

制御の安全

2006.5.28

まえがき

機械装置の危険源は、リスクアセスメントによって同定されるが、そのリスクを低減するために、保護方策(本質安全設計/安全防護/補足の予防策/使用上の情報)が実施される。前項の『機械の安全』による保護方策を行ってもリスクが残存する場合、『制御の安全』によってリスクを低減し安全の確保を図らなければならない。本稿では、機械の制御システムの設計段階において実施しなければならない保護方策について説明する。

1、 制御設計の手順

〈 表-1 〉は、機械装置の制御設計の手順を系統的にまとめたものである。

この設計手順の中で、①の設計条件確認、②の一般仕様確認、③の基本設計から④のリスクアセスメントまでは機械全体について行われる。

機械の制御システムがリスク低減・安全の確保のために関わってくるのは、⑤の保護方策の決定から⑥の安全関連部の安全機能の特定、⑦の安全カテゴリの選定、⑧の安全関連部の詳細設計までである。

ただし、実施した保護方策によって安全が確保されているかどうかは、安全立証について⑩の妥当性確認で検証し、残存リスクについては⑪の技術文書類で説明しなければならない。

〈 表-1、設計手順 〉

設計手順	
1	設計前の必要な条件(環境条件・電源条件・要求事項)を確認する
2	設備の一般仕様(使用法規・規格、客先基準・標準)を確認する
3	個別仕様書(設備仕様、制御仕様、システム仕様)を作成し基本設計する
4	リスクアセスメント(個別仕様書より危険源を同定し評価し査定する)を行う
5	リスクを低減するための保護方策を決定する
6	安全関連部設計のための安全機能を特定する
7	安全カテゴリ(B・1・2・3・4)を選定する
8	詳細設計(通常の制御の設計・安全関連部の設計)する
9	設備製作・据付工事・エネルギー源の繋ぎ込みをする
10	妥当性確認(通常の制御部を含めた安全関連部を検証)する
11	技術書類(据付・操作・保全マニュアル、妥当性確認報告書)を作成する

2、 制御システムの保護方策

〈 図-1 〉は、ISO 12100-1 (JIS B 9700-1)に記載されている機械のリスク低減の保護方策を示したものである。

〈 図-1、保護方策 〉



制御の安全

この保護方策の中で、制御システムで対応できるものを以下に示す。

1) 本質安全設計

制御システムにおける本質安全設計は、設備の一般仕様として規定され、基本設計に含まれる保護方策である。

- 制御電源に感電しない安全なDC24Vの使用
- JIS規格に準拠した電線色の使用
- 感電保護のための機械装置・制御機器への保護接地線の接続

2) 安全防護

機械の安全では、隔離の原則に基づくガードによる保護方策となるが、制御の安全では、停止の原則に基づく保護装置(動作制限・インターロック)による保護方策になる。

①ガード(主に機械による保護方策)

- 固定式ガード、可動式ガード、調整式ガード(機械の保護方策)
- インターロック付ガード、施錠式インターロック付ガード(機械と制御の保護方策)

②保護装置(機械ガード以外の制御装置による保護方策)

- インターロック装置、イネーブル装置、ホールドツーラン制御装置
- 両手操作制御装置、検知保護装置(セーフティ・ライトカーテン、レーザスキャナ)
- 能動的な光電保護装置、機械的拘束装置、制限装置、動作制限制御装置

3) 付加保護方策

緊急時や、予見可能な通常作業・保全作業に必要となる保護方策である。

- 非常停止装置(非常停止釦、セーフティ・ロープ・スイッチ)
- 動力供給の遮断および蓄積エネルギーの消散(封じ込め)に関する方策(ロックアウト)
- 補足された人の脱出および救助のための方策(脱出・救助用の手動手段や要具)
- 機械および重量構成部品の容易で安全な取扱いに関する準備(付属要具の常備)
- 機械類への安全な接近に関する方策(階段、はしご、プラットフォームとそれらのガード)

4) 使用上の情報

機械の意図する使用に必要な指示事項や残留リスクの説明を含む。

- 信号(点滅灯、積層灯、アンドン)及び警報装置(サイレン、ブザー、音声装置)
- 表示、標識、絵文字、警告文(PLラベル、禁止・注意・許可シール)
- 付属文書(据付けマニュアル・操作マニュアル・保全マニュアル)

3、 機械の制御システム内の安全関連部の位置付け

〈 図-2 〉は、機械の構成を表したもので、安全関連部は機械の制御システムに含まれる。非安全関連部の制御機器の始動命令と保護装置の安全確認信号が揃って、動力制御要素の安全リレーまたは安全リレーユニットから運転起動信号が出力され動力出力機器が作動する。

・非安全関連部

通常の制御機器(電源部、PLC、入出力機器、信号・表示機器)から構成されている。

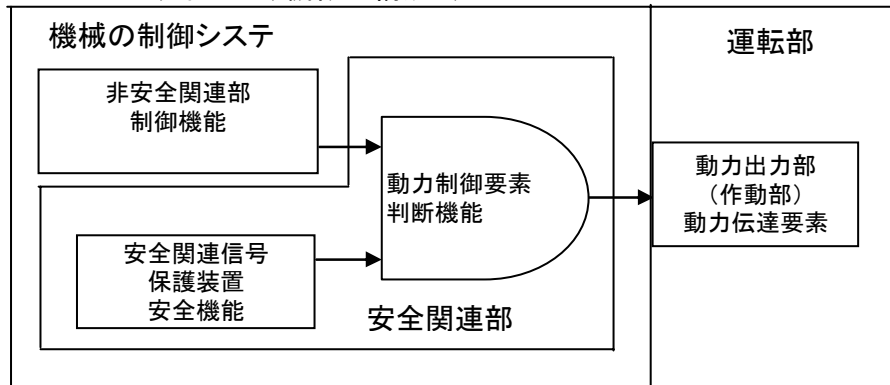
・安全関連部

安全機能を持つ保護装置(完全関連信号の発生)と判断機能を持つ動力制御要素(安全リレーユニット、電磁接触器、電磁弁)で構成される。

・運転部

動力出力機器(モータ、シリンダ)と動力伝達要素(ギヤー、クラッチ、チェーン)と作動部(コンベヤ、リフト、クランプ、ハンド)で構成されている。

〈 図-2、機械の構成 〉



制御の安全

- 4、 安全関連部の安全機能
 故障がリスクの増加に直ちにつながるような機械の機能で、安全関連部に使用する保護装置はいずれかの安全機能を持たなければならない。
 〈表-2〉は、安全関連部の保護装置に要求される安全機能で、保護方策に応じて制御システムに適用する。

〈表-2、安全機能〉

安全機能	
1	保護装置による停止機能(3つの停止カテゴリーのいずれかに従う)
2	非常停止機能(必要な制御範囲だけに適応する)
3	保護装置の手動リセット機能(リセット操作で起動してはならない)
4	起動および再起動(運転条件が整い、全ての安全関連部が正規の状態にある)
5	応答時間の明示(リスクアセスメントで要求される場合)
6	安全関連パラメータの設定(位置・速度・温度・圧力)等の動作制限やインターロック
7	局部制御機能(ティーチング・ペンダント等の局部制御選択は危険区域外に設置)
8	ミュート機能(ミュート中は他の安全が提供され、表示が必要)
9	安全機能の手動休止(設定・調整・保全・修理等のモード選択による自動運転防止)
10	動力源の変動、喪失および復旧(安全関連部の安全状態を維持する)

- 5、 インターロック
 インターロックとは、特定の条件下で人または機械の危険な干渉を避け、安全を確保するらめに必要となる手段である。
 ISO 12100-1:2003 (JIS B 9700-1:2004)では、インターロック装置について、『特定の条件(ガードが閉じていない場合)のもとで危険な機械機能による運転を防ぐことを目的とした機械装置、電気装置、またはその他の装置』と定義している。

下記は代表的なインターロックおよび使用例である。

- 1) 代表的なインターロック
 - ① 起動インターロック
 電源投入時または電源復帰時に機械が自動的に起動するのを防ぐ手段。
 - ② 再起動インターロック
 運転中に危険状態になり検出装置が作動した後、または運転モードを切替えた後に、機械が自動的に再起動するのを防ぐ手段。
 - ③ 相互インターロック
 人と機械可動部が作業場を共有するとき、または機械可動部と他の機械可動部に干渉領域が存在するとき、相互に安全な領域にあることを検知確認し安全を確保して作業または可動できるようにする手段。
 - ④ 自己確認型インターロック
 人と機械可動部が作業場を共有するとき、人または機械可動部が危険領域に進入すると検知装置が作動して機械を停止する手段。
 - ⑤ インターロック付ガード
 インターロック装置を付加したガードで次のような機能を有する。
 ガードが閉じ検知装置により安全が確認されると機械は運転可能となる。
 但し、非安全関連部から運転指令が出力されない限り起動しない。
 機械の運転中にガードを開くと検知装置による安全確認が無くなるため機械は停止する。
 - ⑥ 施錠式インターロック付ガード
 インターロック装置とガード施錠装置を備えたガードで次のような機能を有する。
 ガードが閉じ検知装置と施錠装置により安全が確認されると機械は運転可能となる。
 但し、非安全関連部から運転指令が出力されない限り起動しない。
 機械が停止し施錠装置が解錠されないとガードは開けられない。
 ガードの施錠装置はスプリング施錠・動力解錠でなければならない。

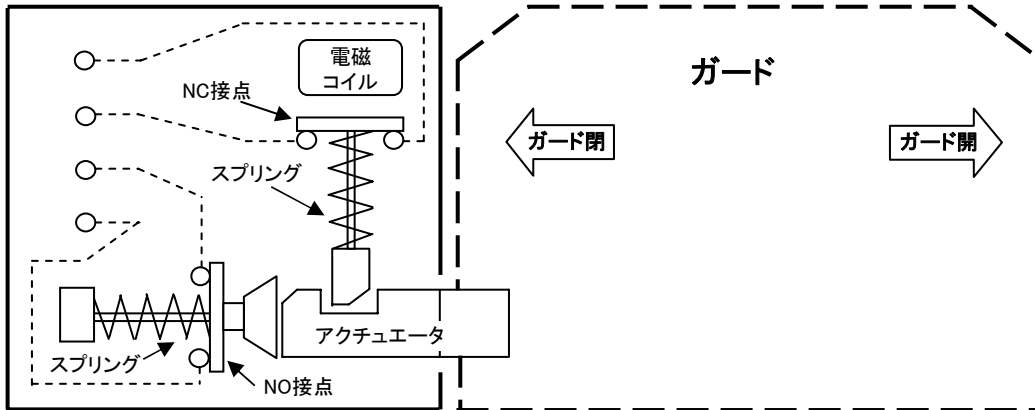
制御の安全

2) インターロックの使用例

① 施錠式インターロック付ガード

ガードが閉じてアクチュエータに押されNO接点がオンし、ガードの閉位置が確認される。アクチュエータはスプリングに押されロック状態になり、ガードは開くことができず、NC接点がオンしてロック確認される。この2つの安全確認によりガード内の機械装置は作動することができる。また、機械装置が停止し電磁コイルに通電しないとロックが解除されずガードを開くことはできない。

〈 図-3、施錠式インターロック付ガード 〉

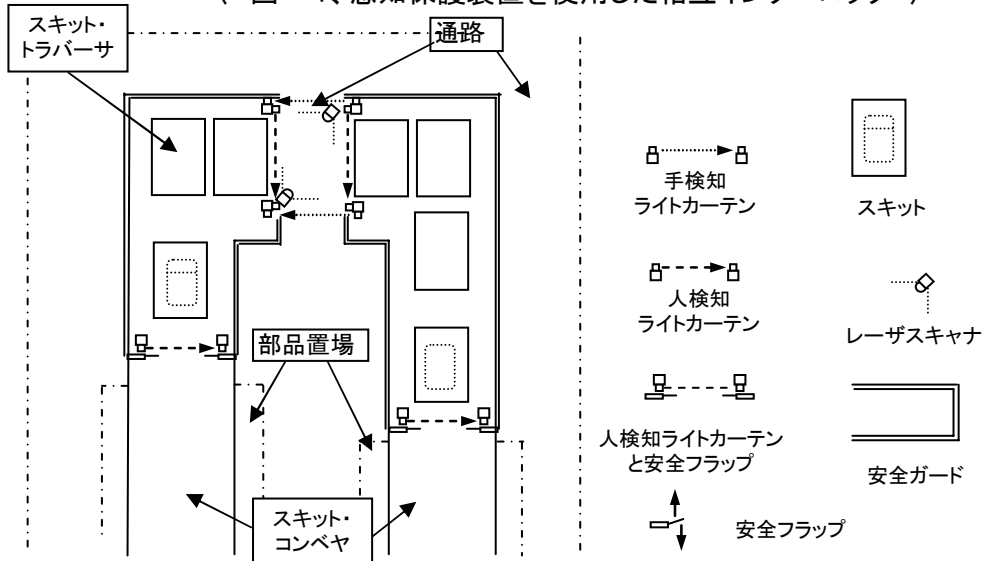


② 感知保護装置を使用した相互インターロック

スキット搬送路と人の通路が交わる所は、安全ライト・カーテンとレイザ・スキャナを併用する。スキットが横行中は人検知ライトカーテンとレーザスキャナをミュートングし、手検知ライトカーテンのみが人の進入を監視する。人の通行の許可については、通路上に信号機を設けることによって行う。また、スキットが作動できる条件は、通路上に人がいないという安全確認信号による。

スキットが出入りする所は、安全ライト・カーテンと安全フラップを併用する。スキットが安全ライト・カーテンを遮る時は、ミュートングを行い走行する。安全フラップには安全リミット・スイッチを付け、ボディとライト・カーテンの隙間からの人の進入を監視する。

〈 図-4、感知保護装置を使用した相互インターロック 〉



制御の安全

- 6、 安全確認型
 安全確保の方法には、安全方策の信頼性の向上による『確率的な安全』と、安全の立証による『確定的な安全』がある。
 確率的な安全では、人が危害を受ける可能性が残るが、確定的な安全では機械が停止しても人は危害を受けない。
 機械の安全確保を確定的な安全で達成するシステムを安全確認型という。

1) 安全確認型と危険検出型の比較 < 図-5 >

①安全確認型

安全確認型とは、安全が確認されている間だけ機械装置が起動し、安全を確認できなければ起動しない、あるいは運転中であれば停止する制御構成である。

②危険検出型

危険検出型とは、危険を検出すれば機械装置は停止するが、危険が検出できなければ危険状態にあっても機械装置は起動し、運転中なら停止しない制御構成である。

< 図-5、安全確認型と危険検出型の比較 >

	安全確認型	危険検出型
透過型 光電管 (セイフティ ・ライト カーテン) と 拡散反射 光電管		
光電管 運転方式	ライトオン(正常時オン) 人が光を遮っていない時、 安全確認信号を送送する。	ライトオン(異常時オン) 人を検知すると、危険検出 信号を送送する。

2) 機械装置の運転・停止状態の比較 < 表-3 >

安全確認型は不具合(障害)の発生において安全機能を喪失せず、機械装置を停止状態にし安全を確保する。それに対して、危険検出型は不具合の発生により安全機能を喪失してしまい、人が遮っても機械装置の運転状態が継続して危険である。

< 表-3、機械装置の運転・停止状態の比較 >

	安全確認信号 (出力接点)	機械状態	危険検出信号 (出力接点)	機械状態
投光器・受光器 故障	オフ(接点开)	停止(安全)	オフ(接点开)	運転(危険)
電源線の切断	オフ(接点开)	停止(安全)	オフ(接点开)	運転(危険)
信号線の切断	オフ(接点开)	停止(安全)	オフ(接点开)	運転(危険)
光軸のずれ	オフ(接点开)	停止(安全)	オフ(接点开)	運転(危険)
レンズの汚れ	オフ(接点开)	停止(安全)	オフ(接点开)	運転(危険)
正常運転時 (人を検知)	オフ(接点开)	停止(安全)	オン(接点閉)	停止(安全)

制御の安全

7、 安全カテゴリ

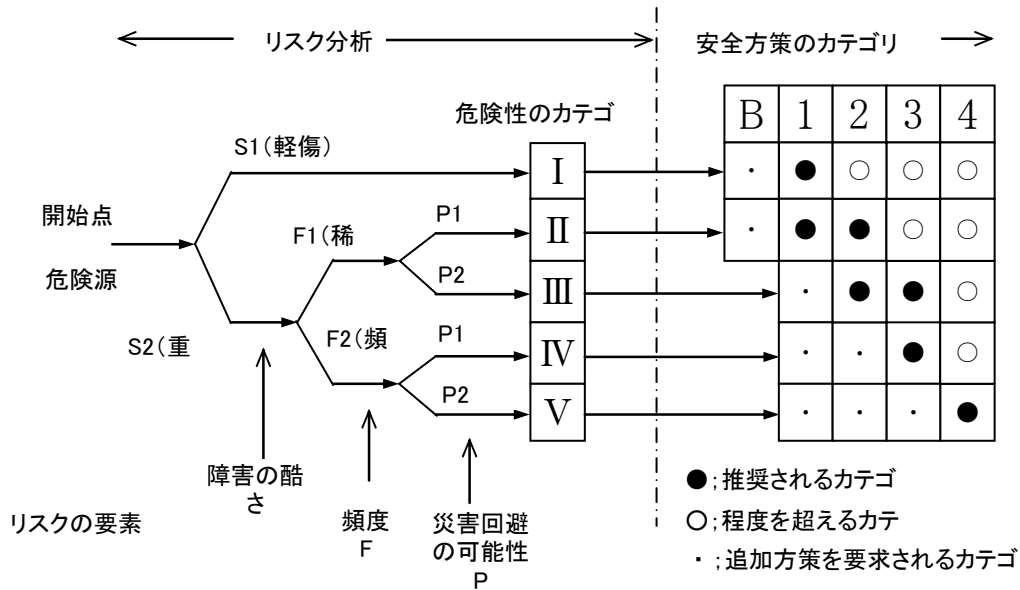
安全カテゴリとは、制御システムの安全関連部の設計に要求される事項で、不具合(障害)に対する安全機能の維持能力の分類である。

言い換えれば、安全確保のためのリスク低減が制御機能による場合、制御システムで生じる故障に対する安全性の達成レベルである。

1) 安全カテゴリの選択

〈 図-6 〉は、リスクアセスメントによって導き出された危険性のカテゴリに対応して制御システムで達成されなければならない安全方策のカテゴリを表している。

〈 図-6、安全装置のカテゴリの選択方法 〉



2) 安全カテゴリの分類

〈 表-4 〉は、制御システム内で構築される安全関連部の安全機能の要求事項と維持能力をカテゴリ(B、1、2、3、4)別に分類したものである。

〈 表-4、安全カテゴリーの分類 〉

	要求事項の要約	安全機能の維持能力
B	・基本安全原則を用いて、制御システム安全関連部の目的機能を実現する	・不具合(障害)発生時、安全機能を失う恐れがある
1	・カテゴリ-Bの要件を満たす ・十分に吟味された高信頼のコンポーネントを使用し、安全の確保は安全原則に従う	・不具合(障害)発生時、安全機能を失う恐れがあるが、発生確立はカテゴリ-Bより低い
2	・カテゴリ-Bの要件を満たす ・安全の確保は安全原則に従う ・安全機能は適当な間隔でチェックされる	・安全機能の喪失はチェックにより検出される ・チェックの間で、不具合の発生が安全機能を失う恐れがある
3	・カテゴリ-Bの要件を満たす ・安全の確保は安全原則に従う ・安全関連部の設計要求事項: 単一不具合(障害)で安全機能を失わない 単一不具合(障害)は可能な限り検出される	・単一不具合で安全機能は失われない ・全てではないが不具合は検出される ・検出されないの不具合の蓄積で安全機能を失う恐れがある
4	・カテゴリ-Bの要件を満たす ・安全の確保は安全原則に従う ・安全関連部の設計要求事項: 単一不具合(障害)で安全機能を失わない 単一不具合は安全機能の要求時またはそれ以前に検出される 検出が不可能な場合、不具合の蓄積が安全機能を失わない	・不具合発生時、常に安全機能が失われない ・不具合は検出され、安全機能が失われるのを防止する

制御の安全

3) 安全関連用語の説明

①基本安全原則

制御システムの安全関連部の設計・製作・選択・編成・組立に関する安全原則で、以下の事項に対する抵抗性が考慮されなければならない。

- ・予想される稼働負荷(遮断容量および頻度に対する信頼性)
- ・作業過程に用いられる材料の影響(洗浄機械の洗剤)
- ・外部からの影響(外部の電磁界、エネルギー供給の中断または停止)

②十分に吟味された安全原則

- ・特定の障害を回避する(間隔による回路短絡の回避)
- ・障害の発生確率を低減する(設計の余裕)
- ・障害時の故障の方向を特定する(障害発生時の動力遮断)
- ・障害の早期検出を実施する(地絡検出)
- ・障害の影響を抑制する(機械設備の接地)

③十分に吟味されたコンポーネント

- ・過去において広く使われて良好な成績を上げ、類似の適用事例で成功したコンポーネント(ヒューズ、ブレーカ、電磁接触器)
- ・安全関連適用例に対してその適正と信頼性を立証できる原則を使って製作され、検証されたコンポーネント(非常停止スイッチ、イネーブルスイッチ)

4) 安全カテゴリの回路例

〈図-7〉、〈図-8〉、〈図-9〉、〈図-10〉、にカテゴリ別の実施回路例を説明する。

[構成部品]

DS: ドアスイッチ、PB: 押釦、KS: ナイフスイッチ、MB: モータブレーカ、
OLR: サーマル補助接点、THR: サーマルリレー、MS: 電磁接触器、M: モータ
CP: サーキットプロテクタ、

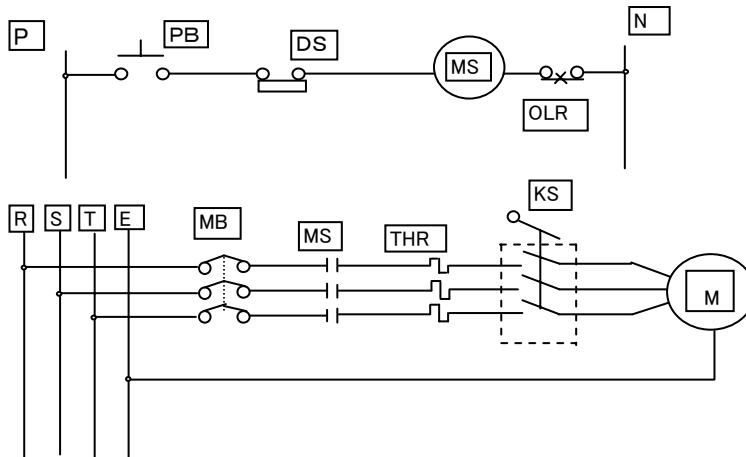
カテゴリ2以上に使用するMSは、強制開離形電磁接触器を使用しなければならない。

①カテゴリBとカテゴリ1の回路例

カテゴリBは、一般リレーを使用した制御回路で対応可能である。

カテゴリ1は、安全規格適合品を使用した制御回路で組まなければならない。

〈 図-7、カテゴリBとカテゴリ1の回路例 〉

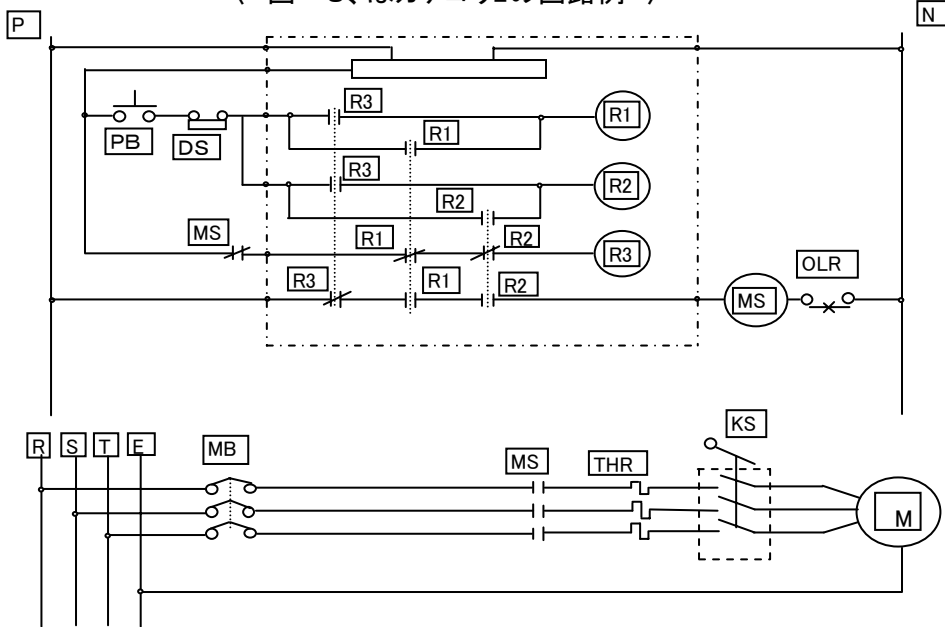


制御の安全

②カテゴリ2の回路例

カテゴリ2は安全リレーを使用した一重回路で組むことができ、
点線で囲われた部分はカテゴリ2の安全リレー・ユニットと置換えられる。
単一故障が発生した場合制御不能になる。

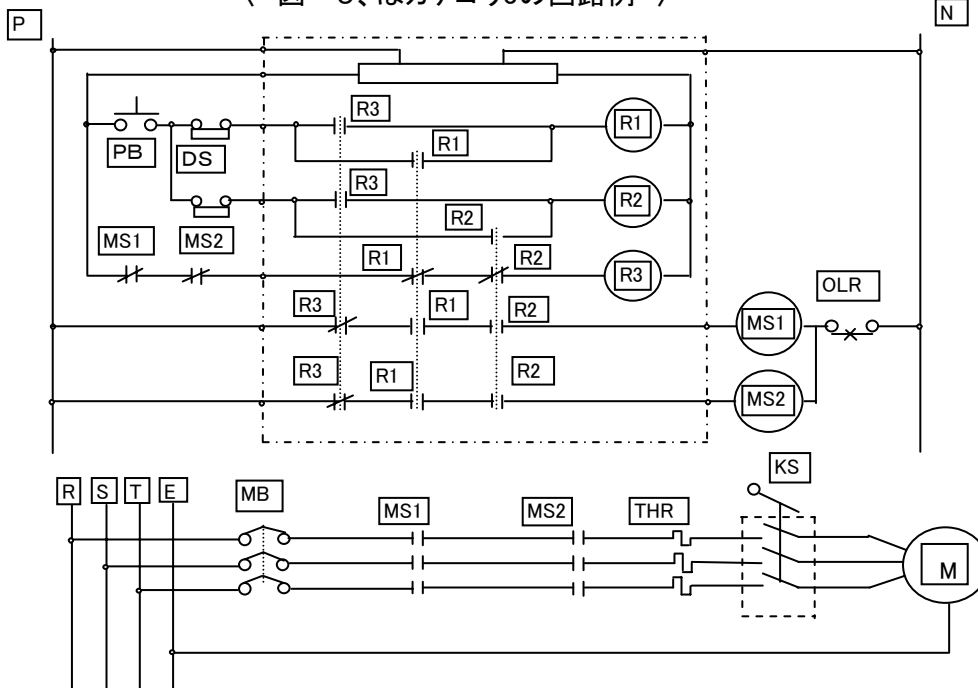
〈 図-8、はカテゴリ2の回路例 〉



③カテゴリ3の回路例

カテゴリ3は安全リレーを使用した二重化回路で組むことができ、
点線で囲われた部分はカテゴリ3の安全リレー・ユニットと置換えられる。
全ての故障は必ずしも検出されない。

〈 図-9、はカテゴリ3の回路例 〉

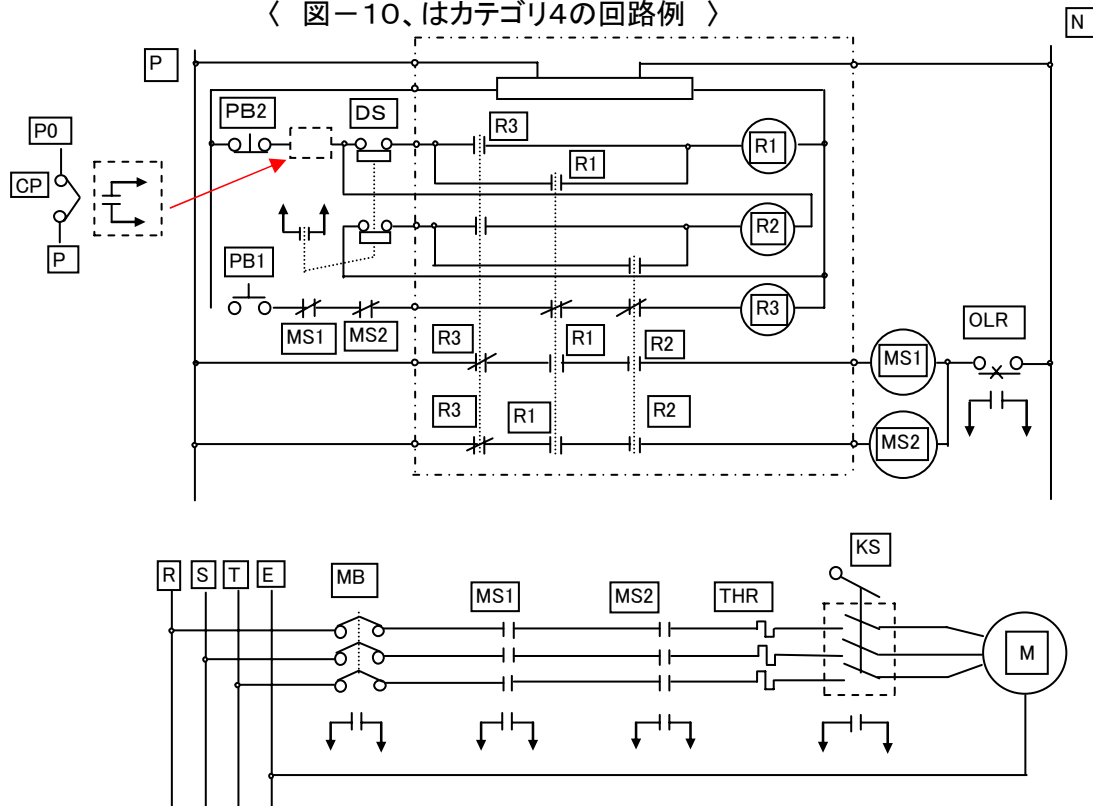


制御の安全

④カテゴリ4の回路例

カテゴリ4は安全リレーを使用した二重化回路で組むことができ、点線で囲われた部分はカテゴリ4の安全リレー・ユニットと置換えられる。故障は適時検出される。

〈 図-10、はカテゴリ4の回路例 〉



8、 ロックアウト

ロックアウトは、工事作業や保全作業の際安全を確保するためにエネルギー源(電源、エア源等)を遮断し、機械装置を動作できなくする追加の保護方策である。

ロックアウト方法としては、下記がある。

- 1) 主ブレーカ外部ハンドルによるロックアウト
 予めロックアウトが可能な機器(電源供給用主ブレーカの制御盤外部ハンドル、エア源供給用ストップバルブ)を使用し、オフ位置で南京錠により固定する。
- 2) ロックアウト・カバー
 後付けロックアウト・カバー(ブレーカ用、ストップ・バルブ用)を使用し、オフ位置で南京錠により固定する。
- 3) 安全リミット・スイッチによるロックアウト
 安全柵の扉または安全ガード(防護ガード)の閉確認用安全リミット・スイッチの専用アクチュエータの代わりに、南京錠が取付けられる作業用アクチュエータを使用して、非常停止状態が解除できないようにする。
- 4) タグアウト
 タグアウトとは、使用する南京錠に使用者の名札を取付けて管理することで、工事作業や保全作業を行う者が、各自携帯し必要に応じて作業場の存在確認に使用することである。

おわりに

本稿に記載した制御設計手順に従って、機械の制御システムのリスクを低減する保護方策が、機械安全に関わる方々の一助になれば幸いである。

制御の安全

参考文献

- 1) JIS B 9700-1: 2004
機械類の安全性-設計のための基本概念、一般原則-第1部: 基本用語、方法論
- 2) JIS B 9700-2: 2004
機械類の安全性-設計のための基本概念、一般原則-第2部: 技術原則
- 3) JIS B 9702: 2000
機械類の安全性-リスクアセスメント原則
- 4) JIS B 9705-1: 2000
機械類の安全性-制御システムの安全関連部-第1部: 設計のための一般原則
- 5) ISO 14119
機械類の安全性-ガード付属のインターロック装置-設計および選択のための原則
- 6) JIS B 9960-1: 1999
機械類の安全性-機械の電気装置-第1部: 一般要求事項
- 7) BIA報告: 1997/6