機能安全活用実践マニュアル

統合生産システム(IMS)編

平成 30 年度厚生労働省委託

機能安全を活用した機械設備の安全対策の推進事業

平成 31 年 3 月

一般社団法人　安全・環境マネジメント協会

はじめに

製造業における生産設備の生産能力と効率の向上のために、生産設備システムの自動化や高度化が指向されており、システム制御技術の進展に加えてシステムエンジニアリングが重要視されるようになってきた。システムエンジニアリングにおいては、生産設備を構成する個々の機械の機能や特徴を把握した上でシステム統合を行わねばならず、最終的にはシステムの目標仕様を、コストパフォーマンスを考慮して実現することが求められる。このようなシステムエンジニアリングの役割を担う立場がシステムインテグレータである。

システムインテグレータは、個々の機械メーカやベンダと生産設備を運用するエンドユーザとの間でシステムの設計から製造、ユーザへの引き渡しまでを行い、近年では、産業用ロボットをはじめとする最新技術を適用するシステムインテグレーション（統合）には不可欠な存在となっている。このようなニーズの下、国内では 2018 年に FA・ロボットシステムインテグレータ協会（通称 SIer 協会）が発足し、システムインテグレータのさらなる活躍が期待されている。しかし、国内でのシステムインテグレーションの歴史は浅く、統合生産システム（IMS）に関する知識やノウハウの蓄積はまだ充分なレベルには達していない。

同様に、統合生産システムにおける安全設計についても、適用する安全知識やスキルは充分普及しているとは言い難く、対応できる人材も充足していない。安全設計の指南となるべき関連安全規格も個別機械やコンポーネントに関しては整備されてきたが、統合生産システムの現行安全規格（ISO 11161）については改訂が遅れている上、この規格で規定されている安全要求事項の実行のための情報が少ないのが現状である。加えて、システム制御の高度化や複雑化が進む中で、システムインテグレーションにおける安全設計の比重と重要性は増しており、システムインテグレータには安全制御への対応能力が求められるようになってきている。

このような状況下で、システムインテグレータが安全設計へ機能安全制御を導入することは必須となりつつあり、「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）が公表され、機能安全規格に準拠した製品（コンポーネント）も市販されるようになってきた。しかし、現実には機能安全を導入した具体的なシステム設計方法を理解することはまだ容易ではない状況にある。

そこで、「機能安全を活用した機械設備の安全対策の推進事業（厚生労働省委託）」の委員会及びワーキンググループにおいて統合生産システムを対象としたシステムインテグレータ向けの機能安全制御の導入、設計方法が議論され、本書が作成された。本書は「安全な生産システムの構築能力向上のための調査研究報告書（日本機械工業連合会発行）」の記載事例を元に作業者と産業用ロボットとの協働運転を新たに想定し、これに対する安全防護の手段として機能安全制御を導入することを目的としている。そのため、安全設計の

過程として、システムインテグレータの役割を明確にした上で、作業や工程の分析、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、及びそれら手段の妥当性の検証についてまとめている。なお、本書の理解を促進するために、「機能安全活用テキスト（中央労働災害防止協会発行、厚生労働省ホームページで公開中）」を先にご覧いただき、機能安全の基礎知識について習得しておくことをお勧めする。

～　目次　～

第１章　IMS 設計コンセプト

本書は、機械安全及び機能安全の基礎知識があることを前提として作成しているので、「機能安全活用テキスト」(厚生労働省ホームページ http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html にて公開)を入手して基礎知識を理解しておくことが望ましい。

１．１　機械安全基礎

(1)　機械の安全化の原則

「人はミスを犯し、機械はいつかは故障する」ことは誰もが認識していることであり、その前提の下に機械設備の安全対策をすべきことは、近年では常識として捉えられている。特に、機械設備が高度化、複雑化するに伴い、人の注意に依存して安全確保することの限界が明白となり、機械設備側の安全化のプロセスが重要となってきた。この安全化のプロセスは、「隔離」の原則と「停止」の原則を成立させることであり、人が機械設備の危険な潜在源(危険源)に近づかないようガード等を設置し、もし、ガード内へ近づく場合は機械設備が停止するような仕組みが基本とされ、国際規格 ISO 12100(第 2 章で後述)やそれに整合する「機械の包括的な安全基準に関する指針」(第 2 章で後述)では、それら原則を実現するための保護方策が述べられている。

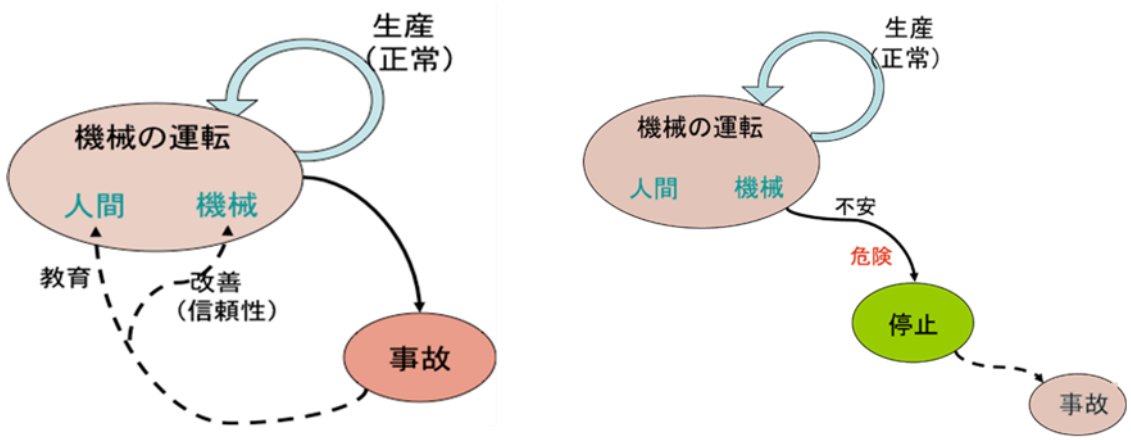
機械設備が産業用ロボットを含む複数の機械が連携するシステムである場合、人や物がその中を移動することを想定すると、上記「隔離」の原則のみの適用は現実的に難しく、「停止」の原則に依存せざるを得ない。しかも、「停止」とは機械設備の重要な制御機能の一つでもあり、機械の故障により停止の失敗は許されない。すなわち、機械の制御機能の故障自体を減らすという高信頼化設計は当然として、さらに、故障の内容(いかに停止できない危険側故障を許容しないか)が問われることになる。

以降、改めて機械の「停止」による安全化原則に対して、安全制御による機能として実現するための考え方を述べる。

(2)　停止による安全確保

機械設備本来の目的である仕事を行うためには、機械自体は正常に機能を発揮して動作し、それに関わる人間は不安なく安全を確保しながら生産に寄与することが求められる。このような合目的的安全状態を維持しつつ機械運転を継続して生産性を向上するのが理想であるが、一度このサイクルから逸脱すると、最悪、事故に至ることになる。事故から生産のプロセスに復帰するためには、機械は修理、改善をし、人間は

教育(反省)してリセットすることになる(図 1-1(a))。しかし、このような事故のフィードバックでは事故の再発は防ぐことはできるが、新しい事故を経験しない限り対策が採れない。そこで、正常な生産サイクルから逸脱しても、事故に至る前にリセットできる段階を準備しておけば、事故を経験せずとも生産のサイクルに戻すことが可能となる。この事故手前の段階は「機械の停止」であり、機械は本来の機能を中止してしまうが、少なくとも人間に危害を及ぼすことはない(図 1-1 (b))



(a) 事故フィードバック　　(b) 停止の確保

図 1-1　人間-機械系における機械停止の仕組み

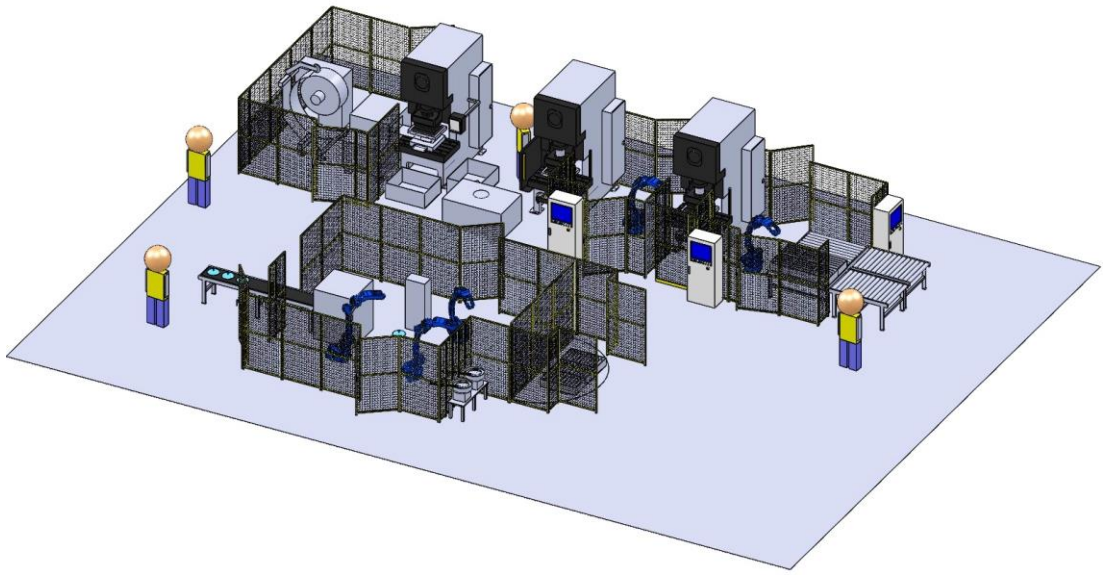


図 1-2　IMS の構成例(「安全な生産システムの構築能力向上のための調査研究報告書」より)

図 1-2 に示すような複数の機械設備が連携して機能する統合生産システム

(Integrated Manufacturing System、以降 IMS と表記する)であっても、上記の「停止による安全確保」の原則は適用される。人間に対して危害を及ぼす可能性の

ある個々の機械(危険源)について、この原則を確立した上で複数機械の運用を考えるべきである。

(3) インタロックに基づく安全制御

一般に、機械を運転する制御系は目的の仕事を達成するために様々な情報や物理量を処理して、結果的に人間の安全状態が確保される。例えば、移動するロボットでは、走行路上の障害物検知によりナビゲーションが成功していれば周囲の人間に衝突することはない。このような制御系(基本制御系と言う)はなるべく本来の機能を維持できるように、高信頼化設計が指向される。正常な制御機能が維持されている限り、人間の安全も確保できることになる。

しかし、運転のための基本制御系も故障や異常の発生は避けられず、これらの機能不全に対して何らかの措置が必要となり、別途、人間の安全を確保する制御系を用意する。この制御は基本制御系に優先して機械の運転停止をもたらす機能、すなわちインタロック機能を有し、この制御系を安全制御系と言う。このようなインタロックを成す制御部は安全関連システムと呼ばれ、基本制御系とは分離して独立で機能させる。

安全制御系におけるインタロック機能は、基本的に図 1-3 の論理積要素で表現される。誤りを含む運転指令入力に対して、運転許可を与える入力は「安全でないにもかかわらず許可を出す」という誤りは許されない。すなわち、安全状態を検出して安全情報を生成する手段(図中の安全確認センサ)には故障に対する出力特性が規定される。同様に、論理積(AND ゲート)演算も、両入力がないにもかかわらず運転出力してはならない特性が要求される。このような物理的特性はフェールセーフと呼ばれ、正常性が確認できなければ、たとえ安全状態を検出しても安全情報を出力しないものとして、電気的にも本質的にエネルギーが小さいことで証明されていたが、電気信号処理の分野では故障時には著しく安全側に遷移する特性(非対称誤り特性)で実現されている。

同様に、論理積(AND ゲート)演算も、両入力がないにもかかわらず運転出力してはならない特性が要求される。そのため、安全関連システムにおける安全制御の基本構成の考え方は、図 1-4 に示すように非安全関連システムと安全関連システムが独立し、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出力が発生することである。安全関連システムの運転許可部分は安全確認型センサが該当し、この部分は安全確保を担う役割のため、非安全関連システムから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 機能は安全関連システムの一部であることに注意が必要である。

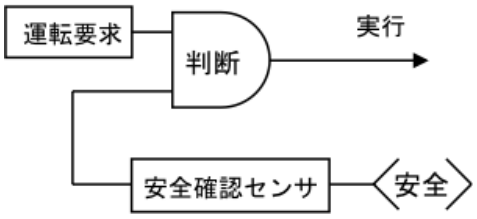


図 1-3　インタロックの基本構造

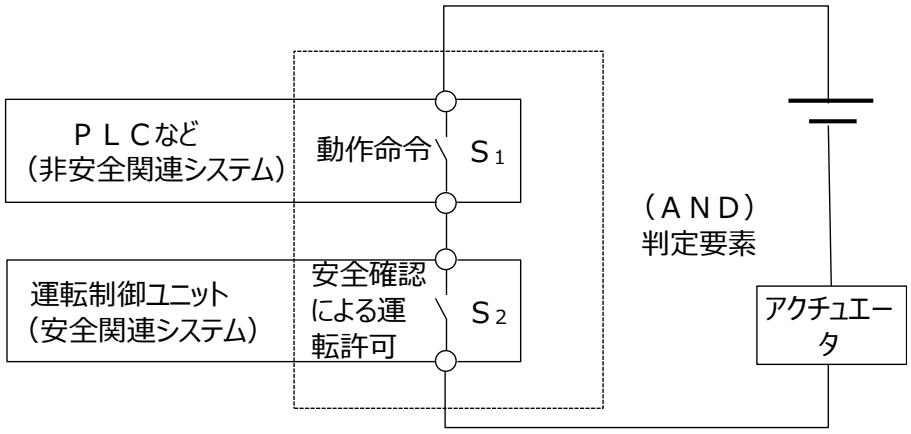


図 1-4　制御システム内の分離と独立

(4) IMS 安全関連システムへの機能安全の導入

図 1-4 に示すようなインタロック構造は電磁リレーを用いて容易に実現でき、安全関連部と非安全関連部は独立した接点として分離している。しかし、現在では、接点が電子式装置に置き換わり、さらにはソフトウェアが関与するようになって、機能安全機器を導入して制御システム全体をフレキシブル化、高機能化することが可能となってきた。

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。従来の非対称誤り特性を有する部品のみに依存せずに、機能診断や冗長化等の高信頼化技術の導入により、危険検出型構造であってもインタロックに適用可能な製品が登場している(ただし、適用範囲はこのセンサの安全性能に依存する)。

以上のような技術的進展に伴い、複合機械システムである IMS の安全関連システムにも機能安全は導入されつつあり、IMS の中核をなす産業用ロボットや連動する周辺

機械設備のシステム統合には、不可欠な技術となりつつある。例えば、産業用ロボットには機能安全制御が盛り込まれている機種があり、ロボットシステム化のためにこの制御の機能を活用することが可能となっている。すなわち、単体機械の安全関連システム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という前提でシステム拡張を図ることができる。

IMS を対象とした複数機械設備のシステムインテグレーションも、個別の機械設備の安全方策を実施した上で、追加のシステム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、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きており(規格上)、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

(5) IMS 安全関連システムによるリスク低減の役割

前述の通り、IMS を構成する個々の機械設備は、基本機械安全規格や個別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、これらの機械設備が装備している安全機能の性能が、システム統合化によって少なくとも損なうことがないように設計することを基本とする。そのため、本書ではシステム統合で追加される安全要件のうち、IMS の安全関連システムに機能安全を導入する場合に関連する事項を対象とする。これは、対象 IMS の工程や作業の分析後に行うリスクアセスメントの結果に基づき、必要な安全性能目標を定めて、それを実現する方策の選定と安全性の妥当性を検証するまでの過程を網羅する。この過程における機能安全制御の位置付けについて、先に論じておく。

IMS の安全関連システムによるリスク低減は、本書で後述するリスクアセスメントの結果に基づいて実施されるが、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 1-5 参照)。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される。すなわち、制御以外の本質的設計や受動的・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。

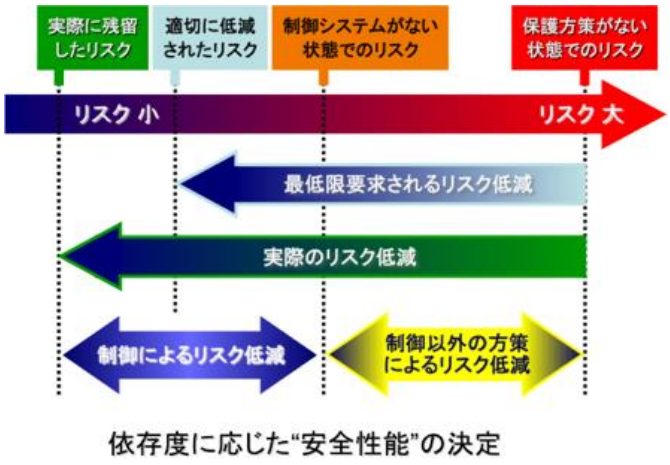


図 1-5　制御によるリスク低減の概念

１．２ IMS 設計コンセプト

IMS の設計が、一般的な機械の設計と典型的に異なることは、ある機械システムやラインの構築のために様々な機械機能を組み合わせることである。その組み合わせを行うシステムインテグレータは、必ずしも個々の機械機能や工程に精通したエキスパートがなるわけではない。例えば、マシニングセンタを主要な

機能としてその周辺にいくつかの機械を並べシステムとして統合させた場合、マシニングセンタを製造する機械メーカがその統合も行うのであれば、主たる機能の研削プロセスについての十分な経験や知識を持ち合わせたシステムインテグレータとなり得る。しかし、このような事情がない限り、システムインテグレータは、一般にはユーザ、機械メーカとは別の立場で、共にコミュニケーションを密にとりながら、システム統合を行うことが必要となる。以降、本書ではシステムインテグレータのことを略してインテグレータと呼ぶ。

インテグレータは関連規格 ISO 11161(第 2 章で後述)では、次のように定義されている。

統合生産システム(IMS)の設計、供給、製造又は組立を行い、保護方策、制御インターフェース及び制御システムの相互接続を含む安全戦略を担当するもの 注記 インテグレータは、メーカ、組立者、エンジニアリング会社又はユーザである場合がある

すなわち、生産システムを構築し、安全の方針を決定・実現する人であり、製造、組立、エンジニアリング会社あるいはユーザであってもよい。

インテグレータが行うタスクの概略を示すと次のようになる。

生産システムの設計 リスクアセスメント 工程分析 作業分析(作業と作業ゾーン) リスク/危険分析による安全戦略の決定 安全戦略に基づく安全防護(ガードと保護装置)の決定 制御範囲の決定 システムの評価及び妥当性確認

１．３ IMS に求められる安全機能

IMS に必要な安全機能は、システム設計次第であることは言うまでもないが、以下の要素はほとんどの IMS に関わる。

- 非常停止及びインタロック制御に関連する停止、あるいは遮断の範囲とアクセス

可能な範囲との関係
この要素はタスクゾーンと制御範囲の関係性として、4.2 節で述べる。

- 調整作業時の、ローカル操作モード
  この要素は操作モードと制御範囲の関係性であるが、今回は触れていない。
- 各機械に加える改造及び安全に関わる信号のやり取り
  この要素は、今回のモデルではプレスの固定ガードの取り外しとして扱っている。
- はしごなどの接近手段の設置による新たなアクセス可能な危険源の発生
  この要素は、今回のモデルでは具体的な項目として登場していない。
- 機械設計としての確からしさ
  例えば、ロボットと固定物の間のクリアランスの確保や、周囲ガードと危険源の安全距離、ライトカーテンなどの検知保護設備の設置位置要求、ガードの強度や、放出物、騒音、放射源などに対する防護性能など。
- 人間工学設計原則

インテグレータは上記の要素を加味し、IMS の安全機能を設計することになる。特に、IMS として特徴的な仕様は、システム全体を停止せずに安全の制御を生かす仕組みにあり、この部分は IMS の安全機能として大きな割合を占める。仮に、システム全体を一括停止するシステムであっても、ローカル操作モードで個別の機械の操作を許す場合やシステム内のいくつかの機械を連動させた調整作業をする場合には、非常停止やインタロック信号の及ぼす制御範囲の検討が必要となる。そのため、タスクゾーンと制御範囲の関係性を吟味してリスクアセスメントを行い、その結果に基づくリスク低減が必要となる。

その他、最近の機械安全においては、ネットワーク時代におけるセキュリティ関連の脅威が取りざたされるようになってきている。例えばウイルスやハッキングなどによる情報の流出や生産の妨害あるいは安全性の低下や安全機能の乗っ取りなどの懸念が現実化しつつある。これらの事象については今回扱わないが、当然、今後の機械設計の課題となる。

1．4 インテグレータが有するべき能力

1.2 節で述べたようにインテグレータは様々な立場がなり得るが、複数の機械をシステムインテグレーション(統合)する担当者とすることが必要である。安全に対する担当者の所在と当事者意識が無いまま仕様が決まることがないよう、複数の機械メーカが存在する統合生産システムの場合は、誰がそのシステム統合における機械安全の担当者となるかを事前に明確にしておかなければならない。これは統合生産システム特有の事象であり、決して自然発生的に決まるものではない。

システム設計においては、個々の機械機能や性能、能力等の詳細はそれらの機械メーカが準備する情報であり、インテグレータはそれらの情報を基に適切な機械やその性能を選ぶこととなる。この作業にもノウハウは必要であるが、特に安全面に関しては、システム化や設置の点から機械メーカの範囲外となる場合も多く、インテグレータの役割が大きい。

前出 ISO 11161 などに適合したシステムを設計できるグローバルなインテグレータとなるには、積極的にシステムに対するリスクアセスメント能力を向上させることが肝要である。ユーザ、メーカ、インテグレータの三者における設計レビューにおいて、機械安全の視点からのリスクアセスメントを主導してまとめ上げることは、インテグレータにとっては非常に重要な能力である。特に、システムの仕様決定段階あるいはシステム設計初期段階から、必要な機械や作業を見越して占有面積やレイアウトを頭に思い描きながら包括的なリスクアセスメントを実施できることが必要である。そのため、機械設計の早期に決定すべき項目を列挙し、それらの設計レビューを繰り返し実施する。例えば、後に詳しく述べる工程分析及び通路や作業スペースなどの人間工学側面も含めた設計レビューを実施し、レイアウト設計へと導くことである。ここで大切なことは、設計の大部分が終わってからリスクアセスメントを行うのではなく、設計初期からリスクアセスメントを実施し、各々の設計レビュー時には、機械のレイアウト、制御、人間工学側面等に対する設計の正しさを確認することである。つまり、リスクアセスメントと設計レビューは不可分で並列的に進行させるべき事項であり、最終段階に至ってリスクアセスメントを行うことにすると、リスクアセスメントの結果を反映させるために、多大な労力、時間、コストがかかってしまう。

また、占有面積や制御盤サイズ、配線ダクトなど後々の変更が難しい機械設計においては、余裕を見た設計手法を採るなどのノウハウの蓄積やユーザとの合意なども必要である。これには、機械的強度が重要になる部分(例：機械シャシやフレーム、ガード、アンカリング、階段やはしごなどの接近手段)なども含まれる。システム設計においては、経験によるノウハウの蓄積の難しさや、それだけでは対応できない事象も多々発生することが考えられる。それを事前に解決するためにもリスクアセスメントを緻密に行う必要がある。

一方、IMS 構築に必要な技術標準類の洗い出しもインテグレータの能力として求められる。IMS 設計前に法令規則、規格類や技術的習慣などを調べ、それらの内容を把握しておかなければ、設計変更が手遅れになったり設置時にそのような不適合が発見されたりすることで致命的なビジネス上のリスクになりかねない。インテグレータは機械側の要素だけではなく、要求事項の変化なども把握するために、常に要求事項の最新情報を入手できる体制を整えておく必要がある。例えば、IMS の中核となり得る協働ロボットに関しては、その使用方法、リスクアセスメント及び妥当性を示す数値的根拠など、新しい知見などにより関連規格の内容が変わる可能性が高く、その変化

に追従していく必要がある。

１．５ IMS 構築のための作業概要

インテグレータが、製品を製造するために複数の単体機械を組み合わせて IMS を構築する作業について、メーカとユーザの関連を含めて作業の流れと概要を表 1-2 に示す。ここに、担当は機械メーカ(M)、機械ユーザ(U)、インテグレータ(I)として表し、各手順が本書で説明されている箇所を示す。

表 1-2 IMS 構築のための安全戦略作業概要

手順	担当	作業内容	解説	本書の対応箇所
1	U(I)	製造製品仕様の決定	製造する製品の形状、材質、構造などの製品仕様及び生産量を決定する。	3.1 仕様の確認
2		統合生産システムの設備選定段階	材料から製品までの製造工程を分析し必要設備を決定する。	3.2 初期工程分析
2.1	U-M (U-I-M)	各工程での製造設備仕様の検討	各工程での生産材、製造設備(単体機械)の必要機械性能・仕様(ユーティリティ含む)を決定する。	
2.2	U-I	各工程及び工程間での作業の検討	各設備(単体機械)における大まかな人の配置を決定する。	
3		統合生産システムの制限仕様の検討段階	各工程での定常作業・非定常作業を検討する。	3.3 後期工程分析
3.1	U-I	各工程での定常作業での人の介入、詳細手順の決定	各設備(単体機械)における段取・設定・調整・生産作業内容の定常作業手順を決定する。	
3.2	U-I	各工程での非定常作業での人の介入の洗い出し	段取り時、トラブル処理などの非定常作業での人の介入を洗い出す。	

4	I	統合生産システムに関連する技術標準類の洗い出しと各設備の妥当性確認	各設備、統合生産システムに関連する法令・技術標準類(機械安全のJIS/ISO/IEC 等)の洗い出しと各設備仕様の妥当性確認を行う。	2.統合生産システム構築関連の法令･規格類
5		統合生産システムの作業分析	製品･設備仕様･工程分析をもとに統合生産システム全体のリスクアセスメントとリスク低減方策を決定する。	3.4 作業分析(作業と作業ゾーン)
5.1	U-I	各機械設備の作業分析	各機械設備に対して各作業者がどのような作業に関わるかを決定する。	
5.2	I	作業ゾーンの決定	5.1 で決定した作業分類で機械設備全体を作業ごとのゾーン(領域)で分ける。	
5.3	I	統合生産システムとしての全作業の整理	統合生産システムとしての全作業ゾーンでの各作業者と各作業の関わりを整理しゾーン間の関連を洗い出す。	
6		統合生産システムの安全戦略(リスクアセスメントとリスク低減方策)	統合生産システム全体の作業分析とその結果に基づくリスクアセスメントとリスク低減方策を決定し妥当性確認を実施する。	4.リスクアセスメントとリスク低減 5.安全要求度水準の決定 6. IMS 安全関連システムの設計と検証
6.1	I	各ゾーンに対するリスクアセスメント(危険源・危険状態・危険事象等についてのリスクの分析・評価)と(リスク評価結果に基づく)リスク	5 の結果から各ゾーンへのアクセスに対するリスクアセスメント(リスクの分析・評価)とリスク低減方策(ガード・インターロック・保護装置)を決定する。	

		低減方策の決定		
6.2	I	各ゾーン間のゾーンまたぎに対するリスクアセスメントとリスク低減方策の決定	6.1 後の各作業ゾーンを通過して別の作業ゾーンへの人及び設備の侵入を考慮したリスクアセスメントとリスク低減を決定する。	
6.3	U-I	制御範囲の決定、整理	6.1、6.2 の結果に基づくリスク低減方策(モード・インターロック・非常停止等)の制御範囲を決定、整理する。	
6.4	I	安全関連システムの機能安全設計	安全関連システムの要求安全度水準PLr を決定し、機能安全設計と安全度水準 PL 評価を行う。	
7		統合生産システムの妥当性確認と技術ファイル	統合生産システムを構築した際の妥当性確認と技術ファイルの作成を行う。	7. IMS 安全関連システムの妥当性確認
7.1	I	妥当性確認	統合生産システムを構築した際の各設備の保護方策の改造、追加の保護方策の妥当性確認を実施する。	
7.2	I	技術ファイル	統合生産システムを構築した各設備・統合生産システムの安全戦略の妥当性確認の技術ファイルを作成し、保管する。	

第２章　統合生産システム構築関連の法令・規格類

２．１　はじめに

国内での機械安全における包括的指針は、平成 13 年(2001 年)都道府県労働局長宛に示された「機械の包括的な安全基準に関する指針(平成 13 年 6 月 1 日基発第 501 号)」(機械包括安全指針とする)である。この指針は、機械安全のための設計の一般原則(リスクアセスメント及びリスク低減)と妥当性確認が示されている国際規格原案 ISO/DIS　12100-1、-2(2000 年)に基づいて示されている。この指針の特徴は、設計者の安全な機械の設計のための規格である機械安全の国際規格原案を機械製造者(設計者)と機械使用者の双方に対して適用する指針として示されていることである。

その後、ISO 12100-1、-2:2003(JIS B 9700-1、-2:2004)が制定され、さらに平成 18 年(2006 年)に労働安全衛生法第 28 条の 2 の公布によりリスクアセスメントとそれに基づくリスク低減が規定されたことを踏まえて機械包括安全指針も平成 19 年(2007 年)に改正された。機械包括安全指針は、国際的な安全規格を基にした指針である。

本章では、まず産業用機械を組み合わせて構築する統合生産システム構築に必要な機械安全、機能安全関連の法令と指針について示す。そして機械包括安全指針の適用も踏まえて、機械の安全規格の中でも安全に関わる制御システム(安全関連システム)構築に使用される機能安全の規格について安全関連システムの設計者が参考とすべき機能安全の規格を理解する上での重要用語について紹介する。

２．２　統合生産に関連する機械安全、機能安全関連の法令と指針

労働現場での統合生産システム構築で留意すべき主要な法令として以下が挙げられる。

(1)労働安全衛生法　第 3 条(事業者等の責務)

では、労働者の安全と健康確保のための義務主体が示されている。生産現場に関連する部分(第 1 項、2 項)の抜粋をまとめると図 2-1 となる。事業者、機械及び統合生産を設計するインテグレータも含めその責務についての理解が必要である。

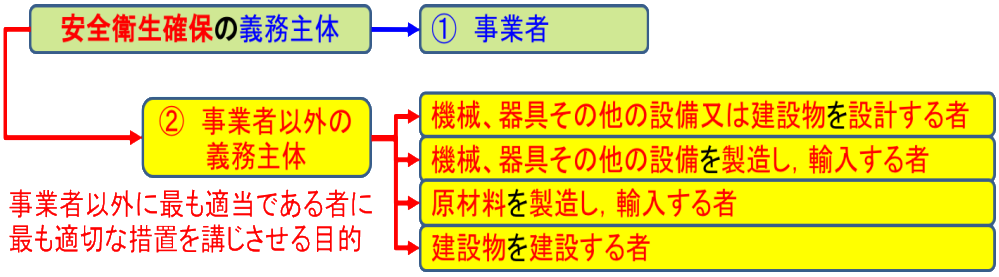


図 2-1 安全衛生確保の義務主体

(2) 労働安全衛生法　第 20 条（事業者の講ずべき措置等）抜粋

機械設備にも関わる事業者の措置内容で、統合生産システム構築時は考慮する必要がある法律であり、労働安全衛生規則　第 101 条～151 条の（機械による危険の防止）一般、個別機械の安全基準と合わせての理解が必要である。

第 20 条 事業者は、次の危険を防止するため必要な措置を講じなければならない。

一 機械、器具その他の設備（以下「機械等」という）による危険

二 爆発性の物、発火性の物、引火性の物等による危険

三 電気、熱その他のエネルギーによる危険

(3) 労働安全衛生法　第 28 条の 2（事業者の行うべき調査等）抜粋

労働安全衛生法　第 20 条を適切に対応するためのリスクアセスメントとリスクアセスメントの結果に基づくリスク低減の推進が示されている。関連指針と合わせて統合生産システム構築のために理解しておくことが必要な法律である。

「事業者は、厚生労働省令で定めるところにより、建設物、設備、原材料、ガス、蒸気、粉じん等による、又は作業行動その他業務に起因する危険性又は有害性等を調査し、その結果に基づいて、この法律又はこれに基づく命令の規定による措置を講ずるほか、労働者の危険又は健康障害を防止するため必要な措置を講ずるように努めなければならない。ただし、当該調査のうち、化学物質、化学物質を含有する製剤その他の物で労働者の危険又は健康障害を生ずるおそれのあるものに係るもの以外のものについては、製造業その他厚生労働省令で定める業種に属する事業者に限る。

2 厚生労働大臣は、前条第一項及び第三項に定めるもののほか、前項の措置に関して、その適切かつ有効な実施を図るため必要な指針を公表するものとする。」

(4) 統合生産システム構築(機械安全、機能安全推進)に関連する厚生労働省指針

① 2006 年(平成 18 年)危険性又は有害性等の調査等に関する指針

https://www.mhlw.go.jp/file/06-Seisakujouhou-11300000-Roudoukijunkyokuanzeneiseibu/0000077404.pdf

② 2007 年(平成 19 年)改正機械の包括的な安全基準に関する指針

https://www.mhlw.go.jp/file/05-Shingikai-11201000-Roudoukijunkyoku-Soumuka/0000021042.pdf

③ 2015 年(平成 28 年)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

https://www.mhlw.go.jp/file/06-Seisakujouhou-11300000-Roudoukijunkyokuanzeneiseibu/0000140170.pdf

２．３　統合生産システム構築で使用する重要用語の説明

(1)　統合生産システム構築で使用する用語

本書では、「機械の包括的な安全基準に関する指針」および「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)に示される用語およびそれ以外に統合生産システム構築で使用する基本的な用語について表 2-1 に示す。なお、ここに記載した用語定義と、JIS の用語定義とは相違する点があるが、本書では、表 2-1 の定義を使用する。

表 2-1　統合生産システム構築に使われる主要な用語

No.	用語 定義または概念
1	**機械** 連結された構成品又は部品の組合せで、そのうちの少なくとも一つは機械的な作動機構、制御部及び動力部を備えて動くものであって、特に材料の加工、処理、移動、梱包等の 特定の用途に合うように統合されたものをいう。
2	**リスク** 機械等による労働者の就業に係る負傷又は疾病の重篤度及び発生の可能性の度合い。
3	**危険事象** 機械等による労働者の就業に係る危険性又は有害性の結果として労働者に就業上の負傷又は疾病を生じさせる事象。
4	**保護方策/リスク低減方策** 機械のリスク(危険性又は有害性によって生ずるおそれのある負傷又は疾病の重篤度及び発生する可能性の度合をいう。以下同じ)の低減(危険性又は有害性の除去を含 む。以下同じ)のための措置をいう。 これには、本質的安全設計方策、安全防護、付加保護方策、使用上の情報の提供及び作業の実施体制の整備、作業手順の整備、労働者に対する 教育訓練の実施等及び保護具の使用を含む。
5	**本質的安全設計方策** ガード又は保護装置(機械に取り付けることにより、単独で、又はガードと組み合わせて使用する光線式安全装置、両手操作制御装置等のリスクの低減のため の装置をいう)を使用しないで、機械の設計又は運転特性を変更することによる保護方策を いう。

No.	用語 定義または概念
6	**安全防護** ガード又は保護装置の使用による保護方策をいう。
7	**付加保護方策** 労働災害に至る緊急事態からの回避等のために行う保護方策(本質的安全設計方策、安全防護及び使用上の情報以外のものに限る)。
8	**使用上の情報** 安全で、かつ正しい機械の使用を確実にするために、製造等を行う者が、標識、警告表示の貼付、信号装置又は警報装置の設置、取扱説明書等の交付等により提供する指示事項等の情報をいう。
9	**残留リスク** 保護方策を講じた後に残るリスク。
10	**機械の意図する使用** 使用上の情報により示される、製造等を行う者が予定している機械の使用をいい、設定、教示、工程の切替え、運転、そうじ、保守点検等を含む。
11	**合理的に予見可能な誤使用** 製造等を行う者が意図していない機械の使用であって、容易に予見できる人間の挙動から行われるもの。
12	**統合生産システム IMS** 材料のハンドリングシステムによってリンクされ協調して一緒に作業する機械のグループで個別の部品または組立品の製造、処理、移動またはパッケージングの目的で、制御装置(すなわち、IMS 制御装置)によって相互接続されているもの。
13	**インテグレータ** 統合生産システムを設計、提供、製造または組み立て、保護方策、制御インタフェース、および制御システムの相互接続を含む安全戦略を担当する者。 注記：インテグレータは、製造業者、エンジニアリング会社、またはユーザであってもよい。

No.	用語 定義または概念
14	**サプライヤー(供給者)** IMS または IMS の一部に関連する機器またはサービスを提供する者(例えば、設計者、製造業者、請負業者、設置者、インテグレータ)。 注記：ユーザはサプライヤーの能力で行動することもできる。
15	**ユーザ(使用者)** IMS を利用し維持する人または人達。
16	**オペレーター(作業者)** 機械の設置、使用、調整、維持、清掃、修理または輸送の任務を与えられた人または人。
17	**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制御(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)（JIS B 9705-1/ISO 13849-2)、機械の安全関連制御システム(SRECS)(JIS B 9961)と同じ意味で用いる。
18	**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がらないような本システムの機能。
19	**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を特定した上で、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。
20	**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)
21	**要求安全度水準** 安全関連システムに要求される信頼性の水準。 要求安全機能の作動が要求された時に、安全関連システムが当該要求安全機能を作動させる確率であり、その水準を表す指標として、JIS C 0508 (IEC 61508)の安全度水準又は JIS B 9705(ISO 13849)のパフォーマンスレベルが用いられる。

No.	用語 定義または概念
22	**作動要求頻度** 要求安全機能の作動が求められる頻度。
23	**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)
24	**障害/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)
25	**危険側故障(dangerous failure)** 制御システムの安全関連部(SRP/CS)を危険状態又は機能不能状態に導く潜在性をもつ故障。
26	**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)
27	**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。
28	**共通原因故障(CCF)** 1つ以上の事象に起因する故障。(JIS B 9961)
29	**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)
30	**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)

２．４　統合生産システム構築に使用する主要規格

統合生産システムを構築する場合、インテグレータは、生産システムに関わる機械設備の法令以外に機械安全の設計を進める上で最も重要な ISO 12100(ISO の A 規格：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)の運用能力に加え、機械設備固有の技術規格(ISO の C 規格)がある場合はその理解と統合生産システムの具体的なリスク低減の設計に使用される国際規格(ISO の B 規格及び IEC の電気安全、機能安全、安全機器・装置の選定と運用に関する規格)の理解とその運用能力が必要である。

図 2-2 は、ISO の C 規格に示されているプレス機械とロボットを使用した統合生産システム構築を事例に、システム構築で求められる規格体系を関連図として示す。

表 2-2 は、図 2-2 に示されている統合生産システム構築に必要な主要規格について種類別に分類し、分類した規格群の概要である。主要規格 JIS の前に*印が示されている JIS 規格は、国際規格に対して JIS 化が遅れていることを示し、主要規格 JIS の後ろに(一致)と記載されている JIS 規格は、対応する国際規格との内容の一致を意味している。*印が示されている JIS 規格については、最新の国際規格も参照してリスク低減方策を進めることを推奨する。

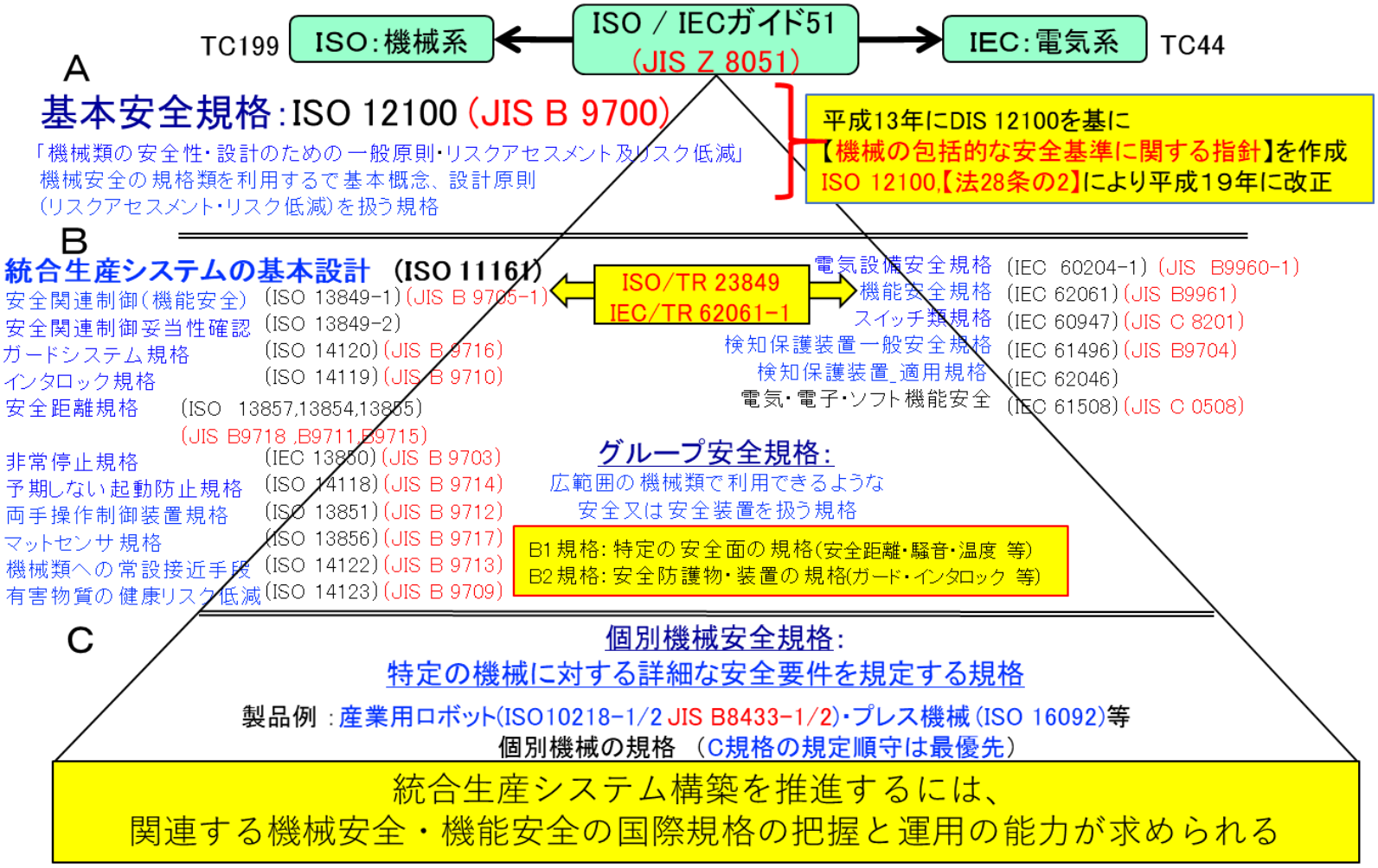


図 2-2 統合生産システム構築に求められる規格体系例

表 2-2　統合生産システム構築に使われる主要規格と概要

規格番号(A)・電気	「機械類の安全性」関連の ISO・IEC 及び関連規格の名称と概要
ISO 12100:2010 JIS B 9700:2013(一致)	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
ISO/TR 22100-1:2015	機械類の安全性―ISO 12100 との関連－第 1 部：ISO 12100 はどのようにタイプ B 及びタイプ C 規格に関連付いているか
ISO/TR 22100-2:2013	機械類の安全性―ISO 12100 との関連－第 2 部：ISO 12100 はどのように ISO 13849-1 に関連付いているか
ISO/TR 22100-3:2016	機械類の安全性―ISO 12100 との関連－第 3 部：安全性規格への人間工学の導入
ISO 12100 は、機械安全を進めるための基本原則が示された唯一の規格で ISO 規格の分類では「A 規格」とされている。 機械設計者が機械安全設計を行うための基本用語、原則、および方法論を規定している。方法論としてリスクアセスメントとリスク低減の原則であるスリーステップメソッド(本質的安全設計方策・安全防護と付加保護方策・使用上の情報)に関する具体的リスク低減の考え方と妥当性の文書化内容について示されている。本規格で示された方法論をもとに以下に示した B 規格・C 規格を加味して機械安全の設計を進めることになる。 また、各 TR(技術報告書)Part1-Part3 は、ISO 12100 の補足としてそれぞれの内容についてリスクアセスメント、リスク低減を進める上での基本的な考え方の側面が示されている。	
IEC 60204-1 :2016 *JIS B 9960-1:2008	機械類の安全性―機械の電気機器－第 1 部：一般要求事項
IEC 60204-11 :2018 *JIS B 9960-11:2004	機械類の安全性―機械の電気機器－第 11 部：1000 VAC 又は 1500 VDC を超え、又 36 kV を超えない電圧用機器の要求事項
上記規格は、各供給電圧区分における機械安全設計の電気設計(感電防止、火災防止)における本質的安全設計方策としての実施内容を示している。方策として外部配線、遮断装置、機器・配線保護、保護接地、制御回路、表示・押しボタン、盤構造、配線・配線方法、モータなどの動力関連機器、照明、標識、技術文書、検証などの具体的な実施基準が示されている。	

規格番号(B)	「機械類の安全性」関連の ISO・IEC 及び関連規格の名称と概要
ISO 13849-1:2015 *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
IEC 62061 :2015 *JIS B 9961:2008	機械類の安全性―安全関連電気・電子・プログラマブル電子制御系の機能安全
ISO 13849-2:2012	機械類の安全性―制御システムの安全関連部－第 2 部：妥当性確認
ISO/TR 23849:2010 IEC/TR 62061-1:2010	機械類の安全性―ISO 13849-1 及び IEC 62061 の機械の安全関連制御システムへの設計への適用の手引
上記規格は、機械安全設計におけるリスクレベルに対応した制御システムの安全関連部の構築(PL/SIL)に関する要求性能の決定から具体的な制御システムの要求性能の達成に関する技術的な考え方、実施内容と妥当性検証の手順について示されている。 また、TR(技術報告書)が、ISO と IEC から発行されているが、内容は同一である。本 TR は、制御システムを構築する場合に IEC 62061(IEC 61508)で構築された電気・電子制御システム(ソフト含む)と ISO 13849 評価関連機器であるインタロックのリミットスイッチ、リレー、コンタクタなどを組み合わせた場合の制御システム性能の妥当性検証の具体的手順が示されている。	
ISO 14118:2017 *JIS B 9714:2006	機械類の安全性―予期しない起動の防止
上記規格は、予期しない起動を防止するためのあらゆる動力源の遮断、エネルギー消散、機械の可動部の固定を含めた予期しない起動防止の技術的手段が示されている。	
ISO 13850:2015 *JIS B 9703:2011	機械類の安全性―非常停止―設計原則
上記規格は、非常停止機能の設計の要求事項、非常停止機器の要求事項及び非常停止機器の運用についての要求事項が示されている。	
ISO 14120:2015 *JIS B 9716:2006	機械類の安全性―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
ISO 14119:2013 *JIS B 9710:2006	機械類の安全性―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
上記規格は、安全防護としての各ガード(固定ガード、可動ガード)を設計するための要求事項及び可動ガードのインタロックを設計するためのインタロックの原則、インタロック装置の規定、インタロックの位置検知器の作動モード、設置、固定、無効化等に関する要求事項が示されている。	

規格番号(B)	「機械類の安全性」関連の ISO・IEC 及び関連規格の名称と概要
ISO 13851:2002 JIS B 9712:2006（一致）	機械類の安全性―両手操作制御装置―機能的側面及び設計原則
上記規格は、両手操作制御装置を安全防護として使用する際の設計原則として、両手操作制御装置の構造、制御システムの安全関連部としての両手操作制御装置の選定基準の分類(タイプⅠ・Ⅱ・Ⅲ(A/B/C))及び設計上の顧慮事項が示されている。	
IEC 62046 :2018	機械類の安全性－人の存在を検出するための保護機器の応用
IEC 61496-1:2012 JIS B 9704-1:2015(一致)	機械類の安全性―電気的検知保護設備―第 1 部：一般要求事項及び試験
IEC 61496-2:2013 JIS B 9704-2:2017(一致)	機械類の安全性―電気的検知保護設備―第 2 部：能動的光電保護装置を使う設備に対する要求事項
IEC 61496-3:2008 JIS B 9704-3:2011(一致)	機械類の安全性―電気的検知保護設備―第 3 部：拡散反射形能動的光電保護装置に対する要求事項
IEC 62046 は、各検知保護装置の選定基準、機械設備に使用する際の設置基準、ミューティング(一次的無効化)、機械起動時の再起動インタロックなどの具体的適用方法が示されている。 IEC 61496 シリーズは、電気的検知保護設備(光線式安全装置、レーザースキャナ等)の装置製造者の要求事項及び装置選定に対する安全関連部に使用する際の故障に対する耐性(危険側故障回避)のレベルが示されている。	
ISO 13856-1:2013 *JIS B 9717-1:2011	機械類の安全性―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
ISO 13856-2:2013	機械類の安全性－感圧保護装置－第 2 部：感圧エッジ及び感圧バーの設計及び試験の一般原則
ISO 13856-3:2013	機械類の安全性－感圧保護装置－第 3 部：感圧バンパー、プレート、ワイヤ及び類似装置の設計及び試験の一般原則
上記規格は、感圧検知保護装置(感圧検知マット、感圧検知フロア、感圧エッジ、感圧バー、感圧バンパー)などに関する保護装置の製造者に対する装置の要求事項、テスト方法についての要求事項が示されている。	

規格番号(B)	「機械類の安全性」関連の ISO・IEC 及び関連規格の名称と概要
ISO 13854:2017 *JIS B 9711:2002	機械類の安全性―人体部位が押しつぶされることを回避するための最小すきま
ISO 13857:2008 JIS B 9718:2013(一致)	機械類の安全性―危険区域に上肢及び下肢が到達することを防止するための安全距離
ISO 13855:2010 JIS B 9715:2013 (一致)	機械類の安全性―人体部位の接近速度に基づく安全防護物の位置決め
ISO 13854 は、本質的安全設計方策として固定部と可動部間での各人体部位が挟まれによる危害を回避するための最低隙間が示されている。 ISO 13857 は、ガードを設計する際に安全防護としての危害を及ぼす危険源領域に対する安全距離を確保するためのガードの高さ、カードから危険源までの安全距離の確保及びカードの開口部形状と開口部寸法に対する開口部からの危険源までの安全距離の確保についての設計内容が示されている。 ISO 13855 は、検知保護装置、インタロック装置、両手操作制御装置等による装置が作動してから人が危険原意到達するまでに危険源が停止することを前提とした安全防護の最小距離(各機器を設置する際の最低限の安全距離)の算出方法が示されている。	
ISO 14122-1:2016 *JIS B 9713-1:2004	機械類の安全性―機械類への常設接近手段―第 1 部:高低差のある 2 か所間の固定された昇降設備の選択
ISO 14122-2:2016 *JIS B 9713-2:2004	機械類の安全性－機械類への常設接近手段－第 2 部:作業用プラットフォーム及び通路
ISO 14122-3:2016 *JIS B 9713-3:2004	機械類の安全性―機械類への常設接近手段―第 3 部:階段、段はしご及び防護さく(柵)
ISO 14122-4:2016 *JIS B 9713-4:2004	機械類の安全性―機械類への常設接近手段―第 4 部:固定はしご
上記規格類は、機械への安全ない接近手段として常設する昇降設備、プラットフォーム、通路、階段、はしご、昇降装置に設置する柵などの設計基準が示されている。	
ISO 14123-1:2015 *JIS B 9709-1:2001	機械類の安全性―機械類から放出される危険物質による健康へのリスクの低減―第 1 部:機械類製造者のための原則及び仕様
ISO 14123-2:2015 *JIS B 9709-2:2001	機械類の安全性―機械類から放出される危険物質による健康へのリスクの低減―第 2 部:検証手順に関する方法論
上記規格は、機械設備から放出される危険物質による健康へのリスクを制限するための一般原則とリスク提言手順と検証手段について示されている。	

規格番号(B)	「機械類の安全性」関連の ISO・IEC 及び関連規格の名称と概要
IEC 61310-1:2007 JIS B 9706-1:2009(一致)	機械類の安全性―表示、マーキング及び操作―第１部：視覚、聴覚及び触覚シグナルの要求事項
IEC 61310-2:2007 JIS B 9706-2:2009(一致)	機械類の安全性―表示、マーキング及び操作―第２部：マーキングの要求事項
IEC 61310-3:2007 JIS B 9706-3:2009(一致)	機械の安全性－指示、マーキング及び作動－第３部：アクチュエータの位置及び操作の要求事項

上記規格の第１部は、機械の HMI において、また、危険区域内にいる人に対して、安全関連情報を伝達するための視覚的手段、聴覚的手段及び触覚的手段に対する要求事項、危険状態、健康に害を及ぼす状態及び何らかの非常事態を示すための、色、安全標識、マーキング及びその他の警告手段、また、機械類を安全に使用し、監視するために用いる表示機器及び操作機器における、視覚シグナル、聴覚シグナル及び触覚シグナルのコード化について規定している。

第２部は、機械の識別のためのマーキング、機械的危険源及び電気的危険源を回避して機械を安全に使用するためマーキング、及び誤接続によって生じる危険源を回避するためマーキングの一般要求事項を規定している。

第３部は、ヒューマン マシン インタフェースにおいて、人が手又は他の身体部分によって操作するアクチュエータに対する安全関連の要求事項としてアクチュエータの動きの標準的方向、アクチュエータの相互配置などが示されている。

規格番号(C)	「機械類の安全性」関連の ISO・IEC 及び関連規格の名称と概要
ISO 10218-1:2011 JIS B 8433-1:2015(一致)	ロボット及びロボット装置－産業用ロボットの安全要求事項－第 1 部：ロボット
ISO 10218-2:2011 JIS B 8433-2:2015(一致)	ロボット及びロボット装置－産業用ロボットの安全要求事項－第 2 部：ロボットシステム及び統合
ISO/TS 15066:2016 TS B 0033:2017(一致)	ロボット及びロボティックデバイス－協働ロボット
IEC 61800-5-2 :2016	可変速電力ドライブシステム－第 5-2 部：安全要求事項－機能
上記規格類は、産業ロボット単体を構築するための要求事項、産業ロボットを使用して生産システムを構築するための要求事項を示している。また、 IEC 61800-5-2 は、産業ロボットを構築するための可変速モータドライブの各安全機能について規定されている。	
ISO 16092-1:2017	機械工具の安全―プレス―Part1:一般安全原則
DIS 16092-2	機械工具の安全―プレス―Part2:機械プレスの安全要求事項
ISO 16092-3:2017	機械工具の安全―プレス―Part3:液圧プレスの安全要求事項
DIS 16092-4	機械工具の安全―プレス―Part4:空圧プレスの安全要求事項
上記規格は、プレス機械とプレス機械に付属する装置(ダイクッション、自動化登に使用される材料、製品の搬送システム等)を設計するための安全要求事項が示されている。	

第 3 章 IMS 構築手順

第 1 章の表 1-2 にしたがって、IMS 構築の検討作業を具体的な製造製品事例について説明する。対象事例は、「平成 28 年度安全な生産システムの構築能力向上のための調査研究報告書」(日本機械工業連合会)で検討された鍋蓋の製造を取り上げる。

３．１ 仕様の確認

表 1-2 の最初の手順 1 は、インテグレータがユーザからの製造製品仕様を確認、決定することである。この段階では、通常は詳細な仕様条件まで決定していないことも多いが、インテグレータとユーザ間での仕様書の取り交わしは必ず実施すべきである。国内では仕様が曖昧なまま手順を進める場合もあり得るが、欧州では安全に関する仕様条件の提示が明確にされ、例えば CE マーキングの一言だけが書かれていたり、ISO 12100 及び IEC 60204-1 適合のような規格番号のみが書かれていたりする場合が多い。これらの簡易な表現しかなくても、それらを引用する多くの規格が紐付けられていることもあり、インテグレータは機械安全規格体系の全体を知っておくべきことに注意が必要である。

その他、要求仕様には適合する法律、規則、規格、標準などの記載と、製造するワークピースに必要な品質レベルなども記載されるため、それらも満たすシステム設計とする必要がある。

以降、ユーザから提供される鍋蓋製造(ステンレス 1t 板から取手付き鍋蓋を製作する)ラインの仕様書例(表 3-1)を基に、製造工程を検討して必要な機械機能を絞り込んでゆく。

表 3-1　鍋蓋製造ライン仕様書

1. ラ イ ン 構 想	(1)ステンレスシートロール(幅 350㎜～450㎜ 1t 100m)を天井クレーンでセットする。 (2)ステンレスシートからプレス機で円盤素材を作る。円盤素材は、素材台車に人手でセットし加工工程に手搬送する。 (3)円盤素材を人がプレスにセットして蓋形状に成型する。 (4)成型された蓋中央に取手を取付ける穴(ピアス)をプレス機であける。 (5)中間製品を目視確認後、台車上のパレット(幅 1.5m×奥行き 0.9m)に積み込む。(30 枚/パレット)台車の入れ替えは人が行い、満杯パレットは、組付け工程のインデックステーブルに手搬送される。 (6)中間製品パレットよりロボットでパレタイズして成型された素材の面取りを行う。面取りは回転砥石に素材を回転させながらエッジ部を当て R1(半径 1㎜)で行う。面取り接触部冷却にクーラントを使用し、クーラントは循環処理する。面取りされた製品は、組立て部に供給される。 (7)取手備品は、パーツフィーダで供給しロボットで組立て部に供給される。 (8)組立治具により、ピアスに取手を内側からネジ止めで取付ける。

	(9)組立てられた製品は、ロボットで打刻機に運ばれる。 (10)ロッド番号を刻印する。(レーザ) (11)製品を製品コンベアで搬出する。製品は、人手目視検査後ペグストッカに詰める。
2. 依 頼 範 囲	(1)シート状のラインに使用する機械の選定(予算内でライン設計により使用機器の変更は可とする。)*実際は、発注側と受注側が見積もり段階で使用機器は決定される。 ①プレス 3 台(用途が異なる) ②ロボット 5 台(ハンドリング重量はハンド部重量を含め 5kg とするが、中間加工製品取り出し等での可動範囲により選定する) ③中加工製品取り出しパレット ④インデックステーブル *面取り機、打刻機、組立装置、パーツフィーダ、コンベアは、ユーザ支給とする。 面取り機 W:500×L:300×H:1,300(㎜)(下部に集塵機) 打刻機 W:1、000×L:1、000×H:1,300(㎜)(レーザー刻印器(クラス 1)) (2)ライン設計 (3)取扱説明書作成 (4)インテグレータによる安全方策 (リスクアセスメントシート、残留リスクマップ及び一覧表の提出を含む)
3. ラ イ ン 構 成	(1)製品種類φ300㎜、φ400㎜の二種類 (2)ロッド 1000 個/ロッド (3)タクト 素材投入部人投入で 30sec/個(φ300㎜) 製品合計 15 万個/年(実働日 250 日) 面取り品質上面取り速度は、35㎜/sec とする。(36sec/個:φ400㎜) (4)稼働時間 1 日 8 時間(午前午後 15 分休憩、昼休み 1 時間:実働 6.5 時間) (5)人員配置(4 名:製造担当(各作業員の役割分担は別表による、保守要員は別部署とする。)) コイル素材供給及び中間製品搬送者:1 名(天井クレーン操作者) 素材を絞りピアスラインへ供給する人:1 名 絞りピアスラインから組付けラインへの搬送者:1 名 製品梱包者:1 名 (6)使用環境 屋内 粉塵:周囲への粉塵発生ないこと 気温:35° CMAX 湿度:50%MAX 標高:300m (7)ユーティリティ 電源:200Vac 3φ 50Hz 圧空:0.4MPa 真空:90kPa 水:上水(2 ㎥メート利/h、0.2MPa)

	(8)設置場所 ①設置領域:15m×20m ②最小搬入間口:2mW×2mh ③搬入距離:30m(途中段差:200mm) ④荷役:天井クレーン (9)準拠する規格、基準等 ①日本国労働安全衛生法令(ガイドを含む) ②国際規格(ISO/IEC) ISO 12100、ISO 11161、ISO 13849-1、-2、ISO 10218-2、ISO 14122 群、IEC 60204 等 ③日本工業規格(JIS) ISO/IEC 該当 JIS、JIS Z 9104 等
4. 製 品 品 質	(1)成型制度:かみ合い部基準寸法に対して-0.5mm 以内 (*+方向の誤差は付加) :曲がり等の基準は、別途製品仕様による。 (2)製品表側の傷:0.5mm 以内とする。詳細検査及びキズ取は別工程で行う。

表 3-1 の仕様書内容を基に、初期の基本仕様を検討する。
製造物は「鍋蓋」であり、その構成部品は取っ手、ねじ、ステンレス板を素材とすることとした。
生産量(1 製品製作に使える時間)により大まかな工程順と機械機能を決定した。
図 3-1 は鍋蓋の製造工程の検討結果である。これらの工程イメージから、必要な機械機能を決定し、生産システムの構築へとつないでいく。

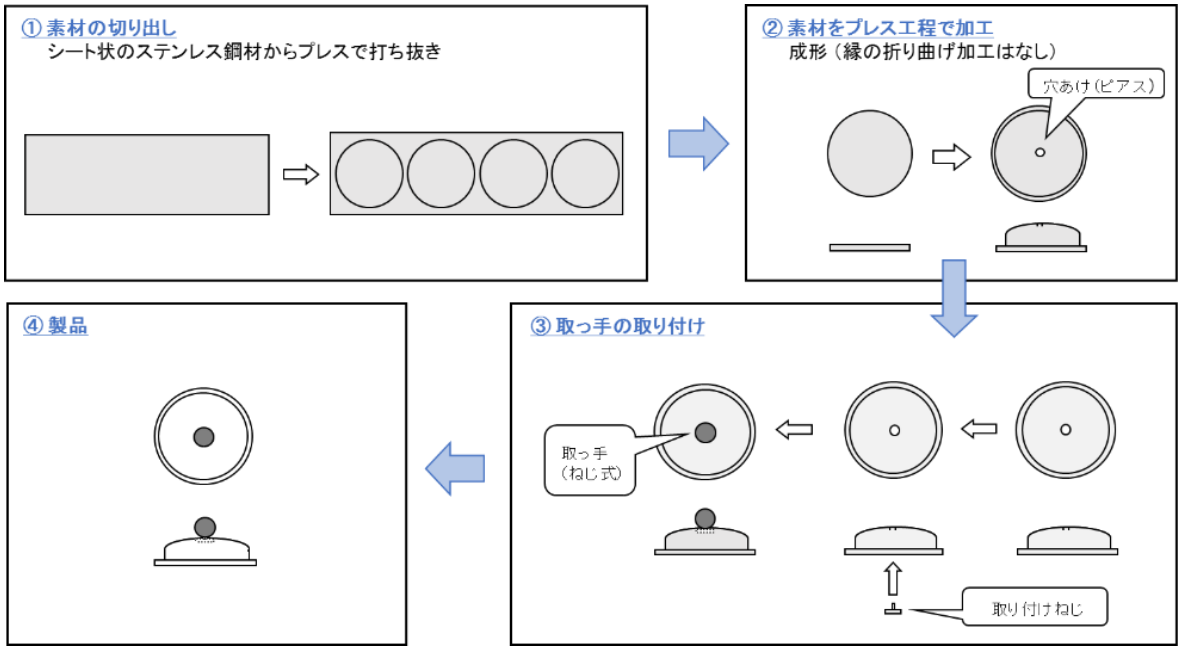
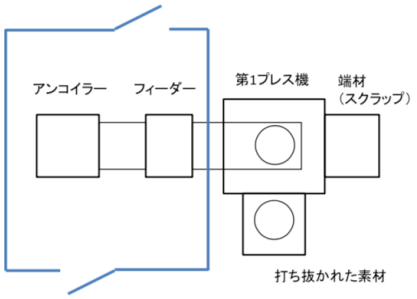
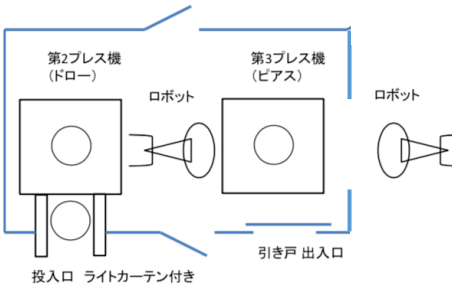


図 3-1　鍋蓋製造工程の検討結果

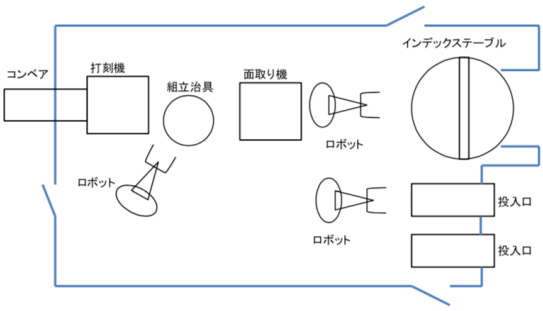
これを更に、以下の 3 つの製造ラインの構成へと広げた。大まかな工程順序案は以下のとおりである。まず、ラインとして図 3-2 に示す 3 つの構成を考えた。1: 素材加工ライン、2: 絞りピアスライン、3: 面取り取っ手取り付けラインである。



アンコイラーから第 1 プレス機(素材)



第 2 プレス機(絞り)と第 3 プレス機(ピアス)



打刻機と面取り

図 3-2　鍋蓋製造ラインの初期構成案

<u>素材加工ライン</u>

1. コイル状の素材をクレーンなどでアンコイラーにセットする
2. シート材をプレスで円形に打ち抜く
3. 作業者が次工程の絞りピアスラインへとワークを運ぶ

<u>絞りピアスライン</u>

4. 円形に打ち抜かれた素材を、手作業で絞り加工プレスに投入する
5. 絞り加工され凹型となった素材を搬送ロボットが次のピアスプレスに搬送する
6. ピアスプレスで穴あけ加工をする
7. 穴あけ加工された素材を搬送ロボットがライン外の目視確認場所に排出する。
8. 目視確認場所でロボットはワークを低速で回転させ、その間に作業者による目視確認を行う。
9. 目視確認後、問題がなければワークを箱詰めし、次工程へと運ぶ。
   ただし、加工後のワーク検査は協働ロボットを用いて、作業者の目視確認により実施する。

<u>面取り取っ手取り付けライン</u>

10. 作業者が素材の入ったパレットを供給コンベアに載せる
11. 作業者が取っ手部品と取っ手固定ねじをそれぞれの供給コンベアに載せる
12. 搬送ロボットがパレットから素材を取り出し絞り加工と穴あけ加工された素材を、ライン内の取っ手組み付け加工機に運ぶ

13. 搬送ロボットが取っ手部品と取っ手取り付けねじを取っ手組み付け加工機へと運ぶ
14. 組み付け加工機内で、鍋蓋素材と取っ手を取り付ける。
15. 鍋蓋に、レーザーマーカによるシリアルナンバーの刻印を行う
16. 刻印後の製品を排出用コンベアにて、システム外へ運ぶ

なお、本書では機能安全を導入する対象として、鍋蓋製造ラインの 2 つ目の「絞りピアスライン」(図 3-3)を取り上げ、このラインを対象に分析を加えてゆく。

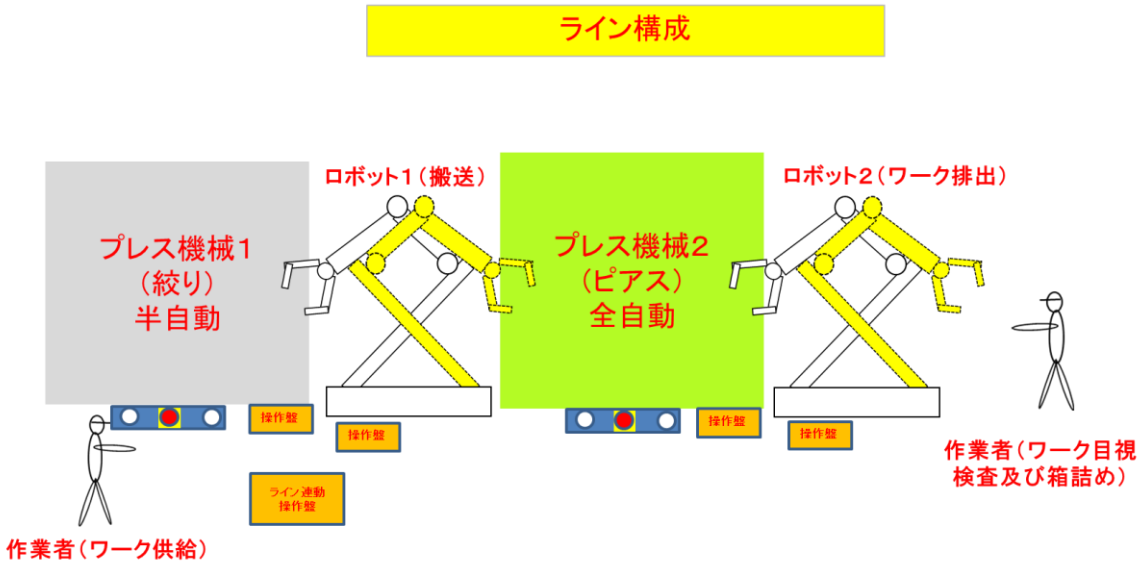


図 3-3 生産システム構成の検討結果(絞りピアスライン)

３．２ 初期工程分析

仕様の確認と初期検討により工程順序案が完成したので、これに対して更に緻密な工程分析を実施する。工程分析は、IMS としてどのような機械機能が必要となるかを決定する作業であり、これは IMS の性能と安全の両方に大きな影響を与えるため、非常に重要なステップである。初期工程分析では、通常、ユーザが提示する製造物の作成のために、どのような機能をどのような順番で適用していくか、を主に分析する。これは、統合生産システムとして、もの(主に製造物)の動線の分析であると言える。

ここでの分析により各機械機能とその並びが決定される。各機械の並びは IMS の空間設計に直結する大きな設計要素である。IMS の空間設計はその後の作業ゾーンと制御範囲の関係や人間工学側面に多大な影響を及ぼす要素であり、ここでの設計の後戻りは時に不可能となりかねない。IMS のリスクアセスメントの事前準備として非常に重要な工程と認識すべきである。製造物実現のために必要な各機械機能や加工工程の選択は、ユーザではなくインテグレータが実施することになる。ただし、インテグレータは必ずしも全ての機械機能に対して精通しているわけではないため、適切な機械機能を選定するには工程分析と機械メーカ、ユーザとの綿密な協議が不可欠である。

本書で対象とした鍋蓋のピアスプレスライン(図 3-3)では、初期工程分析において、

・プレス 2 台の機能･構造
・ロボット 2 台の機能･構造
・プレス･ロボットへの供給エネルギ
・ワーク及び人の流れ

を検討する。特に、ロボット 2 は作業者との検査作業で協働運転を実現できるものを導入する。また、使用するエネルギについては、例えばピアス加工にレーザーを使用するとした場合、リスクアセスメントとリスク低減は機械的加工の場合と大きく異なり、その物理特性に適ったシステム設計を考慮しなければならない。

工程分析段階では、インテグレータの役割はコーディネータとしての機能、つまり、ユーザと機械メーカとの間の橋渡し役が多くなる。例えば、様々な検討段階での設計レビューに対して、ユーザと機械メーカを交えた三者で議論や決定がなされるが、この設計レビューは性能側面だけではなく、リスクアセスメントの要素を盛り込む事が非常に重要であり、ここにインテグレータとしての存在意義もある。この作業をシステム設計の初期から実施し、設計の大きな後戻りやそれに伴うコストの増大を避ける活動を実施する。後々の設計変更が困難になる機械的な要素には、仕様決定時及び設計初期に十分注意を払う必要がある。安全面が置き去りにされると、設備稼働後に重篤な災害が発生し、災害対策への莫大な費用と時間が必要となる可能性が高まる。したがって、インテグレータは、機械や生産システムの設計の前により包括的な視点で機械機能、エネルギ特性、リスクとその低減を結び付けて考える能力を有し、これを仕様決定時あるいは設計の初期段階で発揮して、ユーザと機械メーカ間の合意に導いたり、助言を行ったりする存在となる。

３．３　後期工程分析

初期工程分析により、鍋蓋作成の工程と関連する機械機能を大まかに並べた仕様構想が完了し、次に機械の空間設計へとつながるようにしていく。図 3-3 の絞りピアスラインの基本構成から、より生産システムの構成へと近づけた構想図を展開する。ここでは、IMS の安全化の戦略はまだ決定できておらず、必要な機械機能を並べただけに近いものである。この段階では、この機械の並び後に変更される可能性は十分ある。

また、絞りピアスラインでプレスとロボットがどのような設定･調整作業を行う必要があるかをフロー図等により明らかにしておくことが望ましい。実施する作業とそれらの手順、介入方法が明らかになることで、IMS としての安全戦略が決まることになる。特に注意すべきことは、段取りや調整時、あるいはトラブル対応時は、通常生産時には介入しない設備にも介入が必要となるかもしれないため、漏らさずに分析に含めることである。

図 3-4 は、工程分析により決定した工程順、自動運転に必要な作業者数とその作業種類、決定した機械種類、設計初期に必要となる安全機能や IMS としての制御機能を付加したライン構想図である。例えば、この段階においてはシステムを囲む外周のガードとアクセスドア、各制御盤/操作盤のおおよその位置関係や入力機器の数あたりが読み取れる程度となっている。

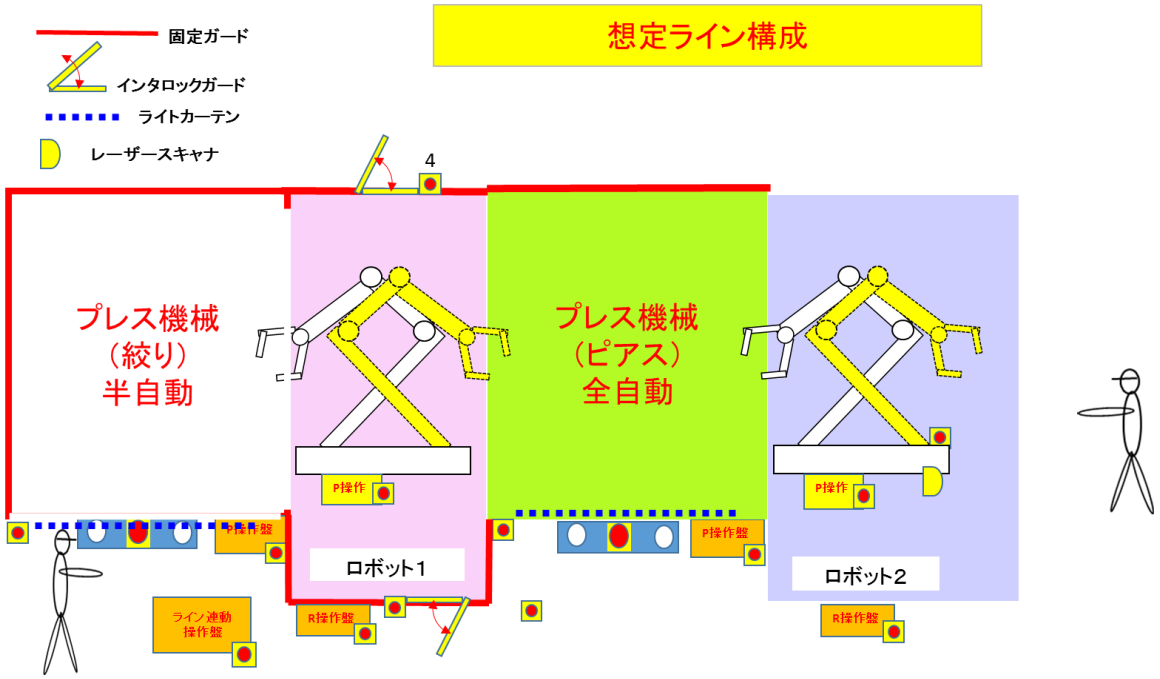


図 3-4 工程分析結果を基にした絞りピアスラインの構想図

３．４　作業分析（作業と作業ゾーン）

作業分析は、作業ベースのリスクアセスメントの一種とも言える。IMS においては、各機械の機械安全としてのリスクアセスメントは実施されており、その中でも作業と関連させたリスクアセスメントも実施される。しかしながら、複数の機械を組み合わせた場合や、工程特有のリスクアセスメントの場合は、機械メーカだけでは完遂できないこともあり得る。そのため、IMS として各機械機能や工程での人の関わりが、どのような局面でどの場所や機械で発生するのか、その場所への到達経路や避難経路などを分析する。これは、統合生産システムとしての、人の動線の分析であると言える。作業分析において最も重要なのは、システム内のどこでどのような作業を行うのかである。この「どこ」に関連づけて作業ゾーンを決定する。作業ゾーンの決定は基本的には、単体機械の塊を一つの単位として考える方がよい。

表 3-2 は、絞りピアスラインにおける作業者と機械作業との関連性を示す文書である。IMS 内部の各機械に、どの作業者がどんな作業で関わるのかを表している。プレスやロボットの調整作業に関しては、その技術レベルに応じた教育を受けた作業者が必要となり、そのような要素も加味される。インテグレータとしてはプレスの調整作業やロボットの教示のような、資格や高度な技能レベルが必要な作業に対してはそのような要件をマニュアル等に記載し、ユーザに要求する必要がある。

表 3-2　作業者と機械作業との関連性

	コイル素材供給及び中間製品搬送者 A	絞りピアスラインへの素材供給者 B	絞りピアスラインから組み立てラインへの搬送者 C
中間材料の絞り・ピアスラインへの搬送	◎		
素材製造ラインの生産トラブル処理	◎		
絞りプレスの製造調整(Change Over)		◎	
絞りプレスの生産トラブル処理		◎	
ロボット１の製造調整(Change Over)		◎	
ロボット１の生産トラブル処理		◎	
ピアスプレスの製造調整(Change Over)		○	◎
ピアスプレスの生産トラブル処理		○	◎
ロボット２の製造調整(Change Over)		○	◎
ロボット２の生産トラブル処理		○	◎
製品品質の目視確認		○	◎
パレット台車の供給取り出し		○	◎
次工程へのパレット台車の搬送			◎

◎：指定作業者が行う作業
○：指定作業者がいない場合の補助作業及び形式変更時の補助作業
製造、調整：装置の治具交換、製品に合わせた位置調整
トラブル処理：設備の材料の引っ掛かり処理、装置動作位置調整等の処理で設備故障を除く作業これ

これは、表 3-3 のようにまとめることもできる。

表 3-3 作業者と機械の関わり

機械のタスク / 人のタスク（定常作業）	プレス１（絞り）	ロボット１（絞り→ﾋﾟｱｽ）	プレス２（ﾋﾟｱｽ）	ロボット２（ﾋﾟｱｽ→パレット台車）
作業者 B（絞りピアスラインへの素材供給者）	◎製造、調整 ◎トラブル処理	◎製造、調整 ◎トラブル処理	○製造、調整 ○トラブル処理	○製造、調整 ○トラブル処理
作業者 C（絞りピアスラインから組付けラインへの搬送者）			◎製造、調整 ◎トラブル処理	◎製造、調整 ◎トラブル処理

作業者の人数と想定される仕事の洗い出しのあとは、作業ゾーンの決定と分析を行う。

図 3-5 は絞りピアスライン内部のプレス 2 台、ロボット 2 台それぞれに作業ゾーンを割り付けたものである。このゾーンは第 4 章で説明する制御範囲と深く結びつく。なお、装置の周囲の作業がなさそうなところにもゾーンを割り付けておくと、後の仕様変更等への対応がスムースとなる場合がある。作業分析を行うためには、作業ゾーンの割り付けを可能な限り設計初期に行っておく必要がある。

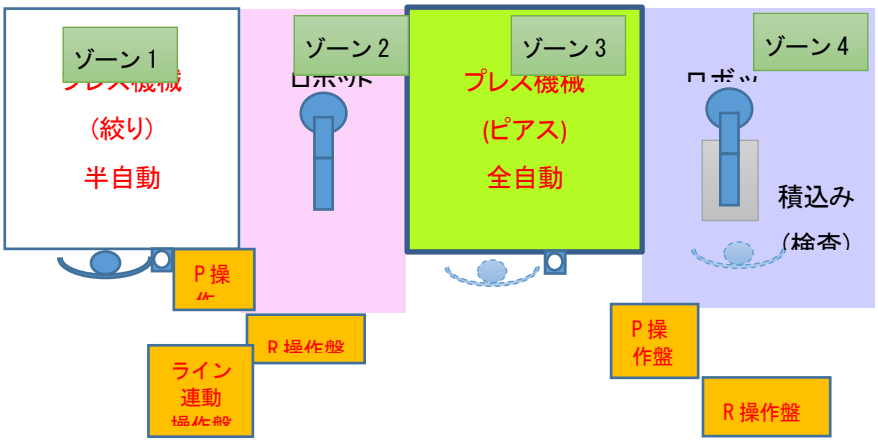


図 3-5　作業ゾーンの割り付け

機械機能と IMS のレイアウト、更に大まかな作業の洗い出しができると、本格的なリスクアセスメントの開始となる。まずは各機械及びその周辺あるいは IMS として新たに発生する危険源を見つけていく。通常この段階では実機あるいはシステムは存在しないため、機械図面を見ながら実施する作業となる。

第４章　リスクアセスメントとリスク低減

４．１　リスクアセスメント

本書では、単独機械でのリスクアセスメントの知識はある前提で、IMS として特に考慮が必要な事項について解説する。

また、リスクアセスメントにおいては、ある程度の構想設計ができており、本署では、構想設計において図 4-1 の様な機械配置とし制御範囲を 4 つにゾーン別けした場合を例とする。なお、IMS のリスクアセスメントにおいては、後述する隣接機械が危険源となることがあり、単体機械に設置されている安全装置がその危険源のリスク低減に有効ではない場合があり、基本的には単体機械に設置されている安全装置は無いものとしてリスクアセスメントを実施する。

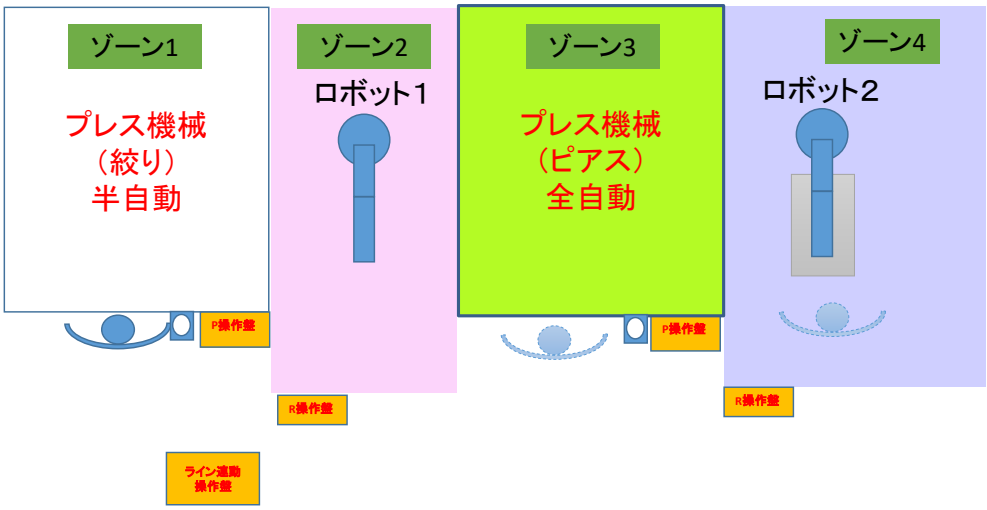


図 4-1 構想設計時のレイアウト

(1)　機械の使用制限

IMS のリスクアセスメントにおいても、前提となる機械の仕様を明確にする。

ア　個々の機械仕様

IMS におけるリスクアセスメントにおいても、まずは個々の機械の仕様を明確にしておく必要がある。

イ　IMS の仕様

IMS においては、個々の機械の配置とレイアウトやワークの流れ、制御区分、制

御区分が異なる機械のオーバーラップ範囲やタイミングを明確にする。

また、作業でアクセスが必要となる場合、アクセスする位置と他の制御ゾーンにある機械との関係も明確にしておく必要がある。

ウ　使用条件

IMS が設置・使用される場所や周辺の物理的環境、係る人の制限の確認を行う。

(2)　危険源・危険状態・危険事象の同定

IMS においては、構想設計において設定したゾーン毎に危険源・危険状態・危険事象を同定していく。

ア　危険源の同定

IMS においてはゾーン内に存在する機械の他、隣接ゾーンからアクセスする機械や放射も危険源として同定する必要がある。今回の例においては、ゾーン 2 のロボットはゾーン 1 やゾーン 3 にもアクセスすることがあり、ゾーン 2 のロボットはゾーン 1 及び 3 の危険源としても同定が必要である。(図 4-2　黒矢印)

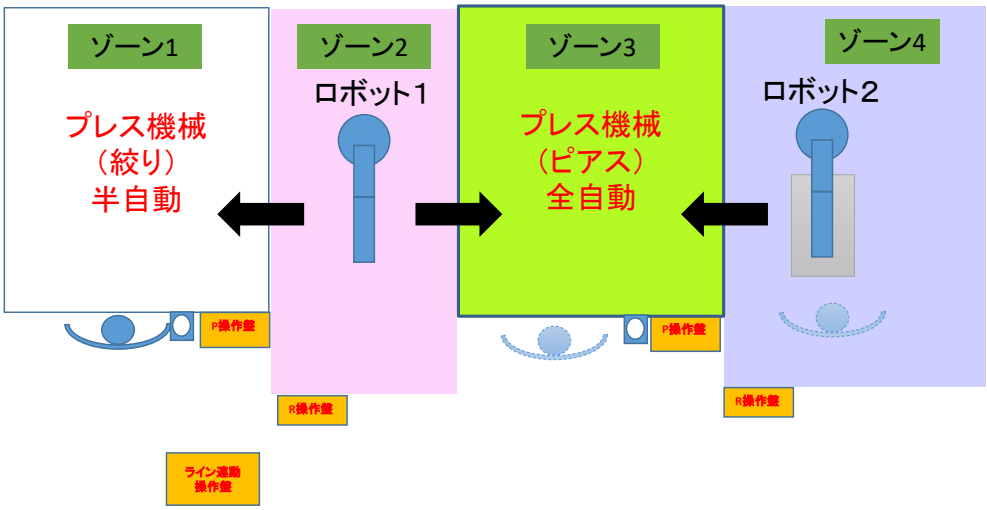


図 4-2 複数ゾーンに関わる危険源

イ 人の存在(作業)の同定

(ア) 必要とされる作業

IMS に係る作業内容と頻度を同定する。IMS の場合、隣接機械の配置等によりアクセス経路が制限される場合もあり、アクセス経路を含めて作業を同定する必要がある

また IMS においては一部の機械が故障した場合、当該機械の運転を停止して作業

者が代わりに作業を行う「バックアップ生産」を行うことを考慮する場合があり、「バックアップ生産」時にどのような作業となるかも同定する必要がある。

ゾーン 3 でのバックアップ作業は、ロボット 1 が故障の場合とロボット 2 が故障の場合でリスクが異なる為、別の作業として同定する必要がある。

なお、本来は機械の搬入・据付や撤去を含めた局面での人の存在(作業)も同定する必要があるが､本書では生産を中心とした作業に限定した例として表 4-1 に示す。

表 4-1 IMS に係る作業例

ゾーン	フェーズ	作業	頻度
1	生産	ワーク投入	1/30s
	段取り	型清掃	4/日
	段取り	型段交換・調整	1/日
	保全	給油、法定定期検査 他	1/半年
	バックアップ	ワーク取出し(ロボット 1 故障時)	1/3 年
	異常処置	清掃(ゴミ処置等)、ワーク姿勢修正(プレス前・後)	1/月
2	段取り	ロボットティーチ	1/半年
	保全	給油、バキュームカップ交換	1/半年
	異常処置		1/月
3	生産	型清掃	1/日
	段取り	型段交換・調整	4/日
	保全	給油、法定定期検査 他	1/半年
	バックアップ	ワーク投入(ロボット 1 故障時)	1/3 年
	バックアップ	ワーク取出し(ロボット 2 故障時)	1/3 年
	バックアップ	ワーク投入&取出し(ロボット 1 及び 2 故障時)	1/5 年
4	生産	品質チェック(ロット毎)	1/時間
	生産	パレット台車交換	1/時間
	段取り	バキュームカップ清掃	1/日
	段取り	バキュームカップ交換	1/半年
	段取り	ロボットティーチ	1/半年
	保全	給油、バキュームカップ交換	1/半年
	異常処置		1/月

(イ) 想定される誤使用

単体機械ではあまり問題にならない誤使用でも､IMS では大きなリスクとなる場合がある。例えば、プレス機械(絞り)において、プレス加工されたワークがズレた場合、単体機械ではズレたワークを手で取り出すだけなので問題にはならないが、IMS ではロボットがワークを搬送するため、ズレたワークを修正しようとした時に進入してきたロボットと接触するといったリスクも想定する必要がある(表 4−2 参照)。

表 4-2 想定される誤使用の例

考慮すべきヒューマンエラー	合理的に予見可能な誤使用の例
機械の使用中に、機能不良、事故又は故障が生じた時の人の反射的な行動	・(絞り)プレス後ずれた製品の位置修正 ・(絞り)吸着不良で落下しそうになった製品を掴もうとする
集中力の欠如又は不注意から生じる(故意ではない)誤った行動	・落としたものの収集やロボット可動範囲への進入
“近道反応”、”省略行動”等の行動	・ロボット可動範囲を通行して反対側へ渡る ・ゾーン間を移動してアクセス
機械の運転を継続させようという動機から生じる不適切な行動	・ロボットが保持しようとする製品の姿勢修正

また、IMS における最も典型的な誤使用は図 4−3 に示す「ゾーン間移動」である。部分的に停止させる事ができるように設計された IMS の場合、作業者がリスク低減されているゾーンから他のリスクが低減されていないゾーンへ侵入できてしまうかどうかの分析は非常に重要である。ゾーン間移動の可能性は、物理的な観点からのみ判断し、ルールなどのソフト面での方策は考慮してはならない。全身のアクセスが可能な場合、複数のゾーンに同時存在する可能性も想定しなければならない。ただし、単体機械のカバーが固定ガードとしての要件を満たす場合(図 4−3 におけるゾーン 1 とゾーン 3 の黒実線)は、アクセスできないとみなしてよい。

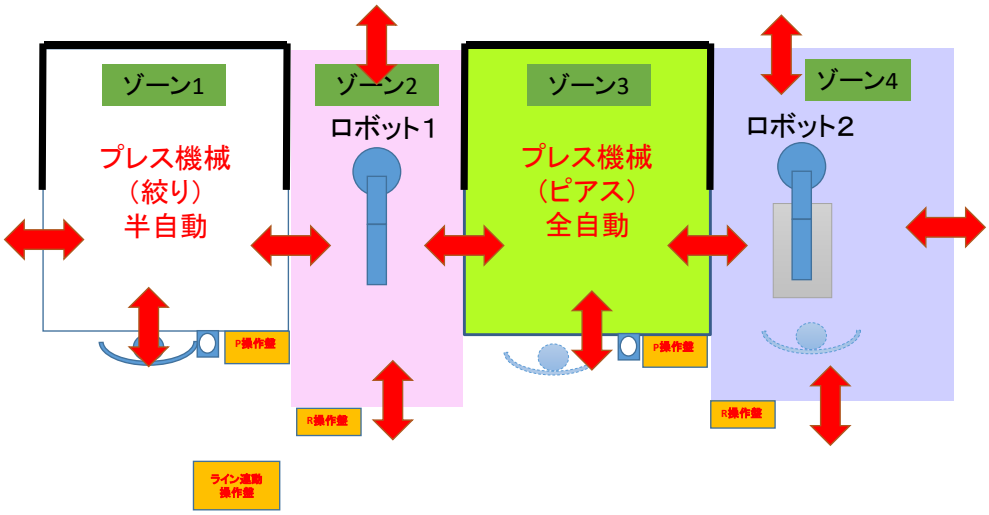


図 4-3 考慮すべきアクセス

（ウ） 危険状態の同定

危険源と人の存在(作業)から危険状態を同定する。人の存在(作業)を中心に危害を及ぼすであろう危険源を関連付ける。表 4-3 に危険状態の例を示す。

表 4-3 危険状態の例

ゾーン	フェーズ	作業	危険源
1	生産	ワーク投入	プレス機械
			ロボット 1
			ワーク
	段取り	型交換・調整	プレス機械
			ロボット 1
			ワーク
		型清掃(定期)	プレス機械
			ロボット 1
			ワーク
	バックアップ	ワーク取出し(ロボット 1 故障時)	プレス機械
			ロボット 1
			ワーク
	異常処置	型の清掃(異物処置)	プレス機械
			ロボット 1
			ワーク
		ワーク姿勢修正	プレス機械
			ロボット 1
			ワーク
		ワーク落下保持	プレス機械
			ロボット 1
			ワーク
	その他	ゾーン 1 への不意の進入	プレス機械
			ロボット 1
	…	…	…
4	段取り	品質チェック	ロボット 2
			ワーク
		台車交換	ロボット 2
			台車
	その他	ゾーン 4 への不意の進入	ロボット 2

（エ） 危険事象の同定

危険状態において、ケガに至る危険事象を同定する。表 4-4 に危険事象の同定例の一部を示す。

表 4-4 危険事象の例

ゾーン	フェーズ	作業	危険源	危険事象
1	生産	ワーク投入	プレス機械	誤ったタイミングでプレス内に手を入れプレスに手を挟まれる
			ロボット 1	人が誤ってゾーン 2 に進入し接触
				進入してきた自動運転中のロボット 1 と接触
				進入してきたティーチ中のロボット 1 と接触
			ワーク	エッジで切創
	段取り	型交換・調整	プレス機械	プレスが起動して手を挟まれる
			ロボット 1	人が誤ってゾーン 2 に進入し接触
				進入してきた自動運転中のロボット 1 と接触
				進入してきたティーチ中のロボット 1 と接触
			ワーク	エッジで切創
		型清掃(定期)	プレス機械	プレスが起動して手を挟まれる
			ロボット 1	人が誤ってゾーン 2 に進入し接触
				進入してきた自動運転中のロボット 1 と接触
				進入してきたティーチ中のロボット 1 と接触
			ワーク	エッジで切創
	バック アップ	ワーク取出し (ロボット 1 故障時)	プレス機械	プレス機械が起動して手を挟まれる
			ロボット 1	人が誤ってゾーン 2 に進入し接触
				進入してきた自動運転中のロボット 1 と接触
				進入してきたティーチ中のロボット 1 と接触
			ワーク	エッジで切創
…	…	…	…	…
4	段取り	品質確認	ロボット 2	運転中のロボット 2 と接触
			ワーク	落下したワークと接触
		台車交換	ロボット 2	運転中のロボット 2 と接触
			台車	台車が重く腰痛
		バキューム カップ清掃	ロボット 2	清掃中、ロボット 2 が動き接触
		バキューム カップ交換	ロボット 2	交換中、ロボット 2 が動き接触
	その他	不意の進入	ロボット 2	動作中のロボット 2 と接触
		その他	ワーク	ロボット 2 で搬送途中、ワークがバキュームカップから外れ飛来し接触
	…	…	…	…

(3) リスクの見積もり・評価

表 4-5、4-6 に基づいたリスク要素の見積もりとリスク評価の一部の例を表 4-8 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、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、表 4-5 では省略する。

表 4-5 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:O</td><td>頻繁:O3</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:O2</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)、又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:O1</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 4-6 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:03	時々:02	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 4-7 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

*ALARP(as low as rteasonably practicable)とは合理的に実現可能な最低の水準の意味。

表 4-8 危険事象の例

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	(ゾーン 1) ワーク投入時	プレスが起動して手を挟まれる	S3 プレス	F3 1/30s	A2 回避不可	4
2		人が誤ってゾーン 2 に進入し接触	S3 ロボット	F1 誤進入は低頻度	A2 回避不可	4
3		進入してきた自動運転ロボット 1 と接触	S3 ロボット	F3 1/30s	A2 回避不可	4
4		進入してきたティーチ中のロボット 1 と接触	S3 ロボット	F1 ティーチは 1/半年	A2 回避不可	4
5		ワークのエッジで切創する	S2 プレス品	F3 1/30s のワーク投入	A2 回避不可	4
	(ゾーン 4) 品質確認時	運転中のロボット 2 と接触	S3 ロボット	F2 4/日の確認	A2 回避不可	4
		落下したワークと接触	S1 プレス品	F2 4/日の確認	A2 回避不可	4
	台車交換	運転中のロボット 2 と接触	S3 ロボット	F2 4/日の確認	A2 回避不可	4
		台車が重く腰痛	S2 プレス品	F2 4/日の確認	A2 回避不可	4
	バキュームカップ清掃中、ロボット 2 が動き接触		S3 ロボット	F2 1/日の清掃	A2 回避不可	4
	バキュームカップ交換、ロボット 2 が動き接触		S3 ロボット	F1 1/半年	A2 回避不可	4

４．２　リスク低減

(1)　IMS のリスク低減方策

IMS においても、ALARP 原則に基づき、リスク低減方策を検討する。本質安全設計によるリスク低減が行えない場合、IMS は基本的にゾーン毎の隔離と停止の保護方策を実施する。

個々の機械が、規格適合しており、必要なガードや安全機能が取り付けられている場合は、それらを改造しない限り、システム側で新たにガードを追加する必要はあまりない。ただし、システム側でガードすることが前提のロボットのように、組み込みによる安全防護を意図する機械類は、インテグレータがそのシステムの安全設計の主体者となる。今回の例では、プレスの固定ガードの取り外しとロボットの防護がこれに当たる。それ以外にも、可動部を持つワーク固定ステーションの追加や、コンベアや可動軸の追加、機械へのワーク供給取出しを許すために、自動ドアへと改造するなどが、よく行われることである。

これらに対して、例えば、

- ドアインタロックや進入検知として使用する保護装置の位置決め

- ガードの開口部の大きさに応じた危険源までの安全距離を満たす距離ガードの設置
- 人間工学原則を満たす設計
- 適切な接近手段の設計
- 押しつぶし等を防止するための最小すき間

などが、制御要素以外の安全機能や設計の重要なポイントとなり、制御要素に優先して実施しなければならない。

また、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なければならない。

図 4-4 にゾーン 1～3 のリスク低減方策例を示す。

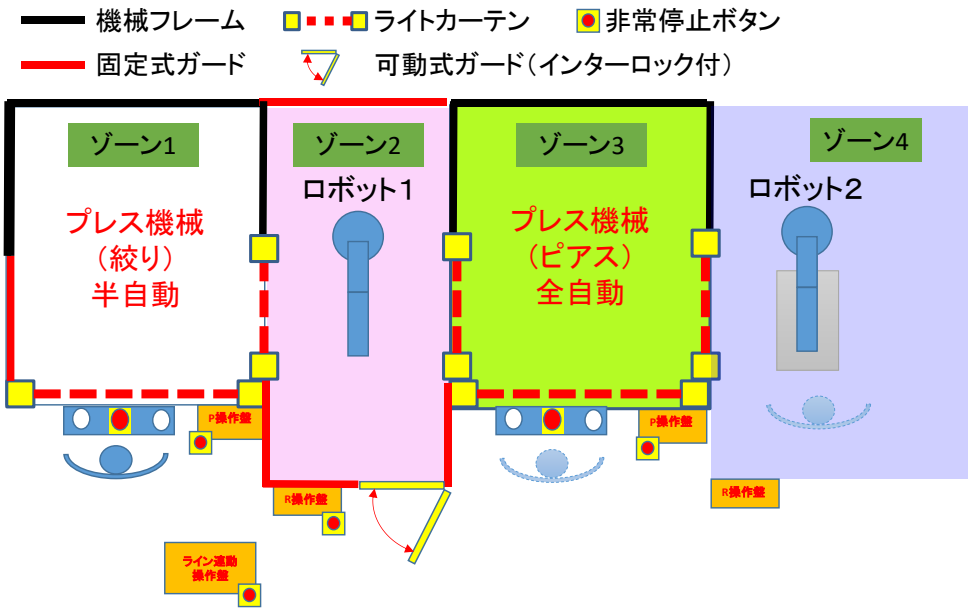


図 4-4 リスク低減方策例

(2) ゾーン間移動に対するリスク低減方策の注意点

ア 必要な機能

ゾーン間移動によるリスク低減方策として、ゾーン間にライトカーテン等の検知保護設備を用いる場合、ゾーン間移動は双方向からありうることを考慮しなければならず、例えばゾーン 1 とゾーン 2 間に設置したライトカーテンは、ゾーン 1 のプレス機械とゾーン 2 のロボット 1 を停止させる機能を有する必要がある（図 4-5 参照）。

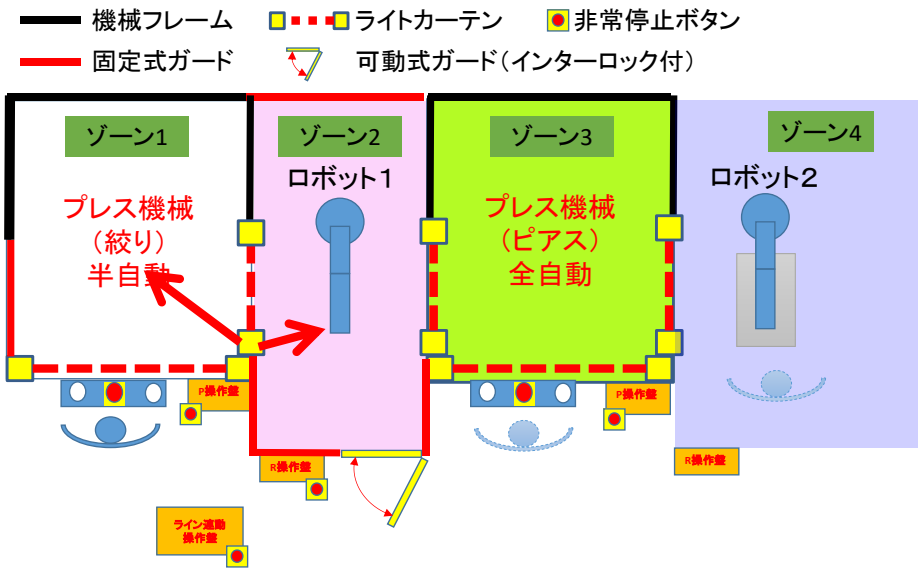


図 4-5 ライトカーテンの停止指令

イ　安全距離の考慮

ゾーン間に設置するライトカーテンにおいては、以下の 2 つの安全距離を考慮しなければならない。

① ロボットの停止距離

② 人のアクセス距離

ロボットの停止距離は、ロボットがライトカーテンを遮光してからロボットが停止するまでの距離（停止時間×速度）を考慮しなければならない。また、人がライトカーテンを遮光してからロボットに到達する前にロボットは停止しなければならない。

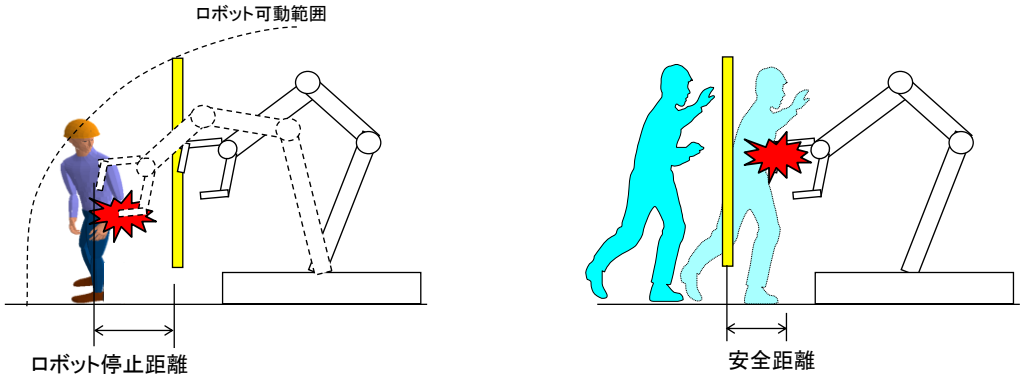


図 4-6 停止距離・安全距離

しかしながら検知保護装置では人の動作制限をすることができず、ゾーン間移動をするロボットは、ロボットの動作範囲をライトカーテンの内側に限定することはできない。このため、ゾーン間移動をする機械がある場合、2 組のライトカーテンを

用いて安全距離を確保する必要がある。2 組のライトカーテンの距離は、ロボットの停止距離か人のアクセス距離(安全距離)のいずれかの大きい方としなければならない。

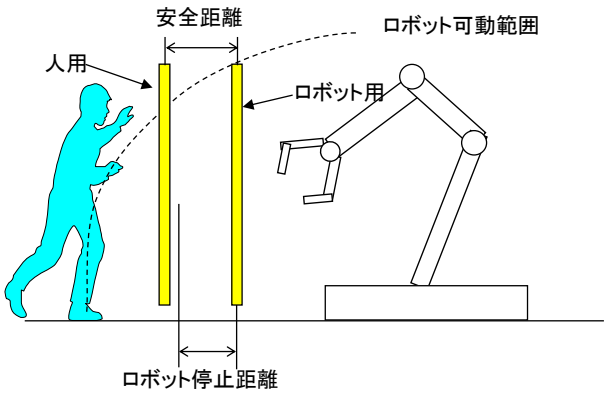


図 4-7 停止距離・安全距離を考慮したライトカーテンの配置

上記を踏まえたゾーン 1～3 の保護方策の配置例を図 4-8 に示す。

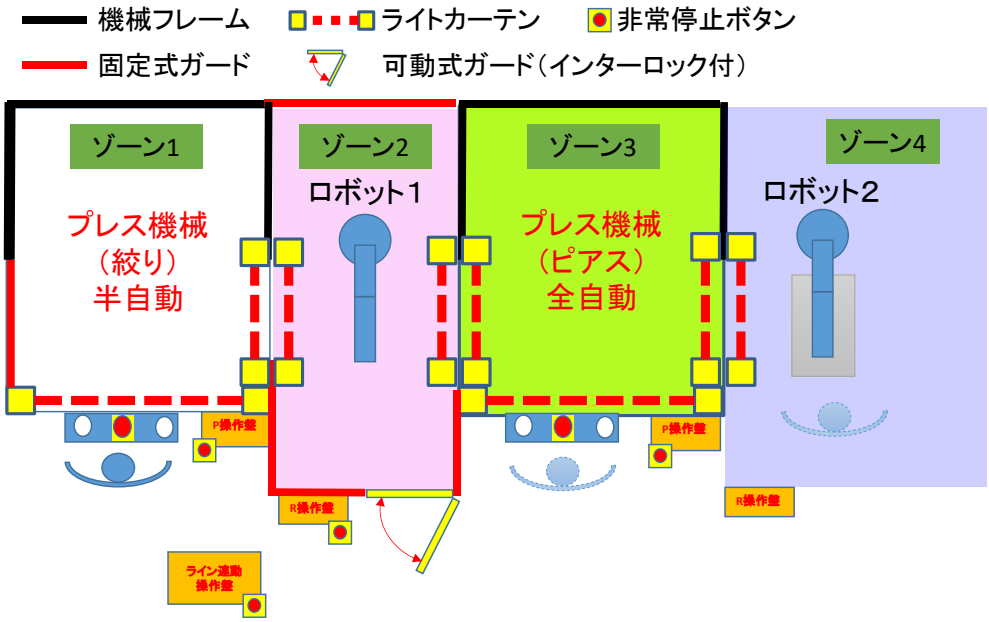


図 4-8 安全距離を考慮した保護方策例

ウ　保全時のバックアップ生産の考慮

上記アに従い双方向のアクセスを考慮すると、例えばロボット用のライトカーテンはゾーン 2 からゾーン 1 へ進入時にゾーン 1 の機械(プレス 1)を停止させるための信号も出力することとなる。(図 4-9 に示すように、安全距離が確保できれば、プレ

ス 1 に近いライトカーテンの出力でプレス 1 を停止させてもよい。）

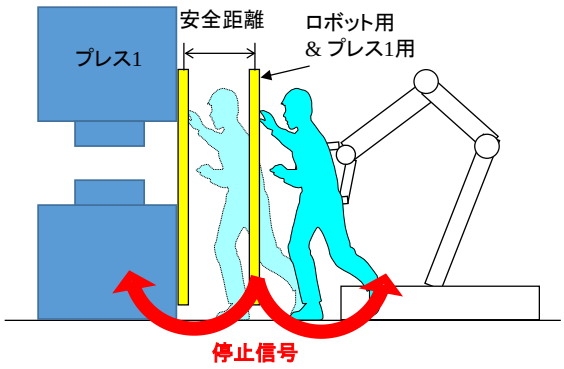


図 4-9 停止信号の共用

IMS は一部の機械が故障した場合にバックアップができるようにゾーンを分けて制御するが、例えばゾーン 2 のロボット 1 が故障時にゾーン 2 の電源を落として保全作業を行う場合、ライトカーテンがゾーン 2 の制御範囲となっていると、ゾーン 2 の電源が落ちることによりライトカーテンからは遮光信号が常に出力されることとなり、プレス 1 を動かすことができなくなる。

また、逆にライトカーテンをゾーン 1 の制御とした場合、ゾーン 1 の電源を落とした時にロボット 1 を動かせなくなる。ただし、この場合にプレス 1 が故障しても生産を続けることが可能かを考えると、プレス 1 での加工が終わっていないワークを搬送する必要はなく、ロボット 1 を動かす必要はないと考えられるため、ライトカーテンがゾーン 1 の制御であっても問題はない。

今回の例では、たとえゾーン 2 にあるロボット 1 を停止させるライトカーテンであっても、ゾーン 1 側の制御とする方が都合がよいが、ゾーン間に設置する検知保護装置の制御は、工程の構成や作業を十分に考慮して次のいずれかを採用する。

① ライトカーテンは共用せずそれぞれのゾーン毎に独自で設置する（この場合、ゾーンの境界には 4 本のライトカーテンを設置することになる）
② バックアップ・電源遮断を含めて工程分析を行い適切なゾーンでの制御とする
③ 両ゾーンから制御（電源供給）できるようにしておく

(3) 機能安全を用いた方策例

ゾーン 4 の RA においては、表 4-9 のリスクが同定されるが、特にロボット 2 との接触による災害の防止について、機能安全を用いた保護方策を実施する場合の例を検討する。

表 4-9 ゾーン 4 のリスク抜粋

4	段取り	品質確認	ロボット 2	運転中のロボット 2 と接触
			ワーク	落下したワークと接触
		台車交換	ロボット 2	運転中のロボット 2 と接触
			台車	台車が重く腰痛
		バキュームカップ清掃	ロボット 2	清掃中、ロボット 2 が動き接触
		バキュームカップ交換	ロボット 2	交換中、ロボット 2 が動き接触
	その他	不意の進入	ロボット 2	動作中のロボット 2 と接触
		その他	ワーク	ロボット 2 で搬送途中、ワークがバキュームカップから外れ飛来し接触

ロボット 2 との接触防止は、図 4-10 の左図のようにレーザースキャナを配置し、右図のような保護停止エリアを設定することで、段取り、又は不意の進入によるロボット 2 との接触防止を図ることとする。(なお、保護停止エリアは、台車の車輪部分を無効化する必要があり、無効化時に死角ができないかの検証が必要となるが、本書では割愛する。)

ただし、レーザースキャナの検出によりロボット 2 全体の動力遮断をしてしまうと品質確認のためにワークを回転させられなくなってしまうため、レーザースキャナの検出でロボット 2 本体は保護停止とし、エンドエフェクタには低推力モータ(保護方策が不要な推力)を使い、ゾーン 4 内のロボット 2 近傍で操作(正転・逆転)できるように操作ボタンを配置する。

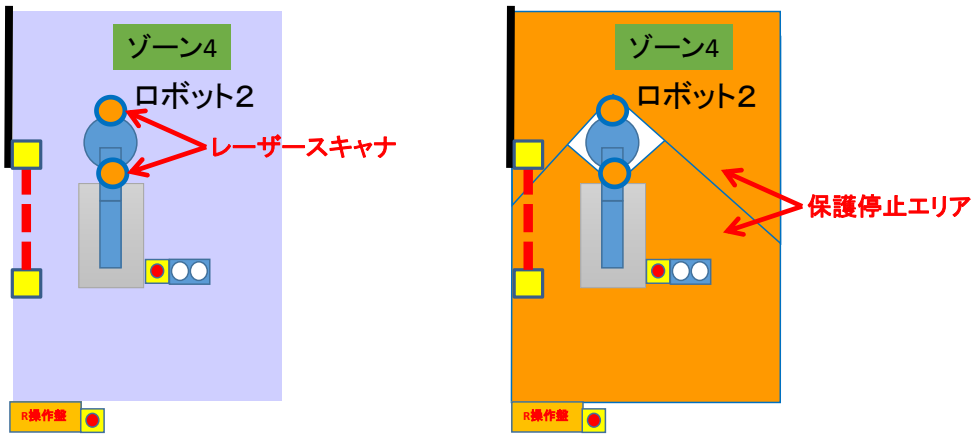


図 4-10 レーザースキャナによる保護方策例

(4) リスク低減方策実施後のリスク見積り・評価

検討したリスク低減方策にてリスク低減できたかの見積もり・評価と方策の妥当性評価を行う。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。

(5)　リスク低減方策の評価

全てのリスク低減方策を検討した後、以下について確認を行う。

- リスクは合理的に実現可能な程度まで低減できているか？
- すべての運転条件及びすべての作業で成立するか？
- 新たに生じた危険源は同定・評価され、必要な場合は方策が講じられているか？（次項参照）
- 残留リスクについては使用者に十分に通知し、かつ警告しているか？
- 作業性を阻害したり、機械の使い勝手を悪くしたりしていないか？
- 他の保護方策の支障にならないか？
- 機械の能力を過度に低減しないか？

(6)　新たに生じるリスクとその低減方策

ア　新たに生じるリスク

IMS において、リスク低減方策実施後に新たに発生する典型的なリスクは、ゾーン間移動により他のゾーンへ進入している時に、他の作業者が機械を再起動してしまうリスクである。

例えば、ゾーン２の可動式ガードから進入しゾーン１又は３へ進入する場合、ゾーン１又は３はライトカーテンにより停止する。この時、ゾーン間移動により全身の進入が可能な場合、ゾーン内に完全に入るとライトカーテンは通光状態となり障害物がないものとされ再起動が可能となる。

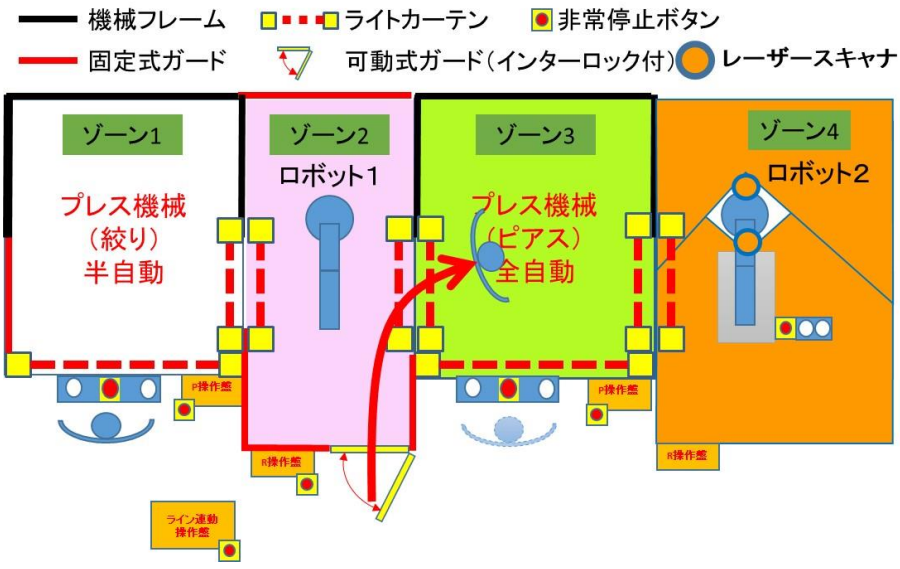


図 4-11　ゾーン間移動によるアクセス

当該リスクの可能性については、以下の観点から判断する

- ゾーン間移動による全身の進入の可否
- 操作盤位置からの視認性

イ　新たに生じるリスクの低減方策

上記リスクの可能性がある場合、以下のいずれか、又は組み合わせによりリスクを低減することができる。

- 操作盤の位置や固定ガードの種類の工夫、必要な場合は鏡やカメラの設置等による操作盤位置からゾーン内部の視認性向上
- ゾーン間に配置したライトカーテンの停止信号保持と表示
- 起動前警報と、退避や脱出手段又は起動阻止手段の設置
- ゾーン間に配置したライトカーテンの停止信号を保持、及び保持の解除(リセット)には進入経路上の安全装置(ゾーン 2 から進入の場合は、可動式ガード)が復帰していることの条件追加
- レーザースキャナによるゾーン内監視

なお、起動前警報については、起動前警報の発報により退避や脱出できる時間や場所・ルートの確保、あるいは起動を阻止できる手段を備える必要がある。

(7)　安全機能の明確化

リスクアセスメントに基づくリスク低減方策のうち、機能安全を用いてリスク低減を行う方策については、1 つの IMS に複数の異なる安全機能がその機能が備わるため、それらについて明確にする必要がある。

明確にする内容は、各々の安全機能が有効となる範囲や、ミューティングが必要な場合はその条件となる。

特にライトカーテン等の機能を IMS として適切に使用するためには、ミューティング機能の適用が不可欠である(ミューティング機能が不要であれば、固定式ガードや可動式ガードが適切)。ミューティング機能とは、安全状態(リスク低減状態)において安全機能を一時的に無効化する機能である。例えば、ライトカーテン LG2-1、LG1-2 は、プレス内に作業者の身体がない(ライトカーテン LG1-1 が通光状態)状態の場合にのみ無効化し、ロボット 1 のプレス内への進入を可能とする。このように各ライトカーテンについてミューティング機能が必要となる場合、ミューティング機能を有効にする条件について明確にしてシステムを構築する必要がある。

以上、ミューティング機能と適用するための条件について以下に示す。

- ミューティング中は、作業者が危険な状況にさらされないこと。
- ミューティング中は、他の方法で安全な状態を確保されること。
- ミューティングが終了すると、自動的にすべての安全機能が回復すること。
- ミューティング機能を含めることが関連する安全機能に要求される安全性を低下させないこと。

－　用途によっては、ミューティング状態の表示信号を検討すること。

保護装置を含む最終的なレイアウト図を図4-12に、安全機能の一覧を表4-10に示す。

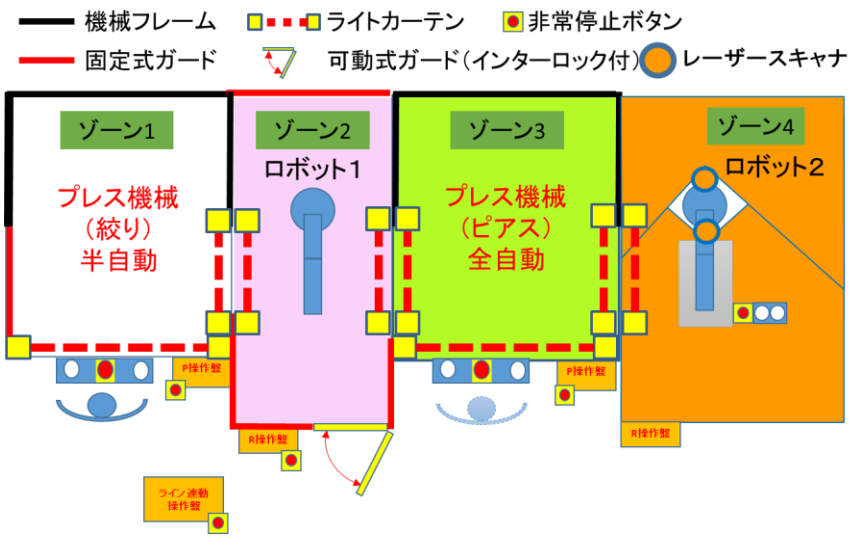


図 4-12 機能安全を用いるリスク低減方策

表 4-10 機能安全のまとめ

安全機能	ゾーン				備考(安全機能の無効化条件)
	1	2	3	4	
非常停止 EMG11	○	○	○	○	
非常停止 EMG1-1	○				
非常停止 EMG1-2	○				
非常停止 EMG2		○			
非常停止 EMG3-1			○		
非常停止 EMG3-2			○		
非常停止 EMG4-1				○	
非常停止 EMG4-2				○	
光線式安全装置 LG1-1	△*1				*1 下死点⇒上死点：プレス機械の上昇行程
光線式安全装置 LG1-2	△*1	△*2			*1 EMG2 を操作、又は DIL1 が開きの時 *2 EMG1-1 又は 1-2 が操作されている、 又は LG-1-1 が遮光時
光線式安全装置 LG2-1	△*1	△*2			
ドアインタロック DIL1		○			
光線式安全装置 LG2-2		△*1	△*2		*1 EMG3-1 又は 3-2 が操作、又は LG3-1 が遮光時 *2 EMG2 操作されている、又は DIL1 が開きの時
光線式安全装置 LG3-2		△*1	△*2		
光線式安全装置 LG3-1		△*1			*1 バックアップモード時の下死点～上死点を除く
光線式安全装置 LG3-3			△*1	△*2	*1 EMG4-1 又は 4-2 が操作、1SC1 又は 2 が検知時 *2 EMG3-1 又は 3-2 が操作、又は LG3-1 が遮光時
光線式安全装置 LG4			△*1	△*2	
レーザースキャナ LSC1				△*1	*1 品質チェックモード時はロボット本体は SS1 エンドエフェクタは動力 ON(低推力制御のため)
レーザースキャナ LSC2				△*1	

○：常時安全機能有効

△：安全機能の条件付無効化有(*1・ *2 ：各安全機能の無効化条件)

(8) 作業ゾーン及び制御範囲以外の要素

完成品の機械装置を組み合わせて構築する IMS としては、個々の機械の規格適合、及びリスク低減の実施は、機械メーカで成されることが多い。

しかし､ロボットのように､インテグレータが IMS 構築の実施主体者となるものや、購入した機械装置に改造を加えたり、はしごや作業プラットフォームなどを IMS に付加したりすることで、機械メーカで実施したリスクアセスメントの前提が成立しないことがありえる。このため、購入した機械に対して、IMS としてのリスクアセスメントも実施する必要がある。特にロボットの場合は、レイアウト設計とそれにかかる制限空間や、正しい制限装置の適用などがリスクアセスメントに大きな影響を与える。

例えば、今回モデルとした IMS では、プレスの固定ガードを一部取り外している。これにより生じる危険源とガードに設けた開口部との距離や、ライトカーテンなどの保護装置の設置位置、ミューティング方法などは新たに検討しなければならない。それ以外にも、協働ロボットを使用するためのアプリケーションを考慮したリスクアセスメントと設計が必要になる。このようなアプリケーションへの考慮は、リスクアセスメントと設計の大きな焦点になる。

第５章　要求安全度水準の決定

５．１　安全関連システムと要求安全度水準の決定方法

(1)　機械安全のリスク低減方策における安全関連システム(SRP/CS)の手順

図 5-1 は、IMS も含めた一般的な機械安全のリスク低減方策の手順における安全関連システムの(SRP/CS)の機械安全設計への適用の考え方を示している。

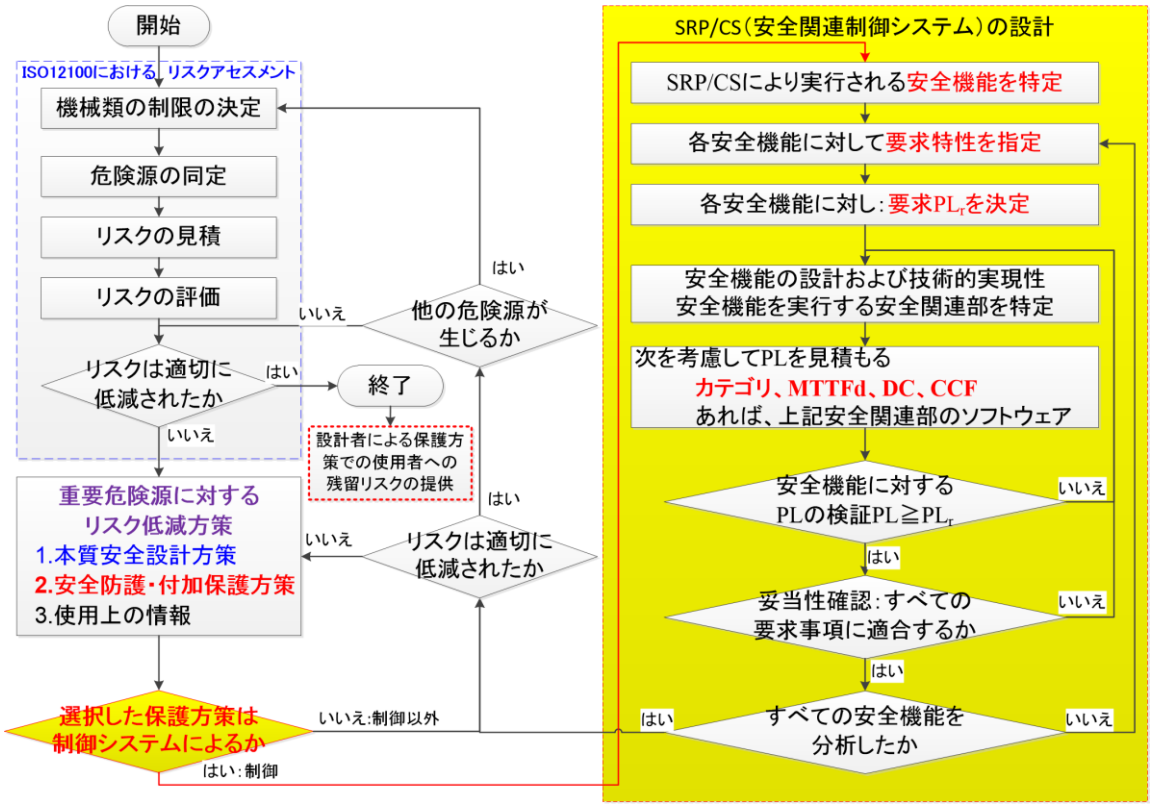


図 5-1 IMS の安全関連システムの設計と設計検証手順

機械安全におけるリスク低減方策は、ISO 12100 に従った機械全体のリスクアセスメント結果に基づいて保護方策を実施する。保護方策において、本質的安全設計方策、安全防護方策、付加保護方策によるリスク低減は、機械的な方策を最優先に合理的に実施できる範囲で検討し実施することが重要である。例えば、機械的な安全防護方策を検討する際は、機械設備の仕様と作業を考慮して人の機械設備内(危険源域)への介入が必要

な場合は、その頻度に合わせて保護装置としてガードのインタロック、検知保護装置等の制御システムによる安全防護の採用を検討し実施する。そして制御システムによる安全防護は、図 5-1 に示した機能安全(SRP/CS:安全関連制御システム)として ISO 13849-1 に示される手順に従った設計を各安全機能に対して実施する。

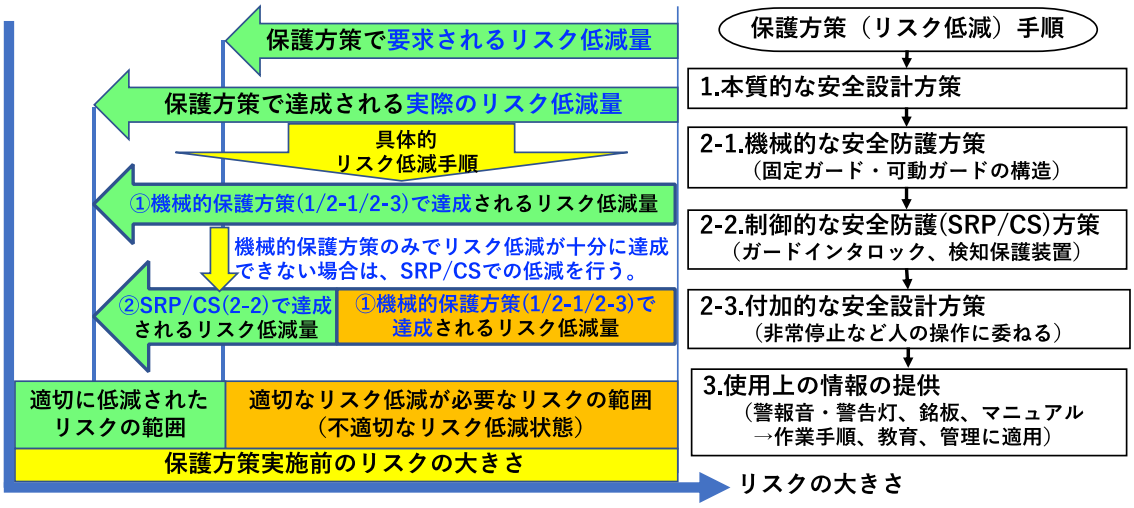


図 5-2 安全関連システムの設計適用

図 5-2 は、機械安全設計における安全関連システムとしての設計の適用手順を示している。

(2) パフォーマンスレベル(ISO 13849-1)と SIL(IEC 62061/IEC 61508)

SRP/CS の設計手順は、ISO 12100 に従ったリスクアセスメント時のリスク分析、リスク評価の結果を考慮(SRP/CS 検討の入力情報)して、リスクレベルに合わせた機能安全適用として SRP/CS に求められる要求安全度水準を決定する。この安全度水準が、機能安全におけるパフォーマンスレベル(ISO 13849-1)であり、また SIL(IEC 62061/IEC 61508)として示されている。

パフォーマンスレベル(PL)は、リスクレベルに合わせて SRP/CS のレベルとして単位時間の危険側故障発生の平均確率(PFH_D)の範囲で安全度水準 a、b、c、d、e の 5 つに分類される。また電気/電子/プログラマブル電子システム(E/E/EP)が、機械安全のリスク低減方策に使用される場合は、リスクレベルに合わせた単位時間の危険側故障発生の平均確率(PFH_D)の範囲で安全インテグリティレベル(SIL)が、安全度水準 1、2、3 の 3 つに分類される。表 5-1 に PL、SIL、PFH_D の関係について示す。

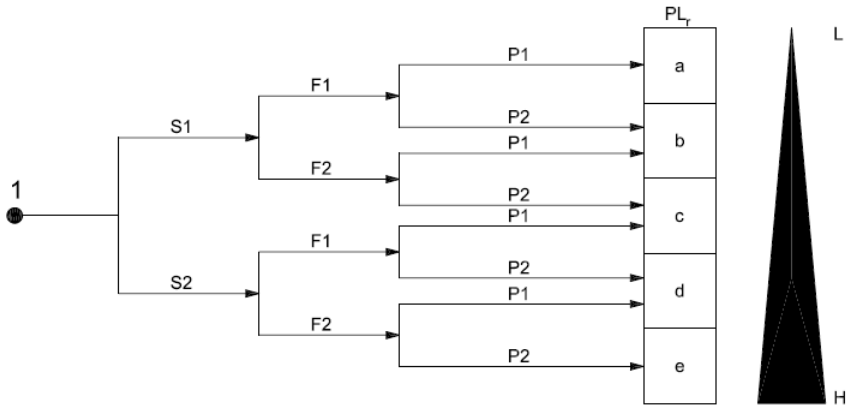
表 5-1　パフォーマンスレベル(PL)、SIL と PFH_D の関係

PL	単位時間当たりの危険側故障発生の平均確率(PFH_D) ［1/h］	SIL
a	$10^{-5} \leqq PFH_D < 10^{-4}$	−
b	$3\times10^{-6} \leqq PFH_D < 10^{-5}$	1
c	$10^{-6} \leqq PFH_D < 3\times10^{-6}$	1
d	$10^{-7} \leqq PFH_D < 10^{-6}$	2
e	$10^{-8} \leqq PFH_D < 10^{-7}$	3

(3)　安全機能の要求パフォーマンスレベル(PLr)の決定

リスクアセスメントに基づくリスク低減方策で特定された全ての機能安全による安全機能は、ISO 13949-1 で示されるリスクグラフ(図 5-3)に基づいて機能安全の設計に求められる要求性能(要求パフォーマンスレベル：PLr)を先ず決定しなければならない。

図 5-3 のリスクグラフは、各安全機能の SRP/CS のリスク評価に対して考慮するものである。



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

リスクパラメータ

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／又は暴露時間が短い

F2　高頻度～連続、及び／又は暴露時間が長い

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 5-3 機能安全の要求性能(PLr)を決定するリスクグラフ(ISO 13849-1 より)

S:傷害のひどさ

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、その状態が認知でき、かつ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。その他は、危険源回避の可能性がほとんどない場合として 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。リスクが高くなるほど、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。(安全機能を実行する制御システムの危険側故障の発生確率を小さくしなければならない。)

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。

５．２ 具体的な要求安全度水準の決定

本書の例(図 5-4)における機能安全を用いる各保護方策の具体的な要求安全度水準の決定例を表 5-2 に示す。

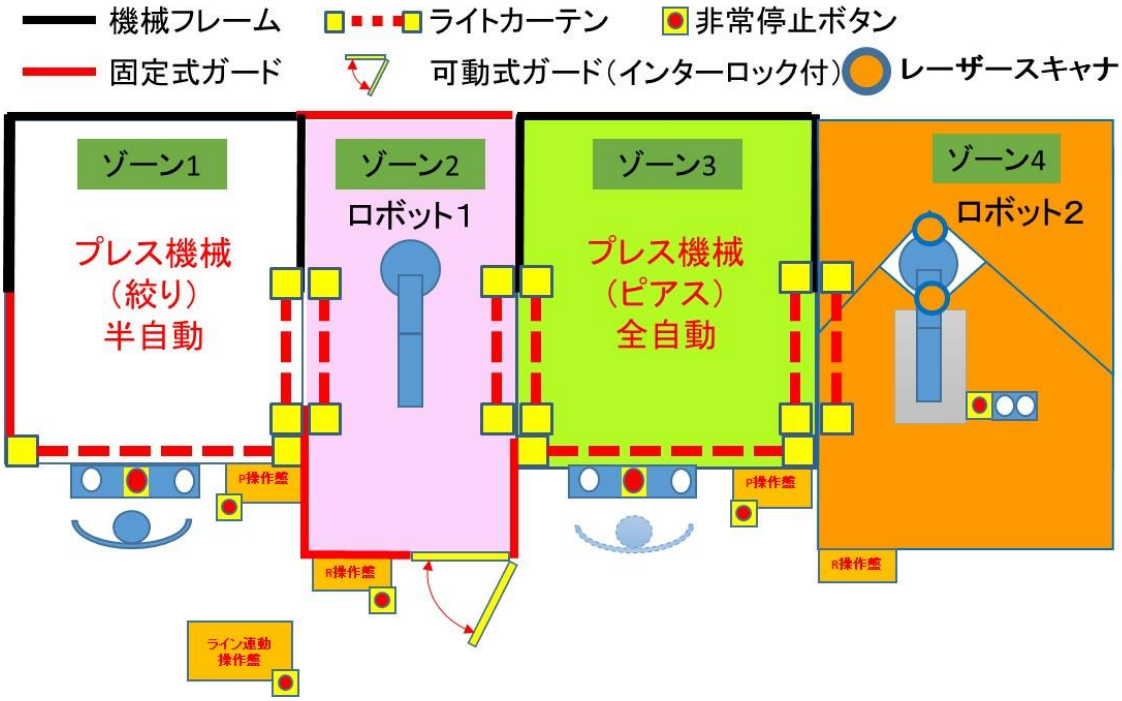


図 5-4 機能安全を用いるリスク低減方策

表 5-2 具体的な要求安全度水準の決定例

保護方策	傷害のひどさ S	暴露の頻度 F	回避の可能性	PLr
非常停止 EMG11	S2	F1	P2	d
非常停止 EMG1-1	S2	F1	P2	d
非常停止 EMG1-2	S2	F1	P2	d
非常停止 EMG2	S2	F1	P2	d
非常停止 EMG3-1	S2	F1	P2	d
非常停止 EMG3-2	S2	F1	P2	d
非常停止 EMG4-1	S2	F1	P2	d
非常停止 EMG4-2	S2	F1	P2	d
光線式安全装置 LG1-1	S2	F2	P2	e
光線式安全装置 LG1-2	S2	F1	P2	d
光線式安全装置 LG2-1	S2	F1	P2	d
ドアインターロック DIL1	S2	F1	P2	d
光線式安全装置 LG2-2	S2	F1	P2	d
光線式安全装置 LG3-2	S2	F1	P2	d
光線式安全装置 LG3-1	S2	F1	P2	d
光線式安全装置 LG3-3	S2	F1	P2	d
光線式安全装置 LG4	S2	F1	P2	d
レーザースキャナ LSC1	S2	F1	P2	d
レーザースキャナ LSC2	S2	F1	P2	d

第６章　IMS 安全関連システムの設計と検証

６．１　はじめに

IMS においても安全関連システムの設計は、一般の機械安全の設計手順と同様である。IMS の安全関連システムの設計は、多くの場合、IEC 62061 または IEC 61508 による電気・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して安全度水準(SIL)で評価された機器(安全 PLC 等)と ISO 13849 ベースのパフォーマンスレベル(PL)で評価される機器(リミットスイッチ、油圧制御・空圧制御バルブ、コンタクタ、リレー等)の組み合わせで構成されている。

本章では、IMS の安全関連システムの設計・設計検証手順を設計、設計検証の事例を入れて示す。

６．２　安全関連システムの設計手順

(1)機能安全(安全関連システム)の設計概要

ア　ISO 13849-1 による安全機能の要求パフォーマンスレベル(PLr)見積事例

リスクアセスメントに基づくリスク低減方策で特定された全ての機能安全による安全機能は、ISO 13949-1 で示されるリスクグラフに基づいて機能安全の設計に求められる要求性能(要求パフォーマンスレベル：PLr)を先ず決定しなければならない。(5.1 節参照)

安全機能の要求パフォーマンスレベル(PLr)の見積もり事例として ISO 13949-1 で示されるリスクグラフを用いて、自動プレス機械のインタロック付き可動ガードのインタロック装置の安全機能に要求される性能レベル(PLr)を導出すると、リスクアセスメントから以下の事象と各リスクパラメータ状況が同定され、リスク見積もり結果から PLr は“d”が要求されることになる。(図 6-1)

- 危険事象：プレス内で作業中にスライドが下降する。
- 傷害のひどさ：プレス機械の加工能力より災害時は、必ず重大災害が生じる。
- 発生頻度：自動プレスであるためガードの開での作業頻度は、スライド内への手または身体の一部が入っての作業頻度、作業時間は、少ない。

- 回避可能性：プレス機械の生産速度は、高速で動作するため、危険事象発生時の回避の可能性は、殆ど不可能と判断される。

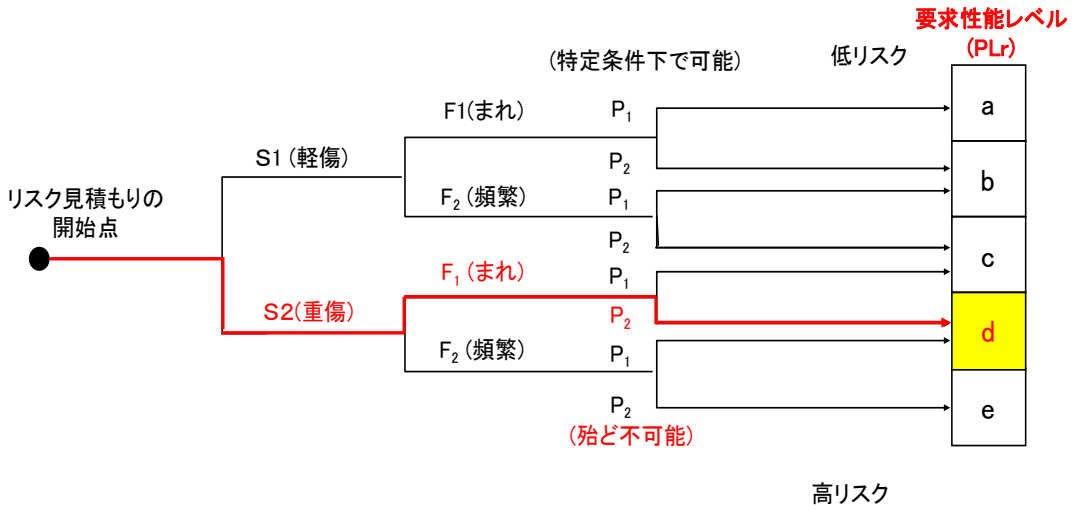


図 6-1 PLr の決定の事例

イ　安全関連システムにより実行される安全機能の特定と要求特性の指定

安全関連システムにより実行される安全機能は、リスクアセスメントの結果としてのリスク低減において制御システムが使用される方策(機能安全による本質的安全設計方策、インタロックまたは検知保護装置などの保護装置による安全防護または非常停止装置などの付加保護方策などのリスク低減：以下機能安全によるリスク低減とする)が、全て対象である(第 5 章図 5-1 参照)。したがって、リスク低減方策として決定した機能安全によるリスク低減方策全てにおいて、安全機能とその要求特性の内容をリスク低減方策の設計方針として示さなければならない。

ここでは、リスク低減方策の設計方針として、安全機能とその要求特性の記載内容を示した図 6-1 の結果に基づき、機能安全(制御システムの安全関連部)の設計手順と設計検証を行う事例を示す。そこで、一般的に機械設備で使用されるインタロック付き可動ガード(図 6-2)のプレス機械へ適用事例として、ISO 13849-1、IEC 62061、ISO 23849 を基に機能安全設計の要求事項を詳述する。

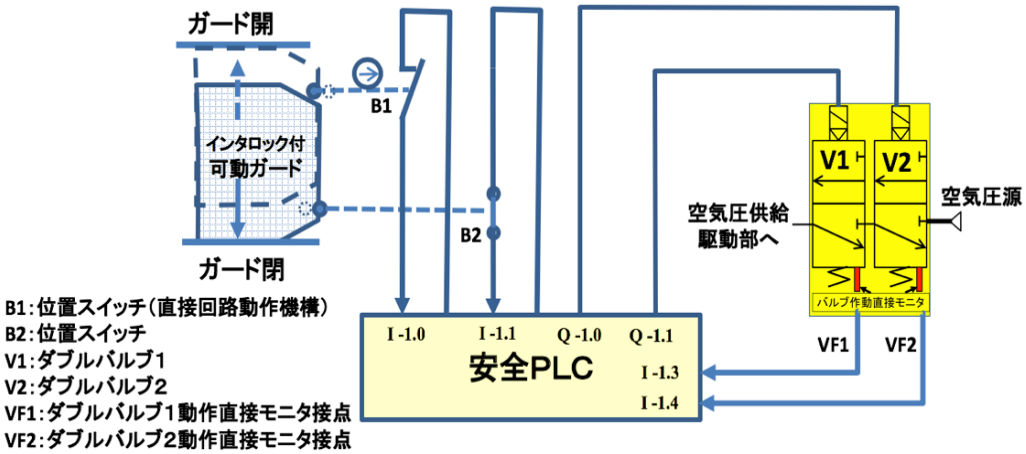


図 6-2 安全 PLC を使用したインタロック付き可動ガードの機能安全事例

【安全機能と要求特性の記載例】

可動ガードインタロックによる停止カテゴリ 0 での機械駆動エネルギーの遮断停止機能：

可動ガードのインタロック装置により可動ガードを開くと、インタロック装置の安全機能:STO(安全トルクオフ)により機械駆動クラッチブレーキバルブへのエネルギー遮断により、機械駆動のクラッチへの空圧エネルギーが遮断されると同時に、機械式ブレーキ開放が解除され機械式ブレーキがかかり、機械が停止しその位置が保持される。

ウ　安全機能の設計

安全機能の要求パフォーマンスレベル(PLr)が決定した後、安全機能を PLr 以上のパフォーマンスレベル(PL)となるように機能安全設計を検討する。図 6-3 に機能安全設計のための PL とカテゴリ、$MTTF_D$、DC_{avg}、CCF の設計上必要な各要件との関係を示す。

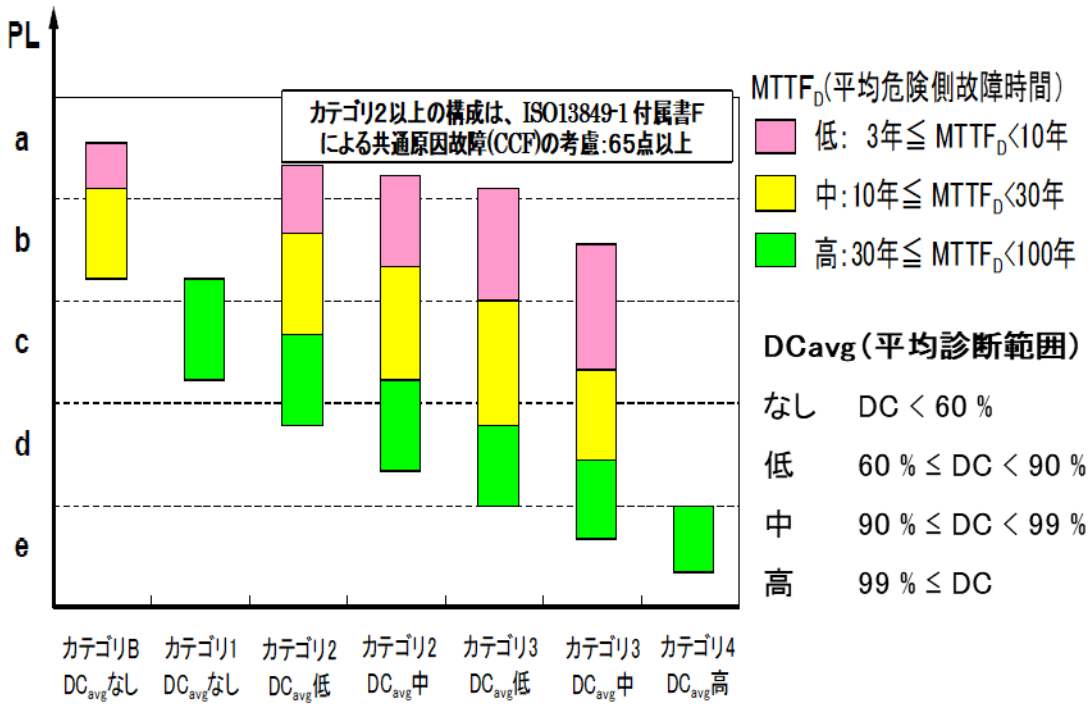
① カテゴリ：SRP/CS のハードウエア構成

② $MTTF_D$：SRP/CS の平均危険側故障時間(単位：年)

③ DC_{avg}：SRP/CS の平均診断範囲のレベル(単位：%)

④ CCF：カテゴリ 2 以上のシステムの共通原因故障の考慮

⑤ PFH_D:危険側故障の平均発生確率(単位：/h)



表K.1－上図 (ISO13849-1:図5の数値)

	危険側故障の平均確率(1/h)及び対応のパフォーマンスレベルPL							
各チャネルのMTTFD(年)	カテゴリB PL DCavg="なし"	カテゴリ1 PL DCavg="なし"	カテゴリ2 PL DCavg="低"	カテゴリ2 PL DCavg="中"	カテゴリ3 PL DCavg="低"	カテゴリ3 PL DCavg="中"	カテゴリ4 PL DCavg="高"	
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b		
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b		
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b		
82		$1.39<10^{-6}$ c	$6.61<10^{-7}$ d	$3.01<10^{-7}$ d	$1.35<10^{-7}$ d	$5.79<10^{-8}$ e	$3.08<10^{-8}$ e	
91		$1.25<10^{-6}$ c	$5.88<10^{-7}$ d	$2.61<10^{-7}$ d	$1.14<10^{-7}$ d	$4.94<10^{-8}$ e	$2.74<10^{-8}$ e	
100		$1.14<10^{-6}$ c	$5.28<10^{-7}$ d	$2.29<10^{-7}$ d	$1.01<10^{-7}$ d	$4.29<10^{-8}$ e	$2.47<10^{-8}$ e	
2500							$9.06<10^{-10}$ e	

図 6-3 PL と「カテゴリ、$MTTF_D$、DC_{avg}、CCF」との関係

各要件の詳細と併せて、図 6-2 の適用事例を設計手順に従って詳述する。

エ　安全機能設計概要の説明(図 6-2 の事例参照)

【安全機能設計概要】

- ガード本体は、ISO 14120 の要求事項を満足した構造でガード本体、隙間からの安全距離は、ISO 13857 に従った安全距離を確保する。

- 保護装置(ガードインタロック)による停止機能：可動ガードを開くとバルブへの制御電源供給遮断によりバルブからの駆動エネルギー源である空気圧供給を遮断する。
- 可動ガード(扉)の保護装置(ガードインタロック)による停止機能の安全確保を保証するための危険源域までの安全距離は、ISO 13855 にて設計した最小距離以上を確保する。
- 機能安全設計は、PLr=d を満足するためにカテゴリ＝3、$MTTF_D$＝中以上、DC_{avg}＝低以上で PL=d を達成する設計とする。

オ　安全関連システムのカテゴリとカテゴリの選定

安全関連システムのカテゴリは、故障に対する耐性能力から B、1、2、3、4 の 5 つの分類がある。表 6-1 にその分類の詳細について示す。

表 6-1　安全関連システム(SRP/CS)の各カテゴリの要求事項

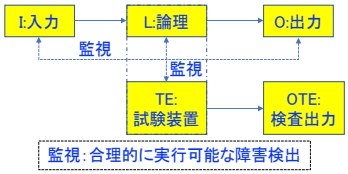
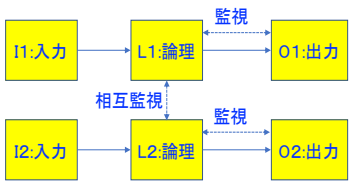
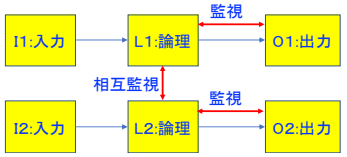
カテゴリ	ISO 13849-1:2015 要求事項要約	各カテゴリの システム挙動 （耐性）	安全を達成するために使用する原理	指定構成
B	SRP/CS 及び／又は保護設備、並びにその構成部品は、予期した影響に耐え得るように、関連する規格に従って設計、製造、選択、組立、組み合わされなければならない。ISO 13849-2”基本的安全原則”を使用しなければならない。	障害発生が、安全機能の喪失をもたらすことがある。	主として、横成部品の選択によって特徴付けられる。	
1	B の要求事項を適用する。ISO 13849-2 に示される”十分に吟味された構成部品”及び”十分に吟味された安全原則”を用いなければならない。	障害発生が、安全機能の喪失をもたらすことがあるが、発生確は、カテゴリ B より低い。		
2	B の要求事項及び十分に吟味された安全原則の使用を適用しなければならない。安全機能は、機械の制御システムによって適切な間隔でチェックしなければならない。	チェック間の障害の発生が、安全機能の喪失をもたらすことがある。安全機能の喪失は、チェックによって検出される。	主として、構造によって特徴付けられる。	
3	B の要求事項及び十分に吟味された安全原則の使用を適用しなければならない。安全関連部は、次のように設計しなければならない。 ●いずれの部分の単一の障害も、安全機能の喪失をもたらさない。 ●合理的に実施可能な場合、単一の障害が検出される。	単一の障害発生時、安全機能が常に実施される。すべてではないが、障害は検出される。検出されない障害の蓄積で、安全機能の喪失をもたらすことがある。		
4	B の要求事項及び十分に吟味された安全原則の使用を適用しなければならない。安全関連部は、次のように設計しなければならない。 ●いずれの部分の単一の障害も、安全機能の喪失をもたらさない。 かつ ●単一の障害は、安全機能に対する次の動作要求時、又はそれ以前に検出される。それが不可能な場合、障害の蓄積が安全機能の喪失をもたらしてはならない。	障害発生時、安全機能が常に実施される。蓄積障害の検出は、安全機能の喪失の確率を引き下げる(高 DC)。障害は、安全機能の喪失を予防できる時間内に検出される。		

図 6-4 にカテゴリ 3 以上で構成されている図 6-3 の事例の安全関連システムの機能ブロック図を示す。

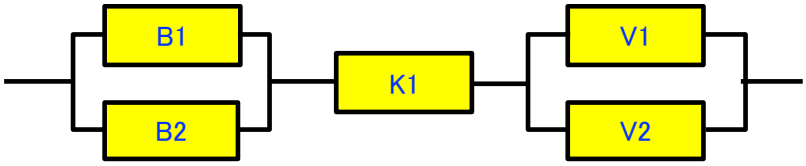


図 6-4　安全関連システムの機能ブロック図記載事例(図 6-2 の事例参照)

図 6-2 のカテゴリ 3 以上の安全関連システム事例の設計概要は、以下である。

- カテゴリ 3 以上の冗長回路で、入力の冗長化、論理は安全 PLC により各安全機能に対する冗長化の要求事項を満足する機器を選定、出力は、ダブルバルブによる冗長対応できる機器を選定。
- 入力の冗長化構成は、IEC 60947-5-1(JIS C 8201-5-1)適合の直接開路動作機構の位置スイッチ B1 の N.C.接点と位置スイッチ B2 の N.O.接点を安全 PLC(安全関連システムとして使用が認証された PLC)に入力し安全 PLC で状態監視する。
- 機械駆動は、ダブルバルブ(V1、V2)により空気圧を機械駆動部に供給する。またダブルバルブ(V1、V2)は、各バルブスプールの動作状態を直接モニタする接点 VF1、VF2 を安全 PLC に入力し、安全 PLC で状態監視する。

カ　安全関連システムの $MTTF_D$ の算出と確認

システム構成が決まれば、PL 設計として安全関連システムの $MTTF_D$ を算出する。液圧式、空圧式、機械式・電気機械式の各単体の $MTTF_D$ は、B_{10D}(機構部品の 10%に危険側故障に至るまでの平均動作回数)、または B_{10}(機構部品の 10%に故障が至るまでの平均動作回数)、または $MTTF_D$ がメーカから提供されている場合はそれを使用し、値がメーカから提供されていない場合は、ISO 13849-1 表 C.1 の B_{10D} または $MTTF_D$ の値を使用する。

以下に個々のコンポーネントの B_{10D}/B_{10} から $MTTF_D$ を求める手順を示す。

① 機械設備(プレス機械)の使用期間は、設備仕様より 30 年間である。機能安全維持のためには、保守を考慮するために使用期間を明確にする必要がある。

② 機構部品の B_{10D} または B_{10} を部品メーカに確認する。

【B_{10}が分からない場合は、ISO 13849-1 の附属書 C の B_{10D} 値を使用する。】

B_{10}が、部品メーカから提供された場合は、危険側故障、安全側故障の発生確率は同等とみなして B_{10} の２倍の値を B_{10D}（B_{10D}=2xB_{10}）とする。

③　安全機能の年間動作回数（n_{op}）を以下の式で算出する。

n_{op}＝d_{op}（稼働日/年）×h_{op}（稼働時間/日）×3,600 / t_{cycle}（作動間隔（秒））

例えば、d_{op}=300 日/年、h_{op}=20 時間/日、 t_{cycle}=10 分（600 秒）

とすると→ n_{op}=36,000 回/年

④ 【B_{10D}】と【n_{op}】から以下の計算で $MTTF_D$ を求める。

$MTTF_D$ ＝ B_{10D} /(0.1 × n_{op})

例えば、B_{10D}=200,000 回とし③の n_{op} の値を使用すると

→ $MTTF_D$= 56 年　として求まる。

⑤ T_{10D}＝(B_{10D} / n_{op})＝機器の 10%危険側故障間隔（年）の考慮

$MTTF_D$ として算出された機器も T_{10D}（年）の作動回数で機器の 10%が故障することになることから各機器の使用も T_{10D}（年）で制限される。各機器は、$MTTF_D$ を使用期間維持するために T_{10D}（年）を考慮してそれ以前に機器の交換を行う必要がある。

例えば、本事例の機械設備の使用期間 30 年の間であり、③で求めた機器の $MTTF_D$= 56 年は、T_{10D}= 5.6 年となるので機器は 5 年程度で交換されることが求められる。

【参考：B_{10D} から $MTTF_D$ を求める計算式】

① 計算条件

(1) B_{10D}＝機器の 10%平均危険側故障回数

(2) n_{op}＝年間操作回数（年間安全機能作動回数）

(3) T_{10D}＝(B_{10D} / n_{op})＝機器の 10%危険側故障間隔（年）

(4) $MTTF_D$＝機器の平均危険側故障時間（年）

(5) λ_d＝危険側故障確率

② 計算式

計算式の前提条件は、故障率一定の指数分布の仮定で考える。

λ_d＝危険側故障確率とし、危険側故障確率 λ_d が一定とした信頼度および故障率（不信頼度）は、指数分布として考えると、それぞれは式(1)、式(2)で示される。

信頼度　$R(t) = e^{-\lambda d \cdot t}$　　－－－(1)

不信頼度 $F(t) = 1 - e^{-\lambda d \cdot t}$　　－－－(2)

10%の危険側故障率(不信頼度)は、(2)式に T_{10D} を代入して求まる。

$$F(T_{10D}) = 1 - e^{-\lambda d \cdot T_{10D}} = 0.1 \quad －－－(3)$$

式(3)の両辺を整理すると(4)式が求まる。

$$e^{-\lambda d \cdot T_{10D}} = 0.9 \quad －－－(4)$$

式(4)式の両辺の対数を取り[式(5)]、それを展開すると(6)が求まる。

$$\mathrm{Ln}\left(e^{-\lambda d \cdot T_{10D}}\right) = \mathrm{Ln}(0.9) \cong -0.10536 \quad －－－(5)$$

$$-\lambda d \cdot T_{10D} \cong -0.10536$$

$$\lambda d \cong {}^{0.10536}/_{T_{10D}} \quad －－－(6)$$

$MTTF_D$(平均危険側故障時間)は、式(7)で示されるので

$$MTTF_D = {}^{1}/_{\lambda d} \quad －－－(7)$$

式(7)に式(6)を代入すると式(8)となる。

$$MTTF_D \cong {}^{T_{10D}}/_{0.10536} \cong {}^{T_{10D}}/_{0.1} \quad －－－(8)$$

(8)式に$T_{10D} = \frac{B_{10D}}{n_{op}}$ を代入すると

$MTTF_D$とB_{10D}の関係式(9)となる。

$$MTTF_D \cong {}^{B_{10D}}/_{0.1\, n_{op}} \quad －－－(9)$$

E/E/PE(電気、電子、プログラマブル電子)機器は、メーカ(個々の企業が開発する場合は開発者)から PL 評価のための $MTTF_D$ または PFH_D を入手する。

各単体の $MTTF_D$ が、決まれば機器を組み合わせたシステムの $MTTF_D$ を算出する。算出方法と算出した値の適用内容について以下に示す。これらの $MTTF_D$ の計算結果は、SRP/CS の PL レベルを判定するために ISO 13849-1 の図 5 または表 K.1 を使用する際に使用する。各サブシステムの $MTTF_D$は、カテゴリ 4 以外は、最大 100 年として制限される。(カテゴリ 4 の場合は、最大 2,500 年)

③　PL 評価のための同一チャンネル全体の $MTTF_D$ の計算式と計算事例

機器が、同一チャネル内で結合されている場合は、図 6-5 の計算式(A)で算出する。

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{N} \frac{1}{\mathrm{MTTF_{D}i}} \qquad ---(A)$$

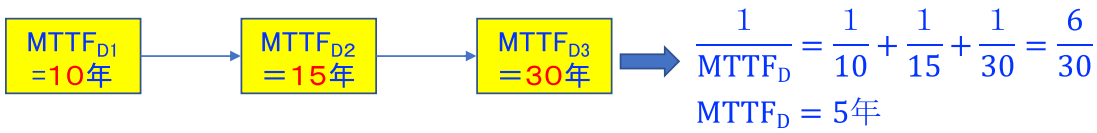
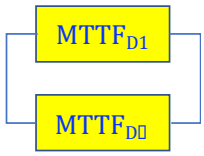


図 6-5　同一チャネル全体の MTTF(MTTF$_D$)の計算式と計算事例

④　PL 評価のための 2 チャンネル全体の MTTF$_D$ の計算式と計算事例

本来の MTTF$_D$ の計算式は、不信頼度計算から図 6-6 の式(B)が求まる。(参考)



$$\mathbf{MTTF_D = MTTF_{D1} + MTTF_{D2} - \frac{1}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}}} \qquad ---(B)$$

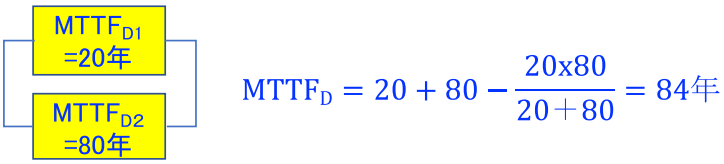
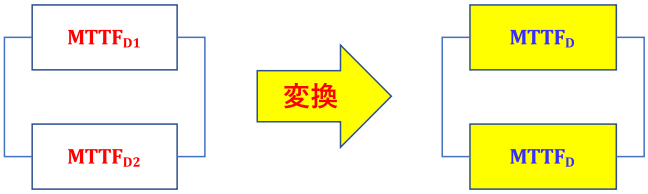


図 6-6　本来の２チャンネル全体の MTTF$_D$の計算式(参考)

PL 評価のためのシステムが冗長(二重化)構成の場合は、図 6-7 で算出する。本計算式(C)は、本来の(二重化)構成の MTTF$_D$ の結果である計算式(B)とは異なるが、ISO 13849-1 の図 5 または表 K.1 を使用してパフォーマンスレベル、PFH$_D$ を決定するための MTTF$_D$ を求めるための計算式(変換式)である。



$$\mathbf{MTTF_D} = \frac{2}{3}\left[\mathbf{MTTF_{D1}} + \mathbf{MTTF_{D2}} - \frac{1}{\frac{1}{\mathbf{MTTF_{D1}}} + \frac{1}{\mathbf{MTTF_{D2}}}}\right] \quad \text{---(C)}$$

図 6-7　PL 評価のための２チャンネル全体の MTTF$_D$の計算式

図 6-7 の計算式(C)の係数 2/3 は、図 6-6 の計算式(B)を用いて図 6-7 の変換図を数式で変換すると計算式(D)で示すことができる。

$$\mathbf{MTTF_{D1}} + \mathbf{MTTF_{D2}} - \frac{1}{\frac{1}{\mathbf{MTTF_{D1}}} + \frac{1}{\mathbf{MTTF_{D2}}}} = \mathbf{MTTF_D} + \mathbf{MTTF_D} - \frac{1}{\frac{1}{\mathbf{MTTF_D}} + \frac{1}{\mathbf{MTTF_D}}} \quad \text{---(D)}$$

計算式(D)の右辺を MTTFD で整理すると計算式(E)となる。

$$\mathbf{MTTF_{D1}} + \mathbf{MTTF_{D2}} - \frac{1}{\frac{1}{\mathbf{MTTF_{D1}}} + \frac{1}{\mathbf{MTTF_{D2}}}} = \frac{\mathbf{3}}{\mathbf{2}}\mathbf{MTTF_D} \quad \text{---(E)}$$

両辺に 2/3 を乗じて左辺と右辺を入れ換えれば以下の計算式(C)と同じ計算式(F)が求まる。

$$\mathbf{MTTF_D} = \frac{2}{3}\left[\mathbf{MTTF_{D1}} + \mathbf{MTTF_{D2}} - \frac{1}{\frac{1}{\mathbf{MTTF_{D1}}} + \frac{1}{\mathbf{MTTF_{D2}}}}\right] \quad \text{---(F)}$$

以下に計算式(B)を用いて変換前後での MTTF$_D$の計算検証結果を図 6-8 に示す。

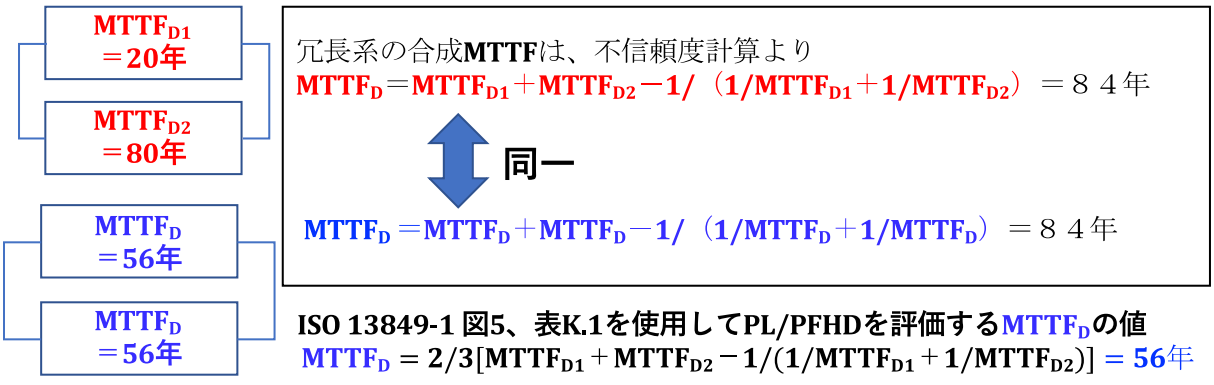


図 6-8　本来の 2 チャンネル全体の MTTF$_D$の計算式と計算検証【参考】

図 6-8 は、式(B)により求められた $MTTF_D$ を本来の $MTTF_D$ の計算式に代入し、本来の $MTTF_D$ は、同じであることの検証結果を示した。機械安全の機能安全設計者は、式(B)が冗長システムの ISO 13849-1 の図 5、表 K.1 を利用して PL を評価するための変換式であることを理解して設計を行うことが必要である。

キ　安全関連システムの DC/DC_{avg} と DC_{avg} の算出と確認

DC(診断範囲)は、検出される危険側故障率と全危険側故障率の比として定義されている。また、システム全体の診断範囲 DC_{avg} は、全ての検出される危険側故障率の合計と全危険側故障率との比として式(G)で示される。

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \cdots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \cdots + \frac{1}{MTTF_{DN}}} \quad ---(G)$$

$1/MTTF = \lambda$ (故障率)と置き換えると式(H)で示される。

$$DC_{avg} = \frac{\lambda D1 \times DC1 + \lambda D2 \times DC2 + \cdots + \lambda DN \times DCN}{\lambda D1 + \lambda D2 + \cdots + \lambda DN} \quad ---(H)$$

各入力、論理、出力の診断範囲 DC の見積もりの目安として ISO 13849-1 附属書 E、表 E.1 を参照する。

診断範囲の例として図 6-2 のシステム構成の DC のレベルを以下に示す。

(例 1)　安全 PLC の安全機能と組み合わせてガードのインタロックに N.O.接点直接開路動作機構の N.C 接点による異種冗長回路で監視するシステム：DC=99%

(例 2)　安全機能の「入力、論理、出力、ソフトウエア」が認証され DC のレベルが明確になっている PLC(安全 PLC)：DC=99%としてガードインタロックの安全機能として直接監視処理などによる DC が確認されているもの。

(例 3)　出力の冗長回路で動作監視するシステム、例として空圧制御のダブルバルブで２個のバルブのスプールの動作をセンサにて直接監視できる構成を持ったもので安全 PLC の安全機能と組み合わせて出力の動作監視を行っているもの：DC=99%

ク　安全関連システムの CCF と CCF の確認

安全関連システムの CCF(共通原因故障)は、システム全体を構成する際の考慮されているレベルを判断する。具体的には ISO 13849-1 附属書 F、表 F.1 で示されて

いる工学的な共通原因故障低減の方策に対する評価事項と採点が示されている。安全関連システムの設計時に設計内容を ISO 13849-1 附属書 F、表 F.1 の内容に従って採点を行い 65 点以上で CCF に対する考慮がなされていると判定される。各採点項目の採点は、満点か 0 点のどちらかで判定する。従って評価項目の内容全てを満足しないものは 0 点とする。以下に ISO 13849-1 附属書 F、表 F.1 の項目を示す。

表 6-2　ISO 13849-1 附属書 F、表 F.1 採点方法及び CCF に対する方策の定量化

No	CCF に対する方策	得点
1	**分離／隔離**	
	信号経路間の物理的な分離、例えば、 －　配線／配管での分離 －　動的試験によるケーブルの短絡及び断線の検出 －　各チャネルの信号経路の個別シールド －　プリント基板上での回路間の十分なクリアランス及び沿面距離	15
2	**多様性(ダイバーシティ)**	
	異なる技術的方式／設計又は物理的原理の使用、例えば、 －　第 1 チャネルは電子又はプログラマブル電子方式で、第 2 チャネルは電気機械式のハードワイヤ方式 －　安全機能の各チャネルは異なる信号によって始動(例えば、位置、圧力、温度)及び／又はデジタル及びアナログによる測定(例えば、距離、圧力又は温度)及び／又は異なる製造業者によるコンポーネント	20
3	**設計／適用／経験**	
3.1	過電圧、過圧力、過電流、過熱などに対する保護	15
3.2	使用のコンポーネントは、“十分吟味されている”	5
4	**査定／分析**	
	制御システムの安全関連部の各部に対して、FMEA が実施されており、その結果は、設計段階において CCF を回避するために考慮されている。	5
5	**適格性(能力)／訓練**	
	CCF の原因及び結果を理解できるような設計者の訓練	5
6	**環境面**	
6.1	電気／電子システムに対して、適切な規格(例えば、**IEC 61326-3-1**)に従ったCCF に対する汚染防止及び電磁妨害の防止(EMC)。 流体システム：圧力媒体のろ過、ほこりの侵入の防止、圧縮空気の水抜き、例えば、圧力媒体の純度に関してはコンポーネント製造業者の要求事項に従う。 **注記**　流体システムと電気システムとの組合せに対しては、これらの両面を考慮することが望ましい。	25
6.2	他の影響 温度、衝撃、振動、湿度のような全ての環境関連(例えば、関連の規格で規定される)の影響に対して耐性の要求事項を考慮する。	10
	合計	**最大 100**

合計得点	CCF を回避するための方策 [a]
65 以上	要求事項に適合
65 未満	要求事項に不適合 ⇒ 追加方策の選択

注[a] 技術方式上の方策が関連しない場合でも、この欄で算定された得点は、包括的な計算のときに考慮することができる。

(2)安全関連システムの文書概要と PL の確認

図 6-4 の事例についての機能安全設計の PL について、(ア)～(ク)の内容を安全関連システムの文書概要として以下にまとめる。(ア)～(ク)ですでに記載した内容もあるが機能安全の文書化のまとめとして示す。

【安全機能と要求特性の記載例】

可動ガードインタロックによる停止カテゴリ 0 での機械駆動エネルギーの遮断停止機能：(【停止カテゴリ 0】: IEC 60204-1(JIS B 9960-1) 箇条 9.2.2 参照)

可動ガードのインタロック装置により可動ガードを開くとインタロック装置の安全機能：STO(安全トルクオフ)により機械駆動クラッチブレーキバルブへのエネルギー遮断により機械駆動のクレッチへの空圧エネルギーが遮断されると同時に機械式ブレーキ開放が解除され機械式ブレーキがかかり、機械が停止しその位置が保持される。

【安全機能設計概要】

- ガード本体は、ISO 14120 の要求事項を満足した構造でガード本体、隙間からの安全距離は、ISO 13857 に従った安全距離を確保。
- 保護装置(ガードインタロック)による停止機能：可動ガードを開くとバルブへの制御電源供給遮断によりバルブからの駆動エネルギー源である空気圧供給を遮断する。
- 可動ガード扉の保護装置(ガードインタロック)による停止機能に安全確保を保証する危険源域までの安全距離は、ISO 13855 にて設計した最小距離以上を確保する。
- 機能安全設計は、PLr=d を満足するためにカテゴリ＝3、$MTTF_D$＝中以上、DC_{avg}＝低以上で PL=d を達成する設計とする。

【カテゴリ構成】

図 6-4 で示した機能ブロック図のカテゴリ構成について以下に示す。

- カテゴリ 3 以上の冗長回路で、入力の冗長化、論理は安全 PLC により各安全機能に対する冗長化の要求事項を満足する機器を選定、出力は、ダブルバルブによる冗長対応できる機器を選定。

- 入力の冗長化構成は、IEC 60947-5-1(JIS C 8201-5-1)適合の直接回路動作機構の位置スイッチ B1 の N.C.接点と位置スイッチ B2 の N.O.接点を安全 PLC(制御システムの安全関連部として使用が認証された PLC)に入力し安全 PLC で状態監視する。
- 機械駆動は、ダブルバルブ(V1、V2)により空気圧を機械駆動部に供給する。またダブルバルブ(V1、V2)は、各バルブスプールの動作状態を直接モニタする接点 VF1、VF2 を安全 PLC に入力し、安全 PLC で状態監視する。

【安全機能の $MTTF_D$ または PFH_D とシステムの PL 評価】

① 入力部サブシステムの評価

- 位置スイッチ B1：B_{10D}＝200,000 回（メーカ値）
  年間動作回数 n_{op} =36,000 回/年→ **T_{10D}(B1)=5.6 年　$MTTF_D$(B1)=56 年**

位置スイッチ B1 の交換周期は 5 年とする。

- 位置スイッチＢ２：B_{10D}＝2,000,000 回(メーカー値)
  年間動作回数 n_{op} =36,000 回/年→ **T_{10D}(B1)=56 年　$MTTF_D$(B1)=560 年**
- 入力部サブシステムの $MTTF_D$ は、B1 と B2 の冗長回路より
  $MTTF_D$(B1/B2)=376 年(カテゴリ 4)【単一チャネルの場合は 100 年で制限】
- 入力の DC(診断範囲)は、安全 PLC により動作状態の冗長監視より **DC=99%**
- カテゴリ 3(DC<99%)・4(DC≧99%)、$MTTF_D$=376 年、DC=99%(高)より
  入力部サブシステムの PL=e (PFH_D=6.44x10^{-9})

② 論理部サブシステムの PFH_D

安全 PLC メーカよりの入手データとして本ガードインタロックに使用する安全機能に対する安全度水準は、「**SIL3、 PFH_D=1.5x10^{-8}**」とのデータを入手。

③ 出力部サブシステムの $MTTF_D$

- 空圧ダブルバルブ V1・V2：B_{10D}＝20,000,000 回(ISO 13849-1 附属書 C・表 C.1)
  バルブ作動サイクル 5 秒(12 サイクル/分)とした年間サイクルより
  年間動作回数 n_{op} =4,500,000 回/年→ **T_{10D}(V1/V2)=4.6 年**
  $MTTF_D$(V1/V2)=46 年

ダブルバルブ(V1/V2)の交換周期は 4 年とする。

- 出力部の DC は、安全 PLC によりバルブスプール動作状態の冗長監視より
  DC=99%
- カテゴリ 4、$MTTF_D$=46 年(高)、DC=99%(高)より

出力部サブシステムの PL=e （PFH_D=6.33x10^{-8}）

④ 安全関連システム全体の PL 評価

入力部サブシステムの評価①、論理部の PFH_D データ②、出力部サブシステムの評価③よりシステム全体の PL 評価は、各 PFH_D データの合計値で評価できる。また、共通原因故障(CCF)に対する低減方策についても設計資料で明確にする必要がある。CCF に対する低減方策採点 65 点以上として以下を評価する。

安全関連システム全体の PL＝6.44x10^{-9}＋1.5x10^{-8}＋6.33x10^{-8}＝8.47x10^{-8}

ISO 13849-1 表 K.1 より　PFHD=8.47x10^{-8}=PLe と評価できる

⑤ 安全関連システムの PL の設計検証

図 6-2 の事例ガードインタロックによる安全機能の設計は、

【設計結果 PL=e ＞ PLr=d】より安全機能の設計として妥当である。

⑥ 安全関連システム(安全 PLC 使用)におけるソフトウエア

図 6-9 に機械安全におけるソフトウエアの検討流れ図と安全 PLC のソフトウエアのソフトの設計内容を示した。

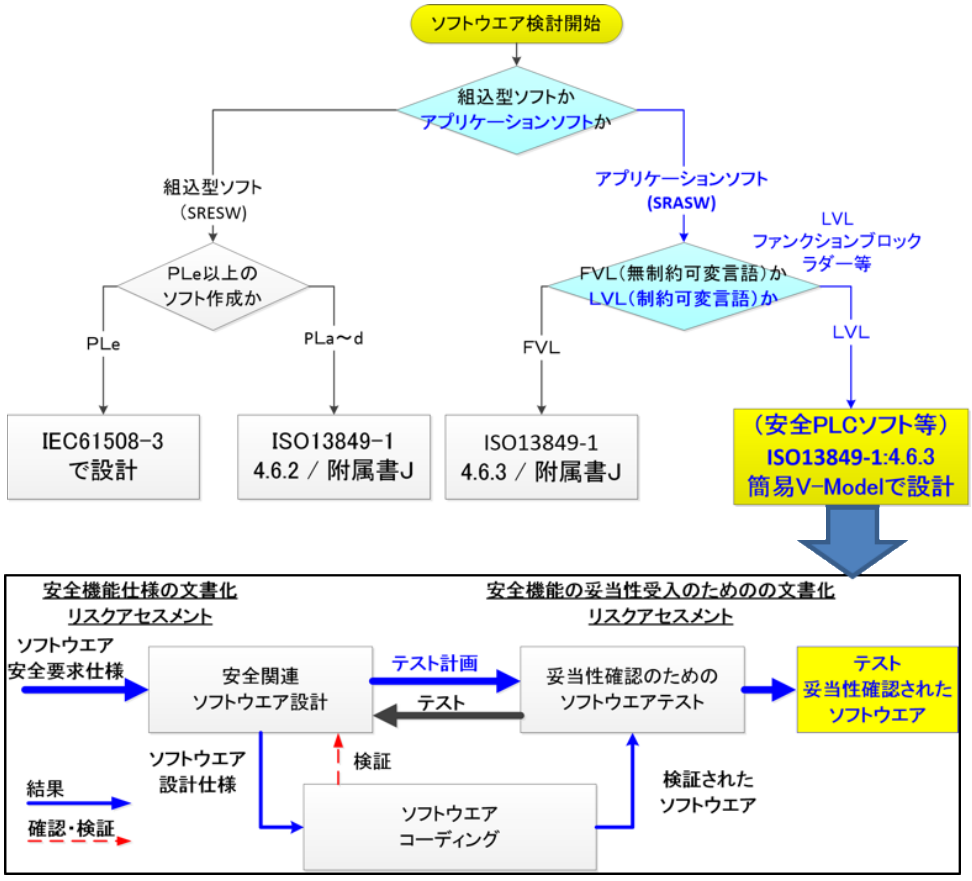


図 6-9　ISO 13849-1 ソフトウエア検討流れ図と安全 PLC

安全 PLC(機械の制御システムの安全関連部)のソフトウエア構築は、一般的に安全 PLC メーカの各安全機能に対するソフトウエアの使用を守って構築することが必要である。その際の作業内容は、図 6-9 に示す簡易Ｖモデルとして表すことができる。

安全 PLC でソフトウエアを構築する際に、一般的に必要と思われる文書について以下に示す。

① リスクアセスメント：リスク低減方策の決定事項を含める
② ハード構成：安全関連システムに関するハードウエア
③ 安全関連ソフトウエア安全要求仕様書：ソフトウエア計画書
④ 安全関連ソフトウエアテスト計画書：品質確認のためのソフトウエア検証計画書
⑤ ソフトウエア設計仕様書：①～④をまとめてソフトウエアでの処理内容を記載
⑥ 機械の制御システムの安全関連部のソフトウエアの記述(コーデング)
⑦ ソフトウエアテスト結果(テストレポート)

安全 PLC ソフトの妥当性説明のために上記以外にも設計、検証過程を記録として残すことも必要である。

６．３　保護装置の活用事例

リスクアセスメントの実施に基づき、リスクが十分許容可能なレベルであれば、リスク低減方策を実施せずとも機械を使用することが可能である。しかし、許容可能なレベルに達していない場合は、リスク低減方策が必要であり、ISO 12100(JIS)に示されている 3 ステップメソッドに基づき、本質的安全設計方策、安全防護および付加保護方策、使用上の情報や、ISO 11161 に示されるタスクゾーン設定や設計方策にてリスク低減を行うことが必要となる。

これらの本質的安全設計方策やタスクゾーンの設定を用いても、もしくは用いることが困難なため、リスクが許容可能なレベルまで低減できない場合は、次のステップとして、タスクゾーンの設定とあわせて、安全防護方策もしくは付加保護方策にてリスク低減を実施する必要がある。

これらの安全防護方策もしくは付加保護方策の代表的な例を、以下に示す。

(1) 安全ガードによる保護

ガードは ISO 12100、ISO 14120 および ISO 11161 に示す要求事項に基づき設置する必要がある。ガードの例として以下があげられる。

ア 固定式ガード

固定式ガードは、取り付けた位置に確実に保持されなければならない。

- 溶接などによって恒久的に固定される、または、
- 特殊ドライバなどの工具を使用しなければ外されたり、開けたりできないように、ねじやナットを用いて固定すること。

なお、固定式ガードは、開閉を行うためにガードの片側にヒンジ機構を持っている場合がある。

イ 可動式ガード

可動式ガードには一般に次のような要求事項があり、必要に応じて機械の制御システムと連携しなければならない。

- 閉じているときはもちろん､開いているときもヒンジまたはガイドレールなどによって、機械類またはその構造物に固定されている状態であること。
- 機械の可動部分がオペレータの動作範囲と重複しているときは､機械の可動部分の方が起動できないこと。また、機械の可動部分が稼動する場合には、オペレータはその範囲内に入ることができないようになっていること｡この仕組みは可動式ガードのうち、インタロック付ガード(必要な場合はロック付き)を用いることで実施できる。
- 可動式ガードのガードがずれたり外されたり､または取り付けたインタロック装置などが欠落あるいは故障した場合は､機械可動部の起動は防止されること。または稼動していれば機械の可動部分は停止すること。これは制御システムの診断機能を用いて実施できる。

(2) 起動機能インタロック付きガード

起動機能インタロック付きガードは、ガードを閉めると他の起動制御器(起動スイッチなど)を用いることなく自動的に機械の起動を行う、インタロック付きガードの特殊な形式。このガードは次のすべての要求を満足できる場合のみ、実施してもよい。

- 基本的にインタロック付きガードとしてすべての要求事項を満足していること。
- 機械のサイクルタイムが短い。

- ガードが開いている間の設定時間は、小さな値にセットすること(例：サイクルタイムと同等)。この時間を越えると、ガードが閉じても起動できないこと。この場合、リセット作業が必要とされる。
- ガードが閉じたときには、必ず身体のすべてが危険区域から完全に外(安全位置)へと出ていること。
- 故障によって意図しない起動などを生じないように、例えば二重化および診断機能を持って設計されていること。
- ガードがそれ自体の重量で下に降りている間に、誤って起動を開始することがないように、例えば、ばね又はカウンタウェイトなどによって開いた状態を確実に維持できること。

(3) 保護装置による制御

機械の安全制御に活用される保護装置の例として、以下があげられる。

ア ドアインタロック装置

特定の条件(一般的にはガードが閉じていない場合)のもとで機械要素の運転を防ぐことを目的とした機械装置、電気装置、又はその他の装置。安全スイッチ、リミットスイッチ、ロック付安全スイッチ、非接触安全スイッチなどがあり、これらのデバイスが取り付けられたガードに対する要求事項として、ISO 12100 および ISO 14119 に基づく下記内容等が求められる。

- ガードが閉じられて危険源が隔離されるまで、運転を許可しないこと。
- 機械の運転中にガードを開けると、運転を停止すること。
- ガードを閉じたことによって、自動的に運転が開始しないこと。
- インタロック装置の無効化可能性の最小化(手の届かない範囲への取り付けなどによるアクセスの制限、工具などで容易に外せない方法での取り付け、状態のモニタリングなど)

図 6-10　ドアインタロック装置事例

イ ライトカーテン

検出区域に存在する不透明な物体によって、装置が放射する光の遮断を検出する光電子発生器と受光器をもち、これによる検知機能をもつ装置。危険源に対しガードを設定することが構造上難しい場合、ガードの開閉頻度が高い場合、またはガードを設置するほどではないが人の進入を検知し危険源を安全に制御する必要がある場合などに使用される。IEC 61496-1、-2 に適合し、Type2 と Type4 がある。

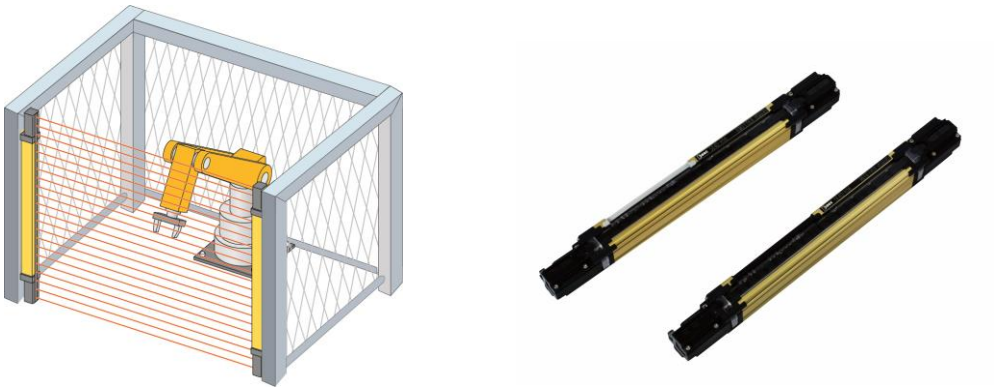


図 6-11　ライトカーテン(光線式安全装置)事例

ウ　レーザースキャナ

その装置の光電式投光器で発生する放射光が、設定された二次元検出区域に存在する物体を照射して生じる拡散反射光を光電受光器が検知することによって物体を検出する装置。 IEC 61496-1、-3 に適合し、Type3 がある。

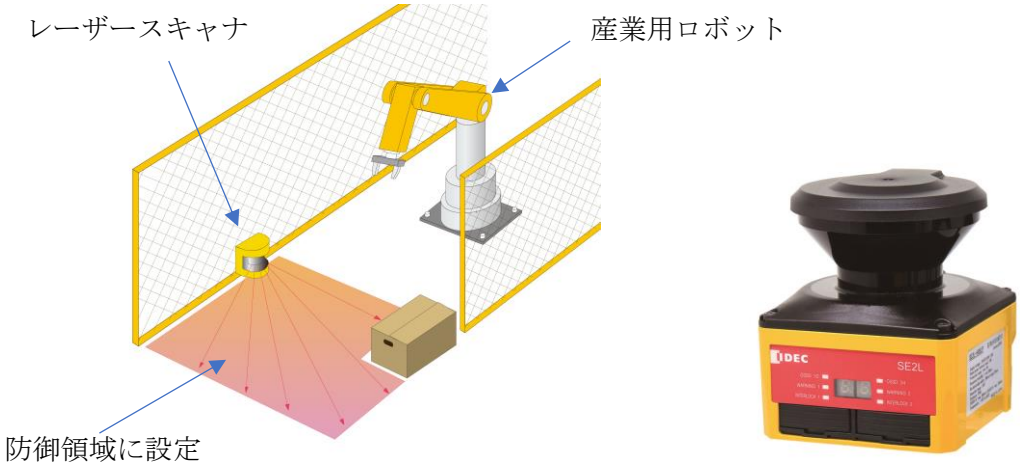


図 6-12　レーザースキャナ事例

エ　圧力検知マットスイッチ

人がマットを踏むことにより、マットに作用する圧力の変化を検知(抵抗値の変化など)して、人体や物体の存在を検知する装置。

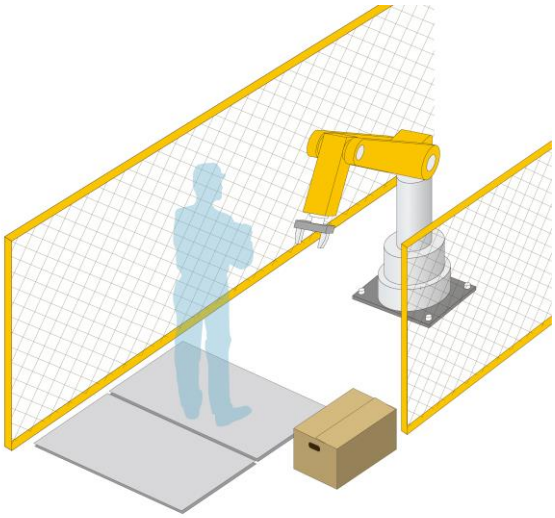


図 6-13　圧力検知マットスイッチ事例

オ　イネーブルデバイス

ガードで危険源を隔離して自動運転を行っている機械も、メンテナンスや段取り替えなどインタロックを無効にした状態で、ガード内で作業を行う必要がある。このような危険区域で作業を行わなければならない場合に、機械の予期しない動作という危険から回避するための安全装置。ロボットのティーチングペンダントや、グリップスイッチなどの手持ちの操作機器に組み込まれて使用される。IMS では 3 ポジションイネーブルデバイスを使う必要がある。

図 6-14　イネーブルデバイス事例

(4) 付加保護方策による保護

ア　非常停止装置

機械設備における非常停止装置は、「発生している、または今にも発生しようとしている」緊急事態を回避するためにオペレータ意思で操作する装置であり、非常停止押しボタンスイッチなどがある。ISO12100 ではリスクアセスメントの結果、必要と判断された場合、必ず適用しなければならない付加保護方策のひとつ。IMS では非常停止装置の操作により、スパン・オブ・コントロールに伴う関連するゾーンの装置や機械を停止させる。

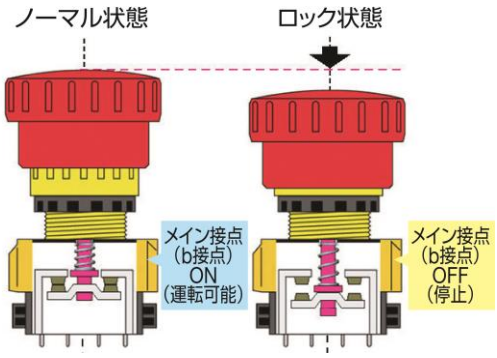


図 6-15　非常停止装置(非常停止押しボタンスイッチ)事例

イ　捕捉された人の脱出及び救助のための方策

オペレータが捕捉される危険源を生じる設備での脱出ルート及び避難場所の確保など、ISO 12100 の要求事項に基づき、捕捉された人の脱出及び救助のための方策を実施する必要がある。

図 6-16　捕捉された人の脱出及び救助のための方策事例

第７章　IMS 安全関連システムの妥当性確認

７．１　妥当性確認の概要

妥当性確認とは、対象となる IMS の設計開発段階で、IMS の安全に関連する機能が、安全要求仕様(目標)及び関連規格の要求事項を満足するかを立証する作業である。直接参照対象となる規格は ISO 11161 となるが、本規格で述べられている設計の妥当性確認は次の通りである。

1　反復プロセスの一部として、インテグレータは設計が要求事項に合致しているかを決定しなければならない。

2　要求事項が合致していない場合、インテグレータは以下を行わねばならない。

・IMS レイアウト、機能性及び又は制限の修正

・介入に関係したリスクを低減するために設備を交換あるいは修正

・新しいアクセス通路及び手段の決定

・介入が実行されなければならない方法を修正

上記のように、妥当性確認はシステム統合にかかる設計過程を対象としており、システムを構成する個別の機械及び機械内部の部品類は、それらのメーカにて規格適合に対する妥当性確認がされていることを前提としている。ただし、インテグレータが購入するこれらの機械の設置や使用条件が正しいかどうかは、インテグレータ自身が妥当性の判断をする必要がある。特に、IMS 制御システムをインテグレータが設計する場合、購入する機械や制御関連装置類を組み合わせ、あるいは機能の変更や追加などを施すことになり、IMS の安全関連システムに対する妥当性確認は必須となる。

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)シリーズが参照される。ただし、本書では前章で述べたように ISO 13849-1 に基づく PL で評価される機器を用いる機能安全設計を対象としているため、主に ISO 13849-2 の妥当性確認方法の概略について紹介する。SIL 要求適合については「機能安全活用テキスト」第 6 章を参照されたい。

７．２　妥当性確認の手順

ISO 13849-2 による妥当性確認とは、安全関連システムが ISO 13849-1 の要求に合致していることを実証することであり、図 7-1 に示すようなプロセスとなる。このプロセスは第 5 章図 5-1 における妥当性確認と PL の検証(安全機能検証)に該当し、分析もしくは分析と試験の組み合わせから構成される。

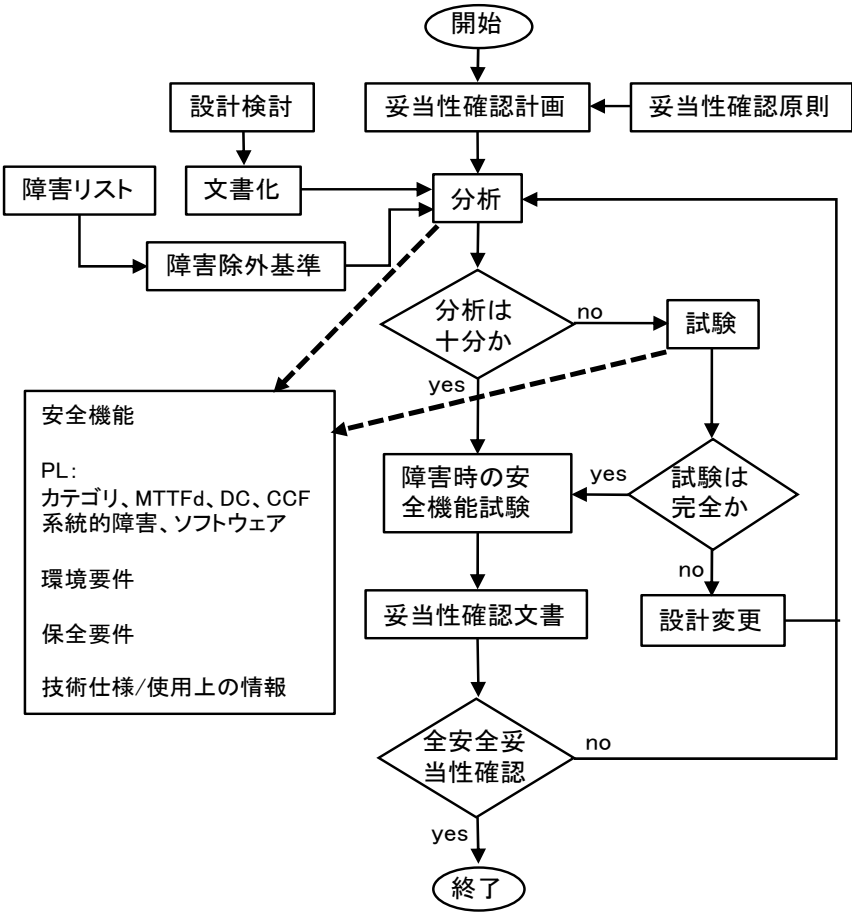


図 7-1　ISO 13849-2 による妥当性確認手順

(1)妥当性確認原則

妥当性確認は、安全関連システムの設計者と独立した人間(あるいは組織)が行うことが望ましいとされる。この独立性は求められる安全性能により変わるが、独立した人間は第三者試験を要求することを意味してはいない。また、障害への対処のため、分析は早期に設計と並行して開始することが望ましい。

(2) 妥当性確認計画

妥当性確認計画には、指定された安全機能とその安全性能の妥当性確認を実施するための要件を全て記載する必要があり、また、妥当性確認を実施するために用いる手段に関する情報も提供する必要がある。主な事項は以下の通り。

- 仕様書
- 使用環境条件
- 基本的安全原則
- 十分吟味された安全原則
- 十分吟味された構成部品
- 考慮すべき故障、故障除外
- 適用する分析・試験

なお、妥当性確認計画には妥当性確認文書も全て含まれる。

(3) 障害リスト

試験手順には、安全関連システムの障害時の挙動について考慮しなければならず、そのために長年の経験及び実績に基づく一般及び特定の障害リストが用意されている(ISO 13849-2 の付属書 A.5、B.5、C.5、D.5)。また、許容できる障害除外リストも記載されているが、これらは恒久的な故障のみ考慮されている。なお、障害の除外は全て十分な根拠に基づかねばならない。

(4) 文書化

妥当性確認のための情報として、主に次のような内容を文書として準備する。

- 安全機能・安全性能の仕様
- 図面類(機械、配線、技術データ等)
- 回路図(接続部含む)
- 回路の機能説明
- 安全関連の信号(タイミングチャート)
- 既に妥当性確認された構成部品の必要情報の記述
- 部品表(定格、故障率等を含む)
- 安全性能に固有の情報(PL 情報等)
- ソフトウェア関係の情報(ソフトウェアが使用されている場合)

なお、文書は、完全で内容的に矛盾なく、論理的に構成され、理解しやすく、検証可能なものでなければならない。

(5) 分析

安全機能に要求される特質の全てを実際に備えていることを示すため、次の情報を

証拠として提供する。

- 機械に関連して特定された危険源
- 信頼性
- システム構成
- システムの挙動に影響を与える定量化不可能で、定性的な側面
- 決定論的根拠（定性的な状況による、製造者の品質、故障率、使用経験など）

また、分析手法として演繹的なトップダウン方法(例えばFTA)、帰納的なボトムアップ方法(例えばFMEA)がある。

(6)試験

分析による妥当性確認が不十分な場合、規定した安全機能及び安全性能の達成度を実証するため、試験は論理的に計画し、実施されねばならない。試験実施前に作成すべき試験計画は以下を含む。

- 試験仕様
- 期待される試験結果
- 試験順序

また、追跡可能な方法で文書化する必要があり、試験記録は以下を含む。

- 試験者の名前
- 試験環境条件
- 試験手順と使用機器
- 試験結果

(7)安全機能の検証

実装された安全機能が、仕様書で要求される特性及び性能基準と完全に一致していることを検証する。そのため、安全関連出力が正しく、かつ仕様に従い論理的に入力によって決定されることを証明しなければならない。このプロセスは、全ての通常及び予見可能な非定常状態をカバーすることが望ましく、規定された安全機能は全ての操作モードで妥当性を確認しなければならない。

安全関連システムのPLの検証については、前章で説明済みであるが、以下の項目が実施される。

- カテゴリの検証
- MTTFd値の検証
- DC値の検証
- 共通原因故障/CCF対策の検証
- 決定論的原因障害対策の検証

なお、機能的要求事項が満たされたかを確認するために、一般的には次のような部

分試験が実施される。

- 機能テスト(冗長システムの各チャンネル)
- 拡張機能テストによる、通常とは異なる、予期しない、あるいは仕様書に記載されていない入力信号、操作手順における安全関連部の挙動に関するテスト
- ブラックボックステスト
- 性能テスト(機能的側面)

(8)環境要求の妥当性確認

安全関連システムの性能は、制御システムの環境条件に対して妥当性を確認しなければならない。この妥当性確認は分析及び試験(必要な場合)により、以下の項目を対象とする。

- 衝撃、振動、不純物の進入に対する予期できる機械的ストレス
- 機械的耐久性
- 電気定格及び電力供給
- 気候条件(温度及び湿度)
- 電磁両立性(イミュニティ)

(9)妥当性確認文書

検証と妥当性確認のプロセスを全て実行後、妥当性確認文書を発行する。この文書には、ハードウェアとソフトウェアの両方について、追跡可能な形で実行された分析と試験に関する情報の全てが含まれる。他の資料が追跡可能、かつ特定可能である場合には、それらを相互参照することが認められている。

７．３　文書化とファイル構成例

(1)機械の技術ファイルと IMS の技術ファイル構成イメージ

図 7-2 は、単体機械の技術ファイルの構成イメージと、IMS としての技術ファイルの構成イメージである。主な内容としては、単体機械の技術ファイルに加え、IMS として準備した機能の技術情報を加えることとなる。単体機械の技術ファイルが開示できない(されない)場合においては、単体機械が規格適合していることを証明する書類(第三者による証明書、レポート、自己宣言書)とそれらに付随するマニュアルなどで代用することは可能であると考えられる。

妥当性評価あるいは確認は、平たく言えば、機械機能が設計意図どおりであることの評価及び確認である。ここでは安全に関する部分の妥当性に関してのみ論じるが、機械の機能性においても同じ事が必要であり、ユーザが欲しがる仕様どおりであるかあるいは機械メーカが提示する仕様どおりであるかどうかということの証明と確認で

ある。安全においては、その多くは設計意図との一致と各要求事項を満たしているかどうかということになる。これは、実現した機械システムが、偶然そのようになったのではなく、意図した活動の結果そのようになっていると表明することとなる。これは、安全制御機能をそれぞれ作動させる機能試験や、ISO 13855 による設置位置計算を満たすことや、リスクアセスメントにより決定したリスク低減の実施や、リスクレベル(要求パフォーマンスレベル)に基づく制御回路設計など、関連する標準類を満たした設計である。また、協働ロボットの力などの制限に対しては、実際に挟まれなどの状況を再現して、その際の力あるいはエネルギーが、ISO TR 15066(JIS TS B0033)で定められた人体部位ごとの限度値を超えないことを確認したりする。

この表明は、CE マーキングなどで準備する技術ファイルの一部として試験データやPL 計算書などにより実施する。

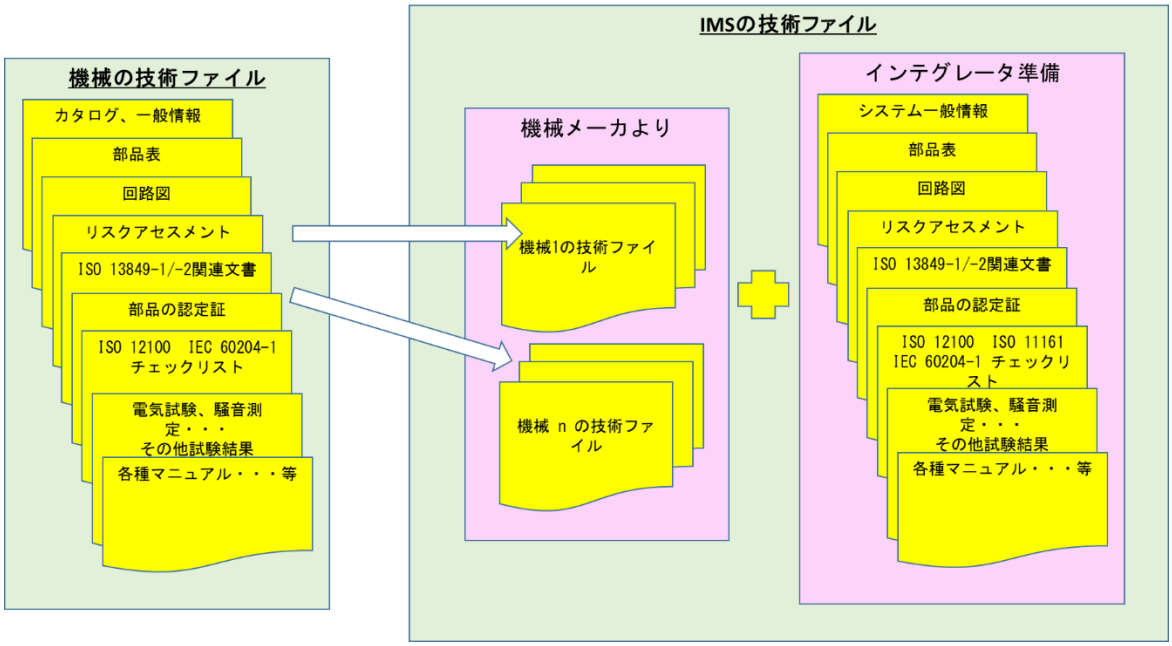


図 7-2 単体機械と IMS の技術ファイルイメージ

(2) IMS の技術ファイル例

図 7-3 は、IMS の技術ファイルの中身として必要なものをより具体的に例示しようとしたものである。IMS の一部として採用する機械は全て規格適合しているものとし、それらの設置条件はメーカ及び関連する技術標準に従うようにする。IMS として追加する機械機能、制御機能、ガード、安全機能、アクセス手段、人間工学原則の遵守などが、機械の使用方法と相容れるものであるのはもちろんのこと、それらにより機械の持つリスクレベルを増大する事や機械のもつ安全機能を損なう事がないようにする必要がある。あるいは、それらに対しては IMS として新たに安全戦略をたて、それに従ったリスク低減を実施していく必要がある。

ここまでに紹介してきた、機械のレイアウト図、ゾーン割り付け情報、作業者とゾーンの関わり、機械と人のゾーンまたぎ、安全機能マトリックス、各モードでの安全機能マトッリクス、作業ゾーン、ゾーンまたぎと制御範囲の関係性などの分析は IMS のリスクアセスメント文書の一部となる非常に重要な文書類となる。またこれらの文書類は、妥当性評価/確認においても活用できるものとなる。

妥当性評価/確認の多くは技術文書のレビューによりなされるが、制御範囲の正しさに関しては、実機でそれぞれの安全機器を作動させてどこで停止したか、意図したコンタクタ等で遮断されているのか、などを実際にテストして確認することがよく行われる。このときも、視覚的に分かりやすいように機械図面上で表したそれぞれの制御範囲の文書と電気図面あるいは制御回路図面があることで、確認もしくは実証が効率的に行えるようになる。

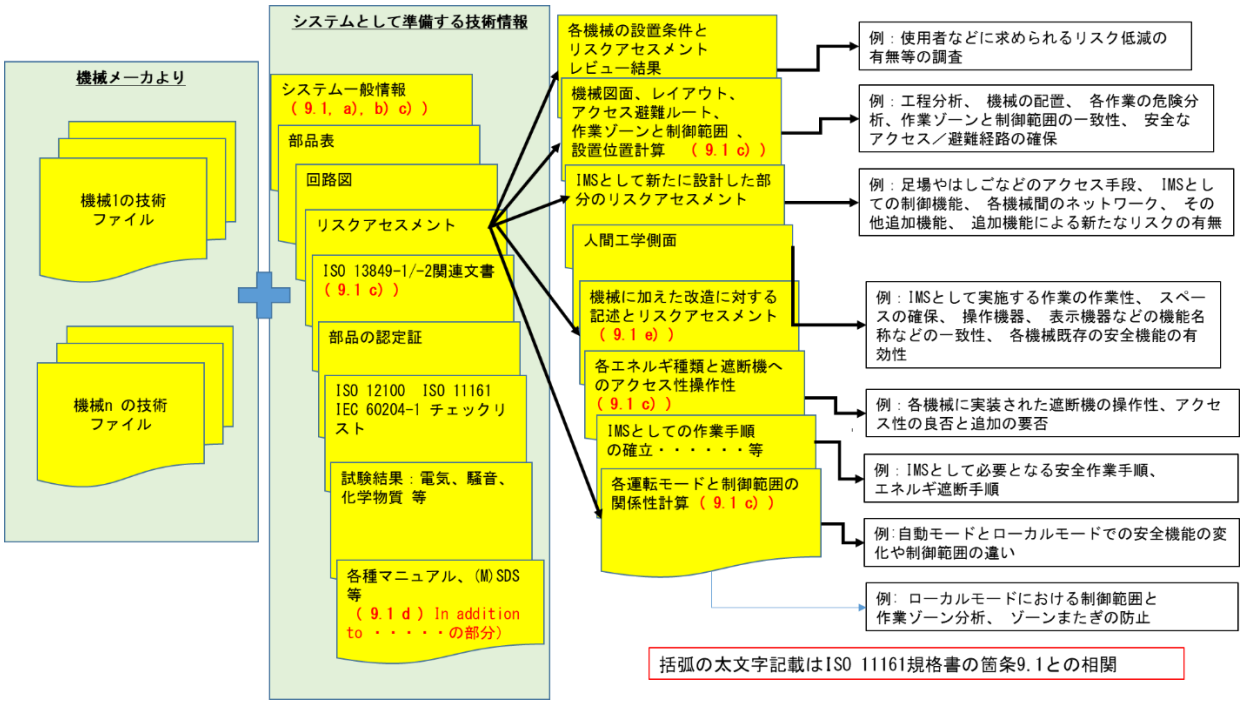


図 7-3 IMS の技術ファイルの例

第８章　使用上の情報

８．１　取扱説明書への記載事項

インテグレータが IMS の取扱説明書を作成する際は、以下の内容を漏れなく記述しなければならない。そして、必要な情報を入手し、それらを取扱指示書に盛り込むことが必要である。またこれらに限らず、リスクアセスメントの結果、使用上の情報として、使用者への提供が必要な情報を漏れなく記述する。

(1)　IMS の機能性

IMS の安全に関わる事項について、間接的に安全に関わる内容も含めて記述する。記述例として以下のことが挙げられる。

- 生産率（作業と生産効率を考慮する）
- IMS のレベル（自動化などの技術や生産工程など）
- 運転モード（手動、自動などをゾーン別、または IMS 全体）
- 構成する機械、複数の IMS の構成要件
- 制御機能（安全関連システムを含む）
- 制御領域（Spans of control）
- 検査要件

(2)　IMS の意図した使用と使用制限の記述

ア　下記ついての記述や図表

- IMS のレイアウト
- 設備の位置と配置
- タスク区域、及び関連した残留リスク
- 種々の制御安全機能及び保護装置の制御の範囲（例えば，保護装置のリセット，イネーブルデバイス，非常停止，制御ステーション，切離し手段）
- 保護装置に対して設置された安全距離と停止時間の詳細
- 作業タスクとタスクを行うための区域、位置及び経路
- 保護方策
- ユーティリティ
- 材料の流れ

例として非常停止押しボタンスイッチの作動範囲を示す図表を図 8-1 に示す。

イ　種々の構成機械と関連装置に関する文書

例えば、ロボット、ライトカーテンの取扱説明書

ウ　構成する機械に元からあった保護方策の修正

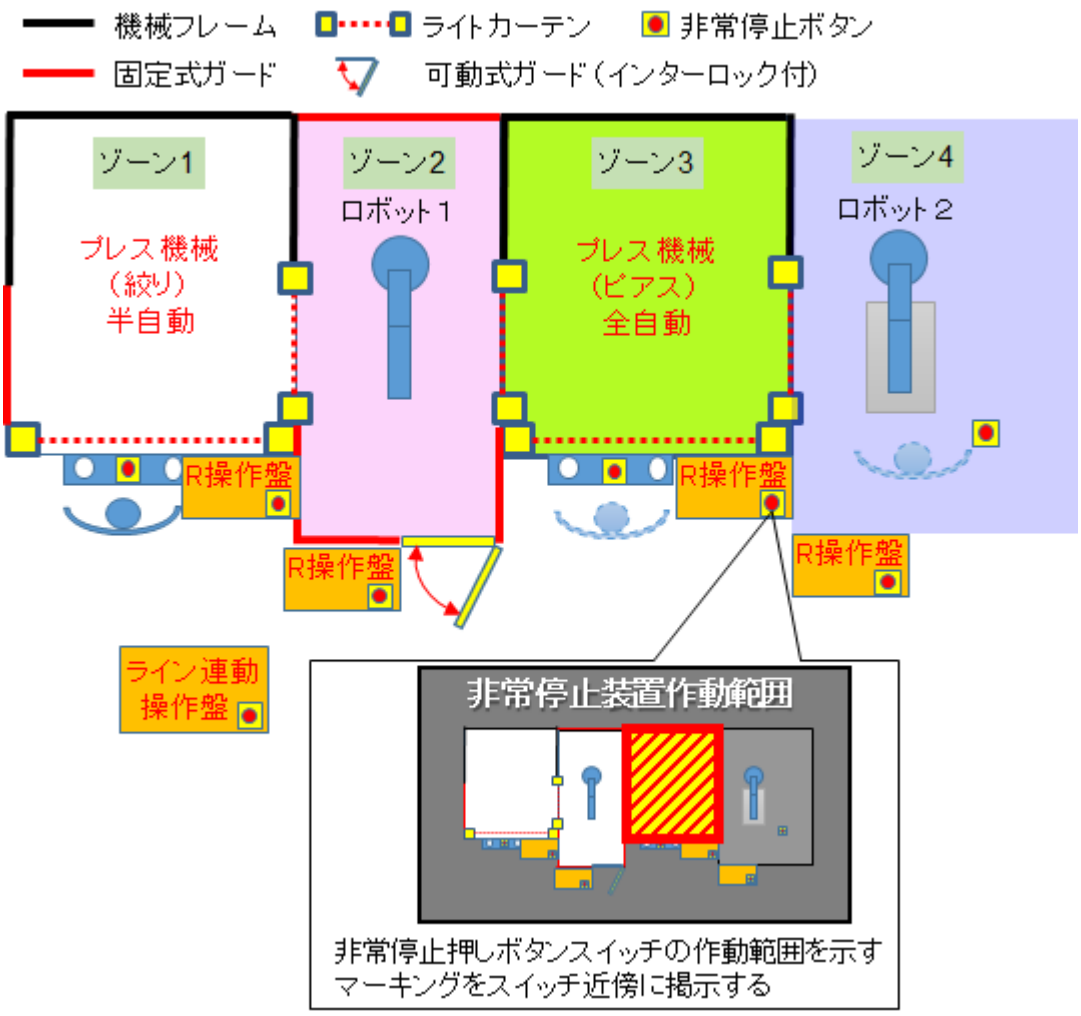


図 8-1　非常停止押しボタンスイッチの有効範囲

８．２　マーキング

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、その IMS で予期される寿命を通じて恒久的に判読可能であることが必要である。マーキングの内容は、JIS B 9700 の 6.4.4 項に従う。具体例として、以下のような事項が少なくとも必要となる。しかし、これらに限定せず、リスクアセスメントの結果、必要となった事項も記述し、場合によっては絵文字を用いる。

- 製造者の商号及び所在地、（該当する場合）公認の代理者
- IMS 名称
- シリーズ又は型式の名称（該当する場合）
- 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 IMS には、そ

れに応じた表示
- 安全に使用するための警告、注意情報

例：保護具着用の必要性、必要な保護具の種類・性能、定期点検個所

絵文字、記号及び色彩は、JIS B 6012-2、ISO 7000 を参照する。

【参照文献】

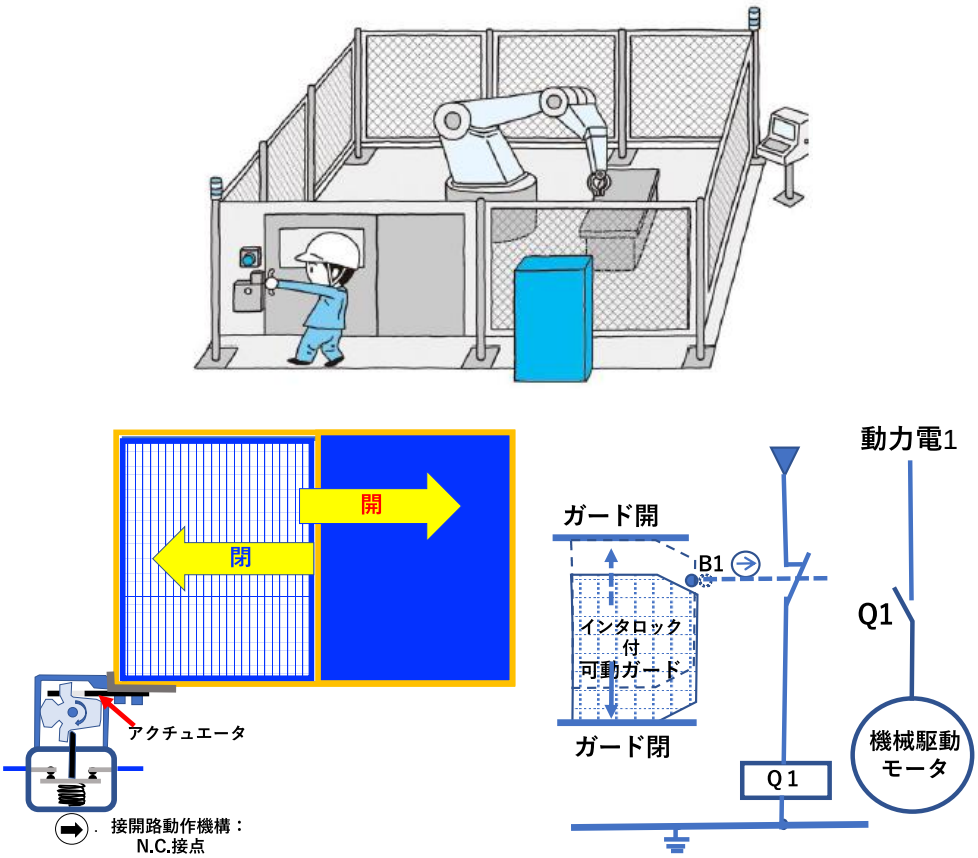
[1] ISO 11161:2007“Safety of machinery－Integrated manufacturing systems－Basic requirements”
[2] JIS B 9700:2013“機械類の安全性－設計のための一般原則－リスクアセスメント及びリスク低減”
[3] ISO 12100:2010“Safety of machinery－General principles for design－Risk assessment and risk reduction”

第９章　演習

９．１　演習―機能安全設計検証

本書で説明した統合生産システム(IMS)における代表的な保護方策を事例に、機能安全の設計の妥当性検証について演習を行う。

演習１：可動ガードのインタロック保護方策の機能安全設計の妥当性検証１



（「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）

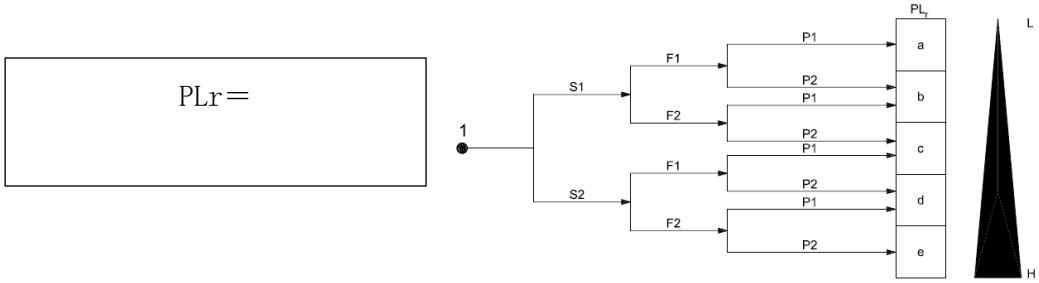
図 9-1　可動ガードのインタロックによる保護方策事例１

図 9-1 の事例は、第 4 章の IMS における可動ガードのインタロックと類似の事例を示した。以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

【演習１－１】

以下の条件で要求パフォーマンスレベル（PLr）を見積もる。

- 安全機能は、ガード開でリミットスイッチが切れ、コンタクタ Q1 の励磁電流を遮断し、モータの動力を停止（STO）させる。
- ガード内部のロボット等の機械設備で発生する危害は重大なものである。
- 通常ガードを開けて設備内に入る頻度は、20 分に１回で１回の作業時間は１分程度である。
- ガード内で危険事象が発生した場合の回避の可能性はないと考える。



【演習１-2】

安全関連システムの機能ブロック図とカテゴリを示し、次にリミットスイッチ B1 とコンタクタ Q1 の $MTTF_D$ と機能安全維持のための推奨交換周期を求め,最後に安全関連システムとして全体の $MTTF_D$ を示す。

リミットスイッチ B1 の B_{10} は、B_{10}＝100,000 回とする。コンタクタ Q1 の B_{10} は、B_{10}＝50,000 回とする。

また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日、(ガードの開閉頻度は 20 分に１回)とする。

機能ブロック図

安全関連システムのカテゴリ＝

B1 の $MTTF_D$＝

B1 の推奨交換周期＝

Q1 の $MTTF_D$＝

Q1 の推奨交換周期＝

安全関連システム全体の $MTTF_D$＝

【演習１-3】

【演習１-1】、【演習 1-2】の結果から ISO 13849-1 表 K.1 を使用して本安全関連システムの PL を求め、機能安全設計の妥当性の検証と理由を示す。

安全関連システムの PL＝

機能安全設計の妥当性の検証：

演習２：方策の機能安全設計の妥当性検証２

演習１と同等の PLr が要求される機械設備に図 9-2 システムの安全関連部の設計として採用した。以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

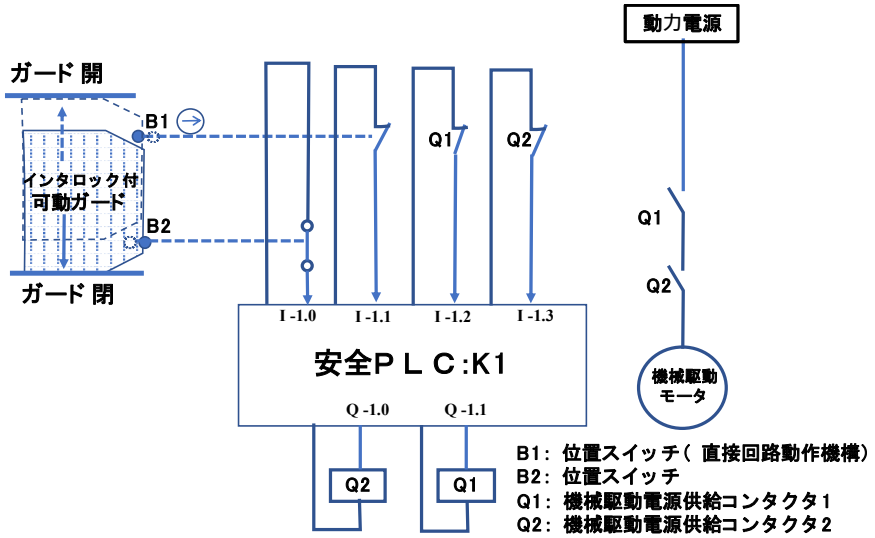


図 9-2 ガードのインタロックによる保護方策事例 2

【演習 2-1】

安全関連システムの機能ブロック図とカテゴリを示し、次にサブシステムとしてのリミットスイッチ B1・B2 の入力部とリンクドコンタクト構成のコンタクタ Q1・Q2 の出力部の $MTTF_D$ と機能安全維持のための推奨交換周期を求める。

図 9-2 に示した方策は、リミットスイッチ B1・B2 の B_{10} は、B_{10}＝100,000 回、コンタクタ Q1・Q2 の B_{10} は、B_{10}＝50,000 回とする。安全 PLC(K1)は、E/E/PE として SIL3(PFH=2.03x10^{-8}/h)の情報をメーカより入手している。

また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日、ガードの開閉頻度は 20 分に 1 回とする。

機能ブロック図 安全関連システムカテゴリ＝

入力部の $MTTF_D$＝
B1・B2 の推奨交換周期＝

出力部の $MTTF_D$＝
Q1・Q2 の推奨交換周期＝

【演習 2-2】

安全関連システムの入力部は、出力部のそれぞれの診断範囲は、ISO 13849 -2 より 99%とした時の入力部と出力部の合成 $MTTF_D$ と平均診断範囲を求める。

入力部と出力部の全体の $MTTF_D$＝
入力部と出力部の全体の平均診断範囲＝

【演習 2-3】

共通原因故障に対する考慮は、満足しているとした時、【演習 2-2】の結果より安全関連システムの入力部・出力部全体の PFH_D を ISO 13849-1 の表 K.1 より求める。次に安全 PLC(K1)の PFH も考慮してシステム全体の PHF_D とパフォーマンスレベルを求め、機能安全設計の妥当性の検証と理由を示す。

入力部と出力部の全体の PFH_D＝
安全関連システム全体の PFH_D＝
安全関連システム全体の PL=
機能安全設計の妥当性の検証：

演習３：ライトカーテンによる保護方策の機能安全設計の妥当性検証

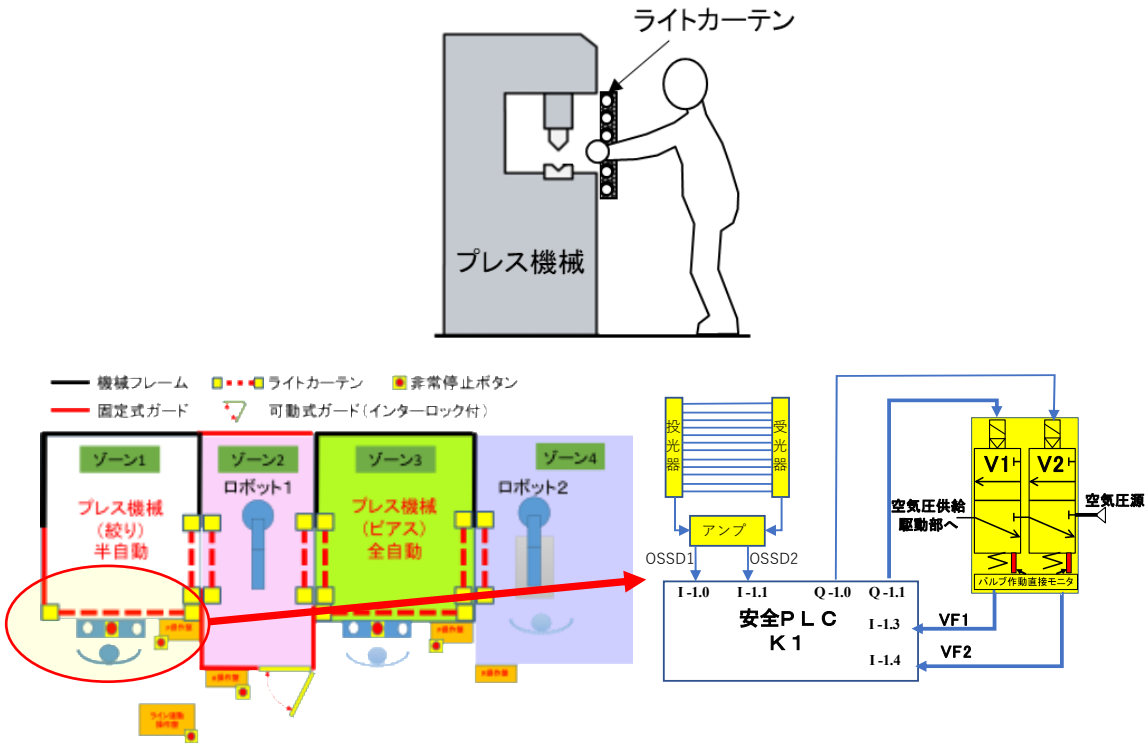


図 9-3　ライトカーテンの設置とプレス機械のライトカーテンによる保護方策事例

図 9-3 は、手で材料の供給を行うプレス機械に対する保護装置としてライトカーテンを適用した事例である。ライトカーテンは、type-4 のライトカーテンで OSSD1/OSSD2 の安全出力信号を持ち、安全 PLC は、プレス制御に関する SIL3 の安全機能を有した PLC である。また、ダブルバルブ（V1、V2）は、バルブのスプールを直接監視できるモニタ（VF1、VF2）を有している。

生産作業は、10 秒に 1 回で生産材料を手でプレス内へ供給する。また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日の作業を行う。表 9-1 には、各機器の安全仕様を示す。安全仕様を確認して以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

表 9-１　安全機器の PL 関連パラメータ

安全機器	DCavg	B_{10D}[回]	PFH[1/時間]	SIL
ライトカーテン	99%	—	1.50×10^{-8}	3
安全ＰＬＣ	99%	—	6.44×10^{-9}	3
ダブルバルブ	99%	各　20,000,000		

【演習 3-1】

このプレス機械の保護方策に使用しているライトカーテンの PLr を示す。

PLr＝

【演習 3-2】

このプレス機械の保護方策の安全関連システムの機能ブロックとカテゴリを示す。

機能ブロック図

安全関連システムのカテゴリ＝

【演習 3-3】

ダブルバルブの $MTTF_D$ と推奨交換周期を求める。

ダブルバルブの $MTTF_D$＝

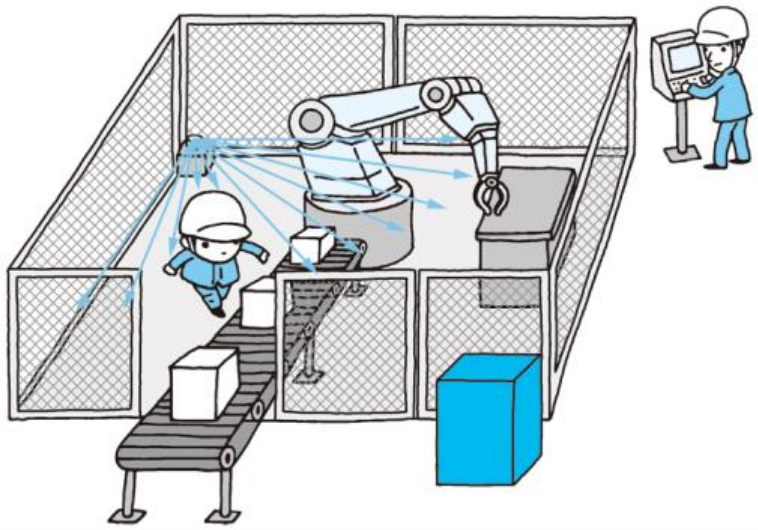
推奨交換周期＝

【演習 3-4】

共通原因故障に対する考慮は、満足しているとした時、【演習 3-1～3】の結果より安全関連制御システムの出力部全体の PFH_D を ISO 13849-1 の表 K.1 より求める。次に安全 PLC(K1)の PFH も考慮してシステム全体の PHF_D とパフォーマンスレベルを求め、機能安全設計の妥当性の検証と理由を示す。

出力部の全体の PFH_D＝ **安全関連システム全体の PFH_D＝** **安全関連システム全体の PL=** **機能安全設計の妥当性の検証：**

演習４：レーザースキャナによる保護方策に対する機能安全設計の妥当性検証



（「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）

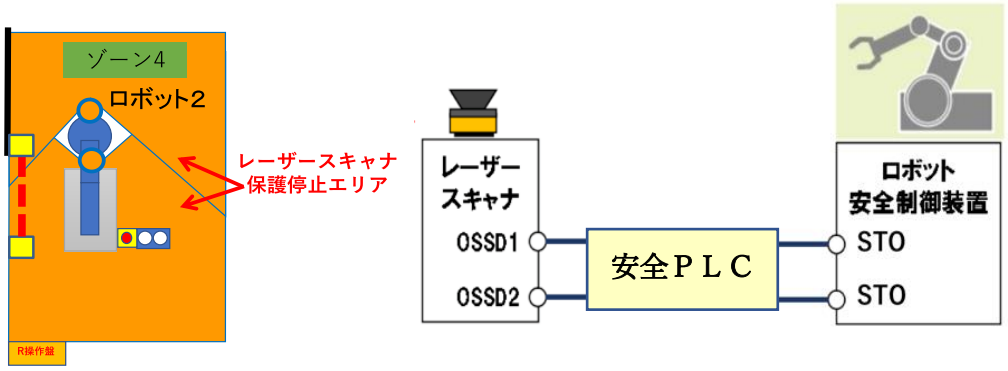


図 9-4　レーザースキャナ設置とレーザースキャナによる保護方策事例

図 9-4 は、ロボットの可動領域に人が侵入した場合の保護装置としてレーザースキャナを適用した事例である。図 9-4 のロボットのリスク低減方策として、以下の方策を採用する。

- ロボットアームの可動範囲に対して保護停止できる範囲でレーザースキャナにより作業者の進入を検知する。
- 速度制御範囲に作業者が入ると、ロボットは、停止カテゴリ 1（IEC 60204-1）で保護停止（SS1）する。
- このリスク低減方策は、ISO 13849-1 の図 A.1 のリスクで見積もると S2/F1/P2 の PLr=d が求められる。

表 9-2 には、各機器の安全仕様を示す。安全仕様を確認して以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

表 9-2　安全機器の PL 関連パラメータ

安全機器	DCavg	PFH[1/時間]	SIL
レーザースキャナ	97%	1.03×10^{-7}	2
安全ＰＬＣ	99%	6.44×10^{-9}	3
ロボット:SS１	92%	3.84×10^{-8}	3

【演習４-1】

保護停止システム全体の PHF_D とパフォーマンスレベルを求め、機能安全設計の妥当性の検証と理由を示す。

安全関連システム全体の PFH_D＝
安全関連システム全体の PL=
機能安全設計の妥当性の検証：

演習５：非常停止装置による付加保護方策に対する機能安全設計の妥当性検証

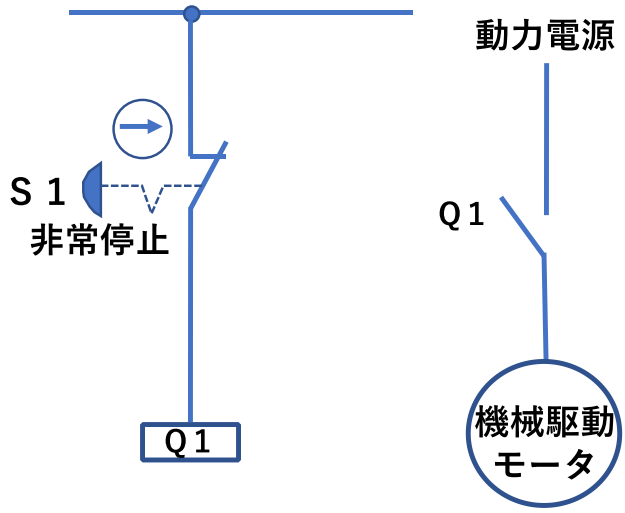


図 9-5　非常停止ボタンによるモータ動力遮断の付加保護方策事例

図 9-5 は、非常停止ボタンで直接コンタクタ励磁回路遮断しモータ動力を遮断する回路事例である。非常停止ボタンの平均操作頻度は、30 分毎に 1 回である。また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日の作業を行う。表 9-3 には、各機器の B_{10} 仕様を示す。非常停止機能の制御システムの安全関連部としての**要求安全性能は、PLr=c** である。B_{10} 仕様を確認して以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

表 9-3　安全機器の PL 関連パラメータ

安全機器	B_{10}[回]
非常停止ボタン S1	500,000
コンタクタ Q1	1,000,000

【演習 5-1】

以下の設問に従って非常停止ボタン S1 とコンタクタ Q1 のそれぞれの $MTTF_D$ および制御システム全体の $MTTF_D$ を求める。

図 9-5 の制御システムのカテゴリ＝

機能ブロック図：

安全機能（非常停止機能）の年間作動回数　n_{op}=

非常停止ボタン S1 の B_{10D}=

コンタクタ Q1 の B_{10D}=

非常停止ボタン S1 の T_{10D}(S1)=

MTTFD(S1)=

【演習 5-2】

制御システム全体の PL と機能安全設計の妥当性の検証と理由を示す。

【演習 5-1】の結果：

PL=,　　PFH_D＝

機能安全設計の妥当性の検証：

【演習に使用する参考資料】ISO 13849-1:2015 表 K.1

	危険側故障の平均確率:PFH_D（1/h）及び対応のパフォーマンスレベル PL						
各チャネルの MTTFD（年）	カテゴリ B PL DCavg＝“なし”	カテゴリ 1 PL DCavg＝“なし”	カテゴリ 2 PL DCavg＝”低”	カテゴリ 2 PL DCavg＝”中”	カテゴリ 3 PL DCavg＝”低”	カテゴリ 3 PL DCavg＝”中”	カテゴリ 4 PL DCavg＝”高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b	
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b	
3.9	2.93×10^{-5} a		1.95×10^{-5} a	1.48×10^{-5} a	9.37×10^{-6} b	4.40×10^{-6} b	
4.3	2.65×10^{-5} a		1.76×10^{-5} a	1.33×10^{-5} a	8.39×10^{-6} b	3.89×10^{-6} b	
4.7	2.43×10^{-5} a		1.60×10^{-5} a	1.20×10^{-5} a	7.58×10^{-6} b	3.48×10^{-6} b	
5.1	2.24×10^{-5} a		1.47×10^{-5} a	1.10×10^{-5} a	6.91×10^{-6} b	3.15×10^{-6} b	
5.6	2.04×10^{-5} a		1.33×10^{-5} a	9.87×10^{-6} b	6.21×10^{-6} b	2.80×10^{-6} c	
6.2	1.84×10^{-5} a		1.19×10^{-5} a	8.80×10^{-6} b	5.53×10^{-6} b	2.47×10^{-6} c	
6.8	1.68×10^{-5} a		1.08×10^{-5} a	7.93×10^{-6} b	4.98×10^{-6} b	2.20×10^{-6} c	
7.5	1.52×10^{-5} a		9.75×10^{-6} b	7.10×10^{-6} b	4.45×10^{-6} b	1.95×10^{-6} c	
8.2	1.39×10^{-5} a		8.87×10^{-6} b	6.43×10^{-6} b	4.02×10^{-6} b	1.74×10^{-6} c	
9.1	1.25×10^{-5} a		7.94×10^{-6} b	5.71×10^{-6} b	3.57×10^{-6} b	1.53×10^{-6} c	
10	1.14×10^{-5} a		7.18×10^{-6} b	5.14×10^{-6} b	3.21×10^{-6} b	1.36×10^{-6} c	
11	1.04×10^{-5} a		6.44×10^{-6} b	4.53×10^{-6} b	2.81×10^{-6} c	1.18×10^{-6} c	
12	9.51×10^{-6} b		5.84×10^{-6} b	4.04×10^{-6} b	2.49×10^{-6} c	1.04×10^{-6} c	
13	8.78×10^{-6} b		5.33×10^{-6} b	3.64×10^{-6} b	2.23×10^{-6} c	9.21×10^{-7} d	
15	7.61×10^{-6} b		4.53×10^{-6} b	3.01×10^{-6} b	1.82×10^{-6} c	7.44×10^{-7} d	
16	7.13×10^{-6} b		4.21×10^{-6} b	2.77×10^{-6} c	1.67×10^{-6} c	6.76×10^{-7} d	
18	6.34×10^{-6} b		3.68×10^{-6} b	2.37×10^{-6} c	1.41×10^{-6} c	5.67×10^{-7} d	
20	5.71×10^{-6} b		3.26×10^{-6} b	2.06×10^{-6} c	1.22×10^{-6} c	4.85×10^{-7} d	
22	5.19×10^{-6} b		2.93×10^{-6} c	1.82×10^{-6} c	1.07×10^{-6} c	4.21×10^{-7} d	
24	4.76×10^{-6} b		2.65×10^{-6} c	1.62×10^{-6} c	9.47×10^{-7} d	3.70×10^{-7} d	
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82		1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91		1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.94×10^{-8} e	2.74×10^{-8} e
100		1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e
110							2.23×10^{-8} e
120							$2{,}03\times10^{-8}$ e
130							$1{,}87\times10^{-8}$ e
150							$1{,}61\times10^{-8}$ e
160							$1{,}50\times10^{-8}$ e
180							$1{,}33\times10^{-8}$ e

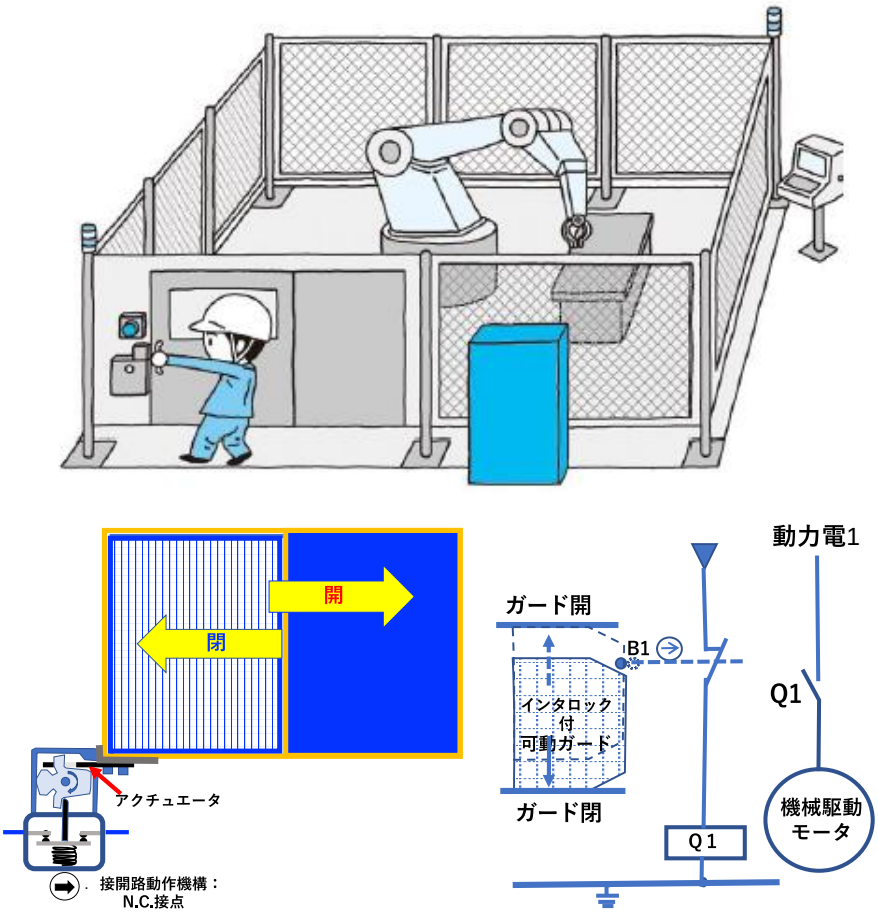
以下、カテゴリ 4 の 2500 年までの「PFH_D・PL」テーブルは省略

付録

演習解答例

演習１解答：

可動ガードのインタロック保護方策の機能安全設計の妥当性検証１



（「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）

図 9-1　可動ガードのインタロックによる保護方策事例１

図 9-1 の事例は、第 4 章の IMS における可動ガードのインタロックと類似の事例を示した。以下の設問に対して演習を行い設計の妥当性を評価し検証を

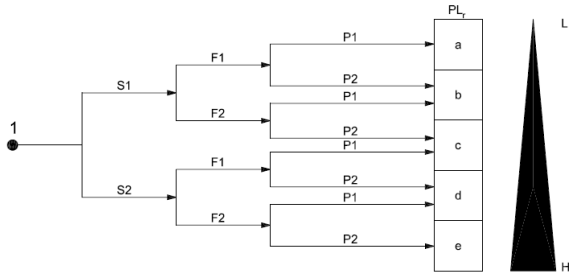
【演習 1-1】

以下の条件で要求パフォーマンスレベル（PLr）を見積もる。

- 安全機能は、ガード開でリミットスイッチが切れ、コンタクタ Q1 の励磁電流を遮断し、モータの動力を停止（STO）させる。
- ガード内部のロボット等の機械設備で発生する危害は重大なものである。

- 通常ガードを開けて設備内に入る頻度は、20 分に 1 回で 1 回の作業時間は 1 分程度である。
- ガード内で危険事象が発生した場合の回避の可能性はないと考える。

PLr＝d
(S2・F1・P2)



【演習 1-2】

安全関連システムの機能ブロック図とカテゴリを示し、次にリミットスイッチ B1 とコンタクタ Q1 の $MTTF_D$ と機能安全維持のための推奨交換周期を求め，最後に安全関連システムとして全体の $MTTF_D$ を示す。

リミットスイッチ B1 の B_{10} は、B_{10}＝100,000 回とする。コンタクタ Q1 の B_{10} は、B_{10}＝50,000 回とする。

また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日、(ガードの開閉頻度は 20 分に 1 回) とする。

機能ブロック図

安全関連システムのカテゴリ＝1

B1 の $MTTF_D$＝200,000/(18,000x0.1)=111 年

B1 の推奨交換周期＝11 年

年間のガード（安全機能）作動回数　n_{op}=20x300x60/20=18,000 回

B_{10D}=100,000x2=200,000　T_{10D}=200,000/18,000=11.1 年

Q1 の $MTTF_D$＝1,000,000/(18,000x0.1)=55 年

Q1 の推奨交換周期＝5 年

B_{10D}=50,000x2=100,000　T_{10D}=100,000/18,000=5.6 年

安全関連システム全体の $MTTF_D$＝55x111/(55+111)=37 年

1/ $MTTF_D$=1/55+1/111=(55+111)/(55x111)

【演習 1-3】

【演習 1-1】、【演習 1-2】の結果から ISO 13849-1 表 K.1 を使用して本安全関連システムの PL を求め、機能安全設計の妥当性の検証と理由を示す。

安全関連システムの PL＝ b

機能安全設計の妥当性の検証：

PLr=d ＞ PL=b より PLr を満足していない。

【補足】カテゴリ B・1 は、機器単体の性能評価であり、DCavg、CCF の考慮外

表 K.1 内に $MTTF_D$ 値がない場合は、表内の小さい方の値を選択する。（37 年⇒36 年）

【演習に使用する参考資料】ISO 13849-1:2015 表 K.1

危険側故障の平均確率:PFH_D（1/h）及び対応のパフォーマンスレベル PL

各チャネルの $MTTF_D$（年）	カテゴリ B PL DC_{avg}＝“なし”	カテゴリ 1 PL DC_{avg}＝“なし”	カテゴリ 2 PL DC_{avg}＝” 低”	カテゴリ 2 PL DC_{avg}＝” 中”	カテゴリ 3 PL DC_{avg}＝” 低”	カテゴリ 3 PL DC_{avg}＝” 中”	カテゴリ 4 PL DC_{avg}＝” 高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b	
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b	
3.9	2.93×10^{-5} a		1.95×10^{-5} a	1.48×10^{-5} a	9.37×10^{-6} b	4.40×10^{-6} b	
4.3	2.65×10^{-5} a		1.76×10^{-5} a	1.33×10^{-5} a	8.39×10^{-6} b	3.89×10^{-6} b	
4.7	2.43×10^{-5} a		1.60×10^{-5} a	1.20×10^{-5} a	7.58×10^{-6} b	3.48×10^{-6} b	
5.1	2.24×10^{-5} a		1.47×10^{-5} a	1.10×10^{-5} a	6.91×10^{-6} b	3.15×10^{-6} b	
5.6	2.04×10^{-5} a		1.33×10^{-5} a	9.87×10^{-6} b	6.21×10^{-6} b	2.80×10^{-6} c	
6.2	1.84×10^{-5} a		1.19×10^{-5} a	8.80×10^{-6} b	5.53×10^{-6} b	2.47×10^{-6} c	
6.8	1.68×10^{-5} a		1.08×10^{-5} a	7.93×10^{-6} b	4.98×10^{-6} b	2.20×10^{-6} c	
7.5	1.52×10^{-5} a		9.75×10^{-6} b	7.10×10^{-6} b	4.45×10^{-6} b	1.95×10^{-6} c	
8.2	1.39×10^{-5} a		8.87×10^{-6} b	6.43×10^{-6} b	4.02×10^{-6} b	1.74×10^{-6} c	
9.1	1.25×10^{-5} a		7.94×10^{-6} b	5.71×10^{-6} b	3.57×10^{-6} b	1.53×10^{-6} c	
10	1.14×10^{-5} a		7.18×10^{-6} b	5.14×10^{-6} b	3.21×10^{-6} b	1.36×10^{-6} c	
11	1.04×10^{-5} a		6.44×10^{-6} b	4.53×10^{-6} b	2.81×10^{-6} c	1.18×10^{-6} c	
12	9.51×10^{-6} b		5.84×10^{-6} b	4.04×10^{-6} b	2.49×10^{-6} c	1.04×10^{-6} c	
13	8.78×10^{-6} b		5.33×10^{-6} b	3.64×10^{-6} b	2.23×10^{-6} c	9.21×10^{-7} d	
15	7.61×10^{-6} b		4.53×10^{-6} b	3.01×10^{-6} b	1.82×10^{-6} c	7.44×10^{-7} d	
16	7.13×10^{-6} b		4.21×10^{-6} b	2.77×10^{-6} c	1.67×10^{-6} c	6.76×10^{-7} d	
18	6.34×10^{-6} b		3.68×10^{-6} b	2.37×10^{-6} c	1.41×10^{-6} c	5.67×10^{-7} d	
20	5.71×10^{-6} b		3.26×10^{-6} b	2.06×10^{-6} c	1.22×10^{-6} c	4.85×10^{-7} d	
22	5.19×10^{-6} b		2.93×10^{-6} c	1.82×10^{-6} c	1.07×10^{-6} c	4.21×10^{-7} d	
24	4.76×10^{-6} b		2.65×10^{-6} c	1.62×10^{-6} c	9.47×10^{-7} d	3.70×10^{-7} d	
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e

以下、$MTTF_D$=47 年を超える「PFH_D・PL」テーブルは省略

演習２解答：

方策の機能安全設計の妥当性検証２

演習１と同等の PLr が要求される機械設備に図 9-2 システムの安全関連部の設計として採用した。以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

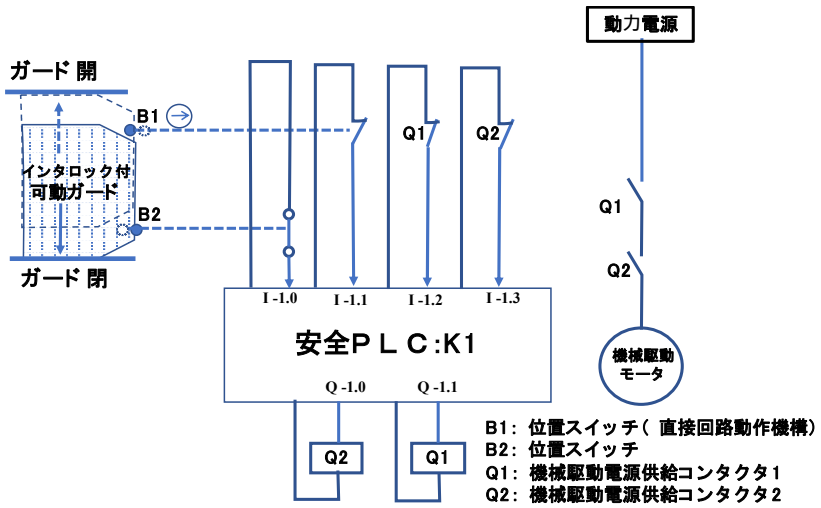


図 9-2 ガードのインタロックによる保護方策事例 2

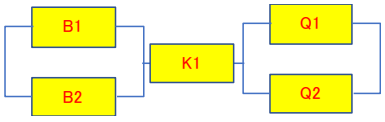
【演習 2-1】

安全関連システムの機能ブロック図とカテゴリを示し、次にサブシステムとしてのリミットスイッチ B1・B2 の入力部とリンクドコンタクト構成のコンタクタ Q1・Q2 の出力部の $MTTF_D$ と機能安全維持のための推奨交換周期を求める。

図 9-2 に示した方策は、リミットスイッチ B1・B2 の B_{10} は、B_{10}＝100,000 回、コンタクタ Q1・Q2 の B_{10} は、B_{10}＝50,000 回とする。安全 PLC（K1）は、E/E/PE として SIL3（PFH=2.03x10^{-8}/h）の情報をメーカより入手している。

また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日、ガードの開閉頻度は 20 分に 1 回とする。

機能ブロック図



安全関連システムカテゴリ＝3 以上（カテゴリ 3 または 4：DC の評価による）

入力部の $MTTF_D$＝2/3x(111+111-1/(1/111+1/111))=111 年

B1・B2 の推奨交換周期＝11 年

年間のガード（安全機能）作動回数　Nop=20x300x60/20=18,000 回

B_{10D}=100,000x2=200,000　T_{10D}=200,000/18,000=11 年　$MTTF_D$＝111 年

出力部の $MTTF_D$＝55 年

Q1・Q2 の推奨交換周期＝5 年

Q_{10D}=50,000x2=100,000　T_{10D}=100,000/18,000=5.5 年

【演習 2-2】

安全関連システムの入力部は、出力部のそれぞれの診断範囲は、ISO 13849 -2 より 99%とした時の入力部と出力部の合成 $MTTF_D$ と平均診断範囲を求める。

入力部と出力部の全体の $MTTF_D$＝55x111/(55+111)=36.8 年

入力部と出力部の全体の平均診断範囲＝99%

【演習 2-3】

共通原因故障に対する考慮は、満足しているとした時、【演習 2-2】の結果より安全関連システムの入力部・出力部全体の PFH_D を ISO 13849-1 の表 K.1 より求める。次に安全 PLC(K1)の PFH も考慮してシステム全体の PHF_D とパフォーマンスレベルを求め、機能安全設計の妥当性の検証と理由を示す。

入力部と出力部の全体の PFH_D＝約 $7.11x10^{-8}$/h

安全関連システム全体の PFH_D＝約 $7.11x10^{-8}$ +$2.03x10^{-8}$＝9.13 $x10^{-8}$/h=PLe

安全関連システム全体の PL=e

機能安全設計の妥当性の検証：PLr=d ＜ PL=e より機能安全設計は、PLr を満足する。

【参考】

入力部・出力部それぞれをサブシステムとして個別に ISO 13849-1 表 K.1 から PFH_D を選択、合算した場合もほぼ同じ結果して算出される。

入力部 $MTTF_D$=111 年、　DCavg=99% → PFH_D=約 $2.23x10^{-8}$/h

出力部 $MTTF_D$=55 年、　DCavg=99% → PFH_D=約 $4.73x10^{-8}$/h

安全 PLC(K1)： $PFH=2.03x10^{-8}$/h

全体の PFH_D=約(2.23+4.73+2.03) $x10^{-8}$/h=約 $8.99x10^{-8}$/h=PLe

【演習に使用する参考資料】ISO 13849-1:2015 表 K.1

	危険側故障の平均確率:PFH_D（1/h）及び対応のパフォーマンスレベル PL						
各チャネルの $MTTF_D$（年）	カテゴリ B PL DC_{avg}=“なし”	カテゴリ 1 PL DC_{avg}=“なし”	カテゴリ 2 PL DC_{avg}=”低”	カテゴリ 2 PL DC_{avg}=”中”	カテゴリ 3 PL DC_{avg}=”低”	カテゴリ 3 PL DC_{avg}=”中”	カテゴリ 4 PL DC_{avg}=”高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b	
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b	
3.9	2.93×10^{-5} a		1.95×10^{-5} a	1.48×10^{-5} a	9.37×10^{-6} b	4.40×10^{-6} b	
4.3	2.65×10^{-5} a		1.76×10^{-5} a	1.33×10^{-5} a	8.39×10^{-6} b	3.89×10^{-6} b	
4.7	2.43×10^{-5} a		1.60×10^{-5} a	1.20×10^{-5} a	7.58×10^{-6} b	3.48×10^{-6} b	
5.1	2.24×10^{-5} a		1.47×10^{-5} a	1.10×10^{-5} a	6.91×10^{-6} b	3.15×10^{-6} b	
5.6	2.04×10^{-5} a		1.33×10^{-5} a	9.87×10^{-6} b	6.21×10^{-6} b	2.80×10^{-6} c	
6.2	1.84×10^{-5} a		1.19×10^{-5} a	8.80×10^{-6} b	5.53×10^{-6} b	2.47×10^{-6} c	
6.8	1.68×10^{-5} a		1.08×10^{-5} a	7.93×10^{-6} b	4.98×10^{-6} b	2.20×10^{-6} c	
7.5	1.52×10^{-5} a		9.75×10^{-6} b	7.10×10^{-6} b	4.45×10^{-6} b	1.95×10^{-6} c	
8.2	1.39×10^{-5} a		8.87×10^{-6} b	6.43×10^{-6} b	4.02×10^{-6} b	1.74×10^{-6} c	
9.1	1.25×10^{-5} a		7.94×10^{-6} b	5.71×10^{-6} b	3.57×10^{-6} b	1.53×10^{-6} c	
10	1.14×10^{-5} a		7.18×10^{-6} b	5.14×10^{-6} b	3.21×10^{-6} b	1.36×10^{-6} c	
11	1.04×10^{-5} a		6.44×10^{-6} b	4.53×10^{-6} b	2.81×10^{-6} c	1.18×10^{-6} c	
12	9.51×10^{-6} b		5.84×10^{-6} b	4.04×10^{-6} b	2.49×10^{-6} c	1.04×10^{-6} c	
13	8.78×10^{-6} b		5.33×10^{-6} b	3.64×10^{-6} b	2.23×10^{-6} c	9.21×10^{-7} d	
15	7.61×10^{-6} b		4.53×10^{-6} b	3.01×10^{-6} b	1.82×10^{-6} c	7.44×10^{-7} d	
16	7.13×10^{-6} b		4.21×10^{-6} b	2.77×10^{-6} c	1.67×10^{-6} c	6.76×10^{-7} d	
18	6.34×10^{-6} b		3.68×10^{-6} b	2.37×10^{-6} c	1.41×10^{-6} c	5.67×10^{-7} d	
20	5.71×10^{-6} b		3.26×10^{-6} b	2.06×10^{-6} c	1.22×10^{-6} c	4.85×10^{-7} d	
22	5.19×10^{-6} b		2.93×10^{-6} c	1.82×10^{-6} c	1.07×10^{-6} c	4.21×10^{-7} d	
24	4.76×10^{-6} b		2.65×10^{-6} c	1.62×10^{-6} c	9.47×10^{-7} d	3.70×10^{-7} d	
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82		1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91		1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.94×10^{-8} e	2.74×10^{-8} e
100		1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e
110							2.23×10^{-8} e
120							$2,03\times10^{-8}$ e
130							$1,87\times10^{-8}$ e
150							$1,61\times10^{-8}$ e
160							$1,50\times10^{-8}$ e
180							$1,33\times10^{-8}$ e

以下、カテゴリ 4 の 2500 年までの「PFH_D・PL」テーブルは省略

演習３解答：

ライトカーテンによる保護方策の機能安全設計の妥当性検証

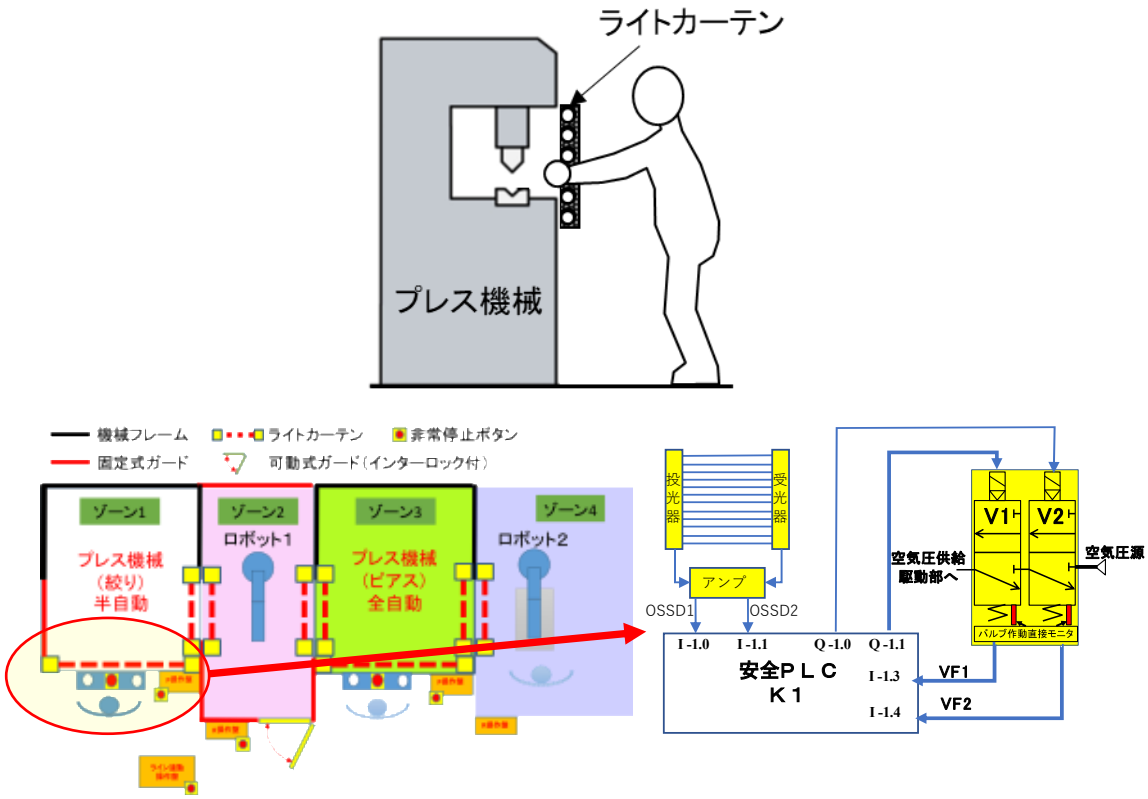


図 9-3　ライトカーテン設置・とプレス機械のライトカーテンによる保護方策事例

図 9-3 は、手で材料の供給を行うプレス機械に対する保護装置として光線式安全装置を適用した事例である。ライトカーテンは、type-4 のライトカーテンで OSSD1/OSSD2 の安全出力信号を持ち、安全 PLC は、プレス制御に関する SIL3 の安全機能を有した PLC である。また、ダブルバルブ（V1、V2）は、バルブのスプールを直接監視できるモニタ（VF1、VF2）を有している。

生産作業は、10 秒に 1 回で生産材料を手でプレス内へ供給する。また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日の作業を行う。表 9-1 には、各機器の安全仕様を示す。安全仕様を確認して以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

表 9-１　安全機器の PL 関連パラメータ

安全機器	DCavg	B_{10D}[回]	PFH[1/時間]	SIL
ライトカーテン	99%	—	1.50×10^{-8}	3
安全ＰＬＣ	99%	—	6.44×10^{-9}	3
ダブルバルブ	99%	各　20,000,000		

【演習 3-1】

このプレス機械の保護方策に使用している光線式安全装置の PLr を示す。

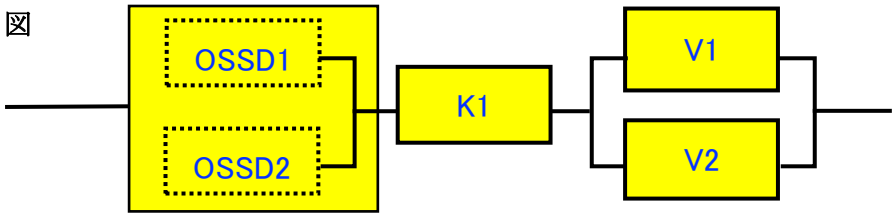
PLr＝e

(S2・F2・P2)

【演習 3-2】

このプレス機械の保護方策の安全関連システムの機能ブロックとカテゴリを示す。

機能ブロック図



安全関連システムのカテゴリ＝3 以上（カテゴリ 3 または 4：DC の評価による）

【演習 3-3】

ダブルバルブの $MTTF_D$ と推奨交換周期を求める。

ダブルバルブの $MTTF_D$＝92 年

推奨交換周期＝9 年

年間の光線式安全装置（安全機能）の作動回数　n_{op}=20x300x(60x6)=2,160,000 回

各バルブの T_{10D}=20,000,000/2,160,000=9.2 年

$MTTF_D$＝92 年→同一性能の冗長化→$MTTF_D$＝92 年

【演習 3-4】

共通原因故障に対する考慮は、満足しているとした時、【演習 3-1～3】の結果より安全関連システムの出力部全体の PFH_D を ISO 13849-1 の表 K.1 より求める。次に安全 PLC(K1)の PFH も考慮してシステム全体の PHF_D とパフォーマンスレベルを求め、機能安全設計の妥当性の検証と理由を示す。

出力部の全体の PFH_D＝約 $2.74x10^{-8}$/h

安全関連システム全体の PFH_D＝$1.50x10^{-8}$ +$6.44x10^{-9}$+約 $2.744x10^{-8}$＝$4.9\ x10^{-8}$/h

安全関連システム全体の PL=e

機能安全設計の妥当性の検証：

(PLr=e) = (PL=e) より機能安全設計は、PLr を満足している。

出力部の全体の PFH_D は、$MTTF_D$=92 年、DCavg=99%、カテゴリ 4

より ISO13849-1 表 K.1 より PFH_D＝約 $2.74x10^{-8}$/h

システム全体の PFH_D＝$1.50x10^{-8}$ +$6.44x10^{-9}$+約 $2.74x10^{-8}$＝$4.9\ x10^{-8}$/h(=PLe)

【演習に使用する参考資料】ISO 13849-1:2015　　表 K.1

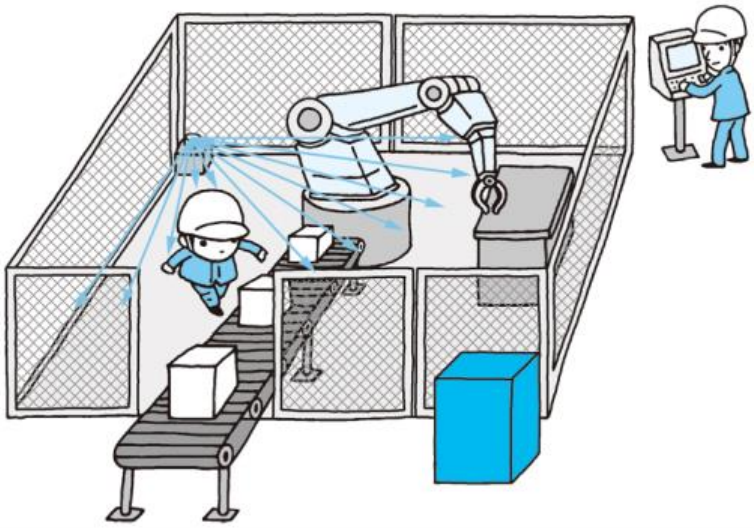
危険側故障の平均確率:PFH_D（1/h）及び対応のパフォーマンスレベル PL

各チャネルの $MTTF_D$（年）	カテゴリ B　PL DC_{avg}=“なし”	カテゴリ 1　PL DC_{avg}=“なし”	カテゴリ 2　PL DC_{avg}=”低”	カテゴリ 2　PL DC_{avg}=”中”	カテゴリ 3　PL DC_{avg}=”低”	カテゴリ 3　PL DC_{avg}=”中”	カテゴリ 4　PL DC_{avg}=”高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
$MTTF_D$ 3.3 年から 24 年の「PFH_D・PL」テーブルは省略							
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82		1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91		1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.94×10^{-8} e	2.74×10^{-8} e
100		1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e
110							2.23×10^{-8} e
120							$2{,}03\times10^{-8}$ e
130							$1{,}87\times10^{-8}$ e
150							$1{,}61\times10^{-8}$ e
160							$1{,}50\times10^{-8}$ e
180							$1{,}33\times10^{-8}$ e
200							$1{,}19\times10^{-8}$ e
220							$1{,}08\times10^{-8}$ e
240							$9{,}81\times10^{-9}$ e
270							$8{,}67\times10^{-9}$ e
300							$7{,}76\times10^{-9}$ e
330							$7{,}04\times10^{-9}$ e
360							$6{,}44\times10^{-9}$ e
390							$5{,}94\times10^{-9}$ e
430							$5{,}38\times10^{-9}$ e
470							$4{,}91\times10^{-9}$ e
510							$4{,}52\times10^{-9}$ e
560							$4{,}11\times10^{-9}$ e
620							$3{,}70\times10^{-9}$ e
680							$3{,}37\times10^{-9}$ e
750							$3{,}05\times10^{-9}$ e
820							$2{,}79\times10^{-9}$ e
910							$2{,}51\times10^{-9}$ e
1000							$2{,}28\times10^{-9}$ e

以下、カテゴリ 4 の 2500 年までの「PFH_D・PL」テーブルは省略

演習４解答：

レーザースキャナによる保護方策に対する機能安全設計の妥当性検証



（「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）

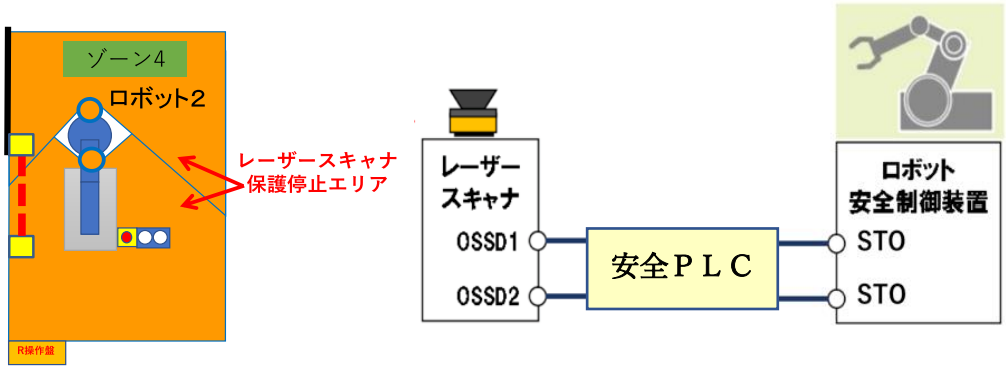


図 9-4　レーザースキャナ設置とレーザースキャナによる保護方策事例

図 9-4 は、ロボットの可動領域に人が侵入した場合の保護装置としてレーザースキャナを適用した事例である。図 9-4 のロボットのリスク低減方策として、以下の方策を採用する。

- ロボットアームの可動範囲に対して保護停止できる範囲でレーザースキャナにより作業者の進入を検知する。
- 速度制御範囲に作業者が入ると、ロボットは、停止カテゴリ 1（IEC 60204-1）で保護停止(SS1)する。

- このリスク低減方策は、ISO 13849-1 の図 A.1 のリスクで見積もると S2/F1/P2 の PLr=d が求められる。

表 9-2 には、各機器の安全仕様を示す。安全仕様を確認して以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

表 9-2　安全機器の PL 関連パラメータ

安全機器	DCavg	PFH[1/時間]	SIL
レーザースキャナ	97%	1.03×10^{-7}	2
安全ＰＬＣ	99%	6.44×10^{-9}	3
ロボット:SS１	92%	3.84×10^{-8}	3

【演習 4-1】

保護停止システム全体の PHF_D とパフォーマンスレベルを求め、機能安全設計の妥当性の検証と理由を示す。

安全関連システム全体の PFH_D＝$1.03\times10^{-7}+6.44\times10^{-9}+3.84\times10^{-8}=1.48\times10^{-7}$/h
安全関連システム全体の PL=d（ISO 13849-1 表 K.1 より）
機能安全設計の妥当性の検証：
(PLr=d) = (PL=d) より機能安全設計は、PLr を満足している。

【演習に使用する参考資料】ISO 13849-1:2015　　表 K.1

危険側故障の平均確率:PFH_D（1/h）及び対応のパフォーマンスレベル PL

各チャネルの $MTTF_D$（年）	カテゴリ B　PL DC_{avg}＝“なし”	カテゴリ 1　PL DC_{avg}＝“なし”	カテゴリ 2　PL DC_{avg}＝” 低”	カテゴリ 2　PL DC_{avg}＝” 中”	カテゴリ 3　PL DC_{avg}＝” 低”	カテゴリ 3　PL DC_{avg}＝” 中”	カテゴリ 4　PL DC_{avg}＝” 高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
$MTTF_D$ 3.3 年から 24 年の「PFH_D・PL」テーブルは省略							
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e
82		1.39×10^{-6} c	6.61×10^{-7} d	3.01×10^{-7} d	1.35×10^{-7} d	5.79×10^{-8} e	3.08×10^{-8} e
91		1.25×10^{-6} c	5.88×10^{-7} d	2.61×10^{-7} d	1.14×10^{-7} d	4.94×10^{-8} e	2.74×10^{-8} e
100		1.14×10^{-6} c	5.28×10^{-7} d	2.29×10^{-7} d	1.01×10^{-7} d	4.29×10^{-8} e	2.47×10^{-8} e
110							2.23×10^{-8} e
120							$2{,}03\times10^{-8}$ e
130							$1{,}87\times10^{-8}$ e
150							$1{,}61\times10^{-8}$ e
160							$1{,}50\times10^{-8}$ e
180							$1{,}33\times10^{-8}$ e
200							$1{,}19\times10^{-8}$ e
220							$1{,}08\times10^{-8}$ e
240							$9{,}81\times10^{-9}$ e
270							$8{,}67\times10^{-9}$ e
300							$7{,}76\times10^{-9}$ e
330							$7{,}04\times10^{-9}$ e
360							$6{,}44\times10^{-9}$ e
390							$5{,}94\times10^{-9}$ e
430							$5{,}38\times10^{-9}$ e
470							$4{,}91\times10^{-9}$ e
510							$4{,}52\times10^{-9}$ e
560							$4{,}11\times10^{-9}$ e
620							$3{,}70\times10^{-9}$ e
680							$3{,}37\times10^{-9}$ e
750							$3{,}05\times10^{-9}$ e
820							$2{,}79\times10^{-9}$ e
910							$2{,}51\times10^{-9}$ e
1000							$2{,}28\times10^{-9}$ e

以下、カテゴリ 4 の 2500 年までの「PFH_D・PL」テーブルは省略

演習５解答：

非常停止装置による付加保護方策に対する機能安全設計の妥当性検証

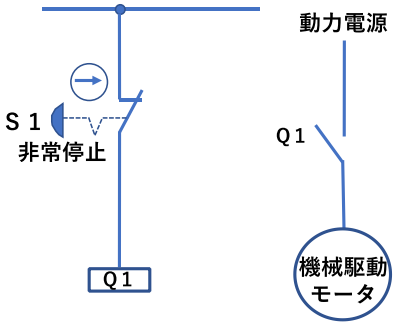


図 9-5　非常停止ボタンによるモータ動力遮断の付加保護方策事例

図 9-5 は、非常停止ボタンで直接コンタクタ励磁回路遮断しモータ動力を遮断する回路事例である。非常停止ボタンの平均操作頻度は、30 分毎に 1 回である。また、この設備は、30 年間使用され、1 日の作業時間は 20 時間、年間作業日数は 300 日の作業を行う。表 9-3 には、各機器の B_{10} 仕様を示す。非常停止機能の制御システムの安全関連部としての**要求安全性能は、PLr=c** である。B_{10} 仕様を確認して以下の設問に対して演習を行い設計の妥当性を評価し検証を行う。

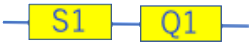
表 9-3　安全機器の PL 関連パラメータ

安全機器	B_{10}[回]
非常停止ボタン S1	500,000
コンタクタ Q1	1,000,000

【演習 5-1】

以下の設問に従って非常停止ボタン S1 とコンタクタ Q1 のそれぞれの $MTTF_D$ および制御システム全体の $MTTF_D$ を求める。

図 9-5 の制御システムのカテゴリ＝1　　機能ブロック図：



安全機能（非常停止機能）の年間作動回数　n_{op}=300x20x60/30=12,000

非常停止ボタン S1 の B_{10D}=500,000x2=1,000,000 回

コンタクタ Q1 の B_{10D}=1,000,000x2=2,000,000 回

非常停止ボタン S1 の T_{10D}(S1)=1,000,000/12,000=83.3 年

MTTFD(S1)= T_{10D}(B1)/0.1=833 年→100 年で制限

コンタクタ Q1 の T_{10D}(Q1)=2,000,000/12,000=166.6 年

MTTFD(Q1)= T_{10D}(Q1)/0.1=1666 年→100 年で制限

【演習 5-2】

制御システム全体の PL と機能安全設計の妥当性の検証と理由を示す。

【演習 5-1】の結果：制御システム全体の PL:カテゴリ 1、$MTTF_D$=50 年

PL=c,　PFH_D＝$1.24x10^{-6}$（ISO 13849-1 表 K.1 より：$MTTF_D$=47 年を選択）

機能安全設計の妥当性の検証：

(PLr=c) = (PL=c) より機能安全設計は、PLr を満足している。

【演習に使用する参考資料】ISO 13849-1:2015　　表 K.1

危険側故障の平均確率:PFH_D（1/h）及び対応のパフォーマンスレベル PL

各チャネルの $MTTF_D$（年）	カテゴリ B　PL DC_{avg}＝“なし”	カテゴリ 1　PL DC_{avg}＝“なし”	カテゴリ 2　PL DC_{avg}＝” 低”	カテゴリ 2　PL DC_{avg}＝” 中”	カテゴリ 3　PL DC_{avg}＝” 低”	カテゴリ 3　PL DC_{avg}＝” 中”	カテゴリ 4　PL DC_{avg}＝” 高”
3	3.80×10^{-5} a		2.58×10^{-5} a	1.99×10^{-5} a	1.26×10^{-5} a	6.09×10^{-6} b	
3.3	3.46×10^{-5} a		2.33×10^{-5} a	1.79×10^{-5} a	1.13×10^{-5} a	5.41×10^{-6} b	
3.6	3.17×10^{-5} a		2.13×10^{-5} a	1.62×10^{-5} a	1.03×10^{-5} a	4.86×10^{-6} b	
3.9	2.93×10^{-5} a		1.95×10^{-5} a	1.48×10^{-5} a	9.37×10^{-6} b	4.40×10^{-6} b	
4.3	2.65×10^{-5} a		1.76×10^{-5} a	1.33×10^{-5} a	8.39×10^{-6} b	3.89×10^{-6} b	
4.7	2.43×10^{-5} a		1.60×10^{-5} a	1.20×10^{-5} a	7.58×10^{-6} b	3.48×10^{-6} b	
5.1	2.24×10^{-5} a		1.47×10^{-5} a	1.10×10^{-5} a	6.91×10^{-6} b	3.15×10^{-6} b	
5.6	2.04×10^{-5} a		1.33×10^{-5} a	9.87×10^{-6} b	6.21×10^{-6} b	2.80×10^{-6} c	
6.2	1.84×10^{-5} a		1.19×10^{-5} a	8.80×10^{-6} b	5.53×10^{-6} b	2.47×10^{-6} c	
6.8	1.68×10^{-5} a		1.08×10^{-5} a	7.93×10^{-6} b	4.98×10^{-6} b	2.20×10^{-6} c	
7.5	1.52×10^{-5} a		9.75×10^{-6} b	7.10×10^{-6} b	4.45×10^{-6} b	1.95×10^{-6} c	
8.2	1.39×10^{-5} a		8.87×10^{-6} b	6.43×10^{-6} b	4.02×10^{-6} b	1.74×10^{-6} c	
9.1	1.25×10^{-5} a		7.94×10^{-6} b	5.71×10^{-6} b	3.57×10^{-6} b	1.53×10^{-6} c	
10	1.14×10^{-5} a		7.18×10^{-6} b	5.14×10^{-6} b	3.21×10^{-6} b	1.36×10^{-6} c	
11	1.04×10^{-5} a		6.44×10^{-6} b	4.53×10^{-6} b	2.81×10^{-6} c	1.18×10^{-6} c	
12	9.51×10^{-6} b		5.84×10^{-6} b	4.04×10^{-6} b	2.49×10^{-6} c	1.04×10^{-6} c	
13	8.78×10^{-6} b		5.33×10^{-6} b	3.64×10^{-6} b	2.23×10^{-6} c	9.21×10^{-7} d	
15	7.61×10^{-6} b		4.53×10^{-6} b	3.01×10^{-6} b	1.82×10^{-6} c	7.44×10^{-7} d	
16	7.13×10^{-6} b		4.21×10^{-6} b	2.77×10^{-6} c	1.67×10^{-6} c	6.76×10^{-7} d	
18	6.34×10^{-6} b		3.68×10^{-6} b	2.37×10^{-6} c	1.41×10^{-6} c	5.67×10^{-7} d	
20	5.71×10^{-6} b		3.26×10^{-6} b	2.06×10^{-6} c	1.22×10^{-6} c	4.85×10^{-7} d	
22	5.19×10^{-6} b		2.93×10^{-6} c	1.82×10^{-6} c	1.07×10^{-6} c	4.21×10^{-7} d	
24	4.76×10^{-6} b		2.65×10^{-6} c	1.62×10^{-6} c	9.47×10^{-7} d	3.70×10^{-7} d	
27	4.23×10^{-6} b		2.32×10^{-6} c	1.39×10^{-6} c	8.04×10^{-7} d	3.10×10^{-7} d	
30		3.80×10^{-6} b	2.06×10^{-6} c	1.21×10^{-6} c	6.94×10^{-7} d	2.65×10^{-7} d	9.54×10^{-8} e
33		3.46×10^{-6} b	1.85×10^{-6} c	1.06×10^{-6} c	5.94×10^{-7} d	2.30×10^{-7} d	8.57×10^{-8} e
36		3.17×10^{-6} b	1.67×10^{-6} c	9.39×10^{-7} d	5.16×10^{-7} d	2.01×10^{-7} d	7.77×10^{-8} e
39		2.93×10^{-6} c	1.53×10^{-6} c	8.40×10^{-7} d	4.53×10^{-7} d	1.78×10^{-7} d	7.11×10^{-8} e
43		2.65×10^{-6} c	1.37×10^{-6} c	7.34×10^{-7} d	3.87×10^{-7} d	1.54×10^{-7} d	6.37×10^{-8} e
47		2.43×10^{-6} c	1.24×10^{-6} c	6.49×10^{-7} d	3.35×10^{-7} d	1.34×10^{-7} d	5.76×10^{-8} e
51		2.24×10^{-6} c	1.13×10^{-6} c	5.80×10^{-7} d	2.93×10^{-7} d	1.19×10^{-7} d	5.26×10^{-8} e
56		2.04×10^{-6} c	1.02×10^{-6} c	5.10×10^{-7} d	2.52×10^{-7} d	1.03×10^{-7} d	4.73×10^{-8} e
62		1.84×10^{-6} c	9.06×10^{-7} d	4.43×10^{-7} d	2.13×10^{-7} d	8.84×10^{-8} e	4.22×10^{-8} e
68		1.68×10^{-6} c	8.17×10^{-7} d	3.90×10^{-7} d	1.84×10^{-7} d	7.68×10^{-8} e	3.80×10^{-8} e
75		1.52×10^{-6} c	7.31×10^{-7} d	3.40×10^{-7} d	1.57×10^{-7} d	6.62×10^{-8} e	3.41×10^{-8} e

以下、カテゴリ 4 の 2500 年までの「PFH_D・PL」テーブルは省略

機能安全活用実践マニュアル
統合生産システム(IMS)編

平成 30 年度　厚生労働省委託事業
機能安全を活用した機械設備の安全対策推進事業

平成 31 年 3 月
(一社)安全・環境マネジメント協会
〒577-0006 大阪府東大阪市楠根 1-8-27
TEL 06-6747-2412
http://www.sema.or.jp/
e-mail sema@sema.or.jp

一般社団法人　安全・環境マネジメント協会　2019.3