

# 機械設備における安全制御の考察

## Study of Machine Safety Control

宮脇信芳 N. MIYAWAKI

Since the establishment of ISO12100 (machine safety basic concepts and design-related general principles) in 2004, machine makers in Japan have been paying great attention to design safety. Especially in the machine control field, safety protection control measures based on system risk assessment are required. In accordance with the popularity of safety control measures, safety machine control systems with a reliable and user-friendly safety PLC (programmable logic controller) have been widely used. "Machinery Safety" means the safety of machines including the control system. This document describes safety design measures, safeguards, complementary protective measures, and additional protection measures based on ISO12100. Furthermore, regarding fail-safe safety systems including safety PLC supporting such measures, using JTEKT's safety PLC TOYOPUC-PCS as an example, the applicable scope of safety PLC and applicable stop categories according to the international safety standard are described. Furthermore, concrete fail-safe control systems using a safety PLC are described.

**Key Words:** machine, inherent safety, functional safety, fail safe, safety PLC

### 1. はじめに

近年の欧州を中心とする機械安全に対する意識の高まりに伴い、EUの機械指令を原点とするEN規格EN292（1992年機械安全欧州規格）を中核とした規格群が体系化され、グローバルスタンダードとしての国際安全規格ISO12100（機械類の安全性－基本概念、設計のための一般原則）が2004年に制定された。また、日本において、2006年4月に労働安全衛生法が改正され、職場における労働災害発生の要因を事前に除くために、設備などに起因する危険性の調査（リスクアセスメント）を実施し、その結果に基づいた対策をとることが必要になっており、機械設備類の安全設計が注目されている。特に制御の技術分野では設備のリスクアセスメントの結果に応じた制御カテゴリによる保護方策（以下、安全制御方策と呼ぶ）が必要となる。安全制御方策の普及に伴い、安全PLCが普及してきている。安全PLCは別名フェールセーフPLCとも呼ばれているが、フェールセーフとは、制御システムにおける故障時、システム自身で故障診断し、故障の場合、安全状態へ移行する制御である。このような制御システムが安全制御回路の特色と

なっている。ここではリスク低減の方策と機械安全制御におけるフェールセーフ制御について説明する。

### 2. リスクアセスメント手順とリスク低減

図1に国際安全規格ISO12100で示される、機械に関するリスクアセスメントとリスク低減手順を示す。

### 3. リスク低減の方策

リスク低減方策としては、まず本質的安全設計（Inherent safety）方策→安全防護による保護方策→付加の保護方策→使用者への情報の順序で保護方策をとり、許容可能なリスクまで低減することを義務付けている。ISO12100の規格体系を図2に示す。

具体的なリスク低減の手順としてA→B→C→Dの順番に保護方策を実施し、最終的に機械システムを許容可能なリスクレベルまで低下させるような安全対策を実施する。

また、これらの安全設計を可能にするためには、安全制御システムが不可欠であり、主として動力の供給/遮

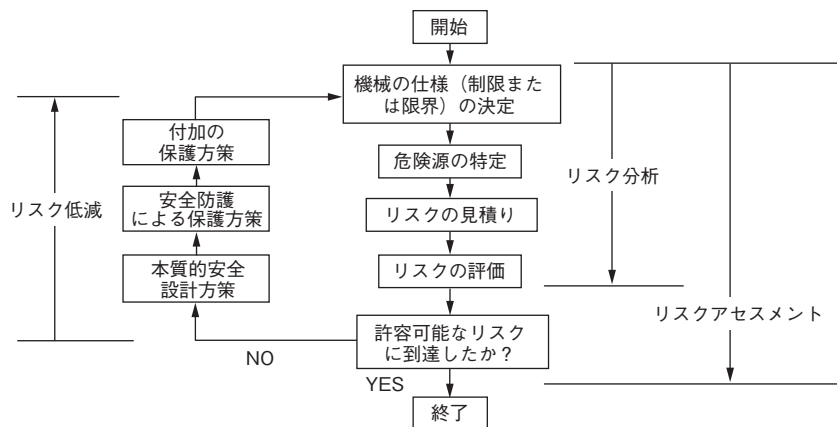


図1 ISO12100で示されるリスクアセスメントとリスク低減  
Risk assessment and reduction procedures based on ISO12100

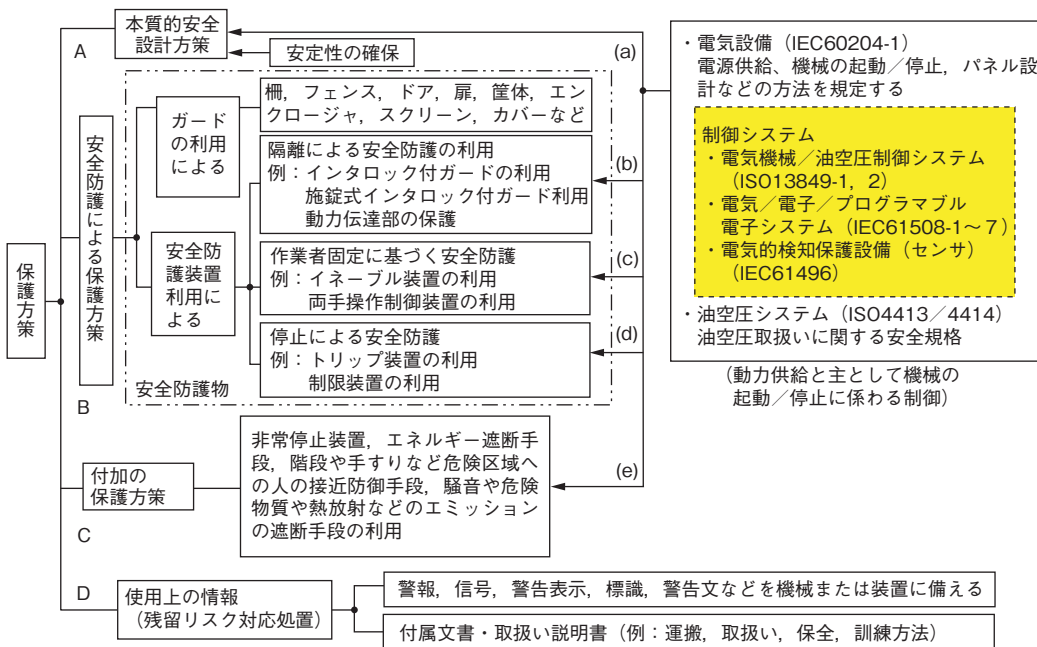


図2 一部関連規格を考慮したISO12100の規格構成<sup>1)</sup>  
Standard system of international safety standard ISO12100

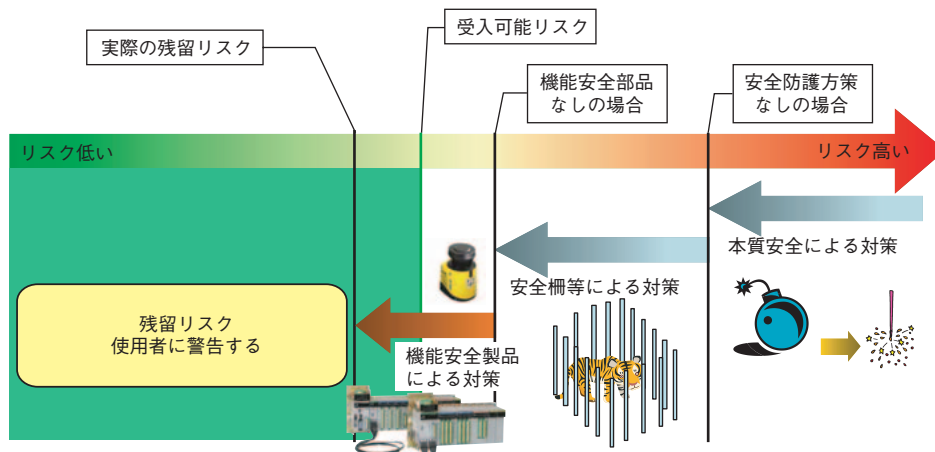


図3 具体的なリスク低減手順のイメージ図  
Image drawing of concrete risk reduction procedures

断と起動／停止の制御を実施する。制御装置としては、安全リレー、安全 PLC が採用されるが、最近では電気／電子／プログラマブル電子システム (IEC61508-1 ～ 7) 規格<sup>2)</sup> に認証された安全 PLC が、安全制御において重要な位置付けとなってきている。

具体的リスク低減の手順のイメージ図を図3に示す。

#### 4. 機械制御における安全課題

可動部のある設備は停止状態から、起動→決められたサイクル動作→再び停止状態を繰り返す。このサイクルにおいて確認が必要な内容を表1に示す。

表1 機械運転サイクル中の安全運転課題  
Safety subjects during machine operation cycle

運転サイクル	安全運転上の課題
1) 起動時	起動によって事故が発生しない危険な状態 (例: 人が危険領域に存在) で起動が行われない
2) 運転中 (継続時)	運転中に危険な状態が発生した場合 (例: 人が危険領域に移動) 設備を停止させる
3) 停止中	機械停止状態から意図しない起動が行われないことを確認する
4) 全てのサイクル中	安全制御系が危険状態 (すなわち故障状態) の場合は、設備を停止させる

あらゆるサイクル中において、安全制御系が危険状態 (すなわち故障状態) となって、制御不能状態に陥る場合は即、事故につながる可能性がある。このような事態を回避するために安全制御装置ではフェールセーフの能力が必要である。国際安全規格では制御システムの安全能力として電気／電子／プログラマブル電子システム規格 IEC61508 における SIL (安全水準度) および ISO13849 におけるカテゴリを定めて、安全能力を査定している。

通常の SIL2 あるいはカテゴリ 3 以上のプログラマブル電子システムにおいては 1oo2 (one out of 2) 以上のアーキテクチャで構成されフェールセーフを実現している。図4に当社製安全 PLC TOYOPUC\*-PCS のアーキテクチャを示す。

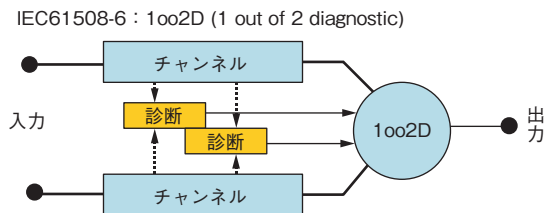


図4 IEC61508-6に基づくTOYOPUC-PCSアーキテクチャ

TOYOPUC-PCS architecture based on IEC61508-6

TOYOPUC-PCS のアーキテクチャは並列接続された二つのチャンネルから構成されており、いずれかのチャンネルの診断試験で障害が検出された場合、あるいは出力状態が一致しない場合、システムは安全状態 (通常は出力 OFF 状態) に速やかに移行する。

#### 5. 安全PLC TOYOPUC-PCS適応範囲

当社製安全 PLC TOYOPUC-PCS の IEC61508 における SIL 値は以下の通りである。

①低需要モード：安全関連システムになされる発動要請の頻度が年 1 回以下または定期チェック (プルーフチェック) 頻度の 2 倍以下の場合 (表2)

表2 低需要運転モード  
Low demand mode of operation

PFD	SIL
$\geq 10^{-4}$ から $< 10^{-3}$ まで	3
$\geq 10^{-3}$ から $< 10^{-2}$ まで	2
$\geq 10^{-2}$ から $< 10^{-1}$ まで	1

PFD =  $1.29 \times 10^{-4}$  (SIL3)

②高需要モードまたは連続モード：安全関連システムになされる発動要請の頻度が年 1 回より大きいかまたは定期チェック (プルーフチェック) 頻度の 2 倍より大きい場合 (表3)

表3 高需要または連続運転モード  
High demand or continuous mode of operation

PFH	SIL
$\geq 10^{-8}$ から $< 10^{-7}$ まで	3
$\geq 10^{-7}$ から $< 10^{-6}$ まで	2
$\geq 10^{-6}$ から $< 10^{-5}$ まで	1

PFH =  $1.56 \times 10^{-8}$  (SIL3)

表 4 EN60204-1 における停止カテゴリと安全 PLC  
Safety PLC and stop category of EN60204-1

停止種類	EN60204-1 条項 9.2.2 停止カテゴリ	説明	安全 PLC 適用範囲
非制御停止	0	機械のアクチュエータ電源を即断する.	適応可能
制御停止	1	機械のアクチュエータが停止するまで電源を供給し、停止後、電源を遮断する.	適応可能
制御停止	2	機械アクチュエータに電源を供給した状態での停止. ISO14118 (EN 1037)「意図しない起動からの保護」に対応した付加的な手段・装置が必要.	安全 PLC だけでは適応不可能

また TOYOPUC-PCS は EN954 のカテゴリ 4 を実現している。このことは TOYOPUC-PCS が一般産業機械のすべての用途に対応可能であることを示している。

また製品の適応可能な停止カテゴリについては EN60204-1 条項 9.2.2 に基づいて次の三つのカテゴリに分類されており表 4 の内容で対応可能である。

## 6. 機械安全制御システムにおけるフェールセーフ制御方策

安全 PLC は図 4 のアーキテクチャにより、フェールセーフを実現している。実際の安全制御システムは IEC61508-6 におけるセンサ部、ロジックソルバ部、アクチュエータ部より構成されており（図 5）、そのプログラミング、各部とのつなぎ配線／回路を含めてシステム全体でフェールセーフ構造を達成する必要がある。

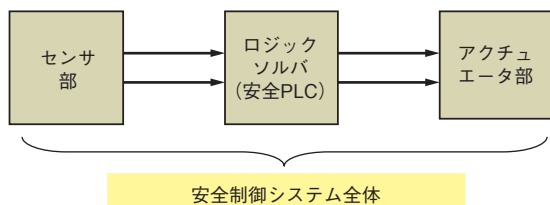


図5 IEC61508-6に基づく安全制御システム  
Safety control system based on IEC61508-6

主なフェールセーフ制御についてその方策を具体的に説明する。

### ① ボタンオフ確認

起動ボタンを押して接点を閉じる動作から、ボタンを離して接点が開く動作（溶着のないこと）を確認して、はじめて起動信号を発生させることが望ましい。（このことにより、起動ボタンの接点溶着による意図しない起

動の可能性を少なくすることができる。）

### ② 再起動防止

起動ボタンによりサイクルが起動され自己保持回路により運転が継続される。作業者が停止操作を実施するか、安全装置が作動した場合、あるいは故障によるフェールセーフの停止があった場合、自己保持を解除し、機械の再起動を防止する。

### ③ ノーマルクローズ接点

作業者が非常停止ボタンを押すときの力、安全柵の扉を開ける時の力、機械がストロークエンドスイッチを押す力など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て、機械を止める。（安全回路配線に断線があった場合、機械を停止させることができる。）

### ④ アンチバレンタ（相反）信号（カテゴリ 3, 4 対応）

相反信号（正信号と負信号）のスイッチを 2 個設置して、安全扉の開閉の信号を監視する。（デバイスの多様性を利用して共通原因による故障の確率を下げる。）

### ⑤ 二重化信号不一致検出（カテゴリ 3, 4 対応）

接点を二重化し、二つの動作が不一致のときは、接点が溶着あるいは接触不良を生じていると見なして、危険な状態を回避するために、機械を停止させる。

安全 PLC を使用して安全回路を構築した場合、二重化信号に対して信号不一致検出は自動的に実施される。

### ⑥ バックチェック

出力におけるイネーブル回路のコンタクタなどの回路において、メイン回路（a 接点）に溶着が発生した場合、対となる b 接点（あるいは補助 b 接点）によってこれを検出し、直ちに機械を停止するか、あるいは次のサイクルの起動をかけない。

### ⑦ テストパルス（安全 PLC 入／出力モジュールに適用）

入力モジュールはテストパルス（数百 μs 幅のパルス）

により自己監視される。入力チャンネル（アドレス）の確認はこの短い期間の間は中断され、接続されたセンサの信号確認はテストパルスの間は考慮される。

出力モジュールは、半導体出力モジュールがテストパルス（数百  $\mu\text{s}$  幅のパルス）により自己監視される。ただし、出力側のアクチュエータがテストパルスにより影響を受けないことを確認しなければならない。

⑧二重信号のクロスショートチェック（カテゴリ 4）

二重入力信号の配線間で短絡した場合、入力信号が同一の信号となる可能性がある。そのため、本故障を防止するために二重信号の配線間のクロスショート検出機能が必要である。カテゴリ 4 の安全 PLC においては、クロスショートの検出ができるようになっている。

⑨トランジスタ出力（カテゴリ 4）

トランジスタ出力モジュールに対する安全 PLC に故障が発生した場合、出力は出力トランジスタにより遮断されるが、共通原因での故障による危険側故障確率を下げるために、さらにリレーによる出力遮断が実施される。これは一つのストレスに対して、トランジスタとリレーによる異質のデバイスにより出力遮断を確実にするためである（TOYOPUC-PCS で実施）。

## 7. 安全PLC回路例

### 7.1 非常停止ボタン回路（図6）

非常停止ボタンは二重で b 接点を採用している。二重入力信号は入力サイドであらかじめ決められた時間内での二重化信号不一致検出を実施している。出力は二重のリレー（コンタクタ）を採用し補助接点の b 接点を入力カードに入力して、起動時の溶着チェックを実施している。（6章③，⑤～⑨に対応）

### 7.2 安全柵ドア監視回路（図7）

ドア監視センサは二重で a, b 接点を採用している。二重入力信号は入力サイドであらかじめ決められた時間内での二重化信号（相反モード）不一致検出を実施している。出力は二重のリレー（コンタクタ）を採用し補助接点の b 接点を入力カードに入力して、起動時の溶着チェックを実施している。（6章③～⑨に対応）

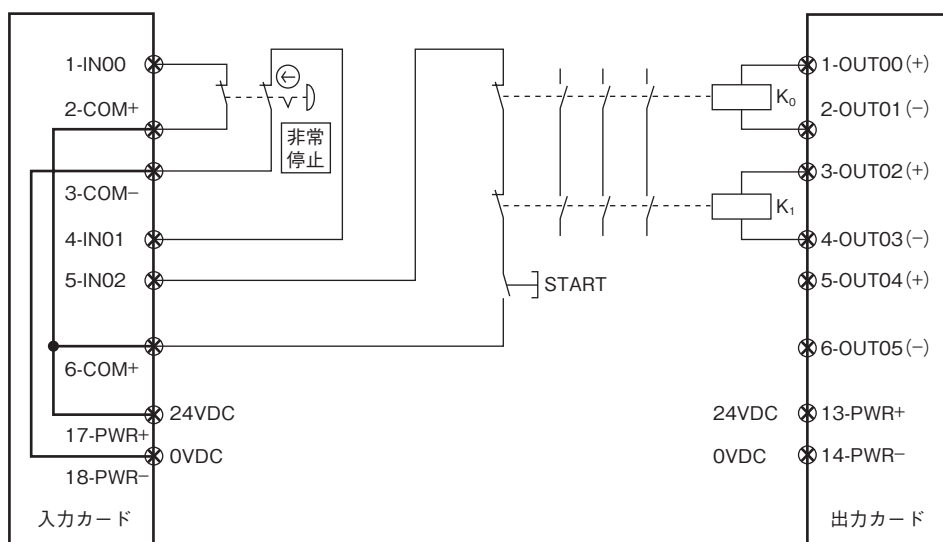


図6 非常停止ボタン回路図  
Emergency stop button circuit

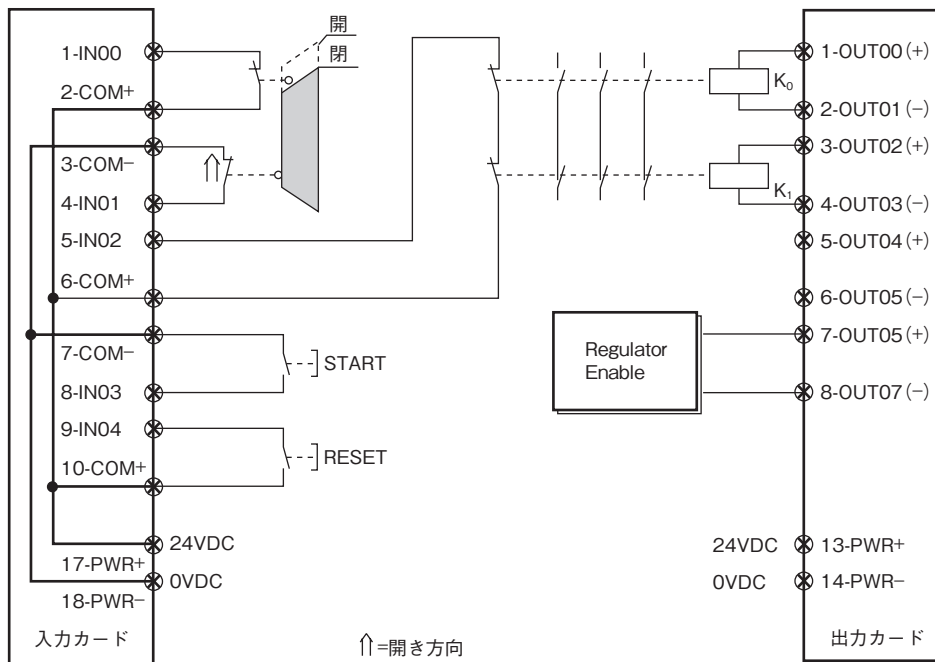


図7 安全柵ドア監視回路図  
Safety fence door monitoring circuit

## 8. おわりに

当社の安全 PLC TOYOPUC-PCS の開発により、グローバルに拡大する自動車生産ラインなどの大規模設備を中心に、従来の安全リレー制御から安全 PLC を採用した安全制御システムの普及が急速に進んでいる。しかし、機械設備の大部分を占める中一小型設備機械については、コスト上の課題があるため、安全 PLC の普及はまだまだである<sup>3)</sup>。今後、ISO12100 の規格化にともない、ますます使いやすく保全性の高い安全 PLC の需要が見込まれると思われる。あらゆる現場における作業者の安全性確保のための安全 PLC の開発が望まれており、引き続き大型設備用から小型設備用の安全 PLC を開発・シリーズ化を進め普及させていきたい。

\* TOYOPUC は(株)ジェイテクトの登録商標です。

## 参考文献

- 1) 蓬原弘一：国際規格に基づく安全，長岡技術科学大学，(2005. 5)3.
- 2) IEC61508-1～7:Functional safety of Electrical/Electronic/Programmable electronic safety related systems Part 1(1998)65.
- 3) 丹羽邦幸，宮脇信芳：計測制御，(2006. 9)34.

## 筆者



宮脇信芳\*  
N. MIYAWAKI

\* 工作機械・メカトロ事業本部 メカトロ制御技術  
部