安全規格

機械類の安全規格の動向

求められる国際安全規格への対応

日本では、労働災害の責任を「作業者の不注意」や「使用方法の不適切」などとして使用者側に求め、メーカ側の責任が問われることが少ないため、機械に対する安全方策よりもコストや作業性を優先させる傾向があります。

これに対し欧州では、『機械は必ず故障するもの、そして人は必ずミスを犯すもの』という意識のもとに安全確保の方法を厳しく規定し、機械に対する安全方策を施しています。
こうした文化の違いから、同じ機械でも安全装置を簡略化した国内向け機械（日本仕様）と、安全装置を装備した欧州向け機械（欧州仕様）との2つの仕様（ダブルスタンダード）を設けている場合もあります。
もちろん、日本では機械に安全装置を装備していないことは、一部のプレス機械などを除いて法的に義務づけられていないだけに違法ではありませんが、安全方策に格差があることはPL法の観点からみても問題があり、製造者は「安全な機械」の製造に努めなければなりません。

そこで現在、安全方策の国際整合化に向けた取り組みが急ピッチで進められており、ISO（国際標準化機構）では、安全に関わる国際規格の作成上の指針「ISO/IEC（国際電気標準会議）ガイド51」に基づき、機械設計の一般原則を定めた国際安全規格「ISO 12100」が、2003年11月に正式発効されました。また日本国内においても労働安全衛生法（二十八条の二）にてリスクアセスメントの実施が努力義務として定められ、2006年4月より施行されています。

機械安全規格の階層と制度

※規格は主なもののみ列挙、プロジェクト段階の表記は省略してあります。

ISO／IEC Guide51

※タイプA―B―Cの階層は、機械・ISO関連

ISO：機械系		IEC：電気系
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 12100／JIS B 9700）	**タイプA規格** **基本安全規格：** すべての機械類に適用できる 基本概念、設計原則 及び一般的側面を規定	
・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 （ISO 13849-1／JIS B 9705-1） ・制御システムの安全関連部　第2部：妥当性確認 （ISO 13849-2） ・非常停止―設計原則（ISO 13850／JIS B 9703） ・両手操作制御装置（ISO 13851／JIS B 9712） ・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 13857／JIS B 9718） ・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 13854／JIS B 9711） ・人体部位の接近速度に基づく安全防護物の位置決め （ISO 13855／JIS B 9715） ・予期しない起動の防止 （ISO 14118／JIS B 9714） ・ガードと共同するインタロック装置 （ISO 14119／JIS B 9710） ・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 14120／JIS B 9716）	**タイプB規格** **グループ安全規格：** 広範囲の機械類に適用できる 安全面、安全防護物を規定	・機械の電気装置　第1部：一般要求事項 （IEC 60204-1／JIS B 9960-1） ・表示、マーキング及び操作 （IEC 61310-1～3／JIS B 9706-1～3） ・電気的検知保護設備 （IEC 61496-1～3／JIS B 9704-1～3） ・人の存在検出の保護機器応用 （IEC/TS 62046） ・安全関連の電気・電子・プログラマブル電子制御システムの機能安全 （IEC 62061／JIS B 9961） ・電気・電子・プログラマブル電子安全関連系の機能安全 （IEC 61508-1～7／JIS C 0508-1～7） ・安全関連アプリケーションにおける通信システムの使用指針 （IEC/TR 62513） ・低圧開閉装置及び制御装置 （IEC 60947／JIS C 8201） ・EMC（IEC 61000／JIS C 61000） ・電源変圧器（IEC 60076）
例： ・工作機械 ・産業用ロボット ・プレス機械 ・包装機械 ・プラスチックおよびゴム用射出成形機 ・ブロー成形機 ・鋳造機械 ・印刷機械 ・押出し機 ・繊維機械 ・エレベータ ・エスカレータ・コンベヤ ・食品機械	**タイプC規格** **個別機械安全規格：** 個々の機械または機械群の 詳細な安全要求事項を規定	〈その他の関連規格〉 ・人間工学の設計原則 ・人体の寸法 ・人間の肉体的能力 ・表示装置と操作機器・記号 ・電気機器記号と電気図記号 ・振動・騒音 ・温度 ・流体動力システムと校正部品

2015年2月現在

機械の包括的な安全基準に関する指針

平成13年6月1日厚生労働省より「機械の包括的な安全基準に関する指針」（基発第501号）が各都道府県労働局長に通達されました。
その後、平成17年4月の労働安全衛生法等の一部改正により、危険性または有害性等の調査（リスクアセスメント）およびその結果に基づく措置の実施が事業者の努力義務として規定されたことや、機械類の安全性に関する国際規格が制定されたことなどにより、機械の製造段階から使用段階にわたる一層の安全確保を図るために、平成19年7月31日に同指針の改正（基発第0731001号）が通達されています。

指針のポイント

機械類の安全に関して、機械の設計・製造・改造等または輸入（以下「製造等という。）を行なう者が実施する事項と事業者が実施する事項が明確に定義されました。指針には、国際規格ISO 12100「機械類の安全性-設計のための一般原則」と同様の内容が盛り込まれています。

指針の概要

目的

機械の危険性または有害性を低減し、機械による労働災害の防止に資する。
・機械の製造等を行なう者の実施事項
・機械を労働者に使用させる事業者の実施事項

適用

機械による危険性または有害性（機械の危険源をいい、以下単に「危険性または有害性」という。）を対象とし、機械の製造等を行なう者および機械を労働者に使用させる事業者の実施事項を示す。

機械の製造等を行なう者の実施事項

1. 製造等を行なう機械の調査等の実施
   （1）機械の制限に関する仕様の指定
   （2）機械に労働者が関わる作業等における危険性または有害性の同定
   （3）（2）にて同定された危険性または有害性ごとのリスクの見積りおよび適切なリスクの低減が達成されているかどうかの検討
   （4）保護方策の検討および実施によるリスクの低減
2. 実施時期
   ・機械の設計・製造・改造等を行なうとき
   ・機械を輸入し譲渡または貸与を行なうとき
   ・製造等を行なった機械による労働災害が発生したとき
   ・新たな安全衛生に係る知見の集積等があったとき
3. 機械の制限に関する仕様の指定　4. 危険性または有害性の同定
5. リスクの見積り等　6. 保護方策の検討および実施　7. 記録

機械を労働者に使用させる事業者の実施事項

1. 実施内容
   （1）機械に労働者が関わる作業等における危険性または有害性の同定
   （2）（1）により同定された危険性または有害性によって生ずるリスクの見積り
   （3）（2）の見積りに基づくリスクを低減するための優先度の設定および保護方策の検討
   （4）（3）の優先度に対応した保護方策の実施
2. 実施体制等　3. 実施時期　4. 対象の選定　5. 情報の入手
6. 危険性または有害性の同定　7. リスクの見積り等
8. 保護方策の検討および実施　9. 記録　10. 注文時の配慮事項等

機械安全に対する基本的な考え方

機械は必ず故障するもの、そして人は必ずミスを犯すものということをまず認めた上で、万一これらが起きても人に危害を及ぼさない構造をシステムの設計段階で構築しておくことが、機械安全の基本となります。
機械安全に関する体系的な技術基準としては、欧州で1993年より施行されている欧州統一規格（EN規格）が代表的なものです。安全に関するEN規格は、欧州域内では機械指令に規定された基本安全要求事項を満足する技術基準として制定されており、1995年からは流通の必須条件であるCEマーキング取得のために、この規格に適合することが主要な条件となっています。

機械災害による危険とは

機械安全の一般原則を定義しているISO 12100（JIS B 9700）によれば、機械による危険源は、次のように分類されています。

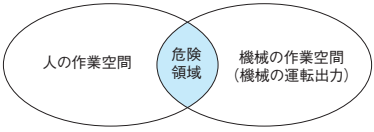
危険源の分類と事例例

①機械的危険源
　押しつぶし、せん断、
　切傷、切断、巻き込み、
　引き込み、捕そく、衝撃、
　突き刺し、突き通し、
　高圧流体の噴出
②電気的危険源
　充電部との接触
　絶縁不良
　静電気 など
③熱的危険源
　火災、爆発
　火傷、熱傷 など
④騒音による危険源
　聴力喪失
　耳鳴り
　平衡感覚の喪失 など
⑤振動による危険源
　腰痛
　全身の障害 など
⑥放射線による危険源
　低周波、無線周波、マイクロ波、
　赤外線、可視光線、紫外線、
　X線、γ線、α線、β線、
　レーザ放射 など
⑦材料による危険源
　有害性、毒性、腐食性、
　粉塵、ミスト、
　爆発 など
⑧非人間工学的危険源
　不自然な姿勢、
　精神的な負担、
　ヒューマンエラー など
⑨すべり、つまずきおよび墜落の危険源
　床面、接近手段の軽視による
　傷害 など
⑩危険源の組み合わせ
　ささいな危険が組み合わされての
　重大な危険 など
⑪機械が使用される環境に関連する危険源
　危険源（温度・風・雪・落雷など）を生じる
　可能性のある環境下での運転 など

機械災害防止の基本

機械災害の発生メカニズム

人が機械を使用して行なう作業においては、『人と機械の運転出力（可動部や放出エネルギー）が同一空間内に同時に存在する場合に、機械の可動部などに人が接触すると、人は災害を受ける』こととなります。
この条件が、機械災害の発生メカニズムということになります。



機械災害防止の基本

機械災害防止の基本は、機械災害の発生メカニズムの条件が成立しないようにすることです。
つまり、『人と機械の運転出力とを空間的に分離する（人の作業空間と機械の作業空間とを完全に隔離し、危険領域を持たない）こと』、あるいは『時間的に分離する（人が作業を行なうときには機械が停止する、または機械が作業を行なうときには人は作業を行なわない）こと』が、機械災害防止の条件です。
言いかえると、『人と機械の運転出力との空間的分離（隔離の原則）または時間的分離（停止の原則）』を実現するシステムを作ること、そしてそのシステムがいつも正常状態にあるか確かめることができることが、人と機械における安全確保の基本です。
これを実現する方法として、原則として下記のような2通りの方法が考えられます。

①隔離の原則：ガードによる安全防護
②停止の原則：安全装置（インタロック装置）による安全防護
　インタロック装置とは、ガードが閉じた状態でなければ機械の運転ができないようにするための装置などのことを言い、機械式、電気式があります。

安全規格

安全方策の手順

安全方策の手順

機械を設計する場合、設計者は設計段階で機械の安全方策の手順に従い、機械の安全性を確保しなければなりません。

ISO 12100に基づいた安全方策の手順

手順1：機械類の各種制限を決定する。

機械の設計は、その制限の決定から開始されます。
(1) 使用上の制限：機械の「意図する使用」などの決定
(2) スペース上の制限：運動範囲、機械の据え付けに対するスペース上の要求事項、作業者-機械間および機械-動力源間のインタフェースなど

▼

手順2：危険源を同定し、リスクアセスメントを実施する。

設計者は、機械によって引き起こされる可能性のある種々の危険源を同定して、傷害または健康障害を起こす恐れのあるこれらの危険源に至るすべての状況を予測しなければなりません。

▼

手順3：可能な限り危険源を削除するか、またはリスクの低減を図る。

▼

手順4：残留リスクに対しては、防護ガードや安全装置などの安全防護を設置する。

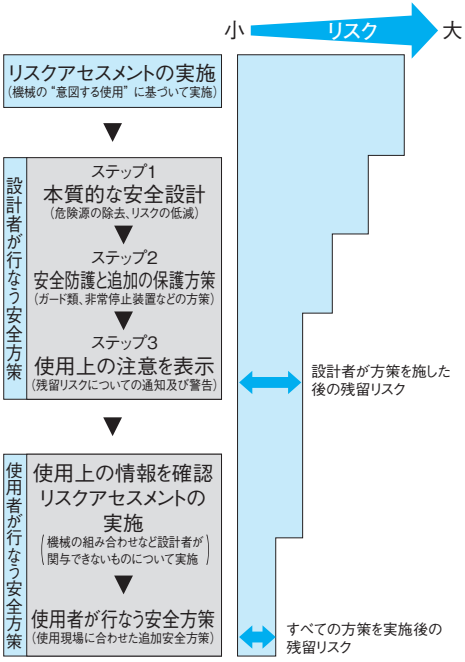
▼

手順5：必要に応じて、追加予防策を考慮する。

設計者は、非常事態に対処するために、追加的な方策（非常停止装置の装備、捕捉された人の脱出および救助に関する予防策など）が必要かどうか、またはこれらの主要な機能の二次的効果として安全性を向上できるかどうかを判断しなければなりません。
例えば、保全の容易さ（保全性）も安全要因の1つです。

▼

手順6：最後まで残るリスクは、すべて使用者に情報提供と警告を行なう。



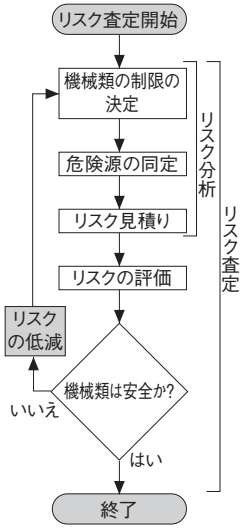
リスクアセスメントと制御カテゴリの評価

リスクアセスメント（リスク査定）

・リスクアセスメントとは、設備や装置が安全かどうか、そのリスクの程度を審査する作業であり、実際には予想される危険に対してリスクパラメータ（傷害の重さ、危険の頻度および継続時間、危険回避の可能性）を査定してリスクレベルを想定し、実際に施行された安全方策が危険に対して想定したリスクレベルに見合ったものかどうかを比較する作業です。
・安全機器においては、制御盤内の安全部分と中継地点に接点を持つ安全機器の機能にエラーが発生した場合が、このリスクアセスメント（リスク査定）の対象となります。
・リスクアセスメントについては、ISO 12100（機械類の安全性-設計のための一般原則）やISO 13849-1（機械の安全性-制御システムの安全関連部分-第1部：設計のための一般原則）などで規定されています。

ISO 12100に基づいたリスクアセスメントおよびリスク低減

リスクアセスメントは、まずISO 12100に基づき機械類の使用時に発生する危険を統計的に分析し、リスクの低減を図らなければなりません。



●機械類の制限の決定
機械類の制限の決定は、下記に基づいて行なわなければなりません。
・機械類の耐用期間の各段階に対する要求事項
・機械類の正しい使い方と動作および予想される誤使用と誤動作を含めての機械類の限界決定
・作業者の性別、年齢、熟練度、利き腕など
・予想される使用者の訓練、経験、能力の度合い
・人が機械類の危険にさらされる頻度および期間

●危険源の同定
機械類のすべての危険状態および危険の原因となり得る事態が、同定されなければなりません。例えば、
・機械的危険
・電気的危険
・化学的危険
・物理的危険
・人力による材料供給または取り出し
・据え付け、調整、掃除、保守などの目的で行なう機械類への接近
・人の行為
・作業手順に影響を与える不履行あるいは逸脱
・機械使用者以外の人との干渉
・機械性能の喪失または安全装置に特に関係のある部品の故障
などから危険を予測します。

●リスク見積り
確認された個別の危険に対する部分的リスクと、リスクに影響を及ぼす要因について考慮し、リスク見積りを行ないます。
リスクに影響する要因とは、次の通りです。
・重大度（予想される災害発生の大きさ）
・人が危険にさらされる頻度および期間
・災害の原因となり得る事態が発生する確率
・技術および人の力によって災害を避けられる可能性
（危険の自覚、速度の低減、緊急停止装置、機能が付与されている装置など）

●リスクの評価
機械類が適正な安全レベルに達したか否か決定します。
安全性が不充分であれば、リスクの低減を図ります。

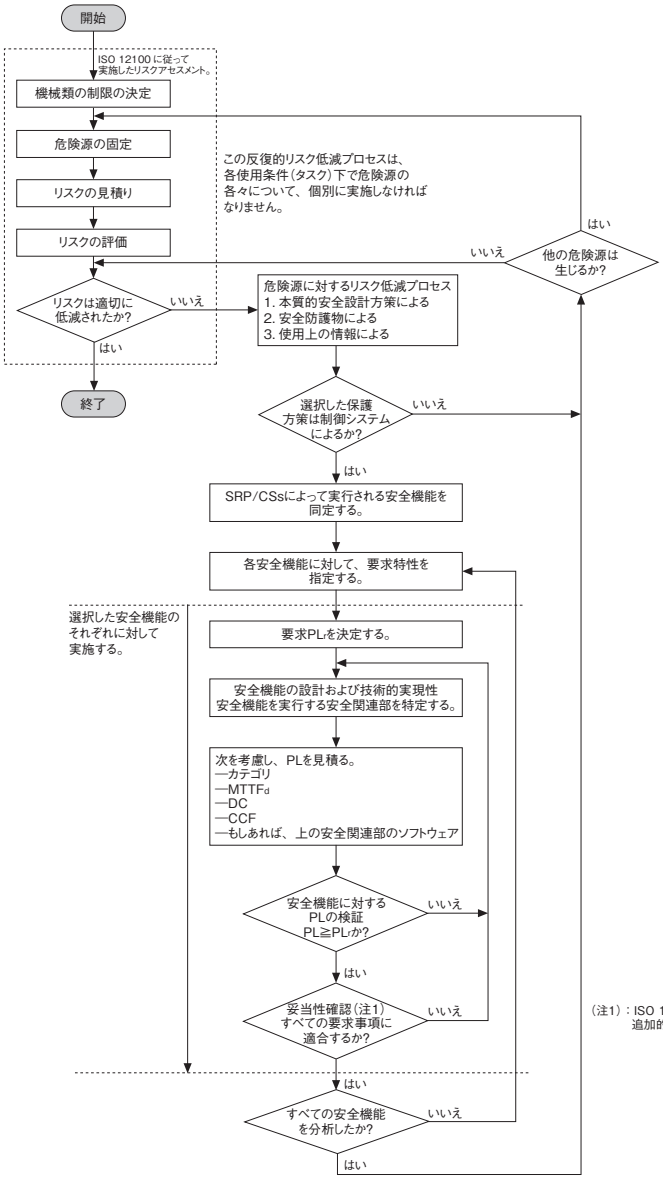
●リスクの低減（安全性達成のための反復処理）
リスクの評価により、リスクの低減が必要な場合は、設計変更、防護ガードや安全装置などの安全防護設置などによる安全方策を実施します。安全方策実施後のリスクの評価で、残留するリスクが受容できない場合は、繰り返し安全方策を実施します。
最後まで残るリスクは、すべて使用者に情報提供と警告を行なわなければなりません。

安全規格

リスクアセスメントと制御カテゴリの評価

ISO 13849-1に基づいたリスクアセスメントおよびリスク低減

制御システムの安全関連部(SRP/CS)は、ISO 12100の原則を十分に考慮し、設計および製作しなければなりません。
また、すべての意図する使用および合理的に予見可能な誤使用を考慮しなければなりません。



(注1):ISO 13849-2で、妥当性確認のための追加的支援策が示される。

パフォーマンスレベルの評価

ISO 13849-1：2006の背景と改定のポイント

はじめに

機械設計の国際的な基準となるISOやIEC規格の中でも最も重要な規格のひとつであるISO 13849-1（機械類の安全制御システムに要求される原則や性能を規定した規格）が、2006年11月に大幅改定されました。従来のISO 13849-1：1999は、「カテゴリ」で安全制御システムを評価してきましたが、ISO 13849-1：2006からは、「PL（パフォーマンスレベル）」によって評価するようになりました。

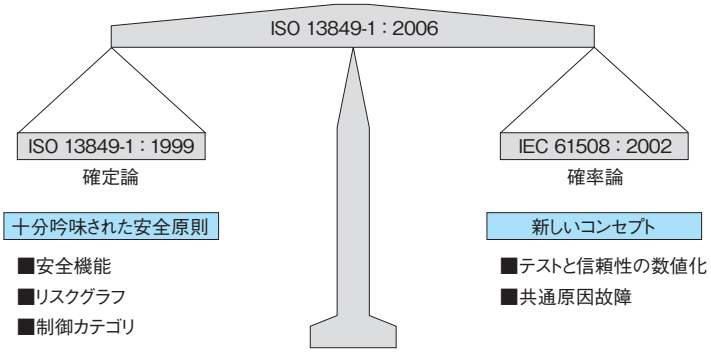
ISO 13849-1改定の背景

従来のISO 13849-1：1999で用いていた「カテゴリ」は、安全関連制御システムのアーキテクチャ（構造）を示していました。これはスイッチやリレーなどに代表される電気機械的部品（非半導体）による確定論的な技術に立脚したものです。
近年の技術の進歩により安全関連の制御システムを構成する部品は、電気機械的部品（非半導体）から電子的部品（半導体）に、制御の方法はハードワイヤによるロジックからソフトウェアよるロジックに移りつつあります。しかし確定論はこれらの部品の「信頼性」や「品質」、ソフトウェアの「信頼性」による安全を考慮することができませんでした。
このような状況の中で、機械類の安全を「信頼性」や「品質」の面から規定しようと、「機能安全規格」と呼ばれるIEC 61508による評価が試みられました。しかしIEC 61508は、原子力や化学プラントも考慮した規格であるため想定範囲があまりにも広く、機械類の安全を評価するには不向きでした。そのため、後に機械類の安全のみを扱うIEC 61508の小型版のような規格IEC 62061が制定されました。
こうして、IECにより機械類の「機能安全」規格が制定されましたが、この規格は「安全関連の電気・電子・プログラマブル電子制御システムの機能安全」を規定したもので、油空圧などの機械類を扱っていないため機械設計者が用いるには不充分でした。またISO 13849-1：1999には「信頼性」や「品質」の概念がなかったため、IEC 61508の「機能安全」の概念を取り入れることによりISO 13849-1：2006として改定されました。ISO 13849-1：2006は、1999年版の「カテゴリ」の概念を基本に残しながら「信頼性」や「品質」の概念を取り入れた、新しい機能安全規格として生まれ変わりました。

改定のポイント

①ISO 13849-1：1999のリスクグラフでは、リスクの見積もりが重症側に比重がありました。（S1を選択した場合、F、Pの選択なし）
ISO 13849-1：2006のリスクグラフでは、リスクの見積もりが均等かつ一義的に求められるようになり、リスクアセスメントをする立場から見て分かり易くなりました。（新旧リスクグラフの比較）
②従来のアーキテクチャ（カテゴリ）による定義に加え、平均危険側故障時間（MTTFd）、診断範囲（DC）や共通原因故障（CCF）を評価する4段階の定義に変わりました。これによって、実際の機械類の使用状況に応じて定量的な評価ができるようになりました。
③リスクアセスメントする立場（ユーザ）から見た要求性能レベルと機械類を設計する立場の目標性能レベルを共有し、指標とすることができます。設計者は、アーキテクチャと構成部品の信頼性の組み合わせにある程度の自由度が持てるようになります。しかしその一方で、安全機能が現場で使用される頻度を想定しなければなりません。

ISO 13849-1：2006の概念



安全規格

パフォーマンスレベルの評価

PL（パフォーマンスレベル）の概念

ISO 13849-1：1999では、予見可能な条件下で制御システムが安全機能を遂行する能力を制御カテゴリB、1、2、3、4で振り分けていました。これに対して、ISO 13849-1：2006では、パフォーマンスレベル（以下、PL）a、b、c、d、eで振り分けられます。PLは、時間当たりの危険側故障確率によりランク分けされます。この危険側故障確率は、ハードウェア並びにソフトウェアの構造（アーキテクチャ）をカテゴリ（Category）、障害の診断範囲（以下、DC）、コンポーネントの信頼性を示す平均危険側故障時間（以下、MTTFd）、そして共通原因故障（以下、CCF）、設計プロセス、運転ストレス、環境条件および運転手順などにより決定されます。

PL（Performance level）
予見可能な条件下で、安全機能を実行する制御システムの能力を指定するレベル。

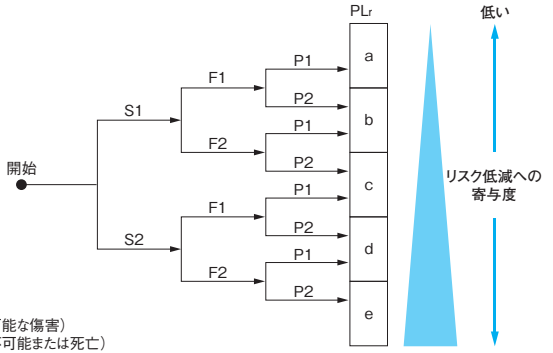
PLの主な決定要素

・カテゴリ（Category）
制御システムの安全関連部のアーキテクチャ（構造）。カテゴリの要求事項はISO 13849-1：1999と基本的には同様ですが、新たにI（入力機器）、L（論理処理）、O（出力機器）の要素を用いて、それぞれのカテゴリの基本的なアーキテクチャ（構造）をより具体的に示しています。
・MTTFd（Mean time to dangerous failure）
危険側故障に至るまでの平均時間。1チャネルシステムが危険側故障を生じないと期待できる動作時間の平均値。
・DC（Diagnostic coverage）の平均
平均診断範囲。検出可能な危険側故障率の合計÷全危険側故障率の合計で算出されます。
・CCF（Common cause failure）
共通原因故障を低減させるような設計手順、工学手法などから定められた値の合計点数。
・系統的故障を防止する方策

新しいリスクグラフと要求パフォーマンスレベル（PLr）の決定

ISO 13849-1：2006では、リスクチャートを用いて、リスク低減を達成するために要求されるPL（PLr）を決定する手法を用いています。リスクチャートを活用し、リスクパラメータ（S、F、P）から、要求される安全制御システムのランクを分ける思想は、ISO 13849-1：1999と同様です。
ISO 13849-1：1999からの変更点は主に2つあります。1つ目は、これまでリスクパラメータのSがS1（軽症）であった場合はリスクパラメータFとPは考慮されませんでしたが、ISO 13849-1：2006ではS1（軽症）の場合もFとPで評価されます。2つ目は分けられたランクごとに要求される安全制御システムの安全機能の遂行する能力の評価指標が、制御カテゴリからパフォーマンスレベル（PL）になりました。

PLr（Required performance level）
要求されるリスク低減を達成するために適用されるパフォーマンスレベル（PL）。



S：傷害のひどさ
S1：軽症（通常、回復可能な傷害）
S2：重傷（通常、回復不可能または死亡）
F：危険源への暴露の頻度および／または時間
F1：まれから低頻度、および／またはさらされる時間が短い
F2：高頻度から連続、および／またはさらされる時間が長い
P：危険源回避また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

パフォーマンスレベルの評価

PL（パフォーマンスレベル）の決定

PL決定の簡易手順：下記、グラフまたは表を用いて4つのパラメータからPLを判定することができます。

グラフを用いた手法

①主にアーキテクチャ　カテゴリ（Category）　5択

B、1、2、3、4

②平均危険側故障時間　MTTFd〔年〕　3択

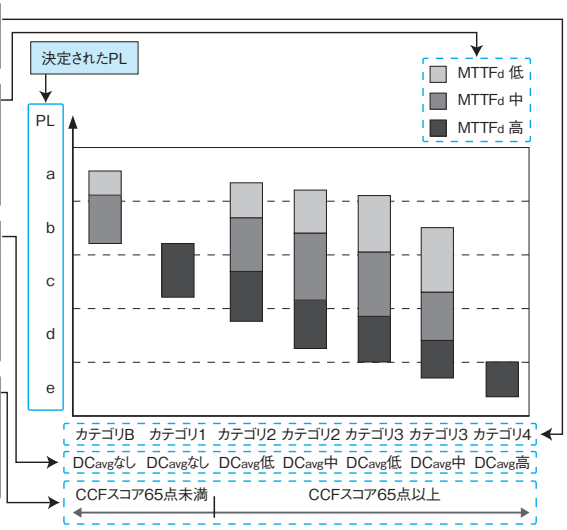
高（High）　〔30年≦ MTTFd ≦ 100年〕
中（Medium）〔10年≦ MTTFd ＜ 30年〕
低（Low）　〔3年≦ MTTFd ＜ 10年〕
※ISO 13849-1：2006 付属書Cを参照

③平均診断範囲　DCavg（DCの平均）〔%〕　4択

高（High）　〔99% ≦ DC〕
中（Medium）〔90% ≦ DC ＜ 99%〕
低（Low）　〔60% ≦ DC ＜ 90%〕
なし（None）〔DC ＜ 60%〕
※ISO 13849-1：2006 付属書Eを参照

④共通原因故障　CCFのスコア〔Yes or No〕　2択

Yes ：65点以上
No ：65点未満
（最大100点）
※ISO 13849-1：2006 付属書Fを参照



表を用いた手法

①主にアーキテクチャ　カテゴリ（Category）　5択

B、1、2、3、4

②平均危険側故障時間　MTTFd〔年〕　3択

高（High）　〔30年≦ MTTFd ≦ 100年〕
中（Medium）〔10年≦ MTTFd ＜ 30年〕
低（Low）　〔3年≦ MTTFd ＜ 10年〕
※ISO 13849-1：2006 付属書Cを参照

③平均診断範囲　DCavg（DCの平均）〔%〕　4択

高（High）　〔99% ≦ DC〕
中（Medium）〔90% ≦ DC ＜ 99%〕
低（Low）　〔60% ≦ DC ＜ 90%〕
なし（None）〔DC ＜ 60%〕
※ISO 13849-1：2006 付属書Eを参照

④共通原因故障　CCFのスコア〔Yes or No〕　2択

Yes ：65点以上
No ：65点未満
（最大100点）
※ISO 13849-1：2006 付属書Fを参照

カテゴリ	B	1	2	2	3	3	4
DCavg	なし	なし	低	中	低	中	高
各チャンネルのMTTFd							
低	a	該当なし	a	b	b	c	該当なし
中	b	該当なし	b	c	c	d	該当なし
高	該当なし	c	c	d	d	d	e

CCFスコア 65点未満
CCFスコア 65点以上
決定されたPL

安全規格

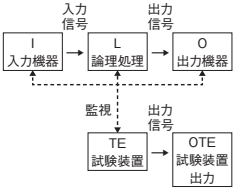
パフォーマンスレベルの評価

①カテゴリ（Category）の決定方法

ISO 13849-1：2006 6.2を参照して決定します。下表はISO 13849-1：2006 6.2の概略をまとめたものです。

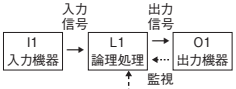
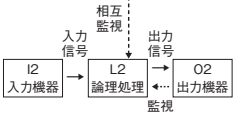
カテゴリ	アーキテクチャ（構造）	要求事項の要約	システムの挙動	安全性の達成に用いる原理	各チャンネルのMTTFd	DCavg	CCF
B		●構成部品、制御システムの安全関連部および（または）保護設備は予想される影響に耐え得るように、関連する規格に従って設計、製造、選択、組み立て、組み合わさなければなりません。 予想される影響には、次のようなものがあります。 ・制動容量およびその頻度に関する信頼性のような予期される操作上のストレス。 ・洗浄機の洗浄剤のような処理材料の影響。 ・機械振動、外部磁界、動力源の中断または妨害のようなその他の関連した外部の影響。 ※カテゴリBに適合する部分には特別な安全方策は適用しません。	●不具合（障害）発生時、安全機能の喪失を招くことがある。	●主に構成部品の選択によって特徴付けられる。	低～中	なし	65点未満
1	入力信号 → 出力信号 I 入力機器 → L 論理処理 → O 出力機器	●カテゴリBの要求事項が適用されなければなりません。 ●安全関連部は、充分吟味された構成部品および安全原則を用いなければなりません。 安全関連の用途のための充分吟味された構成部品とは、次のような構成部品です。 ・従来、同じ適用において良好な結果と共に広く用いられてきたもの。 ・安全関連の適用に対するその適応性および信頼性を示す原則を用いて製作され、検証されてきたもの。 充分吟味された安全原則とは、例えば次のようなものです。 ・「分離による短絡回路の回避」などによる必然的な故障の回避。 ・「構成部品の大型化または定格を下げる」などによる故障可能性の低減。 ・故障時に安全に動作させる例えば、故障時に動力を切り離さなければならない場合は、開回路を確保させる。 ・故障の早期発見。 ・装置を接地することなどにより、故障の結果を制限する。 新たに開発された構成部品および安全原則については、上記の条件を満足する場合、充分に試されたものと同等とみなすことができます。	●不具合（障害）発生時、安全機能の喪失を招くことがあるが、発生する確率はカテゴリBより低い。		高		

パフォーマンスレベルの評価

カテゴリ	アーキテクチャ（構造）	要求事項の要約	システムの挙動	安全性の達成に用いる原理	各チャンネルのMTTFd	DCavg	CCF
2		●カテゴリBの要求事項、および充分吟味された安全原則の使用が適用されなければなりません。 ●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されなければなりません。 安全機能のチェックは、次のように行なわなければなりません。 ・機械の起動時および危険状態が起きる前。 ・リスク査定と操作の種類が定期検査の必要性を示している場合、操作中定期的に。 チェックは、自動式または人により開始できます。 安全機能のチェックの結果は、次のいずれかになるようにしなければなりません。 ・故障が発見されなければ、操作が可能であること。 ・故障が発見されれば、適切な制御作用を開始する出力を発生すること。 この出力は、可能であるならば安全状態を発生しなければなりません。 安全状態を発生することが不可能な場合（例えば、最終のスイッチ装置における接点の溶着）、出力は危険警告を提示しなければなりません。 チェックすることが、危険状態になってはなりません。チェック装置は、安全機能を提供する安全関連部品に組み込むか、または分離してもかまいません。 故障の発見後、安全状態は故障が解消するまで維持されなければなりません。 ※安全機器のチェックは、圧力スイッチまたは温度センサのようにすべての構成部品に適用できないので、カテゴリ2は場合によっては適用不可能です。 ※一般にカテゴリ2は、保護装置および特殊な制御システムにおけるような電子技術で実現可能です。	●チェックの間の不具合（障害）の発生が、安全機能の喪失を招くことがある。 ●安全機能の喪失は、チェックにより検出される。	●主に構造によって特徴付けられる。	低～高	低～中	65点以上

安全規格

パフォーマンスレベルの評価

カテゴリ	アーキテクチャ（構造）	要求事項の要約	システムの挙動	安全性の達成に用いる原理	各チャンネルのMTTFd	DCavg	CCF
3		●カテゴリBの要求事項、および充分吟味された安全原則の使用が適用されなければなりません。 ●安全関連部は、次のように設計されなければなりません。 ・いずれの部品の単一の不具合（障害）も安全機能の喪失を招かない。 ・合理的に実施可能な場合は、常に単一の不具合（障害）が検出される。 ※技術および適用のために必要ならば、形式C規格のメーカは、故障の発見に関するさらに詳細な情報を提供しなければなりません。	●単一の不具合（障害）発生時、安全機能が常に機能する。 ●すべてではないが、不具合（障害）は検出される。 ●検出されない不具合（障害）の蓄積で、安全機能の喪失を招くことがある。	●主に構造によって特徴付けられる。	低～高	低～中	65点以上
4		●カテゴリBの要求事項、および充分吟味された安全原則の使用が適用されなければなりません。 ●安全関連部は、次のように設計されなければなりません。 ・いずれの部分の単一の不具合（障害）も安全機能の喪失を招かない。 かつ ・単一の不具合（障害）は、安全機能に対する次の動作要求時、またはそれ以前に検出される。それが不可能な場合、不具合（障害）の蓄積が安全機能の喪失を招いてはならない。 ・共通モードの不具合を回避するために、多様性による特別な手続きを考慮しなければならない。	●不具合（障害）発生時、安全機能が常に機能する。 ●不具合（障害）はやがて検出され、安全機能の喪失を防止する。		高	高 （故障の蓄積を含む。）	

パフォーマンスレベルの評価

②平均危険側故障時間（MTTFd［年］の平均）の算出方法

(1) 部品ごと

・供給メーカから提供されるMTTFdの値を用います。
・または、ISO 13849-1：2006 付属書CよりMTTFdを決定します。
B10dで規定された場合は、下式でMTTFdを算出します。

$$MTTF_d = \frac{B_{10d}}{0.1 \times n_{op}}$$

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600s/h}{t_{cycle}}$$

B_{10d}：部品の10%が危険側故障に至るまでの平均サイクル数（サイクル）
d_{op}：1年あたりの平均運転日数（d：日）
h_{op}：1日あたりの平均運転時間（h：時間）
t_{cycle}：コンポーネントの連続2サイクルでの開始と開始の間の平均時間（s：秒）

(2) システム全体

・部品ごとのMTTFdから以下により算出します。

直列システムの場合

下式（パーツ・カウント・メソッド）により算出します。

$$\frac{1}{MTTF_d} = \frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}$$

並列システムの場合

・MTTFdが低い部品の値とします。
・または、下式により算出します。

$$MTTF_d = \frac{2}{3}\left[MTTF_{d1} + MTTF_{d2} - \frac{1}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}}}\right]$$

機　種		B_{10d}［サイクル］
セーフティ磁気スイッチ	**BNS260**シリーズ	低負荷時　：25,000,000 最大負荷時：400,000
	BNS36シリーズ	
	BNS120シリーズ	
電磁ロック付セーフティドアスイッチ	**SG-B1**シリーズ	2,000,000
	AZM415シリーズ	NC接点：2,000,000、NO接点：1,000,000（10%抵抗負荷時）
	AZM161シリーズ	NC接点：2,000,000
	AZM170シリーズ	
	TZF/TZMシリーズ	
セーフティドアスイッチ	**SG-A1**シリーズ	2,000,000
	AZ17シリーズ	NC接点：2,000,000、 NO接点：1,000,000（10%抵抗負荷時）
	AZ15シリーズ	
	AZ16シリーズ	
	AZ415シリーズ	
キーセレクタスイッチ	**SG-D1**シリーズ	100,000
セーフティヒンジスイッチ	**TESZ**シリーズ	NC接点：2,000,000、NO接点：1,000,000（10%抵抗負荷時）
	TESシリーズ	NC接点：2,000,000
	T.C236シリーズ	NC接点：20,000,000
イネーブルグリップスイッチ	**SG-C1**シリーズ	2,000,000
ワイヤロープ式非常停止スイッチ	**ZQ**シリーズ	NC接点：100,000（低負荷時） 6,050（最大負荷時）
非常停止スイッチ	**ADRR40RT＋AF10**	NC接点：100,000（低負荷時） 6,050（最大負荷時）
	ADRR40RT＋AF02	
セーフティエッジシステム	**SE-400C**	低負荷時　：20,000,000 最大負荷時：400,000
	SE-100C	
セーフティリレーユニット	**SRB201ZH**	低負荷時（1チャンネル毎）：20,000,000 最大負荷時：400,000
	SRB301ST	
	SRB211ST（V.2）	
	SRB324ST（V.3）	
	AES1337	
	SF-AC	
	AES1235	
ミューティングユニット	**SRB202MSL**	低負荷時（1チャンネル毎）：20,000,000 最大負荷時：400,000
静止モニタユニット	**FWS1205B**	低負荷時（1チャンネル毎）：20,000,000 最大負荷時：400,000
ディレイタイマユニット	**AZS2305**	低負荷時（1チャンネル毎）：20,000,000 最大負荷時：400,000

低負荷：例えば、定格値の20%を意味する。（ISO 13849-2）

安全規格

パフォーマンスレベルの評価

③平均診断範囲［DCavg（DCの平均）］の算出方法

(1) 部品ごと
・すべての自己診断能力を同定します。
ISO 13849-1：2006 付属書Eの表を参照し、
DCを決定します。

(2) システム全体
・部品ごとのDCとMTTFdから下式より算出します。

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \cdots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \cdots + \frac{1}{MTTF_{dN}}}$$

④共通原因故障（CCF）のスコア見積り方法

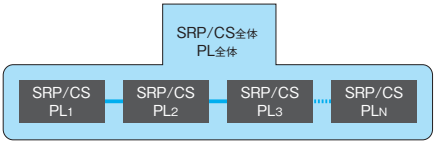
ISO 13849-1：2006 付属書Fの表を参照し、
点数を見積もります。（最大100点）

【分離／隔離】		【アセスメント／分析】	
信号配線の分離	15点	FMEAの実施	5点
【ダイバシティ】		【適格性（能力）／訓練】	
異なる原理を用いた冗長化	20点	設計者／保全者へのトレーニング	5点
【設計／適用／経験】		【環境面】	
例えば、過大圧力や過電圧に対する防護方策	15点	使用環境への対策（EMCなど）	25点
充分に吟味されたコンポーネントの使用	5点	温度、衝撃、振動、湿度など	10点

各グループのPLから全体のPLへの簡易的な決定方法

直列で配置される各グループの制御システムの安全関連部〔以下、SRP/CS（Safety related part of a control system）〕のPLから、
SRP/CS全体のPLの簡易的な決定が下表により可能です。

① 制御システム全体の中で最も低いPL（PL_{low}）を探す。



（例）PL_1=e、PL_2=c、PL_3=c、PL_4=cの場合
PL_{low}=c

② ①で決定した最も低いPLの数（N_{low}）を確認する。

（例）PL_1=e、PL_2=c、PL_3=c、PL_4=cの場合
N_{low}=3

③ 表で制御システム全体のPLを決定する。

（例）PL_1=e、PL_2=c、PL_3=c、PL_4=cの場合
$PL_{全体}$=b

ISO 13849-1：2006 表11より SRP/CSを直列配置した場合のPLの計算
※この表で計算される値は、各PLの中間の信頼性データに基づく。

PL_{low}	N_{low}	⇒	$PL_{全体}$
a	>3	⇒	許容不可
	≦3	⇒	a
b	>2	⇒	a
	≦2	⇒	b
c	>2	⇒	b
	≦2	⇒	c
d	>3	⇒	c
	≦3	⇒	d
e	>3	⇒	d
	≦3	⇒	e

機　種		PL（パフォーマンスレベル）
ライトカーテン	**SF4B**シリーズ **Ver.2**	PLe
	SF4B-Gシリーズ	PLe
	SF4B-Cシリーズ	PLe
	SF4Cシリーズ	PLe
	SF2Cシリーズ	PLe
	SF2Bシリーズ **Ver.2**	PLc
	BSF4-AH80	PLe

機　種		PL（パフォーマンスレベル）
セーフティビームセンサ	**ST4**シリーズ	PLe
セーフティレーザスキャナ	**SD3-A1**	PLd
非接触式セーフティスイッチ	**CSS34**シリーズ	PLe
	MZM100シリーズ	
電磁ロック付セーフティドアスイッチ	**AZM200**シリーズ	PLe
セーフティ漏液センサ	**SQ4**シリーズ	PLe

安全規格

安全インテグリティレベル

安全インテグリティレベル（SIL）の概念

安全インテグリティレベル（SIL：Safety Integrity Level）は、安全制御機能が正しく作動する信頼性を、確率的手法で定量的に規定し、レベル分けする指標です。SILを規定する規格には、IEC 61508、IEC 62061があります。IEC 61508は適用分野が広く、原子力プラント、化学プラントのような、極めて高い安全性を必要とする施設の安全制御まで対象としています。安全機能の作動要求として低頻度作動要求モードおよび、高頻度作動要求または連続モードにより規定され、SIL1～SIL4の4段階で分類しています。IEC 62061では適用範囲を機械類の安全性とすることで、安全機能の作動要求モードを高頻度作動要求モードだけの規定とし、最も高い安全レベルであるSIL4の安全性は要求されないとするなど理解しやすく作成されています。SILでの評価は、複雑な電気・電子の安全システムを得意としますが、非電機系（例：油圧）を含めたシステムには適応できません。

※IEC 61508　電気・電子・プログラマブル電子安全関連系の機能安全
※IEC 62061　機械類の安全性・安全関連の電気・電子・プログラマブル電子制御システムの安全性

SILを決定する安全関連制御機能の目標PFHD

SIL	PFHD
4	$10^{-9} \leqq PFH_D < 10^{-8}$
3	$10^{-8} \leqq PFH_D < 10^{-7}$
2	$10^{-7} \leqq PFH_D < 10^{-6}$
1	$10^{-6} \leqq PFH_D < 10^{-5}$

※PFHD（Probability of dangerous failure per hour）：
安全関連電気制御システムまたはそのサブシステムが、1時間の間に危険側故障を起こす平均確率。〔1/時間〕

PLとの相関関係

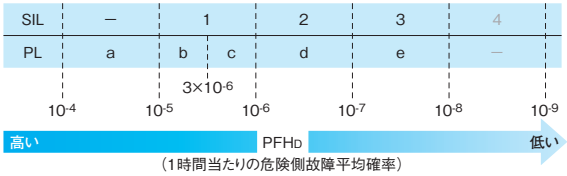
一方ISO 13849-1では、確定論で制御システム安全関連部のアーキテクチャを定義するカテゴリは、油圧・空圧等の非電気系を含む複雑ではない安全システムを得意としています。つまり、IEC 62061は、電気、電子制御系およびプログラマブル電子制御系だけに適用できるものであり、ISO 13849-1は、これ以外の油圧・空圧等の非電気系にも適用できるとしています。
ISO 13849-1：2006では、IEC 62061と同様に信頼性の概念を導入し確率的な要素、つまりSILの考え方を取り入れ、PL（パフォーマンスレベル）での評価となりました。PLはPLa～PLeの5段階で分類されています。
このため機械類の安全システムの評価にはSILとPLを適用対象により使い分けられ、両レベルの共通指標として、PFHD（1時間当たりの危険側故障平均確率）により相関関係が示されており、IEC 62061で認定された安全機器のPFHDを使用し、ISO 13849-1の附属書Kの表によりMTTFdに変換して、ISO 13849-1：2006のPLの選択に使用することができます。

※ISO 13849-1：2006　機械類の安全性ー制御システムの安全関連部

ISO 13849-1におけるPLとSILの関係

PL	SIL（高／継続運転モード）
a	ー
b	1
c	1
d	2
e	3

ISO 13849-1におけるPLとPFHDとの相関関係



（1時間当たりの危険側故障平均確率）

安全規格

停止カテゴリの選定

IEC 60204-1（JIS B 9960-1）に基づいた停止カテゴリ

・停止カテゴリは、機械を安全に停止させるために機械のリスク査定に基づいて、適切に決定されなければなりません。
・機械を停止させる停止機能には、次の3つのカテゴリがあります。

停止カテゴリ	概　要
0	●機械のアクチュエータ（可動部）への電源を瞬時に遮断することによる停止。つまり、制御されない、機械が惰性で動いている可能性がある停止。 ※機械には、それぞれカテゴリ0の停止機能を備えなければなりません。
1	●制御された停止。 機械のアクチュエータ（可動部）には停止するための電源が供給され、停止後に電源が遮断されます。（ブレーキ後に電源を遮断）
2	●制御された停止。 機械のアクチュエータ（可動部）には、電源を供給し続けます。（ブレーキ後も電源を供給）

・機械には、それぞれカテゴリ0の停止機能を備えなければなりません。
・カテゴリ1およびカテゴリ2を備えるのは、機械の安全および機能の要求事項によって必要とされる場合です。
・カテゴリ0およびカテゴリ1の停止は、操作方法に関係なく機能し、カテゴリ0の停止機能が優先されなければなりません。
・停止機能は、関連回路への通電を停止し、関連の始動機能より優先されなければなりません。

非常停止のための追加要求事項

非常停止は、上記の停止の要求事項に加え、次の要求事項があります。

非常停止のための追加要求事項
●非常停止は、すべての運転方法において、他のあらゆる機能および操作より優先されること。 ●危険な状態が発生することが予想される機械のアクチュエータ（可動部）への電源供給は、別の危険を招くことなく、できるだけ早く遮断すること。 （例えば、外部動力が不要な機械的手段による停止、カテゴリ1のための逆相制動） ●リセットによって再起動しないこと。

・必要であれば、追加の非常停止装置を接続する手段を備えなければなりません。
・非常停止は、カテゴリ0またはカテゴリ1の停止として機能しなければなりません。
・非常停止のカテゴリは、機械のリスク査定に基づいて、適切に決定されなければなりません。
・カテゴリ0の停止が非常停止機能に使用される場合は、ハードワイヤによる電気機械的部品のみが使用されなければなりません。さらに、その操作は電子ロジック（ハードウェアまたはソフトウェア）に依存せず、また通信ネットワーク、もしくはリンクを経由した指令に依存されないようにしなければなりません。
・カテゴリ1の停止が非常停止機能に使用される場合は、機械のアクチュエータ（可動部）への電源遮断が最終的に確実に行なわれ、しかも電気機械的部品によって行なわなければなりません。

故障時の基本安全機能

電気機器の故障または乱れが危険状態を招く場合や、機械や加工中の工作物を損傷する恐れのある場合、適切な手段を講じてそのような危険の生じる確率を最小限にする必要があります。
故障時のリスクを最小限にするための手段には、次のようなものがあります。

(1) 実証済みの回路技術および部品の使用
・操作目的の制御回路の結合。
・制御装置（例えば操作コイル）の1つの端子を結合導体に接続し）すべての開閉機能（例えばコンタクタ）を制御電源の非接地側に接続する。
・通電しないで停止させること。
・制御される装置へのすべての充電導体の開閉。
・明確な開放動作をする開閉装置の使用（IEC 60947-5-1）。
・故障が不適当な操作を起こす可能性を低減するような回路設計。

(2) 冗長性を備えること
・部分的または全体的な冗長性を備えることにより、電気回路の1つの単一故障が危険を生じる確率を最小限にすることができます。冗長性は正常運転でも効果的ですが、特殊回路として設計し運転機能が故障したときのみ保護機能を肩代わりさせることもできます。
・正常運転では作動しないオフライン冗長性を使用する場合、適当な手段を講じて、必要な場合はこれらの制御回路が確実に利用できるようにしなければなりません。

(3) 多様性の使用
・種々の動作原理の制御回路および種々のタイプの装置を使用すると、危険を生じる障害および故障の確率を低減できます。
例としては、次のようなものがあります。
1. 通常“開”の接点および通常“閉”の接点を組み合わせてインタロックガードで動作させる。
2. 種々のタイプの制御回路部品を回路に使用する。
3. 電気機械回路と電子回路を組み合わせて冗長性のある構成にする。
4. 電気的システムおよび電気的でないシステム（例えば機械的、油圧、空気圧）を組み合わせて冗長性を機能させて多様性を持たせる。

(4) 機能試験の実施
・機能試験の実施は、自動的に制御システムによって行なうか、手動で検査または試験によって行ないます。実施時期は始業時および一定の間隔をおくか、適宜にこれを組み合わせます。

(5) 接地障害および電圧遮断による誤動作に対する保護
・制御回路の接地障害が原因となって、偶発始動や危険な動きが生じたり、機械の停止が妨害されたりしてはなりません。
・電圧降下または停電が電気機器の機能に不良を起こすおそれのある場合は、不足電圧装置を備え、これによって適切な保護（例えば機械電源の遮断）を設定電圧水準において確実に開始させなければなりません。また、危険な状態を招いたり、機械や加工中の工作物を損傷するおそれがあるため、不足電圧装置が働いた後に自動的に機械を再始動させてはなりません。

米国ロボット規格（ANSI/RIA.15.06-1999）

※最新の規格内容については、ANSI/RIA.15.06-2012にてご確認ください。

産業用ロボットおよびロボットシステムに対する安全要求事項

産業用ロボットに関するすべての要員の安全性を高めるため、ロボット製造、改造、運転、保全や安全装置などに関し具体的に細かく規定し、2002年6月21日以降に製造された、新規ロボットシステム並びに新規ワークセルに対して適用されています。しかし、国際安全規格ISO 12100と大きく異なるものではなく、国際安全規格の考えに影響を受けた作りとなっています。

また、ISO 10218：1992が国際規格として発効され日本でもJIS B 8433として規格化されています。

米国ロボット規格の構成

1. 目的・範囲・適用・適用除外
   1.2 目的
   本規格の目的は、産業用ロボットおよび産業用ロボットシステムの使用に関連して要員の安全性を高めるために産業用ロボットの製造、改造および再組み立て、ロボットシステムの統合／据え付け、並びに安全防護の方法に対する要求事項を規定することである。
2. 参照規格（ISO／IECを参照）
3. 定義（ロボットおよび安全に関する用語）
   3.18 産業用ロボット
   産業オートメーションの用途に用いられ、所定位置に固定する、または移動するために3軸以上がプログラム可能で、自動制御され、再プログラム可能な多用途のマニピュレータ。
4. ロボットの製造・改造・再組み立て
   4.6 ロボットの停止回路
   非常停止はすべての制御に優先し、すべての運動を停止させ、運動源を遮断させること。
   オペレータ制御ステーションの各々に手動の非常停止装置を備えること。ボタンのリセットで再起動しないこと。
5. 安全防護装置の性能に関する要求事項
   5.2 インタロックのための安全防護装置
   故意に無効化できないこと。
   堅牢な取り付けとすること。
   安全性能を保障すること。特にポジティブな引き離し動作によること。
   危険源の抑制時のみ、アクチュエータの解錠を可能とすること。
   安全回路の性能に関して記述した文書を用意すること。
6. ロボットおよびロボットシステムの据え付け
7. 要員の安全防護-序説
8. 要員の安全防護-規定による方法
   8.4 安全防護領域内の要員の保護
   要員が安全防護領域内にいる間、すべての動作または危険なプロセスの再開始を防止する。
9. 要員の安全防護-リスクアセスメントによる方法
10. 要員の安全防護-実施
11. 安全防護装置
    11.2.2 インタロック部
    インタロック付バリアのインタロック部は、身体全体のアクセスの可能性があるとき、動力の利用有りまたは無しによらず、安全防護領域内部から容易に解錠できる。
12. ロボットおよびロボットシステムの保全
13. ロボットおよびロボットシステムの試験、および立ち上げ
14. 要員の安全訓練

ロボット設計に対する要求事項

ISO 12100と同様にまずは設計によるリスクの低減を目指し、それで取り除けないリスクに対し安全防護による対策を行なう。いずれも不可能な場合危険源への警告を行なう。

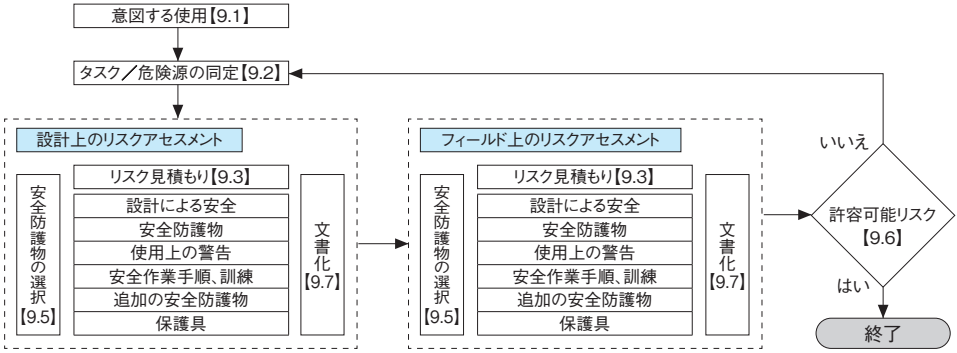
①様々な危険源からの要員保護の達成。
②ロボット軸は駆動源なしで動かせる設計とする。（人が挟まれた場合の解放）
③作動制御装置への要求。
（意図しない操作に対する保護、運転状態表示など）
④ペンダント、数示制御装置への要求。
（自動モードに変更可能、3ポジションイネーブル装置、非常停止回路など）
⑤単一故障で危険源が発生してはならない。
⑥最大移動範囲を持つ一次軸の動作制限に調整可能なメカニカルなストッパをつけるように設計する。
⑦すべてのロボット、付属設備に情報提供の必要がある。
（注意・警告・仕様・認証・保全情報・システム要求事項・故障モード解析など）
⋮
など

安全規格

※最新の規格内容については、ANSI/RIA.15.06-2012にてご確認ください。

リスクアセスメントの考え方

リスクアセスメントは、ロボットおよびロボットシステムの設計開始時に使用者または統合者により実施します。
米国ロボット規格では、設計上のリスクアセスメントだけでなく使用者側でもリスクアセスメントを実施することを指示しています。（フィールド上のリスクアセスメント）



リスク低減カテゴリマトリクス

タスクおよび危険源の組み合わせの各々に対して障害のひどさ、暴露頻度、回避可能性を用いてリスクレベルを確定し、リスク低減のカテゴリを下表に従って確定します。

障害の程度	暴露	回避	リスク低減カテゴリ
S2 重傷	E2 頻繁	A2（不可能）	R1
		A1（可能）	R2A
	E1 希な	A2（不可能）	R2B
		A1（可能）	R2B
S1 軽傷	E2 頻繁	A2（不可能）	R2C
		A1（可能）	R3A
	E1 希な	A2（不可能）	R3B
		A1（可能）	R4

●障害の程度
S1：軽傷（後遺症が残らない）
S2：重傷（後遺症が残るまたは致命的）

●暴露
E1：希な（典型的には、1日または1シフトで1回未満）
E2：頻繁（典型的には、1時間に1回以上）

●回避
A1：回避可能（充分な反応時間またはロボット速度250mm/s未満）
A2：回避不可能（不適切な反応時間またはロボット速度250mm/s以上）

安全防護物選択カテゴリマトリックス

リスク低減カテゴリを用いて、安全防護物および回路に最低限必要な性能を下表に従って確定します。有人プログラムの検証（APV）が行なわれるときには、安全防護物の選択は【10.8プログラム検証中の要員の安全防護】の要求通りでなければなりません。

リスク低減カテゴリ	安全防護物の性能	回路の性能
R1	危険源の除去、または危険源の代替え	信頼できる制御【4.5.4】
R2A	危険源へのアクセスを防止する、または危険源を停止させるための制御装置の構築【9.5.2】	信頼できる制御【4.5.4】
R2B		監視付単一チャネル【4.5.3】
R2C		単一チャネル【4.5.2】
R3A	インタロックなしバリア、クリアランス、手順および設備【9.5.3】	単一チャネル【4.5.2】
R3B		単純【4.5.1】
R4	注意喚起手段【9.5.4】	単純【4.5.1】

- 単一故障で安全機能を損なわない
- 自動監視機能付
- 故障検出時は出力を停止する
- 単一故障は検出される

- 適切な間隔で安全機能がチェックされる
- チェック回路自体が危険状態を引き起こさない

- 安全性が決定されたコンポーネントを含み、製造者で推奨、証明済みの単一の回路設計

- 単純な単一チャネルシステム

MEMO