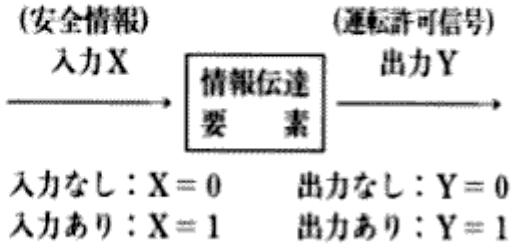
りも著しく高い特性又は安全側にしか故障しない特性をいう。

(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

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)



（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等)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 ガード用のインターロックの回路	機械の運転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侵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類については、部品類ごとに 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　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、その後固定ガ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が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が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