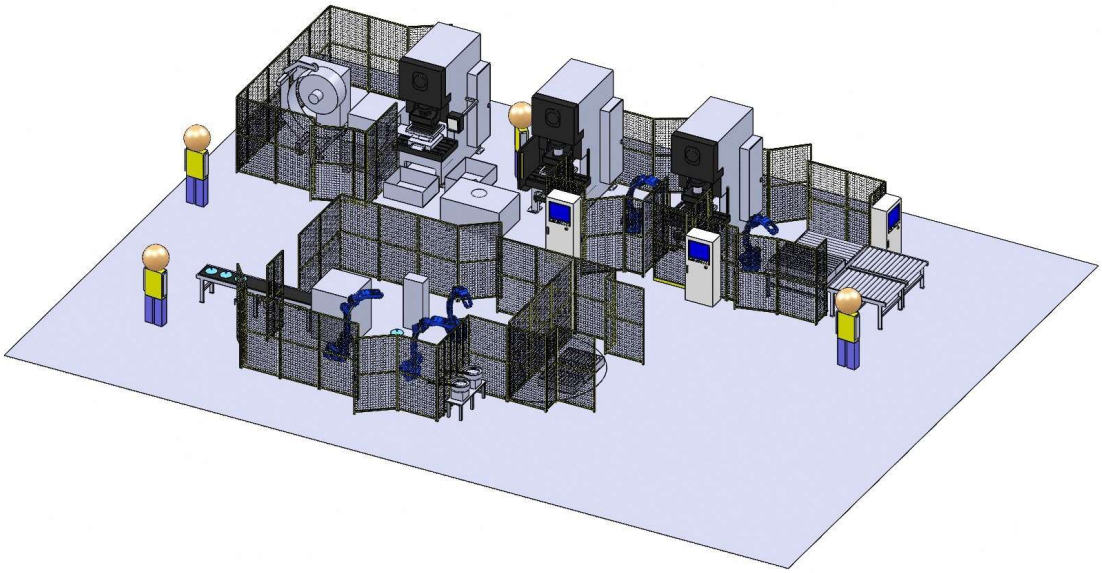
統合生産システムの機能安全設計

−システムインテグレータのための
統合生産システムの安全制御設計指南−



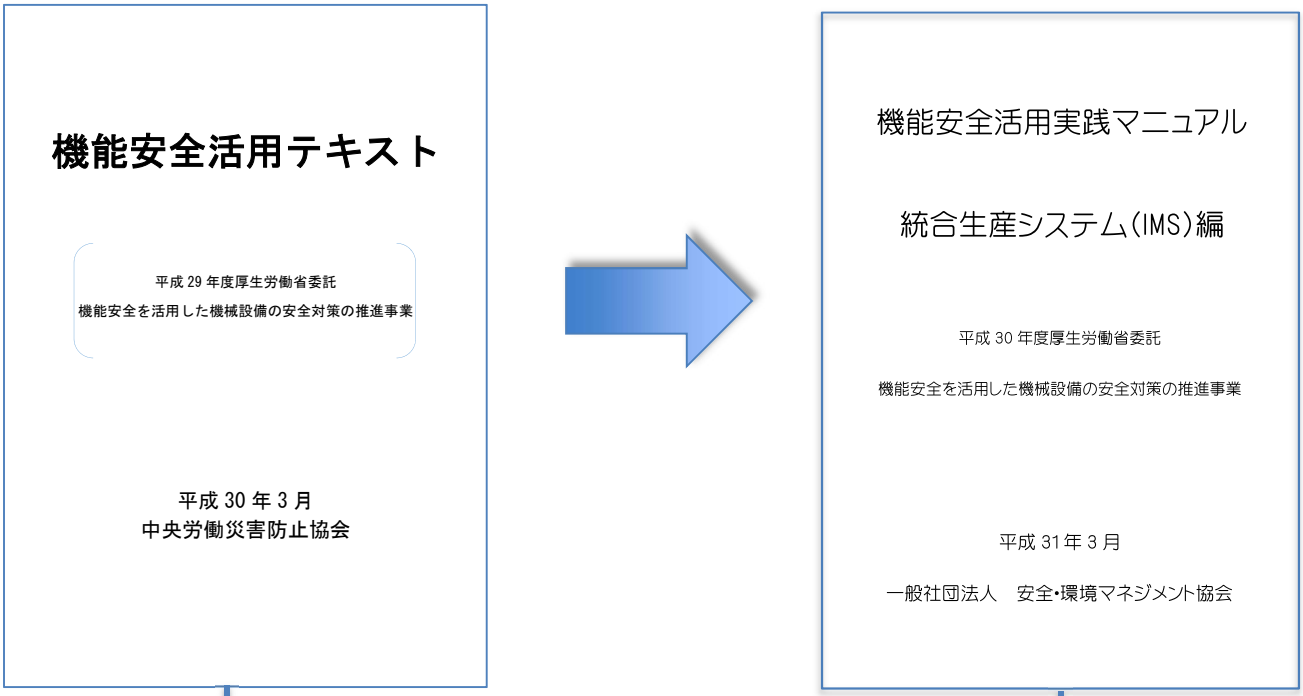
システム制御の高度化や複雑化が進む中で、統合生産システムのシステムインテグレータが安全設計へ機能安全制御を導入することが求められるようになってきました。「機能安全による機械等に係る安全確保に関する技術上の指針（以下、「機能安全指針」）」（平成 28 年厚生労働省告示第 353 号）が公表されて以降、ボイラや産業用ロボットシステムの安全設計に機能安全を導入する方法が紹介されてきましたが、今回は統合生産システムを対象にして、作業や工程の分析、リスクアセスメントから始まる安全設計の手順、機能安全による制御システムの安全目標設定と実現方法、及びそれら手段の妥当性の検証についてご紹介します。

厚生労働省・都道府県労働局・労働基準監督署

はじめに

厚生労働省は、平成30年度に「機能安全活用実践マニュアル　統合生産システム編」を作成しました。このマニュアルは、システムインテグレータが統合生産システムを設計する際、電子制御等による安全機能を付加する安全方策（機能安全）を導入するための考え方や手順をまとめたものです。このパンフレットでは、本マニュアルの概要をご説明します。

なお、本マニュアルは、機械安全や機能安全の基礎知識があることを前提として作成されていますので、活用に当たっては、あらかじめ、「機能安全活用テキスト」（平成29年度発行）をご覧いただき、基礎知識を理解されることをお勧めします。



基礎知識

- 機械設備の安全概論
- 機能安全関連法令と安全規格体系
- リスクアセスメントとリスク低減
- 機械安全における機能安全の適用
- 機能安全による安全関連システムの設計
- 妥当性確認

統合生産システムに特化

- 設計コンセプト
- 統合生産システム関連安全規格
- システム構築手順
- リスクアセスメントとリスク低減
- 安全関連システムの設計と検証
- 演習

「機能安全活用テキスト」PDF 版の入手先:厚生労働省ホームページ
（http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000140176.html）

統合生産システムの設計コンセプト

システムインテグレータとは:統合生産システム(Integrated Manufacturing System)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人あるいは組織※のことです。

※ システムインテグレータは、機械の製造者、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ります。

システムインテグレータは、機械製造者と機械使用者の間で共にコミュニケーションをとりながら、次の業務を実施します。

- 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

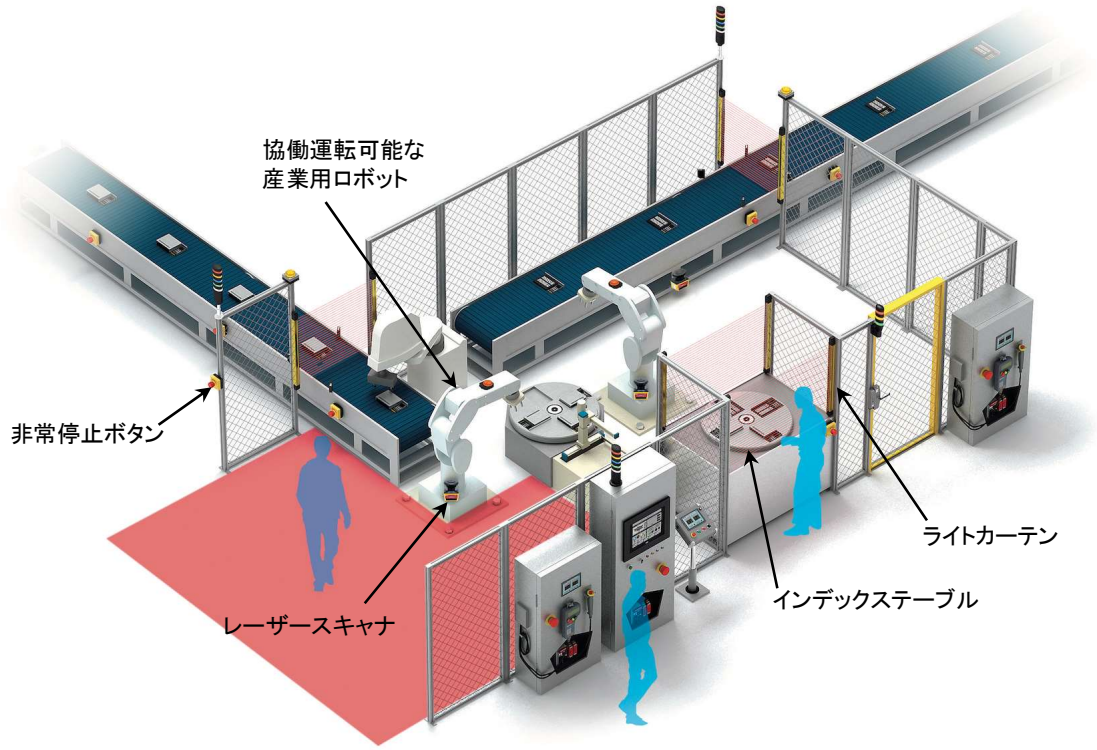


図1　統合生産システムのイメージ(IDEC(株)提供)

システムインテグレータが上記業務を実施することにより、図1のような複数の機械と人が共存する統合生産システムに対して、各種保護装置(ライトカーテン、レーザースキャナ、非常停止ボタン等)を含む機能安全を導入した安全関連システムを設計することができます。

統合生産システム構築手順

システムインテグレータは、機械使用者からの仕様書内容を基に、初期の基本仕様を検討します。例えば、鍋蓋の製造工程として図 2 の工程を想定し、3 つの製造ライン（素材加工ライン、絞りピアスライン、面取り取手取り付けライン）構成を考えます。

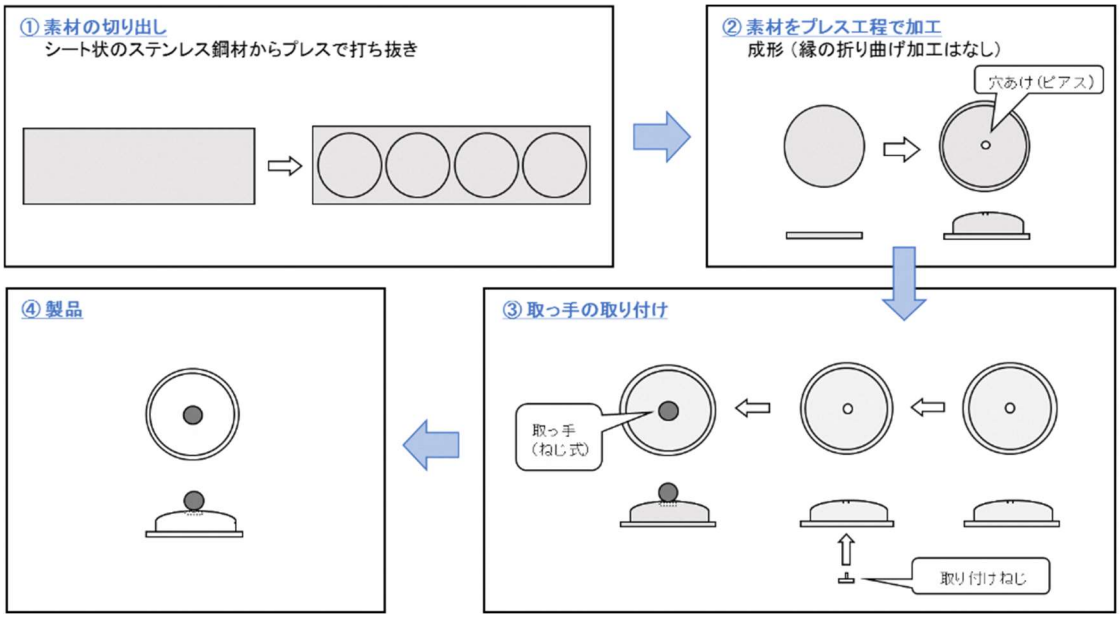


図 2　鍋蓋製造工程の検討結果

次に、工程分析により基本機械構成とワークの流れを定め、さらに作業分析によって作業と作業ゾーンを設定します。例として、図 2 の②の工程（絞りピアスライン）の構成と作業ゾーンの割り当てを図 3 に示します。ゾーン 4 内のロボット 2 はピアス加工後の鍋蓋の目視確認を作業者と協働で行うものとしています。

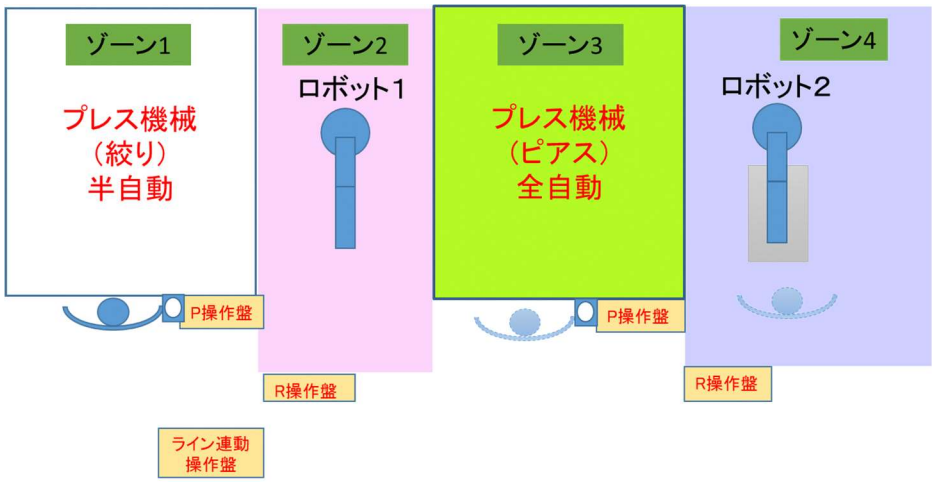


図 3　絞りピアスラインの構成

リスクアセスメントとリスク低減

構想設計において設定したゾーンごとに危険源・危険状態・危険事象を同定して、危険源ごとにリスクを見積もります。特に、部分的に停止できるような統合生産システムでは、最も典型的な意図的・非意図的な危険行動となり得る「ゾーン間移動」（図４のゾーン間の矢印のように作業者が他ゾーンへ移動すること）に対して、リスク低減措置が実施されているゾーンからリスクが低減されていないゾーンに、作業者が侵入できるか否かの分析を行います。

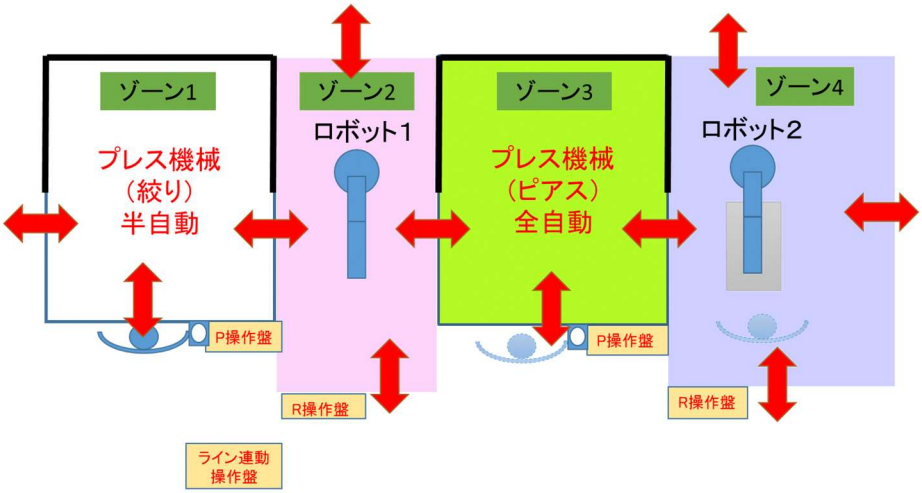


図４　絞りピアスラインで考慮すべき人のアクセス

リスク低減方策の検討は、JIS B 9700 等で規定する３ステップ法（本質的安全設計→工学的方策→管理的方策）により行いますが、本質的安全設計によるリスク低減が行えない場合、基本的にゾーンごとの隔離と停止の保護方策を実施します。特に、図５のようにロボットが隣接するゾーンへ移動できる場合、ライトカーテンはロボット検知用と人検知用の２組必要となり、各々のライトカーテンの配置にはロボットの停止距離や安全距離を配慮しなければなりません。

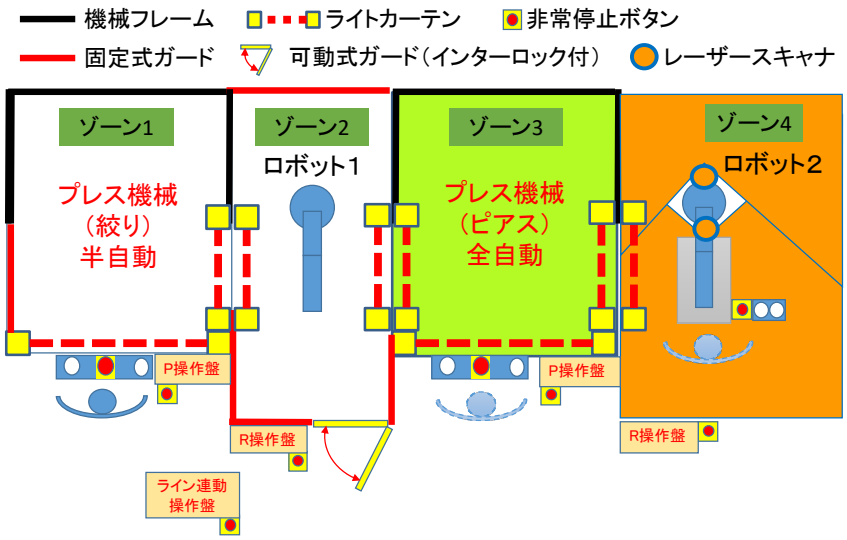


図５　安全距離を考慮した保護方策例

安全要求仕様の決定

安全関連システムを用いた電子等制御によってリスク低減を図る場合、リスクレベルに応じ、それぞれの安全機能に求められる「要求安全度水準」を決定します。この安全度水準の一つがパフォーマンスレベル(PL)(JIS B 9705-1)であり、単位時間あたりの危険側故障発生の平均確率(PFH_D)の範囲で a～e の 5 段階でランク付けされます。図 5 における各安全機能(非常停止ボタン、ライトカーテン、レーザースキャナ)に対して、リスクアセスメント結果とリスクグラフから決まる要求パフォーマンスレベル(PLr)を満たす安全関連システムを実装する必要があります(表 1)。

表 1　安全機能の振る舞い(非常停止のみ抜粋)

安全機能リストと ISO 13849-1(JIS B 9705-1)による PLr(要求 PL) 決定のリスクグラフ評価結果						
安全機能	**設置位置**	**有効ゾーン**	**安全機能の振る舞い**	**リスクグラフ評価**	**PLr**	**PL**
非常停止 EMG11	**統括制御盤**	**全ゾーン**	**非常停止ボタンを押すことで全プレス・全ロボット停止（プレス：停止カテゴリ０、ロボット：停止カテゴリ１）**	**S2-F1-P2**	**d**	
非常停止 EMG1-1	**絞りプレス 両手操作盤**	**ゾーン１**	**非常停止ボタンを押すことで絞りプレスを停止（プレス：停止カテゴリ０）**	**S2-F1-P2**	**d**	

リスクグラフは PLr を傷害のひどさ(S)、危険源への暴露時間・頻度(F)、危険源回避の可能性(P)から決定する手法です。

安全関連システムの設計と検証

安全機能の PLr を実現するため、安全関連システムを設計する上で必要となる要求事項は次のとおりです。各要求事項から PL を決定する方法は図 6 のとおりです。

①カテゴリ:安全関連システムのハードウエア構成
②$MTTF_D$:安全関連システムの平均危険側故障時間(単位:年)
③DCavg:安全関連システムの平均診断範囲のレベル(単位:%)
④CCF:カテゴリ2以上のシステムの共通原因故障の考慮
⑤PFH_D:危険側故障の平均発生確率(単位:/h)

また、安全関連システムの論理部として安全 PLC(プログラマブル・ロジック・コントローラ)を使用する場合、安全 PLC メーカが提供する各安全機能に関するソフトウェアの仕様を守って構築し、ソフトウェア妥当性確認のための各種文書を作成しておく必要があります。

一方、リスク低減のための保護装置の選定については、ISO 11161 に示されるタスクゾーン設定や設計方策によりリスク低減を行うことか必要となります。これらの保護装置の代表的な例として、インタロ

ック式ガード(ドアインタロック装置)、ライトカーテン、レーザースキャナ、圧力検知マットスイッチ、イネーブルデバイス、非常停止装置(付加保護方策として)があります。

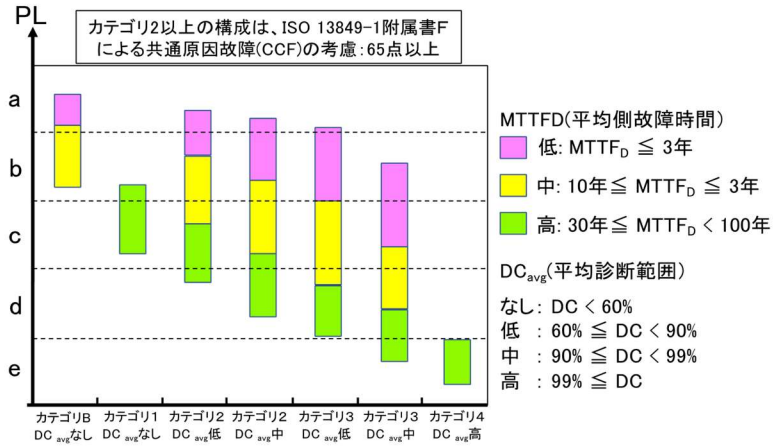


図 6 PL と「カテゴリ、$MTTF_D$、DC_{avg}、CCF」との関係

安全関連システムの妥当性確認

妥当性確認とは、対象の統合生産システムの設計開発段階で統合生産システム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(JIS B 9705-1)の要求事項を満足するかを確認する作業です。このプロセスには、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(PL≧PLr)していることを検証することも含まれ、分析や試験により実施されます。

妥当性確認のための情報は文書として作成しておく必要があります。これらの必要文書は統合生産システムの技術ファイルとして作成されねばならず、特に、リスクアセスメントの関連文書(図 7)は技術ファイルの多くを占める非常に重要な文書類となります。

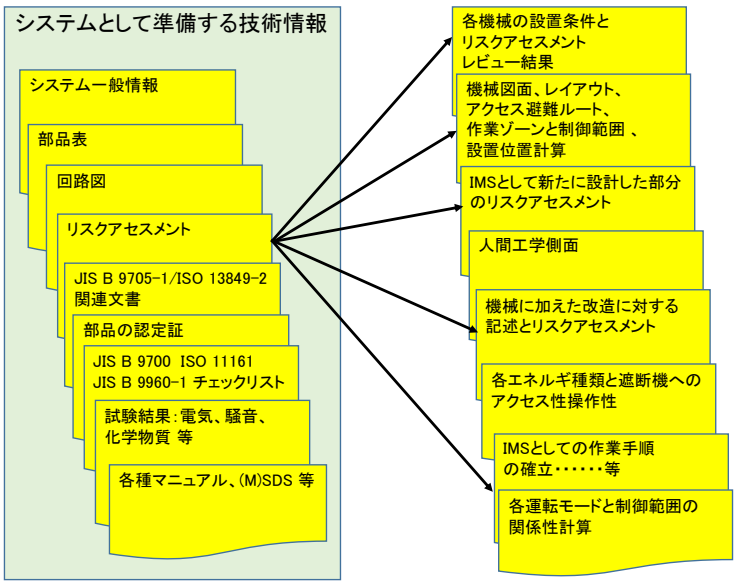


図 7　統合生産システムの技術ファイル構成例

演習

本マニュアルでは、統合生産システムにおける機能安全設計を対象として、可動ガードのインタロック保護方策、光線式安全装置による保護方策、レーザースキャナによる保護方策、非常停止装置による付加保護方策の各々の安全機能に対して、要求安全度水準（PLr）の設定から安全関連システムの $MTTF_D$ あるいは PFH_D を求めることによる妥当性検証までの演習と解答を示しています。

例えば、本マニュアルが事例対象としている協働ロボットへの人の接近を、レーザースキャナの設置により検知して保護停止する場合、図 8 のように安全 PLC を利用して安全関連システムを構築することができ、各機器の安全仕様からこの保護方策の設計の妥当性を評価・検証することができます。

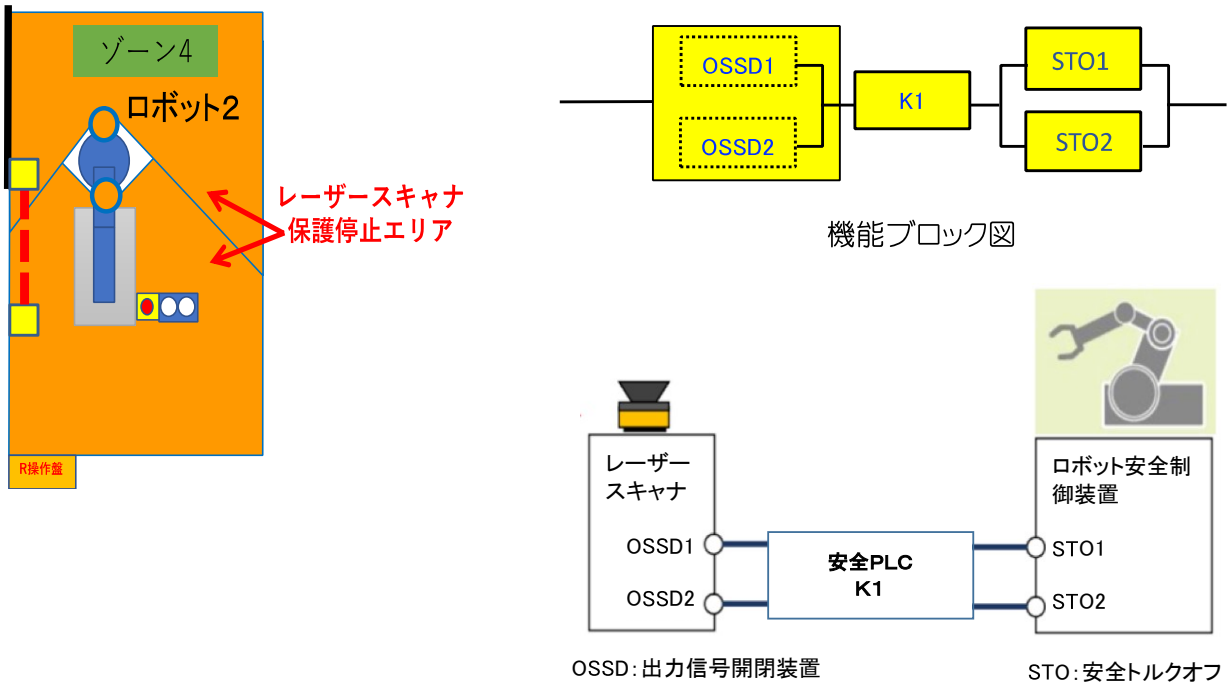


図 8　レーザースキャナによる保護方策事例（図 5 のゾーン 4 対応）

参考資料

1. 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（厚生労働省）
2. 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（厚生労働省）
3. 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）