機能安全活用実践マニュアル
産業用ロボットシステム編

平成 28 年度厚生労働省委託

産業用ロボットのリスクアセスメント促進等事業

平成 29 年 2 月

中央労働災害防止協会

機能安全活用実践マニュアル　産業用ロボットシステム編

平成29年2月

中央労働災害防止協会

機能安全活用実践マニュアル
産業用ロボットシステム編

平成 28 年度厚生労働省委託
産業用ロボットのリスクアセスメント促進等事業

平成 29 年 2 月
中央労働災害防止協会　技術支援部
〒108-0014　東京都港区芝 5－35－2
TEL 03-3452-6375　FAX 03-5445-1774
E メール　sidouka@jisha.or.jp

中央労働災害防止協会　技術支援部　2017.2

はじめに

我が国では、昭和 56 年の産業用ロボットによる初めての死亡災害を契機に、産業用ロボットに関する労働安全衛生規則が整備され、その後、産業用ロボットの設計に当たっての安全要求事項を規定する国内外の安全規格が整備されてきた。このような規則や規格の整備と普及により、産業用ロボットによる労働災害は減少してきているが、いまだに 30 件/年前後発生しており、その過半数は挟まれ・巻き込まれ災害や激突され災害という比較的重篤な危害を生じている。

一方、近年の制御機能の高度化・複雑化の流れは産業用ロボットにも波及して、電気・電子・プログラマブル電子制御システムが積極的に導入されるようになってきた。このような制御システムは、従来のインタロックの仕組みの中ではその機能の一部を活用しているのみであったが、近年、作業者とロボットが作業空間を共有して協働するという新しい運用形態が提案され、安全規格の改正により、制御機能の実現方法が示されるようになった。また、厚生労働省の「機能安全を用いた機械等の取扱規制のあり方に関する検討会」においても、産業用ロボットへの機能安全制御の導入可能性が検討され、産業用ロボット本来の特質を活かしつつ安全確保することが指向されている。

このような状況下で、産業用ロボットメーカが機能安全を導入して協働運転に対応するロボットを市販するようになっているが、ロボット本体以外のエンドエフェクタ（ロボットハンド）の制御や周辺の連携する機械設備の制御はメーカではなく、システム統合者(インテグレータと呼ぶ)の役割となっている。しかし、産業用ロボットの安全規格や機能安全に関する規格は整備されつつあるが、システム統合における機能安全設計の方策は明確になっていない。これらの規格から統合機械システムに機能安全を導入する具体的な設計方法を理解することはかなりハードルが高い状況にある。

本書は、「機能安全の活用促進に関する検討委員会」の「産業用ロボットワーキンググループ」において作成され、産業用ロボットのシステムインテグレータ及びその役割を担う設計者に向けて、機能安全制御を前提としたロボットシステムの設計方法を指南する。なお、機能安全の基礎知識については「機能安全活用テキスト」で習得済みであることが前提である。その上で、産業用ロボットを用いて統合システムを設計する場合に、リスクアセスメントから始まる安全設計の手順、機能安全による制御システムの安全目標設定と実現方法、及びそれら手段の試験と安全性評価についてまとめている。また、インテグレータが実際の手順を理解しやすくするため事例紹介と例題演習を含めており、実務的な内容となっている。本書は 2 日間の講義説明を想定しているが、紙面の都合もあるため、代表的な手段や事例の紹介に留めている。技術内容の詳細や補足説明は関連規格等を参照されたい。

目次

第１章　機能安全設計コンセプト

１　ロボットシステムの構築

産業用ロボットは構造部材にモータ、駆動機構、制御装置、センサ等の部品を組み合わせた製品として市販されているが、通常の産業用機械と大きく異なる点は、ロボット本体だけでは最終製品として完結しておらず、統合システム化によって機能や性能が確定して価値が高まることである。産業用ロボットメーカが準備した機能をプログラム開発によりタスクとして実現することから始まり、エンドエフェクタやセンサ、インタフェース等の付加や他機械との連携、生産システムへの組み込みなどを行って、ロボットを中核とする機械システムを完成させなければ、ユーザはロボットを運用できない。

産業用ロボットのインテグレータはロボットメーカとユーザを結びつける重要な役割を担い、ユーザへのコンサルタントからシステム設計、製作、ユーザへの引き渡しまでに大概次の手順でシステムを構築する。

①　ユーザの要求仕様確認
②　ロボットシステム構想の検討
　（産業用ロボットの選定、全体構成図とレイアウト設計）
③　ロボットシステム仕様書の作成
　（ユーザの承認、受注）
④　詳細設計（機械、電気、プログラム）
⑤　製作、試験
⑥　ユーザ先へ据付、試運転、調整

図 1-1 に一般的な産業用ロボットシステムの構成例を示すが、ロボットメーカは通常図のグレー枠内の要素を「産業用ロボット」として市販しており、インテグレータはこの枠外の要素の選定と仕様の決定、調達とシステム構築を担う。そのため、ロボットアームのリスト部から先のエンドエフェクタ(ハンド)のように直接ロボット本体に装着する要素から、外部のセンサ(外界計測機能)や周辺装置・関連機械までを中核の産業用ロボットに適合させる必要があり、また、これらの要素間及びロボット制御装置との間で制御信号や通信のインタフェースやそれらのプロトコルを決定しなければならない。図には示していないが、実際には関連する作業者を含むロボットと各装置類のレイアウトを設定するため、作業者動線に従い保護装置類との接続が行われる。なお、エンドエフェクタや外部のセンサ、通信インタフェースなどはロボットメーカ

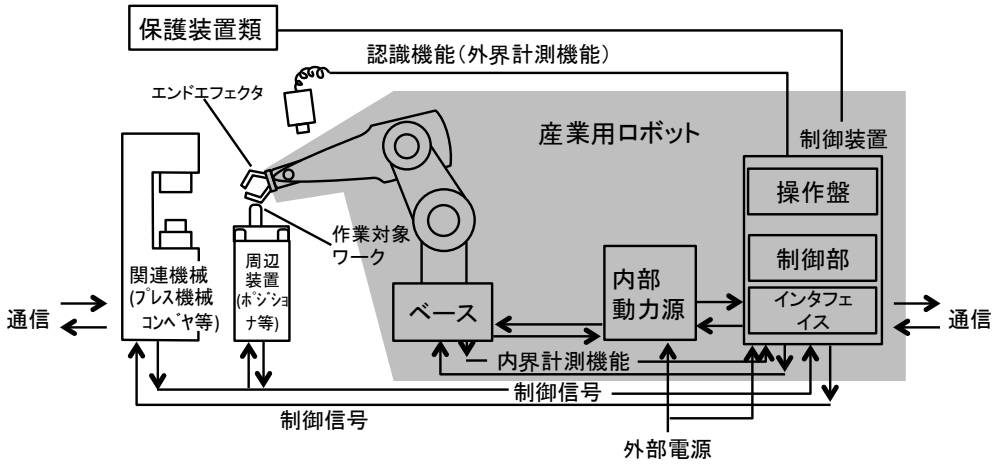


図 1-1　産業用ロボットシステムの構成例

がオプションで準備している場合もある。

本書は、以上のようなロボットシステムの設計に当たり、保護装置類からの信号と各制御信号のうち、安全に関連する情報を扱う制御装置部分に電気・電子・プログラマブル電子制御システムを導入する場合に、その設計方法と手順及び事例を紹介するものである。

2　安全機能の仕様と適用範囲

制御装置の安全関連部分に電気・電子・プログラマブル電子制御を用いた方策を導入する場合、本書の機能安全の対象となり、この方策で使用される部品やソフトウェアの故障や異常によっても安全機能が維持できることを求める。

ロボットシステムの構成要素である産業用ロボット本体や周辺機械設備は、これら単体でのリスク低減方策は既に実施済みで、その方策は機械安全規格に従っていることを前提とする。そのため、システムインテグレーションでは、追加の要求事項を設定しなければならない。産業用ロボット本体及び関連周辺機械単体で規定される安全要求事項に対して、これらを統合するシステムで追加される要求事項の例を表 1-1 に示す。なお、同表における機械単体の機械安全規定には、産業用ロボット以外の一般機械設備も含めて記述している。また、停止機能については、JIS／ISO 規格で、産業用ロボット単体は保護停止（インタロックによる停止）に一時停止が認められており、一般機械設備とは一部異なっている。

表 1-1　システム統合による追加安全規定の例

機能	機械単体の既制定の機械安全規定	システム統合で追加される要求事項例
(a)起動	再起動防止制御に基づく 操作は安全防護空間外から	個別安全防護空間外から意図的な動作を伴う
(b)停止	停止機能は起動機能に優先し、全ての運転に優先する	停止カテゴリ 2 の運転停止状態が可能 制御範囲内で機能
(c)非常停止	非常停止機能とその構造を規定する（追加の危険源を生じない）	一つ以上の非常停止装置を使用 同一操作盤内の非常停止機能は共通
(d)保護装置の機能	隔離による安全防護及び停止に基づく安全防護	人の介入のための保護装置の一時停止が可能 停止不可能な場合は停止される 装置は操作者の直接制御下におかれる
(e)人間工学	視覚表示の必要性とその明瞭性が規定される	レイアウトの視認性､運転サイクルの状況把握 システムの包括的状況の提供
(f)ローカル制御	運転モードはロックされる 非常停止手段を備える	操作時関連設備を他所で扱えない 局所と上位の扱いで危険源を生じない
(g)レイアウト	プラットホーム、通路、はしごなど及びその照明など共通仕様が規定される。エネルギー遮断手段の必要性が示される	材料扱い、保守、交通など空間の割付規定 電気配線の空間的配置 廃棄物の扱い、処理 配管の扱い

産業用ロボットシステムを対象とすると、ロボットや周辺機械の（エンドエフェクタも含む）動作に関わる機能（a～c）に対する要求事項やローカル制御（f)、保護装置機能との信号やりとり（d）については、安全関連制御の対象となり得る。同表には記載していないが、ローカル制御を束ねる統合制御システムや人のシステム内進入（アクセス制御）に関しても安全関連制御の一部となる場合がある。さらに、産業用ロボット特有の安全制御対象として、可動部（エンドエフェクト及びロボットアーム）の位置や速度、エンドエフェクタ部の力（トルク）出力なども含まれる場合があり、停止機能との関連については配慮が必要となる。

本書は、産業用ロボットのシステムインテグレータが市販の産業用ロボット製品を利用することを想定しており、ロボット本体は後述する産業用ロボットの安全規格で規定する安全要求事項は基本的に満足していることが前提である。したがって、産業用ロボット本体が装備している安全機能の性能が、ロボットシステムのインテグレーションによって少なくとも損なわれることがないように設計することを基本とする（ロボット外の付加機能によって新たに発生する危険源に対する安全機能は別途検証）。

設計対象ロボットシステムのリスク低減は後述のリスクアセスメントで述べるが、基本的に危害に至る可能性のある危険事象の発生確率を低減するため、制御装置の安全関連部分に要求されるリスク低減効果（安全性能に該当）目標を決定する（図 1-2 参照）。後述のリスク低減プロセスの中で、制御によるリスク低減は、主に設計図面上で行う本質的安全設計段階の一部と後付けの保護方策適用段階の一部で行われる。この制御によるリスク低減効果を機能安全導入により実現しようとする場合、その効果の証明（妥当性確認）には多くの労力とコストがかかる。特に、機能安全を導入する場合は技術的なハードルが高く、一般的には同図の「制御によるリスク低減」の割合をなるべく減らすことが合理的と思われる。すなわち、制御以外の本質的安全設計や受動的・恒久的な保護方策の確立を優先して、リスク低減における制御システムへの依存度を下げる考え方である。もちろん、制御のみで多くのリスク低減をまかなうことは可能であり、機械制御関係の規格ではそのような意図で説明されている例もあるが、リスク低減は総合的なアプローチを特徴としているので、合理的な設計方針を考慮すべきであろう。

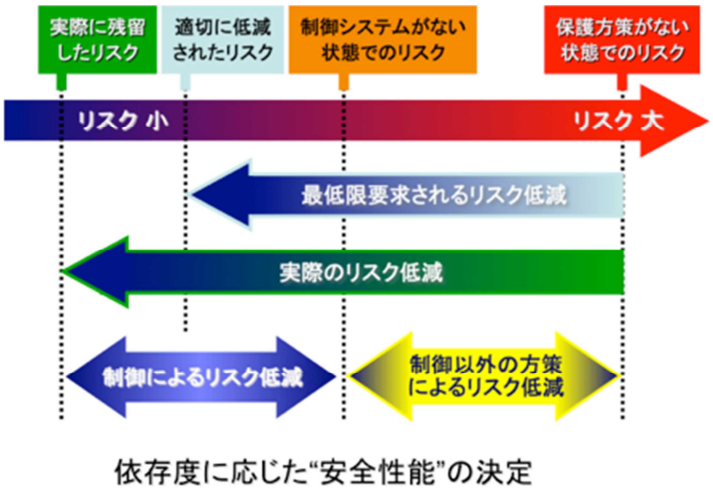


図 1-2　制御によるリスク低減の概念

3　安全関連部の機能分離

ロボットに限らず、機械に関わる人の安全確保の基本は「人と機械の隔離」と「人が機械に接近すると機械停止」を実現することであり、後者は安全制御の範疇であり「インタロック」として説明される。このインタロックは誤りを含む機械運転指令に対して、危険側への誤りのない運転許可が運転出力を支配するという構造である。運転の許可信号は機械の運転状態が安全であることを確認できたときのみ生成され、論理積要素（AND ゲート）で論理処理される。したがって、図 1-3 に示すように、安全確認をするセンサと AND ゲートは少なくとも危険側の誤りを許さない特性（いずれも故

障時は OFF となる）が求められる。運転許可に危険状態を検出して通報するセンサ（危

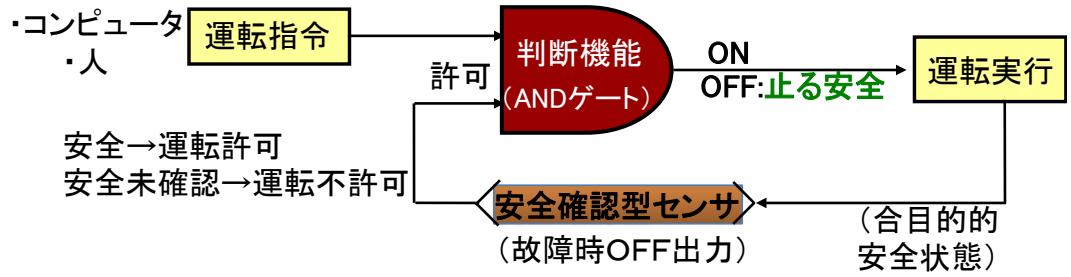


図 1-3　安全確認型インタロック構造

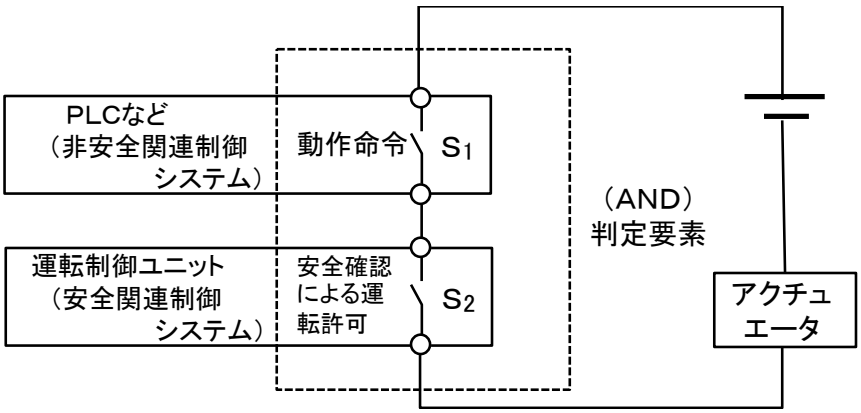


図 1-4　制御システム内の分離と独立

険検出型センサという）を用いる場合は、その出力信号を論理反転しなければならないため、故障時 OFF 出力特性（付加する反転機能を含む）の保証が困難とされてきた。

機械安全規格体系の中で、制御安全規格はこのインタロック構造を前提とし、制御システムのアーキテクチャとシステム挙動の要求事項を規定してきた。制御システムの基本構成の基本的考え方は、図 1-4 に示すように非安全関連部と安全関連部が独立し、両者の出力条件が揃ったときのみアクチュエータによる運動が発生することである。同図はいわゆる安全制御のインタロック構造を表しているが、制御システムによるリスク低減を担うハードウェアを分離独立する方が一般的に設計の複雑さやコスト面からも有利と言われる。ただし、同図の AND 機能は安全関連部の一部であることに注意が必要である。なお、安全関連制御システムには、安全機能を実行するための制御ユニット、人体検知用保護装置（安全確認型センサなど）、安全コンポーネント（安全リレーなど）が含まれる。

機能安全が導入される以前は、同図に示すような機械式接点を有する電磁リレーでインタロックを実現していたため、安全関連部と非安全関連部がハードウェアとして分離していたが、接点が電子式装置に置き換わり、ソフトウェアが関与するようになって、分離・独立構造が明確に表せない場合が出てきた。これは、機能安全機器の登場に伴って制御システム全体をフレキシブル化、高機能化するという制御の大きな転換が主流となっていることを示している。

前述したように、安全制御系のリスク低減効果の検証には非安全系との分離が有利ではあるが、混在する制御系でも機能を実現することは可能となっている。ただし、非安全関連部の不具合等が安全関連部に影響を及ぼさない（少なくとも危険側に）ことを証明しなければならない。

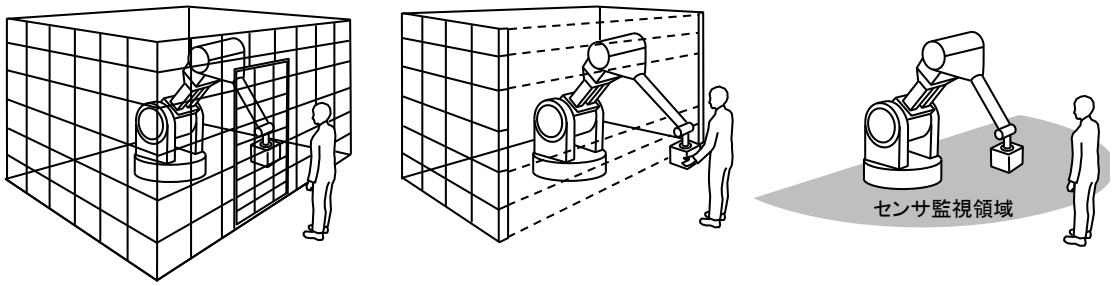
4　産業用ロボットシステムへの機能安全の導入

一方、機能安全規格の側面として、安全性の定量的評価の考え方が入っていることが挙げられる。危険側事象の発生確率を信頼性の観点から数値として算出できるので、例えば、安全確認型センサと危険検出型センサの各々の安全性能を同じ尺度（危険側故障確率）で論じることができる。すなわち、危険検出型センサであっても強力な診断機能が付与されれば、故障時に危険側に推移する確率を下げることが可能となる。

このように、選択できる保護装置が増えてフレキシブルなシステム構成が可能となることで、新しいシステム構成が提案されてきている。例えば、産業用ロボットと人とのワークの授受のアプリケーションを想定すると、ロボットを従来の柵（固定ガード）で囲って人が柵内に進入するときは特定の入口（可動ガード）のみとし、進入時はロボットが停止してワークを授受する構成（図 1-5(a)）が基本である。ロボット自動運転中の人との隔離を基本とするため、単純なインタロック機能で実現できる。

次に、ワークの受け渡しを稼働中のロボットの可動範囲内で行う場合、特定の入口を経由して行う場合は協働運転と見なすことができ、安全関連部の制御系の構成が重要となる。例えば、図 1-5(b)のように光線センサ(ライトカーテン)の一部を無効化して人に近接する場合、このセンサとの連携から近接時のロボット動作を限定するための制御が行われる。そのため、停止機能だけでなくロボット動作に係わる制御(位置、速度、力等)が限定範囲で機能的な安全制御系となる。

さらに、フレキシブルな構成として柵なし環境での協働運転(図 1-5(c))を想定すると、ワーク受け渡し場所は固定する必要はなくなるが、その実現条件として、ロボット可動部と人との距離（速度）を常時モニタするいわゆるバーチャルフェンス機能を構築しなければならない。このような監視のためのセンサには、赤外線、レーザー、電界、超音波、内界センサ（エンコーダ等）等様々な適用が考えられ、安全制御の高機能化に伴う機能安全の安全制御への導入は必然とも言える。



(a)柵あり（可動ガード付き）　(b)開口部あり（光線センサ）　(c)柵なし（センサ監視）

図 1-5　産業用ロボットとのワークの授受のシステム構成

実際に、上記のような協働運転を可能とする産業用ロボットシステムをシステムインテグレータが設計しようとする場合、産業用ロボット本体の持つ機能により主に次の 2 通りのインテグレーションが想定される。

1)　産業用ロボット本体が産業用ロボットの安全規格に適合する製品であり、停止機能を含めて人との相対位置、動作速度、力出力の制御がロボットの制御装置の安全機能として準備される構成（ロボット外からの安全関連情報の信号はロボット内のインタフェースに適合）

2)　産業用ロボット本体は産業用ロボットの安全規格は適合しているが、停止のインタロック機能のみで、ロボット外に安全関連情報の信号を扱う独立した安全関連制御部を設ける構成（ロボット制御装置は外部安全関連制御部の下に繋がる）

当然ながら、1)の場合がインテグレーションは容易であるが、ロボット本体外の制御

範囲とその機能についてはロボットメーカに確認して必要な情報を得る必要がある。一方、2)の場合はインテグレータによる安全関連部の制御設計が重要となる。本書では、既存の機能安全規格適合製品をなるべく利用して、安全関連制御部を構築することを想定しており、いずれの場合でも技術的な選択可能性が広がっているので、以降の内容を理解して実践いただきたい。

5　重要基本用語の定義

本書では、「機能安全活用テキスト」と同様に、「機能安全による機械等に係る安全確保に関する技術上の指針」（平成 28 年厚生労働省告示第 353 号）に記載されている用語を説明したが、機能安全に関する重要な用語は、機能安全に関する規格（JIS B 9705-1 及び JIS B 9961）に基づき補足説明する。

用語	定義または概念
要求安全機能	機械等による労働者の就業に係る危険性又は有害性、それによるリスクを低減するために要求される電気・電子プログラマブル電子制御の機能。
安全関連システム	要求安全機能を実行する電気・電子プログラマブル電子（E/E/EP）制御のシステム。特に断らない限り、「制御」システムを意味するものとする。 本書では、制御システムの安全関連部（SRP/CS）、機械の安全関連電気制御システム（SRECS）（JIS B 9961）と同じ意味で用いる。
機能安全	新たに機械等に電気・電子プログラマブル電子制御の機能を付加することにより、リスクを低減するための措置。
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。（JIS B 9705-1 及び JIS B 9961） 安全関連システムの安全機能は、機能故障がリスクの増加に直ちにつならような本システムの機能。
要求安全機能	機械等による労働者の就業に係る危険性又は有害性、それによるリスクを低減するために要求される電気・電子プログラマブル電子制御の機能。
安全度水準	安全関連システムの信頼性の水準であり、安全機能を実行するための能力を規定する区分レベルとして、安全度水準 SIL とパフォーマンスレベル（PL）が（JIS B 9705-1）用いられる。（JIS B 9705-1 及び JIS B 9961）
故障(failure)	安全関連システムやそれを構成するサブシステム(要素を含む)に要求機能を実行する能力がなくなること。ハードウェア故障(ランダム故障)とソフトウェア故障（系統的故障）がある。（JIS B 9961）
フォールト(fault)	安全関連システムやそれを構成するサブシステム(要素を含む)が、要求機能を実行する能力を低下する、または喪失するような異常状態。（JIS B 9961）故障の結果として障害となる。（JIS B 9705-1）
安全側故障比率(SFF)	サブシステムの全故障の内、サブシステムが危険側故障にならない故障割合。（JIS B 9961）
プルーフテスト	安全関連システムやそれを構成するサブシステム内のフォールトを検出して、必要ならば新品状態に修復する為に実行するテスト。
共通原因故障(CCF)	1 つ以上の事象に起因する故障。（JIS B 9961）
検証	安全関連システム、サブシステム(要素を含む)が関連仕様書の要求事項に適合することを検査により確認すること。（JIS B 9961）

妥当性確認	安全関連システムが特定アプリケーションの機能安全要求事項を満たすことを検査により確認すること。(JIS B 9961)

第 2 章　法規制と関連安全規格

1　　産業用ロボットシステムに関わる法規制

「機能安全活用テキスト」で触れた法規制に対して、本項で詳述する。

(1)　労働安全衛生規則

産業用ロボット及びそのシステムは、各機械に対する共通事項とともに、以下の条項で規制されている。

第三十六条第三十二号	危険業務として産業用ロボットの操作業務を規定、
第百五十条の三	教示等における安全要件、
第百五十条の四	運転中の危険の防止要件、
第百五十条の五	検査時の安全要件、
第百五十一条	点検の実施

(2)　労働安全衛生規則第三十六条第三十一号の規定に基づき厚生労働大臣が定める機械を定める告示（昭和 58 年労働省告示第 51 号）

産業用ロボットとして扱わなくてもよい基準が、本告示により明示された（1983 年 7 月 1 日施行)。特にこの告示で示された『定格出力（駆動用原動機を 2 つ以上有するものにあっては、それぞれの定格出力のうち最大のもの）が 80 ワット以下の駆動用原動機を有する機械』との産業用ロボットから除外する規定は、労働安全衛生規則第 150 条の 4 の規制『産業用ロボットに接触することにより労働者に危険が生ずるおそれのあるときは、さく又は囲いを設ける等当該危険を防止するために必要な措置を講じなければならない。』に適合する必要がない、即ち、柵及び囲いが不要なロボットとして、永らく我が国の工場で運用されてきた。しかし、その後の労働安全衛生規則改正と、それに関連して制定された『機械の包括的な安全基準に関する指針』で、リスクアセスメントに基づくハザードの除去が必要になった。従って全軸 80 ワット以下のモータを使用したロボットであっても、リスクアセスメントの結果によっては柵及び囲いが必要となってきた。このため、人とロボットが安全柵で隔てられることなく、作業領域を共有できる、所謂『協働ロボットシステム』の実現は、実質的に厳しく制限されるようになった。

(3)　国際的な動向

前述した我が国の状況の一方、欧米各国では、2000 年頃から協働ロボットシステム（人とロボットが安全柵で隔てられることなく作業空間を共有するシステム）の実用化が始まり、その実績を基にしてロボットへの安全要求事項を ISO 10218-1:2006（JIS B 8433-1:2007）に盛り込んで 2006 年に国際規格として発行された。さらにロボットシステムとしての安全要求事項を ISO 10218-2:2011（JIS B 8433-2:2015）として 2011 年に発行された（同時に ISO 10218-1 も再改定された)。しかし、協働ロボットシステムは、開発・導入途上の最新の技術であること、また規格審議に十分な時間が取れなかったため、詳細な安全要求事項は、Technical Specification[*1]（技術仕様書）として審議継続することになった。審議された技術仕様書は、2016 年 2 月に ISO/TS 15066:2016 として発行された。

ここで、これら国際規格、技術仕様書の正式名と規格の適用範囲を以下に記す。

● ISO 10218-1:2011 [1]、[2]

Robots and robotic devices — Safety requirements for industrial robots – Part 1: Robots

（ロボット及びロボティックデバイス－産業用ロボットの安全要求事項

－第1部：ロボット）
（適用範囲）産業用ロボットの本質的安全設計、保護方策及び使用上の情報についての要求事項及び指針について規定。産業用ロボットシステムとしてのロボットには言及しない。騒音はロボット単体の重要なハザードとはみなさず、この規格の適用範囲から除外。非産業用ロボットには適用しないが、安全原則は他のロボットに適用することができる。

● ISO 10218-2:2011 [3]、[4]

Robots and robotic devices — Safety requirements for industrial robots – Part 2: Robot systems and integration
（ロボット及びロボティックデバイス－産業用ロボットのための安全要求事項－第2部：ロボットシステム及びインテグレーション）
（適用範囲）産業用ロボット及び産業用ロボットシステムのインテグレーション並びに産業用ロボットセルに対する安全要求事項について規定。インテグレーションには次を含む。

a）産業用ロボットシステム又はセルの設計、製造、設置、運転、保全、又は解体・撤去
b）産業用ロボットシステム又はセルの設計、製造、設置、運転、保全又は解体・撤去に必要な情報
c）産業用ロボットシステム又はセルの構成装置

この規格は、これらのシステムで明確にされる基本的なハザード及び危険状態を規定し、それらハザードに関連するリスクを除去又は適切に低減させる要求事項を提供する。この規格では、プロセス（例：レーザ放射、切り屑の排出、溶接煙）に関連するハザード、騒音は、他の規格を適用し、本規格では取り扱わない。

上記2規格の国内規格は、2015年3月にそれぞれJIS B 8433-1:2015、JIS B 8433-2:2015として発行された。

● ISO/TS 15066:2016*2 [5]

Robots and robotic devices — Collaborative robots
（ロボット及びロボティックデバイス－協働ロボット）
（適用範囲）この技術仕様書は、産業用協働ロボットシステムとその作業環境の安全要求事項について述べ、ISO 10218-1（JIS B 8433-1）に記載の産業用協働ロボットの運転に関する要求事項及びガイダンスを補完し、そしてISO 10218-1（JIS B 8433-1）及びISO 10218-2（JIS B 8433-2）に記載される産業用ロボットシステムに適用する。提示された安全原則は他分野のロボティクスに対して有用でありうるが、非産業用ロボットに対しては適用しない。

【注記】
*1：技術仕様書とは[6]、将来的に国際規格（IS）として合意される可能性はあるが、現時点では次のような理由で、ISOまたはIECが発行する文書
a）ISとして承認されるための必要な支援が得られていない
b）コンセンサスの形成が疑わしい
c）その主題がまだ技術開発の途上にある
d）国際規格として直ちに発行することが不可能な理由が他にある
*2：現在、国内版は作成中で、2017年春に発行される見込みである。

(4)　基発 1224 第 2 号「産業用ロボットに係る労働安全衛生規則第 150 条の 4 の施行通達の一部改正について」(平成 25 年 12 月 24 日発令)、及び基安安発 1224 第 1 号「産業用ロボットに係る労働安全衛生規則第 150 条の 4 の施行通達の一部改正に当たっての留意事項について」(平成 25 年 12 月 24 日発令)

こうした国際的な動向を踏まえて、我が国でも協働ロボットシステムが導入できるようにするために、その方策を示したのが、表題の通達である。従来、各軸 80 ワット以下のモータで構成されたロボットに限られていた人とロボットの協働作業が、80 ワット超のモータで構成されたロボットにも適用できるように『規制緩和』され[7]、協働ロボットが容易に導入できるとの認識が日本国内に広まった。この結果、協働ロボットシステムは、新たな生産方式としての期待が高まった（図 2-1 参照)。

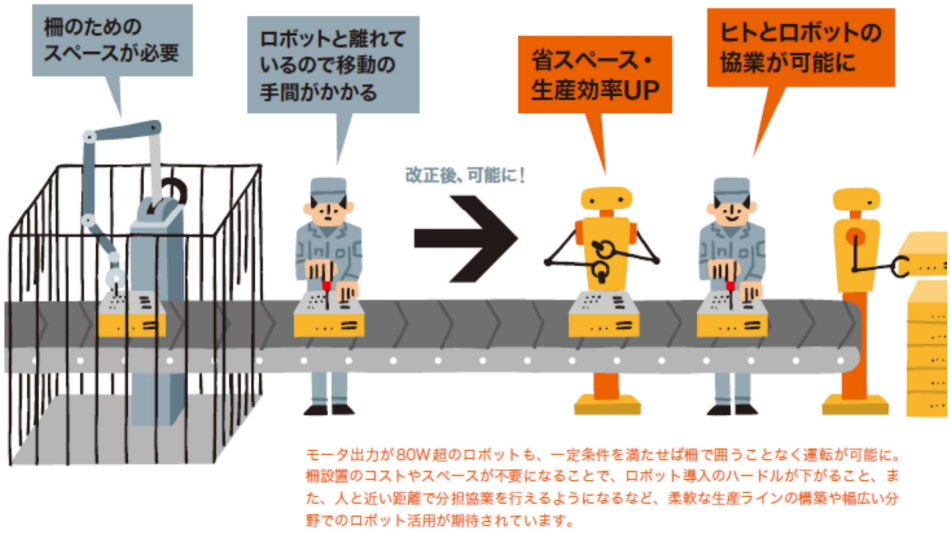


図 2-1　経済産業ジャーナル 2014 年 10・11 月号掲載のイラスト

具体的に基発 1224 第 2 号[*3] では、協働ロボットシステムを実現するために、

『①　ISO 10218―1:2011 及び ISO 10218―2:2011 によりそれぞれ設計、製造及び設置された産業用ロボットを、その使用条件に基づき適切に使用することを求めており、その産業用ロボットは設計者、製造者及び設置者が技術ファイル及び適合宣言書を作成したものであることを条件としている。その前提として、

②　産業用ロボットを使用する事業者が、リスクアセスメント（労働安全衛生法第 28 条の 2 による危険性等の調査）に基づく措置を実施し、産業用ロボットに接触することにより労働者に危険の生ずるおそれが無くなったと評価できることが必要である。そしてその評価結果は、「危険性又は有害性等の調査等に関する指針」(平成 18 年 3 月 10 日付け指針公示第 1 号)に基づいて記録し、保管することが必要になる。』

としている。さらに基安安発 1224 第 1 号では、

『③　産業用ロボットのマニプレータ等の力及び運動エネルギーについては、ISO/TS 15066 が制定され、制御によらず構造的に当該数値以下となることが担保される場合、この観点において危険の生ずるおそれが無いと判断できる一例となる。』

としている。即ち、産業用ロボットが人に接触するときの力と運動エネルギーを

ISO/TS 15066 で規定する値以下にすればよいと規定した。上記①で作成される技術ファイルの内容は附録 A を、適合宣言書の例は附録 B を参照されたい。

従って、協働ロボットシステム実現のためには、国際規格 ISO 10218-1:2011（JIS B 8433-1:2015）及び ISO 10218-2:2011（JIS B 8433-2:2015）に適合すること、さらに人との接触が発生する産業用ロボットにおいては、技術仕様書 ISO/TS 15066 に適合することが必要である。また基発 1224 第 2 号及び基安安発 1224 第 1 号では、上述のように『産業用ロボット』に対して言及し、『産業用ロボットを用いたシステム』とは記述していないので、上述の規格に適合した協働作業用の産業用ロボットを用いるだけでよいような印象を持つかもしれない。しかし、協働作業用に設計製造された産業用ロボットを使用するだけでは不適切で、使用する協働アプリケーションに対処できる機能を持つ産業用協働ロボットを選択することが必須となる。さらにロボットシステムの規格である ISO 10218-2:2011（JIS B 8433-2:2015）への適合を求めていることから、ISO 10218-2:2011 に適合した産業用ロボットシステムとしなければならない。

なお、ISO/IEC 国際規格への適合は、EU 各国などで義務化され、また米国では PL（製造物責任）の観点から実質的に義務化されているのは、ご承知の通りであるが、ISO/IEC が発行する技術仕様書は、EU 各国では義務化されない。従って、我が国は現時点で ISO/TS 15066 が義務化された唯一の国となっている。つまり、我が国では、人とロボットが共存して作業する産業用協働ロボットシステムに対して、高い安全性が要求されていることに留意されたい。

次節に、ISO 10218-1:2011（JIS B 8433-1:2015）が要求する産業用ロボットへの安全性要求事項、及び ISO 10218-2:2011（JIS B 8433-2:2015）が要求する産業用ロボットシステムとしての安全性要求事項を述べる。そして人と産業用ロボットが協働作業するために特別に必要となる安全性要求事項を ISO/TS 15066 に基づいて述べる。また、これらロボット安全規格で使用する主要な用語とその定義を次節に示す。

本章 2、3、4 節に記す内容は、これら規格の主要要求事項をのみ記述したものである。先に述べた**基発 1224 第 2 号と基安安発 1224 第 1 号を遵守するためには、これら規格の全文を熟読し、規格の要求事項に適合させることが必須である。**

【注記】

*3：基発 1224 第 2 号は、ISO 規格への適合を指示しているため、本章の規格番号表示は ISO/IEC 規格番号で表し、規格の参照を容易にするために、ISO/IEC に対応した JIS 規格番号を括弧書きする。

２　ロボット安全規格で使用の用語及びその定義

ISO 10218-1:2011（JIS B 8433-1:2015）、ISO 10218-2:2011（JIS B 8433-2:2015）及び ISO/TS 15066 の各３章で用語とその定義が記述されている中で、本書に関係深い主要用語を表 2-1 に記載する。

表 2-1　ロボット安全規格で使用する用語とその定義

用　語	英語名と定義	出　典
産業用ロボット	(industrial robot) 産業オートメーション用途に用いるため、位置が固定又は移動し、3 軸以上がプログラム可能で、自動制御され、再プログラム可能な多用途マニプレータ。 注記 1 産業用ロボットは、次を含む。 － マニプレータ（アクチュエータを含む)。 － 教示ペンダントを含む制御装置、及び通信インタフェース（ハードウェア及びソフトウェア)。 注記 2 ロボットコントローラによって制御されるあらゆる追加軸を含む。 注記 3 この規格の目的では、次の装置を産業用ロボットとみなす。 － ハンドガイドロボット。 － 移動ロボットのマニプレータ部分。 － 協働ロボット。	Part1、 3.10
産業用ロボットシステム	(industrial robot system) システムは、次を含む。 － 産業用ロボット － エンドエフェクタ － ロボットがタスクを行うために必要なあらゆる機械類、設備、装置、外部の付加軸又はセンサ。	Part1、 3.11
最大空間	(maximum space) 製造者が定めたロボット可動部が届く空間に、エンドエフェクタ及びワークが届く空間を加えた空間	Part1、 3.24.1
制限空間	(restricted space) 最大空間の一部であり、超えてはならない限度を設定する制限装置によって制限する空間。	Part1、 3.24.2
運転空間	(operating space/operational space) 制限空間(3.13.2)の一部で、タスクプログラムによって指令される全ての運動を実行するときに実際に使われる空間。	Part2、 3.13
安全防護空間	(safeguarded space) 周囲の安全防護で定義された空間。	Part1、 3.24.3
協働作業空間	(collaborative workspace) 生産作業中にロボットシステム（ワークを含む）と人間とが、同時に作業を遂行できる作業空間内の空間。	TS、 3.3
協働ロボット	(collaborative robot) 規定された協働作業空間で、人間と直接的な相互作用をするように設計されたロボット。	Part1、 3.2

協働運転	(collaborative operation) 特別の目的で設計したロボットが、定義した作業空間内で人間と直接協働して動く状態。	Part1、 3.4
安全適合監視速度	(safety-rated monitored speed) ロボットフランジに関連する点(例えば、TCP)の直交速度、1 軸又は複数の軸の速度のいずれかが規定された制限値を超えた場合に、保護停止となる安全適合の機能。	Part1、 3.19.1
安全適合低減速度	(safety-rated reduced speed) ロボット速度を250 mm/s以下に制限する安全適合監視速度。 注記 1 安全適合低減速度制限は、低減制御機能に設定する必要はない。 注記 2 安全適合監視速度と安全適合低減速度との違いは、安全適合監視速度制限が250 mm/s を超えない速度に設定できるかどうかである。	Part1、 3.19.2
安全適合ソフト軸/空間制限、安全適合ソフト制限	(safety-rated soft axis and space limiting、safety-rated soft limit) 規定された十分な安全適合性能をもつソフトウェア又はファームウェアを基にしたシステムによって、ロボットの動作範囲に設置された制限。 注記 安全適合ソフト制限は、停止開始点であってもよいし、制限を超えて動作しないことを確実にすることでもよい。	Part1、 3.19.3
安全適合監視停止	(safety-rated monitored stop) 駆動源が切断されない状態でロボットが停止している状況で、ロボットが動作しないことを確実にする、規定された十分な安全性能をもつ監視システム。	Part1、 3.19.6
低減速度制御、低速制御	(reduced speed control、slow speed control) 速度が250 mm/s以下に制限された場合のロボット動作制御のモード。 注記 低減速度は、危険な動作からの回避又はロボットの停止のいずれかのために十分な時間を人に与えることを意図している。	Part1、 3.23
作動制御装置	(actuating control) 制御装置内の機械的機構。 例：接点を開くロッド	Part1、 3.1
同時動作	(simultaneous motion) 単一制御ステーションの制御下における2台以上のロボットの同時動作。	Part1、 3.20

【注】出典欄において、出典規格は以下のように略す。
Part1：ISO 10218-1:2015
Part2：ISO 10218-2:2015
TS　：ISO/TS 15066:2016

ア　産業用ロボットの定義

表 2-1 で示した『産業用ロボット』の定義は、労働安全衛生規則の第 36 条第 31 号での規定、即ち、

『マニプレータ及び記憶装置　（可変シーケンス制御装置及び固定シーケンス制御装置を含む。以下この号において同じ。）　を有し、記憶装置の情報に基づきマニプレータの伸縮、屈伸、上下移動、左右移動若しくは旋回の動作又はこれらの複合動作を自動的に行うことができる機械　（研究開発中のものその他厚生労働大臣が定めるものを除く。以下「産業用ロボット」という。）』

及び、先に示した『昭和 58 年労働省告示第 51 号』と異なるところがある。特にモータ出力による区別は ISO 10218-1 にはない。また ISO 10218-1 では『ロボットコントローラによって制御されるあらゆる追加軸を含む。』は、図 2-2 に示すようなロボットの走行軸が産業用ロボットのコントローラで制御される場合には、走行軸は産業用ロボットの一部として扱わなければならない。従って、システムインテグレータが図 2-2 のようなシステムを設計・製造・設置した場合は、ISO 10218-2:2011（JIS B 8433-2）に適合するだけでなく、走行軸部分を ISO 10218-1:2011（JIS B 8433-1）に適合させなければならないことになる[8]。

図 2-2　走行軸付産業用ロボット

イ　産業用ロボットシステムの定義

我が国の法令において『産業用ロボットシステム』に対する定義はなく、およそのコンセンサスとして、安全柵を含めて、それに囲われた産業用ロボットとその周囲の機器類を『産業用ロボットシステム』または『産業用ロボット』としている。しかし ISO 10218 では明確に定義しているので注意が必要である。特に ISO 10218 は、『ロボットがタスクを行うために必要なあらゆる機械類、設備、装置、外部の付加軸又はセンサ』を産業用ロボットシステムに含めているので、安全柵の内外に関係なく、ロボットのタスクに

関わるものは産業用ロボットシステムに含まれる（図 2-3 参照）。
　例えば、工作機械にワークをロード／アンロードさせるロボットシステムの場合、機械類の 1 つである NC 旋盤は、ISO 23125（JIS B 6031）他の関連規格に適合させるとともに、ロボットのタスクに関わる部分（例えば、チャックの開閉、ドアの開閉）を ISO 10218-2 にも適合させる必要がある。
　さらに、ロボットシステムの設計・製造者は、どの機械・装置がロボットのタスクに含まれるかを取扱説明書などで明確にしておくことが必要である。

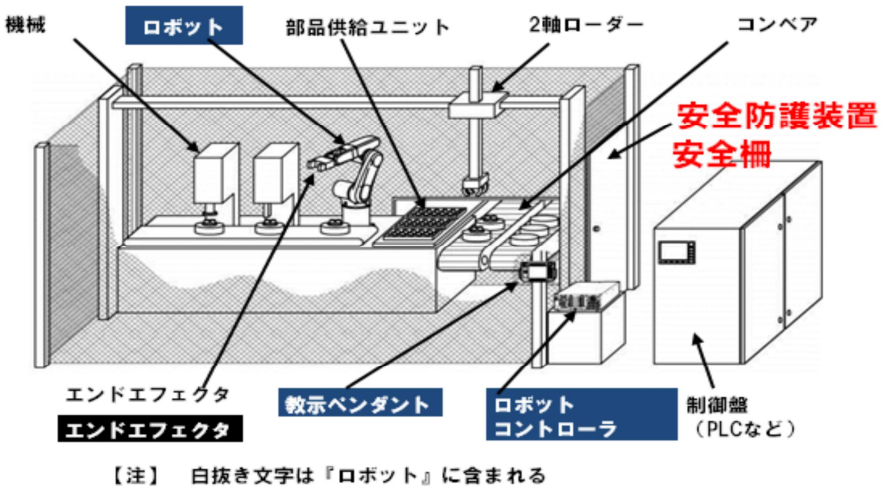


図 2-3　産業用ロボットシステム

3　ISO 10218-1:2011（JIS B 8433-1:2015）の要求事項

　協働ロボットとして使用できる産業用ロボットは、ISO 10218-1:2011（JIS B 8433-1:2015）の要求事項に適合していなければならない。以下に主な要求事項を記す。

ア　一般

　ロボットは、関連する危険源に対して ISO 12100（JIS B 9700）に従って設計しなければならない。
【注記】危険源は第 3 章参照。

イ　動力伝達構成品

1)　一体となったカバー（例：ギアボックス）で保護されない、モータ軸、歯車、駆動ベルト又はリンクのような構成品に起因するハザードの暴露は、固定又は可動ガードによって防止しなければならない。
2)　定期的な保全のために取り除くことが必要な固定ガードの固定器具は、機械又はガードに取り付けたままにしなければならない。
3)　可動ガードは、危険な機械機能が接触する前にその機能が停止するように、危険な 動作に対してインタロックをしなければならない。
4)　インタロックシステムの安全関連制御システム性能は、ISO 12100（JIS B 9700）の 5.4 項（下記**コ**に記述）の要求事項に適合しなければならない。

ウ　動力の消失又は変化

1)　動力の消失又は変化が、危険源となってはならない。
2)　動力の再始動は、いかなる動作も引き起こしてはならない。

エ　構成品の機能不良

ロボットの構成品は、破損若しくは緩み又は蓄積エネルギーの放出によって生じる危険源を最小にする ように設計・製作し、固定し又は内蔵しなければならない。

オ　エネルギー源

ロボットに対しての危険なエネルギー源を全て遮断する方法を備えなければならない。

カ　蓄積エネルギー

1) 蓄積された危険なエネルギーを制御下で放出する方法を備えなければならない。
2) 蓄積エネルギーのハザードを明確にするためのラベルを貼り付けなければならない。

キ　電磁両立性(EMC)

ロボットの設計・製作は、電磁妨害（EMI)、無線周波妨害（RFI）、及び静電気放電（ESD）の予想できる影響による危険な動作又は状態を防止しなければならない。設計上の情報は、IEC 61000-6-2（JIS C 61000-6-2）を参照する。

ク　電気装置（Electrical equipment）

ロボットの電気装置は、IEC 60204-1（JIS B 9960-1）の関連要求事項に従って設計・製作しなければならない。

【注記】JIS B 8433-1:2015 は、ISO 10218-1:2011 の 5.2.7 項に記載の『Electrical equipment』を『電気設備』と訳している。ISO 10218-1:2011 がここで意図するものは、ロボットシステムやロボットラインなどに電源を供給する電源設備などを意図せず、ロボットを構成するロボットコントローラ、コントローラ内の電源やリレー、サーボモータ、配線などの電気装置や電気機器を指すので、注意が必要である。

ケ　作動制御装置

1) 作動制御装置(2節参照）は、意図しない操作を防止するように製作又は配置しなければならない。例えば、適切に設計された押しボタン又はキー選択スイッチを適切な場所に用いればよい。
2) 作動制御装置の状態は、例えば、“動力‘入’”、“不具合（障害）検出”、“自動運転”のように明確に表示しなければならない。表示灯を使用しているのであれば、取付位置は適切で、色は、IEC 60204-1（JIS B 9960-1）に適合していなければならない。
3) 作動制御装置には、その機能を明確に示すためにラベルを張り付けなければならない。
4) ロボット制御システムは、ロボットがペンダント又はその他の教示装置の制御下にある場合には、他の制御元からのロボット動作の始動又は局所制御の選択変更を防止するように設計・製作しなければならない。

コ　安全関連制御システムの性能（ハードウェア及びソフトウェア）

1) 安全関連制御システム(電気、液圧、空気圧及びソフトウェア)は、リスクアセスメントの結果によって下記 4）に示す代替の性能基準が適切であると決定しない限り、下記 3)に掲げる性能基準に適合しなければならない。
2) ロボット及び他の必要な設備の安全関連制御システムの性能は、使用上の情報に

明確に記載しなければならない。

3）制御システムの安全関連部は、ISO 13849-1（JIS B 9705-1）で規定するカテゴリ 3 のアーキテクチャでの PL=d、
又は
IEC 62061（JIS B 9961）で規定するプルーフテスト間隔が 20 年以上で、ハードウェアフォールトトレランスが 1 の SIL2
に適合するように設計しなければならない。

【注記】これら二つの規格は、類似しているが異なる方法で機能安全を取り扱う。設計者は、二つの規格のいずれかを選択して使用してもよい。
本書の第 3 章以降では、ISO 13849-1 を主体に記述する。

4）ロボット及びその意図したアプリケーションに対して行われる包括的リスクアセスメントの結果に基づき、上記 3）で規定した以外の安全関連制御システム性能を適切であると決定してもよい。他の安全関連性能基準を選択することは、特に明示しなければならない。さらに、適切な制限及び注意事項は、影響を受ける設備に付随して提供される使用上の情報に含めなければならない。

サ　ロボット停止機能

1）ロボットは、それぞれに、保護停止機能及び独立した非常停止機能をもたなければならない。

2）これらの機能は、外部保護装置への信号接続を備えなければならない。

表 2-2 に非常停止と保護停止との機能比較を示す。

表 2-2　非常停止と保護停止との機能比較

	非常停止	保護停止
始動位置	オペレータは迅速に妨害なく接近できる	保護装置に対して、始動位置は ISO 13855（JIS B 9715）に示された最小距離の式によって決定される
始動	手動	自動、手動又は安全関連機能による自動的な始動
安全関連システム性能	5.4 項（前記**コ**参照）の性能要求事項に適合	同左
リセット	手動のみ	手動または自動
使用頻度	まれ	様々：運転の都度からまれまで
目的	非常時	安全防護又はリスク低減
効果	全てのハザードへのエネルギー源を除去	安全防護されたハザードを安全に制御

3）非常停止

ロボットは、一つ以上の非常停止機能をもたなければならない。IEC 60204-1（JIS B 9960-1）に基づく停止カテゴリ 0 又は 1 でなければならない。停止カテゴリ 0 又は 1 の選択は、リスクアセスメントによって決定しなければならない。

ここで IEC 60204-1 で規定する停止カテゴリとは以下を示す（IEC 60204-1:2016 の 9.2.2 項参照）。

・停止カテゴリ 0：機械アクチュエータの電源を直接遮断することによる停止。
・停止カテゴリ 1：機械アクチュエータが停止するために電力を供給し、その後停止した時に電源を遮断する制御停止。

・停止カテゴリ 2：機械アクチュエータに電力を供給したままにする制御停止。

4）保護停止

ロボットは、外部の保護装置に接続するために設計した一つ以上の保護停止機能をもたなければならない。保護停止機能の性能は、前記コの要求事項に適合しなければならない。少なくとも一つの保護停止機能は、IEC 60204-1（JIS B 9960-1）で規定する停止カテゴリ 0 又は 1 でなければならない。

ロボットは、IEC 60204-1 で規定する停止カテゴリ 2 を使用した追加保護停止機能をもってもよい。停止カテゴリ 2 の保護停止機能は、ロボット停止後に駆動力を除去しないが、停止状態の監視が必要となる。停止カテゴリ 2 の監視された停止機能は、IEC 61800-5-2 が規定する安全な運転停止(SOS)に対応した電力駆動システムによって得ることができる。

シ　速度制御

1）ロボットのエンドエフェクタ取付フランジの速度、及び TCP（ツールセンタポイント）の速度は、選択できる速度において制御可能でなければならない。TCP の速度を制御できるようにするために、オフセット機能（取付フランジと TCP との相対的な位置を決める）を備えなければならない。

2）低減制御（前記 2 節参照）下の運転時は、TCP 速度が 250 mm/s 以下でなければならない。

3）安全適合低減制御（前記 2 節参照）を備える場合、フォールトが発生したときに TCP の速度が低減速度の制限(前記 2))を超さないように前記**コ**に従って設計及び構成しなければならない。

4）安全適合監視速度（前記 2 節参照）を備える場合は、TCP 速度又は軸速度を前記コに従って監視をしなければならない。

5）手動高速モードがある場合は、250 mm/s を超える速度が実行できる。このモードはプログラム検証に対してのみ使用する。

ス　運転モード

1）運転モードは、モード選択スイッチの各位置にロックすることができ、選択可能でなければならない(例えば、各位置で抜差し可能なキースイッチ)。

2）自動モードでは、ロボットはタスクプログラムを実行し、安全防護は機能していなければならない。

3）手動低減速度では、5.3.5 項（前記ケの 4））及び 5.6 項（前記シ）の規定に適合しなければならない。このモードでは、自動モードは禁止される。

セ　ペンダント制御装置

ペンダント制御装置又は他の教示制御装置が安全防護空間（前記 2 節参照）内からロボットを制御できる場合、

1）ペンダント又は教示制御装置によって始動するロボットの動作は、5.6 項（前記シ参照）に規定する低減制御下になければならない。

2）ペンダント又は教示制御装置は、IEC 60204-1（JIS B 9960-1）に従って、3 ポジションスイッチをもたなければならない。

3）ペンダント又は教示制御装置は､前記サの 1）に従った非常停止機能を備えなけらばならない。

ソ　軸制限

1）制限装置を使用することによって、ロボット周囲の制限空間を設定する手段を備えなければならない。

2）ロボットの 1 次軸（最大移動範囲をもつ軸）の動作を制限するために、調整可能

な機械的ストッパの設置 手段を講じなければならない。
3) 2 次軸及び 3 次軸（2 番目、3 番目に大きい移動範囲をもつ軸）は、調整可能な機械的制限装置又は非機械的制限装置を取り付けられるようにしなければならない。
4) 機械的ストッパは、定格負荷において最大速度状態で、かつ最大伸張時及び最小伸張時の位置でロボットの動作を停止できなければならない。機械的ハードストッパの試験は、いかなる停止の補助もない状態で実施しなければならない。
5) 電気機械的制限装置の制御回路性能は、前記コの要求事項に適合しなければならない。
6) 安全適合ソフト制限に基づく軸及び空間のソフト制限機能を監視し、実行する制御プログラムは、前記コに適合していなければならない。

タ　駆動用動力なしの移動

ロボットは、非常時又は異常状態で、駆動用動力なしで軸が動かせるように設計しなければならない。

チ　つり上げ対策

ロボット及びその附属構成品をつり上げるための指示及び対策は提供され、かつ、予測される負荷を扱うのに十分でなければならない。
例：つり上げフック、アイボルト、ねじ穴、フォークポケット

ツ　電気コネクタ

1) 分離時又は切断時に危険源の原因となる電気コネクタは、意図しない分離を防止するよう設計・製作しなければならない。
2) コネクタには誤接続を防止する手段を備えなければならない。

テ　協働運転

協働運転のために設計されたロボットは、協働運転中であることを示す視覚表示を備えなければならない。更に下記 1) から 4)の一つ以上の要求事項に適合しなければならない。

1) 安全適合監視停止

安全適合監視停止（前記 2 節参照）では、
① 人間が協働作業空間内に存在するとき、ロボットは停止しなければならない。
② 停止機能は、前記コ及び前記サの２)に適合しなければならない。
③ 人間が協働作業空間から離れると、ロボットは自動運転に復帰してもよい。又はロボットは、IEC 60204-1（JIS B 9960-1）に従った停止カテゴリ 2 としてもよい。

ここでは、IEC 61800-5-2 で規定している SOS（Safe operating stop＝安全運転停止）に相当する電気駆動システムが提供する IEC 60204-1（JIS B 9960-1）の監視された停止カテゴリ 2 機能（前記サ参照）を含んでいる。

2) ハンドガイド

① ハンドガイド装置は、エンドエフェクタの近くに配置しなければならない。
② 前記サの 1) 及び前記セの 3) に適合する非常停止を備えなければならない。
③ JIS B3433-1 に適合するイネーブル装置を備えなければならない。
④ ロボットは安全適合監視速度機能が有効な状態で運転しなければならない。（前記シの 4) 参照)。
⑤ 安全適合監視速度（前記 2 節参照）の制限値は、リスクアセスメントによって決定しなければならない。

3）速度及び間隔の監視

① ロボットは、決められた速度、及びオペレータとの間隔を保たなければならない。

② 速度及び間隔の監視機能は、前記コの 3）に適合していなければならない。

③ 協働運転のアプリケーションは、動的で、アプリケーションシステム設計で実施されたリスクアセスメントによって決定されなければならない。

④ ISO 10218-2（JIS B 8433-2）は、協働運転を設計するために使用されなければならない。

⑤ 追加情報は、ISO/TS 15066 に含まれる。

【注記】上記⑤の記述は、原文 ISO 10218-1:2011 5.10.4 に記述されているが、JIS B 8433-1:2015 には記述されていないので、注意が必要である。即ち基発 1224 第 2 号は、ISO 10218-1:2011 への適合を指示しているので、**速度及び間隔の監視アプリケーション用ロボットは、ISO/TS 15066:2016 への適合も必須となる。**

4）本質的設計又は制御による動力及び力の制限

① ロボットの動力又は力を制限する機能は、前記コに従わなければならない。

② ロボットは単に最終的な協働ロボットシステムの中の構成品であり、それだけでは安全な協働運転に対しては十分ではない。協働運転のアプリケーションは、アプリケーションシステム設計で実施されたリスクアセスメントによって決定しなければならない。

③ 追加情報は、ISO/TS 15066 に含まれる。

【注記】上記③の記述は、原文 ISO 10218-1:2011 5.10.5 に記述されているが、JIS B 8433-1:2015 には記述されていないので、注意が必要である。

4 ISO 10218-2:2011（JIS B 8433-2:2015）の要求事項

本規格は安全性要求事項に適合させるための前提として危険源の同定及びリスクアセスメントの実施を要求している。これについては第 3 章で解説する。

基発 1224 第 2 号及び基安安発 1224 第 1 号に適合した産業用協働ロボットシステムを実現するためには、**適用対象外と判断できる要求事項を除き、全ての安全性要求事項に適合させる必要がある**ので、規格を熟読し、それに基づいた設計・製造・据付・運転・保守を実施できるシステムにしていく必要がある。

そこで、産業用協働ロボットシステムも含めて、全ての産業用ロボットシステムが適合しなければならない安全性要求事項の主要点を以下に記す。尚、統合生産システム（IMS）に関する安全性要求事項は、本説明から除外する。

ア 一般原則

1） ロボットシステム及びロボットセルのインテグレーションは, ISO 10218-1（JIS B 8433-2）の要求事項に適合しなければならない。

2） 産業用ロボットシステムは、ISO 12100[9]（JIS B 9700[10]）の原則に従って設計しなければならない。即ち、機械の制限の決定⇒危険源の同定⇒リスクの見積り⇒リスク評価をリスクアセスメントを用いて実施し、危険源を除去することが必要である（詳細は 3 章参照）。

3) ロボットシステムの設計は、容易に運転・保守ができるように、人間工学の原則に従うべきである。これは、操作性・保守性が良くない場合に、作業者は得てして安全装置を無効化するなどして、危険な領域（例：ロボットの稼働領域）に立ち入り、停止条件を取り除いたことにより、ホールド中だったロボットが急に動き出し、作業者が挟まれる労働災害が度々発生しているからである。

イ　安全関連制御システムの性能

1) 安全関連制御システム(電気,油圧,空圧及びソフトウェア)は,リスクアセスメントの結果によって下記 4）に示す**代替の性能基準が適切であると決定しない限り，下記 3）に掲げる性能基準に適合**しなければならない。

2) ロボット及び他の必要な設備の安全関連制御システムの性能は,使用上の情報に明確に記載しなければならない。

3) 制御システムの安全関連部品は、ISO 13849-1（JIS B 9705-1）で規定するカテゴリ 3 のアーキテクチャでの PL=d、又は IEC 62061（JIS B 9961）で規定する,プルーフテスト間隔が 20 年以上で,ハードウェアフォールトトレランスが 1 の SIL2 に適合するように設計しなければならない。

これは、次のことを意味する。

a) いずれの部分に単一の不具合(障害)が生じても安全機能の喪失にはつながらない。

b) 合理的に実行可能な場合は常に,単一の不具合(障害)は,安全機能の次の作動要求時又はその前に検出できなければならない。

c) 単一の不具合(障害)発生時に,安全機能を常に実行し,検出した不具合(障害)が修復されるまで安全状態を維持しなければならない。

d) 合理的に予見可能な不具合(障害)は,全て検出できなければならない。

4) ロボットシステム及びその意図したアプリケーションに対して行われる包括的リスクアセスメントの結果に基づき,上記 3）で規定した以外の安全関連制御システム性能を適切であると決定してもよい。他の安全関連性能基準を選択することは,特に明示しなければならない。さらに,適切な制限及び注意事項は,影響を受ける設備に付随して提供される使用上の情報に含めなければならない。

ウ　環境条件

産業用ロボットシステムは、周囲温度、湿度、電磁妨害、照明などの環境条件を考慮して設計しなければならない。このため、システムで使用する産業用ロボットを含めた機器類、配線類などの各コンポーネントは、予測される運転条件と環境条件に耐えるものを選択する必要がある。

エ　制御装置の位置

自動運転中に必要な機器の操作は、安全柵の外で行えるようしなければならない。また監視しやすい位置に機器を配置することを推奨している。

オ　作動制御装置（Actuating controls）

作動制御装置は、電気電子面において IEC 60204-1（JIS B 9960-1）に適合し、ロボットシステムが危険状態を引き起こす可能性のある外部の遠隔指令（例えば、設備全体を制御するパソコンや PLC からの指令）や条件にも反応しないようにしなければならない。

カ　動力源

1) 全ての動力源（電気、機械的動力、空圧、油圧など）は、その製造者が指定した要求事項に従って使用されなければならない。

2)　電源は IEC 60204-1（JIS B 9960-1)、油圧動力源は ISO 4413（JIS B 8361)、空気圧動力源は ISO 4414（JIS B 8370）のそれぞれの要求事項に適合していなければならない。

キ　等電位ボンディング／接地

保護ボンディング及び機能ボンディングは、IEC 60204-1（JIS B 9960-1）に適合していなければならならない。具体的には IEC 60204-1 に基づき、以下の点への適合が必要になる。

①　すべての露出導電性部分は、保護ボンディング回路に接続する。そしてどのような理由で一部を取りはずした場合も（例えば、定期保全)、残った部分の保護ボンディング回路の導通が失われてはならない。

②　ボンディング接続部の電流容量は、機械的、化学的、電気化学的な影響によって劣化しない。

③　金属製の可とう性ダクト又は非可とう性ダクト並びに金属のケーブル外装は、保護導体として使用してはならない。

④　すべての接続ケーブルの金属ダクトと金属外装（例えば、ケーブル外装、鉛被）は、保護ボンディング回路に接続しなければならない。

⑤　電気装置がふた、扉、カバープレートに取り付けられている場合、保護ボンディング回路の導通性を確保しなければならない。

⑥　保護ボンディング回路には、開閉機器及び過電流保護機器（例えば、スイッチ、ヒューズ）を挿入してはならない。

⑦　保護ボンディング回路の導通性が、取り外し可能な集電子やプラグ／ソケットで切断できる場合、保護ボンディング回路は、充電導体の接点よりも先に閉じ後に開く接点によって開かなければならない。

⑧　各保護導体接続点は、図記号 60417-2-IEC-5019（DB:2002-10）又は文字ＰＥのマーキング又はラベル表示（図 2-4 参照）をするか、緑と黄の２色組合せの色表示をするか、又は記号表示と色表示の組み合わせで識別しなければならない。

⑨　保護導体は、１個所の端末点に１本だけの接続にしなければならない。

⑩　保護導体は。ループインピーダンスを減らすため、可能な限り保護すべき充電導体の近くに配置しなければならない。

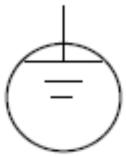


図 2-4　保護ボンディングのラベル表示（保護接地マーク）

ク　エネルギー源の隔離

1)　人が危険なエネルギー源に暴露されないように、危険なエネルギー源を隔離する手段（断路機器)、及びそのエネルギー源のロックアウト機能をもたなければならない。それぞれのエネルギー源毎に断路機器を設けるべきである。

2)　複数の隔離手段を設置する大規模なシステムでは、各断路機器の制御範囲を断路機器ハンドルの近くに明示しなければならない。

ケ　蓄積エネルギーの制御

1)　蓄積された危険なエネルギー（例えば、油空圧アキュムレータ、コンデンサ、バッ

テリ、バネ、カウンターバランス、フライホイール、重力）を制御及び／又は制御下で放出する手段を設けなければならない。

2) 危険なエネルギー源が識別できるようにラベルを貼り付けなければならない。

コ 停止機能

1) 概要

外部の保護装置に接続するために設計した保護停止機能（Protective stop)、及びそれとは独立した非常停止機能（Emergency stop）の両方を持たなければならない。両機能の使い分けの概略を表 2-2（3 節のサ参照）に示す。

2) 非常停止機能

① 動作又は他の危険な機能を始動することのできる各制御ステーションは、IEC 60204-1（JIS B 9960-1）及び ISO 13850 に適合した手動で始動できる非常停止機能を持たなければならない。

② 非常停止機能の作動によってシステム内（場合によってはロボットセル内)、並びに作業空間の他の領域との境界の全てのロボット動作及び危険な機能を停止なければならない。

③ ロボットシステムは,システムに関連する全ての部品に作用する単一の非常停止機能を備えなければならない。

④ 大規模なシステムでは、非常停止機能の制御範囲を明示（ラベルなど）させなければならない。

⑤ 使用上の情報には,それぞれの非常停止装置の制御範囲に関しての情報を記載しなければならない。

⑥ 非常停止機能は,リスクアセスメントによって他の性能基準が適切と決定している場合以外は,前記イの 3）で 規定している要求事項に適合していなければならない。

3) 保護停止機能

① ロボットシステムは,外部の保護装置と接続するように設計された保護停止回路を一つ以上もたなければならない。

② 保護停止機能は,ロボットシステムの全ての動作を停止させ,ロボットシステムの制御下にある他の危険な機能を停止させなければならない。

③ **保護停止機能の性能は,前記イの 3）又は前記イの 4）の要求事項に適合**していなければならない。

④ 駆動システムが IEC 61800-5-2 に適合している場合、停止カテゴリ 2（前記 3 のサ参照）を適用してもよい。

サ エンドエフェクタ

エンドエフェクタは、負荷（ワークなど）を含めて、ロボットの負荷容量及び同的応答範囲内で使用され、またエネルギー供給（例えば、電力、油空圧、真空源）の消失又は変化によって、危険状況となるような負荷（ワークなど）を放出させてはならない。

シ 照明

1) 通常の明るさの周囲照明だけではリスクが生じる可能性のある場合（暗くて誤認識するなど)、運転／操作に必要な照明を設けなければならない。

2) ロボットシステムは,邪魔になるような影の領域がなく、いらいらさせるまぶしさがなく、かつ、照明によって生じる動作部の危険なストロボ効果がないように設計・製作しなければならない。

3) 頻繁な点検及び調整が必要な箇所に対しては、最低限 500 ルクスの照度がなければならない。

ス　イネーブル装置

1)　ISO 10218-1（JIS B 8433-1）に適合したイネーブル装置が、安全防護空間内の人それぞれに提供されなければならない。

2)　それら複数のイネーブル装置は同じ機能性を持たなければならない。

セ　安全防護空間及び制限空間の確立

ロボットシステムの設置面積を小さくするためには、ISO 10218-1（JIS B 8433-1）に適合した産業用ロボットが有するロボット動作制限装置（軸制限装置）又は外付けの装置を用いて、最大空間（前記 2 節参照）を制限することが適切である（制限空間という）。このとき、周囲の安全防護物（安全柵など）は、制限空間（前記 2 節参照）よりも危険源（ロボットの制限領域内など）の近くに設置してはならない。

ソ　システムのレイアウト

1)　ISO 10218-2（JIS B 8433-1）の 5.10（後記ナ参照）項に従ったガードまたは検知保護装置を使用しなければならない。

2)　ガード及び検知保護装置を使用するときは、リスクアセスメントによってロボットの制限空間内で捕捉される又は挟まれる可能性のある箇所を特定し、手動の高速速度モード[*4]の使用を要求するタスクには、最小 500 mm の空隙を設けなければならない。この空隙は、危険源となる計算上の停止位置と建造物、構造物、周囲の防護、ユーティリティ、捕捉又は挟まれを生じ得るロボットの機能を特に補助しているものに限らないその他の機械及び設備との間にも必要である。さらに電気機器用筐体は、ドアを完全に開くことができ、ドアが開いたときであっても脱出経路が常に確保できるように設置し、

　－　ドアは、脱出の方向を考慮して、閉位置へ容易に押すことができる。

　－　ドアが完全に開いたとき、500 mm 以上の空隙がある

こともなる（図 2-5 参照）。

従って、ロボットシステムを工場のどこに設置するかを十分考慮して、ロボットシステムを設計・製造することが重要である。

3)　オペレータが使用しやすいように、制御機器（ティーチペンダントやロボット制御盤など）は、リスクアセスメントの結果に基づき、接近場所の高さから 400 ～ 2000 mm の高さに設置しなければならない。接近（例えば所定のサービスのための）が必要な要素を含んだ電気装置を普通に届く高さより上（例えば、機械の上）に設置する場合は、接近手段（例えば、作業プラットホーム）を備えなければならない。

産業用協働ロボットを使用するときは、危険源が除去できた判断できる場合にロボットに対するこれらの使用は除外できるが、ロボット以外に危険源が存在する場合は、それへの接近を防止するために、これらのガードまたは検知保護装置の使用が不可欠である。

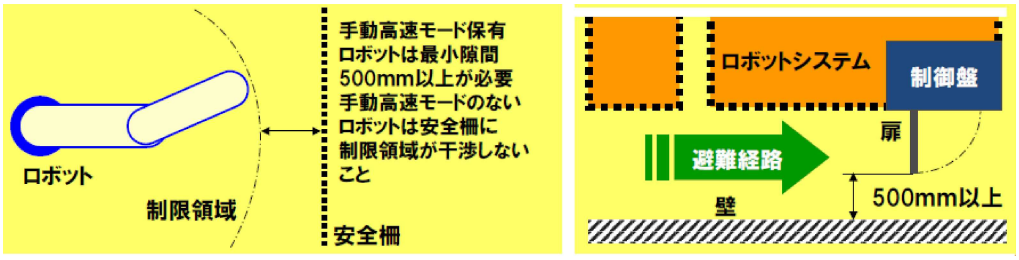


図 2-5　産業用ロボットシステムのレイアウト

【注記】

*4：ロボットの手動運転時に、速度が 250 mm/s を超えて動作することのできる運転モード

タ　材料搬送（マテリアルハンドリング）

部材を安全防護空間に出入りさせる区域では、人が検知されずに危険区域に立ち入ることを防ぐ手段を講じ、これらの手段は、人が危険源と接触するのを防ぐか、又は危険源に到達する前にその他のハザードが発生することなく危険源を安全な状態にするかのいずれかであることが必要である（図 2-6 参照）。

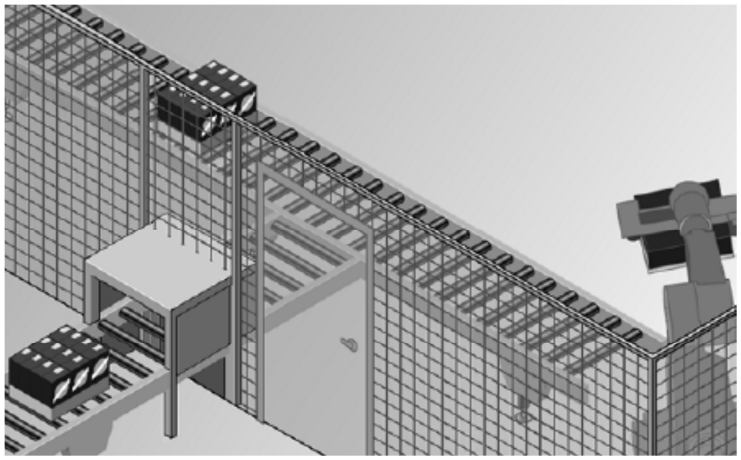


図 2-6　材料搬送部にカバー

チ　工程の監視

工程の監視は、安全防護空間外から行えるようにするのが望ましい。そしてリスクアセスメントの結果に基づき、安全な作業位置及び監視場所（例えば、プラットホーム、監視用通路、遠隔操作での映像システム）を設けなければならない。もし安全防護空間外から監視できない場合、後述する手動低減速度、又は手動高速を用いなければならない。これらの実施も不可能な場合は、ロボットシステムは、プロセスの観察を行うオペレータが危険状態にないことを確実にできる別の制御モードを備えなければならない。

ツ　運転モード

1)　概要

運転モードは、手動モードと自動モードの２つがある。それぞれは ISO 10218-1（JIS B 8433-1）で、以下のように定義されている。

- 手動モード（manual mode）：オペレータによる直接制御を許可する制御状態
- 自動モード（automatic mode）：設定したタスクプログラムに従って、ロボット制御システムが作動する運転モード。

2)　手動モード

①　ISO 10218-1（JIS B 8433-1）に適合したティーチペンダント、又は類似の制御ステーションによってのみ実行できなければならない。

②　これらによる制御（局所制御）中は、予期せぬ危険状態（ロボットが突然動き出すなど）を防止するために、動作の開始及び制御モードの選択が他の機器や外部信号からできてはならない。

③　手動モードは、手動低減モードと手動高速モードの 2 つがあり、手動モードでは、選択されたツールセンターポイント（TCP）の速度が、250 mm/s 以下でなけ

ればならない。

この手動低速モードでは、ロボットシステムのどの部分の動作も、スで述べたイネーブル装置に連動していることが必要である。使用する産業用ロボット単体が250mm/s 以下の速度の製品仕様になっていても、図 2-2 に示すような走行軸付ロボットの場合、走行軸部分の速度が加算されることで、TCP 速度が 250 mm/s を超えることがないように、注意が必要である。

④　手動高速モード

手動高速モード（ツールセンターポイント（TCP）の速度が、250 mm/s を超えるモード）は、プログラム検証だけで使用し、生産では使用してはならない。このモードは、この機能を有する産業用ロボットを使用するときのみに実現可能で、“ソ”で述べた空隙の確保が必要となる。

テ　ペンダント

1)　安全防護空間で使用されるペンダント及びティーチング制御装置は、ISO 10218-1（JIS B 8433-1）に適合したものを使用しなければならない。

2)　ケーブル付き教示ペンダントは、ケーブルの長さが不十分なため、教示ポイントに行くために設備を越えていくことなどがないように、十分な長さのケーブルを持つことも必要である。またそのケーブルは、使用環境条件に耐えられるものでることが必要である。

3)　ケーブルレス及び取り外し可能な教示ペンダントは、操作中のロボットを特定できる手段、通信のインテグリティを確保する接続手段（例として、ログイン、暗号化、ファイヤーウォール）、接続中であることを示す明確な手段（例として、画面表示）を持たなければならない。通信が切れた場合には、制御されている全ての装置を保護停止または非常停止しなければならない。さらにこの後、通信の回復によって、意図的な操作なしに再起動できてはいけない。

ト　手動介入のためのリモートアクセス

1)　ロボットシステムが、物理的に離れた場所（離れた事務所など）にいるオペレータによって遠隔制御される場合、手動遠隔制御は、ロボットシステムが手動モードのときだけ可能で、いかなるときも局所または遠隔の 1 つの制御源だけが有効であること、即ち単一制御点でなければならない。

2)　手動遠隔制御を有効にする操作は、局所制御からだけで可能でなければならない。

3)　局所制御装置（制御盤、教示ペンダントなど）には、ロボットシステムが遠隔制御されていることを表示しなければならない。

表 2-3　安全防護で参照・適合を要求する規格一覧

規格番号	規格名称	対応 JIS
ISO 12100	Safety of machinery - General principles for design - Risk assessment and risk reduction 機械類の安全性－設計のための一般原則 －リスクアセスメント及びリスク低減	B 9700-1
ISO 13849-1	Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design 機械の安全性 — 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	B 9705-1
ISO 10218-1	Robots and robotic devices — Safety requirements for industrial robots — Part 1: robots ロボットおよびロボティックデバイス － 産業用ロボットのための安全要求事項 — 第 1 部：産業用ロボット	B 8433-1
ISO 13856-1	Safety of machinery — Pressure-sensitive protective devices — Part 1: General principles for design and testing of pressure-sensitive mats and pressure-sensitive floors 機械の安全性 —圧力検知保護装置 －第 1 部:圧力検知マット及び圧力検知フロアの設計及び試験のための一般原則	B 9717-1
ISO 13856-2	Safety of machinery — Pressure-sensitive protective devices — Part 2: General principles for the design and testing of pressure-sensitive edges and pressure-sensitive bars 機械の安全性 — 圧力検知保護装置 －第 2 部:圧力検知エッジ及び圧力検知バーの設計及び試験のための一般原則	
ISO 13856-3	Safety of machinery — Pressure-sensitive protective devices — Part 3: General principles for the design and testing of pressure-sensitive bumpers、 plates、 wires and similar devices 機械の安全性 — 圧力検知保護装置 －第 3 部 : 圧力検知バンパ、プレート、ワイヤ及び類似のデバイスの設計及び試験のための一般原則	
ISO 14119	Safety of machinery — Interlocking devices associated with guards — Principles for design and selection 機械の安全性 － ガードと共同するインタロック装置 －設計及び選択のための原則	B 9710

IEC 61496-1	Safety of machinery — Electro-sensitive protective equipment — Part 1: General requirements and tests 機械の安全性 － 電気的検知保護装置 －第 1 部：一般要求事項及び試験	B 9704-1
IEC/TS 62046	Safety of machinery — Application of protective equipment to detect the presence of persons 機械の安全性 — 人の存在を検出するための保護装置のアプリケーション	
ISO 13855	Safety of machinery — Positioning of safeguards with respect to the approach speeds of parts of the human body 機械の安全性 － 人体部位の接近速度に基づく安全防護物の位置決め	B 9715
ISO 13857	Safety of machinery — Safety distances to prevent hazard zones being reached by upper and lower limbs 機械の安全性 － 危険区域に上肢及び下肢が到達することを防止できる安全距離	B 9718
ISO 14120	Safety of machinery — Guards — General requirements for the design and construction of fixed and movable guards 機械の安全性 － ガード － 固定式及び可動式ガードの設計及び製作のための一般要求事項	B 9716

ナ 安全防護（Safeguarding）

1) 設計上でハザードを除去できない、又はハザードを適切に低減できない場合、安全防護を適用しなければならない。

2) 危険エリアへの接近は、ガードや保護装置などの安全防護装置で防がなければならない。

産業用協働ロボットを使用しても上記の除去できないハザードが存在する場合は、本項の要求事項に適合する必要がある。また本項を記載した ISO 102108-2（JIS B 8433-1）は、関連規格への適合を明示しているので、それらへの適合も必要になる。必要に応じて規格を参照戴きたい。本書は、産業用ロボット本体は安全規格適合品を使用することが前提であるため、以下の(ケ)ミューティングと(コ)安全防護装置の一時中断を除き要求事項の説明は割愛し、記述されている項目とともに、参照を指示している規格の一覧を表 2-3 に示す。

〈安全防護として達成が必要な項目〉

（ア） 周囲の安全防護

（イ） 最小安全距離

・ガードに対しての最小安全距離
・保護装置に対しての最小安全距離
・クリアランスを確保するための最小安全距離

（ウ） ガードに対する要求事項

・固定式の距離ガードに対する一般要求事項
・インタロック付き可動式ガードに対しての一般要求事項
・施錠式ガード付きの可動式ガードに対する一般要求事項
・安全防護空間内に進入を可能にする可動式ガード

(エ)　検知保護装置（Sensitive protective equipment）
・保護停止の始動に使用される検知保護装置
・起動防止のための存在検知を使用した検知保護装置
(オ)　手動ローディング／アンローディング又は手動ステーション）の安全防護方策
・動作中の手動ステーション
・共有作業空間のある手動ステーション
(カ)　材料等の搬送用の開口部の安全防護対策
(キ)　隣接する複数のロボットセルの安全防護
(ク)　工具交換システムの安全防護
(ケ)　ミューティング
(コ)　安全防護装置の一時中断

ニ　ミューティングへの要求事項

ミューティングは、ロボットシステムのサイクルというプロセスにおける安全防護機能の自動的に制御された一時休止である。ミューティング時は、人がハザードに晒されないようにし、ミューティング終了時は、人が危険区域で検出されないまま留まることがないようにしなければならない。

ヌ　安全防護物の一時中断への要求事項

1)安全防護物を一時中断することが必要なタスク（例えば、ロボットの教示）は、このタスクのためのリスクアセスメントで決定した適切な安全防護装置を自動的に選択する専用の運転モードを持たなければならない。
2)　この運転モードの選択は、前記イの 3）に適合しなければならない。。
3)　安全防護物の一時中断時は、自動運転の再開ができないこと、またそれを示す視覚的表示をモード選択装置、システムの入口、及び影響のある全ての操作ステーションに備えなければならない。

以上、述べた ISO 10218-2（JIS B 8433-2）の要求事項に適合した上で、以下に述べる産業用協働ロボットシステム固有の安全性要求事項に適合する必要がある。産業用協働ロボットシステムの安全性要求事項は、ISO/TS 15066:2016（JIS は作成中）に示されている。

５　ISO/TS 15066:2016 の要求事項

(1)　概要

協働ロボットシステムでは、ロボットのアクチュエータへ動力供給中に、オペレータが、安全柵などで作業空間が分断されることなく、ロボットシステムの近接で作業することができる[11]（図 2-7 参照）。そのため、オペレータとロボットシステムとの物理的接触が協働作業空間内で生じうるので、以下に述べる安全方策が必要になる。

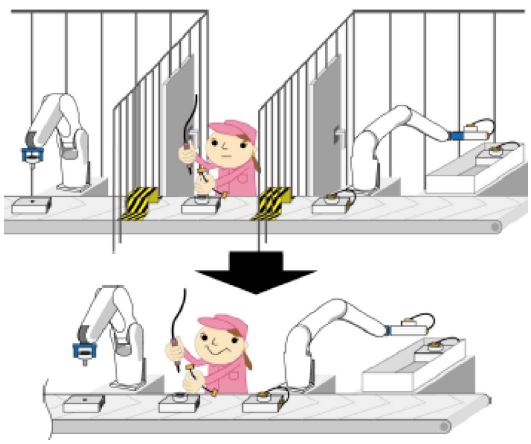


図 2-7　従来型ロボットから協働ロボットへ

(2) 共通要求事項

ISO/TS 15066 では、協働ロボットシステムとして基本的に備えなければならない共通安全方策と、システムを以下の 4 つに分類し、それらに必要な安全方策を規定している。

a) 安全適合監視停止 (Safety-rated monitor stop)
b) ハンドガイド (Hand guide)
c) 速度と分離の監視 (Speed and separation monitoring)
d) 動力と力の制限 (Power and force limiting)

これら 4 つのロボットシステムは、それぞれ単独とは限らず、複数を併せ持つ場合がある。

ア 使用する産業用協働ロボット

使用するロボットは、ISO 10218-1:2011 (JIS B 8433-1:2015) に適合し、使用するアプリケーケーション (上記 a)) に適合する能力を有することが必要である。例えば、ロボットが自動運転動作中に人との接触が発生する可能性あるアプリケーションの場合、上記 d)の動力と力の制限機能、または別の方法を用いて怪我を生じない動力と力以下であることを保証できなければならない。

イ 安全関連制御システムの性能

安全関連制御システムは、ISO 13849-1 (JIS B 9705-1)で規定するカテゴリ 3 及び PL=d、または IEC 62061 (JIS B 9961) で規定するプルーフテスト間隔が 20 年以上で、ハードウェアフォールトトレランスが 1 の SIL2 に適合していることが必要である。

ウ 保護方策

協働作業空間 (前記 2-2 項参照) 内の全ての人間が、保護されなければならない。協働作業空間内で使用される安全防護物 (人の侵入を検知するレーザーセンサなど) は、上記イの安全性能を持たなければならない。

エ 停止機能

1) 協働運転中、オペレータが、いかなる時でも単一動作でロボット動作を停止させるか (例えば、イネーブル装置や非常停止装置の使用)、又は協働作業空間から障害なく退出する方策のどちらかを持たなければならない。
2) 非常停止装置の数と位置は、リスクアセスメントによって決定する。

オ 非協働運転と協働運転間の移行

協働運転のアプリケーション間 (前述の a) ～d))、及び非協働運転と協働運転間の移行は、安全上、協働アプリケーションにおいて重要な部分である。これらの移行中にオペレータに対して、許容できないリスクが発生しないように設計されなければならない。協働運転と非協働運転間の移行を識別するために、視覚的な表示器の使用が有効である。

(3) アプリケーションへの要求事項

ア 安全適合監視停止への要求事項

① ロボット動作が制限されるとき,その制限は ISO 10218-1:2011 (JIS B 8433-1:2015) の **5.12 (協働ロボットへの要求事項)** に適合しなければならない。
② ロボットは、ISO 10218-1:2011 の 5.5.3 (前記 3 のイの 4)) に従って,ロボットは保護停止を達成する機能を備えなければならない。
③ 協働作業空間は、ISO 13855 (JIS B 9715) の要求事項に適合する距離を保証し

なければならない。

安全適合監視停止（前記 2 節参照）アプリケーションでは、オペレータが、ロボットシステムと相互作用し、タスク（例えば、ワークをエンドエフェクタに着脱する）を遂行するために、協働作業空間に進入する前に、安全適合監視停止のロボット機能が協働作業空間内のロボット動作を中止する。協働作業空間内にオペレータが存在しない場合、ロボットは非協働運転（所謂、従来型ロボットとしての稼働）を行ってもよい。ロボットシステムが協働作業空間内で、安全適合監視機能が有効、かつ、ロボット動作が停止中であれば、オペレータは協働作業空間へ進入することができる。オペレータが協働作業空間から退出した後にのみ、ロボットシステム動作は、なんらの追加介入なく再開できる（図 2-8、表 2-4 参照）。

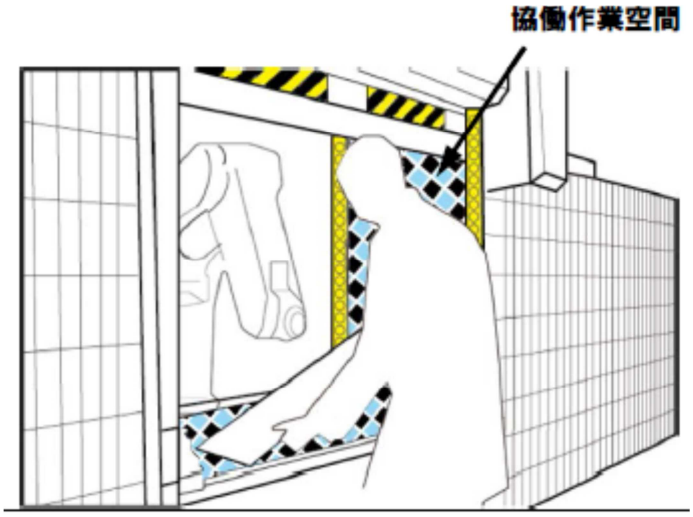


図 2-8　安全適合監視停止システム

表 2-4　ロボットと人の位置との関係によるロボット動作継続／停止

人の位置 ロボットの位置と動作	協働作業空間の外側	協働作業空間の内側
協働作業空間の外側	継続	継続
協働作業空間の内側、かつ動作中	継続	保護停止
協働作業空間の内側、かつ 安全適合停止監視停止中	継続	継続

イ　ハンドガイド

① ロボットシステムがハンドガイド状態になる前に、オペレータが協働作業空間に進入した場合、保護停止が起動しなければならない。

② リスクアセスメントに基づき、人が協働作業空間外の制限空間へアクセスできてはいけない。

③ 本アプリケーションで使用する産業用協働ロボットは、ISO 10218-1（JIS B 8433-1）で規定の安全適合監視速度機能と安全適合監視停止機能を備えていなければならない。

④ 手動操作装置は、

- ISO 10218-1（JIS B8433-1）に適合した非常停止とイネーブル装置を有する。

● ロボット動作及びロボット動作から生じる全ての危険源（例：エンドエフェクタに搭載された制御装置）を直接監視できるように配置されている、
● 使用時のオペレータの位置及び姿勢が更なるハザードを招かない（例：オペレータが重量物の下又はマニプレータアームの下等に位置しない）。
● オペレータが遮るものなく協働作業空間全体を視認できる（例：協働作業空間に進入するオペレータ自身以外の人々）。
を達成できるように配置しなければならない。

⑤ ハンドガイドから非協働運転への移行するとき、ロボットシステムが非協働運転を開始する前に、全ての人が協働作業空間から退出していることを保証しなければならない。

このアプリケーションでは、オペレータはロボットシステムへ動作命令を伝達するために手動操作装置を使用する。オペレータが協働作業空間へ進入することが許可され、ハンドガイドを用いたタスクを行う前に、ロボットは安全適合監視停止を遂行する。タスクは、ロボットエンドエフェクタ、又はその近くにあるガイド装置を手動で作動することによって実行できる（図 2-9 参照）。

産業用協働ロボットが後述する“d”「動力と力の制限」の機能を有し、リスクアセスメントで危険が生じないと確認できた場合、上述の手動操作装置を使用せずに、ハンドガイドを行ってもよい。

図 2-9　ハンドガイド

ウ　速度と間隔の監視

① 本アプリケーションで使用する産業用協働ロボットは、ISO 10218-1（JIS B 8433-1）で規定の安全適合監視速度機能と安全適合監視停止機能を備えていなければならない。

② オペレータの安全がロボットの動作範囲の制限に依存する場合、使用する産業用協働ロボットは、ISO 10218-1（JIS B 8433-1）で規定の安全適合ソフト軸[*7]、及び安全適合空間制限[*8]の機能を有することが必要で、それを用いてロボットの動作範囲を制限しなければならない。

③ このアプリケーションでは、ロボットシステム及びオペレータは、同時に協働作業空間内で作業してもよいが、オペレータとロボット間の保護分離距離[*6]を常に維持しなければならない。ロボット動作中に、ロボットシステムは、決して保護分離距離以上にオペレータに近づかない。

④ 速度と分離監視は、協働作業空間内の全ての人間に適用し、監視人数が制限され、その最大値を超える場合、保護停止が始動しなければならない。監視できる最大人数が使用上の情報に記載されなければならない。

分離距離（具体的には、ロボットの各部、エンドエフェクタ、ワーク、ロボットに取付けられた配線などの様々な機器やその取付具と人との間の距離）が、保護分

離距離よりも低い値まで低減したとき、ロボットシステムは、停止する。オペレータがロボットシステムから離れると、ロボットシステムは保護分離距離を最低限維持しながら自動的に動作を再開できる。ロボットシステムが減速すると、保護分離距離はそれに見合って減少する（図 2-10 参照）。

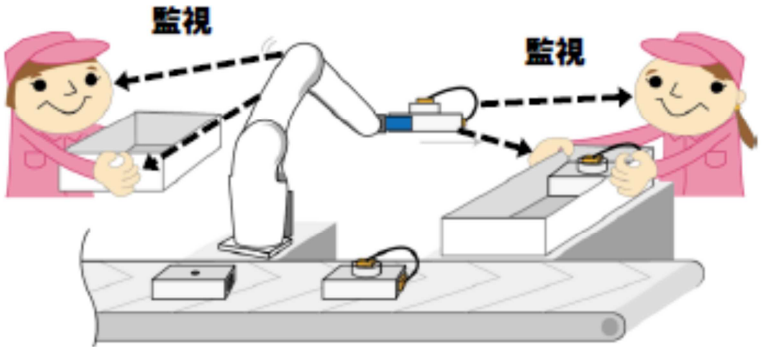


図 2-10　速度と分離の監視

【注記】

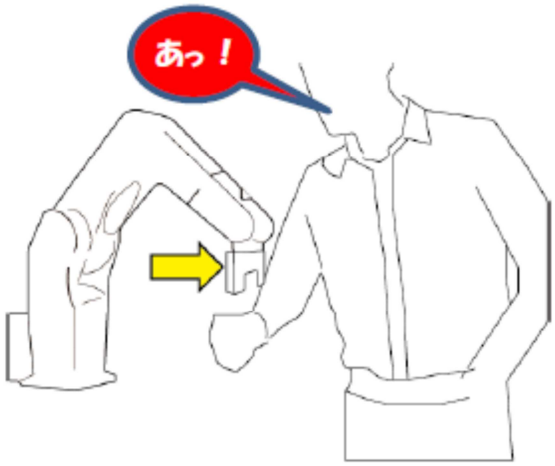
*6：協働作業空間内において、ロボットシステムのあらゆる移動危険部と人間との間で、最短の許容可能な距離。

*7：規定された十分な安全適合性能をもつソフトウェア又はファームウェアを基にしたシステムによって、ロボットの動作範囲に設置された制限。

*8：安全適合ソフト軸によって設定・制限された空間。包含する区域、又は除外区域となる幾何学的形状を定義し、定義された空間内でロボット動作を制限する、又はロボットが定義された空間内へ進入することを防ぐことができる。

エ　動力と力の制限

このアプリケーションでは、ロボットシステム（ワークピースを含む）とオペレータ間の物理的接触は、意図的、又は非意図的の両面から生じうる。そのため、特別に設計されたロボットシステムが必要になる。リスク低減は、本質的安全手段又は、安全関連制御システムを通じてロボットシステムに関連するハザードをリスクアセスメントで決定した限界値(しきい値)以下に保つことで達成される。(図 2-11 参照)。



痛みまたは AIS 1 未満の極めて軽微な怪我を生じる

図 2-11　動力と力の制限

(ア) 使用する産業用協働ロボット

本アプリケーションで使用できる産業用協働ロボットは、スクアセスメントに基づき,準静的接触及び過渡的接触に対する適切な限界値を超えないことによって,オペレータに対して適切にリスクを低減するように設計されなければならない。附属書 A が,どのように限界値が決定されうるかを提供する。

従って、ロボットは ISO 10218-1:2011（JIS B 8433-1)、及び ISO/TS 15066:2016（JIS 制定作業中）とその附属書 A に示される閾値以下であることが重要である。さらに産業用ロボットメーカが保証した動力と力の制御の内容を精査し、導入するロボットシステムの使用条件を保証しているかの検証が必要になる。システムでの使用条件の保証が産業用ロボットメーカから得られない場合は、システムインテグレータ、及び／又はユーザは、附属書 A への適合評価を自ら実施する必要がある。

(イ) ISO/TS 15066:2016 附属書 A

産業用協働ロボットのあらゆる部分、ロボットに取り付けられたあらゆる附属品、エンドエフェクタ、ワークなどのロボットの可動によって人に接触する可能性のある全てのポイントと、そのポイントが接触する可能性のある人体のあらゆる部分に対して、ISO/TS 15066 の表 A.2 で示された「生物力学的限界」以下でなければならない。この表 A.2 とこれに関する図表をまとめたものを表 2-5 と図 2-12 に示す。

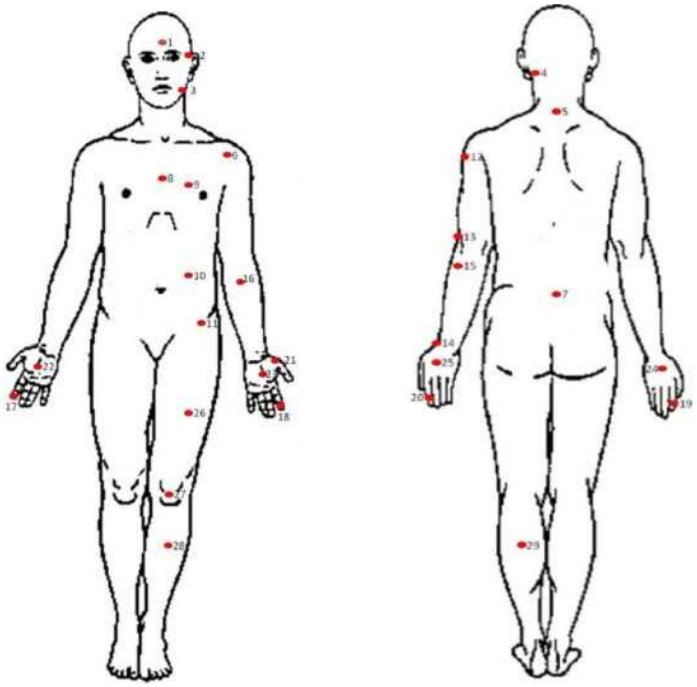


図 2-12　表 2-5 に示す人体部位

表 2－5　生体力学的限界値

身体領域	特定身体領域		準静的接触		過渡的接触	
			最大容認圧力[a] p_S N/cm^2	最大容認力[b] F_S N	最大容認圧力の乗数[c] P_T	最大容認力の乗数[c] F_T
頭蓋骨及び額[d]	*1*	*額の中央*	*130*	*130*	*NA*	*NA*
	2	*こめかみ*	*110*		*NA*	
顔[d]	*3*	*そしゃく筋*	*110*	*65*	*NA*	*NA*
首	4	頚筋	140	150	2	2
	5	第七頚椎骨	210		2	
背及び肩	6	肩関節	160	210	2	2
	7	第五腰椎	210		2	2
胸	8	胸骨	120	140	2	2
	9	胸筋	170		2	
腹部	10	腹筋	140	110	2	2
骨盤	11	骨盤骨	210	180	2	2
上腕及び肘関節	12	三角筋	190	150	2	2
	13	上腕骨	220		2	
前腕及び手首関節	14	橈骨	190	160	2	2
	15	前腕筋	180		2	
	16	腕神経	180		2	
手及び指	17	人差し指腹　D	300	140	2	2
	18	人差し指腹　ND	270		2	
	19	人差し指関節　D	280		2	
	20	人差し指関節　ND	220		2	
	21	母指球	200		2	
	22	手のひら　D	260		2	
	23	手のひら　ND	260		2	
	24	手の裏側　D	200		2	
	25	手の裏側　ND	190		2	
大腿部及び膝	26	大腿筋	250	220	2	2
	27	膝頭	220		2	
下腿部	28	向こう脛	220	130	2	2
	29	ふくらはぎ筋(腓筋)	210		2	
D:利き手、ND:反利き手						

表 2-5 に示す閾値は、1.4×1.4 mm の正方形で４辺の全てで半径 2 mm の丸みをもつ接触試験子を使用したときに与えられるもので、実際の協働ロボットシステムでは、実際の接触状況に合わせた評価が必要になる。表 2-5 中の頭部／額／顔への接触は許されない。

また計測に用いる計測器は、国際試験所認定協力機構（ILAC）が認定し、かつ認定保証期間内のものを使用する必要がある。

ロボットのある部分が身体のある部分に接触すると、力と圧力は、図 2-11 で示すように時間的変動する。従って、静的制限値と過渡的制限値の両面において、閾値を超えないことを保証する必要がある。

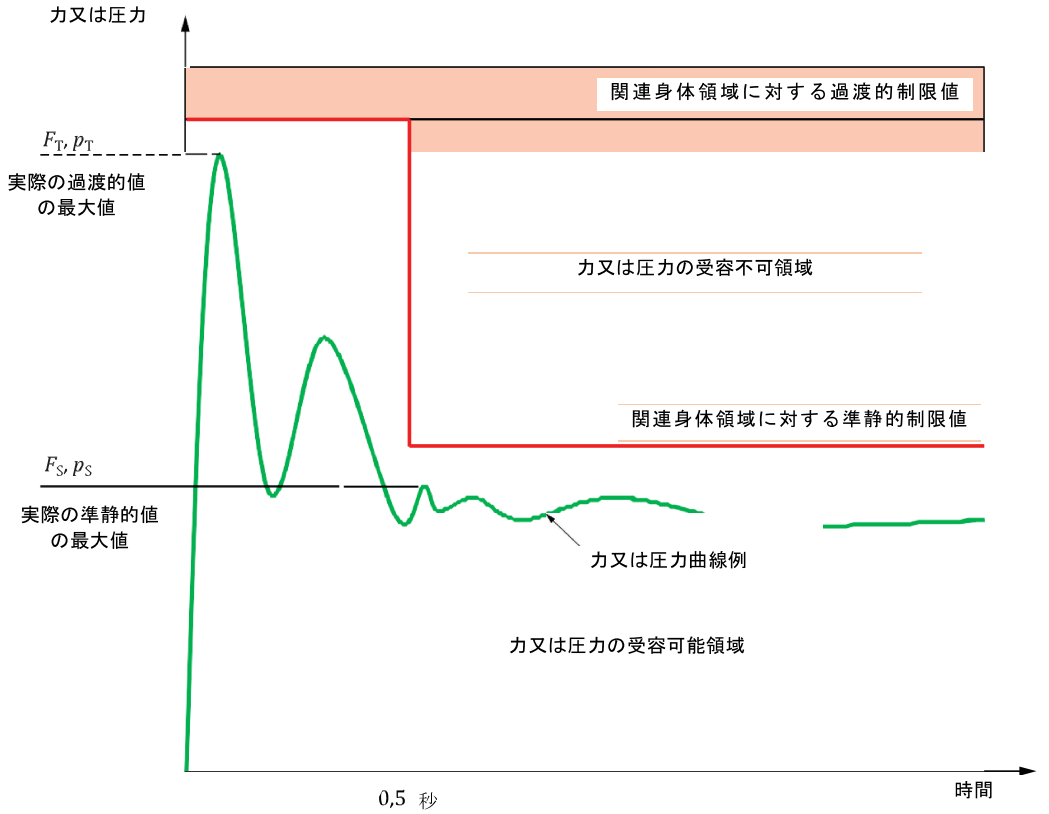


図 2-11　力／圧力の時間的経緯

ロボットが身体に接触すると、人体はロボットの動きに押されて一体となって移動する。即ち、過渡的接触時、ロボットから人に接触面を通じて達成されるエネルギーが、人体に痛み・ダメージ・怪我を生じさせる。従って、衝突時の伝達エネルギーが許容値を超えないことが必要である。この伝達エネルギーは、人体各部の柔らかさの違いにより変化する。伝達エネルギー許容値例を表 2-6 に示す。

表 2-6　伝達エネルギー許容値の例

身体領域	伝達エネルギー E（J）	身体領域	伝達エネルギー E（J）
頭部／額	0.23	骨盤	2.6
顔	0.11	上腕／肘関節	1.5
首	0.84	下腕／手首関節	1.3
背中／肩	2.5	手／指	0.49
胸	1.6	大腿／膝	1.9
腹	2.4	下腿	0.52

表 2-7 に面積 1 cm^2 当たりの最大圧力値に基づくロボット有効質量の作用としての過渡的接触速度制限値の例を示す。

表 2-7　過渡的接触速度制限値の例（mm/s）

有効質量 (kg) / 身体領域	1	2	5	10	15	20
手／指	2 400	2 200	2 000	2 000	2 000	1 900
前腕	2 200	1 800	1 500	1 400	1 400	1 300
上腕	2 400	1 900	1 500	1 400	1 300	1 300
腹	2 900	2 100	1 400	1 000	870	780
骨盤	2 700	1 900	1 300	930	800	720
大腿	2 000	1 400	920	670	560	500
下腿	1 700	1 200	800	580	490	440
肩	1 700	1 200	790	590	500	450
胸	1 500	1 100	700	520	440	400

6　ISO 13849-1:2006（JIS B 9705-1:2011）の要求事項

(1)　概要

ISO 10218-1:2011（JIS B 8433-1:2015）及び ISO 10218-2（JIS B 8433-2)は、直接、間接的に随所で ISO 13849-1:2006（JIS B 9705-1:2011）の参照・適合を要求している。そこで ISO 13849-1:2006 の概要を説明する。

ISO 10218-2:2011 は、参照規格を ISO 13849-1 とせず、ISO 13849-1:2006 としている。これは ISO 10218-2:2011 の発行後に ISO 13849-1 が改定された結果、ISO 13849-1 の改定要求事項が ISO 10218-2:2011 の要求事項と整合性が取れなくなるなどの不都合な箇所が発生することを防止するためである。

尚、ISO 10218-1:2006 は既に失効し、現有効規格は 2015 年に発行された ISO 13849-1:2015 になっている。しかし、ISO 10218-1 及び ISO 10218-2 が参照する内容においては、ほぼ影響を受けていない。

(2)　適用範囲

ソフトウェアの設計を含み、制御システムの安全関連部（SRP/CS）*1 の設計及び統合のための原則に関する安全要求事項及び指針、及び安全機能を実行するために要求されるパフォーマンスレベルを含む特性を規定している。

【注記】

*1：SRP/CS＝Safety-Related Parts of a Control System は、ISO 13849-1:2006 の 3.1.1 で以下のように定義。
安全関連入力信号に応答し、安全関連出力信号を生成する制御システムの部分。
尚、この定義は、現有効規格 ISO 13849-1:2015 でも同じである。

(3)　パフォーマンスレベル

SRP/CS は、要求のリスク低減を達成する安全機能を PL として提供する。設計の本質的な安全部分として、又は安全防護物若しくは保護装置の制御部分として安全機能を提供する際、SRP/CS の設計はリスク低減の方法論の一部である（表 2-8 参照)。

表 2-8　パフォーマンスレベル（PL）

PL	単位時間当たりの危険側故障発生の平均確率（PFHd）[1/h]
a	$10^{-5} \leqq PFHd < 10^{-4}$
b	$3 \times 10^{-6} \leqq PFHd < 10^{-5}$
c	$10^{-6} \leqq PFHd < 3 \times 10^{-6}$
d	$10^{-7} \leqq PFHd < 10^{-6}$
e	$10^{-8} \leqq PFHd < 10^{-7}$

このパフォーマンスレベル PL と IEC 62061（JIS B 9961）で規定の安全インテグリティ SIL 間の関係を表 2-9 に示す。

表 2-9　PL と SIL の関係

PL	SIL
a	-
b	1
c	2
d	3
e	4

(4)　カテゴリ

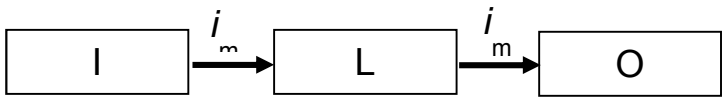
達成した PL の査定を容易にするために、指定の設計基準及び障害条件下での指定の挙動に従った構造分類「カテゴリ」に振り分ける。

ア　カテゴリ B

制御システムの安全関連部は、最小限、関連規格に従い、かつ、次の事項に対して抵抗性をもてるように特定の用途のための基本安全原則を用いて、設計、製造、選択、組立及び結合されなければならない（図 2-12 参照）。

- 予想される操作のストレス、例えば、遮断容量及び頻度に関する信頼性
- 加工材料の影響、例えば、洗浄機の洗剤
- 他の関連する外部影響、例えば、機械的振動、電磁干渉、動力供給の中断又は妨害

カテゴリ B のシステム内では診断範囲がなく（DCavg＝0 %）、かつ、各チャネルの MTTFd は、“低”～“中”までとなる。



i_m　相互接続手段
I　　入力機器（例えばセンサー）
L　　論理
O　　出力機器（例えば接触器）

図 2-12　カテゴリ B のアーキテクチャ

イ　カテゴリ１

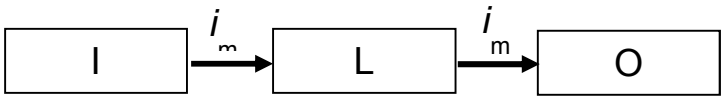
カテゴリ B の要求事項に追加して次を適用する（図 2-13 参照）。

カテゴリ 1 の SRP/CS は、“十分吟味された”コンポーネント及び“十分吟味された”安全原則を用いて設計及び製作しなければならない（ISO 13849-2 参照）。

安全関連への適用のために“十分吟味された”コンポーネントは、次のいずれかのコンポーネントである。

a）類似のアプリケーションにおいて好結果で過去に広く使用された。

b）安全関連へのアプリケーションに対して適切性及び信頼性を論証するための原則を用いて製作され、かつ、検証された。



i_m　相互接続手段
I　　入力機器（例えばセンサー）
L　　論理
O　　出力機器（例えば接触器）

図 2-13　カテゴリ 1 のアーキテクチャ

ウ　カテゴリ２

カテゴリ B 及び十分吟味された安全原則に従うことに追加して、次を適用する（図 2-14 参照）。

その機能を機械制御システムによって、適切な間隔でチェックするように設計しなければならない。安全機能のチェックは、次で遂行しなければならない。

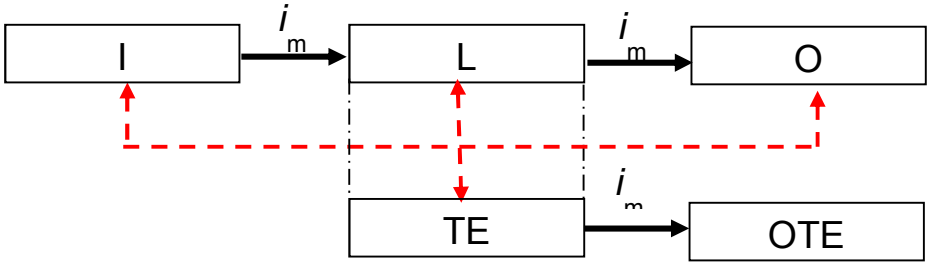
－ 機械の起動時、及び

－ 危険状態の始まる前、例えば、新たなサイクルの起動、他の動きの起動、及び／又はリスクアセスメント及び運転の種類によって必要とする場合で、運転中、定期的に。

このチェックの始動は、自動的である場合がある。安全機能の全てのチェックは、次のいずれかでなければならない。

－ 障害が検出されない場合には、運転を許可する。又は

－ 障害が検出された場合には、適切な制御動作を始動するために出力信号を発生する。



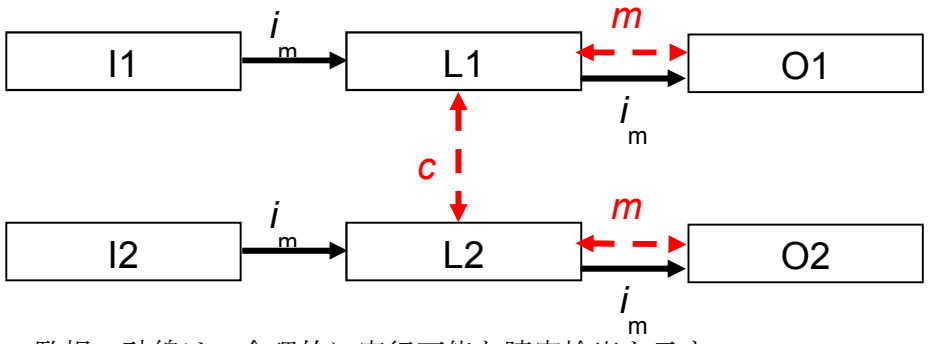
i_m　相互接続手段
I　　入力機器（例えばセンサー）
L　　論理
m　　監視
O　　出力装置機器（例えば接触器）
TE　試験装置
OTE　TE の出力

図 2-14　カテゴリ 2 のアーキテクチャ

エ　カテゴリ３

カテゴリ B に準じた同様の要求事項と十分吟味された安全原則に従うことに加えて、次を適用する（図 2-15 参照）。

カテゴリ 3 の SRP/CS は、そのいずれの部分に単一障害が生じても、それが安全機能の喪失につながらないように設計しなければならない。合理的に実施可能な場合はいつでも、単一障害は、安全機能の次の動作要求時、又はそれ以前に検出されなければならない。障害検出を含む全 SRP/CS の診断範囲（DCavg）は、“低”又は“中”でなければならない。冗長チャネルの各々の MTTFd は、PLr によって、“低”～“高”までででなければならない。CCF に対する方策を適用しなければならない。



監視の破線は、合理的に実行可能な障害検出を示す

i_m　　相互接続手段

c　　相互監視

I1　I2　　入力機器（例えばセンサー）

L1　L2　　論理

m　　監視

O1　O2　出力機器（例えば主接触器）

図 2-15　カテゴリ 3 のアーキテクチャ

オ　カテゴリ４

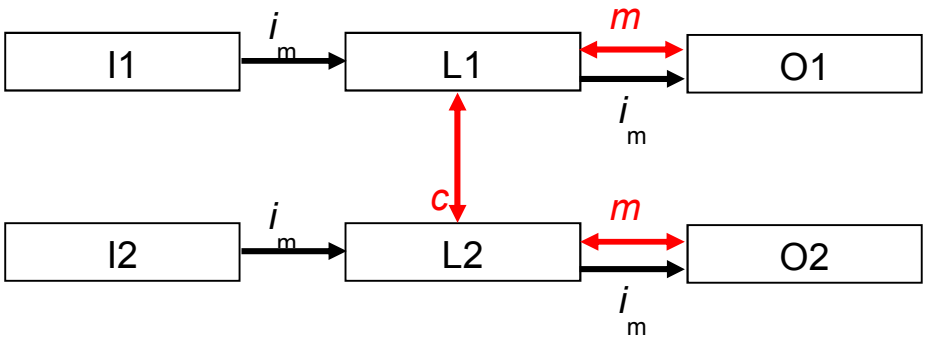
カテゴリ B 及び十分吟味された安全原則に従うことに加えて次を適用する（図 2-16 参照）。

カテゴリ 4 の SRP/CS は、次のように設計しなければならない。

－ 安全関連部のいずれにおいても単一障害は、安全機能の喪失につながらない。かつ、

－ その単一障害は、安全機能の次の動作要求時、又はそれ以前であって、例えば、直ちに、始動時、又は機械の運転サイクルの終了時に検出される。

カテゴリ 4 の監視はカテゴリ 3 より診断範囲が高く勝つ各チャンネルの MTTFd は「高」でなければならない。



監視の実線は、カテゴリ 3 より高い診断範囲を示す
i_m　相互接続手段
c　相互監視
I1　I2　入力機器（例えばセンサー）
L1　L2　論理
m　監視
O1　O2　出力機器（例えば主接触器）

図 2-16　カテゴリ 4 のアーキテクチャ

(5)　平均危険側故障時間（MTTFd）

各チャネルの MTTFd 値は、3 通りのレベルで示される（表 2-17 参照）。また、各チャネル（例えば、単一チャネル、冗長システムの各チャネル）を個別に考慮しなければならない。MTTFd では、100 年の最大値を考慮しなければならない。

表 2-17　平均危険側故障時間（MTTFd）

各チャンネルの指定表示	各チャンネルの範囲
低	3 年≦MTTFd＜10 年
中	10 年≦MTTFd＜30 年
高	30 年≦MTTFd＜100 年

(6)　診断範囲

DC 値は、表 2-18 に示す 4 通りのレベルで示される。DC の見積りは、ISO 13849-1:2006（JIS B 9705-1:2011）の付属書 E を参照する。

表 2-18　診断範囲

DC の指定表示	DC の範囲
なし	DC＜60 %
低	60 %≦DC＜90 %
中	90 %≦DC＜99 %
高	99 %≦DC

(7) PL の算出

カテゴリと PL、DC、MTTFd との関係は図 2-19 で示される。

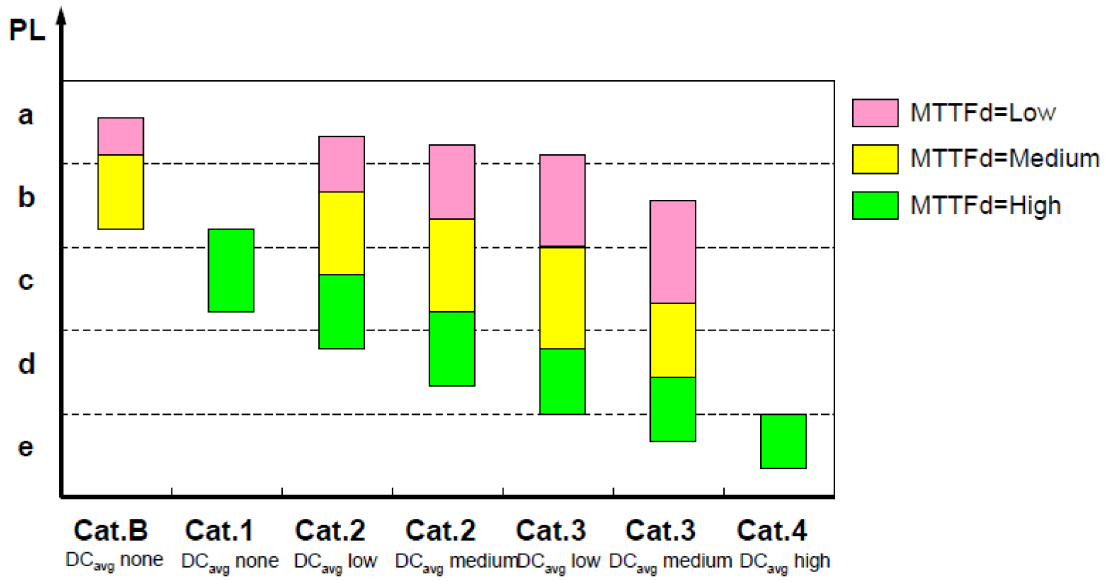


図 2-19　カテゴリと PL、DC、MTTFd の関係

7　IEC 62061:2005（JIS B 9961:2008）の要求事項

(1) 概要

ISO 10218-1:2011（JIS B 8433-1:2015）及び ISO 10218-2（JIS B 8433-2)は、ISO 13849-1:2006（JIS B 9705-1:2011）と同様に、直接、間接的に随所で IEC 62061:2005（JIS B 9961:2008）を参照している。

IEC 62061:2005 は、IEC 61508（JIS C 0508）シリーズをもとに、機械の安全関連システム(本規格では、以降 SRECS（safety-related electrical control system)という。)の設計、統合及び妥当性確認のための要求事項及び推奨事項を規定している。IEC 62061:2005 は,作動中には手で持ち運べない機械(協調して稼動する機械群を含む。)に、安全機能を単独又は組み合わせて実行する制御システムに適用する。

(2) 安全度水準（SIL）

SRECS は、PFH_D（Probability of dangerous failure per hour＝1 時間の間に危険側故障を起こす平均確率）によって分類される。安全度水準の詳細は、テキストの付録を参照。IEC 62061:2005 は、表 2-19 に示すように、IEC 61508 シリーズで規定の SIL4 まで規定していない。

表 2-19　安全度水準を定義する PFH_D

安全度水準	PFH_D
SIL 3	$10^{-8} \leqq PFHD < 10^{-7}$
SIL 2	$10^{-7} \leqq PFHD < 10^{-6}$
SIL 1	$10^{-6} \leqq PFHD < 10^{-5}$

(3) フォールトトレランス

フォールトトレランス（Fault Tolerance）は、安全関連電気制御システム,サブシステム,又はサブシステム要素が,フォールト又は故障が存在する状況で要求機能の実行を継続できる能力を示す。ISO 10218-1:2011（JIS B 8433-1:2015）及び ISO 10218-2（JIS B 8433-2)は、原則、1 を要求している。

(4) プルーフテスト間隔

プルーフテスト間隔は、診断によって検出できない危険側フォールトを見つけるために行うテストの間隔を示す。ISO 10218-1:2011（JIS B 8433-1:2015）及び ISO 10218-2（JIS B 8433-2)は、ロボット及びロボットシステムが長期間使用されることを考慮して、20 年以上としている。

.

参照文献

[1] ISO 10218-1:2011 “Robots and robotic devices ― Safety requirements for industrial robots ― Part 1: Robots”

[2] JIS B 8433-1:2015“ロボット及びロボティックデバイス－産業用ロボットのための安全要求事項－第 1 部：ロボット”

[3] ISO 10218-2:2011“Robots and robotic devices ― Safety requirements for industrial robots ― Part 2: Robot systems and integration

[4] JIS B 8433-2:2015“ロボット及びロボティックデバイス－産業用ロボットのための安全要求事項－第 2 部：ロボットシステム及びインテグレーション”

[5] ISO/TS 15066:2016“Robots and robotic devices ―Collaborative robots”

[6] 日本工業標準調査会ホームページ
https://www.jisc.go.jp/international/iec-prcs.html（2016 年 9 月 20 日閲覧）

[7] 経済産業ジャーナル 2014 年 10・11 月号 p.9、経済産業省

[8] 門脇 敏・福田 隆文・橋本 秀一・大賀 公二・深津 敦：安全工学最前線―システム安全の考え方、pp.49-100、日本機械学会編、共立出版

[9] ISO 12100“Safety of machinery - General principles for design - Risk assessment and risk reduction ”

[10] JIS B 9700“機械類の安全性―設計のための一般原則－リスクアセスメント及びリスク低減”

[11] 橋本秀一：国際規格に基づく協働ロボットシステムの安全、機械設計 2015 年 12 月号 Vol.59 No.12、pp.41-47、日刊工業新聞社

[12] ISO 13849-1:2006“Safety of machinery - Safety-related parts of control

systems - Part 1: General principles for design”
[13] ISO 13849-1:2015 “Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design”
[14] JIS B 9705-1:2011 “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”
[15] 井上洋一・川池襄・平尾祐司・蓬原弘一：安全の国際規格－制御システムの安全、日本規格協会

第３章　リスクアセスメントとリスク低減

１　　リスクアセスメント

(1)　機械の使用制限

ア　機械仕様

ロボットはエンドエフェクタや周辺装置を組み合わせた「ロボットシステム」として構成され様々な用途で使われる。エンドエフェクタはその用途により様々であり、例えば、塗装であればスプレーガン、スポット溶接であれば溶接ガン、製品の搬送であれば把持機構を備えたエンドエフェクタがロボットに装着される。近年では、単一のタスクだけでなく、複数のタスクを行わせるために、複数の機能を持つエンドエフェクタが装着されたロボットも多く導入されている。例えば、溶接ガンと把持機構を備えたエンドエフェクタをロボットに装着することにより、溶接作業だけでなく、溶接作業後に次の工程へ製品を搬送するロボットなどである。

また、ロボットはエンドエフェクタの組み合わせだけでなく、製品の受け渡しをする等の周辺装置と組み合わせて使用される。周辺装置は、機械装置を持たない単純な受け台から、複雑な機構を備えた装置、いわゆる治具と呼ばれる機械装置と組み合わせて使用されたり、工作機械への製品の着脱やコンベア上を流れる製品に対して作業を行ったりこれまでは人が作業を行っていた機械と組み合わせて使用される。さらに、ロボットは、ティーチにより軌跡を含めた動きや速度を自由に設定できるのが最大の特徴である。

ロボットのリスクアセスメントでは、ロボット本体の仕様等だけでなく、エンドエフェクタや周辺装置、更にはティーチによる動作を含めロボットシステムとしての仕様確認が必要である。ロボットシステムのリスクアセスメントにおける機械仕様の具体的確認事項を以下に示す。

（ア）　ロボットシステムの仕様

ロボットシステム全体の具体的確認事項の例を表 3-1 に示す。

表 3-1 ロボットシステムにおける確認すべき仕様

工程概要	ロボットを含む各装置類の配置 製品・材料の流れ 加工・作業内容、加工時の副生物・放出物(フューム、アーク光、熱、音、電磁波、放射性物質)・廃材などの性状・性質・量 タクトタイム、サイクルタイム 稼働時間(日／月／年)、生産台数(時間／日／年) 周辺装置・他の機械や建屋の壁・柱等との距離・空間

（イ）　ロボット本体の仕様

ロボット本体の具体的確認事項の例を表 3-2 に示す。

表 3-2 ロボット本体の確認すべき仕様

大きさ、形状、機構	ロボット全体の大きさ、軸数、垂直／水平多関節 残留エネルギの有無と種類(残圧やスプリングバランサ等)
駆動源・機構	モータ／気圧／油圧他、メカ構造・機構
質量・重心・モーメント	ロボット本体、エンドエフェクタを全体質量 姿勢による重心位置の変化、特に梱包・搬送時の姿勢での重心位置、エンドエフェクタや製品モーメント
最大可動範囲	ロボット本体＋エンドエフェクタを含めた範囲(ロボット自体が移動する場合、その移動範囲を含める)
最大可搬重量	ロボット全体、エンドエフェクタ
最大動作速度	エンドエフェクタを含めた動作速度
設置方法	床起き／天吊り／壁設置 等

（ウ） エンドエフェクタの仕様

エンドエフェクタの具体的確認事項の例を表 3-に示す。

表 3-3 エンドエフェクタの確認すべき仕様

大きさ、形状	大きさ、形状、ロボットへの取り付け位置
重量、重心	重量、重心位置、ロボット本体への装着時の重心のオフセット位置
駆動源・機構	エネルギの種類、アクチュエータ(モータ／シリンダ等)、機構、残留エネルギ有無と種類

（エ） 周辺装置の仕様

ロボットシステム内の周辺装置の具体的確認事項の例を表 3-に示す。

表 3-4 治具・周辺装置の確認すべき仕様

大きさ、形状、	大きさ、形状
重量、重心	装置重量、重心位置
形状	ロボット全体
駆動源・機構	モータ／気圧／油圧他、構造

（オ） 動作の仕様

ロボットシステムにて確認すべき動作仕様の例を表 3-に示す。なお、動作仕様は生産、段取り等すべての作業における動作について確認する必要がある。

表 3-5 確認すべき動作仕様

軌跡	動作軌跡
速度	エンドエフェクタを含めた最大遠位部の速度
待機位置・姿勢	作業待ちの位置や姿勢、複数の位置・姿勢が設定される場合もあり
起動・停止条件	ロボットの起動・再起動・途中起動・停止・一時停止条件

（カ） 製品、材料仕様

ロボットシステムの製品・材料の具体的確認事項の例を表 3-6 に示す。

表 3-6 確認すべき製品・材料の仕様

製品	性状(個体／液体／気体／紛体)、性質(特に健康有害性)、形状、重量、重心
材料	塗料や接着剤等エンドエフェクタや周辺装置で処理される材料の性状、性質、形状、量、 容器を用いる場合は容器の形状、質量
副資材	加工油や洗浄剤等副資材の性状、性質、形状、量 前工程からの残留物質(製品に塗布された防錆油など)
副産物	加工時の副産物・放出物(フューム、アーク光、熱、音、電磁波、放射性物質)

イ 使用条件

ロボットシステムが使用される場所や周辺の物理的環境やロボットシステムに係る人の制限の確認を行う。

（ア） 使用条件

ロボットシステムの使用条件の具体的確認事項の例を表 3-7 に示す。

表 3-7 確認すべき使用条件

周辺環境	温度、湿度、粉塵(種類・濃度)、騒音、電磁波環境、風雨影響等
空間的条件	構造物や他の装置との距離、据付時に必要な作業空間、搬入経路上のスペース等
関係者	機械のライフサイクル各フェーズで係る人の経験・能力 第3者関与の可能性と性質

(2) 危険源・危険状態・危険事象の同定

ア 危険源の同定

（ア） ロボットシステムの危険源の同定

機械の使用制限において確認されたエンドエフェクタを含めたロボット本体や各装置を含めたロボットシステムの危険源を同定する。ロボットシステムの危険源には、ロボット単体等のリスクも取り込む必要があり、ロボットや購入した装置の取扱説明書等の確認が必要となる。

ロボットシステムにおける危険源の例を表 3-8 に示す。

表 3-8 ロボットシステムの危険源の例

No	種類	危険源の例	
		原因	潜在的結果
1	機械的危険源	- ロボットセルに於ける，ロボットアーム（背面を含む）全ての部分、エンドエフェクタ又は可動部の移動 - 外部軸（サービス位置でのエンドエフェクタ工具を含む）の移動 - エンドエフェクタ上又は外部軸上の，ハンドリング中の部品及び連携している設備上の鋭利な工具の移動又は回転 - すべてのロボット軸の回転動作 - 材料または製品の落下又は放出 - エンドエフェクタの故障（分離） - だぶだぶの衣服、長い髪 - ロボットアームと全ての固定物の間 - エンドエフェクタと全ての固定物（柵、はり（梁）など）との間 - 取付具の間（落下）：シャトルの間、ユーティリティ - 自動モード中に閉じ込められたオペレータのために準備されている（セル用扉を使っての）ロボットセルからの脱出ができない状態 - ジグ又は把持具の意図しない移動 - ツールの予期しない開放 - ハンドリング中の機械又はロボットセル部分の意図しない移動 - エンドエフェクタ又は関連設備の意図しない動作又は起動（ロボットで制御された外部軸、丸と（砥）石などのプロセスに特有のものなど） - 蓄積された動力源からの潜在的エネ	- 押しつぶし - せん断 - 切傷又は切断 - 巻込み - 引込み又は捕捉 - 衝撃 - 突刺し又は突き通し - こすれ，擦り傷 - 高圧流体／ガスの注入又は噴出

表 3-8 ロボットシステムの危険源の例

No	種類	危険源の例	
		原因	潜在的結果
		ルギの予期しない放出	
2	電気的危険源	- 充電部又は接続部への接触（電気キャビネット、端子箱、機械の制御盤） - システム，電気キャビネット及び端子部分の様々な電圧の取り違え，すなわち，動力電圧と制御電圧（110V と 24V) - 電気的（電子的）回路内の個々の部品への接触。例えば，コンデンサ - アークフラッシュへの暴露 - 高電圧又は高周波を使用した処理。例えば，静電塗装，電磁誘導加熱 - 高電圧を使用した溶接	- 感電死 - 感電 - やけど - 溶融物の放出
3	熱的危険源	- エンドエフェクタ又は関連する設備若しくはワークピースの高温表面（例えば、溶接トーチ、鍛造工程での高温材料、射出成形、研磨機及びバリ取り） - 低温の表面又は低温の物体（低温貯蔵プロセス） - プロセスによって生じる爆発しやすい雰囲気，例えば，塗装（粉末状の微粒子，粉体塗装），可燃性溶剤，研磨塵及び切削切り粉 - プロセスを支援するために必要な過度な温度[熔融材料 ; 調理又は加熱用のオーブン（圧力釜）; 冷凍庫又は冷却装置など]	- やけど(高温又は低温) - 放射傷害
		- 可燃性の材料(内側の集塵システム，洗浄タンク，シーラント)	
4	騒音の危険源	- 大きな騒音源となる特定の用途（例えば，ウオータジェットカッター，スタンピングプレス，ポンプ及びバルブ操作、金属除去作業） - 通常の会話で人との協調行動が出来ない場合を含めて、聞き取りを妨げる又は危険警告信号が理解できない騒音レベル	- 聴覚喪失 - バランスの喪失 - 認識力，方向感覚の喪失 - 周囲の条件または注意力散漫の結果として生じる他のあらゆる（例えば，機械的な）危険
5	振動の危険源	- 振動源との直接接触 - 接続、締結の緩み - 構成品又は部品の調整不良	- 疲労 - 神経障害 - 血管障害 - 衝撃
6	放射の危険源	- ロボットシステムの適切な運転での EMF 妨害 - プロセスに関連する放射への暴露，例えば，アーク溶接，レーザ	- やけど - 目及び皮膚疾患 - 関連の疾病
7	材料／物質の危険源	- 有害な流体で覆われたコンポーネントへの接触 - 機械的及び電気的コンポーネントの	- 過敏症 - 火災 - 化学的なやけど

表 3-8 ロボットシステムの危険源の例

No	種類	危険源の例	
		原因	潜在的結果
		故障 - 腐食性ガス及び腐食性粉塵	- 吸入疾患
8	人間工学的危険源	- 設計が適切でない（遠すぎたり高すぎたりする）教示ペンダント，人間-機械インタフェース（HMI）タッチスクリーン又はオペレータ用パネル - 設計が適切でないロード／アンロード用作業位置（例えば，部品箱の位置とロード／アンロード作業区域の距離が遠い - 設計が適切でないイネーブル装置 - 制御器具（ボタン・スイッチ等）の不適切な位置又は識別（例えば、届きにくい） - （トラブルシュート、修理、調整のために）接近が必要なコンポーネントの不適切な位置 - 隠れた危険源、不適当な又は遮られた局部照明	- 健康的でない姿勢又は過度の頑張り（繰返しの緊張） - 疲労
9	機械を使用する環境に関する危険源	- 地震多発区域に設置 - 電磁妨害又はエネルギ源のサージ - 湿気 - 温度	- やけど - 疾患又は疾病 - すべり，墜落 - 呼吸障害 - 衝突
10	危険源の組合わせ	- ロボットシステムの起動指令を一人の人が出したとき，このことが他の人には予測できない状態 - 複数の故障および条件から発生する危険源 - 正しくない又は不要な行動をすることによって，重要な問題及び複雑な問題の識別が不可能となること - 被害の程度を増加させる行動。すなわち､鋭利な端部を避けようとして，代わりに高温の表面に接触する - 残留力（慣性､重力､ばね/エネルギー蓄積手段）のある状態で動作を必要とする把持装置の意図しない解放 - 想定される機能に対する安全防護装置の故障	- 危険源と危険状態のあらゆる組合せの結果

（イ） 危険源の同定例

ロボットシステムにおける網羅的な危険源の同定方法として、表 3-のような表を用いて構成要素ごとに危険源の同定を行っていくとよい。なお、リスクの見積りにおいては、危害のひどさの大小にかかわらず考えられる危険源は全て同定する。

なお、このマニュアルでの参考事例として、以下のロボットシステム（図 3-1）を想定する。

① 治具に作業者が製品をセット
② ロボットが接着剤を塗布

③　製品をコンベアに移載(コンベアで製品は次工程へ搬送)

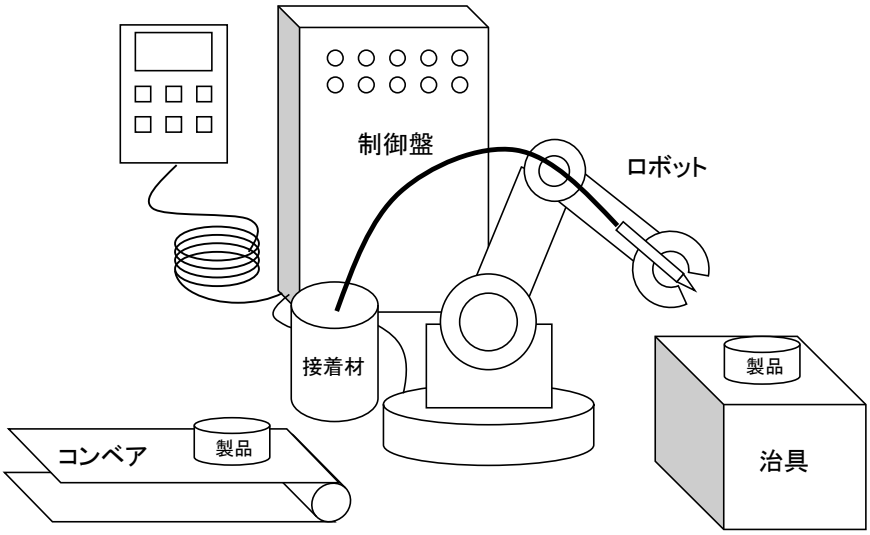


図 3-1 例題とするロボットシステム

表 3-9 ロボットシステムの危険源例

危険源の種類 / 構成要素	機械的				電気的	熱的	騒音	振動	放射	材料物質		人間工学	環境	組合せ
	動力（挟まれ等）	重量物	滑り・躓き・墜落	その他（切創等）						有害物質	爆発・火災			
ロボット*1	●	●			●	●	●							
治具	●	●		●	●		●					●		
コンベア	●	●			●									
配線			●		●									
制御機器		●			●									
製品				●		●				●		●		
接着剤										●				
接着剤用ポンプ	●				●	●	●							
…														

*1：エンドエフェクタ含む

イ　危険状態の同定

（ア） 必要とされる作業

ロボットシステムに係る作業内容と頻度を同定する。例を表 3-1 に示す。

表 3-10 ロボットシステムの作業例

運搬	ロボット本体・エンドエフェクタ・治具・周辺機械の梱包・運搬
据付	ロボット本体・エンドエフェクタ・治具・周辺機械の開梱・据付の為の移動、据付
調整	一般的な機械調整、電気調整、ティーチ作業、試運転
生産	製品のセット・取り出し
段取り	材料や副資材の補給・交換、エンドエフェクタ・周辺装置交換
保全	清掃・消毒、消耗品の補給・交換、部品(モータ、ブレーキ、ギア、ケーブル、電気部品)交換、ティーチ(変更)作業
トラブルシューティング	製品の流れ不良の処置、ハンドリング不良の処置、周辺装置動作不良処置
廃却	分解、運搬
その他	ロボットシステム近傍の通行

（イ） 想定される誤使用

ロボットシステムにおける予見される誤使用による危険状態の例を表 3-11 に示す。

表 3-11 誤使用による危険状態の例

考慮すべきヒューマンエラー	危険状態(危険事象の例
手抜き（ショートカット)、最小抵抗経路(「近道行動」「省略行動」)、用途外使用（代用)、意図しない接近・進入	・ロボットシステム内を通行する ・製品のセットミスの修正

（ウ） ロボットシステム危険状態の例

ロボットシステムにおける具体的な危険状態(危険事象)の例を表 3-12 に示す。

表 3-12 危険源・危険状態・危険事象の例

No	作業区分	危険状態
1	据付での運搬	ロボット(重量物)をフォークリフトで運搬する
2	据付・保全	ロボットの可動範囲内でのティーチ
3	生産作業－製品セット	製品をロボットの可動範囲内の治具にセットする
4	生産作業－製品セット(トラブルシューティング)	セットを忘れ部品をセットする ずれた部品を再セットする
5	トラブルシューティング	コンベア上製品の流れ不良を直す
6	保全	ロボットのモータを交換する
7	その他―通行	ロボットシステム近傍の通行
…	…	…

ウ　危険事象の同定

ロボットシステムにおける危険事象の例を表 3-に示す。

表 3-13 危険事象の例

分類	例
機械	エンドエフェクタ部製品検知による一時停止状態からの運転再開 供給エネルギの遮断・変動による把持力低下 ロボットモータのブレーキ摩耗による制動力低下 ロボットモータのブレーキ解放によるアームの自重落下
人	ティーチ中意図した動作とは違うボタンを操作する ティーチ中ペンダントが体に触れロボットが動く 他人がシステムを自動運転させる ロボットの自動運転の起動操作後、製品をセットし直す
自然現象	地震によるロボット・ロボット制御盤の転倒

エ　ロボットシステムにおける危険源・危険状態・危険事象の例

表 3-14 にロボットシステムにおける危険源・危険状態・危険事象の一例を示す。なお、1 つの危険状態でも、発生過程・原因が異なる危険事象がある場合、それぞれの保護方策が異なることがあるため、別々に同定する。

表 3-14 危険源・危険状態・危険事象の例

No	作業区分	危険源	危険状態	危険事象
1	据付	ロボット	ロボットをフォークリフトで運搬する	バランスを崩し落下させ作業者に接触
2	据付／保全―ティーチ	ロボット	ロボットの可動範囲内でロボットを操作する	ボタン操作を誤りロボットが動き挟まれる
3				体がボタンに触れロボットが動き挟まれる
4				他人が自動運転させロボットが動き挟まれる
5	製品セット	ロボット	ロボットの可動範囲内で製品をセットする	誤ったタイミングで入りロボットに挟まれる
6	製品セット／トラブルシューティング	ロボット	起動後に忘れた部品をセットする	運転しているロボットに挟まれる
7	製品セット	接着剤	空気中に放出された残留物質を吸引する	有害物質吸引による健康障害
8	製品セット	治具	無理な姿勢となる	繰り返し無理な姿勢による腰痛
9	トラブルシューティング	ロボット コンベア	コンベア上の製品の流れ不良を直す	自動運転継続条件が揃いロボットが動き挟まれる
10				止めていたが他人の操作でロボットが動き挟まれる
11	保全	ロボット	ロボットのモータ交換	ブレーキが解放されたアームが自重落下し挟まれる
12	その他	ロボット	運転中のロボットの可動範囲内を通行する	ロボットに激突され、挟まれ
13	その他	制御盤	ロボットシステム近傍を通行する	地震により転倒し人が押しつぶされる
…	…	…	…	…

(3)　リスクの見積もり・評価

表 3-～表 3-に基づいたリスク要素の見積もりとリスク評価の例を表 3-に示す。なお、最初の見積もりでは、危険事象の“発生確率:0”は、まだ保護方策がされていない状態での評価となり全て“頻繁:03”が選択されるため、省略する。

表 3-15　各リスク要素の定義

<table>
<tr><th>リスク要素</th><th>選択肢</th><th>選択基準</th></tr>
<tr><td rowspan="3">危害のひどさ:S</td><td>重篤:S3</td><td>致命傷(死亡)、身体に後遺障害(欠損、機能障害)を伴うもの</td></tr>
<tr><td>休業:S2</td><td>休業を必要とする傷害。肢の骨折や縫合を必要とする傷害、後遺障害が残らない筋骨格障害</td></tr>
<tr><td>不休:S1</td><td>軽微な傷害（通常は回復可能)。こすり傷、裂傷、挫傷、応急処置を要する軽い傷</td></tr>
<tr><td rowspan="3">頻度・時間:F</td><td>ライン作業:F3</td><td>ライン作業。サイクル毎に作業者が製品・部品をセットしたり取り出したりする作業</td></tr>
<tr><td>段取り作業:F2</td><td>段取り作業。定期的なツールの交換や補給品の供給・交換、清掃・消毒など</td></tr>
<tr><td>保全作業等:F1</td><td>保全作業等。機械の修理や点検、不定期の清掃・消毒など</td></tr>
<tr><td>回避性:A</td><td>回避不可:A2</td><td>リスクの認知性と抑制・回避行動より判断する
<table>
<tr><th>抑制・回避
認知性</th><th>可能</th><th>不可能</th></tr>
<tr><td>認知可能</td><td>回避可:A1</td><td>回避不可:A2</td></tr>
<tr><td>認知不可能</td><td>回避不可:A2</td><td>回避不可:A2</td></tr>
</table>
※適切な理由がない限り“回避不可:A2”を選択</td></tr>
<tr><td rowspan="3">発生確率:0</td><td>頻繁:03</td><td>機械として保護方策を実施していない＝頻繁に危険事象等が発生する
― 構想設計後の最初に行うリスクアセスメントにおける見積もりにて選択される</td></tr>
<tr><td>時々:02</td><td>人への依存がある保護方策(“付加保護方策”や“使用上の情報”での方策)、または信頼性を確認していない保護方策を実施している＝時々危険事象等などが発生する
― 非常停止ボタンやロックアウト対応器具の設置､手動の残留エネルギーの開放･抑制手段など使う人に操作などを要求する保護方策。
― 注意ラベル､保護具の使用､作業手順の遵守等の使用上の情報提供による保護方策</td></tr>
<tr><td>稀:01</td><td>人への依存度がほとんど無い信頼性のある保護方策を実施している＝危険事象等が発生することは、稀である。
― 関係する法・省令・規則・指針や JIS/ISO/IEC に従った安全防護
― 機械系は適切な強度計算等により信頼性が確認したもの
― 制御系の機能安全は、要求される信頼性(PLr)に合致している。</td></tr>
</table>

表 3-16　具体的なリスク評価表の例

危害のひどさ:S	頻度・時間:F	回避性:A	発生確率:O		
			頻繁:O3	時々:O2	稀:01
重篤:S3	ライン作業:F3	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	段取り作業:F2	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	保全作業等:F1	回避不可:A2	4	3	2
		回避可:A1	4	3	2
休業:S2	ライン作業:F3	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	段取り作業:F2	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	保全作業等:F1	回避不可:A2	4	3	2
		回避可:A1	2	2	1
不休:S1	ライン作業:F3	回避不可:A2	4	3	2
		回避可:A1	4	3	2
	段取り作業:F2	回避不可:A2	4	3	2
		回避可:A1	2	2	1
	保全作業等:F1	回避不可:A2	1	1	1
		回避可:A1	1	1	1

表 3-17　リスクレベルの定義

リスクレベル	定義
4	許容不可なリスク。ALARP 原則を適用しリスク低減が必要
3	ALARP 原則が適用されていなければ許容不可のリスク。
2	許容可能なリスク
1	無条件で許容可能なリスク

表 3-18 リスクの見積もりと評価

No	作業-危険源-危険状態-危険事象		ひどさ:S	頻度:F	回避:P	リスク
1	据付の為、ロボットをフォークリフトで運搬する時バランスを崩し落下させ周辺作業者に接触		S3 ロボット質量1000kg	F1 据付作業は低頻度	A2 回避不可	4
2	ロボットの可動範囲内でロボットティーチ中、	ボタン操作を誤りロボットが動き挟まれる	S3 ロボット推力 2000N	F1 ティーチは低頻度	A2 速度により回避不可	4
3		体がボタンに触れロボットが動き挟まれる	S3 ロボット推力 2000N	F1 ティーチは低頻度	A2 速度により回避不可	4
4		他人が自動運転させロボットに動き挟まれる	S3 ロボット推力 2000N	F1 ティーチは低頻度	A2 速度により回避不可	4
5	製品セットにおいて、誤ったタイミングで入りロボットに挟まれる		S3 ロボット推力 2000N	F3 製品セットは高頻度	A2 高速時は回避不可	4
6	起動後に忘れた部品をセット中、起動しているロボットに挟まれる		S3 ロボット推力 2000N	F3 製品セットは高頻度	A2 高速時は回避不可	4
7	製品セット中、残留接着材から空気中に放出された残留物質を吸引し健康障害を負う		S2 重篤疾病	F3 製品セットは高頻度	A2 回避不可	4
8	製品セットで無理な姿勢を繰り返し、腰痛になる		S2 重篤疾病	F3 製品セットは高頻度	A2 必要作業	4
9	コンベア上製品の流れ不良を直している時	自動運転継続条件が揃いロボットが動き挟まれる	S3 ロボット推力 2000N	F1 異常は低頻度	A2 高速時は回避不可	4
10		止めていたが他人の操作でロボットが動き挟まれる	S3 ロボット推力 2000N	F1 異常は低頻度	A2 高速時は回避不可	4
11	保全でロボットのモータ交換時、ブレーキが解放されロボットアームが自重落下し、挟まれる		S3 アーム重量 100kg	F1 異常は低頻度	A2 高速時は回避不可	4
12	運転中のロボット可動範囲内を通行し、ロボットに挟まれる		S3 ロボット推力 2000N	F1 通路としての代用は稀	A2 高速時は回避不可	4
13	床面に設置した制御盤が地震により転倒し人が押しつぶされる		S3 重篤疾病	F1 地震は稀	A2 回避不可	4
…	…		…	…	…	

２　リスク低減

(1)　ロボットシステムのリスク低減方策例

ALARP 原則に基づき、リスク低減方策を検討する。表 3-に各リスクに対する低減方策例を、図 3-2 に各方策のロボットシステムへの適用例を示す。

表 3-19　各リスクに対する低減方策例

No	作業-危険源-危険状態-危険事象		リスク低減方策例
1	据付の為、ロボットをフォークリフトで運搬する時バランスを崩し落下させ周辺作業者に接触		フォークフォークポケットを設ける 吊り金具
2	ロボットの可動範囲内でロボットティーチ中	ボタン操作を誤りロボットが動き挟まれる	ティーチ時の速度制限 ホールド・トゥ・ラン ロボットへの軸名称・動作方向表示
3		体がボタンに触れロボットが動き挟まれる	ティーチペンダントのイネーブルスイッチ設置
4		他人が自動運転させロボットに動き挟まれる	キー付運転モード切替スイッチ (ティーチ時抜けて携帯可)
5	ロボット工程に製品セットにおいて、誤ったタイミングで入りロボットに挟まれる		ライトカーテンを設置し製品セット時にはロボットを保護停止させる
6	起動後にセットを忘れ部品をセット中、起動しているロボットに挟まれる		〃
7	製品セット中、残留接着材から空気中に放出された残留物質を吸引し健康障害を負う		排気装置による残留物質換気
8	製品セットで無理な姿勢を繰り返し、腰痛になる		製品セット高さ・方向の適正化
9	コンベア上製品の流れ不良を直している時	自動運転継続条件が揃いロボットが動き挟まれる	レーザスキャナを設置し、人の接近時はロボットを減速運転させ、更に接近時は保護停止させる
10		止めていたが他人の操作でロボットが動き挟まれる	制御盤の起動装置へのロックアウト
11	保全でロボットのモータ交換時、ブレーキが解放されロボットアームが自重落下し、挟まれる		ロボットアーム固定装置による落下防止 注意ラベル貼付
12	運転中のロボット可動範囲内を通行し、ロボットに挟まれる		レーザスキャナを設置し、人の接近時はロボットを減速運転させ、更に接近時は保護停止させる
13	床面に設置した制御盤が地震により転倒し人が押しつぶされる		制御盤の床面へのアンカ固定
…	…		…

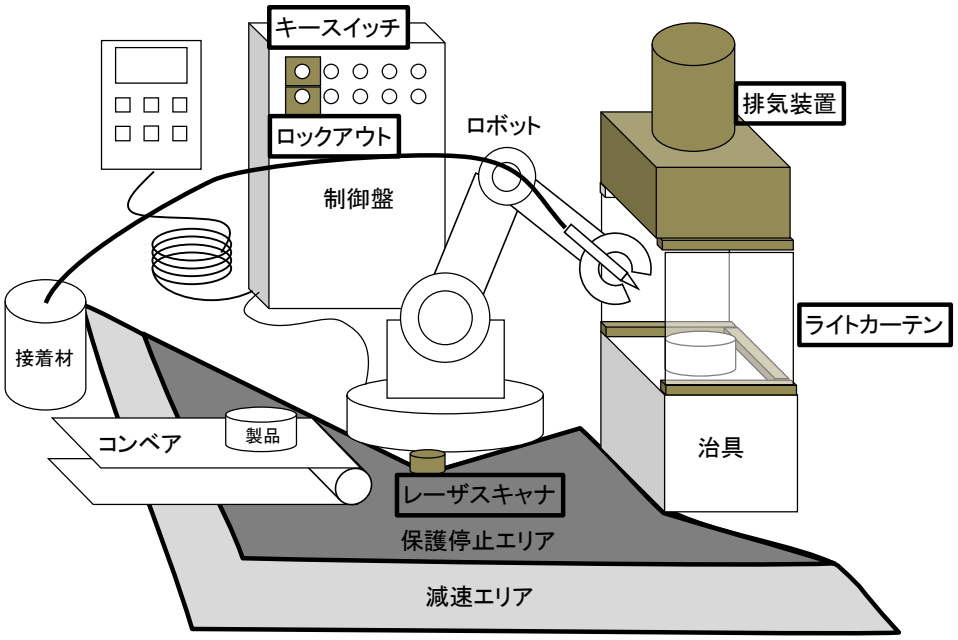


図 3-2 リスク低減方策後のロボットシステム例

(2) リスク低減方策実施後のリスク見積り・評価

表 3-で検討したリスク低減方策にてリスク低減をできたかの見積もり・評価と方策の妥当性評価を行う（表 3-20)。なお、リスク低減方策のうち、法や指針、JIS 等で具体的な要求事項が定められている方策については、当該要求事項に合致するよう設計されるものとして評価を行う。表 3-21 は、初期リスク評価から再リスク評価までを一覧できるようにまとめたシートである。

表 3-20　リスク低減方策実施後のリスク見積り・評価

No	リスク低減方策	保護方策後のリスク見積もり・評価					
		ひどさ:S	頻度:F	回避:P	発生確率:0	リスク	妥当等
1	フォークフォークポケットを設ける吊り金具	S3 ロボット質量 1000kg	F1 据付作業は低頻度	A2 回避不可	02 作業者による利用	3	取説に記載要
2	ティーチ時の速度制限、ホールド・トゥ・ラン、ロボットへの軸名称・動作方向表示	S3 ロボット推力 2000N	F1 ティーチは低頻度	A2 回避不可	01 無意識でも有効	2	
3	イネーブルスイッチ	S3 ロボット推力 2000N	F1 ティーチは低頻度	A2 回避不可	01 無意識でも有効	2	
4	キー付運転モード切替スイッチ (ティーチ時抜いて携帯可)	S3 ロボット推力 2000N	F1 ティーチは低頻度	A2 回避不可	02 作業者による利用	3	取説に記載要
5	ライトカーテンを設置し製品セット時にはロボットを	S3 ロボット推力 2000N	F3 製品セットは高頻度	A2 回避不可	01 無意識でも有効	2	

表 3-20　リスク低減方策実施後のリスク見積り・評価

No	リスク低減方策	保護方策後のリスク見積もり・評価					
		ひどさ:S	頻度:F	回避:P	発生確率:O	リスク	妥当等
	保護停止させる						
6	〃	〃	〃	〃	〃	2	〃
7	排気装置による残留物質換気	S2 重篤疾病	F3 製品セットは高頻度	A2 回避不可	O1 無意識でも有効	2	
8	製品セット高さ・方向の適正化	S2 重篤疾病	F3 製品セットは高頻度	A2 回避不可	O1 無意識でも有効	2	
9	レーザスキャナを設置し、人の接近時はロボットを減速運転させ、更に接近時は保護停止させる	S3 ロボット推力 2000N	F1 異常は低頻度	A2 回避不可	O1 無意識でも有効	2	
10	制御盤の起動装置へのロックアウト	S3 ロボット推力 2000N	F1 異常は低頻度	A2 回避不可	O1 無意識でも有効	3	取説に記載要
11	ロボットアーム固定装置による落下防止 注意ラベル貼付	S3 アーム重量 100kg	F1 異常は低頻度	A2 回避不可	O2 作業者による利用	3	取説に記載要
12	レーザスキャナを設置し、人の接近時はロボットを減速運転させ、更に接近時は保護停止させる	S3 ロボット推力 2000N	F1 通路としての代用は稀	A2 回避不可	O1 無意識でも有効	2	
13	制御盤の床面へのアンカ固定	S2 重篤疾病	F1 地震は稀	A2 回避不可	O1 無意識でも有効	2	
…	…		…				

表 3-21 ロボットシステムのリスクアセスメント例(全体)

No	作業-危険源-危険状態-危険事象		保護方策前のリスク見積もり・評価				リスク低減方策	保護方策後のリスク見積もり・評価					
			ひどさ:S	頻度:F	回避:P	リスク		ひどさ:S	頻度:F	回避:P	発生確率:0	リスク	妥当性等
1	据付の為、ロボットをフォークリフトで運搬する時バランスを崩し落下させ周辺作業者に接触		S3 ロボット質量1000kg	F1 据付作業は低頻度	A2 回避不可	4	フォークフォークポケットを設ける 吊り金具	S3 ロボット質量1000kg	F1 据付作業は低頻度	A2 回避不可	02 作業者による利用	3	取説に記載要
2	ロボットの可動範囲内でロボットティーチ中、	ボタン操作を誤りロボットが動き挟まれる	S3 ロボット推力2000N	F1 ティーチは低頻度	A2 速度により回避不可	4	ティーチ時の速度制限 ホールド・トゥ・ラン ロボットへの軸名称・動作方向表示	S3 ロボット推力2000N	F1 ティーチは低頻度	A2 回避不可	01 自動的に有効	2	
3		体がボタンに触れロボットが動き挟まれる	S3 ロボット推力2000N	F1 ティーチは低頻度	A2 速度により回避不可	4	イネーブルスイッチ	S3 ロボット推力2000N	F1 ティーチは低頻度	A2 回避不可	01 自動的に有効	2	
4		他人が自動運転させロボットに動き挟まれる	S3 ロボット推力2000N	F1 ティーチは低頻度	A2 速度により回避不可	4	キー付運転モード切替スイッチ (ティーチ時抜いて携帯可)	S3 ロボット推力2000N	F1 ティーチは低頻度	A2 回避不可	02 作業者による利用	3	取説に記載要
5	製品セットにおいて、誤ったタイミングで入りロボットに挟まれる		S3 ロボット推力2000N	F3 製品セットは高頻度	A2 高速時は回避不可	4	ライトカーテンを設置し製品セット時にはロボットを保護停止させる	S3 ロボット推力2000N	F3 製品セットは高頻度	A2 回避不可	01 無意識でも有効	2	
6	起動後にセット忘れ部品をセット中、起動してい		S3 ロボット	F3 製品セッ	A2 高速時	4	〃	S3 ロボット	F3 製品セッ	A2 回避不	01 無意識で	2	

	るロボットに挟まれる		推力2000N	トは高頻度	は回避不可			推力2000N	トは高頻度	可	も有効		
7	製品セット中、残留接着材から空気中に放出された残留物質を吸引し健康障害を負う		S2 重篤疾病	F3 製品セットは高頻度	A2 回避不可	4	排気装置による残留物質換気	S2 中毒	F3 製品セットは高頻度	A2 回避不可	01 無意識でも有効	2	
8	製品セットで無理な姿勢を繰り返し、腰痛になる		S2 重篤疾病	F3 製品セットは高頻度	A2 必要作業	4	製品セット高さ・方向の適正化	S2 重篤疾病	F3 製品セットは高頻度	A2 回避不可	01 無意識でも有効	2	
9	ロボット近傍でコンベアセンサを調整する	自動運転継続条件が揃いロボットが動き挟まれる	S3 ロボット推力2000N	F1 異常は低頻度	A2 高速時は回避不可	4	レーザスキャナを設置し、人の接近時はロボットを減速運転させ、更に接近時は保護停止させる	S3 ロボット推力2000N	F1 異常は低頻度	A2 回避不可	01 無意識でも有効	2	
10		止めていたが他人の操作でロボットが動き挟まれる	S3 ロボット推力2000N	F1 異常は低頻度	A2 高速時は回避不可	4	制御盤の起動装置へのロックアウト	S3 ロボット推力2000N	F1 異常は低頻度	A2 回避不可	02 作業者による利用	3	取説に記載要
11	保全でロボットのモータ交換時、ブレーキが解放されロボットアームが自重落下し、挟まれる		S3 アーム重量100kg	F1 異常は低頻度	A2 高速時は回避不可	4	ロボットアーム固定装置による落下防止注意ラベル貼付	S3 アーム重量100kg	F1 異常は低頻度	A2 回避不可	02 作業者による利用	3	取説に記載要
12	運転中のロボット可動範囲内を通行し、ロボットに挟まれる		S3 ロボット推力2000N	F1 通路としての代用は稀	A2 高速時は回避不可	4	レーザスキャナを設置し、人の接近時はロボットを減速運転させ、更に接近時は保護停止させる	S3 ロボット推力2000N	F1 通路としての代用は稀	A2 回避不可	01 無意識でも有効	2	
13	床面に設置した制御盤が地震により転倒し人が押しつぶされる		S3 重篤疾病	F1 地震は稀	A2 回避不可	4	制御盤の床面へのアンカ固定	S2 重篤疾病	F1 地震は稀	A2 回避不可	01 無意識でも有効	2	

第 4 章　安全関連システムの要求安全度水準の決定

１　　概要

安全関連システム（油空圧制御を含む場合もあり）は、リスクアセスメントの結果によって、本章 3 節で示す代替の性能基準が適切であると決定しない限り、2 節に掲げる要求安全度水準に適合しなければならない。そして、決定されたロボット及び他の必要な設備の安全関連システムの安全度水準は、使用上の情報に明確に記載しなければならない。なお、本書では安全関連システムを電気・電子・プログラマブル電子（PE/E/PE）制御システムの安全関連部と定義しているが、産業用ロボットが油空圧制御システムを有して、さらに安全制御を担う場合は、安全関連システムに含むものとする。

２　要求安全度水準の標準

産業用ロボット、及び産業用協働ロボットの安全関連システム（Safety-Related Electrical Control System、略称 SRECS に該当）の要求安全度水準は、ISO 10218-2（JIS B 8433-2）で以下のように標準のレベルが指定される。

● ISO 13849-1:2006（JIS B 9705-1:2011）に基づいて、
　・カテゴリ 3、
　・PL＝d

または、

● IEC 62061:2005（JIS B 9961:2008）に基づいて、
　・プルーフテスト間隔：20 年以上、
　・ハードウェアフォールトトレランス：1
　・SIL2

上記の要求安全度水準は、次のことを意味する。

a）いずれの部分に単一の不具合（障害）が生じても安全機能の喪失にはつながらない。

b）合理的に実行可能な場合は常に，単一の不具合（障害）は，安全機能の次の作動要求時又はその前に検出できる。

c）単一の不具合（障害）発生時に，安全機能を常に実行し，検出した不具合（障害）が修復されるまで安全状態を維持される。

d）合理的に予見可能な不具合（障害）は，全て検出できる。

これら 2 規格は，類似しているが異なる方法で機能安全を取り扱っている。設計者は

これら 2 規格のいずれかを選択使用してよい。しかし、一般的にロボットシステムにおいては、入力部、演算部、出力部を容易に区別できるので、ISO 13849-1 を用いたほうがよいと言われている。

ISO 10218-2 はこれら 2 つ規格の発行年を ISO 13849-1 は 2006 年版、IEC 62061 は 2008 年版に限定している。これはこれら 2 規格の改定によって、ISO 10218-2 の要求事項に対して齟齬が発生するのを防止するためである。ISO 13849-1 の 2006 年版は、既に 2015 年版（ISO 13849-1:2015、JIS 版は 2016 年 12 月時点で未発行）に入れ替えられた。しかし ISO 13849-1 の改定は、本章 2、3 節で示すような安全要求水準の決定及びその達成に対して、一部を除いて大きな影響を及ぼしていない。

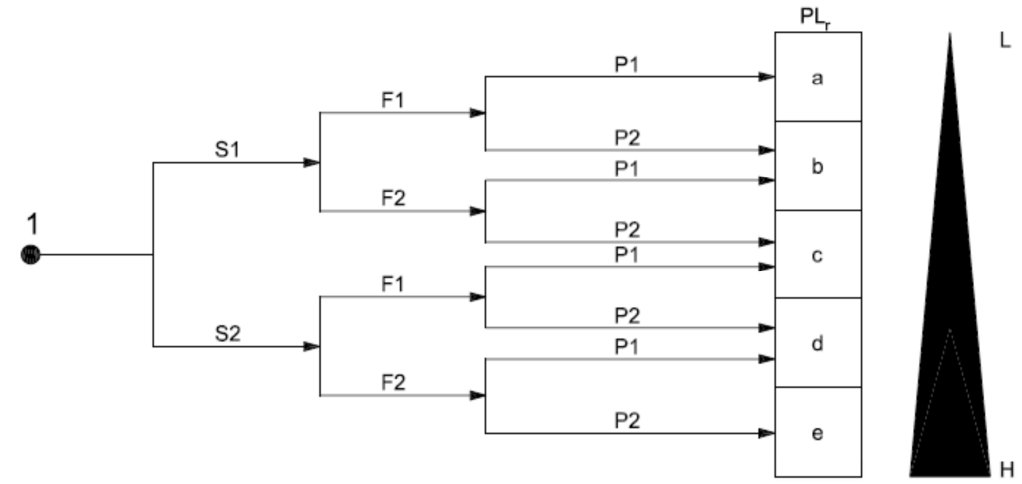
３　ISO 13849-1 を用いた要求安全度水準の決定

産業用ロボット、及び産業用協働ロボットの安全関連システムの安全性能は、3 章で述べたリスクアセスメントとリスク低減の結果に基づき、上記標準レベル以外の要求安全度水準を選択できる。他の安全関連性能基準を選択決定したときは、そのことを明示しなければならない。さらに、適切な制限及び注意事項は、影響を受ける設備に付随して提供される使用上の情報に含めなければならない。

ロボットシステムおける要求安全度水準としての要求パフォーマンスレベル PLr は、機能が独立している限り、その機能単位（例：ロボット非常停止回路、ロボット保護停止回路、ロボットイネーブル装置回路、ロボットのタスクに関与しない部品供給用のドアスイッチ回路）で決定すればよい。

ISO 13849-1 における PLr の決定方法としては、図 4-1 のリスクグラフを用いて導出する例が説明されている。同図の左側から、S:危害の頻度、F:危険源にさらされる頻度又は時間、および P:危険源の回避可能性又は危害を抑える可能性の項目について順次選択することによりリスクの大きさを分類することができる。このリスクの大きさが PLr のレベルに対応しており、PLr=e が制御システムへのリスク低減の寄与度が高い。すなわち、第 3 章で定義されたリスク要素の内、「危険事象の発生確率」のみ図 4-1 のリスクグラフで評価されていないことから、PLr のレベルはこの「危険事象の発生確率」に関連してリスク低減に寄与する度合いを示していることが分かる。結局、保護方策によるリスク低減の目標は、「危険事象の発生確率」を低減するための安全性能の目標を定めていることになる（第 3 章表 3-15 参照）。

このリスクグラフにより PLr を求めるにあたり、各リスク要素の査定で注意すべき点を次に述べる。



記号の説明

1　リスク低減に安全機能の寄与度を評価するための開始点
L　リスク低減への寄与度“低”
H　リスク低減への寄与度“高”
PL_r 要求パフォーマンスレベル
S　傷害のひどさ
S1　軽症（通常，回復可能な傷害）
S2　重傷（通常，回復不可能又は死亡）
F　危険源への暴露の頻度及び／又は時間
F1　まれ～低頻度，及び／又はさらされる時間が短い
F2　高頻度～連続，及び／又はさらされる時間が長い
P　危険源回避又は危害の制限の可能性
P1　特定の条件下で可能
P2　ほとんど不可能

図 4-1　PLr のリスクグラフ(JIS B 9705-1:2011 より)

S:危害の程度

安全機能の故障によって生じるリスク見積りでは、軽傷（通常、回復可能）及び重傷（通常、回復不可能）及び死亡だけを考慮する。S1 及び S2 の決定のために、通常、事故の重大性及び正常状態への回復過程を考慮することが望ましい。例えば、単純な打撲傷及び/又は裂傷は S1 に分類され、一方、切断又は死亡は S2 に分類されることになる。

F:危険源にさらされる頻度又は時間

一般的に、パラメータ F1 又はパラメータ F2 を選択するための妥当な時間を特定することはできない。しかし、疑問が生じる場合、次の説明をすることによって決定を容易にすることがある。

人が頻繁又は継続的に危険源に暴露される場合、F2 を選択することが望ましい。同一又は異なる人のいずれが、継続的に危険源に暴露されているかは無関係である（例えばリフトの使用)。頻度のパラメータは、危険源への頻度及び接近時間に従って選択することが望ましい。

安全機能の動作要求頻度が設計者によって既知である場合、その要求頻度及び要求時間を危険源への接近頻度及び接近時間の代わりに選択することができる。この規格では、安全機能の動作要求頻度は 1 年に 1 回以上を想定している。

危険源への暴露の期間は、設備使用時間の合計と関連させて、平均値をベースとして

評価することが望ましい。例えば、ワークピースを搬入及び移動するようなサイクル運転中に機械のツール間に定期的に入ることが必要な場合、F2 を選択することが望ましい。もし機械への接近が時々必要であるという程度ならば、F1 を選択できる。

ISO 13849-1:2015 では、頻度が 15 分に 1 回を超える場合は、F2 とすることを推奨している。また累積された暴露時間が作業時間の 1/20 を超えず、かつ頻度が 15 分に 1 回を超えなければ F1 を選んでよいとしている。F1/F2 選択の参考にするとよい。

P：危険源回避の可能性

事故が起こる前に危険状態を認知し、回避することができるかどうかを知ることは重要である。例えば危険源を直接その物理的特性によって同定できるのか、又は、例えば表示装置のような技術的手段によってだけ認知できるのか、それを検討しておくことは重要である。パラメータ P の選択に影響する他の重要な要素は、例えば次を含む。

- 監督付き又はなしの運転
- 熟練者又は非専門者による運転
- 危険源発生の速度（例えば、直ちに又はゆっくり）
- 危険源回避の可能性（例えば、脱出）
- 工程に関する実際の安全経験

危険状態が発生して、事故を回避する又はその効果を顕著に低減するための現実的機会が存在する場合だけ P1 を選択することが望ましい。危険源回避の可能性がほとんどない場合は P2 を選択することが望ましい。

リスクアセスメントの結果に従い、安全関連システムによって実行されるそれぞれの安全機能に対して要求パフォーマンスレベル PLr を決定する。また、その決定の過程を文書化しなければならない。PLr は高くなるほど、安全関連システムによって提供されるリスク低減量は大きくなければならない。

設計の最後の妥当性確認のフェーズにおいて、各安全機能が実現した結果としてのパフォーマンスレベル PL が、要求パフォーマンスレベル PLr を達成したかどうかを評価する。

４　PLr 決定の例

図 4-1 のリスクグラフを用いて、比較的大型で高速な産業用ロボットの挟圧の危険源について PLr を導出すると、以下の条件の場合、PLr は“e”が要求される（図 4-2 参照）。

・危険事象　：製品セットにおいて、誤ったタイミングで入りロボットに挟まれる
・怪我の酷さ：ロボットの推力 2000N のため、重大災害が生じる
・発生頻度　：毎サイクル毎に製品セットするため、高頻度

・回避可能性：ロボットは 1 m/s の高速で動作するため、回避不可

この結果は、ISO 13849-1 において標準で規定されている要求安全度水準よりも高い（より厳しい）。

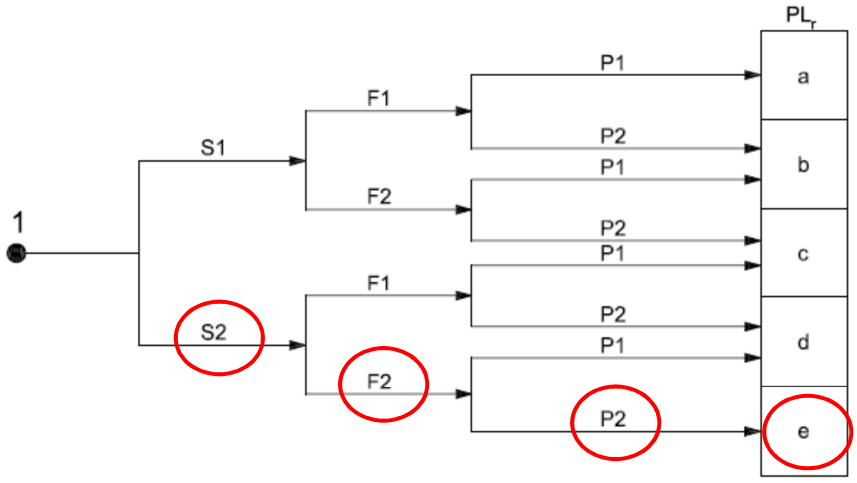


図 4-2　PLr の決定の例

第 5 章　ロボットシステムの設計

１　　概要

協働作業ロボットシステムを設計する手順は、先ず第 3 章のリスクアセスメントの手順に従って、ロボットシステムに関する危険源、危険事象を洗い出し、それぞれのリスクを見積る。リスクが許容できない危険源について、3 ステップメソッド（本質的安全設計、安全防護と付加的防護策、使用上の情報）によりリスク低減を実施し、許容できるリスク以下とする（「機能安全活用テキスト」参照)。すべての危険源が許容できるとき、協働作業ロボットは安全であるとみなす。さらに、リスク低減方策として安全関連システムを適用する場合、第 4 章の手順に従って、安全関連システムの要求安全度水準を求めなければならない。これにより、制御システムの安全仕様が求められる。

特に、産業用ロボットのシステム化により他の周辺機械や装置との連動を実現する場合、制御システムによる安全確保が必要となる。また、作業者がロボットと動作空間を共有する協働作業ロボットシステムを構築する場合、本質的に危害のおそれがないほど極低出力ロボットでない限り、安全制御によるリスク低減は不可欠となる。本章では、このような協働作業ロボットシステムの設計を行う上で、特に理解が必要なリスク低減策について解説する。

２　ロボットの安全要求事項

(1)　要求事項全体

産業用ロボットの安全要求事項は、第 2 章で紹介した JIS B 8433-1（ISO 10218-1）に規定されている。その概要を表 5-1 に示す。本書の第 2 章 2 節、および第 3 章 2 節も併せて参考にしてほしい。

表 5-1 において、「5.5 ロボット停止機能」、「5.6 速度制御」及び「5.10 協働運転要求事項」は、協働作業ロボットとして特別な機能及び条件が要求されている。例えば、ロボットに軽くぶつかったときに、ロボットが一時停止し、しばらく後で動き出すのはロボット停止機能の保護停止要求を満足しなければならない。また、人が接近したときにロボットが減速して動作するのは、速度制御の安全適合速度監視の要求を満足しなければならない。すなわち、ロボット自体がこれらの安全要求に適合しているか、ロボットの外部に回路や装置を追加して要求適合しなければならない。

本章では、これらの特別な要求について解説する。

表 5-1　ロボットの安全設計要求事項（JIS B 8433-1(ISO 10218-1)より）

JIS B 8433-1	要求事項	内容
5.2	一般要求事項	動力伝達構成品、動力の消失又は変化、構成品の機能不良、エネルギー源、蓄積エネルギー、電磁両立性(EMC)、電気設備
5.3	作動制御装置	意図しない操作からの保護、状態表示、ラベル付け、単一制御点
5.4	安全関連制御システム性能	性能要求事項、他の制御システム性能基準
5.5	ロボット停止機能	非常停止、保護停止
5.6	速度制御	低減速度制御運転、安全適合の低減制御、安全適合監視速度
5.7	運転モード	モード選択、自動モード、手動低減速度、手動高速モード
5.8	ペンダント制御装置	動作制御、イネーブル装置、ペンダントの非常停止機能、自動運転の始動、ケーブルレス教示制御装置、複数のロボットの制御
5.9	同時動作制御	単一ペンダント制御、安全設計要求事項
5.10	協働運転要求事項	安全適合の監視停止、ハンドガイド、速度及び間隔の監視、本質的設計又は制御による動力及び力の制限
5.11	特異点保護	
5.12	軸制限	機械的及び電気機械的軸制限装置、安全適合ソフト軸及び空間制限、動的制限装置
5.13	駆動用動力なしの移動	
5.14	つり上げ対策	
5.15	電気コネクタ	

(2)　ロボット停止機能

それぞれのロボットは、保護停止機能及び独立した非常停止機能を持たなければならない。これらの機能は、外部保護装置への信号接続を備えなければならない。

ア　非常停止機能

非常停止機能は、JIS B 9960-1（IEC 60204-1)の停止カテゴリ 0 又は 1 による停止である（第 2 章 2 節参照）。JIS B 9703（ISO 13850)非常停止規格にも適合することが求められている。

なお、サーボモータやインバータが参照する安全規格、IEC 61800-5-2 可変速電力ドライブシステムー第 5-2 部 :安全要求事項ー機能では、停止カテゴリ 0 を STO (Safe Torque Off)、停止カテゴリ 1 を SS1(Safe Stop 1)そして停止カテゴリ 2 を(Safe Stop

2)と呼んでいる。最近では、ロボット分野でもこれらの略称を使用することが増えている。

ロボットの制御ステーションは、手動で始動できる次の非常停止機能を備えなければならない。

a)安全関連制御システム性能(PLr/SIL)及び JIS B 9960-1 (IEC 60204-1)の要求事項に適合する。

b)ロボットの他の全ての制御に優先する。

c)全ての危険源を停止する。

d)ロボットアクチュエータから駆動用動力を除去する。

e)ロボットシステムによって制御される危険源の制御の能力を備える。

f)リセットするまで維持する。

g)手動動作によってだけリセットでき，リセット後は再起動を引き起こしてはならない。リセットは，再起動を可能にすることだけでなければならない。

イ　保護停止

ロボットは、外部の保護装置に接続するために設計した一つ以上の保護停止機能をもたなければならない。保護停止は、全てのロボット動作を停止し、ロボット駆動用アクチュエータへの動力を除去又は制御し、かつ、ロボットが制御する他のあらゆる危険源の制御を可能にしなければならない。この停止は、手動又は制御論理によって始動してもよい。

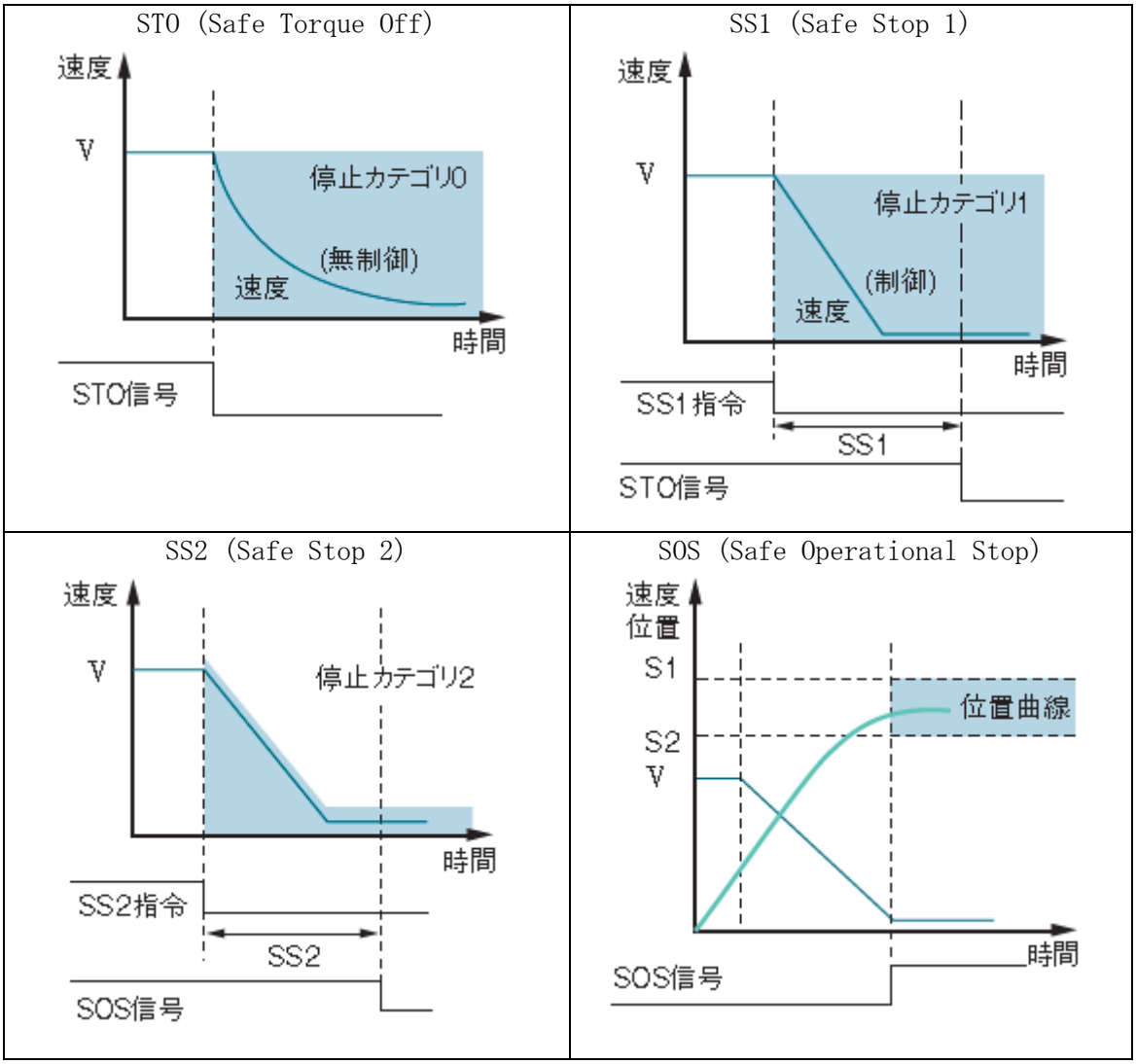
少なくとも一つの保護停止機能は、JIS B 9960-1(IEC 60204-1)で規定している停止カテゴリ０(ST0)又は１(SS1)でなければならない。ロボットは、JIS B 9960-1(IEC 60204-1)で規定している停止カテゴリ２(SS2)を使用した追加保護停止機能を持ってもよい。停止カテゴリ２の保護停止機能はロボット停止後に駆動力を除去しないので、停止状態の監視が必要となる。

停止状態の監視方法は、外部からの位置監視、電力駆動装置(サーボモータ等)による位置監視がある。特に、IEC 61800-5-2 では、安全な位置停止(Safe Operational Stop)と呼んでおり、駆動システムの停止カテゴリ 2(SS2)と SOS の組み合わせにより、監視された保護停止機能が実現できる。

もし、監視された停止状態での意図しないロボット動作、又は保護停止機能の不具合（障害）が検出された場合は、停止カテゴリ 0 による停止とならねばならない。加えて、監視された停止機能の安全性能は、その安全機能の PLr/SIL に適合しなければならない。

ロボット停止機能(ST0、SS1、SS2 及び SOS)の比較を表 5-2 に示す。

表 5-2　ロボット停止機能の比較



(3)　速度制御

安全防護のない協働作業ロボットでは、ロボットの速度、とりわけエンドエフェクタやツールセンタポイント(以下、TCP と呼ぶ)の速度は、危害のひどさ及び回避性の見積もりに大きく影響する。従って、これらの速度は制御可能であること、および TCP の速度を制御できるようにするためにオフセット機能（取付フランジと TCP との相対的な位置を決める）を備えなければならない。

ア　低減速度制御運転

低減制御下の運転時は、TCP 速度が 250 mm/s 以下でなければならない。できれば、250 mm/s より遅い速度も選択できることが望ましい。

イ　安全適合の低減制御

安全適合の低減制御を備える場合，不具合（障害）が発生したときに TCP の速度が低減速度の制限(上記 250mm/s)を超さないように、要求安全度水準(PLr/SIL)に従って設計及び構成しなければならない。また，不具合（障害）が発生した場合は，(2)の保護停止をしなければならない。

ウ　安全適合監視速度

安全適合の監視された速度を備える場合は、TCP 速度又は軸速度を要求安全度水準(PLr/SIL)に従って監視しなければならない。もし，その選択した速度の制限を超えた場合は，保護停止しなければならない。

TCP 速度又は軸速度を監視する方法として、ロボットや軸外部に速度計を設置する方法と、駆動システム自体が速度監視機能を備える方法がある。後者の場合、IEC 61800-5-2 では安全速度制限 SLS(Safety Limited Speed)と呼んでいる。SLS の動作を図 5-1 に示す。

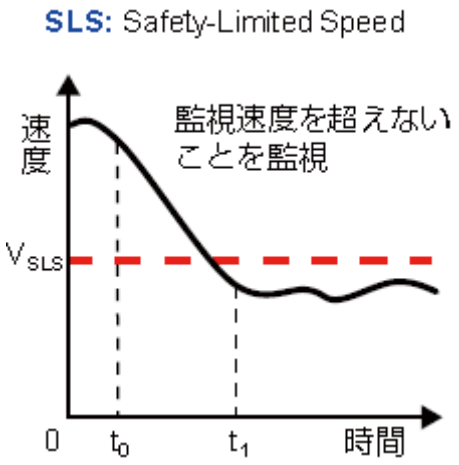


図 5-1　安全速度制限 SLS の動作

(4)　協働運転要求事項

協働運転のために設計されたロボットは，協働運転中であることを示す視覚表示を備えなければならず，更に以降の一つ以上の要求事項に適合しなければならない。

ア　安全適合の監視停止

作業者が協働作業空間内に存在するときは，ロボットは停止しなければならない。停止機能は，「JIS B 8433-1(ISO 60128-1)，5.5 ロボット停止機能」の要求に適合しなければならない。人間が協働作業空間から離れると，ロボットは自動運転に復帰してもよい。

ロボットが停止カテゴリ 2 (SS2)により停止する場合，停止状態を安全関連制御システムによって監視しなければならない。前述の、IEC61800-5-2 の SOS を含んでもよい。監視停止機能の不具合（障害）は，停止カテゴリ 0 (ST0)としなければならない。

イ　ハンドガイド

ハンドガイド装置がある場合，エンドエフェクタの近くに配置し，非常停止装置とイネーブル装置を備えなければならない。

ロボットは、本節（3）ウに示した安全適合監視速度機能が有効な状態で運転しなければならない。安全適合の監視された速度制限の値は，リスクアセスメントによって決定しなければならない。

ウ　速度及び間隔の監視

ロボットは，決められた速度及びオペレータとの間隔を保たなければならない。決められた速度又は間隔の維持の不具合(障害)が検出されたときは，保護停止にならなければならない。速度及び間隔の監視機能は，安全性能要求に適合していなければならない。使用上の情報には，実行速度値と間隔の指示とを含めなければならない。

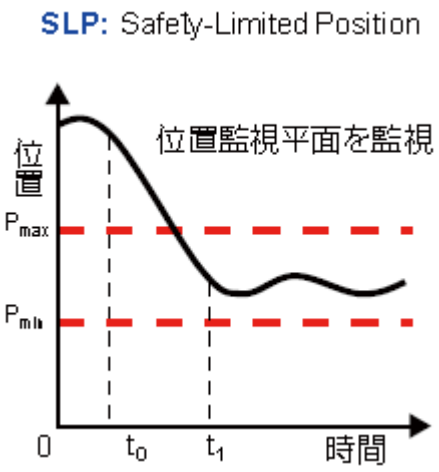


図 5-2　安全位置制限 SLP の動作

作業者とロボットの相対速度は、両者間の最小安全距離に関わる。最小距離の計算は、JIS B 9715（ISO 13855)に詳しい。

安全適合監視速度を実現する機能 SLS に対して、ロボットの位置を制限及び監視する機能としては、IEC 61800-5-2 の安全位置制限 SLP（Safety Limited Position)がある。SLP は、ロボットエンドエフェクタ又は TCP が指定の位置監視平面から出ないように監視し、指定外の位置に出ると保護停止する（図 5-2）。SLP の位置位置平面の設定方法は、ロボット供給者が専用ツールとして提供することが多い（第 8 章事例参照）。

エ　本質的設計又は制御による動力及び力の制限

ロボットの動力又は力を制限する機能は，安全性能要求に従わなければならない。いずれの制限値を超えた場合も保護停止としなければならない。変動するロボット出力が許容範囲にあることを監視する機能としては、IEC 61800-5-2 の安全トルク範囲 STR(Safe Torque Range)がある(図 5-3）。特に、ハンドガイドより密接

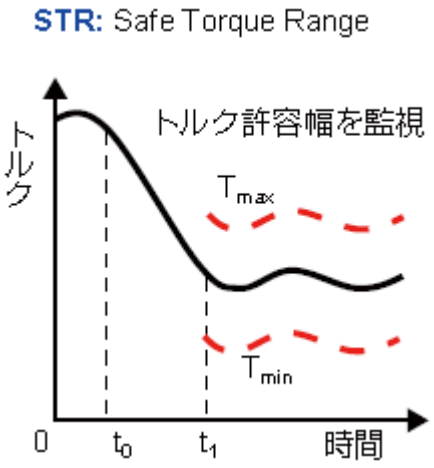


図 5-3　安全トルク範囲 STR の動作

なロボットとの接触状態を前提とした協働運転を行う場合、この STR は重要であり、アプリケーションや関連タスク、及び作業者との位置関係によって動的監視も機能しなければならない。

ロボットは、協働ロボットシステムを構成する一部品であり，それだけで安全な協働運転を達成できるとは限らない。協働運転のアプリケーションについて、正しい手順によりリスクアセスメントと適切なリスク低減方策をに実施しなければならない。このリスク低減方策には、制御されたロボットの速度や距離などの制限値の決定も含む。使用上の情報には，これらの制限値の設定について詳細を含めなければならない。

3　ロボットシステムの安全要求事項

(1)　安全コンポーネント

ロボットが前節において説明した安全要求事項を満たす機能を持っていれば、それらの機能を利用することで安全かつ使い勝手の良い協働作業ロボットを達成できるだろう。しかし、ロボットの設置条件やアプリケーションの種類によっては、ロボット外部に安全関連制御システムを構築する必要がある。例えば、図 5-4 のような安全コンポーネントを組み合わせて、制限区域の設定や非常停止/保護停止を実現する。

なお、具体的な事例については、第 8 章で説明する。

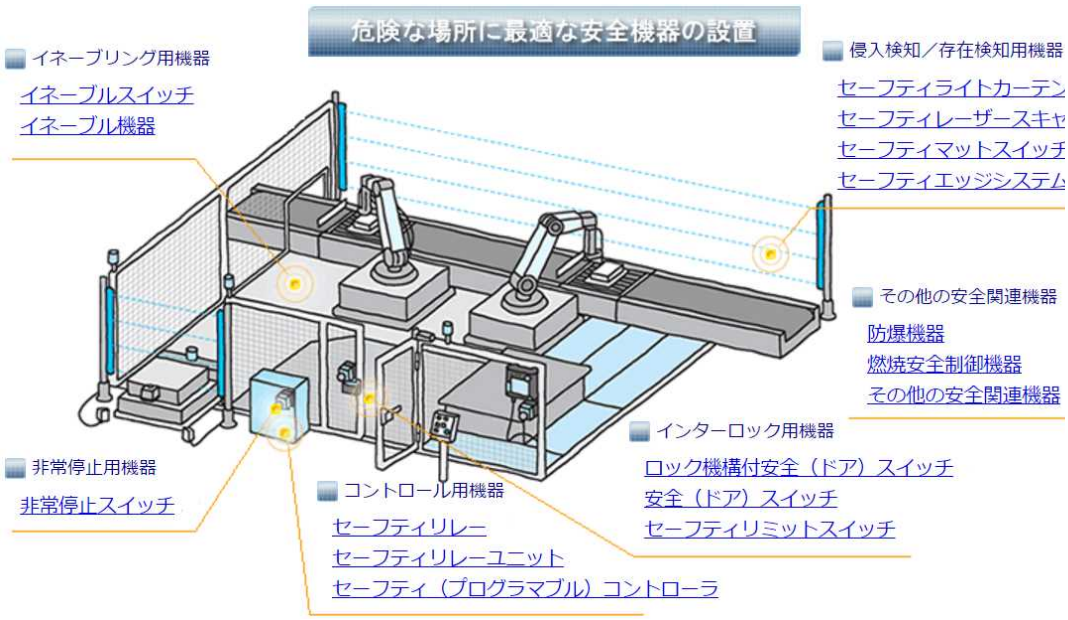


図 5-4　安全コンポーネントの種類
（（一社）日本電気制御機器工業会ホームページより）

ア　イネーブリング用機器

手動低減速度モードあるいは手動高速モードにおいて、ロボット動作のホールド・ツウ・ランを実現するために用いられる。ペンダント又は教示制御装置は，JIS B 9960-1 に従って 3 ポジションスイッチをもたなければならない。

継続的に中央のイネーブル位置に保持されているとき，イネーブル装置はロボット

図 5-5 イネーブルスイッチ及びイネーブルスイッチを使用したティーチングペンダントとグリップスイッチ(IDEC ホームページより)

の動作，及びロボットによって制御された他の危険源を許可する。詳細は、JIS B 8433-1 (ISO 10218-1) 5.7 及び 5.8.3 を参照のこと。ロボットのイネーブル装置に使用される 3 ポジションイネーブルスイッチについては　JIS C 8201-5-8(IEC60947-5-8) を参照のこと。

イ　非常停止用機器

ロボットの非常停止機能のために用いられる非常停止装置については、JIS B 8433-1、5.5.2 の要求を満足しなければならない。また、ペンダントまたは教示用制御装置にも非常停止装置が必要である(JIS B 8433-1(ISO 10218-1)、5.8.4 の要求)。非常停止スイッチは、JIS B 9960-1(IEC 60204-1) 及び JIS B 9703(ISO 13850)の要求を満足しなければならない。 非常停止装置に用いられる非常停止スイッチについては、JIS B 8201-5-5(IEC60947-5-5)に従わなければならない。。非常停止スイッチは、JIS B 9960-1(IEC 60204-1) 及び JIS B 9703(ISO 13850)の要求を満足しなければならない。

ウ　コントロール用機器

安全関連制御システムにおいて、安全スイッチやセンサの入力信号を受けて、安全確保のために適切な動力、軸の停止や減速等の運転モード切替の指示を行う。プログ

図 5-6 非常停止スイッチの例(IDEC ホームページより)

ラムが不要な安全リレーユニットと、安全制御方策をプログラムする安全コントローラ/安全 PLC(シーケンサ)がある。

以前は、安全制御方策が簡単であったため、安全コントロール用機器への要求は少なかった。その後、機能安全技術の高度化とともに停止や減速、起動条件などを細かく制御したい要求が多くなり、安全コントローラ/安全 PLC が多く使われるようになってきた。

なお、ロボットコントローラが安全性能要求を満たした保護停止や安全適合監視速度の機能を持つ場合もあるが、本書ではそれらを安全コントローラ/安全 PLC とは区別するものとする。

JIS B 8344-2 (ISO 10218-2)では、協働作業ロボットの安全関連電気制御システム(SRECS)には、JIS B 9705-1(ISO 13849-1)カテゴリ 3/PLd、又は JIS B 9661(IEC 62061) SIL2 以上を要求している（第 4 章参照）。

図 5-7　安全リレーユニット、安全コントローラ、安全 PLC の例
（三菱電機ホームページより）

エ　インタロック用機器

インタロック用機器は、可動ガードや扉の開閉状態と施錠/解錠の監視と、それに応じたロボットの起動と停止を制御する。例えば、ロック機構付き安全スイッチ、安

図 5-8 インタロック用機器（ガードインタロックスイッチ）
（オムロンホームページより）

全(ドア)スイッチやセーフティリミットスイッチがある。インタロック用機器は、JIS B 8344-1(ISO 10218-1)、5.2.1 の要求を満足しなければならない。

オ　侵入検知/存在検知用機器

セーフティライトカーテン、セーフティレーザースキャナなどの危険区域や制限区域に作業者が侵入した、又は作業者が存在していることを検知するセンサである。特に、協働作業用ロボットにおいて安全防護(ガード)を設置したくなければ、侵入検知/存在検知用機器を用いてリスク低減を行わなければならない。

また、保護停止等におけるロボット停止位置の監視に、ライトカーテンを使用することもある。ライトカーテンを位置監視平面とみなして、ロボットがライトカーテンを越えるとロボットを停止する。

セーフティライトカーテン

レーザースキャナ及びセーフティマットスイッチ

図 5-9　侵入検知/存在検知用機器(オムロンホームページより)

いずれの場合も、安全関連制御システムとしての安全性能要求を満足しなければならない。

(2) リスク低減事例

これらの安全コンポーネントを使用した典型的なリスク低減方策については、第 8 章の事例で述べる。以下の事例について紹介する。

・施錠式ガードによる機械の起動/停止：施錠式インタロック
・ペンダントによるロボットティーチング：3 ポジションイネーブルスイッチ
・ライトカーテンによる侵入検知：ライトカーテン
・レーザースキャナによる存在検知：レーザースキャナ
・ロボットの安全速度制限(SLS)
・ロボットの安全位置制限(SLP)

4 ロボットシステムの設計手順

(1) アーキテクチャ構成

最初に検討するのは、リスクアセスメントのリスク低減方策を、入力/処理/診断/出力などのサブ機能に分割して、それらをロボットの安全関連機能及び/又はロボット外部の安全コンポーネントにどのように割り当てるかである。

ロボットの安全機能が豊富な場合、適切なセンサやスイッチ類の追加だけでリスク低減が達成できる。一方、リスク低減方策としての安全機能が多様で複雑である場合、あるいはロボットの安全機能が少ない場合、ロボット外部のリスク低減方策が増える

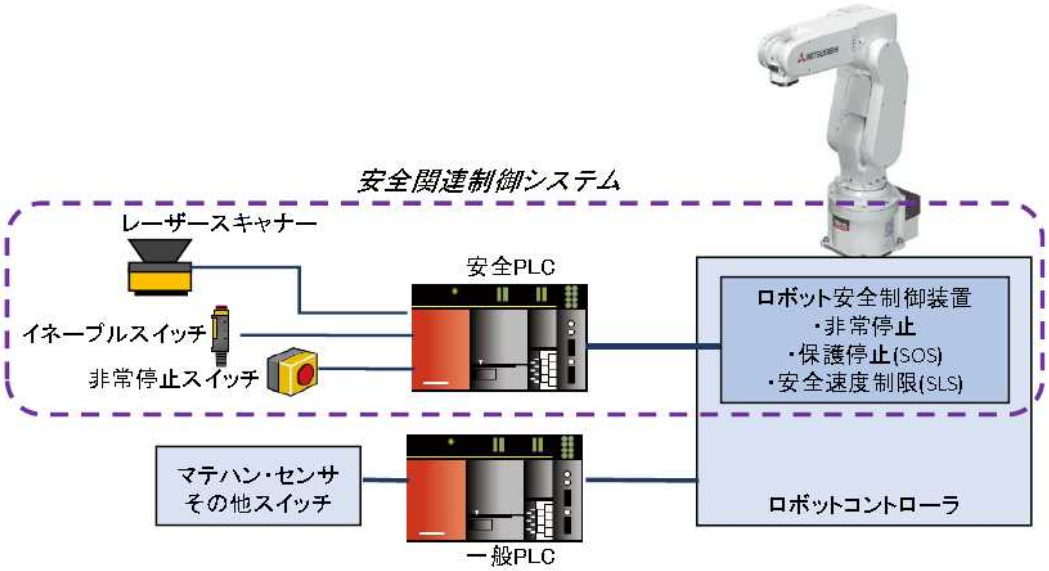


図 5-10　協働作業ロボットの安全関連制御システムの構成例

だろう。

典型的な、協同作業ロボットの安全関連システムの構成例を図 5-10 に示す。保護停止や安全適合監視速度は、ロボット安全制御装置が担当するので、安全 PLC はそれらの条件判定とモード指示、および非常停止要求を制御する。

(2) 安全コンポーネントの選定

安全関連制御システムの機能をサブ機能に分割し、最終的には安全コンポーネントに機能を割り付ける。そのとき、安全コンポーネントの安全性能(PL/SIL)に注目し、要求性能を達成できるような安全コンポーネントを選択しなければならない。安全性能を達成するために、多重化や診断が必要な場合があるので、製品仕様を考慮する。

例えば、ライトカーテンは自己診断能力によりタイプ 2 とタイプ 4 があるが、協働作業ロボットの安全性能要求 PL=d/SIL2 を満足できるのはタイプ 4 である。

(3) 安全関連ハードウェア

協働作業ロボットの安全関連システムの回路又は装置を、インテグレータ又はユーザが開発することは、ほとんどないと考える。理由は、安全関連システムのハードウェアを JIS C 0508 機能安全規格に従って開発するには、開発工数と期間を必要とするためである。本書では、安全関連ハードウェアの開発方法については言及しない。

(4) 安全関連ソフトウェア

ここで作成する安全関連ソフトウェアとは、安全 PLC が実行する安全制御プログラムのことである。安全 PLC の安全制御プログラムは、安全 PLC 供給者が提供する専用プログラミングツールまたはエンジニアリングツールにより作成する。記述する言語は、PLC でよく使われる言語の、ラダー(LD)またはファンクションブロック(FBD)であることが多い。

ア 安全運転方案（安全要求仕様書）

安全制御によるリスク低減方策を検討すると、ロボットシステムの安全関連の運転操作に関する方案が列挙できる。これを、安全運転方案として安全要求仕様書にまとめる。妥当性確認では、実現した安全関連システムがこの要求を達成したかどうかを確認する。

イ ソフトウェア仕様書

ソフトウェア仕様書は、安全要求仕様を実現するための具体的な実現仕様を設計する。入出力デバイスアドレス、変数/シンボル、処理(ロジック)などを明確にする。また、これらの設計が安全要求仕様書をすべての要求を満足しているかの検証を行う。この検証は、設計レビューとして実施される。

安全関連システムが簡単な場合、プログラミングツールにより安全制御プログラムを作成し、ツールが生成するドキュメントをソフトウェア仕様書としてもよい。この場合も設計レビューは必須である。

ウ　プログラム(コーディング)

プラグラムのバージョン管理は重要である。検証および妥当性確認が不十分な安全関連プログラムの出荷は、障害の要因となる。誰が何の権限で承認してリリースするか、安全 PLC 実機にダウンロードするかをルール化しておくことが必要である。

エ　モジュール試験/結合試験

安全 PLC のプログラミングツールは、プログラムのシミュレーション機能を備えていることが多く、安全 PLC 実機を用いることなくモジュール試験を行うことができる。試験結果は文書化する。

結合試験は安全 PLC にプログラムをダウンロードして、機能や性能を試験する。ただし、この時点でロボットシステム全体が完成していない場合、すべてのソフトウェア試験を完了できない。この場合は、最終的な据付時において試験を実施するための計画をたてなければならない。

オ　妥当性確認

ソフトウェア妥当性確認は、安全制御プログラムが安全要求仕様を満足したかを確認する。安全ソフトウェアの責任者が最終リリース試験で確認できるものと、PL/SIL の達成のように設計仕様書から確認できるものがある。妥当性確認の内容と結果は、文書化しなければならない。

(5)　ハードウェアとソフトウェアの結合試験

安全関連制御システムは、最終的には協働作業ロボットとして据付けた状態で、妥当性確認を行わなければならない。一般に、この作業はロボットシステムインテグレータとユーザにより実施される。妥当性確認において是正措置が必要な場合は、その是正措置について文書化し、使用上の情報として提供しなければならない。

最終的な据付け以前に、安全関連制御システムのハードウェア、ソフトウェアの結合試験が可能な場合は、両者の開発(納入)責任者により試験を実施できる。この試験結果は文書化され、上記の妥当性確認に提供されなければならない。

第６章　使用上の情報

１　　概要

ISO/TS 15066 と ISO 10218-2（JIS B 8433-1）は、産業用協働ロボットシステムの使用者に対して、以下の使用上の情報を提供することを求めている。またこれに限定せず、リスクアセスメントの結果などに基づき、使用者にとって必要な情報を提供する必要がある。

尚、ISO 10218-1（JIS B 8433-1）が要求する使用上の情報については、本書では省略する。

２　取扱説明書への記載事項

以下の内容を漏れなく記述する。

ア　輸送・保管

a）機械毎の保管条件
b）寸法，質量，及び重心の位置
c）輸送に関する表示（例えば，つり上げ装置のつり位置を示した図面）

イ　設置、立上げ、検収、引渡し、及び移管

a）固定及び振動減衰の要求事項
b）組立及び取付条件
c）使用及び保全に必要な空間
d）許容できる環境条件（例えば，温度，湿度，振動，電磁放射）
e）ロボットシステムを動力供給源に接続するための指示（特に，電気的過負荷に対する保護について）
f）廃棄物の撤去及び廃棄についての助言
g）必要な場合は，使用者が応じなければならない保護方策についての推奨（例えば、追加が必要又は一時的に必要な ISO 12100（JIS B 9700）で規定する安全装置，安全距離，安全標識及び信号）
h）最初の使用及び生産に投入する前に，ロボット及びその保護方策の初期試験並びに検査をどのように行うかについての指示事項（低減速度制御の機能的試験を含む。）

ウ　運転開始の手順

a）動力の供給前の検証内容

1）ロボットは，適切に，機械的に据え付けられ，安定している。

2）電気的接続は正しく，かつ，電源（すなわち，電圧，周波数，電波妨害レベル）は，規定値内である。

3）適切な電気的接地（等電位）がされている。

4）制御システムの安全関連部品は，適切に設置されている。

5）他のユーティリティ（例えば，水，エア，ガス）は，適切に接続され，規定値内にある。

6）インタロックを含む周辺設備は，適切に接続されている。

7）制限空間を確立する制限装置（利用されているとき）は，設置されている。

8）適切な安全防護手段が適用されている。

9）物理的な環境が明記されている（例えば，照明及び騒音のレベル，温度，湿度，大気の汚染物質）。

10）妥当性が確認された全てのプログラム（通常の制御及び安全関連）の適切なバージョン（変更管理された）がインストールされている。

b）動力開始後の検証内容

1）起動，停止及びモード選択（施錠付きスイッチを含む。）の制御装置が，意図したとおりに機能する。

2）意図したとおりに，各軸は動作し，制限されている。

3）非常停止回路及び保護停止回路（含まれている場合）並びにそれらの装置が機能している。

4）外部動力源の切離し及び隔離が可能である。

5）教示及びプレーバック能力が正しく機能する。

6）環境条件の両立性［例えば，爆発，腐食，湿度，ちり（塵），温度，電磁妨害（EMI），無線周波数妨害（RFI），静電気放電（ESD）］が考慮されている。

7）全ての安全防護装置，保護装置，イネーブル装置及びインタロックが，意図したとおりに機能する。

8）その他の全ての安全防護（例えば，バリア，警告装置）が適切に配置されている。

9）手動モードにおいて，ロボットは適切に動作し，生産物又はワークピースを扱える。

10）自動運転（通常運転）において，ロボットは適切に動作し，定格速度及び定格負荷で意図したタスクを実行できる。

エ　システムの情報

a）システム，附属品，ガード及び／又は保護装置の詳細な記述

b）禁止されている使用方法を含めて，ロボットシステムが目的とする用途の包含

する範囲。本来のロボットシステムのバリエーションがある場合には，それを考慮する。

c) 制御システム及びその安全度水準，安全回路として独立した停止回路，安全コントローラ，並びに安全な通信によって実行される安全機能を記載した安全要求仕様書。それらに関連する安全関連システムの性能

d) その他の制御器機能，操作盤，教示ペンダント，イネーブル装置及び認識用表示器

e) 図表（レイアウト，制御，電気，液圧，空圧など）

f) 例えば，発生する放射，ガス，蒸気，ちり（塵），並びに，振動等の他の危険源に関係するデータ及び使用した測定方法に関する記述

g) 電気的設備についての技術的な文書

h) 等電位ボンディング（接地）要求事項の仕様書。電気的接地（等電位）は，IEC 60204-1（JIS B 9960-1）に従って設けなければならない。

i) ロボットシステムが強制力のある要求事項に適合していることを証明する文書

j) 構成する機械に元からあった保護方策の修正

k) エンドエフェクタ（アーム先端のツール）負荷分析，エネルギー喪失の事象があったときの動き，人の介在への考慮，保全及び想定される寿命

l) 他の機械に対するインタフェース要求事項

m) 動的制限区域の位置

n) システムの想定される寿命

o) 非常停止装置の制御範囲に関しての情報

p) ケーブルレス又は取外し可能な装置（ワイヤレスペンダントなど）の使用時、保管方法とシステム設計上の情報

q) アプリケーションで協働ロボットを使用するための仕様データ（説明，図，及び写真）

r) 協働作業空間及び作業場全体に適用される安全防護物，並びに協働ロボットシステムの記述及び仕様データ

s) 協働運転の関連する種類の選択及び選択解除のための制御の記述

t) 空間的な環境状態，入口，出口及び交通路の記述

u) 機器，設備，機械，機器のオプション品，ツール及びロボットシステムのそれらを含むアプリケーション並びにそれらの位置決めに関連する作業エリア内で見られる生産財の記述

v) 詳細な図面と写真

w) 作業タスクに関する全作業活動の時系列に順序だてした仕様書，特に協働作業空間内のもの

x) 全作業タスク局面におけるロボットと人間の危険な距離の測定に関する文書

y) ロボットの型式、及び協働ロボットアプリケーションの簡単な説明

z) 作業場アプリケーションの説明（協働ロボットを含む作業場の名称）

オ　システムの使用

a）残留リスク，設計者が採用した保護方策では除去できないリスク

b）あるアプリケーションにとって，ある附属品の使用によって，及びそのようなアプリケーションに必要な特有の安全防護装置に関連して発生する可能性がある特定のリスク

c）予見可能な誤使用及び禁じられている使用法

d）材料の流れ

e）意図した使用

f）タスク区域及び関連した残留リスク（ISO 11161 参照）

g）オペレータのタスク，タスクを行うための位置及び経路

h）種々の制御及び保護装置（例えば，保護装置，保護装置のリセット，イネーブル装置，非常停止，制御ステーション，切離し手段）の制御の範囲（ISO 11161 参照）

i）手動操作部（アクチュエータ），イネーブル装置，保護停止の詳細記述

j）セッティング及び調整

k）停止（特に，非常停止）のモード及び手段

l）不具合（障害）の同定及び位置の特定，修理並びに介入後の再スタート

m）使用及び訓練が必要な保護具

n）安全機能に影響の可能性のある構成部品の変更又は付加設備（ハードウェア及びソフトウェアの両方）の追加後に必要な試験／調査の指示

o）切り離されたペンダントは接近できる状態から取り除かなければならないことの説明

p）システム設備の不具合（障害）及び非常事態の復帰のための指示

q）遠隔制御運転のための訓練要求事項

r）無効な非常停止の使用を防ぐために，使用していないケーブルレスペンダントの保管場所及び設計

s）安全関連設備の定期的な機能試験の要求事項

t）プロセス独特の消耗品の適切な選択，準備，使用目的及び保全に関しての手引

u）エンドエフェクタの故障が潜在的に危険状況となる場合は，通常運転での想定できるパラメータを基に，エンドエフェクタの意図した製品寿命

v）タスクに要求される照明のレベル

w）動的制限区域の場所、及びロボットに組み込まれた安全適合ソフト軸及び空間制限機能を，ロボット製造業者の指示に従って使用する場合，それらの手段によって確立したプログラムされた制限についての情報

x）リモートアクセス機能を有する場合、遠隔タスクのために遠隔及び局所オペレータの両方の訓練のための適切な要求事項

y）オペレータの関連する全作業活動，又は運転の記述

z）協働ロボットシステムの関連する作業活動又は運転の記述

カ　保全

a）安全機能の検査の項目及び頻度

b）一定の技術的知識又は特定のスキルが必要な保全作業は，技能がある人だけ（例えば，保要員，専門家）が行うのが望ましいことの説明

c）特定のスキルを必要としない保全作業（例えば，消耗部品の交換）は，使用者（例えば，オペレータ）が行ってもよいことの説明

d）保全要員がタスクを合理的に行うことができる図表及び図面（不具合発見のタスク）

e）安全関連部品を交換するための情報（製造部品番号，部品の仕様）

f）部品交換の定められた製造業者への連絡のための情報

g）エネルギー制御及び分離が必要なタスク

h）安全防護装置の手動による中断に対する安全作業実施

キ　使用中止

a）使用中止，解体及び廃棄に関連する情報

ク　非常事態

a）使用する消防設備の情報

b）有害物質の放出又は漏れの可能性についての警告

c）非常事態の影響を阻止する手段（実施可能な場合）

d）駆動力を用いない非常時又はロボットの異常な動作に対するロボット製造業者からの指示とともに，ロボットシステム関連設備の障害復旧のための詳細な指示

ケ　ロボットの仕様

次の情報が、産業用ロボットの製造者から提供された取扱説明書に記載されていることを確認し、不足していれば製造者へ要求する。特に第三者認証を受けていない産業用ロボットでは、記載漏れが発生しやすいので、注意する。

a）ISO 9946（JIS B 8431） に従う情報

b）ISO 10218-1（JIS B 8433-1） に従う情報

c）該当する場合，ペンダントを使用しての手動高速制御

d）制限装置の設置について，機械的停止制限機能の数，位置及び調整範囲を含めた指示，並びに非機械的制限装置の数，位置，実装及び動的制限（含まれる場合）の機能を含めた指示

e）イネーブル装置の数及び操作についての情報並びに追加の装置の設置に関する説明情報

f）最大変位の 3 軸についての停止時間及び停止距離，又は角度の情報

g) ロボット内部の潤滑，ブレーキ又は伝達システムに使用されている流体又は潤滑油の仕様

h) 動作範囲及び負荷容量の限界を定義する情報（ワーク及びその保持器具の最大質量並びに重心位置を含む。）

i) ロボット及びロボットシステムに適用する関連規格の情報（第三者によって認証されたものも含めて）

j) 該当する場合，ロボットの同時動作及びプログラマ／オペレータに必要な特別な訓練に関する指示

k) 駆動力を用いない非常時又はロボットの異常な動作に対する指示

l) 安全適合ソフト軸及び空間制限機能を使用することによって設定したプログラムされた制限

m) 協働運転用に設計されたロボットシステムに対して，ロボットが協働ロボットとして統合に適していることの宣言

コ　産業用協働ロボットシステムの基本情報

a) メーカ又はインテグレータ（インテグレータが協働ロボットシステムを設計した場合）

b) 試験機関（試験が行われた場合）

c) ロボットの型式，及び協働ロボットアプリケーションの簡単な説明

d) 作業場アプリケーションの説明（協働ロボットを含む作業場の名称）

サ　産業用協働ロボットシステムの仕様

a) アプリケーションで協働ロボットを使用するための仕様データ（説明，図，及び写真）

b) 協働作業空間及び作業場全体に適用される安全防護物，並びに協働ロボットシステムの記述及び仕様データ

c) 協働運転の関連する種類の選択及び選択解除のための制御の記述

シ　産業用協働ロボットシステムの作業空間

a) 空間的な環境状態，入口，出口及び交通路の記述

b) 機器，設備，機械，機器のオプション品，ツール及びロボットシステムのそれらを含むアプリケーション並びにそれらの位置決めに関連する作業エリア内で見られる生産財の記述

c) 詳細な図面と写真

ス　産業用協働ロボットシステムの作業タスク

a) オペレータの関連する全作業活動，又は運転の記述

b) 協働ロボットシステムの関連する作業活動又は運転の記述

c) 全作業活動の時系列に順序だてした仕様書，特に協働作業空間内のもの
d) 全作業局面におけるロボットと人間の危険な距離の測定に関する文書
e) 協働作業空間の記述，又は図面

セ　産業用協働ロボットシステムの動力制限及び力制限

a) 次の事項を含むロボット，ツール及びワークピースに固有の情報
   1) 有効負荷
   2) ロボット可動部の総質量
b) 次の事項を含む，ロボットシステムとオペレータ間で予期され，合理的に予見可能な接触状態
   1) 接触しうる特定の身体部
   2) 接触が過渡的又は準静的かどうかの宣言
   3) 予期される表面エリア又は接触表面に関連した幾何学的状態
   4) 接触に係る最大許容生物力学的限界
c) 提案される選択されたリスク低減の手段
   1) 推奨される能動的又は受動的リスク低減の手段
   2) 安全適合速度制御が使用される場合、安全適合速度の制限値
d) 附属書 A と異なる方策を用いる産業用協働ロボットシステムでは、動力と力の制限機能を設定するために使用される関連データ及び情報

3　産業用協働ロボットシステムに必要なマーキング

産業用協働ロボットシステムは、ISO/TS 15066 と ISO 10218-2（JIS B 8433-2）の要求事項に基づき、システムにマーキングが必要である。マーキングは、記述された内容が目視でき、かつ読みやすく消えないように表示されていなければならない。

- 製造業者の商号及び所在地並びに（該当する場合）公認の代理者
- 機械名称
- シリーズ又は型式の名称
- 製造番号（あれば）
- 製造年（製造工程が完了した年）
- 潜在的に爆発しやすい雰囲気で使用するために設計製作された機械には、それに応じた表示

参照文献

[1] ISO 10218-1:2011 “Robots and robotic devices - Safety requirements for industrial robots - Part 1: Robots”

[2] JIS B 8433-1:2015“ロボット及びロボティックデバイスー産業用ロボットのための安全要求事項－第1 部：ロボット”

[3] ISO 10218-2:2011“Robots and robotic devices - Safety requirements for industrial robots - Part 2: Robot systems and integration

[4] JIS B 8433-2:2015“ロボット及びロボティックデバイスー産業用ロボットのための安全要求事項－第2 部：ロボットシステム及びインテグレーション”

[5] ISO/TS 15066:2016“Robots and robotic devices ―Collaborative robots”

第７章　妥当性確認

１　　概要

妥当性確認は、設計開発した安全関連システム及びその組み合わせが、安全要求仕様及び関連規格の要求事項を満足していることを確認する。協働作業ロボットの場合、この確認は JIS B 8433-1 及び-2（ISO 10218-1 及び-2)の妥当性確認を参照して実施しなければならない。本章では、このふたつの規格の妥当性確認について解説する。

なお、安全関連システムのハードウェア、ソフトウェアの妥当性確認、特に安全性能（PL/SIL）についての妥当性確認については、ISO 13849-2、JIS B 9961（IEC 62061）及び JIS C 0508(IEC 61508)シリーズを参照する。本章の後半では、ISO 13849-2 に基づく PL の妥当性確認方法の概略及び PL 計算ツールについて紹介する。

２　協働作業ロボットの妥当性確認

(1)　ロボット単体の妥当性確認

ロボット製造業者は、JIS B 8433-1（ISO 10218-1)の第４章及び第５章に規定した原則に従って、適切な安全保護装置を含めた協働作業ロボットの設計及び製造の検証及び妥当性確認をしなければならない。

合理的に予見可能な危険源が同定され、修正活動がなされるのであれば、リスクアセスメントの評価について再確認をするのが望ましい。リスクアセスメントは、それぞれのロボットに対して何が適切な保護方策なのかを導き出すものである。

ア　検証及び妥当性確認方法

検証及び妥当性確認は，例えば次の方法によって満足することができる。

JIS B 8433-1（ISO 10218-1)の付属書Ｆ表 F.1 には、規格の要求それぞれについて、以下の A～G のどの方法が適用可能かを示している。表 7-1 に付属書Ｆ表 F.1 の一部を示す。

- A　目視検査
- B　実用試験
- C　測定
- D　運転中の観察
- E　用途特有の計画、回路図及び設計資料のレビュー
- F　タスクに基づくリスクアセスメントのレビュー
- G　仕様書及び使用上の情報

表 7-1　安全要求事項及び方策の検証手段の一部　（JIS B 8433-1（ISO 10218-1 より）

箇条	適用可能な安全要求事項及び／又は方策	検証及び／又は妥当性確認の方法（6.2 参照）						
		A	B	C	D	E	F	G
5.2	一般要求事項							
5.2.1	固定又は可動ガードは，モータ軸，歯車，駆動ベルト又はリンクのような危険源への暴露を防止するように取り付ける。	x			x			
5.2.1	5.2.1 定期的な保全のために,取り外すことを目的とした固定用装置は他の用途に適用できない構造となっている。		x					x
5.2.1	可動ガードは,危険になる前に危険な移動が停止するように危険な移動に対してのインターロックをとる。		x	x	x	x		
5.2.1	インタロックシステムの安全関連制御システム性能は,5.4 の要求事項に適合している。					x		
5.2.2	動力の消失又は変化が，危険源とならない。		x		X	x		
5.2.2	動力の再始動は，動作の始動にならない。		x		X	x		
5.2.2	電気，液圧，空気圧又は真空圧の動力源の消失又は変化が危険源とならない。		x		x			
5.2.2	設計によって保護されない危険源に対して,他の保護方策で保護している。	x						x
5.2.2	予想される使用に対して保護がない危険源は,使用上の情報を明確にしている。						x	x
	...							

イ　要求される検証及び妥当性確認

附属書Ｆ（表 7-1 を含む）は、検証もしくは妥当性確認又はその両方を実施しなければならないロボットの安全性に必要な特定の性能要求事項を表にしたものである。要求事項がロボットの設計・製作に見合ったものであるなら、要求事項はその決定のための評価を適切な方法により実施しなければならない。

なお、表 F.1（表 7-1）にある項目は，それぞれのロボットに全てを適用しなくてもよい。それらの項目には検証及び／又は妥当性確認が不可能であることがあるかもしれない。表 F.1 は包括的でも制限でもない。特定のロボットの設計によっては、追加の検証要求事項があるかもしれない。表 F.1 をチェックリストとして使用するのであれば、その内容は評価されるロボットの構成要素及び評価のための適した方法を、再確認及び限定をする必要がある。

ここで、協働作業ロボットについて、適用可能な項目全てを検証もしくは妥当性確認又はその両方を確実に実施するのは、製造業者の責任である。

(2)　協働作業ロボットシステムの妥当性確認

前節は、ロボット製造業者によるロボット単体の妥当性確認方法について述べた。本節では、ロボットシステムの製造業者又はインテグレータによる協働作業ロボットシステムの妥当性確認の方法について述べる。

ア　一般要求

ロボットシステムの製造業者又はインテグレータは、JIS B 8433-2 (ISO 10218-2) に規定した原則に従って適切な安全防護装置を含めてロボットシステムの設計及び製作の検証及び妥当性確認をしなければならない。

リスクアセスメントは，全ての合理的に予見可能な危険源が同定され，是正処置がされていることが再確認されることが望ましい。

JIS B 8433-2 (ISO 10218-2)附属書 A（本書表 3-8 参照）で同定している危険源の全てをそれぞれのロボットに適用はしないので、もたらされた危険状態に関連する危険のレベルは、ロボットシステム間では同じではなく、また、ロボットシステムの特定のアプリケーションには、附属書 A で同定されていない危険源が含まれている。リスクアセスメントは、保護方策の対象となるロボットシステムのためにどのような保護方策が適切であるかの決定を導くのに必要である。

イ　検証及び妥当性確認の方法

検証及び妥当性確認は、次の事項に含まれる方法によって満たすことが可能であるが、限定はしない。JIS B 8433-2 (ISO 10218-2)付属書 G 表 G.1(一部を表 7-2 に示す）には、各要求事項が下記 A～I のどの手法によって確認できるかを示している。

- A 目視検査
- B 実際の試験
- C 測定
- D 運転中の観察
- E アプリケーション特有の概要図，回路図及び設計資料の再確認
- F 安全関連のアプリケーションのソフトウェア及び／又はソフトウェア文書の再確認
- G タスクベース・リスクアセスメントの再確認
- H レイアウト図及び文書の再確認
- I 仕様書及び使用上の情報の再確認

表 7-2　安全要求事項及び方策の検証手段の例（JIS B 8433-2（ISO 10218-2)付属書 G 表 G.1 より）

箇条	安全要求事項及び／又は方策	検証及び／又は妥当性確認の方法（6.2 参照）								
		A	B	C	D	E	F	G	H	I
5.2	安全関連制御システムの性能（ハードウェア及びソフトウェア）									
5.2.1	性能能力，性能決定のためのデータ及び基準を使用上の情報に表明。	x								x
5.2.2	性能が PL＝d，カテゴリ 3 のアーキテクチャ。					x	x			x
5.2.2	性能が SIL2，プルーフテスト間隔が 20 年以上でハードウェ					x	x			x

	アフォールトトレランスが 1。									
5.2.3	性能決定のために使用されるリスクアセスメントの結果。							x		x
5.3	設計及び配置									
5.3.1	条件に基づいて設計され，選択されたシステム。	x		x						x
5.3.2	自動モード選択は，安全防護空間の外でなければならない。	x	x			x				
5.3.3	作動制御装置は，JIS B 9960-1 の要求事項を満足している。	x								
5.3.3	ロボットシステムは，危険状態を引き起こすどのような外部の遠隔指令又は条件にも反応してはならない。		x		x					
	...									

ウ　必要な検証及び妥当性確認

JIS B 8433-2 (ISO 10218-2)附属書Gは、検証又は妥当性確認をしなければならないロボットシステムの安全性に不可欠な特定の性能要求事項の一覧表である。適切な方法を使用して、要求事項がシステムの設計及び製作が要求事項を満足しているかを決定するために、要求事項を評価しなければならない。

なお、表 G.1（表 7-2）の項目の全てをロボットシステムごとに適用する必要はない。項目によっては検証及び／又は妥当性確認が不可能なものがある場合がある表 G.1（表 7-2）は，包括的なものでも、制限するものでもない。特定のロボットシステムの設計によっては、追加の検証要求事項がある場合がある。表 G.1（表 7-2）をチェックリストとして使用する場合は、その内容を再確認し、評価する実際のロボットシステムの構成及び適切な評価方法を限定する必要がある。

全ての該当項目の検証及び／又は妥当性確認を確実に行うことは、インテグレータの責務である。

エ　保護設備の検証及び妥当性確認

ロボット製造業者の指示と一致した方法で行い、ロボットシステムに適切に適用して同定された危険源を軽減するように設置された保護設備かどうかを検証しなければならない。

危険源への接近を防ぐには、次の方法で達成しなければならない。

1)接近する前に危険源をなくす。

2)意図しない運転からの危険源の発生を防ぐ。

3)部品及び工具の飛散を防止する。

4)プロセス上の他の危険源（例えば、騒音、レーザ、放射線など）を制御する。

設置された保護設備は、次の事項を検証しなければならない。

1)ガードの種類、開口部の寸法、ガードの配置、適切な安全距離、高さ

2)安全防護空間内から作動が可能でないリセット制御

3)保護装置の種類、検出能力、保護装置の配置、適切な安全距離、大きさなど

4)バイパス及びミューティング機能

付加保護方策があることを検証しなければならない。

1)説明書

2)訓練資料

3)警告

4)保護具

5)手順書

6)その他の適切な方策

3　要求安全度水準(SIL/PL)の適合性評価

SIL/PL への適合性では、PFDd/PFHd あるいは MTTFd、DCavg の数値指標に目がいくが、それだけが SIL/PL の要求ではない。JIS C 0508-2(IEC 61508-2)付属書 A や JIS C 0508-3(IEC 61508-3)付属書 A、B には、安全関連部の開発において採用すべき手法が SIL 毎に示されている。SIL/PL の性能を達成するためには、これらの開発手法や技法についての要求も満足しなければならない。

これらの要求への対応方法は、開発計画書(V&V プラン)あるいは設計仕様書、試験仕様書に記載されているので、その内容を確認する。別の方法で代替した場合は、その妥当性について判断する。この判断には、規格要求からチェックリストを作成し、要求への対応を記載する。

SIL2 チェックリストの例を表 7-3 に示す。この表は、JIS C 0508-2 表 A.16（決定論的原因故障を管理するための技法）の SIL2 要求の一部を抽出したものであり、要求度 M は必須(Mandatory)、HR は強く推奨(Highly Recommend)、R は推奨(Recommend)を意味する。表右側の対応は、具体的な対応方策について記述した文書及び該当箇所を記載する。

これらのチェックリストにより、安全関連システムの安全性能(SIL/PL)を達成できたかどうかの妥当性確認を一覧的に実施できる。

表 7-3　SIL2 要求適合チェックリストの例（JIS C 508-2 表 A.16 に基づく）

表 A.16−環境上のストレス又は影響によって生じる決定論的原因故障を管理するための技法及び手段			
ID	技法または手段	要求度	対応
1	危険側故障をもたらすことがある電源喪失，電圧変動，過電圧，低電圧，交流電源周波数変動などの現象に対する手段	M	
2	通信線からの電力線の分離	M	
3	電磁イミュニティの増大	M	
4	物理的環境（例えば，温度，湿度，水，振動，ほこり，腐食性物質）に対する手段	M	
5	プログラムシーケンス監視	HR	

４　PL（Performance Level）

ここでは、安全度水準の定量的指標のひとつである、JIS C9705-1（ISO 13849-1）の PL の計算方法について説明する。詳細は、ISO 13849-2 を参照してほしい。

(1)　カテゴリ

カテゴリとは、障害に対する抵抗性および障害発生後の安全関連システムの挙動に関する分類である。カテゴリは、その構造的配置、障害検出および信頼性によって 5 段階（B、1～4）に決定される。カテゴリの詳細は、「機能安全活用テキスト」にあるので、ここでは言及しない。

(2)　MTTFd (Mean Time to Dangerous Failure)

MTTFd とは、安全関連システムが危険側故障を起こすまでの平均時間のことである。

部品は、その使われ方によって故障率の考え方がふたつある。ひとつは、電気・電子部品のように連続的に使用することによる経年劣化による故障である。連続稼働時間と各部品の危険側故障率から MTTFd が決まる。一方、スイッチやリレー接点は、作動回数によって劣化する。動作要求頻度によって MTTFd が決まる。

MTTFd の値は、メーカからの公表値または JIS B 9705-1 付属書 C、D を参照する。表 7-4 にメーカ公表値の例を示す。

表 7-4. MTTFd と B10d の値の例（オムロンホームページより）

品名	型式	安全機能	B10d(回)	MTTFd(年)	備考
非常停止ボタンスイッチ	A22E	NC接点出力	1.00E+05		NC接点は IEC 60947-5-1 (直接開路動作機構)に適合しています。
	A165E	NC接点出力	1.00E+05		NC接点は IEC 60947-5-1 (直接開路動作機構)に適合しています。
インターロックスイッチ	D4NS	NC接点出力	2.00E+06		Type 2 (ISO 14119)のインターロックスイッチとして使用できます。NC接点は IEC 60947-5-1 (直接開路動作機構)に適合しています。
	D4SL	NC接点出力	2.00E+06		Type 2 (ISO 14119)のインターロックスイッチとして使用できます。NC接点は IEC 60947-5-1 (直接開路動作機構)に適合しています。
安全リレーユニット	G9SA-301			100	
	G9SA-321-T			100	瞬時出力部
	G9SA-321-T			68	オフディレー出力部

ア　スイッチ・接点の MTTFd

具体的には、全数の 10%が危険側故障となる動作回数である B10d という値から MTTFd を求める。ここで、MTTFd を得るには、その部品の一年間当たりの動作回数(Nop)を決めなければならない。すなわち、非常停止スイッチ等の動作頻度を想定しなければならない。

MTTFd = B10d/0.1×Nop　　Nop = dop×hop×3600/tcycle　　（式１）

tcycle　：1 操作サイクルの平均時間間隔　（単位：秒/サイクル）

hop　：1 日あたりの稼動時間（単位：時間/日）

dop：年間の稼動日数（単位：日/年）

イ　２チャンネルの MTTFd

入力＝論理部＝出力のように、安全関連システムが要素の直列構成となっている場合、安全関連システムの MTTFd は要素それぞれの $MTTFd_i$ から計算できる。

$MTTFd = 1/\Sigma(1/MTTFd_i)$

この安全関連システムが２チャンネル構成(2 out of 2)の場合、その全体の MTTFd は次式となる。ここで、MTTFd1, MTTFd2 は各チャンネルの MTTFd である。

MTTFd ＝ 2/3[　MTTFd1 ＋ MTTFd2 － 1/(1/MTTFd1＋1/MTTFd2)]　　（式２）

表 7-5 MTTFd の分類

分類	MTTFd の値
低	3 年≦MTTFd＜10 年
中	10 年≦MTTFd＜30 年
高	30 年≦MTTFd＜100 年

例えば、2 チャンネルが同一の場合(MTTFd1＝MTTFd2)、MTTFd＝MTTFd1＝MTTFd2 となる。このことから、2 チャンネルの簡易的な MTTFd 計算方法として、2 チャンネルのうち小さい値を全体の MTTFd とすることも認められている。

MTTFd は、その値によって３段階（低/中/高）に分類される（表 7-5)。

(3)　DC (Diagnostic Coverage)

安全関連システムの危険側故障を回避するには、構成部品の危険側故障を可能な限り診断することである。この危険側故障率の診断率、すなわち要素の全危険側故障率(分母)に対する診断可能な故障率(分子)を DC と呼ぶ。

DC は要素に対して採用する診断手法に依存する。代表的な診断手法の DC は、JIS B 9705-1(ISO 13849-1)に記載されている。そのため、要素ごとに DC は異なる値となるため、安全関連システム全体を評価する場合は、平均値の DCavg を用いる。

DCavg は各要素の MTTFdi と DCi から求めることができる。さらに、DC は 4 つのレベル(None, Low, Medium, High)に分類される（表 7-6)。

$$DCavg = \Sigma(DC_i/MTTFd_i)/\Sigma(1/MTTFd_i) \quad (式３)$$

表 7-6　DCavg の分類（JIS B 9705-1 表 6）

DCavg	
None	DCavg<60%
Low	60%≦DCavg<90%
Medium	90%≦DCavg<99%
High	99%≦DCavg

(4)　CCF(Common Cause Failure)

共通原因故障(CCF)は，安全関連システムの二重化チャンネルにおいて共通の原因となる危険側故障である．例えば、温度や電気ノイズなどの環境条件、両チャンネルが同じソフトウェアを使っていた場合のバグなどがある。もちろん、二重化チャンネルが効果を発揮するためには、CCF をできる限り回避しなければならない。

JIS B 9705-1 (ISO 13849-1)は、CCF を回避するための手法を紹介している。各手法に点数(スコア)をつけ、採用した手法の合計スコアが 65 点以上になることを要求している。これは、カテゴリ２以上の二重化チャンネルにおいて必須要求である。スコアの見積もり例を表 7-7 に示す。

表 7-7　CCF の見積もり（JIS B 9705-1(ISO 13849-1)表 F.1）

No.	アイテム	制御回路のスコア	最大可能なスコア
1	分離と隔離		
	信号系統間の物理的分離	15	15
2	多様性(ダイバシティ)		
	異なる技術／設計や物理的原則が使用されている	20	20
3	設計／アプリケーション／経験		
3.1	過電圧、過圧力、過電流などの保護	無	15
3.2	十分吟味されたコンポーネントが使用されている	5	5
4	アセスメント／分析		
	故障モードと影響分析の結果が、共通原因故障の防止に、設計上考慮されているか？	5	5
5	能力(適格性)／訓練		
	設計者／保守作業者は、共通原因故障の原因と結果を理解するための訓練を受けているか？	なし	5
6	環境		
6.1	適切な規格に準じたCCFに対する汚染の防止と電磁両立性(EMC)	25	25
6.2	その他の影響 温度、衝撃、振動、湿度など(関連する規格で規定)、すべての関連する環境的影響への耐性要求事項は考慮されているか？	10	10
	合計	80	最大100

(5)　PL の評価

安全関連システムの PL は、これまで述べた４つのパラメータ（カテゴリ、MTTFd、DCavg、CCF）によって求めることができる。例えば、表 7-8 と図 7-1 から PL を求めることができる。図表中に CCF の記載がないが、カテゴリ２以上の二重化アーキテクチャに対する必須要求である。

こうして導き出した安全関連部の PL が、該当安全機能の PLr を達成したかを評価して、妥当性確認を行う。もし、PLr を達成していなければ安全関連部の設計を見直すか、制御系とは別のリスク低減方策を選択する。なお、妥当性確認と評価の結果は文書化しなければならない。

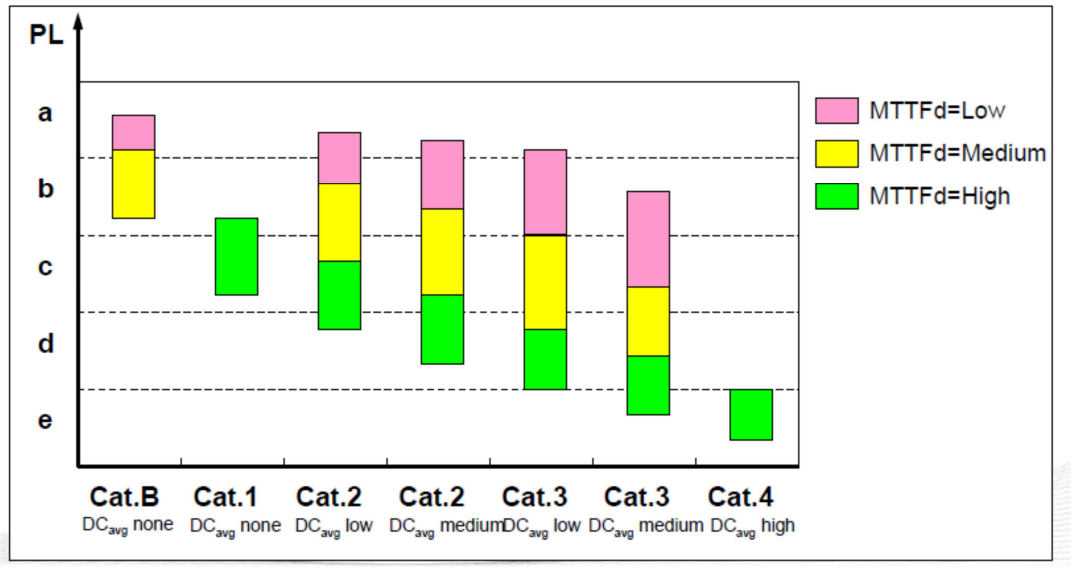


図 7-1　カテゴリ、DCavg、MTTFd と PL の関係　（JIS B 9705-1 図 5）

表 7-8 カテゴリ、DCavg、MTTFd と PL の関係（JIS B 9705-1 表 7）

カテゴリ	B	1	2	2	3	3	4
DCavg	なし	なし	低	中	低	中	高
各チャネルの MTTFd							
低	a	―	a	b	b	c	―
中	b	―	b	c	c	d	―
高	―	c	c	d	d	d	e

５　SIL（Safety Integrity Level）

JIS B 9705-1 (ISO 13849-1)の PL と並んでよく使われている安全度水準の指標が、JIS B 9961 (IEC 62061)の SIL(Safety Integrity Level)である。SIL も PL と同様に、対象機械のリスクアセスメントを行って、安全機能ごとの要求 SIL を決め、安全関連システムの設計後に SIL を満足したか妥当性確認を実施する。

PL と SIL の対応関係を表 7-9 に示す。SIL4 に対応する PL は定義されていない。SIL4 はガス爆発など多数が致命傷に至るリスクであるが、機械設備ではそのような事故はないためである。

表 7-9　PL と SIL の関係　（JIS B 9705-1 (ISO 13849-1) 表 4）

PL	SIL 高／継続運転モード
a	-
b	1
c	1
d	2
e	3

(1)　安全側故障比率(SFF: Safe failure fraction)

SFF はあるサブシステムにおいて、危険側故障にならない故障の割合であり、次式で表される。分子は、検出できない危険側故障率、分母は全故障率である。

$$SFF = (\Sigma\lambda_S + DC \times \Sigma\lambda_D)/(\Sigma\lambda_S + \Sigma\lambda_D) \qquad (式４)$$

λS：安全側故障率

λD：危険側故障率

DC：診断率

(2)　ハードウェアフォールトトレラント(HFT:Hardware Fault Tolerant)

HFT=N とは、そのサブシステムにおいて N+1 個の故障によって安全機能の失敗を起こし得ることを意味する。二重化構成なら、HFT=1 であり、三重化なら HFT=2 となる。

HFT と SFF により、そのサブシステムが達成できる SIL の上限が決められており、表 7-10 に示す。この表による SIL 上限は、PFH_D の値に優先する。

表 7-10 HFT と SFF による SIL 上限（JIS B 9961 (IEC 62061)表 5 より）

SFF	HFT		
	0	1	2
SFF＜60%	許されない	SIL1	SIL2
60%≦SFF＜90%	SIL1	SIL2	SIL3
90%≦SFF＜99%	SIL2	SIL3	SIL3
99%≦SFF	SIL3	SIL3	SIL3

(3) 共通要因故障(CCF)

PL と同じ概念であり、JIS B 9961 付属書 F のチェックリストから、その手法を採用していれば得点を加算していき、得点から CCF 係数（β）を求める（表 7-11）。CCF 係数は、二重化構成の PFH_D 計算において用いられる。

表 7-11 CCF 係数（β）の推定（JIS B 9961(IEC 62061)表 F.2 より）

合計得点	CCF 係数（β）
＜35	10%
35 - 65	5%
65 - 85	2%
85 - 100	1%

(4) PFH_D (Probability of dangerous failure per hour)

PFH_D とは、安全関連システムが 1 時間あたりに危険側故障を起こす確率である。PFH_D の計算は、アーキテクチャによって異なる。

診断機能を持たないサブシステムの直列構成の場合、いずれかの危険側故障によって全体システムが危険側故障に陥るので、PFH_D は次式で示される。

$$PFH_D = \Sigma\lambda_{Di} \quad （式５）$$

λ_{Di}：サブシステム i の危険側故障率

各サブシステムが診断率 DCi の診断機能を持つ場合、上式は未検出危険側故障について考慮すればよいので、次式となる。

$$PFH_D = \Sigma\lambda_{Di}(1 - DC_i) \quad （式６）$$

λ_{Di}：サブシステム i の危険側故障率

DC_i：サブシステム i の診断率

二重化アーキテクチャの場合、各チャンネルにおいて診断機能を持たない場合、次式となる。ここで、プルーフテスト間隔とは、サブシステムに未検出危険側故障が蓄積していないこと、すなわち新品同様であることを確認するプルーフテストの実施間隔である。

$$PFH_D = (1-\beta)^2 \times \lambda_{D1} \times \lambda_{D2} \times T_1 + \beta(\lambda_{D1} + \lambda_{D2}) \quad （式７）$$

β：CCF 係数

λ_{D1}、λ_{D2}：チャンネル 1、2 の危険側故障率
T_1：プルーフテスト間隔またはサブシステムの寿命のいずれか短い方

診断機能付き二重化アーキテクチャの場合、計算式はより複雑になる。二重化チャンネルが同じ設計のサブシステムである場合は、以下の式となる。

$$PFH_D=(1-\beta)^2\{\lambda_D^2\times DC\times T_2+[\lambda_D^2\times(1-DC)]\times T_1\}+\beta\lambda_D \quad (式８)$$

T_2：診断テスト間隔

これらの式から、安全関連システムの PFHD を求め、表 7-12 に示す範囲を満足すればよい。

表 7-12　SIL 毎の要求 PFH_D

SIL	PFH_D
SIL3	$10^{-8} \leqq PFH_D < 10^{-7}$
SIL2	$10^{-7} \leqq PFH_D < 10^{-6}$
SIL1	$10^{-6} \leqq PFH_D < 10^{-5}$

６　評価ツール

(1)　PL 計算ツール SISTEMA

SISTEMA ソフトウェアツールは、JIS B 9705-1 (ISO 13849-1)に従った安全評価のための包括的な支援を提供する。SISTEMA は、指定のアーキテクチャに基づいた安全関連制御コンポーネントの構成をモデル化する。そして、安全関連システムが達成する PL をはじめ、多様な詳細レベルに応じた信頼性値を自動的に計算する。

操作方法は、本章の PL において説明した各種パラメータ（カテゴリ、MTTFd、DCavg、CCF）を、ブロックまたはコンポーネント毎にダイアログに入力する。パラメータを修正・変更すると、全体の結果は自動的に再評価されるため、手計算による手間と時間を大幅に省くことができる。また、結果は妥当性確認の文書として扱うことができる。

さらに、主な制御機器メーカが各社のコンポーネントのパラメータをライブラリとして提供しているので、SISTEMA にコンポーネントのライブラリを読み込むことで、パラメータ入力の手間も省略できる。

SISTEMA は、ドイツ法的損害保険(DGUV)の試験研究機関(IFA)が開発および配布しているソフトウェアであり、同機関のサイトから無料でダウンロードできる。最新版は英語のマニュアルしかないが、旧版の日本語解説書が(一社)日本機械工業

連合会および(一社)日本印刷機械工業会から発行されている。（平成 21 年度　印刷産業機械の機能安全に関する調査研究報告書）

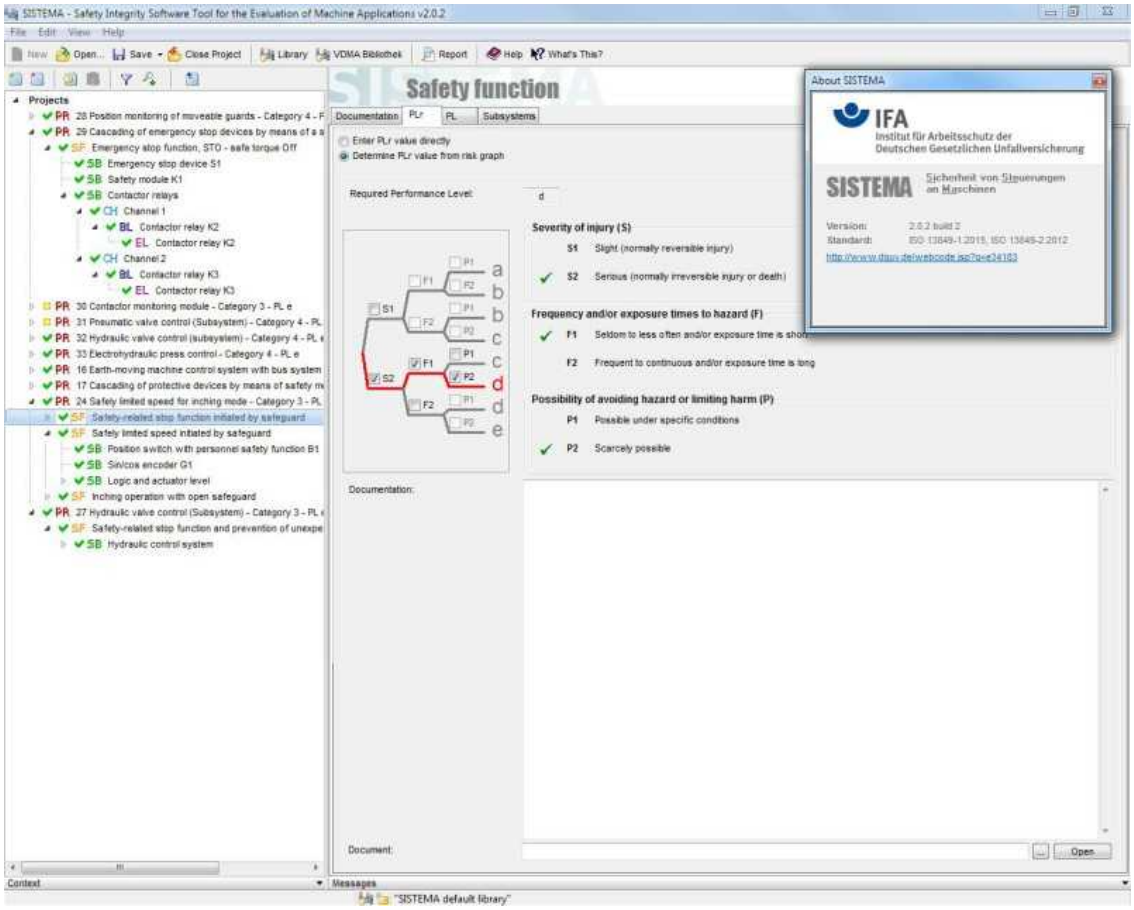


図 7-2　SISTEMA の画面例

SISTEMA のダウンロードサイト(DGUV/IFA)

http://www.dguv.de/ifa/praxishilfen/practical-solutions-machine-safety/software-sistema/index.jsp

7　安全関連アプリケーションソフトウェアの妥当性確認

(1)　安全 PLC/安全コントローラのアプリケーション設計手順

安全関連システムに市販の安全 PLC あるいは安全コントローラを使用する場合、

達成できる安全レベル(SIL/PL)は、その安全 PLC が第三者認証を取得している最高レベルまでである。安全関連系の設計者は、安全回路（安全入出力および診断方式を含む）を検討し、安全 PLC を用いて実現する。

安全 PLC を用いた機能安全系の開発に関する要求は、JIS B 9961 (IEC 62061)に詳しい。ここでは、現状の安全 PLC を用いた安全関連システムの一般的な開発手順と要求について具体化する。

最初に、冗長構成や診断を含む入出力の安全アーキテクチャを決める。次に、機械をどのように動かすか、あるいは安全をどのように確保するかについて検討する。一般に、状態遷移図や状態遷移表を用いて、安全センサやスイッチの動作によって常に安全が確保できるかどうかを確認する。これが、機械の安全運転方案となる。この方案は、文書化されて検証(レビューなど)されなければならない。

安全運転方案は､安全 PLC のアプリケーションソフトウェアとして実現される。このとき、ソフトウェア仕様書の設計及びレビューが必要である。ただし、アプリケーションソフトウェアが簡単かつ自明であるときは、ソフトウェア仕様書は作成しなくてもよい。

一般に、安全 PLC のソフトウェア設計ツール（エンジニアリングツール）は、ツール内にシミュレータやデバッガを備えているので、実機にソフトウェアをダウンロードする前にツール単独で試験を行う。この試験仕様と結果についても文書化しなければならない。

安全アプリケーションソフトウェアが完成すると、実機にダウンロードして組み合わせ試験を実施する。多くの場合、対象機械を設置しないでガードやライトカーテン等の安全関連制御系のみにより、安全アプリケーションシステムの動作確認を行う。この結果も組み合わせ試験仕様および結果として文書化する。最後に、機械を運用する場所に機械および安全関連システムを組み合わせた最終形態で、妥当性確認を実施する。

妥当性確認では、安全制御系の応答時間やガード等の安全距離などについても確認する。

８　変更と確認

(1)　安全関連システムの変更

安全関連システムについて、設計中の不具合処置や仕様変更、あるいは使用中の機会の変更・改修などを行う場合は、その変更が及ぼす影響について分析しなければならない。これを影響分析（インパクトアナリシス）という。

例えば、運転法案を見直した場合は、安全ソフトウェアのどこをどのように修正するのか、他の機能と干渉することはないか、性能面に影響ないかなどを分析する。

そして、影響のある個所、多くの場合は下流設計について、設計見直しを行い、安全回路やソフトウェアの修正を行う。

影響分析の結果は、文書化しなければならない。

文書や設計図は、変更履歴を管理しなければならない。指定した時点の文書やシステム構成を再現できることが求められる。これを構成管理という。決して、安全関連ソフトウェアのバージョン管理だけを意味するものではなく、図面や文書、試験パラメータやデータまでが管理の対象である。

(2) 変更点の試験と妥当性確認

変更に関連する試験を再試験する。仕様変更の内容によっては、試験仕様や試験データの見直し、あるいは試験項目の追加となる。再試験の範囲は、影響分析の結果に基づく。すべての試験をやり直す必要はない。

試験の変更も影響分析の結果として文書化する。

安全関連システムの仕様変更が大きく、システム性能や構成に影響がある場合は、妥当性確認をやり直す。妥当性確認の結果も文書化される。

第８章　事例

本章の事例１～４は、「安全 PLC を用いた機械・設備の安全回路事例集」（(一社)日本電機工業会 PLC 技術専門委員会、2011 年 5 月発行）から引用している。

１　施錠式ガードによる機械の起動／停止：施錠式インタロック

(1)　機械・設備イメージ

ガードで囲われた区域への扉にロック機構付の安全スイッチが取り付けられた，施錠式インタロックの設備例を図 8-1 に示す。

なお、施錠式インタロックを含む安全関連システムへの要求安全度水準（PLr）は、リスクアセスメント結果に基づき PLr=e とする。

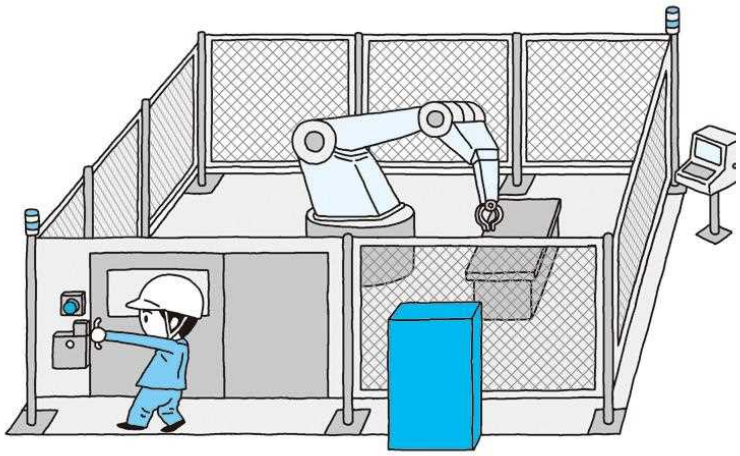


図 8-1　施錠式インタロックの設備例

(2)　機能

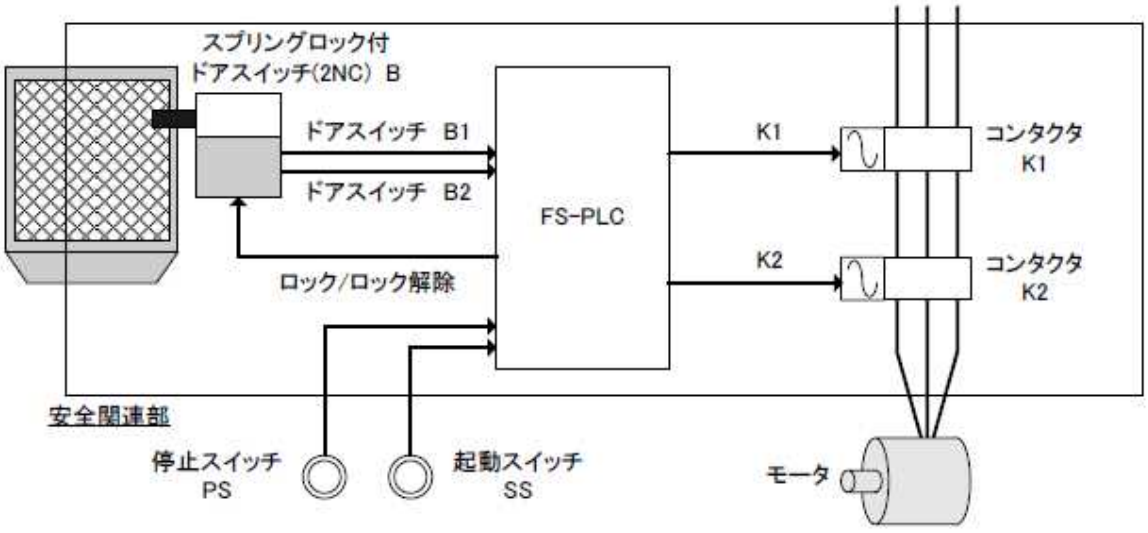
安全柵の扉についたスプリングロック式安全スイッチにより，ロボットの動力遮断まで扉が開かないようにする。スプリングロック式安全スイッチは，通常時バネの力でロックされているが，ソレノイドに電流を流すとロック解除されて扉を開けることができる。この状態遷移を表 8-1 に示す。

- 扉開状態とは，扉が開いている状態(ドアスイッチ B1,B2=OFF)であり，ロックは解除(L=ON)，機械は停止している状態(K1,K2=OFF)である。

- 扉を閉じると(B1,B2=ON)，扉閉解錠状態になるが(L=ON)，機械は停止したまま(K1,K2=OFF)である。
- 扉閉解錠状態で起動スイッチを押すと(SS=ON)，ロック施錠(L=OFF)して機械を起動する(M=ON)ことができる。
- 機械が稼働しているのは，扉閉施錠状態のみである。停止スイッチ(PS=ON)により機械は停止(K1,K2=OFF)しロックが解除される(L=ON)。なお、この停止機能は安全関連部ではない停止機能である。
- 機械が稼働している状態で無理に扉を開けると(B1,B2=OFF)，扉開状態となり機械は停止し(K1,K2=OFF)ロックは解除される(L=ON)。

表 8-1　状態遷移表

状態	イベント(変化)	動作	次の状態
①扉開 扉開(B1,B2=OFF) ロック=解除(L=ON) 機械=停止(K1,K2=OFF)	扉の閉鎖(B1,B2＝ON)	なし	②扉閉解錠
②扉閉解錠 扉閉(B1,B2=ON) ロック=解除(L=ON) 機械=停止(K1,K2=OFF)	扉の開放(B1,B2=OFF)	なし	①扉開
	起動スイッチ(SS=ON)	コンタクタ K1,K2=ON ロック施錠 L=OFF	③運転中
③運転中 扉閉(B1,B2=ON) ロック=施錠(L=OFF) 機械=稼動(K1,K2=ON)	停止スイッチ (PS=ON)	コンタクタ K1,K2=OFF ロック解除 L=ON	②扉閉解錠
	扉の開放(B1,B2=OFF)	コンタクタ K1,K2=OFF ロック解除 L=ON	①扉開



※別途 コンタクタ（K1，K2）の b 接点を安全 PLC に入力する EDM 監視回路が必要

図 8-2　施錠式インタロックの回路構成

(3) 回路構成

安全関連システムを図 8-2 の実線囲みで示す。停止スイッチ PS 及び起動スイッチは安全関連部ではない。

(4) タイミングチャート

安全関連システムの動作タイミングを図 8-3 に示す。

安全関連システムではない停止スイッチ（PS）および起動スイッチ（SS）は汎用的スイッチを使用するが、接点固着防止のために通常接点オフ（ノーマルオープン）、立下り検出で動作要求として使用する。

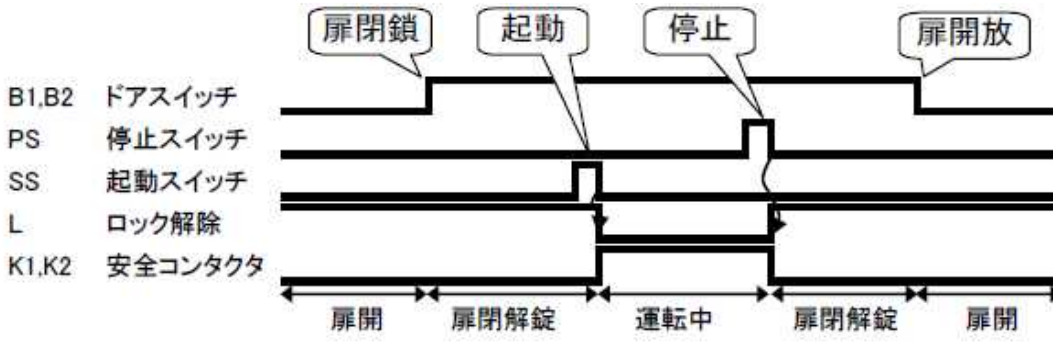


図 8-3　施錠式インタロックのタイミングチャート

(5) 安全機器のパラメータ

安全コンポーネントの PL 導出のためのパラメータ参考値を表 8-2 に示す。これらの値は、安全コンポーネント製造業者から入手する。入手できない場合、JIS B 9705-1 (ISO 13849-1)付属書 K を参照する。

表 8-2　施錠式インタロックの安全機器のパラメータ

部品番号	部品名称	B10d [千回]	MTTFd [年]	MTTFd 値 [年]	DCavg [%]	PFHd [/時間]
B	スプリングロック付ドアスイッチ	500	1,042	100	99	2.47×10-8
FS-PLC	安全 PLC	－	－	100	99	2.31×10-9
K1	コンタクタ	2,000	4,167	100	99	2.47×10-8
K2	コンタクタ	2,000	4,167	100	99	2.47×10-8

B/K1/K2：nop=1[cycle/h]×16[h/d]×300[d/y]=4,800[cycle/y]

(6) 安全ブロック図

施錠式インタロックの安全ブロック図は，図 8-4 による。

安全 PLC が入力部（ドアスイッチ）及び出力部（コンタクタ）の診断を行うことで、それぞれのサブシステムで DCavg=99%を達成している。

二重系の入力部及び出力部は、規格に基づいて二重系を構成するサブシステムのうち MTTFd 値の悪いもの（ここでは両者同じ値）を、入力部及び出力部の MTTFd とする。

安全関連システム全体の MTTFd 計算は、PFHd＝1/MTTFd であることから、各サブシステムの PFHd の合計の逆数を求めればよい。

以上の計算から、安全関連システムは、カテゴリ４、PL=e であることが導かれる。これは PLr=e を満足する。

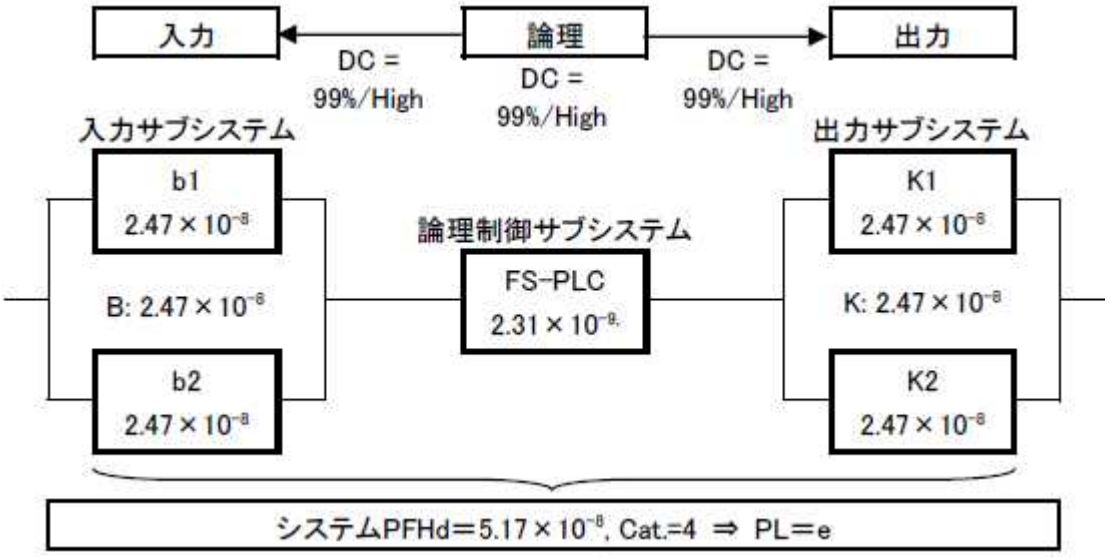


図 8-4 施錠式インタロックの安全ブロック図

２　ペンダントによるロボットティーチング：３ ポジションイネーブルスイッチ

(1)　機械・設備での使用例

３ポジションイネーブルスイッチを備えたペンダントによるティーチング例を図 8-5 に示す。３ポジションイネーブルスイッチの使用等を考慮したリスクアセスメントに従い，PLr=d とした。

図 8-5　ペンダント(３ポジションイネーブルスイッチ)の設備例

３ポジションイネーブルスイッチの操作ボタンを，定められた位置まで押して保持している間に限り，機械やロボットの手動運転を許可する。その手動運転中，機械の予期しない動作に対して，３ポジションイネーブルスイッチから手を離す，又は強く握り込んでしまっても３ポジションイネーブルスイッチが回路を遮断し，手動運転を停止させる。

JIS B 9960-1 (IEC 60204-1)及び IEC60947-5-8 で定義された，３ポジションイネーブルスイッチの動作に関する要求事項は次のようになっている。

- 押されていない状態をポジション１と定義し，スイッチを OFF する。
- 中間位置まで押している状態をポジション２と定義し，スイッチを ON する(機械の起動許可)。
- 中間位置を過ぎて押された状態ポジション３と定義し，スイッチを OFF する。

ポジション３からポジション２に戻ってもスイッチが ON してはならない。３ポジションイネーブルスイッチは, 強制開離（直接開路）機構を持つものを使用する。

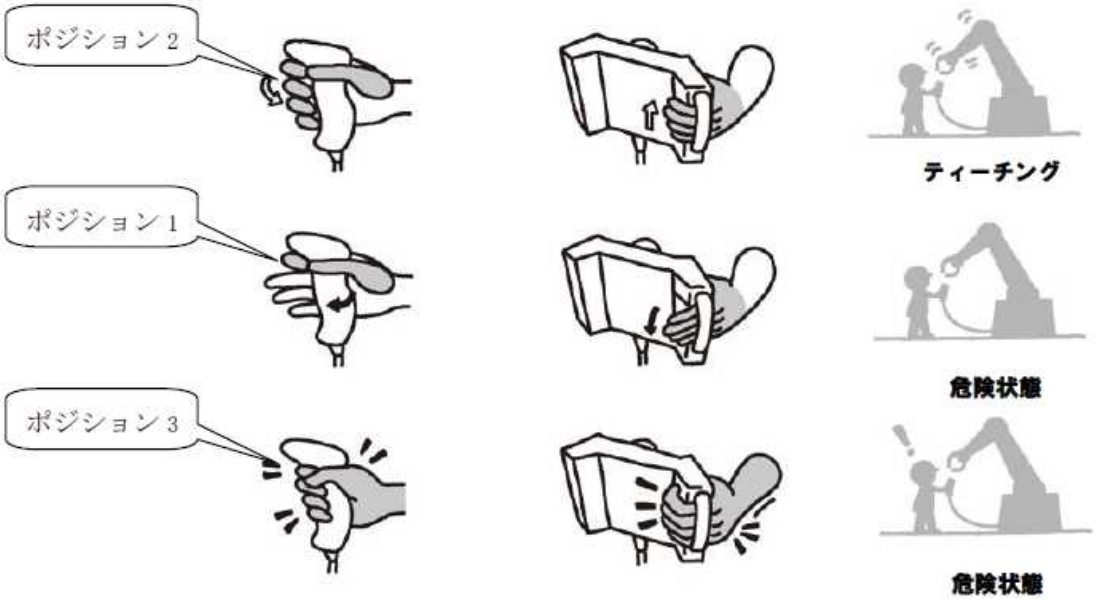


図 8-6　ペンダント(３ポジションイネーブルスイッチ)の動作

(2)　機能

手動運転の対象となるロボットの動力源の開閉を行うコンタクタの接点を ON/OFF することにより，ロボットの起動・停止を制御する。

３ポジションイネーブルスイッチ, コンタクタは安全 PLC に接続する。安全 PLC は，プログラムによりコンタクタの ON/OFF を制御する。

安全 PLC が自己診断により異常を検出した場合には，プログラムによらずコンタクタは OFF となる。また, リセットするまでコンタクタは OFF のままである。以上の状態遷移を表 8-3 に示す。

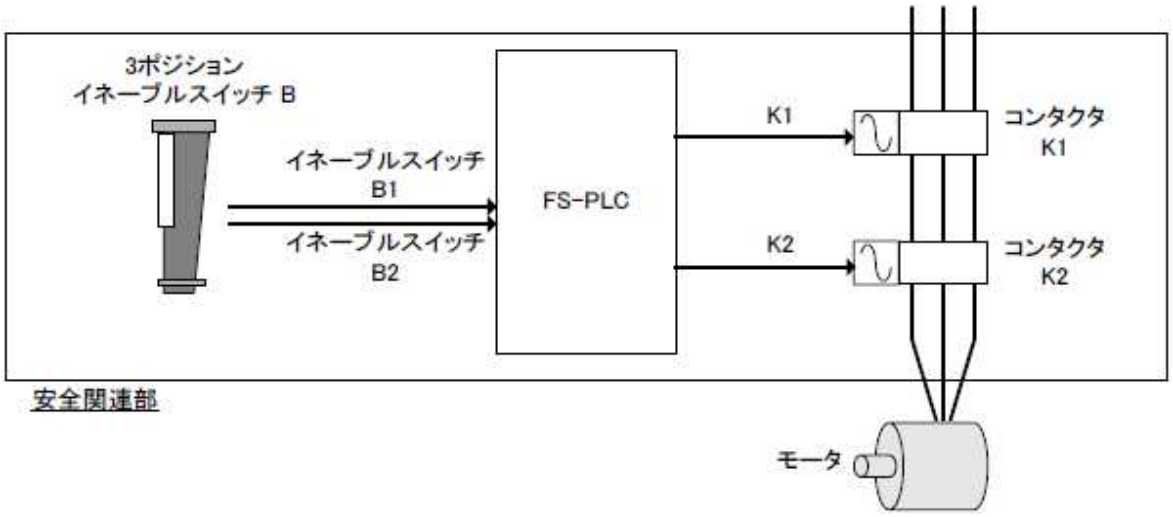
- ３ポジションイネーブルスイッチが軽く押下された状態(ポジション２：ON)でコンタクタ ON，すなわち機械の動力源を起動する。ただし，機械の動作は制限される(ティーチングモード)。
- ３ポジションイネーブルスイッチを握り込んでいない状態(ポジション１：OFF)である時, 安全PLCはコンタクタをOFFにして機械の動力源を遮断する。これにより，作業者の安全が確保される。
- ３ポジションイネーブルスイッチを強く握り込むと(ポジション３：OFF)，安全 PLC はコンタクタを OFF にして機械の動力源を遮断する。これにより，作業者の安全が確保される。

表 8-3 状態遷移表

状態	イベント(変化)	動作	次の状態
①ポジション 1 もしくはポジション 3 (B1,B2=OFF) 機械= 停止 (K1,K2=OFF)	ポジション 1->2(軽く握る) (B1,B2=ON)	コンタクタ K1,K2=ON	②ポジション 2
	ポジション 3->1(手を離す) (B1,B2=OFF のまま)	なし	①ポジション 1
	スイッチ故障 (B1=ON,B2=OFF または B1=OFF,B2=ON)	なし	③スイッチ故障
②ポジション 2 (B1,B2=ON) 機械= 稼働 (K1,K2=ON)	ポジション 2->1(手を離す) (B1,B2=OFF)	コンタクタ K1,K2=OFF	①ポジション 1
	ポジション 2->3(強く握る) (B1,B2=OFF)	コンタクタ K1,K2=OFF	①ポジション 3
	スイッチ故障 (B1=ON,B2=OFF または B1=OFF,B2=ON)	コンタクタ K1,K2=OFF	③スイッチ故障
③スイッチ故障 機械= 停止 (K1,K2=OFF)	なし	―	―

(3) 回路構成

回路構成を図 8-7 に示す。実線囲み部分が安全関連システムである。



※

別途 コンタクタの b 接点を安全 PLC に入力する EDM 監視回路が必要

図 8-7 ペンダント(３ポジションイネーブルスイッチ)の回路構成

(4) タイミングチャート

安全関連システムの動作タイミングを図 8-3 に示す。

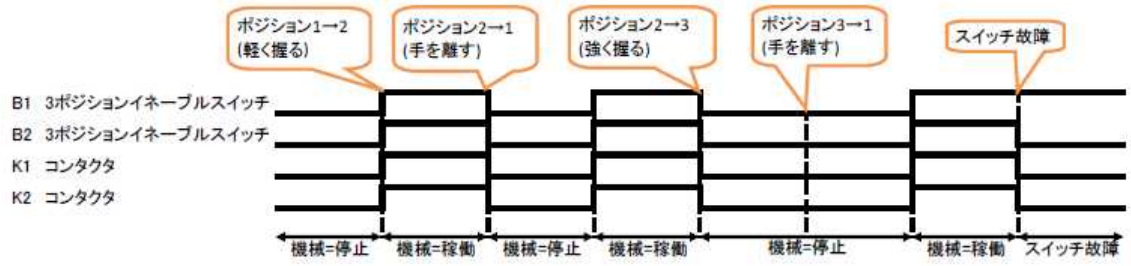


図 8-8 ペンダント(３ポジションイネーブルスイッチ)のタイミングチャート

(5) 安全機器のパラメータ

安全コンポーネントの PL 導出のためのパラメータ参考値を表 8-4 に示す。

B：nop=10[cycle/d]×300[d/y]=3,000[cycle/y]

表 8-4 ペンダント(３ポジションイネーブルスイッチ)の安全機器のパラメータ

部品番号	部品名称	B10d [千回]	MTTFd [年]	MTTFd 値[年]	DCavg [%]	PFHd [/時間]
B	ペンダント(３ポジションイネーブルスイッチ)	100	333	100	99	2.47×10-8
FS-PLC	安全 PLC	―	―	100	99	2.31×10-9
K1	コンタクタ	2,000	4,167	100	99	2.47×10-8
K2	コンタクタ	2,000	4,167	100	99	2.47×10-8

K1/K2：nop=1[cycle/h]×16[h/d]×300[d/y]=4,800[cycle/y]

(6) 安全ブロック図

安全ブロック図は図 8-9 となり、これより安全関連システムは PLr=d を満足している。

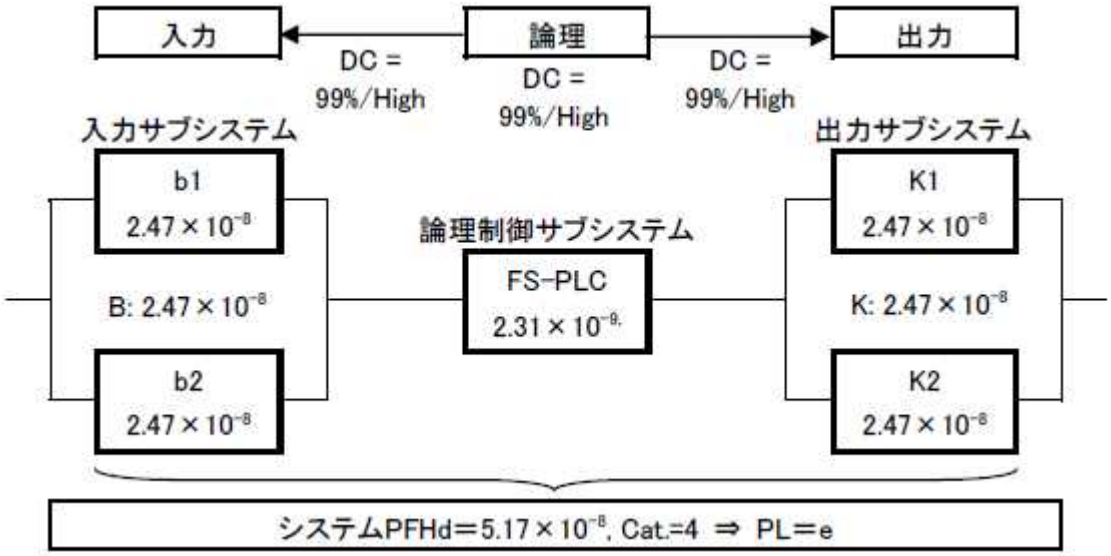


図 8-9 ペンダント(３ポジションイネーブルスイッチ)の安全ブロック図

３　ライトカーテンによる侵入検知：ライトカーテン

(1)　機械・設備イメージ

開口部にライトカーテンを設置し，作業者が材料の供給や取り出しのために，ロボット動作中に危険エリアに侵入(ライトカーテンが遮光)した際，ロボットが非常停止するアプリケーションである（図 8-10）。

ライトカーテンを含む安全システムの故障の場合，動作中のロボットと作業者の接触の可能性があり，重傷が考えられる事等を考慮してリスクアセスメントをした結果，PLr＝e とした。

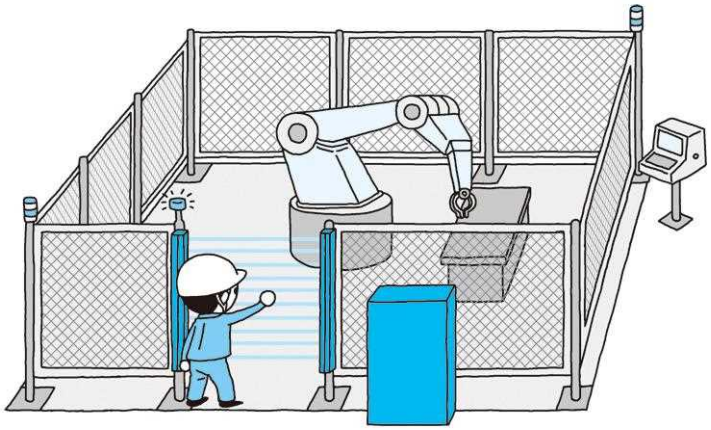


図 8-10　ライトカーテン タイプ４の設備例

(2)　機能

PLr=e であるため，ライトカーテン(F1)は，JIS B 9704-2 (IEC 61496-2)のタイプ４認証品を使用する。JIS B 9704-2 (IEC 61496-2)の認証品は，自己診断機能があり，検出方式は「透過型」であり，全ての光軸が入光状態でのみ，出力を ON にする。

ライトカーテン(F1)と出力を制御するコンタクタ(K1,K2)は，安全 PLC に接続する。安全 PLC は，プログラムによりコンタクタ(K1,K2)の ON/OFF を制御し，ロボットを停止させる。また，安全 PLC は自己診断により異常を検出した場合には，プログラムによらず出力を OFF 状態とする。

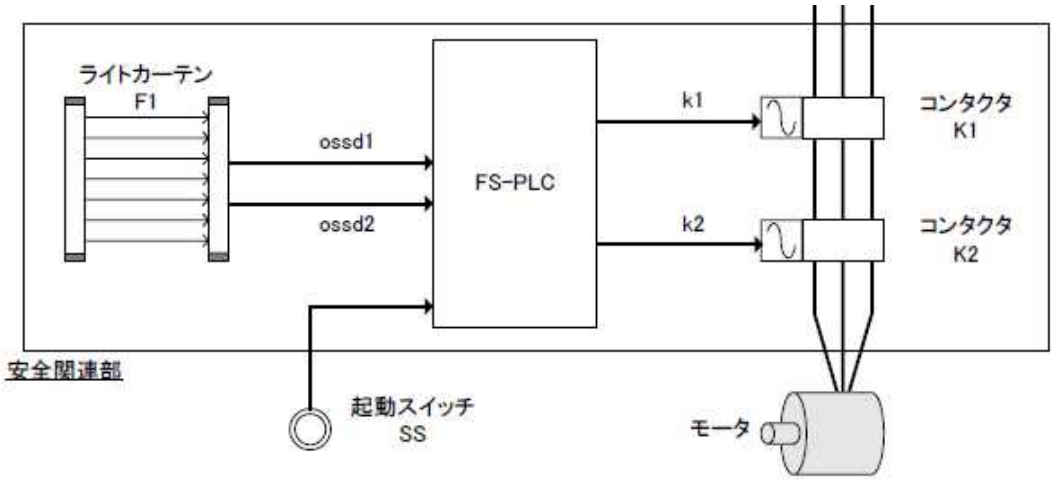
安全 PLC のプログラムで以下の機能を実現する。状態遷移は表 8-5 に示す。

- 運転準備状態の時に，ライトカーテン(F1)に入光があり，OSSD1 と OSSD2 が ON した後で，起動スイッチ(SS)を押すと，安全 PLC の出力を ON にし，運転状態とする。
- 運転状態の時に，ライトカーテン(F1)が遮光され，OSSD1 または OSSD2 の入力が OFF になった場合は，安全 PLC の出力を OFF にし，非常停止状態とする。

- 非常停止状態では，起動スイッチ(SS)を押下しても安全 PLC の出力は，OFF のままである。
- 非常停止状態で，ライトカーテン(F1)が ON(OSSD1,OSSD2=ON)した場合に，運転準備状態に戻る
- 起動スイッチ(SS)の故障により誤って起動しないように，起動スイッチ(SS)は ON→OFF 立下りをリセット条件とする。
- 電源投入時に，ライトカーテン(F1)の出力が ON になっても，安全 PLC の出力は OFF のままである(起動インタロック)。
- ライトカーテン(F1)が遮光され，安全 PLC の出力が OFF になった後に，ライトカーテン(F1)の入光があったとしても，安全 PLC の出力は OFF のままである(再起動インタロック)

表 8-5　状態遷移表

状態	イベント(変化)	動作	次の状態
①運転準備 モータ停止(K1,K2=OFF) ライトカーテン(F1)入光 (OSSD1,OSSD2=ON)	起動スイッチ(SS)押下 (SS=ON)	コンタクタ K1,K2=ON モータ動作	②運転中
②運転中 モータ動作(K1,K2=ON) ライトカーテン(F1)入光 (OSSD1,OSSD2=ON)	ライトカーテン(F1)遮光 (OSSD1 または OSSD2=OFF)	コンタクタ K1, K2=OFF モータ停止	③非常停止
③非常停止 モータ停止 (K1,K2=OFF)	起動スイッチ(SS)押下 (S1=ON)	―	③非常停止
	ライトカーテン(F1)入光 (OSSD1,OSSD2=ON)	―	①運転準備



※別途 コンタクタの b 接点を安全 PLC に入力する EDM 監視回路が必要

図 8-11 ライトカーテン タイプ 4 の回路構成

(3) 回路構成

回路構成を図 8-11 に示す。実線囲み部分が安全関連システムである。

(4) タイミングチャート

安全関連システムの動作タイミングを図 8-12 に示す。

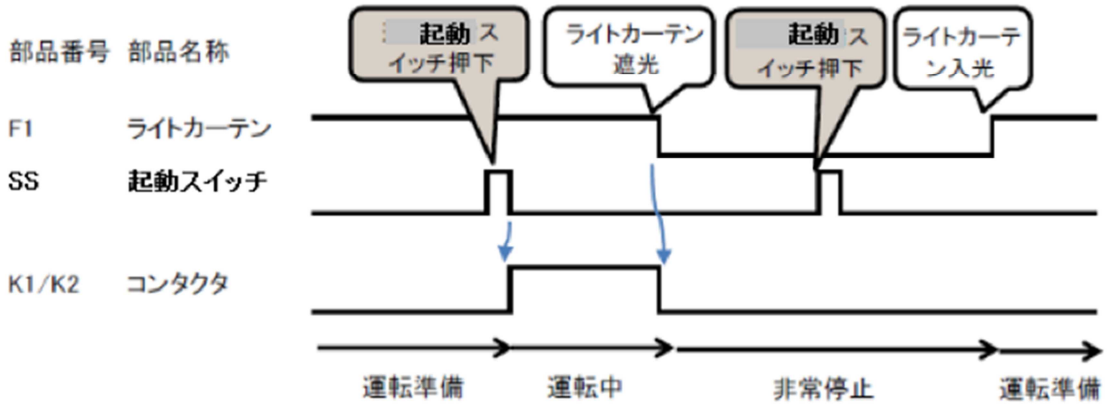


図 8-12 ライトカーテン タイプ 4 のタイミングチャート

(5) 安全機器のパラメータ

安全コンポーネントの PL 導出のためのパラメータ参考値を表 8-6 に示す。

表 8-6 ライトカーテン タイプ 4 の安全機器のパラメータ

部品番号	部品名称	B10d [千回]	MTTFd [年]	MTTFd 値[年]	DCavg [%]	PFHd [/時間]
F1	ライトカーテン	－	－	100	99	2.47×10-8
FS-PLC	安全 PLC	－	－	100	99	2.31×10-9
K1	コンタクタ	2,000	4,167	100	99	2.47×10-8
K2	コンタクタ	2,000	4,167	100	99	2.47×10-8

K1/K2：nop=1[cycle/h]×16[h/d]×300[d/y]=4,800[cycle/y]

(6) 安全ブロック図

安全ブロック図は図 8-13 となり、PL=e となる。

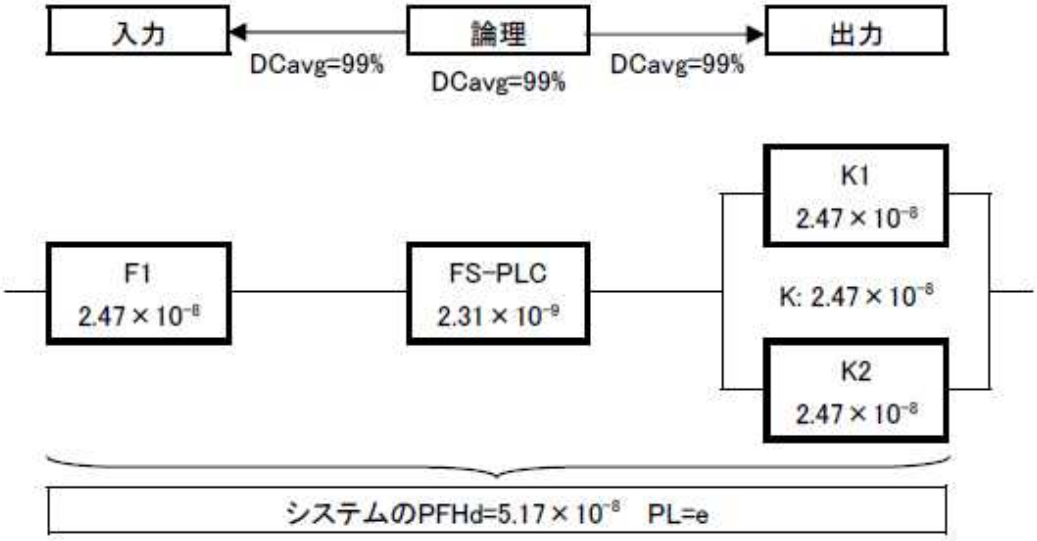


図 8-13 ライトカーテン タイプ 4 の安全ブロック図

４　レーザースキャナによる存在検知：レーザースキャナ

(1)　機械・設備イメージ

ロボット稼働エリアにレーザースキャナを設置し，ロボットが動作中に作業者が危険エリアに存在していることを検知し，ロボットを停止させる(起動させない)アプリケーションである。

作業者が，危険エリア内にいた場合に，他の作業者から死角になる場所にいても検知することで，不用意な起動／再起動から保護することが可能である。

この例の場合では，リスクアセスメントの結果，PLr＝d とした。

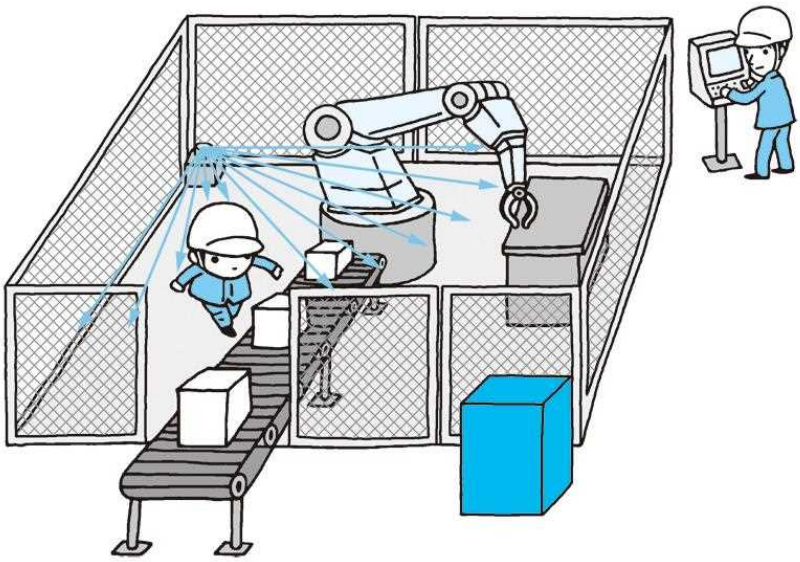


図 8-14　レーザースキャナーの設備例

(2)　機能

レーザースキャナ(F1)は，レーザー光をスキャンさせ，その反射光をモニタ(周囲の物体にあたって反射，受光するまでの時間により物体までの距離を計算する)することで，エリア内の安全を監視する。レーザースキャナ(F1)は，JIS B 9704-3 (IEC 61496-3)の認証品を使用する。JIS B 9704-3 (IEC 61496-3)の認証品は，自己診断機能があり，指定した範囲に何もない状態でのみ，出力を ON する。自己診断による故障の検出や外乱光などによるレーザースキャナ(F1)の異常により，出力は OFF 状態となる。

レーザースキャナ(F1)と出力を制御するコンタクタ(K1,K2)は，安全 PLC に接続

する。安全 PLC のプログラムで以下の機能を実現する。状態遷移は表 8-7 に示す。

- 運転準備状態の時に，レーザースキャナ(F1)出力（OSSD1 と OSSD2）が ON した後で，起動スイッチ(SS)を押すと，安全 PLC の出力を ON にし，運転状態とする。
- 運転状態の時に，レーザースキャナ(F1)出力（OSSD1 または OSSD2）が OFF になった場合は，安全 PLC の出力を OFF にし，非常停止状態とする。
- 非常停止状態では，起動スイッチ(SS)を押下しても安全 PLC の出力は，OFF のままである。
- 非常停止状態で，レーザースキャナ(F1)が ON(OSSD1,OSSD2=ON)した場合に，運転準備状態に戻る。
- 起動スイッチ(SS)の故障により誤って起動しないように，起動スイッチ(SS)は ON→OFF 立下りをリセット条件とする。

表 8-7　状態遷移表

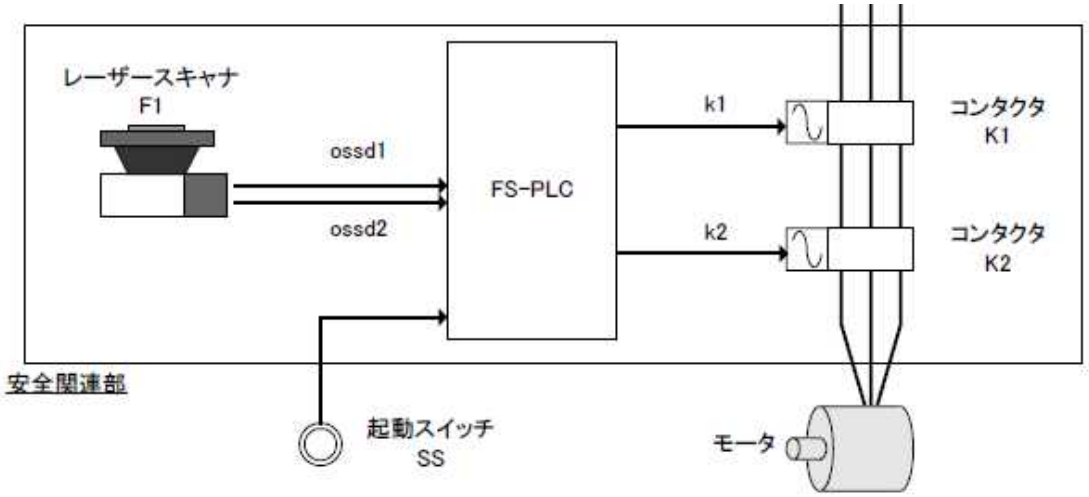
状態	イベント(変化)	動作	次の状態
①運転準備 モータ停止(K1,K2=OFF) レーザースキャナ(F1)出力 ON(OSSD1,OSSD2=ON)	起動スイッチ(SS)押下 (RS=ON)	コンタクタ K,K2 =ON モータ動作	②運転中
②運転中 モータ動作(K1,K2=ON) レーザースキャナ(F1)出力 ON (OSSD1,OSSD2=ON)	レーザースキャナ(F1) 出力 OFF(OSSD1 または OSSD2=OFF)	コンタクタ K1,K2 =OFF モータ停止	③非常停止
③非常停止 モータ停止(K1,K2=OFF)	起動スイッチ(SS)押下 (RS=ON)	－	③非常停止
	レーザースキャナ(F1) 出力 ON (OSSD1,OSSD2=ON)	－	①運転準備

(3)　回路構成

回路構成を図 8-15 に示す。実線囲み部分が安全関連システムである。

(4)　タイミングチャート

安全関連システムの動作タイミングを図 8-16 に示す。



※別途 コンタクタの b 接点を安全 PLC に入力する EDM 監視回路が必要

図 8-15 レーザスキャナの回路構成

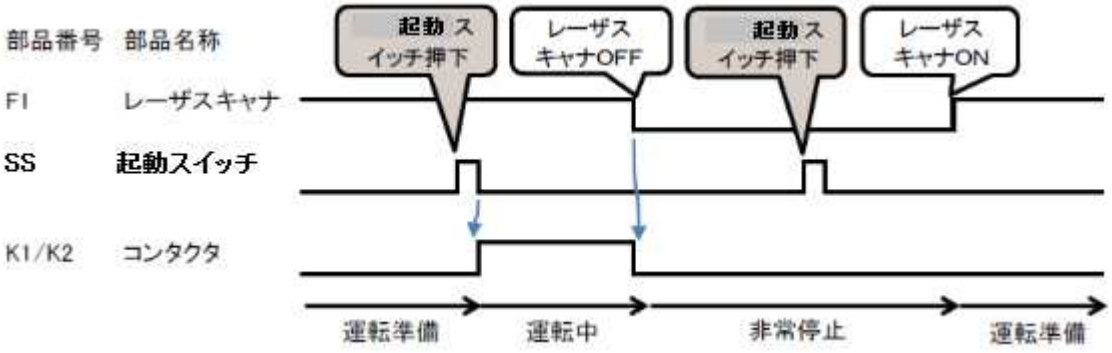


図 8-16 レーザスキャナのタイミングチャート

(5) 安全機器のパラメータ

安全コンポーネントの PL 導出のためのパラメータ参考値を表 8-7 に示す。

表 8-7　レーザスキャナの安全機器のパラメータ

部品番号	部品名称	B10d [千回]	MTTFd [年]	MTTFd 値[年]	DCavg [%]	PFHd [/時間]
F1	レーザスキャナ	－	－	100	90	1.03×10-7
FS-PLC	安全 PLC	－	－	100	99	2.31×10-9
K1	コンタクタ	2,000	4,167	100	99	2.47×10-8
K2	コンタクタ	2,000	4,167	100	99	2.47×10-8

K1/K2：nop=1[cycle/h]×16[h/d]×300[d/y]=4,800[cycle/y]

(6) 安全ブロック図

安全ブロック図は図 8-17 となり、PL=d となる。

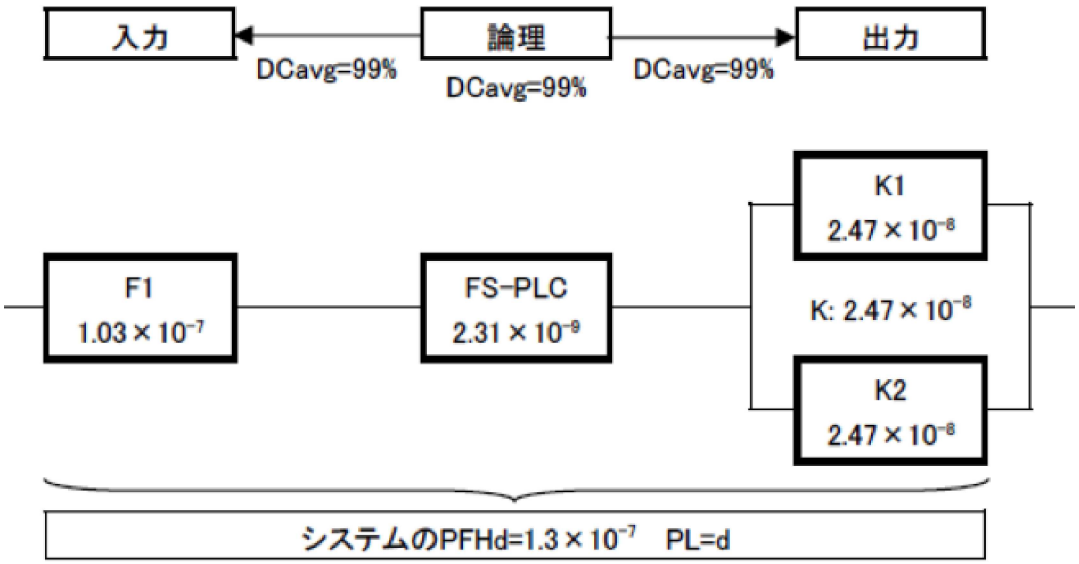


図 8-17　レーザスキャナの安全ブロック図

５　ロボットの安全速度制限(SLS)

(1)　機械・設備イメージ

リスクアセスメントにより適切な安全対策が実施された場合、ロボットを囲む柵のない機械設備の運用が可能である。第 5 章において、協働作業ロボットのリスク低減方策として、安全適合監視速度機能について述べた。ここでは、安全適合監視速度機能の具体的事例として、ロボットの安全速度制限(SLS: Safety Limited Speed)を紹介する。SLS は、IEC 61800-5-2 可変速ドライブの機能安全規格に定義された安全機能の一つである。

図 8-18 において、ロボットの周辺には停止エリアと制限エリアのふたつの領域が設定されている。身体の一部が制限エリアに進入したとき、エリアセンサ（レーザスキャナ）がこれを検知して、ロボットコントローラはロボットを指定の安全速度以下で運転する。さらに身体の一部が停止エリアにまで進入すると、エリアセンサはそれを検知し、ロボットコントローラはロボットを即時停止する。

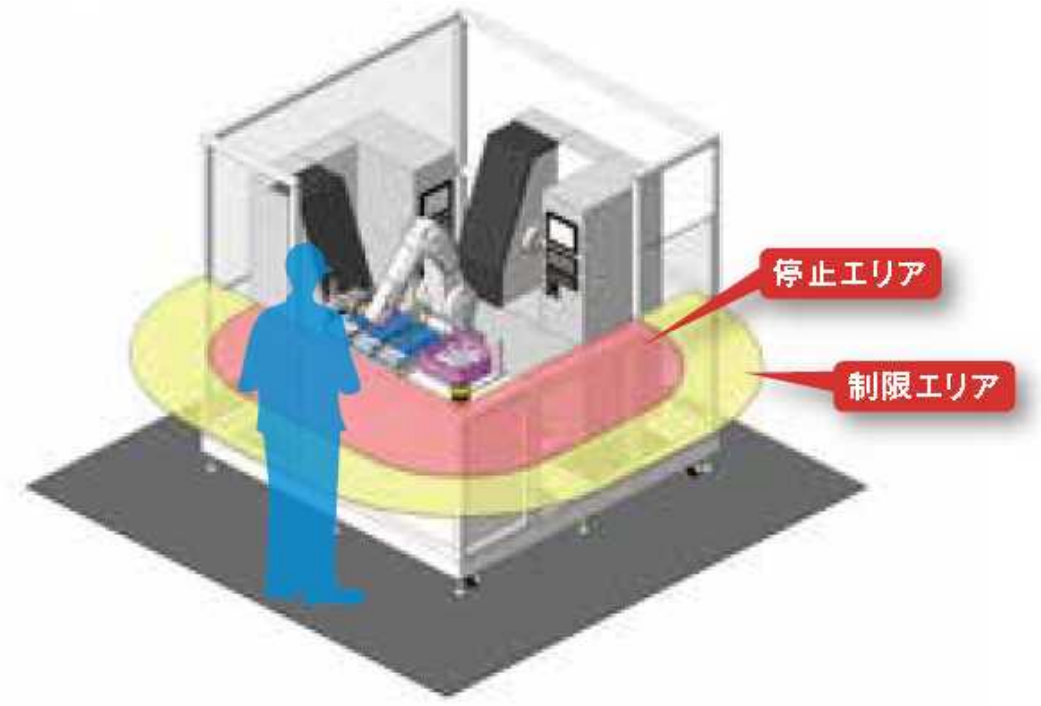


図 8-18　ロボットの安全速度制限(SLS)
(三菱電機　「MELFA ロボット安全オプションカタログ」より)

(2)　システム構成

図 8-18 のシステム構成を図 8-19 に示す。

非常停止、エリアセンサ、ライトカーテンなどの安全センサなどによる安全制御ロジックは安全シーケンサが実行する。同時に、安全シーケンサはエリアセンサやライトカーテンの入力信号を「ロボット安全オプション」に送る。

ロボットコントローラは規格適合した安全関連制御系を内蔵しており、で安全機器の信号、ロボットの位置、速度、トルクを監視している。ロボットコントローラは、速度異常を監視しながらロボットの速度制御を行っている。

安全機器、安全シーケンサおよび安全オプションなどは、安全規格に適合した製品である。詳しくは、第 5 章を参照してほしい。

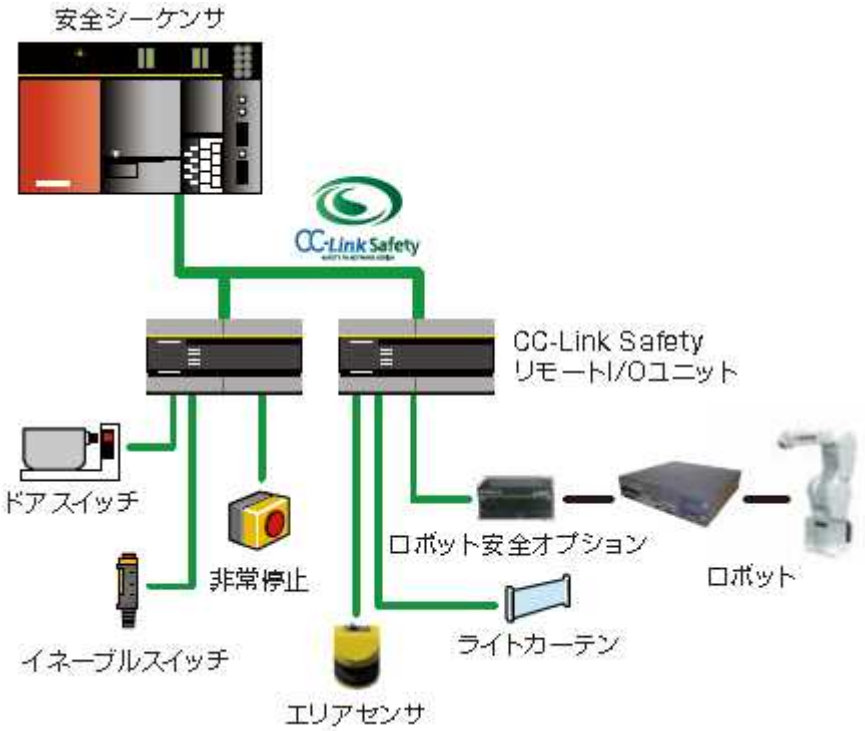


図 8-19　システム構成図

(三菱電機　「MELFA ロボット安全オプションカタログ」より)

(3)　機能の設定

SLS を使用するために必要な設定は、ロボットコントローラの安全監視機能の設定である。この設定は、ロボット製造業者が提供するロボットコントローラの専用ツールを用いて行うことができる。

人が制限区域に進入したときの安全速度を指定する。また、減速するまでの時間も設定する。速度監視を設定したとき、ロボットがその設定値を越えた場合、ロボットは停止する。

もうひとつの設定は、エリアセンサ（レーザスキャナ）である。エリアセンサは、

専用の設定ツールを用いて、警告エリアと非常停止エリアをそれぞれ角度と距離で設定できる。一般的に、ツールで扇形を描くようにして設定する（図 8-20）。なお、警告エリア進入は非安全情報、非常停止エリア進入は安全情報であるため、前者はエリアセンサからの一重の信号線、後者は二重化された安全信号(OSSD1/2)として通知される。

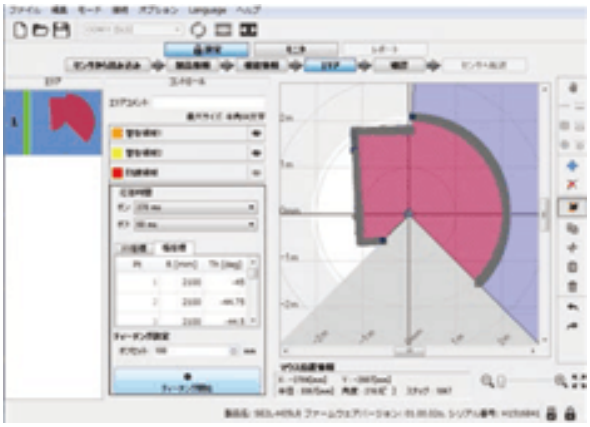


図 8-20　レーザースキャナーの領域設定画面
（IDEC ホームページより）

今回の場合、制限エリアへの進入検知も安全情報として扱うため、エリアセンサを 2 台用いる。1 台のエリアセンサは停止エリアを定義し、進入検知の安全信号(OSSD1/2)は、安全オプションの非常停止端子に接続する。停止エリアに進入する

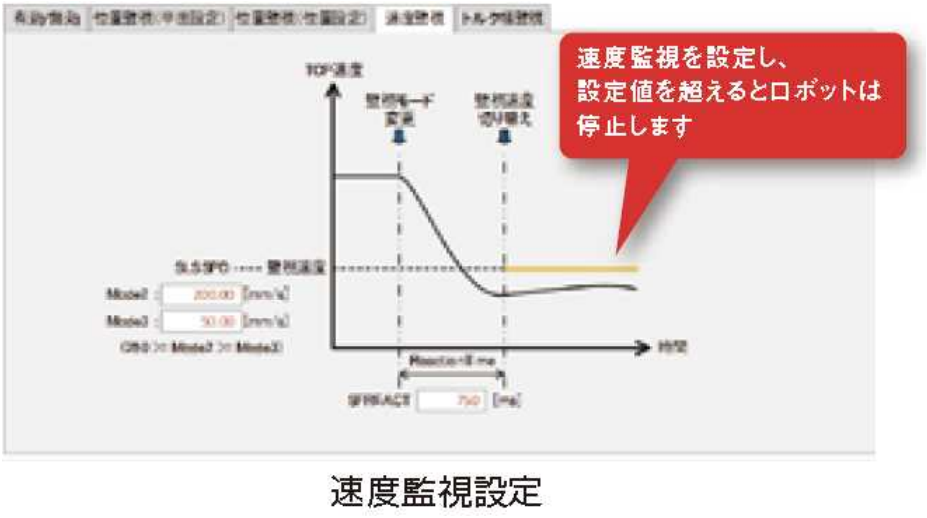


図 8-21 ロボットコントローラの速度監視設定画面
(三菱電機　「MELFA ロボット安全オプションカタログ」より)

と、非常停止となる。

もうひとつのエリアセンサは、制限エリアへの侵入で安全信号（OSSD1/2）が出力される、すなわち制限エリアを非常停止エリアとして定義する。この信号は、安全オプションの SLS 用端子に接続する。すなわち、制限エリアに進入すると、この信号により安全オプションはロボットコントローラに対して SLS 運転を指示する。SLS の制限速度は、図 8-21 で設定した値である。

(4) 妥当性確認

第 4 章で述べたように、協働作業ロボットは JIS B 8433-1 (ISO 10218-1)に適合し、かつ SIL2/PLd の安全性能を達成していなければならない。さらに、本章の 1～4 の事例で示したように、安全センサや安全 PLC などもそれぞれの安全規格に適合し、MTTFd や DCavg などの安全パラメータが製造業者から入手可能でなければならない。もし、使用する安全コンポーネントが規格適合していない、もしくは安全パラメータが入手できない場合は、インテグレータまたは使用者が自身でパラメータを導出しなければならない。

加えて、SLS の速度やエリアセンサの設定などが妥当であるかどうかの確認が必要である。例えば、ロボットの通常速度と制限区域、停止区域の範囲、人体の接近速度など当初の安全要求を満足したかどうか妥当性を確認する。また、据え付け状態でのリスクアセスメントも必要である。

協働ロボットシステムの妥当性確認の詳細については、第 7 章を参照してほしい。

６　ロボットの安全位置制限(SLP)

(1)　機械・設備イメージ

第 5 章では、ロボットの位置監視について安全位置制限(SLP: Safety Limited Position)について述べた。本節では、その具体的な事例について紹介する。

SLP は、IEC 61800-5-2 可変速ドライブの機能安全規格に定義された安全機能の一つである。

図 8-22 において、安全柵が閉まっているとき、ロボットは高速で動作する。安全柵が開けられると、ドアスイッチがそれを検知しロボットコントローラに伝える。すると、ロボットは監視平面の内側で低速で動作を継続する。ロボットは監視平面を越えないように、位置制限の運転を行う。作業者は安全柵内の監視平面外側で検査作業などを実施することができる。

監視平面にはライトカーテンを設置し、作業者が監視平面内側に侵入するとそれを検知し、ロボットを非常停止する。前節の停止区域と同様である。

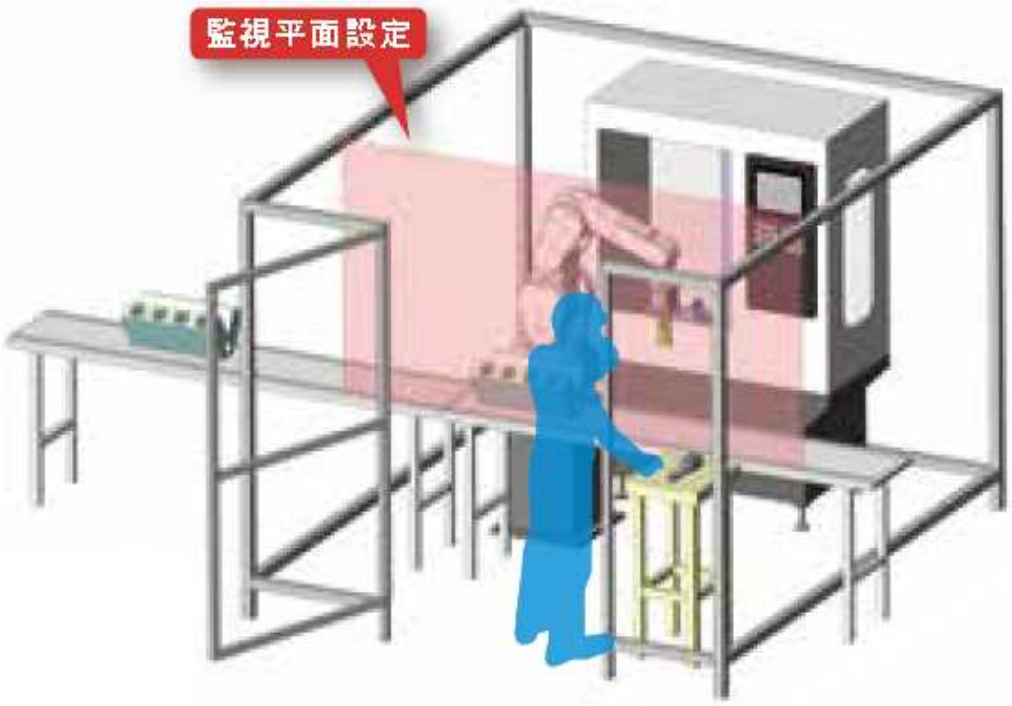


図 8-22　ロボットの安全速度制限(SLP)
(三菱電機　「MELFA ロボット安全オプションカタログ」より)

(2)　システム構成

図 8-22 の安全制御系のシステム構成は、前節の図 8-19 と同じである。ロボット

コントローラがロボットの位置情報を安全情報として処理しており、安全オプションが他の安全機器からの情報入力を扱う。

(3) 機能の設定

SLP の設定は、前節と同様、ロボットコントローラの専用ツール(RT ToolBox2)により、簡単に行うことができる。

設定する項目は、安全柵が開いたときの安全速度と、ロボットの可動範囲の境界である監視平面である。監視平面は、いろいろな角度で設定できる。次に、監視位置を設定する。監視位置は、中心座標からの任意の球面として定義できる。監視位置の球面が監視平面に近づいたとき、ロボットは停止する。この球面の設定におい

図 8-23　ロボットの安全位置制限の設定
(三菱電機　「MELFA ロボット安全オプションカタログ」より)

ては、ロボットのエフェクタの大きさや種類、ロボットの動きや速度について考慮しなければならない。

なお、人が監視平面の内側に進入することはライトカーテンで監視しているため、特別な設定はない。

(4) 妥当性確認

SLP も SLS と同様に、専用の設定ツールを用いてパラメータ設定するだけで使用できる。安全機器や安全コントローラは規格適合品を適切に使用すれば、安全コントローラの安全度水準(SIL2/PLd)と同じレベルまで達成できる。

安全度水準以外にも、安全柵が開いてからロボットが減速するまでの時間、監視球面の半径とライトカーテンの最小検出寸法に対する追加の安全距離（検知されるまでに進入する指先、指などの長さ）、安全柵内の作業性などを考慮して、安全要求を満足したか妥当性を確認する。

協働ロボットシステムの妥当性確認の詳細については、第 7 章を参照してほしい。

第 9 章　演習

1　　演習事例

本章では、協働作業ロボットについてリスクアセスメント、リスク低減対策及び妥当性確認までの演習を行う。

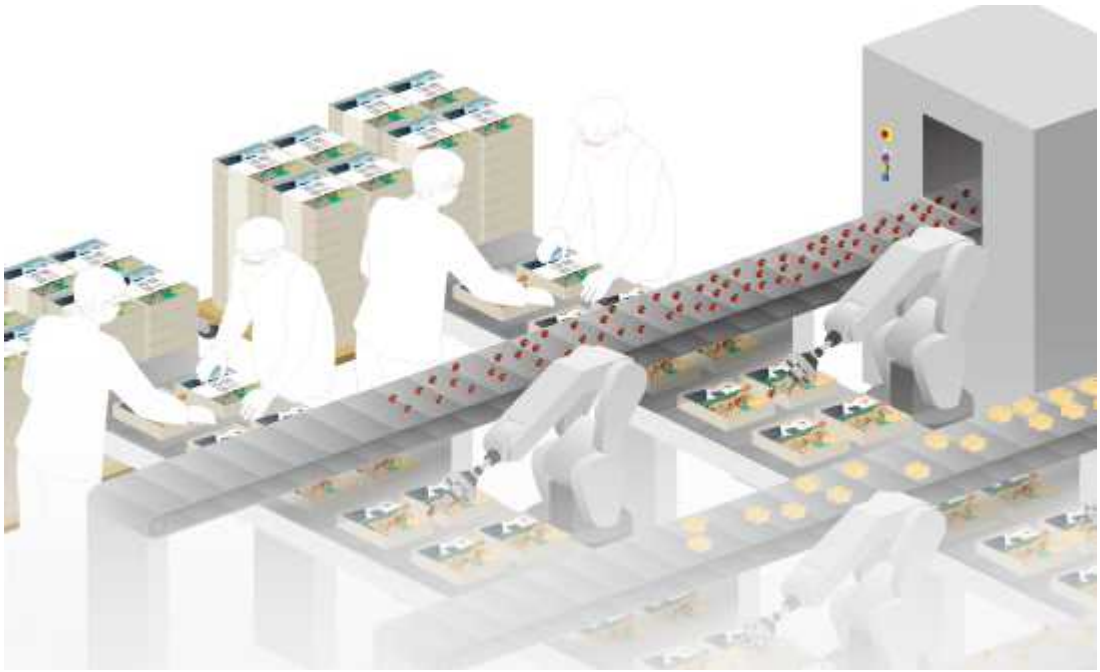


図 9-1　弁当箱詰めロボット（IDEC ファクトリーソリューションズより）

対象とするロボットシステムは図 9-1 の弁当箱詰めロボットシステムであり、基本構成とタスクは次の通りである。

・ロボット及び人間が協働で弁当具材を弁当箱に詰める作業を行う。
・右側のフライヤー/オーブンから調理された具材が上側のコンベアで運ばれてくる。
・弁当箱は下側のコンベアで右から左奥（作業者側）に運ばれる。ロボットは上側のコンベアの具材を掴んで、弁当箱の所定の位置に詰める＝12 セット/分
・作業者は弁当のパッキング内容を確認し、包装及び台車に載せる。
・弁当に不備（詰め忘れなど）があれば、作業者が該当コンベア（ロボットの近く）に行って具材を詰めなおす＝3 分に 1 回程度
・平均 30 分ごとに弁当メニューが切り替わる。ロボットのハンドは変更なく、プログラムが切り替わる。
・一日の作業終了時に、ロボット、コンベア等の清掃およびメンテナンスを実施する

・清掃作業のし易さのため、可能ならロボットにガードをつけたくない。
・作業者が具材コンベアに近づいても、ロボットを非常停止したくない＝再起動に時間がかかるため。

２　リスクアセスメントとリスク低減方策

表 9-1　協働作業ロボットの仕様一覧

分類	項目	仕様・制限
工程概要	ロボットを含む各装置類の配置	
	製品・材料の流れ	
	加工・作業内容、加工時の副生物・放出物(フューム、アーク光、熱、音、電磁波、放射性物質)・廃材などの性状・性質・量	
	タクトタイム、サイクルタイム	
	稼働時間(日／月／年)、生産台数(時間／日／年)	
	周辺装置・他の機械や建屋の壁・柱等との距離・空間	
本体	大きさ、形状、機構	
	駆動源・機構	
	質量・重心・モーメント	
	最大可動範囲	
	最大可搬重量	
	最大動作速度	
	設置方法	
エンドエフェクタ	重量、重心	
	駆動源・機構	
周辺装置	大きさ、形状、	
	重量、重心	
	形状	
	駆動源・機構	
動作	軌跡	
	速度	
	待機位置・姿勢	
	起動・停止条件	
製品･材料	製品	
	材料	
	副資材	
	副産物	
使用条件	周辺環境	
	空間的条件	
	関係者	

(1) 機械の使用制限

図 9-1 の中央のロボットに関して、リスクアセスメントに必要な機械の使用制限を列挙しなさい。第 3 章 1 （1）を参考にして、表 9-1 の様式にまとめなさい。なお、前頁の説明に書かれていない仕様や制限については、本演習に限り空白でもよい。

(2) リスクアセスメント

図 9-1 の中央のロボットに関して、リスクアセスメントを実施しなさい。コンベア、フライヤーについてリスクアセスメントする必要はない。添付の表 9-6 を使用すること。

・ロボットに関する危険源は、第 3 章表 3-8 を参考にして、表 9-2 に記入すること。
・ロボットに関する作業は、第 3 章表 3-10 を参考にして、表 9-3 に記入すること。
・リスクの見積もり・評価は、第 3 章の表 3-15、表 3-16、表 3-17、表 3-18 に基づいて実施すること。
・表 9-4 の記載方法は、第 3 章の表 3-14、表 3-18 を参考にすること。

表 9-2 ロボットシステム危険源洗い出しシート例

危険源の種類 ＼ 構成要素	機械的				電気的	熱的	騒音	振動	放射	材料物質		人間工学	環境	組合せ
	動力（挟まれ等）	重量物	滑り・躓き・墜落	その他（切創等）						有害物質	爆発・火災			
ロボット*1														

*1：エンドエフェクタ含む

表 9-3　ロボットシステム作業洗い出しシート例

フェイズ	作業内容
運搬	
据付	
調整	
生産	
段取り	
保全	
トラブルシューティング	
廃却	
その他	

(3)　リスク低減方策

リスクアセスメントの結果、リスクが 4 の危険源および危険事象に対して、リスク低減方策を考えなさい。第 3 章の表 3-19 を参考に、表 9-6 のリスク低減方策の列に記載しなさい。

ただし、顧客の要求事項である、「可能であればガードなし」を考慮すること。

ロボットのリスク低減方策は、本書の第 5 章を参考にすること。

(4)　リスク低減方策の効果－リスクアセスメント

上記のリスク低減方策の効果を評価しなさい。第 3 章表 3-20 に従って、リスク低減方策を実施後の条件下での、リスクを見積もりなさい。表 9-6 の保護方策後：リスク見積もりの列に記載しなさい。

もし、その結果がリスク 3 以上の場合は、追加のリスク低減方策を検討しなさい。

(5) リスク低減方策の要求安全度水準（PLr）

上記のリスク低減方策のうち、制御システムによる方策について、第 4 章に従って要求安全度水準（PLr）を求めなさい。第 4 章図 4-1 に従って求め、表 9-6 右端の妥当性の欄に PLr を記載しなさい。

３　リスク低減方策の実現

(1) 安全適合監視速度

図 9-1 のロボットのリスク低減方策として、作業者がロボットに接近すると、それを検知してロボットを減速させる速度制御（JIS B 8433-1 (ISO 10218-1) 5.6.4 安全適合監視速度）を採用するとする。

・ロボットアームの可動範囲(具材コンベアから弁当コンベアまでの半径 1m)を速度制御の範囲とする→レーザースキャナにより作業者の進入を検知する。
・レーザースキャナはロボット基部、コンベアよりも高い位置に配置する。なお、ロボット後方には人が立ち入らない。ロボットに対して弁当コンベア側から接近する。
・速度制御範囲に作業者が入ると、ロボットのハンドツール部の速度を 200mm/s 以下とする。
・また、ロボットはこの速度を監視し、速度超過時には保護停止する。
・安全適合監視速度の機能を有するロボットを選択する。
・このリスク低減方策は、PLr=d の要求がある。

(2) 安全システム構成

レーザースキャナとロボット安全制御装置のシステム構成図を作成しなさい。

なお、レーザースキャナは、OSSD1/OSSD2 の出力信号を持ち、ロボット安全制御装置は、安全適合速度監視用の SLS1/SLS2 の安全入力端子を持つ。それぞれの信号仕様を表 9-4 に示す。

表 9-4　安全機器の信号仕様

安全機器	信号/端子	意味
レーザースキャナ	OSSD1/OSSD2	ON:速度制御範囲に進入なし OFF:速度制御範囲に進入あり
ロボット安全制御装置	SLS1/SLS2	ON:通常運転速度 OFF:減速運転(安全適合監視速度)

(3) 安全機器の設定パラメータ

レーザースキャナ（速度制御）、ロボット安全制御装置に対して設定する安全関連パラメータを決めなさい。

・レーザースキャナー：速度制御を行う範囲（エリア）
・ロボット安全制御装置：安全適合監視速度（上記エリア内に人が侵入したときの制限速度）

【解答例】

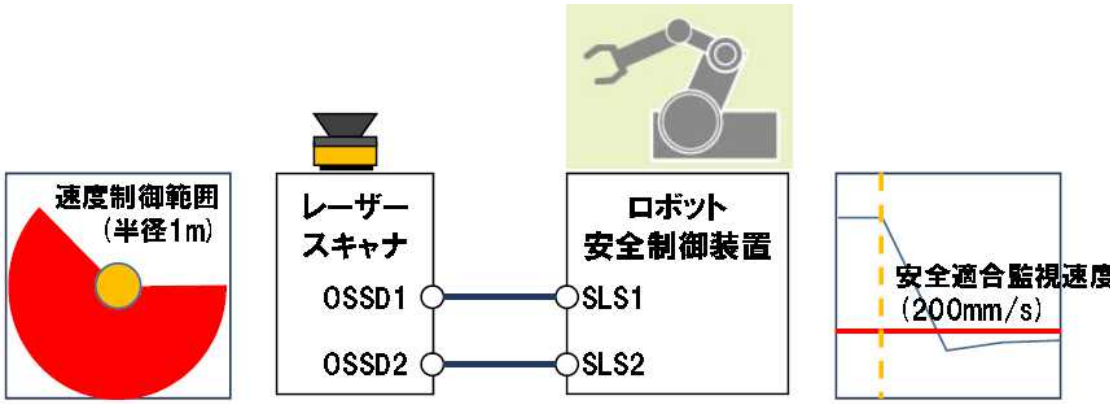


図 9-2　安全システム構成図および設定パラメータの設定例

4　妥当性確認

(1)　安全関連システムの PL 評価

前節の安全適合監視速度を実現する安全関連システムについて、PL を求めなさい。図 9-3 の記入様式に、第 6 章 4 節に従ってパラメータを記入しなさい。

なお、レーザースキャナとロボット安全制御装置の MTTFd および DCavg は表 9-5 とする。

(2)　妥当性確認

上記の結果が、リスク低減方策の安全要求性能を満足したか、確認しなさい。

表 9-5　安全機器の PL 関連パラメータ

安全機器	DCavg	MTTFd[年]	PFHd[1/時間]	PL
レーザースキャナ	99%	480	2.4×10^{-7}	d
ロボット	99%	340	3.4×10^{-7}	d

【解答】

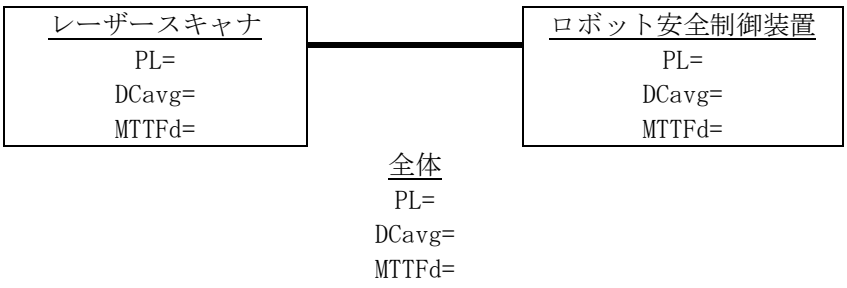


図 9-3　安全関連システムの妥当性確認

表9-6 リスクアセスメントシート（弁当箱詰めロボット対象）

No	作業-危険源-危険状態-危険事象	保護方策前：リスク見積				リスク低減方策	保護方策後：リスク見積					妥当性
		ひどさS	頻度F	回避P	リスク		ひどさS	頻度F	回避P	確率0	リスク	
例	作業者が具材を取るためコンベアに接近時にロボットハンドと衝突、または作業台との間に挟まれる	S2	F2	A2	d	作業者がロボットに接近すると、ロボットを減速制御する（JIS B 8433-1 5.6.4 安全適合監視速度）	S2	F2	A2	01	2	PLr=d
1												
2												
3												
4												
5												
6												
7												
8												
9												
10												

附録 A　技術ファイルの内容例

基発 1224 第 2 号「産業用ロボットに係る労働安全衛生規則第 150 条の 4 の施行通達の一部改正について」では、ISO 10218-1:2011 及び ISO 10218-2:2011 に適合した産業用ロボットをその使用条件に基づき適切に使用することを求めている。これらの規格に規定される措置を実施していることの証明は、技術ファイル及び適合宣言書が作成されていることである。通常、これらの書類は産業用ロボットメーカが作成するが、ロボットシステムインテグレータが作成する場合は本附録 A と B を参照されたい。

技術ファイルの構成

①ロボットの全体的説明

②ロボット全体図、制御回路図、ロボット運転の理解に必要な関連する記述と説明

③ロボットが ISO 10218-1,-2 に適合することの確認に必要な完全な詳細図面、付随する計算書、試験結果、証明書等

④以下の内容を含むリスクアセスメントを実施した手順を示す文書

・ロボットに適用される要求事項リスト

・同定された危険源の除去及びリスク低減のために実施された保護方策の説明

・該当する場合、ロボットに関連する残留リスクの明示

⑤使用した他の規格及び技術仕様書、また、それらの規格等に含まれる関連要求事項の説明

⑥メーカ、またはメーカかその正式な代表者によって選定された機関が実施した試験結果を示す技術報告書

⑦ロボット取扱説明書の写し

⑧該当する場合、組み込まれた部分完成ロボットの組み込み宣言書及びこのロボットに関する組み立て説明書

附録 B　適合宣言書の内容例

適合宣言書の構成

① メーカ名称、住所及び正式な代表者氏名

② 技術ファイル（附録 A）を編纂する権限を付与された者の名称及び所在地

③総称としての表示名、機能、モデル、型式、製造番号、商品名を含むロボットの説明及び識別方法

④適合性を宣言しようとする安全規格の全ての関連規定を満たすことを明白に宣言する文書

⑤該当する場合、その他使用された技術規格及び技術仕様書の参照

⑥適合宣言を実施した場所及び日付

⑦メーカ名又はその正当な代表者の代理として適合宣言書を作成した者の名称および署名

適合宣言書の様式例 1（JIS Q 17050　適合性評価-供給者適合宣言より）

（この規格に従った）供給者適合宣言書

1）番号:_____

2）発行者の名称:_____

発行者の住所:_____

3）宣言の対象:_____

4）上記宣言の対象は、次の文書の要求事項に適合している:

文書番号	表題	版数/発行日

5）製品について:_____

_____

6）追加情報:　_____

_____

_____

7）代表者又は代理者の署名:_____

（発行場所及び発行日）

（氏名、役職名）　　（発行者から権限を与えられた者の署名又は同等の印）

適合宣言書の様式例 2（欧州機械指令適合−完成機械用）

ORIGINAL

Declaration of Conformity

as per Annex II part 1A of the Directive 2006/42/EC and in accordance with Annex III of the Decision No 768/2008/EC
of the European Parliament and of the Council, for completed machinery (as defined in Article 1 (1) (a) to (f) of 2006/42/EC)

---Name, Model and Type of the machine---

Serial Number(s) or manufacturing number (s):

Function of the machinery *(e.g. welding robot, punching machine)*

CE

Manufacturer:	**Person Authorised to compile the technical file:**
(indicate full business name and business address)	*(indicate full business name and business address)*
Authorised Representative in the EU: *(indicate full business name and business address or write not applicable if no Authorised representative has been appointed)*	**Notified Body:** *(only to be used in case of compliance assessment Module G according Decision 768/2008/EC) (indicate NB's number, full business name and business address or write not applicable)* **Certificate of Conformity** ***N°:*** ***Date:***

Hereby, we declare that the above mentioned completed machinery has been designed and manufactured in accordance with, and fullfils all the relevant provisions of the directives as listed below (strike-through if not applicable):

- ☐ Machinery Directive 2006/42/EC
- ☐ Low Voltage Directive 2006/95/EC
- ☐ ATEX Directive 94/9/EC
- ☐ Other: .....

And in accordance with the following harmonised standards:

☐ EN ISO 12100	☐ EN 842	☐ EN ISO 11161	☐ EN ISO 13855	☐ EN 60204 - 1
☐ EN 349	☐ EN 953	☐ EN 13478	☐ EN ISO 13857	☐ EN 61310
☐ EN 614 - 1	☐ EN 981	☐ EN ISO 13849	☐ EN ISO 14122	☐
☐ EN 626	☐ EN 1037	☐ EN ISO 13850	☐ EN ISO 14159	☐

As well as in accordance with the following standards or norms:

_____

_____

If a notified body is mentioned above, it has performed a module G conformity assessment check as set out in the Decision 768/2008/EC and issued a certificate of conformity.
Otherwise, the conformity has been assessed by the manufacturer or his authorised representative according to module A or A1 as set out in the Decision 768/2008/EC.

A technical file in accordance with Annex VII part A of Directive 2006/42/EC has been compiled, a copy can be requested via registered letter addressed to the Vice President Production Engineering, Toyota Motor Europe NV/SA at the abovementioned address and will be provided in electronic format.

Location & Date of issuance of the Declaration: _____

Name: _____
Function: _____
On behalf of: _____

Signature & Company Stamp