Safety Compendium

PILZ
THE SPIRIT OF SAFETY

機能安全規格の適用のために




Safety Compendium

Safety Compendium

1

序文

1 序文

1 序文

いつも当たり前に存在すると思われていて、なくなって初めてその大切さに気づくもの、それが安全です。安全は、人や機械、環境を守るものです。

第 1 次産業革命のさなかの 1787 年、エドモンド・カートライトが最初の力織機を導入したことが機械化の歴史の始まりとなりました。当時、何よりも求められていたのは生産性の向上でした。織工の安全を気にかける者はほとんどいなかったのです。これとは対照的に、今日では、生産プロセスの効率と人の安全の両方に等しく目が向けられています。

したがって、この Safety Compendium では、実際の規範的原則や技術的原則を伝えるだけでなく、安全性と経済性の間の数多くの関係を明らかにすることも重要な要素となっています。古い格言にある通り、最初から安全を考慮に入れて正確に設計すれば、効率的な手順や、利用者の高い支持はおのずと達成されるのです。

この第 5 版は、新たに作成されたものではなく、更新バージョンです。現在では、標準的な著作物として認識されるようになったこの Safety Compendium を、当社のエキスパートが拡張し、「Safety in Industrie 4.0」や「人とロボットの協働」などの最新トピックを盛り込んでいます。

究極的には、将来、スマートファクトリーの生産プロセスを決定するのはデジタルデータとその効率的なやりとりである、ということになるでしょう。この分野では安全な通信に対するニーズが高まっています。安全な通信には、機械の安全とデータや IT に関するセキュリティの要件の両方が含まれます。そして、最後に、スマートファクトリーにおいては、人間の役割に対する考え方が変わりつつあります。人間だけが持つスキルが、生産性の向上とさらなる効率化に寄与することになります。これは、ロボット工学などの多くの分野で、人が今以上に機械に接近すること、あるいは人と機械が作業スペースを共有することを意味します。この Safety Compendium では、このような状況で「安全」に対して求められる要件を明らかにするとともに、その要件を満たす方法について説明しています。

「安全」はもはや、効率性や使いやすさと対立する規範的義務に過ぎない、とは見なされなくなりました。今日ではむしろ、成熟した安全性は、生産を可能にし、効率を高めるために極めて重要な必要条件となっています。

この精神にのっとり、この Safety Compendium をお読みいただくことが生産的な経験となることを、心から願っています。

Renate Pilz
経営パートナー
Pilz GmbH & Co. KG

1.1 著者

Christian Bittner は、Pilz GmbH & Co. KG 内のコンサルティングサービスグループのグループマネージャで、EN ISO 12100 の規格委員会の委員などを務めています。直接お客様に接する立場にあり、リスクアセスメントの実行や、安全コンセプトの策定、CE マーキングやその他の安全サービスの創出を担当しています。

Holger Bode は、Pilz GmbH & Co. KG のプレスワーキンググループでプレスのアップグレードや新しい取り付けに関する国際プロジェクトの企画を担当しています。職務には、全面移行対策の策定や、制御コンセプト、ハザードアセスメント、安全コンセプトの創出が含まれます。また、Pilz GmbH & Co. KG の認証検査機関の品質マネージャであり、マネジメントチームの一員でもあります。

Arndt Christ は、Pilz GmbH & Co. KG のカスタマーサポート部長です。この部門内のテクニカルサポートやコンサルティングユニットなどのグループの責任者であるとともに、システム統合やトレーニングチームの責任者でもあります。安全関連のあらゆるテーマに関するお客様の要求を熟知し、安全技術分野でユーザフレンドリな実装を保証しています。

Roland Gaiser は、Pilz GmbH & Co. KG で発展中のアクチュエータシステム部門の部長です。また、エスリンゲン大学のメカトロニクス･電気工学学部で、システム開発やシミュレーションについての講義を行っています。アクチュエータシステムの基本的開発の分野について広範な知識を有しています。

Andreas Hahn は、Pilz GmbH & Co. KG の製品マネジメントにおいてネットワーク、制御システム、アクチュエータ技術を担当するシニアマネージャです。規格委員会の委員や、各種団体のワーキンググループのメンバーも務めています。オートメーションソリューションの設計において、長年の経験を有しています。

1.1 著者

Jurgen Hasel は、Festo Didactic SE のトレーナー兼コンサルタントです。セミナーでは、空圧、電気式空圧、バルブ端末、安全技術に重点を置いています。以前は、Festo AG の開発部門に所属していました。数年間にわたり、Pilz GmbH & Co. KG のトレーニング部門と密接に連携しています。ピルツでは、製品中立なトレーニングの一環として、TÜV Nord 認定 CMSE (Certified Machinery Safety Expert ／認定機械安全エキスパート) コースを教えています。

Thomas Klindt 教授／博士は、NOERR 国際法律事務所のパートナーであり、バイロイト大学の製品および技術法の名誉教授でもあります。国内外の製造物責任訴訟手続きや製品リコール、損害賠償請求を監督する、同事務所内部の製品安全および製造物責任プラクティスグループに所属しています。

Michael Moog は、Pilz GmbH & Co. KG の標準化スペシャリストとして、国際規格委員会の業務の調整を担当しています。自身も規格委員会で活動し、規格の理論的研究と実用的解釈を統合することで、お客様やピルツ内部をサポートしています。特に、世界中で遵守される安全記アックや製品規格、これらに対応する各国の法的枠組みを扱い、「Approval Procedures for Plant and Machinery in North America (北米における設備と機械の認証手続き)」などのセミナーでその知識を広めています。

Alfred Neudorfer 博士は、ダルムシュタット工科大学の機械工学部で講師を務めていました。日本の長岡技術科学大学でも安全技術の客員教授を務めました。安全関連製品の設計を主題とした講義やセミナー、技術論文を多数手がけています。

Andreas Schott は、Pilz GmbH & Co. KG 内のトレーニングおよび教育部門の責任者です。グループマネージャとしてチームと協力し、製品中立コースと製品別コースの両方で教育的かつ実用的な価値の高いトレーニングコンセプトを生み出すことに取り組んでいます。州認定の電気エンジニアおよびソフトウェアプログラマとして長年の経験があり、安全技術に関するお客様の実用的な要件に精通しています。

1.1 著者

Eszter Sieber-Fazakas (法学修士) は、NOERR 国際法律事務所の弁護士で、同事務所内の製品安全および製造物責任のプラクティスグループの一員です。このグループは国内外の製造物責任の訴訟手続きや製品リコール、損害賠償請求を監督しています。

Klaus Stark は、Pilz GmbH & Co. KG の革新マネジメント部門の責任者です。1996 年以降、製品マネジメント部長を務めていましたが、2008 年に国際営業部長の職を引き継ぎました。ZVEI の「Safety Systems in Automation (オートメーションにおける安全システム)」技術委員会の委員長や、技術イニシアチブのスマートファクトリー KL e. V. の取締役を務めるなど、オートメーションを支援する各種の委員会に積極的に関与しています。

Jochen Vetter は、Pilz GmbH & Co. KG でロボットサービスのチームリーダーをしています。直接お客様に接する立場にあり、HRC に関するサービスの実装を担当し、HRC アプリケーション向けのリスクアセスメントと安全コンセプトの創出に携わっています。また、HRC アプリケーションの普及を受けて、TS 15066 に準拠した生体力学的制限値の技術測定チェックも担当しています。

Gerd Wemmer は、Pilz GmbH & Co. KG のカスタマーサポート部門のアプリケーションエンジニアです。機械製造業者からエンドユーザまで、幅広いお客様向けのコンサルティングやプロジェクトエンジニアリング、安全コンセプトの作成を担当し、長年にわたる安全技術の実地経験があります。

Harald Wessels は、Pilz GmbH & Co. KG の製品マネジメントにおいて製品横断的な問題を担当する部門マネージャを務めています。産業アプリケーションにおける通信を扱う国際規格委員会への参加などが担当業務です。オートメーションで使用するフィールドバスシステムやネットワークに関して広範な知識を有しています。

1.1 著者

Matthias Wimmer は、規格や規制に関し、十分な情報に基づいて対処できるようにするためにピルツの規格グループ内で活動しています。国際規格ワーキンググループの ISO/TC199/WG8 のメンバーであり、機能安全の規格 (EN ISO 13849-1 を含む) の開発の方向づけにおいて重要な役割を果たしています。また、ピルツアカデミーのトレーニングコースやセミナーを通じ、社内外の幅広い聴衆に知識を広めています。

Michael Wustlich は、Pilz GmbH & Co. KG でソフトウェア、アプリケーションおよびテスト部門のグループマネージャです。標準化された認定製品の形でユーザレベルの安全関連ソフトウェアを開発する業務などに携わっています。チームとともに、全製品グループ向けの体系化されたアプリケーションテストの仕様と設計を担当しています。

2

製造物責任

2 製造物責任

欠陥製品に対する責任は、欧州の製造物責任指令 85/374/EEC により、欧州において整合化されました。この法規制は、1990 年 1 月 1 日に施行されたため、この時点以後に市場に投入された製品に対してのみ有効です。判例法に基づき策定されたそれ以前の製造物責任法は、この指令によって停止されていないため、製造物責任指令の規定は、それ以前の法の規定に加えて適用されます。これは、ドイツの製造物責任法だけでなく、各加盟諸国の法律についても同様です (製造物責任指令の第 13 条)。

製造物責任指令は、加盟諸国が製造物責任に関する国内規制を施行することに関し、大幅な選択の余地を残しています。例えば、これは、開発リスクに対する責任を盛り込むオプションについて適用されます (製造物責任指令の第 15 条第 1 (B) 項)。ルクセンブルクとフィンランドに加え、限定的な範囲でフランスとスペインが、このオプションを行使しました。製造物責任指令が最小限の整合化のみにとどまるものかどうかという疑問については、欧州司法裁判所 (ECJ) は、一貫性のある判例法に従って、完全な整合化という立場を取っていることに留意する必要があります。したがって、加盟諸国は、消費者保護のために、同指令から逸脱して EU の法律に定められた規格を超えて製造物責任を拡大適用することを禁じられています。

法的側面に関するこの ECJ の判決にもかかわらず、EU の製造物責任指令は、依然として EU 加盟各国で国内法として一律に導入されていません。

市場参入時には、これに加え、EU 加盟各国の国内の契約／責任／民事法に関する製造物責任面をさらに考慮に入れる必要があります。

本 Safety Compendium では、現在の EU 加盟 28 か国のこのような複雑な法的枠組みについて取り上げることはできません。本書の主たる目的は、欧州の機械安全に関する基礎知識を伝達することです。

3

規格、指令、法律

3 規格、指令、法律

3 規格、指令、法律

3.1 欧州連合 (EU) 域内の規格、指令、法律

欧州連合では、ますます緊密な統合が進行しています。これは、機械製造業者にとっては法律、規則、規制のいっそうの整合化を意味します。少し前までは、各国が日常生活の様々な分野や経済に関する独自のガイドラインを発行していましたが、今日では、欧州域内の規制は標準化の一途をたどっています。

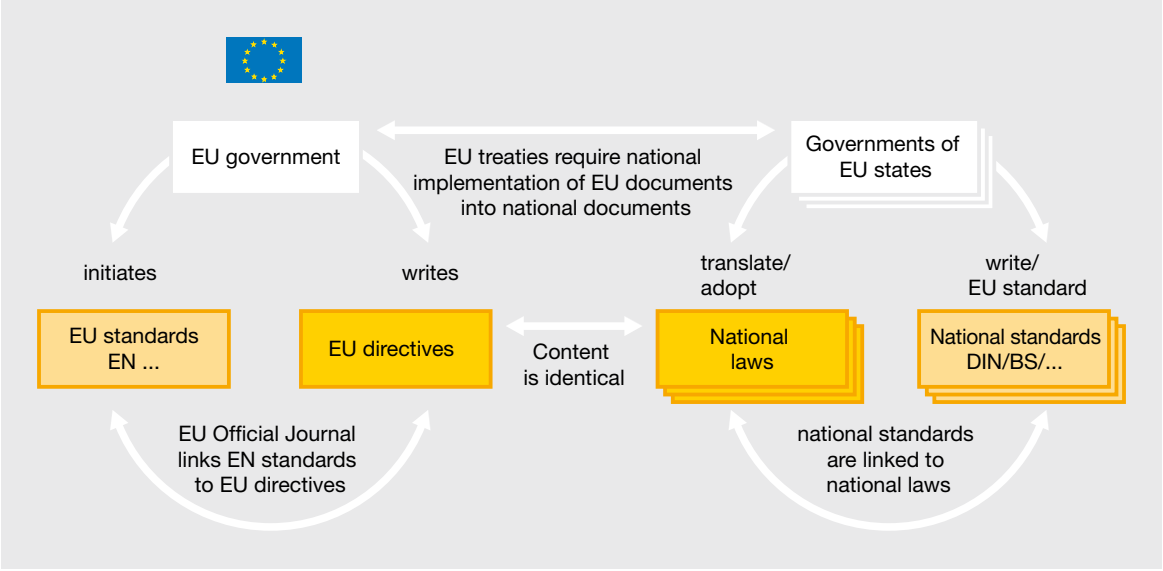
欧州の法律、指令、規格は、どのように関係しているのでしょうか？

まず、EU は、指令を通じて一般的な安全目標を明確に示します。これらの安全目標は、より明確に定める必要があり、規格を通じて実際の規定が定められます。

EU 指令は通常、具体的な問題を扱います。指令自体が個人や企業に直接影響することはありません。指令は、EU 各国の合意を通じてのみ効力を生じ、EU 域内の各国で国内法に組み込まれます。EU 各国では、法律や規制は関連する EU 指令を参照するため、指令が国内法のレベルに格上げされます。指令が採択されてから、国内法に組み込まれるまでの間、移行期間が置かれることはもちろんです。指令は、この期間中に各国の国内法に組み込まれます。しかし、ユーザにとって通常、これは重要ではありません。なぜなら、指令自体がそれぞれの有効期限を明確に示しているからです。したがって、これらの文書のタイトルに「指令」と記述されていても、EU 域内では実務的に法律のレベルになります。

法律と指令の関係は、上記の通りですが、規格の問題については、これから説明します。

規格自体は、読むと興味深いものですが、EU 官報で発行されるか、国内の法律または規制によって参照されるまで、それだけでは法律との直接の関連性はありません。これらは、規格が「適合性の推定」を取得するために使用できる発行物です。「適合性の推定」とは、製造業者が、規格の仕様に従っている限り、規格の対象となる、規格に対応する指令の要件を満たしていると見なすことができることを意味します。そのため適合性の推定は、言わば適切な行為を確認するものです。公式かつ法的には、これは立証責任の転換と呼ばれます。製造業者が整合規



EU 域内の整合規格と法律の関係

3.1 欧州連合 (EU) 域内の規格、指令、法律

格を適用している場合に、何らかの疑いがあるときは、不法行為が証明される必要があります。製造業者が整合化された規格を適用していない場合、その製造業者は、指令に準拠していることを証明する必要があります。
製造業者が規格に準拠していないとしても、不適切な行為を行ったとは必ずしも言えません。特に、革新的な産業では、関連規格が存在しない、あるいは不十分な可能性があります。その場合、製造業者は、関連指令の安全目標に準拠するために必要な注意を払ったことを独自に立証する必要があります。通常、このような方法はより複雑ですが、特に革新的な産業では避けられないことがあります。

EU がすべての規格を官報で発行しているわけでないために、多くの規格が依然として整合化されていないことは、ここで強調しておく必要があります。そのような規格は技術的に大きな関連性があると見なされる場合でも、適合の推定はありません。但し、EU 官報に記載されていない規格が、整合化と同等のステータスになることがあります。例えば、既に整合化されている規格が関連する規格を参照する場合などです。EU 官報に記載されていないその規格は、言わば非公式な手段を介して整合化されることになります。

3.2 CE マーキング

3.2.1 機械安全の基礎 : 機械指令と CE マーク

機械指令 (MD) は、欧州域内の貿易障壁を取り除き、自由な域内市場を実現することを目的に、1993 年に批准されました。機械指令は、2 年間の移行期間を経て、1995 年 1 月 1 日に法的拘束力を生じました。これは、人と機械の相互作用に関する標準化された安全衛生要件を定めており、機械安全に関して存在する各国の数多くの規制に取って代わっています。機械指令 2006/42/EC は、2009 年 12 月 29 日から適用されています。

CE マークの「CE」は、「Communauté Européenne」(欧州共同体) を表しています。製造業者は、自社の製品に関連する欧州域内市場の指令をすべて考慮し、該当する適合性評価手順をすべて適用したことを証明するために、このマークを使用します。CE マークが貼付された製品は、国内規制を考慮せずに輸入および販売することができます。そのため、CE マークは「ヨーロッパへのパスポート」と呼ばれます。

一般的に言うと、新しいコンセプト (「ニューアプローチ」) に基づく指令はすべて CE マーキングについて定めています。ある製品が、CE マーキングについて定めた複数の指令の適用範囲に該当する場合には、CE マーキングは、その製品がそれらすべての指令の規定に準拠していると推定されることを示します。

3.2.2 法的原則

CE マーキングの貼付義務は、CE マーキングについて定めた指令の適用範囲に該当する製品で、単一市場に投入されるすべての製品に適用されます。したがって、CE マークは、指令の適用範囲に該当する以下の製品に添付すべきです。

- 製造国が加盟国であるか第三国であるかにかかわらず、すべての新品製品
- 第三国から輸入された使用済み製品、および中古製品
- 大幅に改造されており、新品の製品として指令の適用範囲に該当する製品

これらの指令では、特定の製品を CE マーキングの適用対象外としている場合があります。

製造業者は、自社製品が関連指令の要件を満たしていることを示すために EC 適合宣言書を使用します。

以下の情報は、機械指令の観点から CE マーキングについて説明することを目的としています。

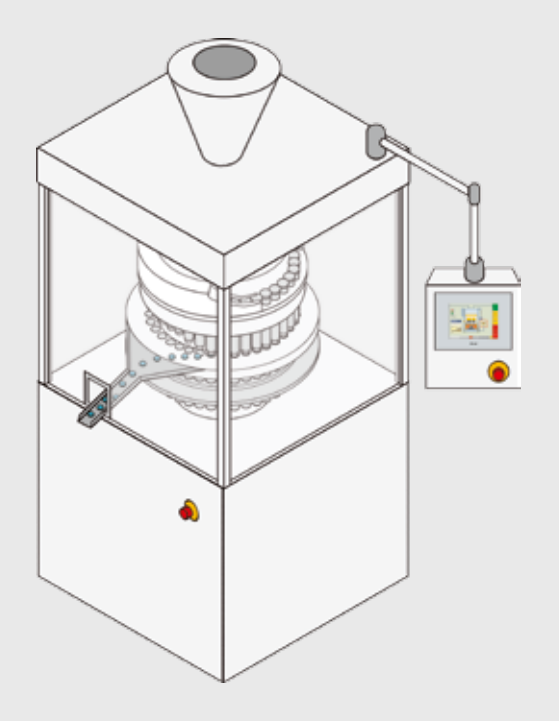
3.2 CE マーキング

3.2.3 機械の CE マーキング

3.2.3.1 機械とは？

以下は、機械指令における機械の定義の1つです。

連結された部品や部分から成る組立て品で、少なくともその 1 つ以上が動き、全体で特定の用途を満たすもの (機械指令の第 2 条を参照)。



機械指令における機械の例

機械指令では、以下も機械と見なされます。

- 機械または複雑な設備から成る組立て品 (複雑な設備には、複数の機械から成る生産ラインや特殊用途機械が含まれます)
- 安全部品 (どの部品を安全部品に分類するかという問題には、大いに議論の余地があります。機械指令の附属書 V には、極めて包括的な安全部品のリストが記載されています。)
- 機械の基本機能を変更することができる、互換性のある機器
- 機械を組み立てるために、他の機械／機械部品に組み込まれる予定の半完成機械

3.2.3.2 設備と機械の CE マーキング

機械指令によると、機械製造業者とは、様々な原産地の機械や機械部品を組み立てて、市場に投入する者を言います。

製造業者は、実際の機械製造者である場合もあれば、機械の運用者 (機械を改造した場合には、それによって製造業者となる) の場合もあります。組み立てられた機械の場合には、各種の機械部品が新しい機械を構成するように各種の機械から新たな設備を組み立てた製造業者、組立て業者、プロジェクトマネージャ、エンジニアリング会社、あるいは作業者自身であることもあります。

しかし、機械指令によると、機械の設計と製造に責任を負うのは、1 社 (1 人) の製造業者に限られます。この製造業者またはその法定代理人は、設備全体の管理手順を実施する責任を負っています。この製造業者は、製品を市場投入するために必要な以下の手順について責任を負う法定代理人を指名することができます。

- 設備の技術資料の作成
- 技術資料の発行
- 設備の取扱説明書の提供
- 設備の適切な位置への CE マークの貼付、および設備全体に関する EC 適合宣言書の作成

3.2 CE マーキング

製造業者は、契約の作成過程や部品の要件マニュアルにおいて、早期に安全面を考慮することが重要です。これらの文書は、機械のパフォーマンスの観点からのみ作成してはなりません。製造業者は、技術資料の全体について責任を負い、各サプライヤがこのプロセスで引き受ける部分を決定する必要があります。

3.2.3.3 欧州経済領域での機械の使用

製造場所や製造日にかかわらず、1995 年 1 月 1 日以降に初めて欧州経済地域で使用されるすべての機械には、EU の機械指令が適用されるため、CE 認定を受ける必要があります。

3.2.3.4 組立て機械

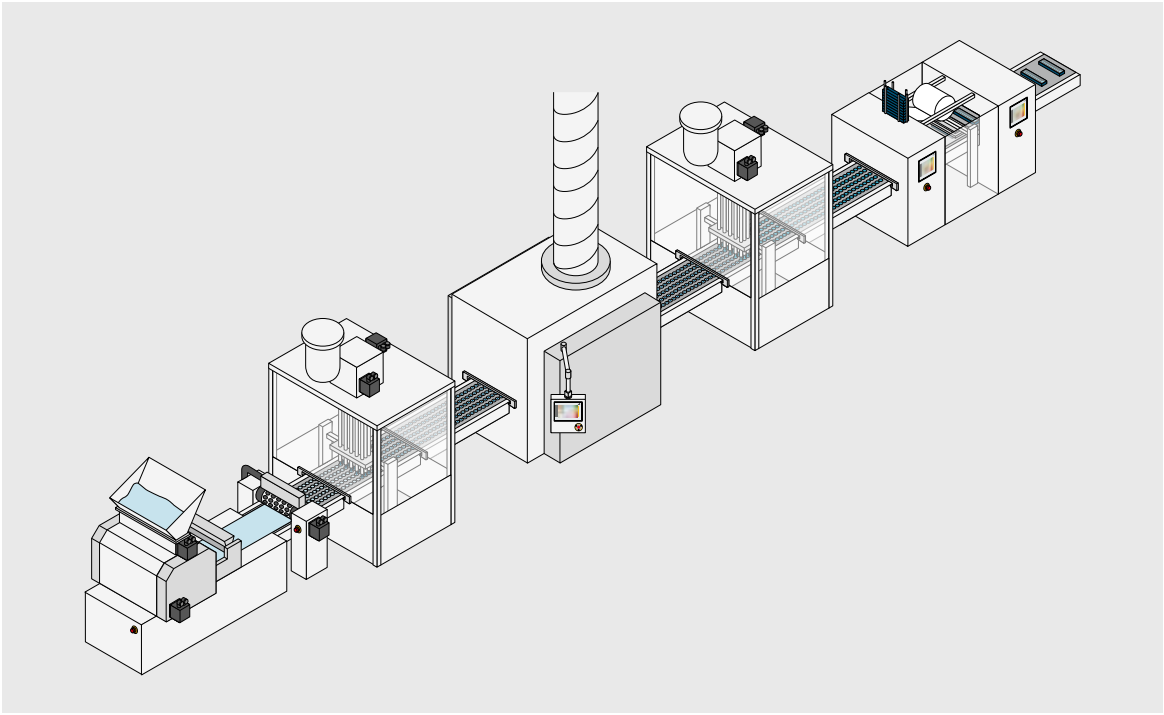
大規模な生産ラインでは、機械は、個別の機械を複数組み合わせて組み立てられた機械で構成される場合が多くあります。個々の機械にそれ自体の CE マークが貼付されている場合でも、設備全体の CE マーキングプロセスを経ることが必要になります。

3.2.3.5 EU 域外の国からの機械の輸入

EU 域内で使用するために第三国から機械を輸入する場合には、EU 市場への投入時にその機械が機械指令に準拠している必要があります。欧州経済領域内で初めて機械を市場投入する者は誰でも、適合を証明するために必要な文書を持っているか、またはその文書を入手できる必要があります。これは、取り扱う機械が「古い機械」であるか「新しい機械」であるかにかかわらず、適用されます。

3.2.3.6 自己使用の機械

機械指令は、自身が使用するために機械を製造するユーザにも、機械指令の準拠を義務付けています。自由貿易という観点では、(機械を売買するわけではないので) 何ら問題はありませんが、機械指令は、このような新しい機械の安全レベルが、市場投入されている他の機械の安全レベルと同等であることを保証するために適用されます。

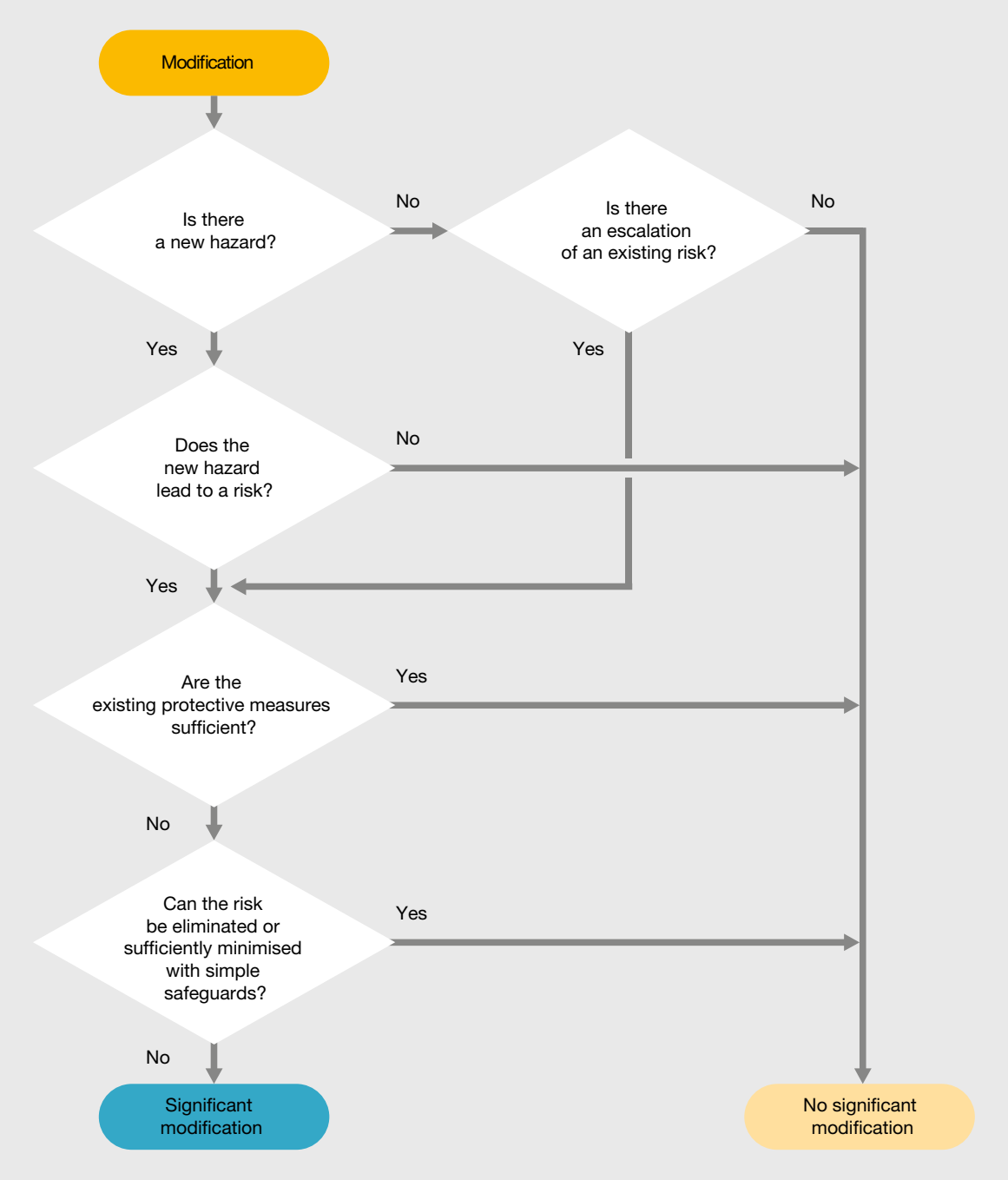


個々の機械および設備全体の CE マーキング

3.2 CE マーキング

3.2.3.7 機械のアップグレード

基本的に、機械指令は、新しい機械に対する要件を定めるものですが、新しいハザードが予期される程度に機械が改造された場合には、そうしたアップグレードが大幅な改造と見なされるかどうかを判断するために分析を実行することが必要になります。これに該当する場合には、新しい機械と同様の対策が講じられます。



「機械の大幅な改造」の決定木、出典： 連邦労働社会省

3.2 CE マーキング

3.2.3.8 連結された機器

ある機械に生じたイベントが別の機械に安全関連の影響を及ぼす場合には、そのシステムは、もはや単一の機械と見なすことはできません。

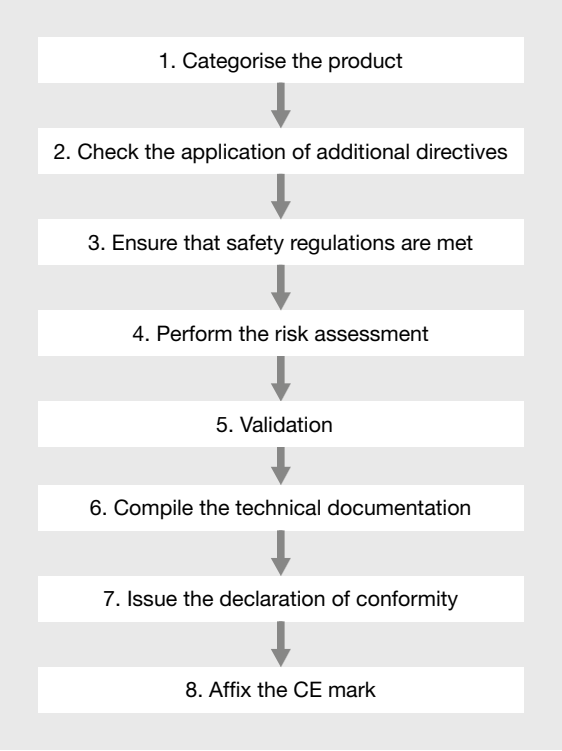
これには、次のような基本原則が適用されます。連結された設備は、(特に、機械指令に関する) 最新の法的ステータスに準拠しなければならず、設備全体に対して適合性評価手順を繰り返す必要があります。

通常、新しく追加された機械や、新しい機械と既存の機械の間のインタフェースは、適切な安全対策を見極めるために、まずリスクアセスメントを受ける必要があります。これに基づいて、安全コンセプトが、安全設計 (安全要件の仕様) やシステム統合とともに策定されます。このプロセスは、実施された安全対策がすべての要件を満たしていることを証明するための安全機能の妥当性確認によって完了します。連結された機器の場合にも、このプロセスは、システム全体に対する EC 適合宣言書で終了する必要があります。

異なる規格を参照して製造された新しい機械に既存の機械を連結する場合は、独特の問題が存在します。特に、EN 954-1 に基づき製造された機械が、13849-1 に基づき製造された別の機械に連結される場合には、これが該当します。EN 954-1 は、2011 年 12 月 31 日まで有効でした。これには、安全技術の統合が含まれていますが、部品の妥当性確認は含まれていません。現行規格の EN ISO 13849-1 は、安全機能の妥当性確認を要求しています。この場合、両方の機械の安全機能に関するデータは形式が異なるため、連結された新しい機械の妥当性確認はさらに困難になります。経験豊富なピルツは、このようなケースでサポートを提供することができます。ピルツは、法定代理人として、常に現行規格を考慮に入れながら、第三者に代わって EC 適合性評価手順を実施します。

3.2 CE マーキング

3.2.3.9 CE マークを取得するまでの 8 ステップ



ステップ 1: 製品を分類する

CE マーキングプロセスは、製品の分類で始まります。以下の質問に回答する必要があります。

- その製品は機械指令の対象となりますか？

ここでは、機械指令 2006/42/EC によって (以前の規格とは異なり) 新たに導入された製品 (圧力容器、蒸気ボイラ、ケーブル鉄道など) がある一方で、除外された製品 (家電機器、オフィス機器など) もあることに留意することが重要です。

- その製品は機械指令の附属書 IV に列挙されていますか？

機械指令の附属書 IV は、プレス、木工機械、運搬用エレベータ等、「特に危険」と見なされる機械を列挙しています。この場合、CE マーキングと適合性宣言では特別な要件を満たす必要があります。

- その機械は、サブシステムまたは半完成機械ですか？

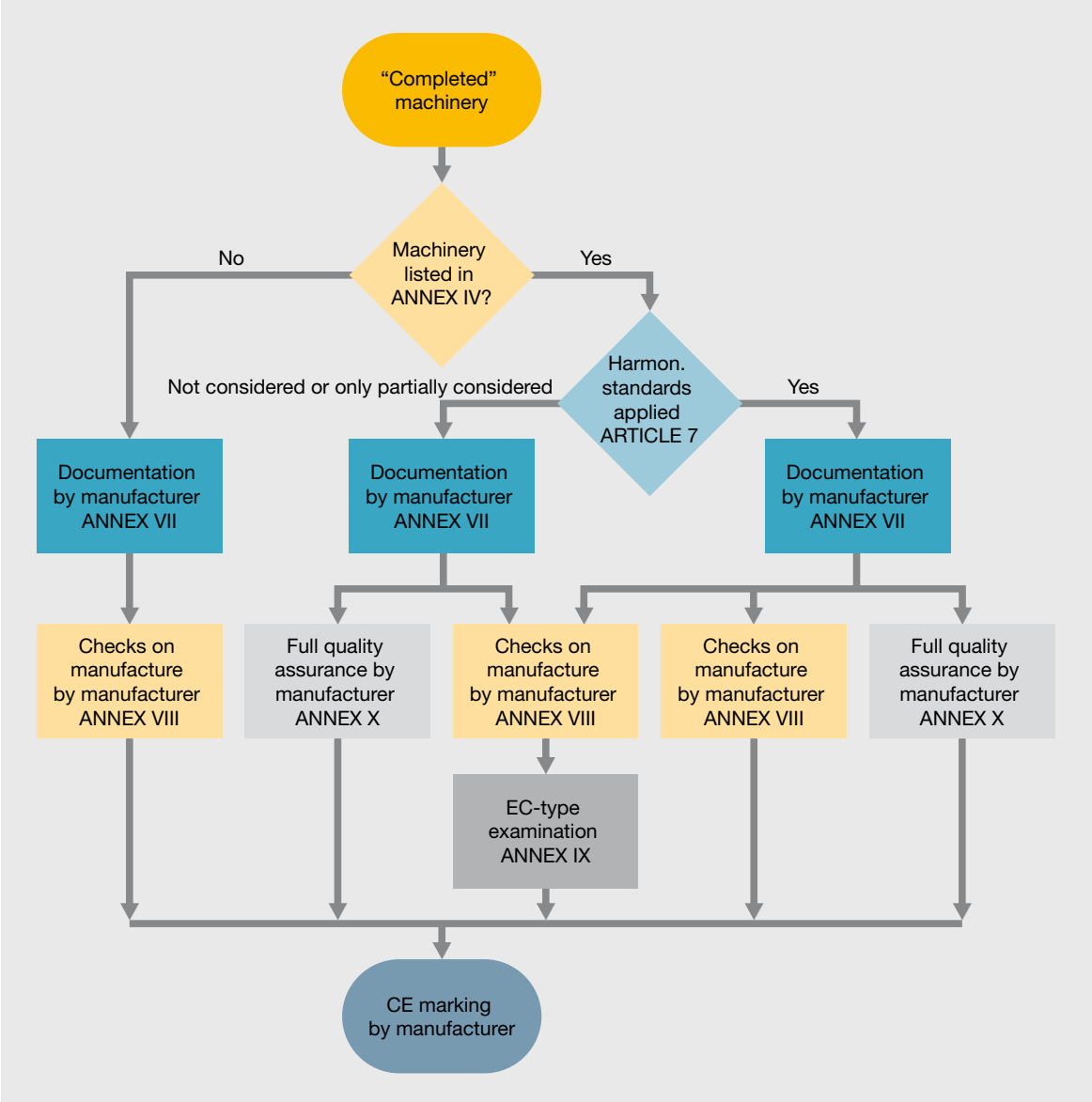
製造業者は、機械指令の附属書 I の全範囲を満たす作動可能な機械に関する EC 適合宣言書を発行します。附属書 I の全範囲をまだ満たすことができないロボットなどのサブシステムの場合には、附属書 II の B に従って組込み宣言書を発行します。

機械指令 2006/42/EC が有効になった瞬間から、すべての半完成機械は、附属書 II に従って組込み宣言書を添付する必要があります。同時に、製造業者はリスクアセスメントを実行するとともに、附属書 VI に適合する組立て説明書を提供する必要があります。このような機械は不完全であり、単独では使用できないため、製造業者の宣言書または組込み宣言書によって、事実上、このサブシステムの使用は禁止されることになります。

3.2 CE マーキング

▸ それは安全部品ですか？

安全部品は、機械指令 2006/42/EC に適合する機械と見なされるため、CE マークを付与されます。



新機械指令に基づき導入される可能性のあるアセスメント手順

3.2 CE マーキング

ステップ 2: その他の指令の適用を確認する

機械に別の面を対象とする他の EU 指令が適用されるだけでなく、その EU 指令にも CE マークの貼付が定められている場合には、CE マークを貼付する前に、これらの指令の規定を満たす必要があります。例えば、機械に電機機器が含まれるときは、多くの場合、低電圧指令が適用され、さらに、EMC 指令が適用される可能性もあります。

ステップ 3: 安全規制への準拠を確認する

機械指令の附属書 I に準拠して本質的安全衛生要件を満たすことは製造業者の責任です。これらの要件に関する記述はいくらか抽象的ですが、具体的な詳細は、EU 規格を通じて定められています。

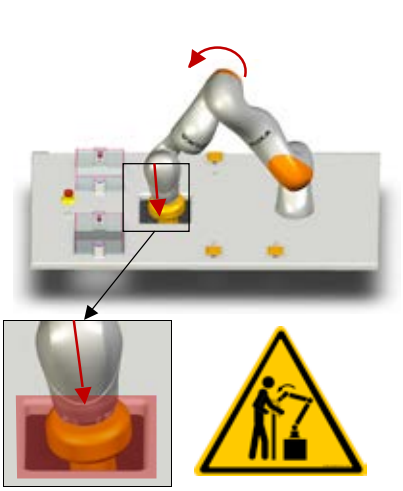
EU は、指令と関連整合規格のリストを公開しています。これらの規格の適用は任意ですが、準拠することで、規制に対する適合性の推定を取得することができます。その結果、要求される証拠の量を大幅に削減でき、リスクアセスメントを組み込みために必要な労力が大幅に軽減されます。

3.2 CE マーキング

ステップ 4: リスクアセスメントを実行する

PILZ
THE SPIRIT OF SAFETY

Pilz GmbH & Co. KG

Hazard Identification		Hazard No:	2.14
Title	Hazards generated by quasi-static contact between the robot and parts of the system		
Location	Robot, robot area (working range of the robot)		
Impact of hazard	Finger, Hand ND		
Life phase	Normal operation, setup, maintenance, servicing and repair		
Activity	Automatic mode, semiautomatic mode, tooling/adjusting, programming/testing, eliminating disruptions in the workflow, monitoring production processes, troubleshooting and fault rectification, cleaning/maintenance, repair		
Explanation of activity	n/a		
Type of hazard	Mechanical hazard		
Origin or consequences	Shearing, crushing		
Description	During operation and the associated movements of the robot arm there is a danger of limbs between crushed or severed between the robot arm and fixed parts of the system.		

Risk estimation and risk evaluation			
Degree of possible harm:	11	Possibility of avoidance:	2.5
Probability of occurrence of a dangerous event:	2.5	Frequency of exposure:	5
Pilz Hazard Rating (PHR):	**343**	**Risk level:**	High risk

Risk reduction concept	Reference
Risk reduction 1: Design safeguards: System parts must be designed in such a way according to EN 349 that they cannot form any hazardous crush or shear points with the robot. Any remaining crush points must be designed in accordance with ISO TS 15066. **Risk reduction 2: Technical safeguards:** Optimisation of the robot path in order to avoid crush and shear points. The following measures must be taken using safety proven software in accordance with TS 15066: - Reduction in velocity - Reduction in force	EN ISO 12100 EN ISO 13849-1 EN 349 EN ISO 10218-2 EN ISO 13857 EN ISO 13850 ISO TS 15066

Risk Assessment: Robot Manufacturing Application/Trade Fair 1

Pilz GmbH & Co. KG によるリスクアセスメントからの抜粋

3.2 CE マーキング

製造業者は、機械に関連するハザードをすべて明らかにするために、リスクアセスメントを実行する義務があります。その後、機械の設計および組立ての際に、このアセスメントの結果を考慮する必要があります。リスクアセスメントの内容および範囲は、どの指令にも規定されていませんが、EN ISO 12100 には、一般的な手順が記載されています。

機械が最初に市場投入された時点以降のライフサイクル全体を考慮に入れながら、意図された用途に基づき、関連ハザードをすべて特定する必要があります。機械のオペレーション、清掃、メンテナンススタッフなど、機械に接する様々なグループを考慮する必要もあります。

各ハザードについてリスクアセスメントを実行し、リスクを評価します。最先端技術に基づいて、規格に準拠したリスク低減策を策定します。同時に残留リスクを評価します。危険点から発生する残留リスクを許容レベルまで低減できない場合には、追加の対策が必要です。必要な安全性が達成されるまで、この反復プロセスを継続します。

ステップ 5: 妥当性確認

妥当性確認は、適合性評価手順の重要なステップです。基本的には、機械が安全規制を満たしていることの証明は、妥当性確認によって行われます。妥当性確認に関する情報はすべて、第 3.6 章で確認できます。

ステップ 6: 技術資料を作成する

技術資料は、機械指令に準拠して、特に次の内容で構成されます。

- 機械の全体的な図面と制御回路の図面
- 完全かつ詳細な図面 (機械が本質的安全衛生要件を満たしていることを確認するために必要な計算書やテスト結果等を添付)
- 機械の設計時に用いた本指令の基本的要件、規格、その他の技術仕様のリスト、機械によって発生するハザードを除去するために実装された保護対策の説明 (一般にはリスク分析の対象範囲)
- 技術レポートまたは証書、適合性を示すレポートまたはテスト結果
- 機械の取扱説明書
- 機械の一般的説明
- 適合性宣言書または組込み宣言書、および組立て説明書
- 機械、または機械に組み込まれた装置の適合性宣言書

この文書は、物理的な紙文書でいつまでも提供可能である必要はありませんが、その重要性に応じた期間内に収集して提供することが可能である必要があります。製造日から少なくとも 10 年以上保存し、国内の関連当局に提示できる必要があります。連続して製造する場合には、この期間は、最後の機械の生産日に開始しなければなりません。

3.2 CE マーキング

ステップ 7: EC 適合宣言書を発行する

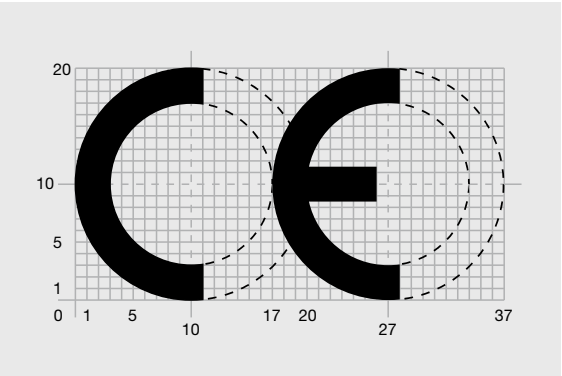
製造業者は、EC 適合宣言書を発行することで、製品に適用される指令をすべて考慮したことを宣言します。EC 適合性宣言の署名者は、会社を代表する権限を有している必要があります。つまり、署名者は、自己の職務のために、EC 適合宣言書への署名などの法的取引を行う法的権限を持っている必要があるということです。

会社の権限を有する従業員が EC 適合宣言書に有効な署名をした時点で、自然人である責任者、および該当する場合は法人である会社の責任が発生します。

宣言書は、法定代理人が署名することもできます。

機械指令は、技術資料の作成権限者を指名するための宣言も要求しています。この権限者は、EU 域内に定住している必要があります。

ステップ 8: CE マーキングを貼付する



CE マークの特徴

CE マークは、EC 適合宣言書が発行された後に貼付することができます。

完成品の機械の CE マーキングは、部品などの他の CE マーキングとは明確に区別できることが重要です完成品の機械の CE マーキングは、他のマーキングと混同されないように、機械の型式を記載したプレートに添付することが推奨されます。このプレートには、製造業者の名前と所在地も記載する必要があります。

3.3 指令

現在利用可能な約 30 の有効な指令のうち、一般的な機械メーカーに関係するものはごくわずかです。一部の指令には、指令番号 (2006/42/EC など) に加えて、非常に長い、あるいは官僚的なタイトルがついています。指令番号の末尾には、違いが見られる場合があります。この部分には、言語圏や発行日に応じて EC、EU、EG、EWG などの略称が含まれるためです。その結果、通常は、指令を名称で識別するのは非常に困難です。このような長いタイトルは (誤解につながる可能性があるにもかかわらず) 個々に省略されることもよくあります。以下にいくつかの主要な指令の公式なタイトルと通常使用される非公式の略されたタイトルのリストを示しています。

指令	略されたタイトル (非公式)	公式タイトル
2006/42/EC	機械指令	機械類に関する 2006 年 5 月 17 日付欧州議会・理事会指令 2006/42/EC、および修正指令 95/16/EC (改正)
2001/95/EC	製造物安全一般指令	2001 年 12 月 3 日付欧州議会・理事会指令 2001/95/EC
2014/30/EU	EMC 指令	電磁両立性に関する加盟諸国の法律の整合化のための 2014 年 2 月 26 日付の欧州議会・理事会指令 2014/30/EU (改正)
2014/53/EU	無線機器指令	無線機器の市場投入に関する加盟諸国の法律の整合化および指令 1999/5/EEC の廃止に関する 2014 年 4 月 16 日付の欧州議会・理事会指令 2014/53/EU
2003/10/EC	騒音指令	物理的要因 (騒音) に起因する危険性への労働者の曝露に関する安全衛生最低要件に関する 2003 年 2 月 6 日付の欧州議会・理事会発行の指令 2003/10/EC
2014/35/EU	低電圧指令	特定の電圧範囲内での使用を目的として設計された電気機器の市場投入に関する加盟諸国の法律の整合化のための 2014 年 2 月 26 日付の欧州議会・理事会指令 2014/35/EU
規制 (EU) 2016/425	PPE 指令	個人用保護具および理事会指令 89/686/EC (2019 年 4 月 20 日までの移行期間に適用される 89/686/EEC) の廃止に関する 2016 年 3 月 9 日付の欧州議会・理事会規制 (EU) 2016/425

指令の目的は、EU 域内の物品の自由な移動を保証することです。指令の全文はオンラインで確認できます。本書では、これらのすべての指令のうち、機械指令についてのみ詳細に検討します。但し、関連規格のリストではもちろん、他の指令に関係する規格を参照しています。

3.3 指令

3.3.1 機械指令

2006/42/EC には、機械の機能安全の面で特別な意味があります。一般に「機械指令」として知られるこの指令は、機械に関する欧州の安全要件の標準化に関わるものです。

3.3.1.1 内容

機械指令は、機械安全の主要な面を対象としています。機械指令の内容は以下の通りです。

- 範囲、市場投入、流通の自由
- 適合性評価手順
- CE マーキング
- 本質的件安全衛生要
- 機械のカテゴリおよび適用される適合性評価手順
- EC 適合宣言書および型式審査
- 認証機関の要件

3.3.1.2 法的効力

機械指令 2006/42/EC は、2009 年 12 月 29 日以降、旧バージョンの 98/37/EC に取って代わりました。移行期間はありませんでした。

3.3.1.3 機械指令に関する規格

機械指令に列挙されている規格であって、それゆえに整合化されたと見なされるすべての規格の名前を挙げることは、この時点では意味がありません。2016 年の冬の時点で、直接列挙されている規格は 750 を超えていました。さらに、直接列挙されている規格を通じて間接的に関連するすべての規格を追加することは、本書の範囲をはるかに超えてしまいます。そのため、以下の章では、一般的に重要性のある機械指令の規格を集中的に取り上げます。

3.4 規格

3.4.1 発行者と範囲

欧州レベルでの法律の整合化は、規格の整合化のきっかけにもなりました。ほぼすべての国で、従来から独自の規格協会が 1 つ以上存在しています。また、国際的な協力機構もいくつか存在します。これは、同じ規格が異なる名称、異なるレベルで発行されていることを意味します。すべてではないにしても、ほとんどのケースで規格の一般名が国内規格の名称の一部として残されて、認識可能です。詳細は以下の通りです。

3.4.1.1 国際規格

国際レベルでは、エンジニアリングスタンダードの最も重要な発行者は、おそらく国際電気標準会議 (IEC) と国際標準化機構 (ISO) で、どちらもジュネーブに本部があります。 IEC は、主に電気および電子分野に関する問題に関係しており、ISO は、主に機械に関する問題を扱っています。現在、100 か国を優に超える国が両組織に加盟しており、IEC と ISO が策定した規格を非常に重要視しています。

EN 規格は欧州レベルで適用されます。通常、EN 規格は、EU のイニシアチブとして CEN と CENELEC を通じて策定されます。IEC や ISO と同様に、CEN と CENELEC も規格の策定を分担しています。CENELEC は、電気分野の問題を担当しています。

今日では、多くの規格が、EU との協力によって、CEN および CENELEC を通じ、IEC または ISO 規格として一括して策定されています。EN IEC または EN ISO の規格は、このような取り組みの成果です。

3.4.1.2 国内規格

欧州全土に存在する国内規格と規格協会は、ほとんど手に負えないほど多様です。少なくとも EU では、大部分の規格を EN 規格として直接作成し、その後、国内レベルで反映することを目標としています。つまり、EN 規格が国内規格として宣言されるか、または国内規格が EN 規格として導入されます。

例えば、ドイツでは、ドイツ規格協会 (Deutsches Institut für Normung - DIN) が国内規格の発行に責任を負っています。今日では、DIN 規格は、CEN または CENELEC と連携して、DIN EN ISO または DIN EN として直接策定することが一般的な慣行となっています。通常、これらの規格間の唯一の違いは、EN、ISO または IEC 規格の前に付く国の略称です。

同じ規格が EU レベルでは、EN ISO や EN IEC 規格として施行されますが、全く同じドイツの規格が DIN EN ISO または DIN EN と呼ばれます。他の欧州諸国でも、この手順はほぼ同じですが、規格を発行する協会が異なっています。オーストリアではオーストリア規格協会 (Österreichisches Normungsinstitut - ÖNorm)、イギリスでは英国規格協会 (BSI) です。

ISO 規格が EN 規格になる場合には、そのタイトルは EN ISO となります。さらに、これが DIN 規格になる場合には、完全なタイトルは、DIN EN ISO となります。協会がローカルなものであるほど、名前の前の方に表示されます。これには奇妙な例外があります。IEC 規格は、EN 規格になると、IEC の名前は省略されます。IEC 61508 は、欧州規格では EN ~~IEC~~ 61508、ドイツでは DIN EN ~~IEC~~ 61508 になります。

中国やスイスなど、多くの国は、一元的な規格協会による、欧州と同様の手順に従っていますが、その他の場所では、依然として驚くような状況であることもあります。米国では、ANSI、OSHA、RSA、UL などによって規格が発行されています。

3.4 規格

3.4.2 EN エンジニアリング安全規格

この時点で、本書において欧州のエンジニアリング安全規格の完全なリストを提供する意図はまったくありません。機械指令だけでも、760 以上の規格が整合規格として列挙されています。以下のセクションでは、一般的な安全規格をいくつか選んで検討しています。個々の規格の重要性に応じて、様々な詳細レベルの説明がなされています。

規格	整合化	タイトル
EN 349:2008	有	機械類の安全性 人体の部位が押しつぶされることを回避するための最小間隔
EN 547-1 ～ -3:2008	有	機械類の安全性 人体測定値
EN 574:2008	有	機械類の安全性 両手操作制御装置 – 機能面 設計の原則
DIN EN ISO 14120:2016 (EN 953:2009 の後継)	有	機械類の安全性 ガード – 固定および可動式ガードの設計および構造に関する一般要件
EN 1005-1 ～ -4:2008 EN 1005-5:2007	有 いいえ	機械類の安全性 人間の身体能力
EN 1037:2008 ISO 14118:2000 と同一	有	機械類の安全性 想定外の起動防止
EN ISO 14119 (EN 1088:2008 および ISO 14119:2006 の後継)	有	機械類の安全性 ガード関連のインターロック装置設計および選定の原則
DIN EN ISO 11161:2010	有	機械類の安全性 統合生産システム – 基本要件
EN ISO 12100:2010 (EN ISO 12100-1 および 2、EN ISO 14121、 EN 292 の後継)	有	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とリスク低減
EN 12453:2000	無	工業、商業、車庫用ドアおよびゲート 電動式ドア使用の安全性 – 要件
EN ISO 13849-1:2015 (EN ISO 13849-1:2009 の後継)	有	機械類の安全性 制御システムの安全関連部 - パート 1: 設計のための一般原則
EN ISO 13849-2:2012	有	機械類の安全性 制御システムの安全関連部 - パート 2: 妥当性確認
EN ISO 13855:2010	有	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
EN ISO 13857:2008	有	機械類の安全性 危険区域への上肢および下肢の接近を防ぐ安全距離

3.4 規格

規格	整合化	タイトル
ISO/TR 23849:2010 (IEC/TR 62061-1:2009 と同一)	無	機械の安全関連制御システムの設計に ISO 13849-1 および IEC 62061 を適用するためのガイダンス
EN 60204-1:2010	有	機械類の安全性 機械の電気機器 – パート 1: 一般的な要件
EN 60947-5-1:2009 EN 60947-5-2:2012 EN 60947-5-3:2005 EN 60947-5-4:2003 EN 60947-5-5:2013 EN 60947-5-6:2001 EN 60947-5-7:2003 EN 60947-5-8:2006 EN 60947-5-9:2007	有	低電圧開閉装置および制御装置 パート 5: 制御回路装置および開閉素子
EN 61326-3 パート 1 および 2:2008	無	測定、制御および試験所用電気機器 –EMC 要件
EN 61496-1:2010	有	機械類の安全性 電気的検知保護設備 - パート 1: 一般要件およびテスト
IEC 61496-2:2013 CLC/TS 61496-2:2006	無	機械類の安全性 電気的検知保護設備 - パート 2: 能動的光電保護装置 (AOPD) を使用する機器の特定要件
CLC/TS 61496-3:2008 (EN 61496-3:2003 の後継)	無	機械類の安全性 電気的検知保護設備 - パート 3: 拡散反射形能動的光電保護装置 (AOPDDR) の特定要件
EN 61508 パート 1 ～ 7:2010	無	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
EN 61511 パート 1-3:2004	無	機能安全 - プロセス産業分野の安全計装システム
EN 61784-3:2010	無	産業用通信ネットワーク – プロファイル – パート 3: 機能安全フィールドバス – 一般規則とプロファイル定義
EN 61800-5-2:2007	有	可変速電気駆動システム – パート 5-2: 安全要件 – 機能
IEC/TS 62046:2008	無	機械類の安全性 人間の存在を検出する保護設備の使用基準
EN 62061:2016	有	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機能安全
IEC/TR 62685:2010	無	産業用通信ネットワーク – プロファイル – IEC 61784-3 機能安全通信プロファイル (FSCP) を使用する安全装置のアセスメントガイドライン
NFPA 79:2013	無	産業用機械

3.4 規格

3.4.3 一般規格と設計仕様

3.4.3.1 EN ISO 12100 と EN ISO 14121

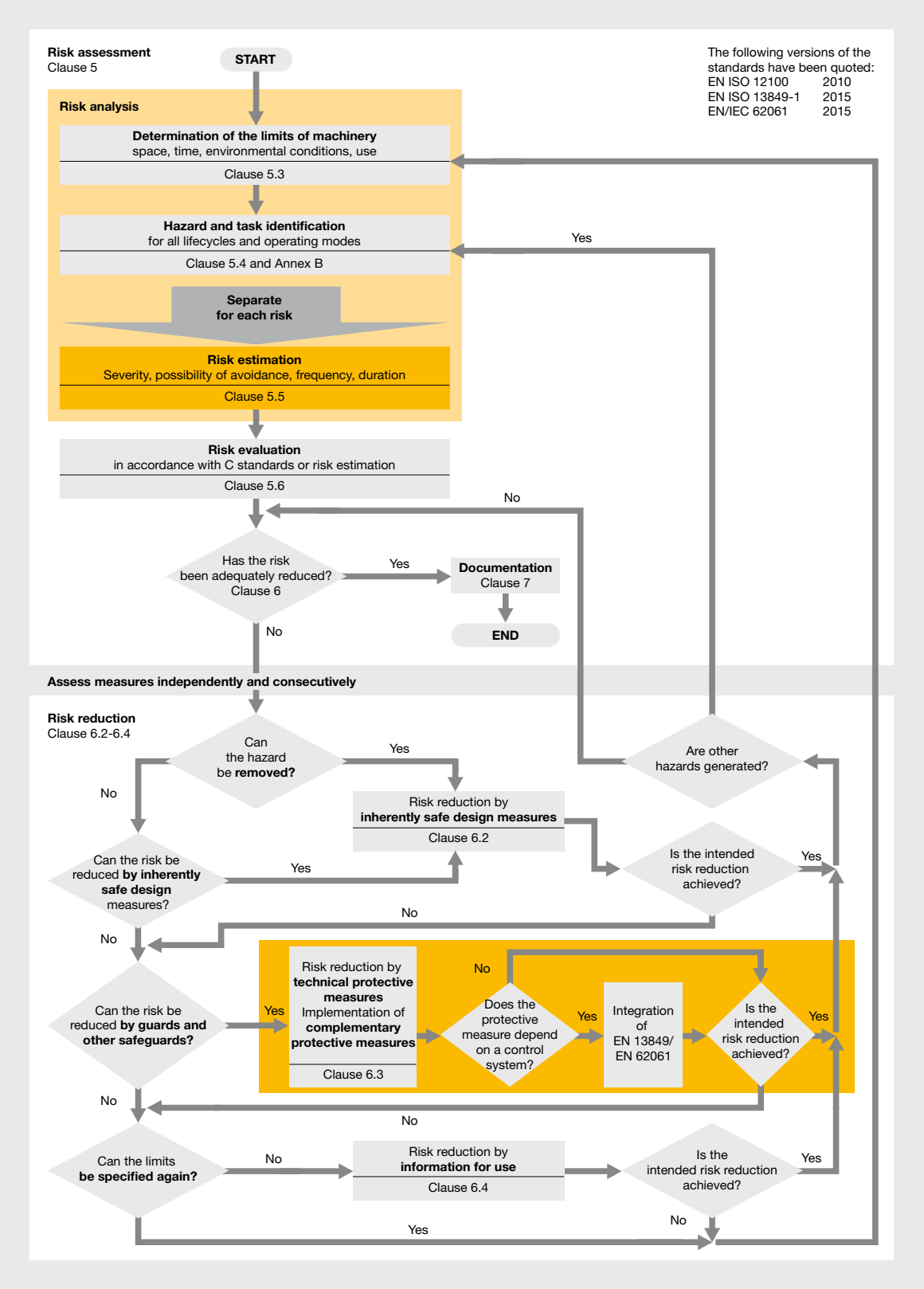
規格	整合化	タイトル
EN ISO 12100:2010 (EN ISO 12100-1 および -2、EN ISO 14121-1 の後継)	有	機械類の安全性 設計のための一般原則 – リスクアセスメントとリスク低減

2010 年に、EN ISO 12100 によって、EN 12100-1 および -2 に加え、EN 14121-1 のさらなる概要が提供されました。この規格は、名前を挙げている規格と内容は同じもので、それらを単に 1 つの文書にまとめたものです。

次のページ (3-22 ページ) に示されている図は、この規格で検討されている個々の要素を示しています。この規格では、考慮が必要なハザード、リスク要因、設計原則を豊富に取り上げています。

図の中で、背景が濃い黄色の部分は、ユーザ規格 EN ISO 13849-1 と EN/IEC 62061 の適用範囲であり、詳細に検討されています。この図では、可能な限り、関連する面を取り上げている規格内の対応セクションを参照しています。いくつかの点は複数の規格に記載されていますが、概してその詳細レベルは異なっています。

3.4 規格



EN ISO 12100 に適合するリスクアセスメントとリスク低減

3.4 規格

3.4.3.2 IEC/TR 62685: テスト要件と EMC

規格	整合化	タイトル
IEC/TR 62685:2010	無	産業用通信ネットワーク – プロファイル – IEC 61784-3 の機能安全通信プロファイル (FSCP) を使用する安全装置のアセスメントガイドライン

IEC/TR 62685 は、ドイツ BGIA の文書、GS-ET-26 のテスト要件から作成されたもので、安全機能内の安全部品の要件を取り上げています。ラベル付けと EMC に加え、機械および気候テストも扱っており、EN ISO 13849-1 と EN 61784-3 の不備な点をいくつか補っています。文書全体は、設備や機械の製造業者よりも安全部品の製造業者に関連性の高いものとなっています。しかし、この文書には、EMC 要件の優れた比較が掲載されており、機械の製造業者にとっても興味深いかもしれません。

3.4.3.3 EN 61784-3: 安全フィールドバス

規格	整合化	タイトル
EN 61784-3:2010	無	産業用通信ネットワーク – プロファイル – パート 3: 機能安全フィールドバス – 一般規則とプロファイル定義

EN 61784-3 シリーズの規格は、EN 61508 の仕様に基づいて、様々なフィールドバスプロファイルに関するあらゆる種類の安全強化を取り上げています。これらの強化は、セキュリティプロファイルとして扱われ、これらのプロファイルのメカニズムと技術的詳細を示しています。平均的な機械製造業者の関心を引くのは、一般的な安全原理について記載している EN 61784-3 の一般的な部分ぐらいでしょう。プロファイル文書の EN 61784-3-x は、主に、公開されたプロファイルのいずれかに適合する独自の安全装置を製造したいと考える装置製造業者を対象としています。この場合、これらのプロファイルの背景にある関連ユーザグループと協力したり、EN 61784-1 および -2 シリーズ、ならびに EN 61158 に示された基本プロファイルに精通することは理に適っています。EN 61784 と EN 61158 の関連部分で構成される完全なプロファイルは、1 つで 500 ～ 2,000 ページになります。プロファイルを全部合わせると、約 10,000 ページになります。

3.4 規格

3.4.3.4 EN ISO 13849-1

規格	整合化	タイトル
EN ISO 13849-1:2015	有	機械類の安全性 制御システムの安全関連部 - パート 1: 設計のための一般原則
EN ISO 13849-2:2012	有	機械類の安全性 制御システムの安全関連部 - パート 2: 妥当性確認

内容

EN ISO 13849-1 では、リスクグラフを使用してリスクに適した信頼性クラスを割り付けるという問題を取り上げるとともに、構造的統計手法に基づく安全機能のアセスメントを扱っています。目的は、リスクを低減するための安全対策の適切性を確認することです。EN ISO 13849-2 は、EN ISO 13849-1 に関する妥当性確認の面について記載しています。そのため、両方の規格を合わせると、EN 62061 と実質的に同じになります (但し、まったく同一ではありません)。

この規格に基づき要求される計算に伴う作業は、適切なソフトウェアを使用した場合、大幅に軽減されます。Safety Calculator PAScal などの計算ツールは、無料ソフトウェアとして以下で提供されています。
https://www.pilz.com/de-INT/eshop/00105002187038/PAScal-Safety-Calculator、
webcode: web150431

PAScal Safety Calculator

範囲

EN ISO 13849-1 は、機能安全の一般規格です。ISO レベルで採択され、EU 域内で機械指令と整合化されています。そのため、EU 域内で適合性の推定を与えることができます。範囲は、機械の電気的・電子的・プログラマブル電子的・機械的・空圧的・油圧的安全です。

リスクアセスメント／リスク分析

EN ISO 13849-1 では、グラフを使用してリスクを評価します。評価対象の基準には、怪我の程度、危険暴露の頻度、危険を回避する可能性があります。アセスメントの結果は、リスクを最小化するための個々の安全機能に要求されるパフォーマンスレベル (PL_r) です。

リスクの発生を防止するか、リスクを十分に低減するために、分類した各リスクに 1 つ以上の対策を適用する必要があります。パフォーマンスレベルとして表される対策の質は、各リスクについて決定されたレベルに少なくとも対応している必要があります。

3.4 規格

要求されるパフォーマンスレベル (PL_r) の決定

パフォーマンスレベル (PL) を評価するために検討が必要なパラメータは以下の 3 つだけです。

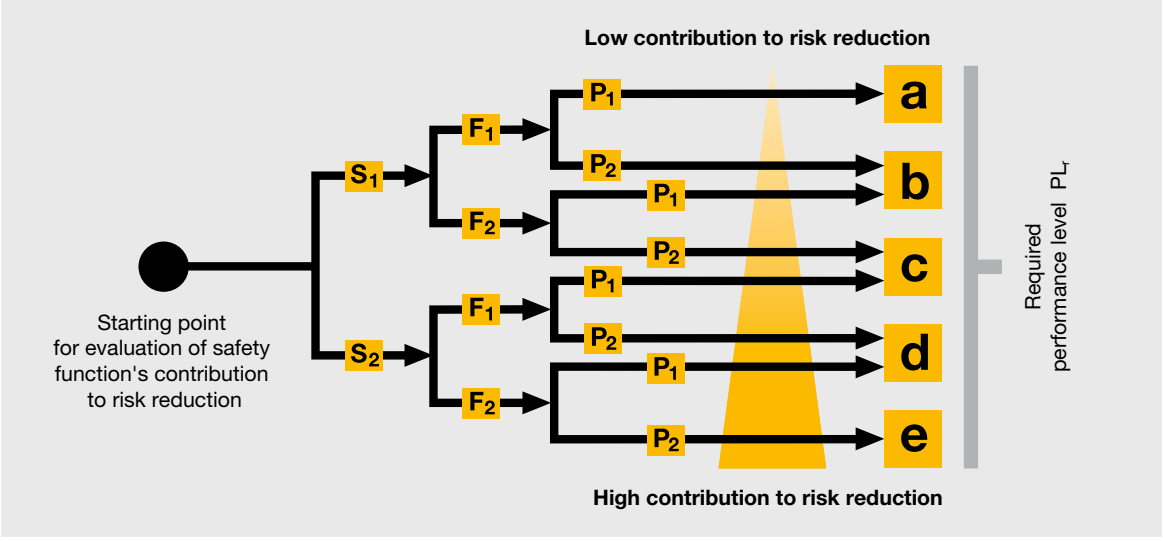
怪我の程度	S
軽傷 (通常回復可能な怪我)(G)	S_1
重傷 (死亡を含む回復不可能な怪我)(R)	S_2

危険暴露の頻度／時間	F
ほとんどなし～低頻度／短時間の暴露	F_1
頻繁～連続／長時間の暴露 (R)	F_2

危険を回避できる可能性	P
特定の条件下で可能性あり (B)	P_1
ほとんどない (B)	P_2

要求されるパフォーマンスレベル、PL_r は、以下のグラフと各パラメータの分類を使用して計算されます。リスクのアセスメントは、グラフの開始点で始まり、リスクの分類に応じて対応する道筋をたどります。要求されるパフォーマンスレベル、PL_r a、b、c、d、e は、すべてのパラメータが評価されてから決定されます。

この規格の最新バージョンでは、ハザードの発生確率を評価するオプションが新たに追加されました。この確率が低すぎるという結論になった場合には、以前に決定した PL_r を 1 レベル下げることができます。しかし、これには落とし穴が潜んでいます。この質問を評価するには、同等の機械を使用すべきであるということになっていますが、その機械には十分な安全対策が施されています。そうでなければ市場投入されていないからです。したがって、同等の機械の事故発生率が低いことは、関連するハザードを低に分類する十分な根拠とはなりません。その代わり、これは実装されている安全対策が適切であること (またこれらを低減することが誤りであること) の証明となります。



EN ISO 13849-1 に適合するリスクグラフ

3.4 規格

システムの実装評価／審査

EN ISO 13849-1 は、安全な装置といったものは存在しないという前提に基づいています。装置は、要件が増大するアプリケーションでの使用に合わせて適切に設計することでのみ、適切なものとなります。アセスメントの一環として、各装置には、その適切さを示す PL (パフォーマンスレベル) が決められます。単純な部品は、$MTTF_d$ (危険側故障までの平均時間) または $B10_d$ 値 (部品の 10% が危険側故障に至るまでの平均サイクル数) で表すこともできます。

以下では、装置またはその部品の故障がシステムの安全性に及ぼす影響、そのような故障が発生する可能性、PL の計算方法について検討します。

共通原因故障 – CCF 要因の決定

共通原因故障に対する対策のアセスメントは、複数の個別要素で構成されます。ここでは、チャンネルの分離などの構造面とともに、設計者のトレーニングなどの組織面が影響を及ぼします。評価スケールを使用して、0 ～ 100 % のスコアを付けることができます。

要件	スコア
安全回路およびその他の回路の物理的分離	15 %
多様性 (異なる技術の使用)	20 %
設計／アプリケーション／経験	20 %
アセスメント／分析	5 %
能力／トレーニング	5 %
環境の影響 (EMC、温度 ...)	35 %

EN ISO 13849-1 では、得られた合計スコアが≥ 65 % の場合には、CCF の影響は許容範囲と見なされます。

PL アセスメント

IEC ISO 13849-1 では、自己診断率 (DC)、システムカテゴリ、システムの $MTTF_d$ を使用して、PL を決定します。DC は、λ_{DD} (検出された危険側故障の故障率) および λ_{Dtotal} (全危険側故障の故障率) に応じて異なります。最も単純なケースでは、これは次のように表されます。

$$DC = \Sigma\lambda_{DD}/\Sigma\lambda_{Dtotal}$$

複雑なシステムでは、平均 DC_{avg} は次のように計算されます。

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

DC の値には、次のサイズ範囲が割り付けられます。

自己診断率	DC の範囲
なし	DC < 60 %
低	60 % ≤ DC < 90 %
中	90 % ≤ DC < 99 %
高	99 % ≤ DC

同種または 1 チャンネルのシステムでは、$MTTF_d$ 値は、およそ、1 チャンネルの $MTTF_d$ 値に対応する、各部品の逆数値の和として確定することができます。

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{d,i}}$$

3.4 規格

2 チャンネルの異種システムでは、両方のチャンネルの $MTTF_d$ 値は別個に計算する必要があります。両方の値は、下記の式を使用して、$MTTF_d$ の計算に算入されます。

$$MTTF_d = \frac{2}{3}\left[MTTF_{d,C_1} + MTTF_{d,C_2} - \frac{1}{\frac{1}{MTTF_{d,C_1}} + \frac{1}{MTTF_{d,C_2}}}\right]$$

ここでもテーブルを使用して、この数値から定性的評価を引き出します。この数値は、その後の検討で使用します。

$MTTF_d$ アセスメント	$MTTF_d$
低	3 年 ≤ $MTTF_d$ < 10 年
中	10 年 ≤ $MTTF_d$ < 30 年
高	30 年 ≤ $MTTF_d$ < 100 年

システムのアーキテクチャは、5 つの異なるカテゴリに分類することができます。どのカテゴリに分類されるかは、そのアーキテクチャだけでなく、使用する部品や自己診断率によっても異なります。安全機能は、一部分のエラーが安全機能全体の機能不全につながらないように、複数の部分 (通常、サブシステムと呼ばれます) に分割されることに留意してください。これらのサブシステムにはそれぞれ、独自のカテゴリがあります。

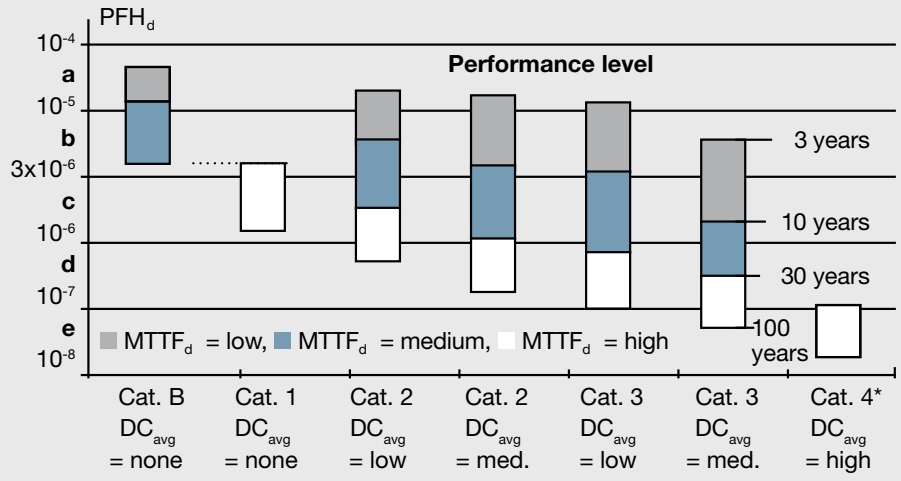
アセスメントの最終段階では、グラフを使用し、最近計算された値に基づいて PL を割り付けます。

最も実用的なアプローチは、最初にカテゴリと DC の列を選択することです。次に、バーから該当する $MTTF_d$ 範囲を選択します。これで、左側の目盛りから PL の結果を読み取ることができます。それでも、ほとんどの場合に、ある程度の解釈が必要になります。通常、$MTTF_d$ の範囲と PL の間には明確な関係が存在しないからです。

カテゴリ 4 では、グラフに示されているより大きい $MTTF_d$ の値 (したがって、より小さい PFH_d 値 - 1 時間あたりに危険側故障を起こす確率) も使用することができます。ここでは、DIN EN ISO 13849-1 規格の附属書 K を適用する必要があります。

最終ステップでは、リスクアセスメントから得た要求される PL_r レベルを、得られた PL と比較します。得られた PL が要求される PL_r 以上の場合には、実装の要件は、満たされていると見なされます。

Relationship between the categories DC, $MTTF_d$ and PL



* In Cat. 4 $MTTF_d$ up to 2,500 a is possible

EN ISO 13849-1 に準拠して PL を決定するためのグラフ

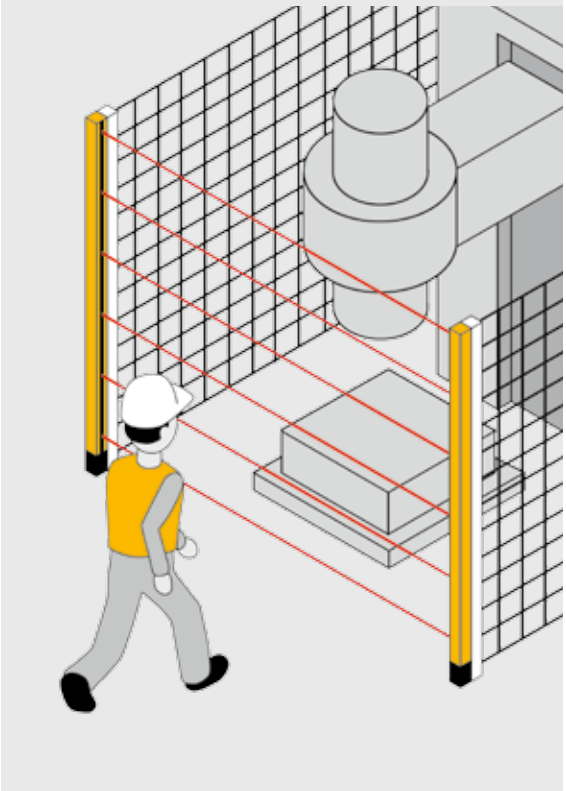
3.4 規格

3.4.3.5 EN ISO 13855

規格	整合化	タイトル
EN ISO 13855:2010 (EN 999 の後継)	有	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

EN ISO 13855 は、主に人間の接近速度について定めています。このような接近速度は、安全対策の設計時および適切なセンサ技術の選択時に考慮する必要があります。接近の方向とタイプに応じて、異なる速度とサイズが定められています。間接的な接近も考慮されています。

全体的な停止性能の測定に関する問題は、安全距離の測定とともに考慮されています。全体的な停止性能をどのように測定すべきで、どのように測定すべきでないかについて、明確な仕様が定められています。



安全防護物は、作業者が危険動作に接近するのを防止します。

3.4.3.6 EN ISO 13857

規格	整合化	タイトル
EN ISO 13857:2008	有	機械類の安全性 危険区域に上肢および下肢が到達することを防止するための安全距離

2008 年に初めて発行された EN ISO 13857 では、上肢および下肢が危険区域に到達するのを防ぐために必要な安全距離について検討しています。強調すべきは、この規格では、様々な人体測定データ (サイズ、四肢の長さなど) が他の集団やグループ (アジア諸国、スカンジナビア、児童など) に適用される場合があり、これが他のリスクを発生させる可能性があることを明確にしている点です。 したがって、この規格の適用は、特に社会全体に適用する場合や他の国に輸出する場合には制限される場合があります。

3.4 規格

3.4.3.7 EN 61511: プロセス産業分野の安全計装システム

規格	整合化	タイトル
EN 61511 パート 1-3:2004	無	機能安全 - プロセス産業分野の安全計装システム

EN 61511 シリーズの規格は、プロセス産業の設備やシステムに関する安全性の問題を扱っています。EN 61508 の分野別規格である EN 61511 シリーズは、EN 62061 の姉妹規格です。これは、3 つの規格に含まれる共通の考察と数学的原理に反映されています。しかし、大部分のエンドユーザと部品製造業者にとって重要な違いは、要求モード間の区別です。エンジニアリングでは、高頻度作動要求モードが常に想定されますが、EN 61511 は、低頻度作動要求モードも認めています。このモードの重要な特徴は、安全機能の要求 (操作) が年 1 回未満であることです。その結果、EN 61511 は、PFH (高頻度作動要求モードでの故障の確率) と SILcl (達成可能な最大安全度水準) とともに、PFD (低頻度作動要求モードでの故障の確率) を導入しました。特に、留意すべきは、低頻度作動要求モードの SILcl は、高頻度作動要求モードの SILcl とは異なる場合があることです。

3.4.3.8 EN 62061

規格	整合化	タイトル
EN 62061:2016	有	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機能安全

内容

EN 62061 は、リスクグラフを使用するリスクアセスメントの問題を扱っています。このケースでは、リスクグラフはテーブル形式です。また、構造的統計手法に基づく安全機能の妥当性確認についても述べています。EN ISO 13849-1 と同様に、目的は、リスクを低減するための安全対策の適切性を確認することです。

EN 13849-1 と同様に、この規格に基づき要求される計算には、多大な作業が伴いますが、Safety Calculator PAScal (https://www.pilz.com/de-INT/eshop/ 00105002187038/PAScal-Safety-Calculator, webcode: web150431) などの適切なソフトウェアを使用すれば、これを大幅に軽減することができます。

範囲

EN IEC 62061 は、機能安全の一般規格の 1 つです。IEC レベルで採択され、EU 域内で内の規格として整合化されています。そのため、EU 域内で適合性の推定を与えることができます。その範囲は、機械の電気的・電子的・プログラマブル電子的安全です。この規格は、機械、空圧、油圧のエネルギー源を対象としていません。それらのケースでは、EN ISO 13849-1 の適用が推奨されます。

3.4 規格

リスクアセスメント／リスク分析

IEC 62061 のリスクアセスメントは、テーブルとリスクグラフを使用して行われます。個々のリスクごとに行われる評価には、可能性のある怪我の程度、暴露の頻度と時間、リスクを回避できる可能性、リスクの発生確率が含まれます。アセスメントの成果は、個々のリスクに対して要求される安全度水準 (SIL) です。

リスクアセスメントのその後の段階では、リスクグラフを使用して決定されたレベルと、選択したリスク低減対策を合致させます。リスクの発生を防止するか、リスクを十分に低減するために、分類した各リスクに 1 つ以上の対策を適用する必要があります。この対策の SIL は、リスクに基づき決定される、要求される SIL に少なくとも対応している必要があります。

要求される SIL の決定

EN IEC 62061 によると、アセスメントが必要なパラメータは 4 種類あります。各パラメータには、以下のテーブルのスコアに従ってポイントが与えられます。

上記の項目に基づく SIL の分類は、以下のテーブルを使用して行われます。このテーブルでは、結果を、Class Cl と比較します。Class Cl は、頻度、時間、確率、回避のスコアの合計です。OM が表示されている領域は、このケースでは他の対策を用いることが規格で推奨されていることを示しています。

Frequency and duration of exposure	Fr < 10 min	Fr ≤ 10 min
≤ 1 hour	5	5
> 1 hour – ≤ 1 day	5	4
> 1 day – ≤ 2 weeks	4	3
> 2 weeks – ≤ 1 year	3	2
> 1 year	2	1

Probability of occurrence	Pr
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Avoidance	Av
Impossible	5
Rarely	3
Probable	1

Consequences		Class Cl = Fr+Pr+Av				
	S	3-4	5-7	8-10	11-13	14-15
Death, losing an eye or arm	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
Permanent, losing fingers	3		OM	SIL 1	SIL 2	SIL 3
Reversible, medical attention	2			OM	SIL 1	SIL 2
Reversible, first aid	1				OM	SIL 1

OM = other measures recommended

EN IEC 62061 に適合するリスクグラフ

3.4 規格

システムの実装評価／審査

この原則は、安全な装置といったものは存在しないということを前提としています。装置は、要件が増大するアプリケーションでの使用に合わせて適切に設計することでのみ、適切なものとなります。アセスメントの一環として、各装置には、その適切さを示す SIL が決められます。単純な部品は、$MTTF_d$ または $B10_d$ 値により表すこともできます。

以下では、装置またはその部品の故障がシステムの安全性に及ぼす影響、そのような故障が発生する可能性、SIL の計算方法について検討します。

共通原因故障 – CCF 要因の決定

CCF 要因は、個々のアクセスメントを複数組み合わせて決定されます。検討が必要な最初の重要パラメータの 1 つは、システムアーキテクチャです。特に、共通原因による複数の部品の故障など、系統的影響のアセスメントを行う必要があります。分析手順とともに、開発者の能力と経験も評価されます。評価スケールを使用して、100 ポイントが割り付けられます。

要件	ポイント
安全回路およびその他の回路の物理的分離	25
多様性 (異なる技術の使用)	38
設計／アプリケーション／経験	2
アセスメント／分析	18
能力／トレーニング	4
環境の影響 (EMC、温度 ...)	18

次のステップでは、以下のテーブルを使用し、獲得したポイントに基づいて β 要因 (ベータ) を決定します。

	β 要因 – 共通原因要因
<35	10 % (0.1)
35-65	5 % (0.05)
66-85	2 % (0.02)
86-100	1 % (0.01)

3.4 規格

SIL アセスメント

EN 62061 では、達成可能な最大 SIL は、ハードウェアフォルトトレランスと安全側故障の割合 (SFF) の間の依存関係により決定されます。SFF は、考え得るすべてのタイプの部品故障を評価し、かつそれぞれの故障によって安全な状態になるか危険な状態になるかを確認することで計算します。その結果、そのシステムの SFF が導き出されます。

構造分析でも、フォルトトレランスがあるかどうかが示されます。フォルトトレランスが N の場合、N+1 の故障の発生は、安全機能の損失につながる可能性があります。次のテーブルは、フォルトトレランスと SFF に基づく最大可能 SIL を示しています。

安全側故障の割合 (SFF)	ハードウェアフォルトトレランス 0	ハードウェアフォルトトレランス 1	ハードウェアフォルトトレランス 2
< 60 %	許可されていない	SIL 1	SIL 2
60 %–< 90 %	SIL 1	SIL 2	SIL 3
90 %–< 99 %	SIL 2	SIL 3	SIL 3
99 %	SIL 2	SIL 3	SIL 3

各部品の故障率 λ と、その λ_D 割合 (危険側故障) は、PFH_D の公式によって決定できます。公式はアーキテクチャによって異なります。これらの公式は極めて複雑になることがありますが、常に以下の形式をとります。

$$PFH_D = f(\lambda_{Di}, \beta, T_1, T_2, DC_i)$$

変数の説明 :

T_2 診断テスト間隔

T_1 最小テスト間隔および使命時間

ハードウェア、フォルトトレランス、カテゴリ、DC、PFH_D、SFF を合わせて検討することで、以下の SIL の割付けが行われます。常にすべての条件を満たす必要があります。条件が 1 つでも満たされていなければ、SIL は得られていません。

PFH_D	カテゴリ	SFF	ハードウェアフォルトトレランス	DC	SIL
≥ 10^{-6}	≥ 2	≥ 60 %	≥ 0	≥ 60 %	1
≥ $2x10^{-7}$	≥ 3	≥ 0 %	≥ 1	≥ 60 %	1
≥ $2x10^{-7}$	≥ 3	≥ 60 %	≥ 1	≥ 60 %	2
≥ $3x10^{-8}$	≥ 4	≥ 60 %	≥ 2	≥ 60 %	3
≥ $3x10^{-8}$	≥ 4	> 90 %	≥ 1	> 90 %	3

最終ステップでは、リスクアセスメントから得た要求される SIL レベルを、得られた SIL と比較します。得られた SIL が要求される SIL 以上の場合には、その実装の要件は満たされていると見なされます。

3.4 規格

3.4.3.9 EN 60204-1

規格	整合化	タイトル
EN 60204-1:2010	有	機械類の安全性 機械の電気機器 – パート 1: 一般的な要件

整合規格 EN 60204-1 は、電圧が最大 1000 VDC ～ 1500 VAC までの非ハンドガイド式機械の電気的安全について検討しています。したがって、その範囲は、影響を受けない産業用機械がほとんど存在しないほど広範です。

3.4.3.10 EN 61508

規格	整合化	タイトル
EN 61508-1:2010 EN 61508-2:2010 EN 61508-3:2010 EN 61508-4:2010 EN 61508-5:2010 EN 61508-6:2010 EN 61508-7:2010	無	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

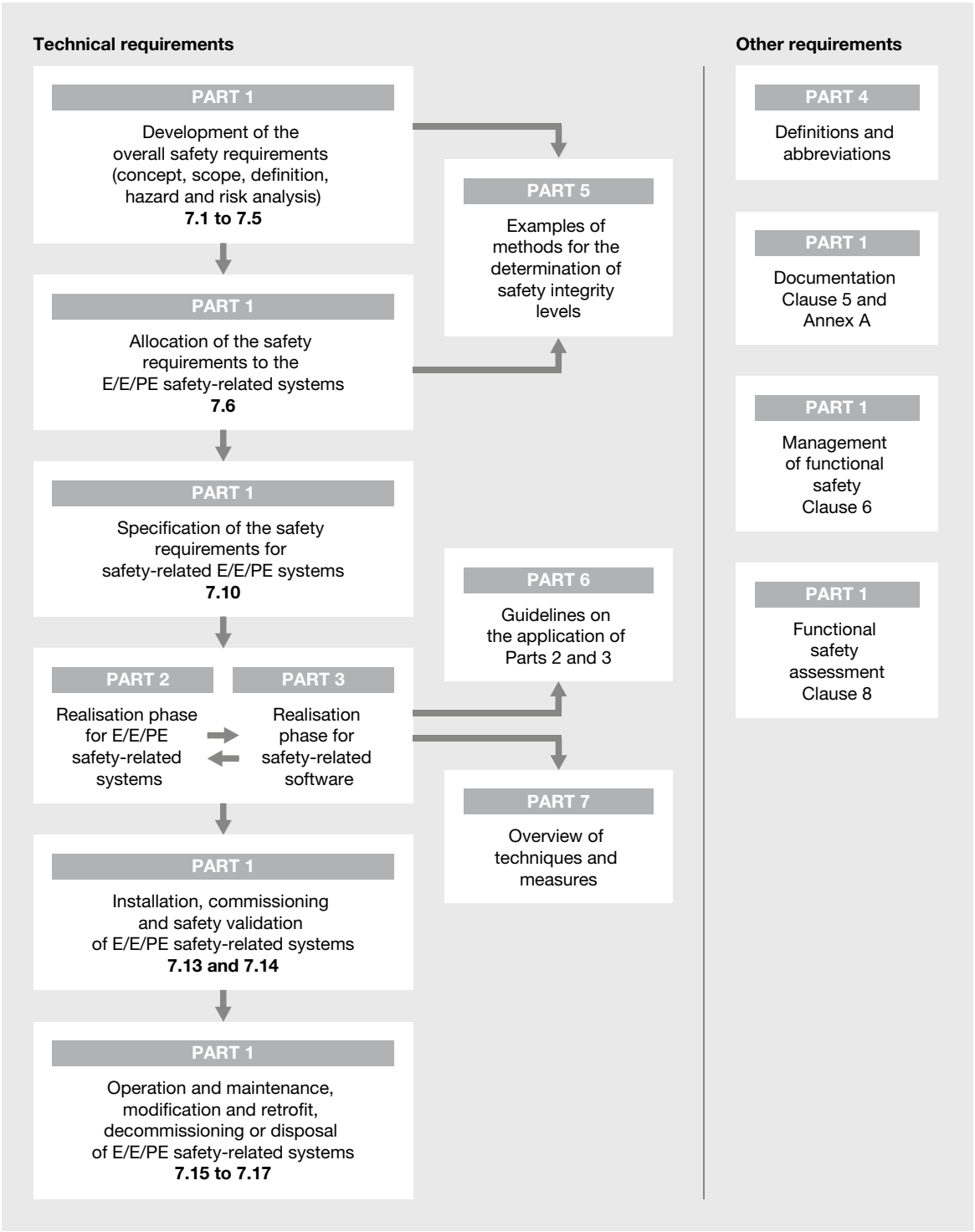
EN 61508 は、制御システムの機能安全を扱う重要規格です。合計 7 つのパートがあり、テキストのページは全体で約 1000 ページに及びます。EN 61508 の規格パッケージの全体が 2010 年に全面的に改訂され、現在は、第 2 版が利用できます。

EN 61508 の主要部分は、安全性の観点から見たライフサイクル全体の検討 (パート 1) であり、各ステップの手順の詳細な要件と内容を定めており、機械メーカーと安全部品製造業者のいずれにとっても同様に極めて重要です。

この規格は、電子システムとそれに対応するソフトウェアの設計にも重点を置いています。しかし、この規格は実際には拡大適用され、その他システム (機械、空圧、油圧) にも頻繁に適用されます。安全リレー、プログラマブル安全システム、安全センサ／アクチュエータ技術などの安全部品の製造業者は、この規格から最もメリットを得られる可能性があります。
全体としては、安全レベルの定義については、エンドユーザやシステムインテグレータには、EN 61508 ではなく、もっとわかりやすい EN 62061 や EN ISO 13849-1 を利用することが推奨されます。

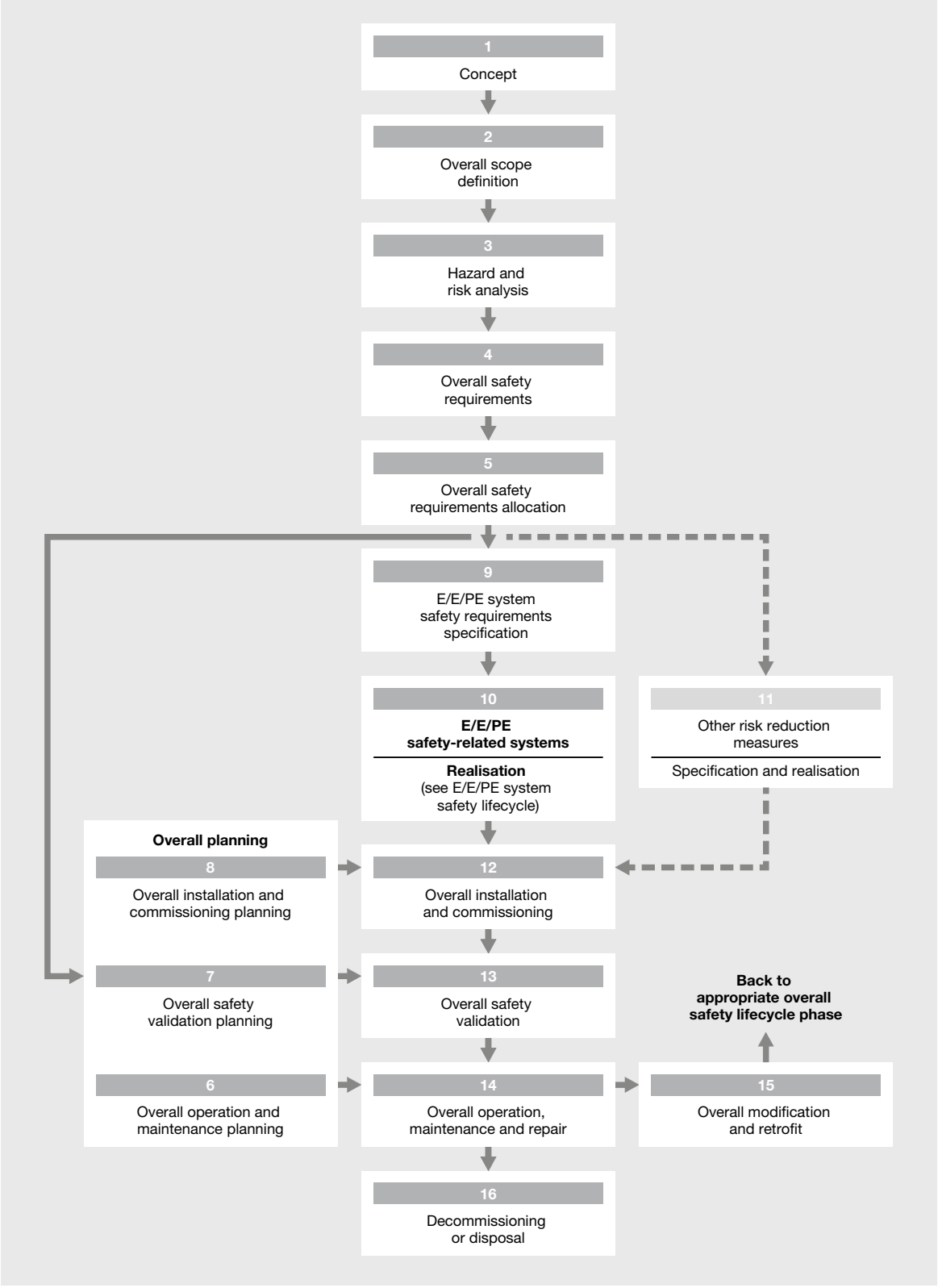
EN 61508 のもう 1 つの分野別規格が、EN 61511 です。これは、プロセス産業に適用されます。

3.4 規格



DIN EN 61508-1 からの抜粋、EN 61508 に適合する安全アセスメントの全体的枠組み。
IEC 61508 シリーズの規格の全体的枠組み

3.4 規格



EN 61508-1 に適合する全安全ライフサイクル

3.4 規格

3.4.3.12 EN 61326-3

規格	整合化	タイトル
EN 61326-3 パート 1 および 2:2008	無	測定、制御および試験所用電気機器 –EMC 要件

EN 61326-3-1 と EN 61326-3-2 の発表により、2008 年以降は、安全装置の EMC レベルに関するイミュニティ要求の情報を提供する規格が 2 つになりました。どちらのパートも異なるイミュニティ要求を定めています。パート EN 61326-3-1 は、より厳格な要求を定めた一般セクションです。このパートは、特に機械工学的観点で作成されています。これとは対照的に、パート EN 61326-3-2 は、プロセス産業の観点から作成されており、イミュニティ要求は大幅に低くなっています。したがって、エンジニアリングでは、最低限として、EN 61326-3-1 に準拠したテスト要件が満たされていることを常に確認すべきです。どちらの規格も最近始まったばかりで、参照できる前身規格が存在しないため、関連装置の証書に反映されるようになるには、まだしばらく時間がかかるでしょう。一般に、製品規格や分野別規格にも、EMC 要件が定められていますが、これらは、通常、EN 61326-3-1 に定められた要件を下回っています。

3.4.4 製品規格

3.4.4.1 EN ISO 14119

規格	整合化	タイトル
EN ISO 14119:2013	有	機械類の安全性 ガード関連のインターロック装置設計および選定の原則
ISO/TR 24119	無	機械類の安全性 ポテンシャルフリー接点を持つインターロック装置との併用によるフォルトマスキングの評価

前身規格である EN 1088 と ISO 14119 は、EN ISO 14119:2013 の発行によって統合されました。この規格は、ガード、すなわちゲート、カバー、フラップに加えて、これらの装置の位置を検出するセンサ技術を扱っています。また、ガードロック装置についても取り上げています。

この規格の目的は、機械の作業者が安全機器を無効にできないようにする対策を改善するための正確な要件を定めることでもあります。作業者はインターロックを無効にしてインターロックガードの安全機能を無効にしようとする場合がしばしばあることが、調査によって判明しています。安全機器を無効化できる原因は、主に機械の設計上の欠陥にあります。ISO/TR 24119 は、EN ISO 14119 と同時に発行されます。これは、EN ISO 14119 のスピンオフです。ISO/TR 24119 では、1 つの主題、つまり、連結された安全扉のスイッチの評価のみを扱っています。背景にあるのは、この種のアプリケーションに関連して繰り返し発生する故障の積み重ねです。これは設備の安全機能の損失につながる恐れがあります。

3.4 規格

3.4.4.2 EN 61496 および IEC/TS 62046

規格	整合化	タイトル
IEC/TS 62046:2008	無	機械類の安全性 人間の存在を検出する保護設備の使用基準
EN 61496-1:2012	有	機械類の安全性 電気的検知保護設備 - パート 1: 一般要件およびテスト
IEC 61496-2:2013	無	機械類の安全性 電気的検知保護設備 - パート 2: 能動的光電保護装置 (AOPD) を使用する機器の特定要件
CLC/TS 61496-3:2008	無	機械類の安全性 電気的検知保護設備 - パート 3: 拡散反射形能動的光電保護装置 (AOPDDR) の特定要件

61496 シリーズは、電気的検知保護設備の製品別要件を定めていますが、IEC/TS 62046 は、光線装置、ライトグリッド、スキャナなどの電気的検知保護設備の選択と測定に重点を置いています。したがって、機械のアクセス領域の設計や資材チャンネルの保護に関して、機械メーカーの重要な規格の 1 つとなっています。

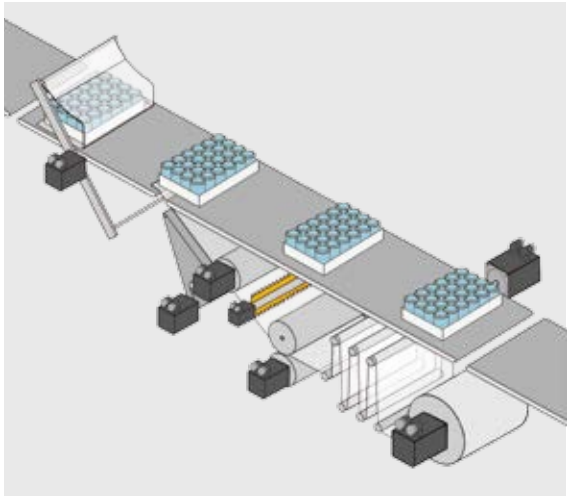
EN 61496 シリーズの規格は、電気的検知保護設備を取り上げています。これには、ライトグリッド、レーザスキャナ、光線装置、安全カメラシステム、その他のセンサなどの装置が含まれます。これらはすべて非接触型保護に使用できます。EN 61496 は、安全部品の製品規格であるため、使用している安全部品がこれらの規格への適合を意図している場合にのみ、一般ユーザに関連があります。

3.4 規格

3.4.4.3 EN 61800-5-2

規格	整合化	タイトル
EN 61800-5-2:2007	有	可変速電気駆動システム、パート 5-2: 安全要件 – 機能

EN 61800-5-2 は、ドライブの製造業者とユーザの両方を対象としています。ドライブベースの安全の問題を扱っていますが、安全関連の適切性に関する要件は定めていません。安全レベルは設定されておらず、明確なハザードやリスク評価もありません。その代わりに、この規格には、アプリケーション環境内のドライブのメカニズムと安全機能、およびドライブのライフサイクルにおけるメカニズムと安全機能の検証・計画方法についてが記載されています。この規格は (常に存在するドライブの機械的側面を考慮して、EN ISO 13849-1 との近似が予測されていたかもしれませんが) 技術的には EN 61508 に基づいています。



安全ドライブの製造業者は EN 61800-5-2 を重視します。

3.4 規格

3.4.5 アプリケーション規格

3.4.5.1 EN ISO 11161: 統合生産システム

規格	整合化	タイトル
EN ISO 11161:2010	有	機械類の安全性 統合生産システム – 基本要件

この規格は、機械と部品で生産システム (IMS) を組み立てる際の安全面について扱っており、個々の部品や機械の要件は扱っていません。この規格は、機械や部品を組み込むマシンプールや設備を操作または設計する運用者やシステムインテグレータにとって特に関心を引くもので、EN ISO 12100 と緊密に連携して適用すべきです。

3.4.5.2 NFPA 79

規格	整合化	タイトル
NFPA 79:2015	無	産業機械用の電気規格

この規格は、主に米国市場にとって重要ですが、アジアでも適用されます。これは欧州規格の EN 60204-1 と非常によく似ています。

この規格は、産業機械の安全な電気設計、操作、点検に関するものです。

3.5 規格、指令、法律の国際比較

安全部品、設備、機械の CE 適合性評価手順と CE マーキングを組み合わせた整合規格とともに、欧州で確立された EU 指令の極めて包括的なシステムは、世界中で自動的に受け入れられるわけではありません。一部の国では、法的拘束力のある他の法律、指令、規格が適用され、円滑な輸出のために遵守され、実施されています。安全な設備や機械は、基本的に、これらの国の労働安全の向上にも貢献するものですが、各国に固有の要件や実装レベルの分類は大幅に異なっており、欧州で一般的な高レベルの安全が必ずしも達成されていないことがよくあります。本 Safety Compendium では、主にヨーロッパの規格、指令、法律のみを扱っていますが、以下のセクションでは、欧州域外および世界の他の地域の状況についての概要を簡単に説明します。

3.5.1 アメリカの指令と法律

3.5.1.1 北米 (米国 + カナダ)

米国

米国では一般的に、設備や機械の安全要件に関して欧州とは別の法律、指令、規格が適用されます。CE マークと CE 適合宣言は、法的に認められていません。CE 適合だけに基づく輸出は間違いなく違法となり、製造物責任に関して非常に危険と分類されます。

一般に、設備や機械は、州、郡または地方自治体の専門職員、いわゆる管轄権者 (AHJ) による認証がなければ試運転することはできません。これらの検査官は、例えば、電気設備や機械安全 (電気設備／フィールド検査官)、爆発防護 (危険区域検査官)、または圧力装置の安全性 (圧力容器基準検査官) の認証を担当します。通常は、認証がなければ試運転は行われません。安全性の逸脱が確認されると、通常は、欠陥が修正されるまで赤色のタグが付けられ、運転が停止される可能性があります。この場合、製造業者は米国の現場で複雑かつ高コストな改造および変換措置を行うことになり、該当する場合には、試運転の遅延により不履行の約定違約金が発生します。

米国の基本的な労働安全対策の規定と監視は、米国労働省の下部機関である労働安全衛生局 (OSHA) が担当し、OSHA の規格で最低要件を定めています。これらは、連邦規則集 (CFR) の 29 CFR 1910 で確認することができ、主に機械と設備の運用者を対象としています。

製造業者の観点から見ると、設備および機械の安全に関する状況は、いくらか複雑になります。

3.5 規格、指令、法律の国際比較

まず、CEN/CENELEC と EN 規格を持つ欧州のように、米国には、1 つの規格発行機関による統一された規格システムがありません。規格を作成して発行できる認証機関が複数存在しているのです。通常、これらは製造業者の団体です。欧州で特によく知られている著名な機関は
以下の通りです。

- ANSI: 米国規格協会
- NEMA: 米国電機製造業者協会
- NFPA: 米国防火協会
- UL: 米国保険業者安全試験所

しかし、ほとんどの場合、設備や機械の分野でこれらの種類の基準を適用することは法的に要求されません。しかし、非常に重要な米国の製造物責任法により、製造業者は自社の設備や機械に適用される規格を確認するために必ず規格の検索を行う必要があります。製品ごとの適用がある場合には、規範となる要件を完全かつ正確に機械や設備に実装すべきです。そうすることで、不要な製造物責任リスクを防止することができます。

常に遵守し適用すべき規格の例は以下の通りです。

- NFPA 70 – 米国電気工事規定 (NEC)
- NFPA 79 – 産業機械用の電気的規格
- UL 508A – 産業用制御パネル

このリストで明らかなように、設備および機械の電気的安全は特に重要です。

機械的安全は、欧州の整合規格に比べて重要性が低く、上記の検査官による認証においても重要ではありません。

そのため、欧州で見られるような、設備や機械の電気的および機械的安全に関する包括的な製品規格は米国には存在しません。存在するのは、工作機械や成形機など、金属加工の設備や機械に適用される一連の規格 ANSI B11 だけで、これには、電気的要件に加えて、明確な機械的安全要件も定められています。

米国の機械的設備や機械の安全に関しては、欧州の機械指令に準拠して整合化された A、B、C 規格に基づく機械的安全要件を一貫して実装することが、米国で適用される安全要件を満たす重要な基盤となります。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。米国にあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5 規格、指令、法律の国際比較

カナダ

カナダでは一般的に、設備や機械の安全要件に関して欧州と異なる法律、指令、規格が適用されます。CE マークと CE 適合宣言は、法的に認められていません。CE 適合だけに基づく輸出は間違いなく違法となり、製造物責任に関する理由で推奨されません。

カナダでは一般に、州の専門職員、いわゆる安全当局職員 (SAO) による認証がなければ機械や設備の試運転は行われません。カナダでは、管轄権者 (AHJ) という用語も使用されています。これらの安全検査官は、例えば、電気設備や機械安全 (電気設備／フィールド検査官)、爆発防護 (危険区域検査官)、または圧力装置の安全性 (圧力容器基準検査官) の認証を担当します。通常は、認証がなければ試運転は承認されません。安全性の逸脱が確認されると、欠陥が修正されるまで運転が停止される可能性があります。

この場合、製造業者はカナダの現場で複雑かつ高コストな改造および変換措置を行うことになり、該当する場合には、試運転の遅延により不履行の約定違約金が発生します。

カナダの基本的な安全衛生対策の規定および監視は、カナダ労働安全衛生センター (CCOHS) が担当しています。カナダのこの機関は、米国の OSHA (3.5.1.1/USA を参照) に相当し、主に設備と機械の運用者に適用される設備および機械の安全衛生に関する最低要件も定めています。

製造業者の観点から見ると、設備および機械安全に関するカナダの状況は、米国に比べてやや明快です。

米国とは違い、規格発行機関 (カナダ規格協会 : CSA) が 1 つであるカナダでは、CEN/CENELEC と EN 規格を持つ欧州と同様に、統一された規格システムが存在します。したがって、カナダには、CSA 規格と呼ばれる 1 種類の規格しかありません。しかし、ほとんどの場合、設備や機械の分野でこれらの種類の基準を適用することは法的に要求されません。カナダの製造物責任法はそれほど厳格ではありませんが、それでも製造業者は自社の設備や機械に適用される規格を確認するために必ず規格の検索を行うべきです。製品ごとの適用がある場合には、規範となる要件を完全かつ正確に機械や設備に実装すべきです。そうすることで、不要な製造物責任リスクを防止することができます。

常に遵守し適用すべきカナダの規格の例は以下の通りです。

- CSA 22.1 – カナダ電気規則 (CEC)
- CSA 22.2 No.286 – 産業用制御パネルおよび組立て品
- 電気機器のフィールド評価に関する SPE 1000 標準規則

このリストで明らかなように、設備および機械の電気的安全は特に重要です。

機械的安全は、欧州の整合規格に比べて重要性が低く、上記の検査官による認証においても重要ではありません。

そのため、欧州で見られるような、設備や機械の電気的および機械的安全に関する包括的な製品規格はカナダには存在しません。

3.5 規格、指令、法律の国際比較

しかし、以下の重要なカナダ規格は、機械の安全防護物を扱っており、遵守する必要があります。

- Z432 – 機械の安全防護

この規格には、設備や機械の種類にかかわらず、安全防護物の基本的な電気的要件と機械的要件の両方が含まれており、欧州の A 規格、あるいは概ね B 規格に相当します。

カナダの機械的設備や機械の安全に関しては、欧州の機械指令に準拠して整合化された A、B、C 規格に基づく機械的安全要件を一貫して実装することが、カナダで適用される安全要件を満たす重要な基盤となります。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。カナダにあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5.1.2 南米

ブラジルを除き、現時点では、南米諸国で適用される設備および機械の具体的な製品別安全要件はありません。各国の標準化機構が存在し、国内規格を策定するとともに、ISO や IEC 規格を国内規格に変換しています。しかし、ここで重視されるのは、現時点では、ほとんど消費者製品の規格のみです。したがって、南米に設備や機械を輸出する場合には、クライアント／購入者／運用者に対する書面形式の具体的な問い合わせなどによって、満たす必要のある安全要件をケースごとに確認することが推奨されます。欧州指令とその整合規格が安全性に関して南米で一定の重要性を認められている場合でも、それらが一般に受け入れられていると決めてかかってはなりません。

ブラジル

2010 年時点で、ブラジルには、機械と (機械) 設備の最低安全要件を定めた次の法律が存在します。

- Norma Regulamentadora 12 (NR-12) – MÁQUINAS E EQUIPAMENTO

この法律は 1978 年から施行されていますが、当局による実施・取締りにはあまり一貫性がありませんでした。2010 年の最新の (基本的には全面) 改正によって、当局による監視措置が導入され、NR-12 は実質的に法的拘束力を有するようになりました。

3.5 規格、指令、法律の国際比較

この改正では、欧州機械指令 2006/42/EC に合わせて大幅な変更が行われました。特定種類の機械に関する個別の特別要件を定めた機械指令の附属書 I の安全要件が、可能な限り実際に採用されました。そのため、この法律は、欧州では「ブラジル機械指令」とも呼ばれています。

NR-12 は、欧州機械指令とは異なり、主に機械の運用者を対象とし、中古、使用済みおよび新品の機械に適用されます。

NR-12 に準拠した安全要件の実装を確認するために、欧州で規定されたような適合宣言書は、現時点では運用者、製造業者のいずれに対しても要求されません。この場合、運用者は、設備や機械が NR-12 に準拠した安全要件を満たしていることを確認する必要があります。したがって、ここでは結論が逆になり、ブラジルに機械を輸出する企業は通常、安全要件の確認を必要とする運用者に対応することになります。言い換えれば、NR-12 の不遵守があった場合に実装を確保するために、当局によってそれに対応する強制措置を課されるのは、運用者であるということです。

単純ではあっても過小評価すべきでない要求の 1 つに、ブラジルポルトガル語の取扱説明書、取り付け説明書、メンテナンス説明書の提供があります。これは、EU 加盟国のポルトガル語版と同じものではありません。

NR-12 の整合規格は現時点では存在しませんが、欧州の整合化システムに基づいて、整合規格で NR-12 を徐々に補完するための初期の検討と協議が国内レベルで進んでいます。これに関連し、安全部品などの証明の実現性が検討されています。しかし、当面は実現しそうにありません。

標準化に関しては、ブラジルの標準化機構である Associação Brasileira de Normas Técnicas (ABNT) は、ブラジル固有の国内規格、NBR (Norma Brasileira Regulamentadora) を定めるだけでなく、ますます多くの ISO や IEC 規格を国内規格に変換しつつあります。しかし、ISO 規格と IEC 規格の現行バージョンが採用されず、代わりに旧バージョンが使用されている場合が多くあります。そのため、ブラジルの標準化システムは、包括的であるとは見なされますが、ほとんどの場合、現在の国際標準化や欧州標準化と同等のステータスにあるとは見なされていません。

現行の欧州指令や整合規格に準拠して製造された CE 適合の設備や機械は、一般に、ブラジルで問題なく試運転をするための良好な前提条件を備えているという逆の結論が成立します。それでもなお、ブラジルに設備や機械を輸出する場合には、クライアント／購入者／運用者に対する書面形式の具体的な問い合わせなどによって、満たす必要のある安全要件をケースごとに確認することが推奨されます。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。ブラジルにあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5 規格、指令、法律の国際比較

3.5.2 アジアの指令と法律

3.5.2.1 ロシア／ロシア連邦

2011 年まで、設備と機械は、ロシア連邦への輸入資格を得るために特定の前提条件に基づき GOST-R 証書を提出することが必要でした。証明が必要な製品を決定するための基準としての基盤を形成するために、(国際的な) 関税番号 (HS コード – Harmonized Commodity Description and Coding System) が役立っていました。

2009 年 9 月に、ロシア連邦によって以下の命令が施行されました。これは、機械と設備の基本的な最低安全要件に加え、証明手順と組み合わせた必須の適合性評価手順を定めたものです。

- ロシア連邦政府の命令 N 753 – 機械および設備の安全性に関する技術規制 (TR)

ロシア連邦の機械に関する様々な安全関連規制や適合性評価手順と整合化するための、EU とロシア連邦の間の契約による整合化プロセスが、この基盤となっています。この命令には、2 つの附属書が含まれています。1 つは、証明が必要な機械のリスト、もう 1 つは、ロシアの適合性宣言で十分な機械のリストです。

証明義務
証明義務により、機械は、現地の認証試験機関による検査を受けて、TR 証書の交付を受ける必要があります。この手順は、機械指令に準拠した型式審査に相当します。

適合性宣言
適合性宣言で十分な場合でも、これに加えて、国が認証した証明機関による審査、認証取得および登録が必要です。この種の適合性宣言は、機械指令と対応する整合規格に基づいて欧州で一般的かつ許容されている機械製造業者による自己証明とは異なります。

ここでも関税番号は、一定の役割を果たしています。証明や適合が必要な (機械だけでない) すべての製品が含まれる包括的なリストがあるからです。

ロシアの機械安全を確保するための基盤となっているのは、ロシアの規格である GOST (Gossudarstwenny Standart) です。現時点で、機械に特化した安全規格は数多く存在しています。ロシアの国内規格である GOST-R に加え、ISO 規格と IEC 規格が次々に GOST R ISO、GOST ISO、GOST R IEC あるいは GOST IEC に変換されています。独自の要求事項が加えられることもあれば、わずかしか変更されないこともあります。さらに、相当する機械関連の ISO 規格や IEC 規格が存在しない場合には、欧州機械指令の整合化セクションから、EN 規格がロシアの GOST EN 規格として採用されています。

2010 年 7 月に、ロシア、ベラルーシ、アゼルバイジャンのユーラシア 3 か国間で関税同盟 (CU) が結ばれました。これは 2015 年に拡大され、アルメニアとキルギスタンが加盟しました。この関税同盟には、中長期的には、他の旧ソ連諸国も加盟することになります。

3.5 規格、指令、法律の国際比較

機械に関する TR は、関税同盟に加盟するすべての国で有効で、関連するロシア GOST 規格は適合性の基準として認められています。

EAC (ユーラシア適合) は、独自の適合性マークで、外部から視認できるマークとして存在します。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。ロシアにあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5.2.2 日本

日本の労働安全衛生法は、特定の機械 (クレーン、リフトなど) 関連の設計に対する要件を定めています。この法律では、機械の運用者がリスク分析の責務を負うことが明記されています。機械の運用者は、作業現場の安全を確保する義務も有しています。機械の運用者は、機械の購入時に機械製造業者に機械が安全に設計されていることを証明するリスク分析レポートの発行を要求することになっています。また、この法律には圧力容器や、食品業界の包装機械、自走機の要件も定められています。

日本では一般に、IEC および ISO 規格が国内の JIS 規格 (日本工業規格) として採用されていますが、労働安全衛生法はこれらの各規格を直接参照していません。そのため、これらの JIS 規格を適用し、実装することは法律上の義務ではありません。

設備と機械の承認または認証に関する具体的な義務は、現時点ではありません。

3.5 規格、指令、法律の国際比較

3.5.2.3 中国

中国では、国家安全生産監督管理総局が安全衛生対策の規定と監視を担当しています。監視は、現地の安全衛生検査官によって保証されます。設備や機械には中国の機械安全規格が使用されています。

また、中国には、2002 年 5 月から独自の認証システムである中国強制製品認証 (CCC) があります。認証製品のマークには CCC マークが使用されます。

現時点では、消費者製品、電子製品、工業製品分野から、132 の製品グループに分かれた 23 の製品カテゴリについて証明義務が定められています。

設備や機械は、この対象ではありません。HS コード (Harmonized Commodity Description and Coding System) と呼ばれる国際的に整合化された関税番号は、中国の関税マニュアルに定められた既存の証明義務に関する重要な検索基準となっています。その他の検索基準は、ある製品に有効な中国の規格が必須となっているかどうかを確認することです。

中国には独自の国内規格システムがあり、国家標準化管理委員会 (SAC) がこのシステムの整備を担当しています。この標準化機構は、国内規格の GB または GB/T を発行しています。

- GB = Guobiao (国内規格という意味)
- GB/T = Guobiao/Tujiàn (推奨される国内規格という意味)。GB 規格で参照されている場合は義務になる

機械安全の分野では、SAC は一般に国際規格の ISO と IEC を採用していますが、多くの場合、独自の個別要求事項が加えられ、国際的な最新バージョンに基づいてはいません。

国際規格が存在しないときは、場合によっては、機械指令に整合化された欧州 EN 規格が同じ方法で中国の国内規格に変換されます。中国語での発行に起因するアプリケーションの問題がありますが、英語による公式バージョンの規格は、現時点では例外的なケースでのみ利用可能です。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。中国にあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5 規格、指令、法律の国際比較

3.5.2.4 韓国

韓国では、韓国産業安全衛生公団 (KOSHA) が安全衛生対策の整備、実装、監視を担当する政府機関です。KOSHA の取り組みの基盤となっているのは、韓国の労働安全衛生法です。KOSHA が実施する監視の重要要素は、各種の安全部品、機械、設備の認証手順です。2008 年 12 月まで存在していた法律上の義務を伴う 13 の既存証明システムは、新しい統一証明システムに移行しました。これは、2011 年 6 月から始まる移行期間とともに法的拘束力をもって導入されました。これは、証明書により文書化され、KCs マーク (韓国認証安全マーク) を使用する

設備や機械に示されています。国が認証した以下の試験機関が証明を担当しています。

- ERI – EMC Research Institute
- KETI – Korea Electronics Technology Institute
- KTL – Korea Testing Laboratory

輸出前に、輸入者としての機械および設備の製造業者が要求する証明または認証手順は 2 種類あります。これらの手順は、以下の良好な試験結果とともに実施される必要があります。

危険な機械に対する証明義務
危険な機械については、独立した現地の認証試験機関によって完全な機械試験を実行する必要があります。この試験手順は、クレーン、圧力容器、リフト、自走式リフティングプラットフォーム、特定の斜行リフト、プレス、プレスブレーキ、圧延機、射出成形機、ハンドヘルドチェーンソーについて法律で定められています。内容面で、この試験手順は機械指令の附属書 Ⅳ に準拠した型式審査にほぼ相当します。

機械製造業者による自己証明
ここでは、機械の製造業者は、各機械の型式について韓国の該当する安全要件／規格が適用、実装、検査、文書化され、その結果、満たされていることを現地の認証試験機関で確認するために包括的な文書を使用する必要があります。この手順は、以下の種類の固定機械に適用することができます。産業用ロボット、研削盤、工作機械、木工機械、印刷機、混合および破砕器、食品加工機械、コンベヤ、車両用リフト。提供される文書は、完全な EU 適合性評価手順において作成する文書と内容の点で同じです。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。韓国にあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5 規格、指令、法律の国際比較

3.5.3 オセアニアの指令と法律

3.5.3.1 オーストラリア

2013 年以降、必要な安全衛生対策を実施するための統一法が、6 つの州のうち 4 つの州、および 2 つの準州で適用されています。法的枠組み条件の整備と規定、およびその監視については国の機関であるオーストラリア労働安全庁が担当しています。安全衛生の基盤となっているのは、連邦法である労働安全衛生法 (WHS) です。

ビクトリア州と西オーストラリア州だけが労働安全衛生法として独自の安全衛生要件を定め、実施しています。

定められている安全衛生要件は一般に法的拘束力があるため、遵守する義務があります。様々なアプリケーションガイドラインや実施ガイドラインが存在し、これらは Model Codes of Practice (モデル実施準則) と呼ばれています。これらは主に、設備や機械の製造業者でなく、現地の運用者を直接の対象としています。それでも、製造業者は、オーストラリアでの試運転中に発生する恐れのある問題を回避するために、これに対処する必要があります。
監視は、各州および準州の検査官によって行われます。

英連邦の一員であるオーストラリアは、昔から英国の行政手続きを模範としています。欧州機械指令や関連整合規格との共通点のおかげで、これは機械や設備の製造業者にとって重要な安全衛生対策においても顕著です。

オーストラリアには独自の規格システムがあり、オーストラリア規格協会がその整備を担当しています。この標準化機構は、国家規格の AS 規格を発行しています。
機械安全分野に適用される AS 規格は以下の通りです。

- AS 4024.xxxx 規格シリーズ – 機械類の安全性
- AS 60204.1 – 機械の電気機器、一般要件
- AS IEC 61511.x 規格シリーズ – プロセス産業の機能安全
- AS 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機能安全

オーストラリアの安全衛生法で実装することを法的に義務付けられた具体的要件が現時点で存在しない場合でも、これらの規格は常に遵守すべきです。オーストラリアの機械安全規格は、主に (全部ではありません)、ISO や IEC 規格の他、欧州機械指令に整合化された規格を受け入れてこれを基盤としています。但し、国際規格や欧州規格の現行バージョンが常に採用されているわけではありません。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。オーストラリアにあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5 規格、指令、法律の国際比較

3.5.3.2 ニュージーランドの指令と法律

ニュージーランドでは、2015 年以降、必要な安全衛生対策を実施するための労働安全衛生 (Health and Safety Work Act: HSW) 法が適用されています。法的枠組み条件の整備と規定、およびその監視については国の機関である労働安全局 (WorkSafe New Zealand) が担当しています。

定められている安全衛生要件は一般に法的拘束力があるため、遵守する義務があります。様々なアプリケーションガイドラインや実装ガイドラインがありますが、これらは主に、設備や機械の製造業者でなく、現地の運用者を直接の対象としています。それでも、製造業者は、ニュージーランドでの試運転中に発生する恐れのある問題を回避するために、これに対処する必要があります。
ニュージーランドでは、監視も現地の検査官によって行われます。

英連邦の一員であるニュージーランドは、昔から英国の行政手続きを模範としています。欧州機械指令や関連整合規格との共通点のおかげで、これは機械や設備の製造業者にとって重要な安全衛生対策においても顕著です。ニュージーランドには独自の規格システムがあり、ニュージーランド規格協会がその整備を担当しています。この標準化機構は、国内規格の NZS 規格を発行しています。

一般に、対応するオーストラリアの AS 規格は、以下のように、機械安全分野の AS/NZS 規格として採用されています。

- AS/NZS 4024.xxxx 規格シリーズ – 機械類の安全性

ニュージーランドの安全衛生法で実装することを法的に義務付けられた具体的要件が現時点で存在しない場合でも、これらの規格は常に遵守すべきです。

AS 規格と同様に、ニュージーランドの機械安全規格も、ISO や IEC 規格の他、欧州機械指令に整合化された規格を受け入れてこれを基盤としています。但し、国際規格や欧州規格の現行バージョンが常に採用されているわけではありません。

機械および設備の安全に関する国ごとの特別な考慮事項について具体的な質問がございましたら、ピルツまでお問い合わせください。ニュージーランドにあるピルツの現地法人で、オートメーション、設備および機械の安全に関する国際的に定評あるピルツのサービスをご利用いただくことで、このトピックに関する各国ごとの質問に的確なサポートを提供いたします。

3.5 規格、指令、法律の国際比較

3.5.4 概要

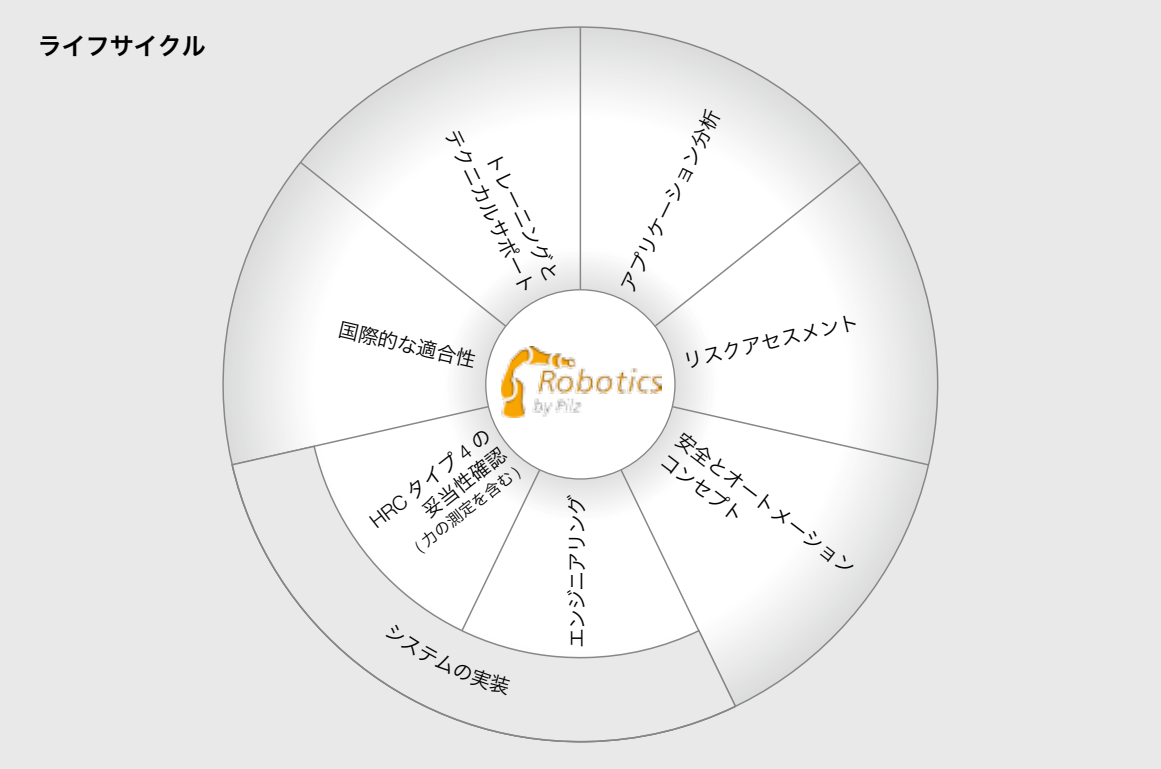
機械や設備の安全に関する欧州の要件と世界各国の要件を簡単に比較してきましたが、これらはもちろん不完全なものです。この比較では、欧州域外における設備や機械の安全要件が、場合によっては非常に多様であること、とりわけ、極めて一貫性に欠けていることを明らかにすることだけを目的としています。

そのため、機械と設備の製造業者は、自社の製品に関連する国ごとの特別な法律、指令、規格に早めに対処し、これらをよく理解しておく必要があります。それが、欧州域外に設備や機械を問題なく輸出するための基本的な要件です。

しかし、一般的に言って、それぞれの設備や機械に関連する EU 指令と整合規格を遵守し、実際に実装することは、時間とコストを管理可能に維持しながら世界各地に設備や機械を輸出できるようにするための主要な前提条件であると言えます。

また、これは特に、非常に詳細な整合規格システムを持つ欧州指令のコンセプトが国際的にも普遍的な意義を持つことを示しています。EU には、安全関連の全分野を対象としながら、なおかつ統一性が維持された、設備と機械に関する包括的な安全コンセプトが存在します。この種の安全コンセプトを持つ国は、現時点では、EU 域外にはありません。機械や設備の製造業者は、これに依拠することができますが、CE マークと CE 適合性宣言は世界で実際に法的に認められているわけではありません。CE 適合は世界各国に輸出するための事実上のフリーパスになるという考えを、まだ多くの機械や設備の製造業者が抱いていますが、これは明らかに間違っています。結局のところ、これは、本質的には自社の製品に適用される指令や整合規格をすべて遵守、適用し、実際に実装したと主張する製造業者による「単なる」自己証明に過ぎません。欧州域外の様々な国では、限られた範囲で信頼されているに過ぎません。

3.6 産業用ロボット、人とロボットの協働 (HRC)



アプリケーションの分析
計画されているロボットアプリケーションの主要周辺装置を文書化します。サイクル時間、反復精度、作業スペース、危険領域などのプロセスと安全関連要件がシステムの素案に取り込まれます。その後に技術的・経済的評価を実施します。

リスクアセスメント
適用される規格および指令に準じてロボットアプリケーションを見直し、存在する危険を評価します。

安全コンセプト
機械的・電気的・組織的対策を通じてロボットアプリケーションの安全を確保するため、きめ細かい技術ソリューションを作成します。

安全設計
必要な保護対策を綿密に練ることで、アプリケーションの危険ゾーンを削減または排除します。

システムの実装
リスクアセスメントと安全コンセプトの結果は、選択した安全対策を通じて個別の要件に合うように実装されます。

妥当性確認
リスクアセスメントと安全コンセプト、および ISO/TS 15066 の制限値に従った衝突測定のパフォーマンスを審査し、反映します。

国際的な適合性
欧州の CE マーキング、米国の OSHA、ブラジルの NR-12、韓国の KOSHA、ロシアの GOST、あるいは中国の CCC などの規制要件に機械が適合していることを保証します。

トレーニングと技術サポート
ロボットの安全アプリケーションに関する専門知識を普及させます。

3.6 産業用ロボット、人とロボットの協働 (HRC)

3.6.1 産業用ロボットの使用に関する規範的仕様

機械指令 2006/42/EC によると、ロボットシステムは半完成機械です。つまり、ロボットシステムは、最初は安全でないものに分類され、CE マーキングが必要であることを意味します。

ロボットシステムは、それ自体では特定された目的を持たないからです。その用途は、ロボットアプリケーションを作成して、ロボットにツールを装備するインテグレータによってのみ定められます。

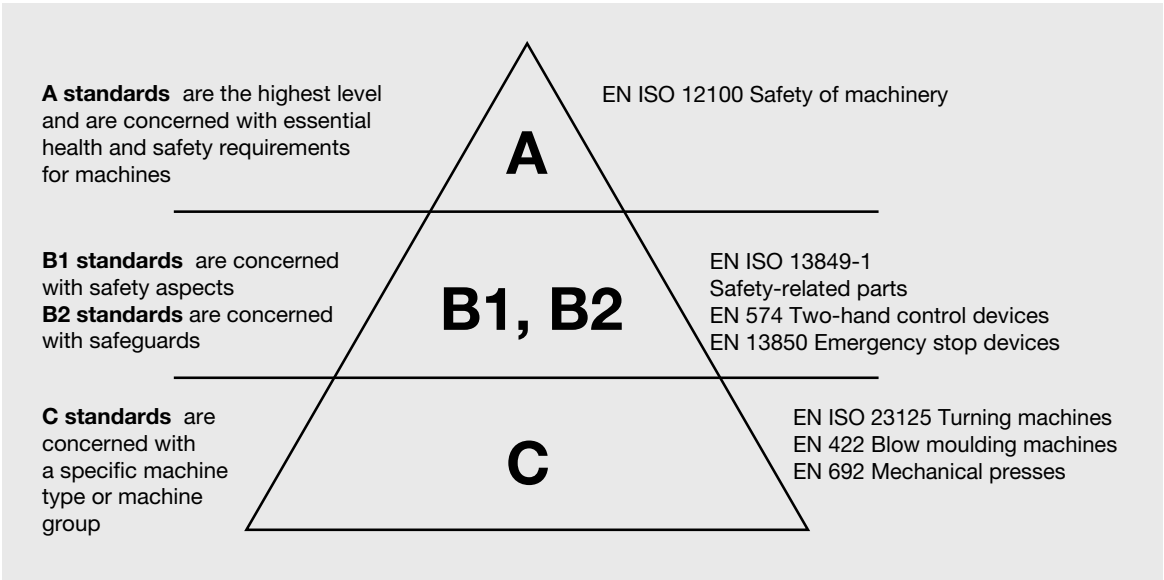
インテグレータは、その機械 (ロボットセル) の市場投入者であり、EC 適合宣言書で終わる適合性評価を実施する必要があります。

詳細な安全要件としては、ISO 10218「産業用ロボットの安全性」パート 1:「ロボット」およびパート 2:「ロボットシステムと統合」という 2 つの規格が、以前は利用できました。両パートの英語バージョンは、EN ISO 10218-1:2011 および EN ISO 10218-2:2011 として発行されており、機械指令 2006/42/EC に列挙されています。

EN ISO 10218-1 は、実際のロボットシステムにのみ関係しています。

これとは対照的に、EN ISO 10218-2 はロボットアプリケーション全体に視点を拡大しています。

どちらの規格も C 規格です。つまり、これらは、階層構造ではタイプ A およびタイプ B 規格の上位に配置される製品別規格です。



しかし、時間とスペースの点でそれぞれの作業エリアが重なる可能性がある、人と機械の実際の協働を安全に実施することに関して言うと、これらの規格は不十分であることがわかっています。これらの規格には抜け穴が存在していましたが、それは ISO/TS 15066 の発行によって閉じられました。

HRC は、協働中、常に人の安全が保証されるようにするための保護対策を要求しています。ISO/TS15066 では、保護原則として 4 種類の協働が詳細に示されています。加えて、人とロボット間の接触の生体力学的な最大許容値も定められています。

3.6 産業用ロボット、人とロボットの協働 (HRC)

3.6.2 EN ISO 10218-2 の観点からのロボットアプリケーション

前述の通り、EN ISO 10218-2 は、より幅広い範囲に重点を置き、ロボットアプリケーション全体を検討しています。

ロボットセルは、以下の部品で構成することができます。

- 産業用ロボット
- エンドエフェクタ (ロボットツール)
- ワークピース
- 機械装置

回転ドライブ技術とは対照的に、ロボット規格では、安全機能に明確な名前や規定がありません。

産業用ロボットシステムの安全機能には、以下のものが含まれる場合があります。

- 安全停止
- 安全減速
- 安全軸制限
- 安全作業スペース監視
- その他

しかし、詳細な仕様は常に製造業者に固有であり、様々に異なる場合があります。この理由から、各製造業者の証書を点検して、安全機能のパフォーマンスレベルを分類できるようにすることが非常に重要です。

制御システムの安全関連部のパフォーマンスレベルは、EN ISO 10218-2 の第 5.2 章に記載されています。5.2.2 では、EN ISO 13849-1 に適合する 2 チャンネル制御構造は、PL d、Cat. 3 と規定されています。

3.6.3 人とロボットの協働と ISO/TS 15066

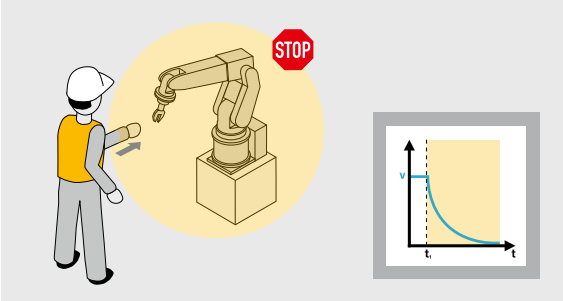
EN ISO 10218-2 は、人とロボットの協働のトピックに簡単にしか触れていません。この理由から、技術仕様の ISO/TS 15066 が作成されました。これは 2016 年 2 月から利用できるようになり、HRC のトピックを詳細に検討しています。

ISO/TS 15066 では、保護原則として 4 種類の協働が示されています。これら 4 つの方法は、HRC アプリケーションの保護対策として、それぞれを個別に適用することも、組み合わせて適用することもできます。

方法 1: 安全適合の監視停止

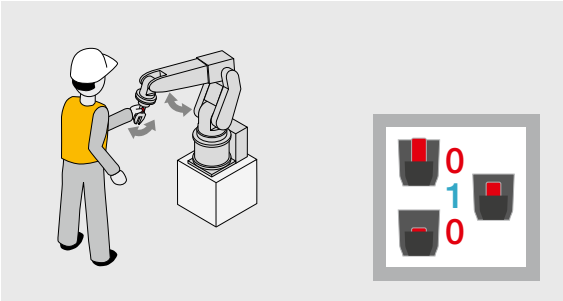
人はロボットが停止した時だけロボットに近づくことができます (「安全適合の監視停止」)。ここでは、センサ技術の各種の面は検討されていません。

ロボットシステムは、不意に自動的に再起動するものであってはなりません。これは、例えば、制御システムの安全関連部の故障によって発生する可能性があります。



方法 2: ハンドガイド

この場合も、人は静止しているロボットにのみ近づくことができます。ロボットシステムのハンドガイドは、手動操作するイネーブル装置によってのみ有効にすることができます。

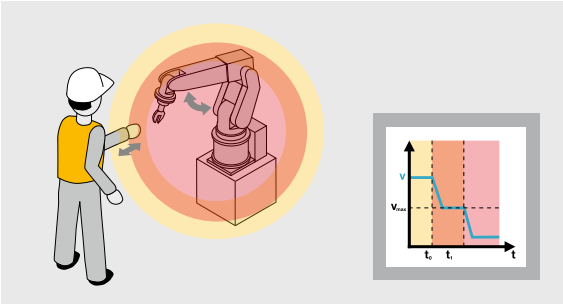


3.6 産業用ロボット、人とロボットの協働 (HRC)

方法 3: 速度および間隔の監視

この方法では、人とロボット間の距離がセンサによって常時監視されます。ロボットシステムは、それに応じて安全に減速した速度で稼働します。

人がロボットに近づけば近づくほど、ロボットの動作が減速されていきます。距離が近くなりすぎると、安全停止が作動します。



安全関連の方法で、方法 3 に完全に対応できるセンサ技術は現時点では市場に存在していません。

固定バージョンで、スキャナや SafetyEYE を使用することで可能です。

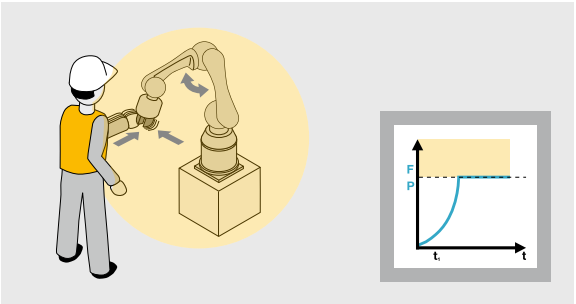
最初の 3 つの方法では、人と機械の間の距離を維持することで安全が保証されます。ここでは、人とロボットの間の接触は許容されません。これらの 3 つの方法のうち 1 つを実装した場合には、特別な HRC ロボットは必要ありません。速度監視または作業スペース監視のための対応する安全パッケージを製造業者が装備した、標準的な産業用ロボットを使用することができます。

方法 4: 動力および力の制限

方法 1 ～ 3 とは対照的に、方法 4 では、「特定の状況」で人とロボットの接触が可能です。しかし、アプリケーションの製造業者は、人とロボットの間の接触が人にとって危険でないことを保証する必要があります。

アプリケーションの製造業者は、適合宣言書への署名によってこれを確認します。

安全な HRC アプリケーションでは、各種の協働に応じて特別に設計されたロボットシステムが必要です。リスク低減は、協働の種類のアプリケーションを通じて実施するか、ロボットおよび作業スペースの本質的に安全な設計によって実施することができます。この場合の「本質的」とは、ロボットシステムの設計特性に起因する危険な接触が発生し得ないことを意味します。



3.6 産業用ロボット、人とロボットの協働 (HRC)

力／動力低減ロボット

センサ技術によって接触を「感知」して動作を停止するロボットシステムです。この接触検出は、ロボット制御システムの一部を使用して行われます。制御システムの安全関連部に有効な要件について、TS 15066 は、先に説明した EN ISO 10218-2 (PL d, Cat.3) の第 5.2 章を参照しています。

接触を低減するには、エッジや角を丸くしたり、パッドを取り付けたり、あるいは接触面をできるだけ大きくして圧力を分散させるなどの設計上の対策を通じた複数の方法があります。技術的な保護対策を用いることもできます (例えば、ロボットの力の低減やロボットの軌道の調整によって、特に傷つきやすい身体領域との接触を避けるなど)。スタッフのトレーニングも、怪我のリスクを低減するために効果があります。

しかし、最終的には、起こり得る接触が、安全性の観点から無害であるかどうかを計算するための計測手順を用いることが絶対的に必要不可欠です。技術仕様 ISO/TS 15066 の附属書 A は、12 の身体領域に分類された 29 の特定の身体部位を示した身体モデルを提供しています。

身体部位モデルは、力や圧力の観点から身体各部 (頭、手、腕、脚など) の痛覚しきい値の詳細を示しています。制限値は痛みが始まる時点を指定します。

これらの制限値は、接触の発生時に、対応する身体領域にかかってよい力の上限を規定します。最も傷つきやすい部位は頭です。想定された用途での使用中に、頭部との接触が発生する可能性を最大限に排除できなければなりません。アプリケーションが、人とロボットの接触時にこの制限の範囲内に保たれる場合には、規格に適合しています。

ISO でも、接触の種類を明確に区別しています。接触には、次の 2 つのタイプがあります。

- **人とロボットの過渡的な接触。**これはロボットからの衝撃に対応します。人は、ロボットに衝突されますが、身を引くことができ、身動きができなくなるわけではありません。この種の接触は、TS 15066 では準静的な接触より危険性が低いと見なされています。そのため、この TS では、人が押しつぶされることがない接触の場合には制限値を 2 倍にすることを認めています。但し頭部は例外です。ここでは、頭部の制限値を 2 倍にすることは認められません。
- **人と機械の準静的な**接触。この接触は人が押しつぶされる衝突に相当します。人のすぐ近くに対抗面 (アプリケーションまたは建築による構造物) があります。回避することができず、対応する身体領域が押しつぶされ、人は身動きがとれず、逃れられない可能性があります。この TS では、接触の最初の 0.5 秒について制限値を 2 倍にすることのみ認めています。しかし、これは頭部に影響する身体領域には有効ではありません。

3.6 産業用ロボット、人とロボットの協働 (HRC)

3.6.4 妥当性確認

妥当性確認とは、実際のアプリケーションの確認を意味します。リスクアセスメントから導き出されたリスク低減対策がすべて完全に実装されていることを再確認します。

アプリケーションは設定が完了し、すぐに出荷できる状態であるべきです。

ロボットセルの妥当性確認フェーズは次のレベルで構成されます。

レベル 1: パフォーマンスレベル (PL) の計算

必要な PL_r は、設計フェーズで既に決定されています。ここでは、すべての安全機能について、要求されるパフォーマンスレベルが、選択された部品によって実際に達成されているかどうかを確かめるためにチェックを実行します。

これは、Safety Calculator PAScal などの支援ツールで実行することもできます。

レベル 2: 安全関連チェック

すべての部品が、完成したロボットセル上に適切に実装されているかどうかをチェックします。目的は、取り付け、プログラミング、試運転の間に異常がないか確認することです。ロボットシステムは自由度が高いため、そのチェックは特に困難です。ロボットの妥当性確認だけでなく、アプリケーションの他のすべての周辺装置の妥当性確認を行う必要があります。

レベル 3: オーバーラン測定

光学的安全防護物がシステムに取り付けられている場合には、それらが EN ISO 13855 に準拠して取り付けられているかどうかのチェックを行う必要があります。これは、校正済みで証書を発行されているオーバーラン測定装置で実行し、試験に合格した場合には、その光学的安全防護物の品質シールによって確認できます。次回の検査時期を、その品質シール上で明確に読み取れるようにしておくことも必要です。

レベル 4: 接触の試験

人とロボットの接触が起こり得る HRC アプリケーションのうち、前述の方法 4 に適合するものは、ISO/TS 15066 の生体力学的制限値を維持する必要があります。

本質的に安全なロボットシステムであるか、力／動力低減ロボットシステムであるかにかかわらず、生体力学的制限値を遵守することは絶対に必要です。

ISO/TS 15066 には、協働ロボットシステムの数学的設計に関する指示が記載されています。しかし、これは理論的アプローチに過ぎません。このアプローチは、過渡的な接触のみを考慮しています。準静的な接触に関する数学的なソリューションはありません。そのため、実際に発生する接触値の実地検証が絶対に必要です。

接触の試験中に、発生する可能性のある接触の全シナリオを、実際の状況で確認します。ここでは、ISO/TS 15066 で提供されている情報を使用して、あらゆる身体部位のシミュレーションを実行します。このために特別に開発された衝突測定装置を使用して、接触の特性値を記録します。

3.6 産業用ロボット、人とロボットの協働 (HRC)

3.6.5 測定の目的

基本的に、ロボットの動作はすべて危険になり得ます。そのため、人をロボットから保護する必要があります。作業者を保護するために、これまで実践されていたことは、人と機械の厳格な分離でした。ロボットは作業の実施中は常にセル内に隔離されていました。

しかし、新世代のロボットや技術のおかげで、最近では、接触が危険でなくなった場合には安全柵は不要になることがあります。

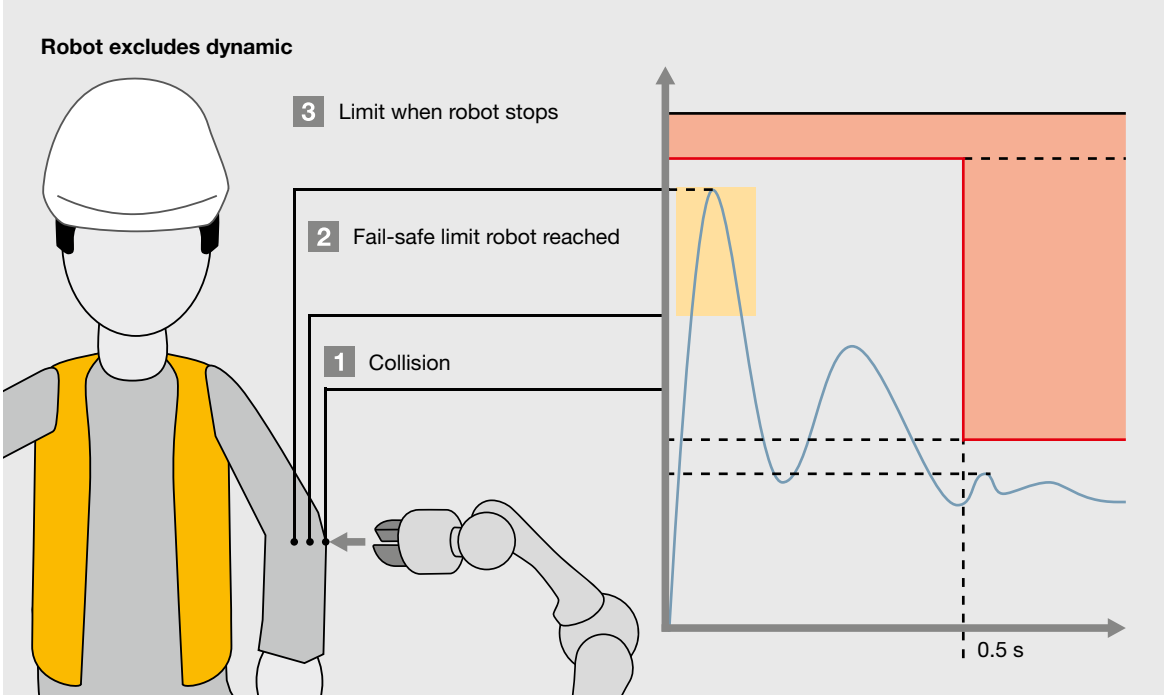
人とロボットが作業スペースを共有し、安全を確保するための安全柵が存在しないロボットアプリケーションでは、CE マーキングプロセスの責任者は、制限値を遵守する責任があります。

ロボットシステムはこれを自分で行うことができないからです。ロボットシステムは、力学を考慮に入れていません。

力／動力低減ロボットシステムでは、制御システムの安全関連部に制限値を入力します。これらは接触を安全なものにすることを目的としています。しかし、これらの値は絶対的なものとは見なされません。

実際には何が起きるでしょうか？

1. 接触が発生すると、ロボットは、まず抵抗を「感知」します。最初は、ロボットの力は規定された力の上限に達していません。ロボットは軌道を維持しようとして、ドライブの動力を増やします。
2. 反対に動く力が増すと、ロボットは接触について設定された力の制限に達します。
3. ロボットは、この時点で初めて動作を停止し始めます。停止距離は、接触後、つまり人体に達してから発生します。



HRC の方法 4 に注意

3.6 産業用ロボット、人とロボットの協働 (HRC)

規格適合の人とロボットの協働用の衝突測定セット

軽量なロボットであっても、オーバーランと応答時間の問題を検討する必要があります。実際には、接触値が設定値の数倍に達することもあります。

通常は、ロボットの動力の低減が唯一の解決策です。

それでもなお、誠意を持って適合性宣言書を提出できるようにするためには、技術的測定を使用して接触値をチェックすることが必要不可欠です。

そのような測定の種類やその他の測定手法は、理解しやすく、透明性があり、再現可能であることが重要です。

この特定の力と圧力を測定するためにピルツが衝突測定装置、PROBmdf を開発したのは、そのためです。スプリングとそれに対応するセンサを備えた装置によって、人体にかかる力を正確に測定し、制限値と比較します。この測定装置は、ロボットのアームと、柔軟性のない固定面との間の、リスクアセスメントで決定された位置に取り付けられます。これは、作業者がロボットと設備の間で押しつぶされる場合などの準静的な接触をシミュレートします。測定はソフトウェアを通じて開始され、その後、データが処理されて文書化されます。

試験は、測定ポイントに応じて、最大 10 回まで実施することが推奨されます。妥当性確認には、最高値、すなわち「最悪のケース」が使用されます。制限値を超えた場合には、追加の安全対策としてライトグリッドやガードなどを取り付ける必要があります。

この衝突測定装置は、ISO/TS 15066 に適合するピルツの完全な妥当性確認製品セットの一部になっています。このセットには、フィルムやスキャナを使用する測定装置に加え、各種の身体部位をシミュレートするために使用できる様々なスプリングが含まれています。ピルツは、トレーニング、メンテナンス、校正、定期的なアップデートが含まれる製品セットをレンタルで提供しています。

3.7 EN ISO 13849-1 に適合する安全プログラミング

大多数の安全技術やこれに課される要件に対応する上で最適なハードウェアが設置された、とします。

ユーザは次に、EN ISO 13849-1 に準拠して進め、製造業者が規定した $B10_D$ 値、$MTTF_D$ 値または PFH_D 値を使用して、安全機能のパフォーマンスレベルを決定することになります。(注 : アーキテクチャ、診断範囲なども要求されます。) ここでは、安全機能の実装にプログラマブルシステム (制御システム) を使用することがますます増えているという事実が見過ごされがちです。現在では、これらの制御システムのアプリケーションプログラム (SRASW) も安全機能の品質に影響を与えるため、ソフトウェアエンジニアリングについて、対応する方法や手順を規定し、適用する必要もあります。実際のプログラミング (コーディング) だけでは十分ではないからです。

よく言われることですが、「バグのないソフトウェアなど存在しません！」どれほど慎重に苦労してプログラミングをしても、プログラミングコードのエラーは避けられません。1,000 行のコードには、平均で 2 つのエラーが含まれると考えられます。

ソフトウェアのエラーが致命的となった例に、「セラック 25」があります。このケースでは、ソフトウェアのエラーによって、がん性腫瘍の放射線療法を行う装置が、過剰な放射線を照射したことで、3 年間で 3 人の犠牲者を出しました (https://ja.wikipedia.org/wiki/Therac-25)。

一般的なソフトウェアのエラーとはどのようなものでしょうか？プログラミングエラーまたはバグとも呼ばれるソフトウェアのエラーの例は以下の通りです。

- 構文エラー : 文法規則の違反
- セマンティックエラー : コマンドコードの混同など
- ランタイムエラー : 連続ループなど
- 論理エラー : 不正確な解決方法など
- 設計エラー : 要件定義におけるエラーなど
- 動作エラー : 動作コンセプトの混乱など

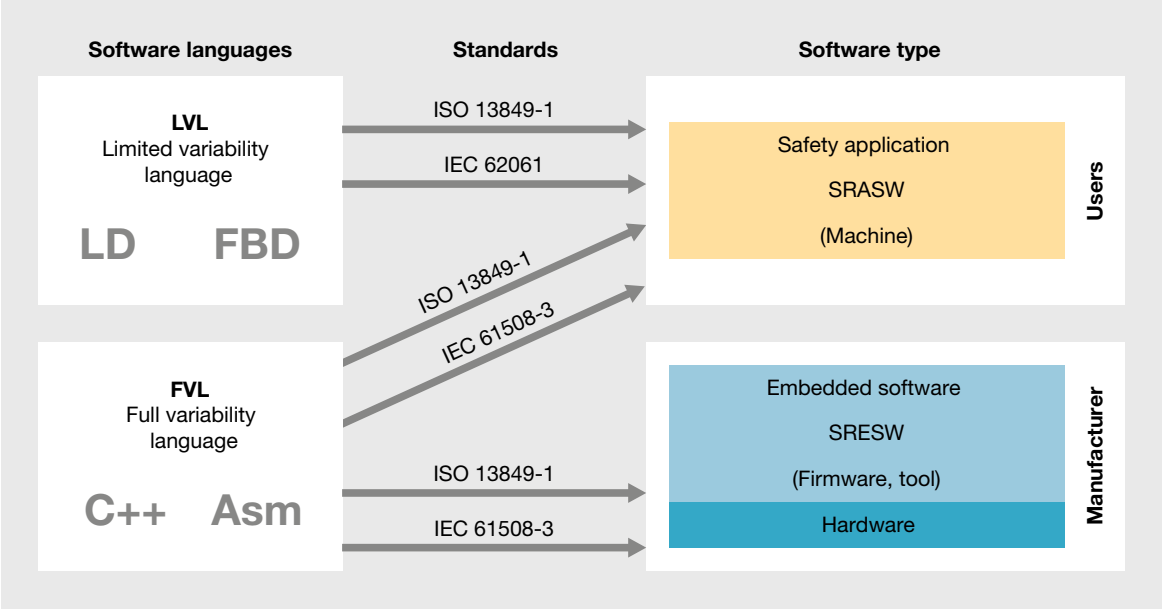
3.7.1 安全関連ソフトウェア

安全コントローラ (PSS 4000 など) には、安全関連ソフトウェアと呼ばれる 2 種類のソフトウェアが含まれます。ソフトウェアが安全コントローラの機能の製造業者によって開発されたか、ユーザによって開発されたかで区別されます。製造業者によって開発されたソフトウェアはファームウェアまたはオペレーティングシステムとも呼ばれ、EN ISO 13849-1 の規範的な用語では、安全関連組込みソフトウェア (SRESW) と呼ばれます。アプリケーションプログラムとも呼ばれる、安全コントローラのユーザが開発したソフトウェアは、安全関連アプリケーションソフトウェア (SRASW) と呼ばれます。

さらに、EN ISO 13849-1 には、このアプリケーションソフトウェア (SRASW) を開発するための 2 種類のプログラミング言語も区別しています。

無制限あるいはあらゆる種類の言語を対象とするプログラミング言語は、無制約可変言語 (FVL) と呼ばれます。FVL 言語の一般的な例には、C または C++ があります。これらの言語のアプリケーション分野には、SRESW の開発なども含まれます。

3.7 EN ISO 13849-1 に適合する安全プログラミング



一方、言語や機能の範囲が制限されるプログラミング言語は、制約可変言語 (LVL) と呼ばれています。これらの言語は、主に SRASW の開発に使用されます。これらの言語には、過去に開発されたライブラリファンクションを、新しいアプリケーションコードと結合できるという特性があるため、安全機能に要求される仕様に適合しています。LVL の典型的な例には、ラダーダイアグラムやファンクションブロックなどの PLC 言語があります。オートメーションシステムの PSS 4000 では、LVL としてプログラミング言語のストラクチャードテキストを使用することも可能です。C や C++ のような高水準言語機能を、LVL とも見なされ得る程度に制限するコントローラ製造業者がますます多くなっています。

安全関連組込みソフトウェアの開発については、これ以上詳しくは取り上げません。SRASW の開発での FVL の使用も、推奨できません。これらのプログラミング言語を使用すると系統的なプログラミングエラーの確率が増すからです。

3.7.2 リスクアセスメントに関するソフトウェア

安全関連の保護対策が EN ISO 12100 に基づくリスクアセスメントの一環として規定されている場合には、安全コントローラや安全機能が統合されたオートメーションシステムの使用が増加します。既に述べた通り、ここでは、安全コントローラをハードウェア部品としてパフォーマンスレベルで分類することだけが重要なのではありません。安全関連アプリケーションソフトウェアのエンジニアリングも、安全機能の品質に影響を与えます。EN ISO 13849-1 に準拠して要求されるパフォーマンスレベルに基づいて、安全関連アプリケーションソフトウェアはパフォーマンスレベルにも適合する必要があります。

例えば、安全機能が PL d のパフォーマンスレベルを必要としている場合には、SRASW は、少なくとも PL d のパフォーマンスレベルを達成する対策に対応する必要があります。逆の場合、パフォーマンスレベル PL e の要件を満たす SRASW の開発を行っても、安全コントローラ全体は、パフォーマンスレベル PL c のハードウェアを併用した場合、最終的には PL c のパフォーマンスレベルしか達成しないことになります。

3.7 EN ISO 13849-1 に適合する安全プログラミング

3.7.3 ソフトウェア開発の基本的要件

SRASW の開発に課される要件は、EN ISO 1384-1 のセクション 4.6.3 でより詳細に検討されています。ここでは、開発するソフトウェアの要件に加え、開発ツールと開発プロセスにも要件が課されています。

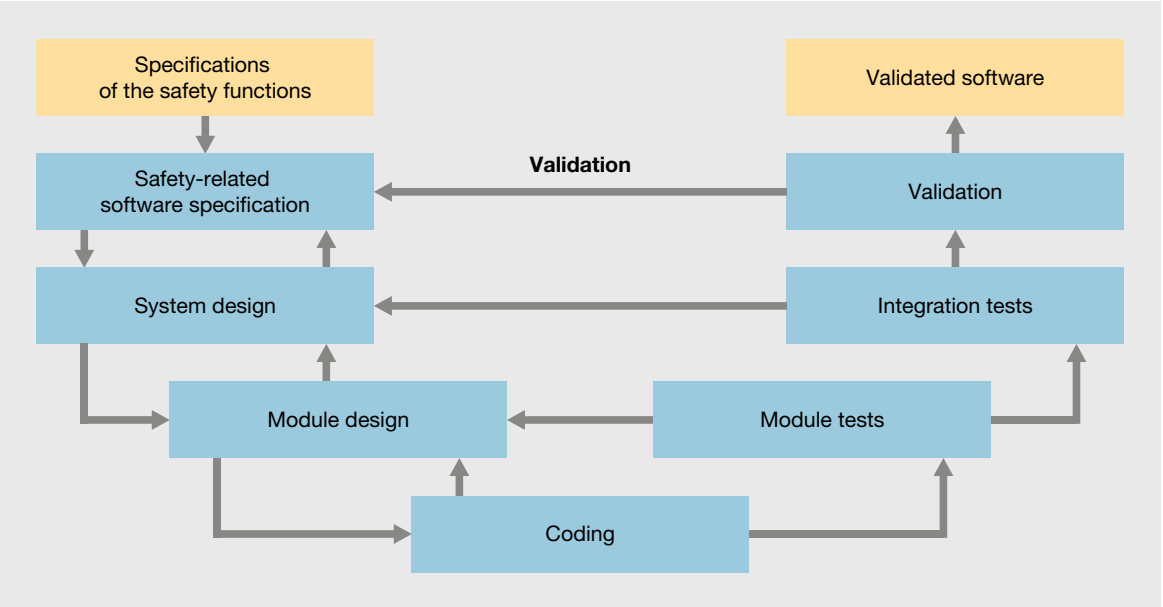
パフォーマンスレベルが a から e までの安全機能で使用される SRASW の一般要件は以下の通りです。

- 検証と妥当性確認を伴う開発ライフサイクル
- 仕様と設計の文書化
- モジュラ式の構造化プログラミング
- ファンクションテスト
- 改造後の適切な開発活動

安全関連ソフトウェアの開発サイクルは、簡易版の V モデルを使用して表すこともできます。V モデルの左の枝は、ソフトウェア開発の設計関連の開発段階を示しています。ここでは、過去の作業段階の結果と比較して、各開発段階を検証 (チェック) します。V モデルの右の枝は、検証および妥当性確認とも呼ばれるチェックを実行する時の活動を表しています。このモデルは、各設計関連開発段階には検証または妥当性確認が伴う一方で、試験に必要な試験計画は、開発段階と並行し、かつ開発段階とは独立して既に作成済みであるべきだということも説明しています。

エラー防止対策とともに、V モデルを一貫して適用することは、エラーを最小限に抑えたソフトウェアエンジニアリング／開発につながるはずです。EN ISO 13849-1 に適合する安全関連ソフトウェアの最も重要な要件である、読みやすい、わかりやすい、テスト可能、使いやすいという特質によって分類されるソフトウェアです。モジュラ式の構造化プログラムの開発も、結果として当然に保証されるはずです。SRASW をプログラミングする際に選択できる良い方法の 1 つとして、製造業者が証明済みのソフトウェアモジュール／ブロックを参照することがあります。

実際には、変更によって開発は頻繁に中断されますが、それは自然なことです。開発中は、これらを日常的に考慮し、その影響を評価 (インパクト分析) する必要があります。これらの活動はすべて、V モデルに従って実行し、変更履歴を使用して記録もすべきです。どのような場合でも、開発プロセスの全活動を文書化することは当然に義務付けられています。



3.7 EN ISO 13849-1 に適合する安全プログラミング

3.7.4 パフォーマンスレベルを向上させるための追加的な故障防止対策

既に述べた通り、PL a ～ e までのパフォーマンスレベルを達成するには基本的な対策が必要です。さらに、パフォーマンスレベルが PL c から e に増加する場合には、追加的な故障防止対策を導入する必要があります。SRASW の仕様を確認するとともに、安全機能、パフォーマンス基準、制御アーキテクチャの他、外部エラーの検出と取扱いに関する正確な情報を、ライフサイクルに関与する人々に提供する必要があります。

さらに、ツールの選択には特別な注意を払う必要があります。

3.7.5 プログラミングツール、言語、ライブラリ

この意味でのツールは、プログラミングツール、ライブラリ、言語の選択と理解されています。

プログラミングツールは、以下のような系統的エラーの防止機能を備えているべきです。

- データ型の不一致
- インタフェースの不完全な呼出し
- 再帰
- …

チェックはコンパイル時には既に実行済みでなければならず、ソフトウェアのランタイムまで待つべきではありません。

さらに、使用されるプログラミングツールは、モジュラ式プログラミング手順のアプリケーションに適しており、IEC-61131-3 で認められた言語のサブセットを使用するべきです。一般に、ラダーダイアグラムやファンクションブロックなどのグラフィック言語は、純粋なテキストベース言語より読みやすく、理解しやすくなっています。グラフィック型プログラミング言語の使用が推奨されているのはそのためです。

プログラミングツールの PAS4000 は、オートメーションシステム PSS 4000 の一部ですが、インストラクションリストやストラクチャードテキストなどのテキスト型プログラミング言語だけでなく、ラダーダイアグラムやピルツ独自の PASmulti など、グラフィック型プログラミング言語も提供しています。

PNOZmulti のグラフィックプログラミングは PNOZmulti 製品レンジの一部です。

検証済みのファンクションブロックライブラリは、可能な場合は常に参照すべきです。安全システムの製造業者は、プログラミングツールのライブラリで検証済み・証明済みのファンクションブロックを多数提供しています。もう 1 つのオプションは、EN ISO 13849-1 に適合する SRASW 開発の要件に基づき、各種のプロジェクトにおいて開発・文書化されたアプリケーション固有のファンクションブロックライブラリを参照することです。

3.7.6 ソフトウェアの構造化とモジュラ構造

クリーンな構造化とモジュラ式で設計されたソフトウェアは、故障防止と変更処理のための基盤となります。これには、ソフトウェアの仕様と設計フェーズという早い時点で注意を払う必要があり、この手順は、検証済みのライブラリファンクションブロックを使用することでサポートされます。独自に開発したブロックの場合には、データまたは制御フローを表すために準公式的な手順 (グラフィカルな方法) も適用する必要があります。ステータスダイアグラムやプログラムフローチャートなどの方法は、特にこれに適しています。開発するファンクションブロックは、コードの長さを最小限にしてプログラムし、entry と exit で実行する必要があります。

3.7 EN ISO 13849-1 に適合する安全プログラミング

3 段階のアーキテクチャはが優れていることは、以下のように実証されています。

- 入力 : 安全入力を通じて安全センサの情報と信号を記録する
- 処理 : 安全な状態につながる安全機能を実装するために情報を処理する
- 出力 : 安全出力を通じて作業者ファンクションを作動させる

安全出力の作動とともに、これらを 1 つのプログラムセクションでのみ使用することが非常に重要です。ここで、これらの規範的要件を遵守しないと、特に、設備と機械レベルで危険な状態が発生する恐れがあります。一般に、SRASW のプログラマは、防御的プログラミング形式を採用する必要があります。防御的プログラミングでは、ランタイム時に (プログラム内の) 異常なプロセス、データ、値を検出し、事前に決定した方法でこれらに対応するソフトウェアの開発を目標としています。

これは、例えば、以下を通じて実現することができます。

- 変数の範囲チェック
- 値の妥当性テスト
- セット・リセットコマンドの回避
- ソフトウェアのグループ化と構造化

3.7.7 部品の SRASW と非 SRASW

PSS 4000 など最新のオートメーションシステムは、非安全関連のプログラミングと安全関連のプログラミングを結合します。特に、この種のコントローラを使用する場合あるいはこの種のオートメーションシステム向けのソフトウェアの開発時には、これらのソフトウェアコンポーネントは、異なるファンクションブロックで、定義されたインタフェースとともに実装しなければなりません。安全関連データと非安全関連データの間の論理結合が作成されていない結果として、安全関連信号の整合性が低下する (例 : これらの信号の OR リンクを通じて) ことは特に重要です。

3.7.8 ソフトウェアの実装とコーディング

EN ISO 13849-1 からの要件は、コードは読みやすく、理解しやすく、かつテスト可能でなければならないということです。したがって、組織内で明確なプログラミングガイドラインを定義することが重要です。プログラマは全員、これらのガイドラインを理解し、適用できなければなりません。規範的要件の 1 つに、ハードウェアのアドレス (E1.0 など) の使用は避け、その代わりにシンボリック変数 (Input_EStop_Channel 1 など) を使用する必要があると定められているように、プログラミングガイドライン (コーディング規則) には、変数の構文などを含めることができます。

作成したコード (アプリケーションプログラム) は、可能な場合は、シミュレーションや、制御およびデータフロー分析 (PL d と e の場合) を使用して検証すべきです。

3.7 EN ISO 13849-1 に適合する安全プログラミング

3.7.9 テスト

非常に時間がかかるテストフェーズは、多くの場合、ソフトウェアのコーディング後に行われます。既に述べた通り、SRASW の開発時には、エラーを防止する対策をすべて講じた場合でも、エラーが発生する可能性があります。これらのエラーは、可能な場合には常にテストフェーズで発見すべきです。このテストフェーズを十分に実行できるようにするには、仕様フェーズと同時に詳細なテスト計画の作成に着手する必要があります。この計画には、テストの完了条件と使用ツールとともに、すべてのテストケースをリストアップしておくべきです。

機能的挙動とパフォーマンス基準のブラックボックステストにより、十分な検証方法が構成されます。ブラックボックステストとは、テスト対象の内部構造に関する知識なしに、テスト基準を作成し、実行する方法を言います。PL d と PL e のソフトウェアの場合には、制限値の分析に基づき実行するテストケースが推奨されます。この場合、システムは、想定されているアプリケーションの範囲を超えて慎重にテストされます。例えば、パラメータは、規定された制限値より高い値にさらされる可能性があります。しかし、ブラックボックステストを開始する前に、I/O テストを用いて、使用される安全関連信号が SRASW で正確に使用されていることも確認すべきです。

PL ／カテゴリ	EN ISO 13849-2 に適合する確認手段
すべての PL_r	機能的挙動とパフォーマンス (時間特性など) のブラックボックステスト
PL_r d または e の場合に推奨	加えて、制限値分析に基づく拡張テストケース
すべての PL_r	安全関連の入力および出力信号が正確に使用されていることを確認するための I/O テスト
故障検出を伴う PL_r およびカテゴリ	ソフトウェアベースの故障制御対策の適合性を評価するために、分析的に予め決定された故障とともに、予測される対応をシミュレートするテストケース

3.7 EN ISO 13849-1 に適合する安全プログラミング

3.7.10 文書化

開発ライフサイクルでは、実行コードの結果に加え、すべての活動を文書化する必要があります。SRASW に対する変更がそれ以降に実施された場合には、それも文書化する必要があります。完全で、利用可能で、読みやすく、理解しやすくなければならないという原則は、文書化にも適用されます。 ファンクションブロックは、これらの要件に従ってコード内で文書化する必要があります。また、ファンクションブロックはすべてモジュールの見出しを含んでいなければならないという要求もあります。これには、法人の機能の概要、I/O の概要、バージョン、仕様などが含まれている必要があります。さらに、コードに関する十分なコメントと宣言行を提供する必要があります。

3.7.11 検証

検証では、多くの場合、「4 つの目」の原則と呼ばれるコードレビュー方法が用いられます。4 つの目の原則とは、文書またはコードのチェックは、作成者ではなく別の適格な者が行うということを意味します。

3.7.12 コンフィグレーションマネジメント

コンフィグレーションマネジメントは、SRASW を開発する会社に推奨されます。これは、SRASW の開発に関して作成されたすべての関連文書、ソフトウェア、モジュール、テスト結果、ツールのコンフィギュレーションを特定し、アーカイブする必要があることを意味しています。

3.7.13 変更

SRASW に対する変更のすべてについて、チェックを実行し、この変更が、ソフトウェアの開発に関する EN ISO 13849-1 からの要件および安全性にどの程度影響を及ぼすか見極める必要があります。これは、SRASW に対する変更に関してであっても、V モデルだけでなく、規範的な仕様と方法を適用しなければならないことを意味しています。さらに、変更は明確かつ十分に文書化する必要があります。

3.7.14 概要

安全関連ソフトウェアの設計エンジニア、開発者、プログラマはすべて、適切なコンポーネント (ハードウェア) の選択を行うだけでなく、SRASW 開発の体系的なアプローチにも従うべきです。ソフトウェアとそれに含まれる可能性のあるエラーは、安全品質において重要な役割を果たすため、ハードウェアコンポーネントの適切な選択と同程度に重視すべきです。

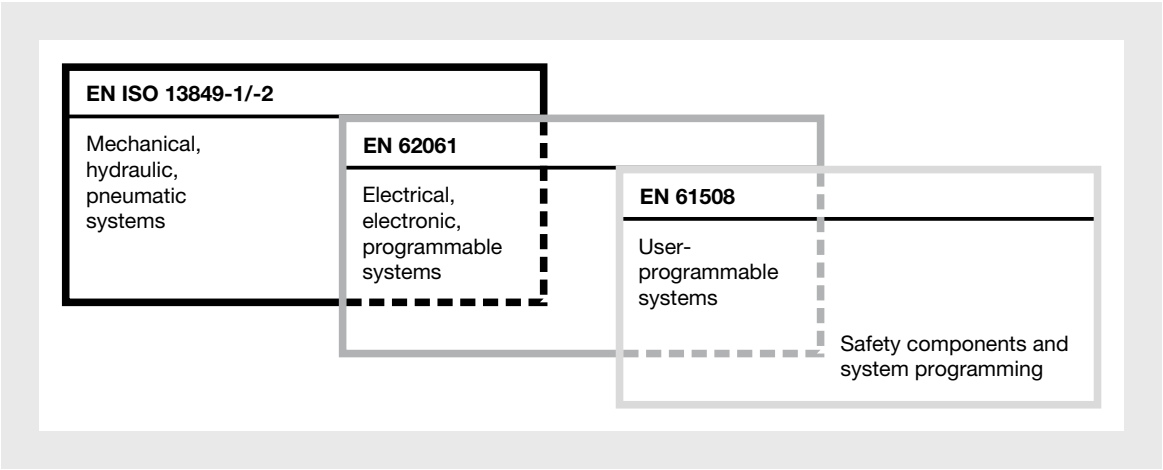
また、ここに記載する対策は、努力なしには開発・適用できないことを認識することが必要です。

3.8 妥当性確認

妥当性確認 (Validation: ラテン語で強い、強力、健康的を意味する validus が語源) とは、実行しようとしている作業および関連する問題解決に関する計画または解決法のテストを表しています。検証とは、対応する仕様に関する計画または解決法のテストを表しています。これらを合わせた両方のプロセスは、それぞれの解決法の適合性を証明するために使用されます。

機械工学では、妥当性確認のプロセスは、設備または機械が特定の想定用途の要件を満たしているという証拠を提供する必要があります。検証のプロセスも、制御システムの技術的装置と安全関連部の機能を検査し、それによって、これらが仕様に従って安全に機能を実行することを確認するものです。検証と妥当性確認のプロセスから得た結果と解決法を文書化することで、設定した目標が実際に達成されたことを確認します。

整合規格の EN ISO 12100 は、その基本的な専門用語、設計の原則、リスクアセスメント (分析と推定) の手順に加えて、リスクアセスメントの原則とリスク低減によって、安全関連システムまたは機械や設備の制御システムの安全関連部に適用される主要な手順を規定しています。以下のその他の整合規格は、この基本となる規格を基盤として使用して、制御システムの安全関連部と安全防護物の設計、構造、統合について定めています。EN ISO 13849-1/-2、および EN 61508 とその分野別規格である EN 62061 (妥当性確認の出典)。EN 62061 とは対照的に、EN ISO 13849-1/-2 は電気的システムに制限されておらず、機械的システム、空圧システム、油圧システムにも適用できます。両規格 (EN ISO 13849-1/-2 と EN 62061) とも、機械に関する安全関連制御システムの設計と実装に関する基本的要件を規定しており、無効となった EN 954-1 の後継規格です。EN ISO 13849-1 または EN 62061 を適用する場合、制御システムの安全関連部の設計と実装および妥当性確認プロセス内のその後のアセスメントに多くの相違点があります。



一般規格と分野別規格の構造と重複部分

3.8 妥当性確認

3.8.1 EN ISO 13849-1/2 に適合した安全機能の検証

要求される特性データ : PL、(制御) カテゴリ、$MTTF_d$、DC、CCF、$B10_d$

規定された要件は、安全機能を実装するための設計 (コンポーネントとアーキテクチャの選択) の基盤となります。計画されたコンポーネントはサブシステムに分類され、達成可能なパフォーマンスレベル (PL) が明確化されます。計画された安全機能の検証 : 達成可能な PL ≥ PL_r。妥当性確認プロセスでは、全体的な仕様の範囲内で、設備と機械に関する制御システムの安全関連部のコンフィグレーションと機能の適合性を確認します。注 : 各種の機械システム向けの妥当性確認プロセスの実施方法と妥当性確認ツールに関するガイダンスは、EN ISO 13849-2 で確認することができます。

3.8.2 EN 62061 に適合した安全機能の検証

要求される特性データ : PFH、SIL、$MTTF_d$、DC、CCF、$B10_d$。安全機能の実装は、規定された要件に基づき設計されます。これには適切な部品の選択と一貫性のあるアーキテクチャの開発が伴います。計画された部品はサブシステムに分類され、安全度水準 (SIL) を決定する基盤となります。計画された安全機能の検証 : 達成した SIL ≥ 要求される SIL。

PL (EN ISO 13849-1)	SIL (EN 62061)
a	-
b	1
c	1
d	2
e	3
-	4

パフォーマンスレベル (PL) と安全度水準 (SIL) の比較チャート

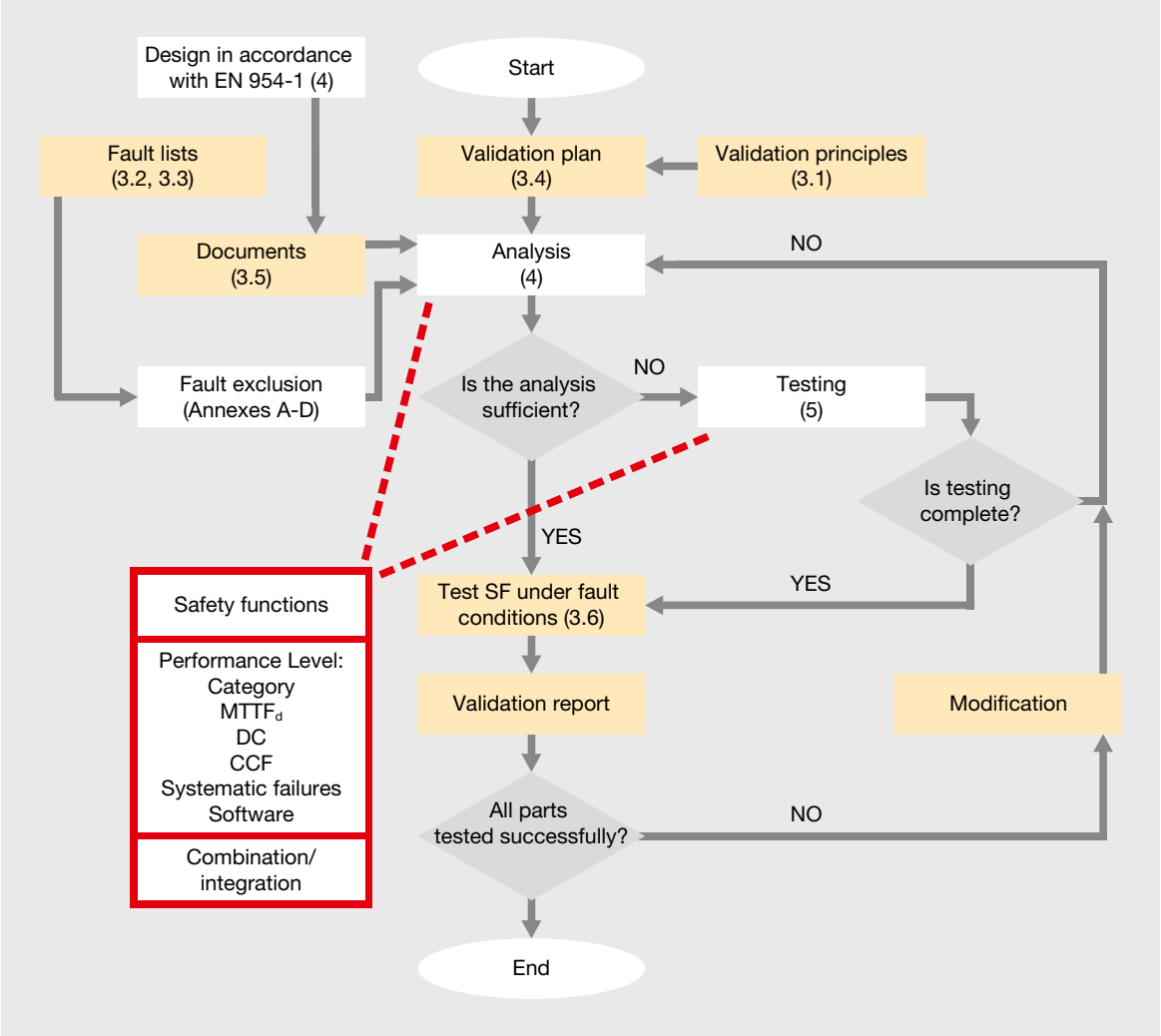
制御システムの安全関連部の検証では、要件と仕様が、適用される規格と安全関連仕様に従って満たされていることを証明する必要があります。これらの要件は、特に以下を参照します。

- リスクアセスメントと安全コンセプト／設計に従って定められた安全機能の特質
- 安全機能に応じて定められたカテゴリの規格適合アーキテクチャ

制御システムの安全関連部の検証は、徹底的な分析に加え、必要な場合には追加の (機能) テストと故障シミュレーションで構成されます。分析は、設計プロセスの開始と同時に始めることが推奨されます。そうすることで、故障／問題が早期に特定され、それに応じて対処することができるからです。

分析とテストの実行方法は、制御システムの規模、複雑さ、設備または機械内での統合方法によって異なります。したがって、特定の分析やテストについては、制御システムの開発が一定レベルに達して初めて実行することは理に適っています。分析は、その独立性を確保するために、独立した人物または機関に委託するべきです。妥当性確認を実施するには、まず妥当性確認計画を作成し、分析とテストの範囲を決定する必要があります。正確な範囲と 2 つのプロセスのバランスは、使用されている技術とその複雑さによって常に異なります。次ページの図は、妥当性確認プロセスの概要を図示しています。

3.8 妥当性確認



EN ISO 13849-2 に適合する妥当性確認計画

3.8.3 妥当性確認計画に関する一般情報

妥当性確認計画には、指定された安全機能とそのカテゴリの妥当性確認を実施するための要件をすべて記載する必要があります。また、妥当性確認計画では、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ります。テスト対象の制御システムまたは機械の複雑さによっては、妥当性確認計画において、以下の情報を提供する必要があります。

- 妥当性確認計画を実施するための要件
- 操作条件と環境条件
- 基本的な安全原理と十分に吟味された安全原理
- 十分に吟味された部品
- 故障の想定と故障の除外
- 適用する分析とテスト

妥当性確認計画には、妥当性確認文書もすべて含まれます。

3.8 妥当性確認

3.8.4 分析による妥当性確認

制御システムの安全関連部の妥当性確認は主に分析によって行います。安全機能 (SRCF) に要求される特質のすべてを実際に備えていることを示す証拠を提供する必要があります。分析には以下の要因が含まれます。

- 機械に関連して特定されたハザード
- 信頼性
- システム構造
- システムの挙動に影響する、定量化できない質的側面
- 経験値、高品質な機能、故障率などの確定論的な論点

「トップダウン」／「ボトムアップ」分析手法

分析手法は、2 種類の手法から選択することができます。演繹的な「トップダウン」手法と機能的な「ボトムアップ」手法です。演繹的な「トップダウン」手法は、フォルトツリー解析またはイベントツリー解析の形で適用できます。帰納的な「ボトムアップ」手法の例には、故障モードと影響解析 (FMEA) と故障モード、影響および致命度解析 (FMECA) があります。

3.8.5 テストによる妥当性確認

分析による妥当性確認が十分でない場合には、妥当性確認を完了するために追加のテストが必要になります。制御システムとその要件の多くが複雑を極めるため、ほとんどの場合で追加テストを実行することが必要です。

実際には、テストにはテスト計画が要求され、これには以下を含む必要があります。

- テストの仕様
- 予測される結果
- 各テストの時系列での記載

テスト結果は、追跡可能な方法で文書化する必要があり、テスト記録は、最低でも以下を含んでいる必要があります。

- テストを実施した個人または機関の名前
- テスト時点の環境条件
- テストの手順と使用機器

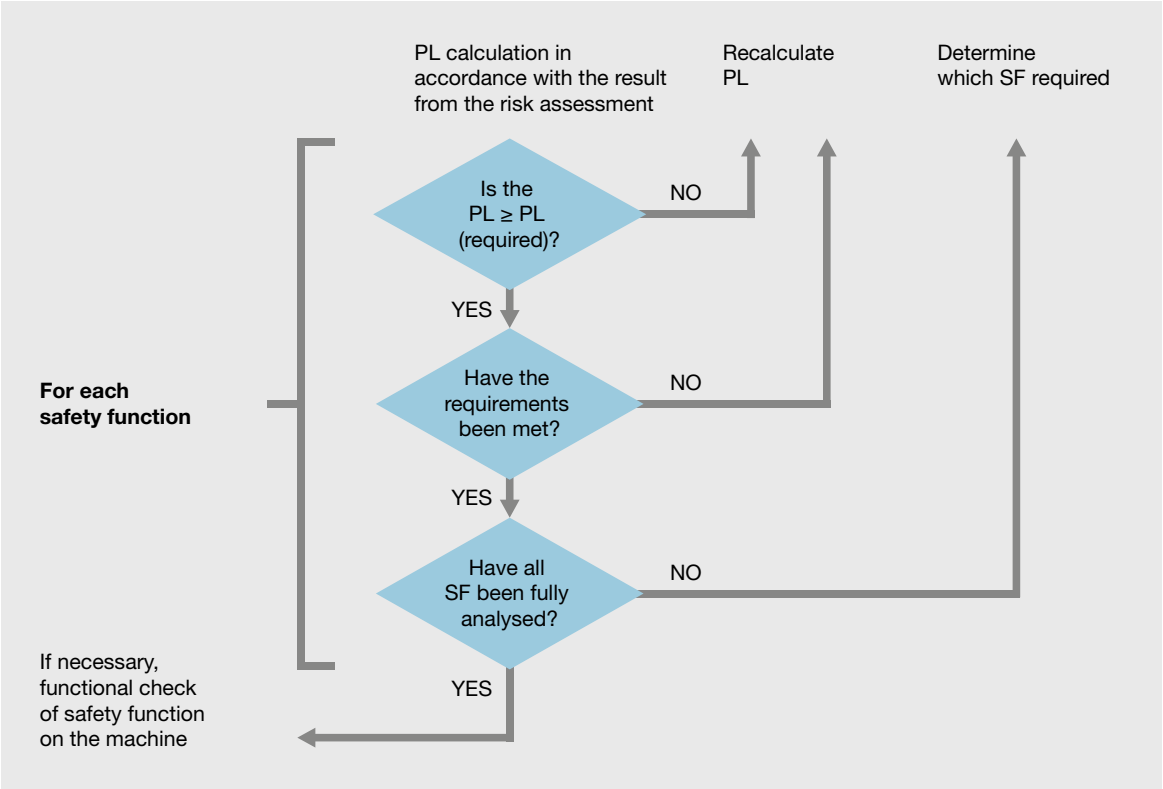
目的と所定の安全目標が実際に達成されていることを証明するために、テスト結果は、その後、テスト計画の仕様と比較されます。

3.8.6 安全機能の検証

妥当性確認の重要な要素は、安全機能が意図した仕様、機能、カテゴリ、アーキテクチャに適合していることを検証することです。規定された安全機能の妥当性確認を、設備／機械のすべてのオペレーティングモードで行うことが重要です。各安全機能の基本的な妥当性確認とともに、安全機能内の PL/SIL 値の妥当性確認にも重要な役割があります。以下のステップは、PL を達成した安全機能を検証する際に要求されます。

- カテゴリの妥当性確認
- $MTTF_d$ 値の妥当性確認
- DC 値の妥当性確認
- 共通原因故障／ CCF 対策の妥当性確認
- 決定論的原因故障対策の妥当性確認

3.8 妥当性確認



検証および妥当性確認のフローチャート (出典 : ピルツのトレーニング教材)

安全機能の妥当性確認は非常に複雑なプロセスであるため、この場合には、計画／実装された安全機能の計算に使用できるソフトウェアツール (PAScal など) を使用することが得策です。これらの計算ツールは、計画された (または採用された) 部品の安全関連の特性値に基づいて、必要とされる値や要求されるデフォルト値 (PL_r または SIL) などの値の妥当性を確認します。ソフトウェアベースツールの利点は、安全機能の妥当性確認に伴う各段階をステップごとにガイドしてくれる点です。テスト実施者は、安全機能のグラフィックモデリングツール内のオプションを利用することで、計算のセキュリティを強化するとともに、結果の追跡可能性を高めることができます。

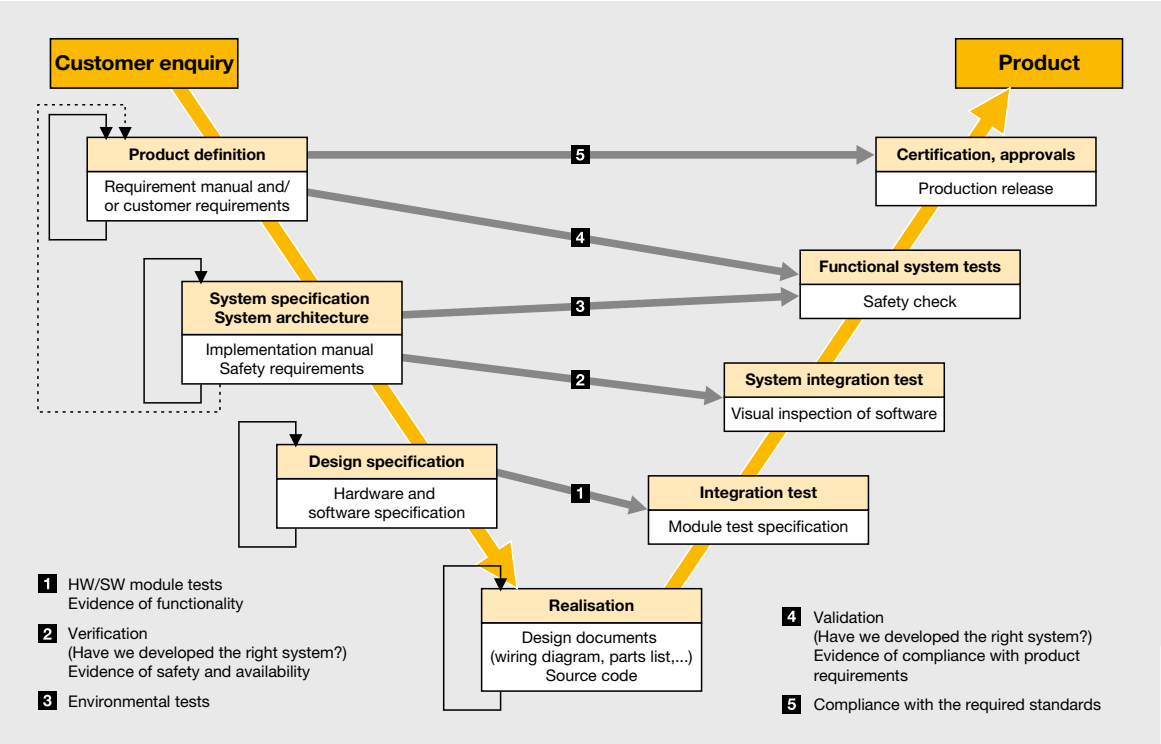
3.8 妥当性確認

3.8.7 ソフトウェアの妥当性確認

EN 62061 および EN ISO 13849-1/-2 規格の規定は、すべてのパフォーマンスレベルと安全度水準に対する、機械分野における安全関連ソフトウェアの開発を認めています。その結果、ソフトウェアは、高度の責任を担い、実装される安全機能の品質を大きく左右します。そのため、作成されたソフトウェアが明確で、読みやすく、テストとメンテナンスが可能であることは極めて重要です。ソフトウェアの品質を保証するために、ソフトウェアは開発時にも妥当性確認プロセスの対象とされています。基本原則は以下の通りです。

- V モデルに従って作業を進めること (検証および妥当性確認を含む開発ライフサイクル)
- 仕様と設計の文書化
- モジュラ式の構造化プログラミング
- ファンクションテストの実施
- 変更または調整後の適切な開発活動

この場合には、ソフトウェアが安全要件仕様に適合していることを確認するために対応するレポートも作成します。このレポートは設備または機械に妥当性確認レポートの一部となります。安全機能の妥当性確認と同様に、ソフトウェアに対しても、プログラマ自身ではなく独立第三者による妥当性確認を行うべきです。



Pilz GmbH & Co. KG のエンジニアリングプロジェクト向けの V モデル

3.8 妥当性確認

今日では、関連する安全制御システムの安全関連ソフトウェアの開発とプログラミングに利用できる非常に優れた証明済みのソフトウェアツールがいくつか存在しています。ソフトウェアツールを利用することで、妥当性確認プロセス全体を簡素化できます。ソフトウェアに含まれるブロックは基本的に事前に証明され、同時に妥当性が確認されているからです。これらのソフトウェアブロックをアプリケーション内で多く使用すればそれだけ、妥当性確認の作業が軽減されます。同じことは、パラメータ化可能なユーザソフトウェアを使用する場合にも当てはまります。これにも、事前に妥当性を確認済みのブロックが含まれています。その後の一連のファンクションテストでは、安全機能の動作がその仕様に適合していることを証明する必要があります。これには、予測される故障のシミュレーションが含まれます。

3.8.8 環境要件に対する耐性の妥当性確認

制御システムの安全関連部のパフォーマンスを確認する際には、制御システムのその後の使用方法や環境的立地などの環境条件がシステムに関して重要な役割を果たします。関連キーワードには、防水や振動保護が含まれます。そのため、システムの分析によってシステムの妥当性確認を行う必要があります。具体的に言うと、制御システムまたはシステムが衝撃、振動、汚染物質の侵入など、環境影響からの広範なストレスに耐え得る機械的耐久性を備えていることを分析によって示す必要があります。制御システムの安全関連部は、あらゆる状況下で安全な状態を維持する必要があります。分析では、温度、湿度、電磁両立性などの要因も考慮すべきです。

3.8.9 妥当性確認レポートの発行

検証と妥当性確認のステップをすべて実行したら、最後に、妥当性確認レポートを発行します。これには、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テストに関する情報のすべてが含まれます。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ます。制御システムの安全関連部のいずれかが妥当性確認プロセスを経ていない場合には、除外につながった要因とともに、その安全関連部を明記すべきです。

3.8.10 結論

メンテナンスと修理／定期点検

当然ながら、年月によっても、安全関連制御システムのパフォーマンスは劣化します。摩耗、腐食、持続的な (機械的) ストレスは安全性の低下につながります。極端なケースでは、制御部品だけでなく、制御システム全体の危険側故障を引き起こすことさえあり得ます。そのため、制御システムの安全関連部の定期的なメンテナンスを行うとともに、定期点検を実行して機能安全を確認することが必要です。メンテナンスと修理の計画とともに、定期点検の記録は書面形式で利用できるようにすべきです。ファンクションテストは適格な人物が実行する必要があります。産業安全規則 (Ordinance on Industrial Safety) の§ 3 に準拠するハザードアセスメントに基づき、機械または設備の運用者は、定期点検のタイプ、範囲および頻度を規定する必要があります。産業安全規則の詳細、および当社サービスの詳細情報は、www.pilz.com でご覧いただけます。

3.8 妥当性確認

3.8.11 附属書

ここでのトピックは、十分に吟味された基本的な安全原理と安全部品に加えて、故障の除外が中心です。以下は EN ISO 13849-1 と EN ISO 13849-2 の仕様に対応し、安全関連の考慮事項の簡単な概要を示しています。

EN ISO 13849-1/EN ISO 13849-2 に準拠した基本的な安全原理

基本的な安全原理の特徴は以下の通りです。

- 強度、耐久性、弾力性、摩耗を考慮した適切な資材と製造方法の使用
- ストレスとひずみを考慮した正確な寸法と成形
- 圧力制御バルブやチョークなどの圧力制限対策
- 速度制限対策

EN ISO 13849-2 の附属書 A ～ D には、機械、油圧、空圧、電気／電子システムに影響を及ぼす基本的な安全原理のリストが含まれています。

EN ISO 13849-1/EN ISO 13849-2 に準拠し、十分に吟味された安全原理

十分に吟味された安全原理の特徴には、例えば、以下のようなものがあります。

- 部品の可動部の安全な位置などを通じた故障の回避
- 部品の大型化または定格を下げるなどによるエラーの確率の低減
- 強制的な電気の切断 / 強制的な接点開放による故障モードの定義
- 部品を増やすなどによる故障の影響の軽減

EN ISO 13849-2 の附属書 A ～ D には、機械、油圧、空圧、電気／電子システムの十分に吟味された安全原理のリストが含まれています。

EN ISO 13849-1/EN ISO 13849-2 に準拠し、十分に吟味された部品

部品は、以下の場合には、十分に吟味されていると見なすことができます。

- 複数のアプリケーションで過去に使用されたことがあり、良好な結果を残している場合
- 部品の適切性と信頼性を立証する原理を使用して製造されている場合

ネジ、バネ、カムなどの機械システムの部品およびコンタクタやリレーなどの電気システムの部品で、十分に吟味されているものリストは、EN ISO 13849-2 の附属書 A ～ D で確認できます。現時点では、空圧および油圧システムの部品で十分に吟味されたものはリストに挙げられていません。

EN ISO 13849-2 に準拠した故障の除外

故障の除外を適用するための要件は、妥当性確認計画に記載する必要があります。故障の除外は、それぞれ合理的で追跡可能な説明によって正当化できることが重要です。EN ISO 13849-2 の附属書 A ～ D は、故障の前提に基づく、可能性のある故障の除外の概要を示しています。例えば、以下のようなものがあります。

- 機械システム部品の大型化または定格を下げるなどによる破損
- 空圧システムの安全装置による自発変化
- 油圧システムの強制作動による切り替え時間の変化
- 電気／電子システム上の相互に絶縁された隣接する接点間の短絡

3.8 妥当性確認

ピルツがお客様に提供できるサポート

Pilz GmbH & Co. KG は、設備や機械のライフサイクル内の妥当性確認など、幅広いサービスを提供しています。開発ソリューションは、リスクアセスメントと安全コンセプトを反映することで、システム統合の実際の要件に適するように調整されています。ピルツによる妥当性確認の後は、実施した対策の客観的かつ体系的なレビュー、技術的保護対策の評価、そして最後にファンクションテストが行われます。適用される安全規格および指令のすべてへの適合が保証されます。機械の妥当性確認の実績が豊富なピルツのエンジニアが、設備や機械のセーフティクリティカルなファンクションを検査するための構造的な方法を開発しています。 計算ツールの PAScal は、それぞれの安全機能で達成されたパフォーマンスレベルの検証に役立ちます。

ピルツの妥当性確認には以下が含まれます。

- リスクアセスメントからの要件と安全コンセプトの反映
- 計算ツールの PAScal や Sistema などに基づいて行う、EN ISO 13849-1 / EN IEC 62061 に従って達成したパフォーマンスレベルの妥当性確認
- 取扱説明書の妥当性確認
- ファンクションテストと故障シミュレーションの実施 (安全チェック)
- 安全関連ソフトウェアおよびハードウェア機能のテスト
- センサ／アクチュエータおよび配線のテスト
- 計測 (接地導体、音響レベルなど)
- 詳細な結果を含むテストレポートの発行
- EC 適合宣言書に署名することで、「正式代表者」としての責任の受け入れ

ピルツの妥当性確認による利点

- 適格な方法による適合性評価手順
- 妥当性確認と CE マーキングの関連側面をすべて考慮
- ピルツの安全エキスパートによるサポート

CE マーキングによって安全プロセス全体を完了

機械の安全ライフサイクルを完了するために、最終的なサービスとして CE マーキングを提供します。この場合には、ピルツは、適合性評価プロセス全体を実施し、手順の全体について責任を負います。正式代表者として EC 適合宣言書に署名することで、ピルツは指令の要件を満たしていることを証明します。その結果、お客様は、欧州域内市場全体で機械が必要とする「パスポート」を取得することになります。

定期検査、そして規格、指令、製品開発に関する最新知識は、設備や機械を長期的に安全に操作したいと願うすべての人にとって必要不可欠です。産業安全規則によると、電気的検知保護設備 (ライトグリッド、光線装置、スキャナなど) は適切なコンフィグレーションと取り付け、定期的な検査を行うことが必要不可欠です。これについての全責任は運用者に委ねられています。

定期的な検査による安全確保

DIN EN ISO 17020 に従って DAkkS (ドイツの認証機関) より認証を取得した独立検査機関が、客観性、お客様の設備や機械の高可用性、さらには、お客様のスタッフの最高の安全性を保証します。

ピルツは、プロセスの終了時に検査レポートを提出し、すべての結果についてお客様と協議します。検査に合格したら、設備にピルツの品質証書が発行されます。

3.9 証明と認証

お客様が、証書や第三者証明のサービスプロバイダを品質の保証と見なす傾向が強まっています。しかし、基本的には、証書には法的拘束力がなく、実際には誰でも発行できます。これらは単に、特定の業務が関連仕様に従って実施されたことを第三者が確認したことを示すに過ぎません。事実、証書は第三者の検査の品質について一切触れていません。証書を発行する会社の能力について正確な知識があること、あるいは必要に応じて問い合わせを行うことが重要なのはそのためです。

認証を受けた会社では、状況は異なります。認証には法的拘束力があり、国家機関のみが発行できるものだからです。公的認証機関は、認証によって、会社や機関が特定の適合性評価手順を実施する能力を備えていることを認証します。適合性評価は、定義または目標ごとに特定の仕様が満たされているかどうかを確認する手順です。認証を受けた会社や機関が証書を発行する場合には、その会社または機関は、そのために必要な能力を備えていると考えることができます。

3.9.1 認証 : お客様向けの品質シール

認証を受けた適合性評価機関 (以下「認証済み機関」と言います) は、一般には、試験所や校正試験所であったり、検査機関や証明機関であったりします。これらの機関は、製品、設備、またはマネジメントシステムの適合性を評価するために、マネジメントシステム、個人、製品などの試験、検査、証明などのサービスを提供します。通常、評価は、規格に記載された要件などの特定の要件が満たされていることを証明するために必要なテスト手順の一環として行われます。

欧州での認証は、認証指令 765/2008/EC によって一律に規制されています。2010 年 1 月 1 日以降、すべての加盟国は、単一の国家認証機関を運営することが義務付けられています。これは適合性評価機関を認証し、監査を通じて定期的に評価することで、要件の継続的な遵守を保証しています。認証プロセスではとりわけ、組織の独立性、品質管理、スタッフのトレーニング、校正計測装置のマネジメント、業務手順、記録と試験レポートの取扱いを審査して、組織が関連 EN/ISO 規格に適合していることを確認します。国家認証機関はまた、オンサイトでの証明作業の実際の実施状況も検査・評価します。認証は、認証済み機関とその顧客の両方にとって有益です。認証機関が規格に従って正確に業務を実施していることが顧客に示されるからです。同時に、顧客は審査を実施する組織の能力について評価基準を得ることができます。

通常、組織は単独で業務を実施し、そのパフォーマンスに関する技術的な独立評価を受け取ることはなく、あったとしてもごくまれにしかありません。認証機関による定期的な評価では、正確かつ信頼性の高いデータの継続的な提出に関して施設の運営のあらゆる側面を審査します。認証機関は改善すべき領域を特定して審議します。評価の終了時には、詳細なレポートを提供します。必要な場合には、認証機関はその後の活動を監視することができます。そうすることで、審査される会社は、適切な是正措置を確実に導入することができます。

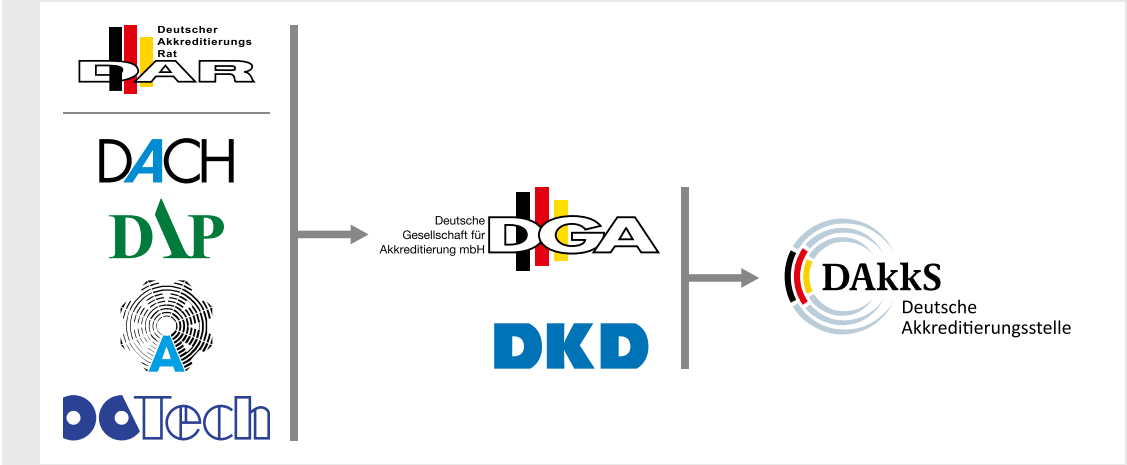
3.9 証明と認証

欧州の認証機関の例

3.9 証明と認証

ドイツでは、連邦経済産業省が設立したドイツの認証機関 (Deutsche Akkreditierungsstelle GmbH* [DAkkS]) がこれを担当しています。過去のすべての認証機関 (DACH、DAP、TGA/DATECH、DKD) は、2010 年の初めに DAkkS と統合されました。

* オーストリアの場合は、bmwfi、スイスの場合は、スイス認証サービス (Schweizerische Akkreditierungsstelle [SAS])



ドイツの認証機関は DAkkS に合併

DAkkS と国際試験所認定協力機構 (ILAC)、国際認定フォーラム (IAF) と欧州認定協力機構 (EA) の間の協定によって、認証は引き続き世界中で認められています。

国際的に認められている DAkkS

MRA = 相互承認協定
MLA = 国際相互承認協定

3.9 証明と認証

これらの協定によって、世界中のすべての認証済み機械が標準レベルの能力を備えており、実施サービスが非常に厳格な品質要件を満たしていることが保証されています。認証は国内的にも国際的にも技術的能力の指標として高く評価されています。多くの産業分野では、試験サービスのサプライヤに関する認証を日常的に規定しています。

ISO 9001 の証明とは異なり、認証は、技術的能力を判断するために特別に開発された基準と手順を使用し、それによって試験所や検査サービスから提供される試験、校正、測定データが正確で信頼できることを顧客に保証します。認証済み機関は、関連認証機関のシンボルによって確認することができます。通常、シンボルは試験レポートまたは校正レポートに記載されています。ドイツ内の認証済み機関のリストは www.dakks.de に掲載されています。

ピルツ検査機関用の DAkkS のロゴの例

3.9.2 認証または証明

認証では、技術的能力を判断するために特別に開発された基準と手順を使用します。スペシャリストである技術評価者は、試験や校正データの作成に影響を及ぼす組織内のすべての要因を徹底的に評価します。この基準は、認証済み機関を評価するために世界中で使用されている ISO/IEC 17020、ISO/IEC 17025、ISO 15189 などの国際規格に基づいています。認証済み機関は、以下のような技術的能力に関する要因を特に評価するために、この規格を使用します。

- スタッフの技術的能力
- テスト方法の有効性と適切性
- 国家規格に適合する計測と校正の追跡可能性
- テスト装置の適格性、校正、メンテナンス
- テスト環境
- テスト品目のサンプリング、取扱い、輸送
- テストデータおよび校正データの品質保証

このプロセスによって、認証は、認証済み機関が提出する試験および校正データが正確かつ信用できることを組織およびその顧客に保証します。

例えば、ISO 9001 に従った証明は、製造およびサービス組織で広く使用されています。これは、製品、サービスおよび手順が、要求される品質規格を満たしていることを証明するものです。例えば、組織の品質マネジメントシステムを ISO 9001 に従って証明する目的は、マネジメントシステムがこの規格に適合していることを証明することです。試験所や検査機関は ISO 9001 に従って証明を受けることができますが、認証とは異なり、その証明は技術的能力に関しては何も述べていません。

3.9 証明と認証

3.9.3 労働安全規則に適合するテストと認証

欧州の雇用主はすべて、従業員に安全な作業機器を提供する法的義務を負っています。ドイツでは、これは、産業安全規則 * (BetrSichV) によって遅くとも 2002 年 10 月から規制されています。この規制の実施は、1989 年に EU が採択し、その後改正された作業機器指令 2009/104/EC によって義務付けられています。

* オーストリアの場合は作業機器に関する命令、スイスの場合は傷害保険に関する連邦法 (AIA)

雇用主は、作業機器を初めて使用するときと、その後の定期点検を通じて、この要件を保証することが義務付けられています。雇用主は、法定の仕様を考慮して、点検の間隔を自分で決定する必要があります。また、これらの点検が有資格者によってのみ実行されることを保証する必要もあります。労働安全に関する技術規則 1203 は、「有資格者」に課される要件を定めています。基本的に、有資格者は点検分野に関する専門的なトレーニングを受けており、一定量の専門的な経験と最近の専門的な活動歴があり、かつ定期的かつ継続的に関連トレーニングを受けている必要があります。雇用主は、どのスタッフを「有資格者」に指名するかを自由に決めることができますが、有資格者の能力について確信があり、裁判所で証明できる必要があります。

あるいは、これらのテストを外部の業者に委託することもできます。しかし、これによって、雇用主は、テストの実施会社の能力を確認する責任を免除されることはありません。証明を受けた会社とは異なり、認証済み機関は、この点で特に役立つことがわかります。このような機関の能力について法的拘束力のある宣言を行うことで、立証責任を満たすのは認証だけだからです。

Pilz GmbH & Co. KG は、認証済み検査機関を運営しており、設備や機械に関する安全防護物のテストを企業から受託することができます。認証によって、そのサービスは世界中で認められています。この検査機関は、ドイツだけでなく EU 加盟各国において有資格の検査員を手配することができます。そのため、ピルツは EU 域内だけでなく世界中でサービスを提供することができます。2015 年に、ドイツの認証機関 (DAkkS) が認証を更新しました。このことは、ピルツが機械工学分野のタイプ C 検査機関に適用される EN ISO/IEC 17020:2012 の要件をすべて満たしており、事前に定められた適合性評価業務を実行する能力があることを示しています。ピルツは非常に複雑な試験を行うこともできます。当社の検査機関は以下のサービスを提供しています。

EU の作業機器指令実施の例

3.9 証明と認証

- 電気的検知保護設備 ESPE (ライトカーテン、スキャナ、安全カメラシステム) の検査
- 所定の安全距離を確認するための停止パフォーマンスの計測
- 追加の安全防護物 (E-STOP、安全扉、両手操作) の検査
- 産業安全規則の最低要件の遵守の検証
- 機械指令 (CE) の最低要件の遵守の検証

お客様が自社のテストまたは計測ニーズを満たす認証済み検査機関を選択した場合には、検査機関は、確実に正確かつ信頼できる結果を提供することができます。検査機関の技術的能力は以下のような要因によって異なります。

- スタッフの資格、トレーニング、経験
- 正確な校正とメンテナンスが行われている適切な装置
- 適切な品質保証手順
- 十分なテスト手順
- 妥当性が確認されたテスト方法
- 国家規格に基づく検査
- 正確な記録手順とレポートの発行
- 適格なテスト施設

これらの要因はすべて、認証済み検査機関が技術的に適格であり、提供するテストの実施能力があることを確認する上で役立ちます。

3.9.4 結論

基本的に、どの会社も、作業用機器の検査を自社のスタッフに行わせることもできれば、外部の会社に委託することもできます。しかし、どのような場合でも、検査実施者は有資格者である必要があります。スタッフを選んだ場合には、通常、雇用主がその資格を評価できます。外部の業者を選んだ場合には、証拠書類を当てにするしかありません。一般に、証書には十分な説得力はありません。法律上の紛争では、通常は、正式な要件を満たさないからです。これとは対照的に、関連サービスの認証は、信頼性の高い法的安全性を提供することができます。

情報リンク :

- DAkkS: http://www.dakks.de
- EA: http://www.european-accreditation.org
- ILAC: http://www.ilac.org

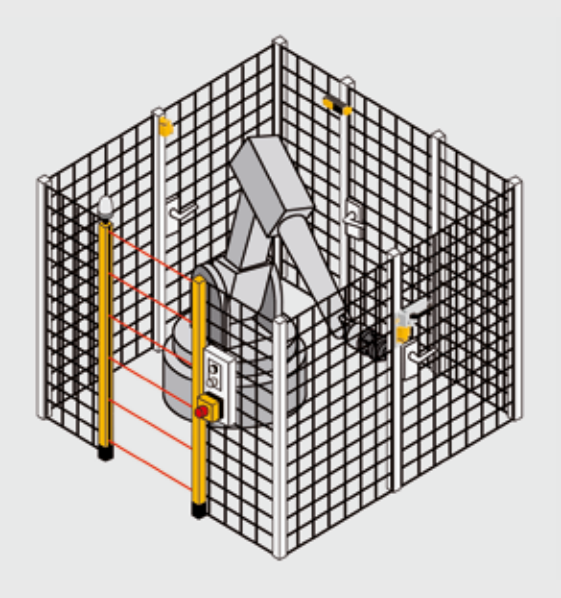
4

安全防護物

4 安全防護物

4.1 安全防護物に関連する欧州連合の規格、指令、法律

安全防護物は、作業者を機械の操作中に発生する恐れのある危険から可能な限り保護するために必要とされます。具体的には、通常は、フェンスやバリヤなど、物理的に機械への接近を妨げるものです。しかし、場合によっては、このような固定式ガードの選択が不可能であったり、ふさわしくなかったりすることもあります。このような場合は、誰かが危険源に近づくと機械の一部または全部を停止するか、または別の手段で機械を安全なステータスにする制御技術ソリューションが選択されます。このような危険保護も適切ではないと判明した場合、またはこれらの対策を適用しても潜在的な危険が残る場合には、表示的安全技術が最終的な選択肢です。つまり、残存する危険性が取扱説明書または機械自体に示されます。



ガードバリヤや安全装置による危険防止

4.1 安全防護物に関連する欧州連合の規格、指令、法律

機械の安全防護物を取り扱う規制は膨大な数になります。まずは、欧州指令 2006/42/EC を検討してみましょう。

機械指令 (2006/42/EC)

1.4. ガードおよび保護装置に必要な特性

1.4.1. 一般的な要件

ガードおよび保護装置は以下の通りでなければならない。

- 頑丈な構造である。
- 確実に固定されている。
- さらに新たな危険の原因となることがない。
- 容易に迂回処置を講じたり、不動作にしたりすることができない。
- 危険なゾーンから十分に距離が離れたところに位置している。
- 生産プロセスの観点にもたらす障害を最小限に抑えている。
- 作業の実施が必要な領域のみにアクセスを限定することにより、可能であればガードを取り外すことなく、または保護装置を不動作にすることなく、ツールの取り付けおよび交換 (またはそのいずれか一方)、ならびにメンテナンスを目的とした不可欠な作業を可能にする。
- 可能な場合、ガードは材料または物体の飛び出しや落下に対する、また機械からの排出物に対する防護を提供しなければならない。

1.4.2. ガードに対する特別要件

1.4.2.1 固定式ガード

固定式ガードは、工具を使用してのみ開いたり、取り外したりすることができるシステムで固定されていなければならない。ガードが取り外された場合、その固定システムは、ガードまたは機械に取り付けられたままの状態でなければならない。可能な場合、ガードは固定具がない状態では所定の場所に取り付けできない構造でなければならない。

1.4.2.2 インターロック方式の可動式ガード

インターロック方式の可動式ガードは、以下の通りでなければならない。

- 開いているときには、可能な限り機械に取り付けられたままである。
- 意図を持った行動によってのみ調節を可能とするよう設計、製造されている。

4.1 安全防護物に関連する欧州連合の規格、指令、法律

インターロック方式の可動式ガードは、以下のようなインターロック装置を伴わなければならない。

- ガードが閉じられるまで機械の危険な機能が始動するのを防止し、ガードが閉じていない場合には必ず停止指令を発する。

機械の危険な機能によるリスクがなくなる前に、作業者が危険なゾーンに立ち入ることが可能な場合に、可動式ガードにはインターロック装置に加え、以下のようなガードのロック装置が備えられていなければならない。

- ガードが閉じられ、ロックされるまで、機械の危険な機能が始動するのを防止する。
- 機械の危険な機能による傷害のリスクがなくなるまで、ガードを閉じ、ロックされた状態に保つ。

インターロック式の可動式ガードは、その部品の１つがなくなったり、故障したりした場合に、機械の危険な機能が始動しないようにするか、または停止するよう設計されていなければならない。

1.4.2.3 アクセスを制限する調整式ガード

作業上厳密な意味で必要な、可動部品の領域へのアクセスを制限する調整式ガードは、以下の通りでなければならない。

- 関係する作業の種類に応じて、手動または自動で調整が可能である。
- 工具を必要とせず、容易に調整が可能である。

1.4.3. 保護装置に関する特別要件

保護装置は、以下のように設計され、制御システムに組み込まれなければならない。

- 作業者の手の届く範囲にある限り、可動部品が始動できない。
- 可動部品が動いている限り、人の手がそれに届かない。
- その部品の１つがなくなったり、故障したりした場合に、可動部品を始動させないようにするか、または停止させる。保護装置は、意図を持った行動によってのみ調節可能でなければならない。

4.1 安全防護物に関連する欧州連合の規格、指令、法律

ここでは、上記の要件における多くの点を以下の通り個別に検討します。

可能な場合、ガードは材料または物体の飛び出しや落下に対する、また機械からの排出物に対する防護を提供しなければならない。ここでは、能動的な方向性の保護について説明されています。危険なゾーンに接近中における危険を考慮するだけでは不十分で、機械自体に起因し、外部に影響を及ぼす危険に対する保護が必要となる場合もあります。

安全防護物は、生産プロセスの観点にもたらす障害を最小限に抑えなければなりません。

固定式ガードの追加要件に、ガードが取り外された場合、その固定システムは、機械またはガード自体に取り付けられたままの状態でなければならないということがあります。よって今後は、例えば、ガードの取り外し後に紛失しないよう、保護カバーのネジを固定する必要があります。

この非常に厳格な要件は、実現可能性という点において多くの疑問を投げかけています。例えば、これは安全フェンスのすべてのネジに当てはまるでしょうか？極端な場合、安全フェンスの床の固定具さえもこの要件の対象となります。

欧州委員会が発行した「機械指令 2006/42/EC への適合のためのガイド - 第 2 版 - 2010 年 6 月」と題する解説において、1 つの解釈が示されています。この要件は、機械の作業者が取り外しを行うことが予期される場所で使用される固定式ガードに求められる、という解釈です。実例としては、毎月清掃を行うためにガードを開くというような場合になります。その一方、これは、一般的なオーバーホールや、より大規模な修理のためだけにガードを取り外すような場合には適用する必要はありません。したがって、機械の製造業者がこれに応じて装置を分類することが望ましいと言えます。

保護装置は、意図を持った行動によってのみ調節可能でなければなりません。この要件は、光線装置またはライトカーテンに関して特に意味を持つものです。これらの装置は、機械の始動時に調整されますが、それ以降は正当な理由なく調整できないようにすべきです。そうしないと、必要な安全距離が保証されなくなる可能性があります。

4.1 安全防護物に関連する欧州連合の規格、指令、法律

4.1.1 ガードの規格

機械指令の法規制に加えて、現在、安全防護物に関する以下の欧州規格が存在します。

規格	タイトル
EN ISO 14120:2015	機械類の安全性 - ガード - 固定式ガード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
EN ISO 14119:2013	機械類の安全性 - ガードと共同するインターロック装置 – 設計および選択のための原則

4.1.2 ガードの寸法規格

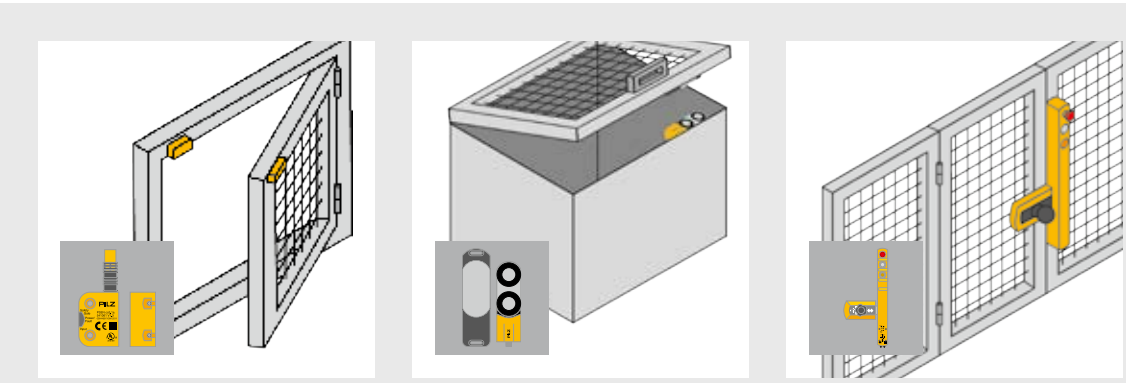
規格	タイトル
EN ISO 13857:2008	機械類の安全性– 危険区域に上肢及び下肢が到達することを防止するための安全距離 (ISO 13857:2008)
EN 349:1993+A1:2008	機械類の安全性ー 人体部位が押しつぶされることを回避するための最小すきま

4.1.3 保護装置または電気的検知保護設備の設計に関する規格

規格	タイトル
EN 61496-1:2013	機械類の安全性 電気的検知保護設備 - パート 1: 一般要件およびテスト
EN 61496-2:2013	機械類の安全性 電気的検知保護設備 - パート 2: 能動的光電保護装置 (AOPD) を使用する機器の特定要件
CLC/TS 61496-3:2008	機械類の安全性 電気的検知保護設備 - パート 3: 拡散反射形能動的光電保護装置 (AOPDDR) の特定要件
EN ISO 13855:2010	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

4.2 ガード

ガードは、機械の危険から人を保護するための物理的バリヤの一形態として特に必要とされる、機械の一部です。場合によっては、人が偶然近づくことによってスピードを重視するプロセスが中断することが許されない場合など、同じ安全防護物が同時に機械を人から保護することもあります。以下では、最初のシナリオのみを検討しています。



ガードの例

「ガード」は、後に取り扱うライトカーテンや光線装置などの「保護装置」や「電気的検知保護設備」とは異なり、機械の作業者と危険の間に物理的なバリヤを形成します。このような種類の安全防護物は、危険に近づくのを防止するものではなく、危険に近づいたときに人または人体部位を検知するものです。この場合、危険区域に達する前に危険が除去されるように、下流のコントローラを介して機械が停止されます。その設計に応じて、ガードは、ハウジング、ケーシング、シールド、ドア、カバーまたはその他の形式として実装することができます。したがって、ガードには、様々な種類や形式が用意されています。

4.2.1 固定式ガード

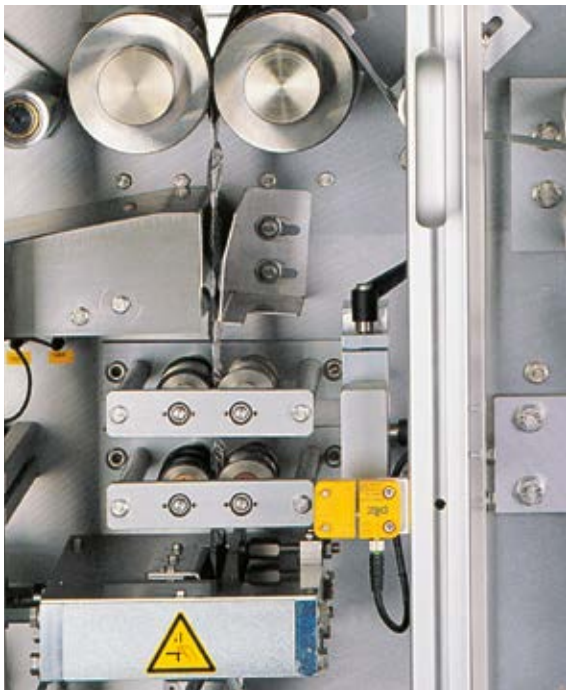
固定式ガードは、機械に恒久的に取り付けられるものです。この種類の安全防護物は、通常の運転条件でガードを取り外す必要がない場合、または作業プロセスにおいてアクセスが必要とされない場合に適しています。例として、モータファンの前面にあるチェーンカバーやグリルがあります。

4.2 ガード

4.2.2 可動式ガード

危険領域へのアクセスが必要な場合、安全扉などの可動式ガードが使用できます。

アクセスを必要とする頻度によって、固定式ガードと可動式ガードのどちらが必要であるのかが決まります。その決定を行う際に、この規格が役立ちます。

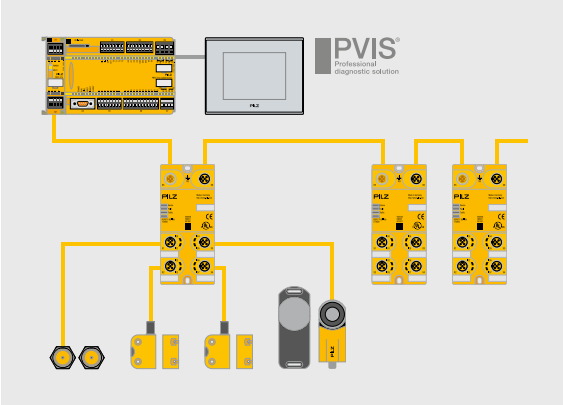


EN 14120
機械の設定、プロセスの修正、またはメンテナンスのためにのみアクセスが必要となる場合には、以下の種類のガードを使用する必要があります。

a) 予期できるアクセスの頻度が高い場合 (例えば、週に 1 回以上) または固定式ガードの取り外しもしくは交換が困難な場合には、可動式ガード。可動式ガードは、インターロックまたはガードロック付きのインターロックを備えるものとします (ISO 14119 参照) 。

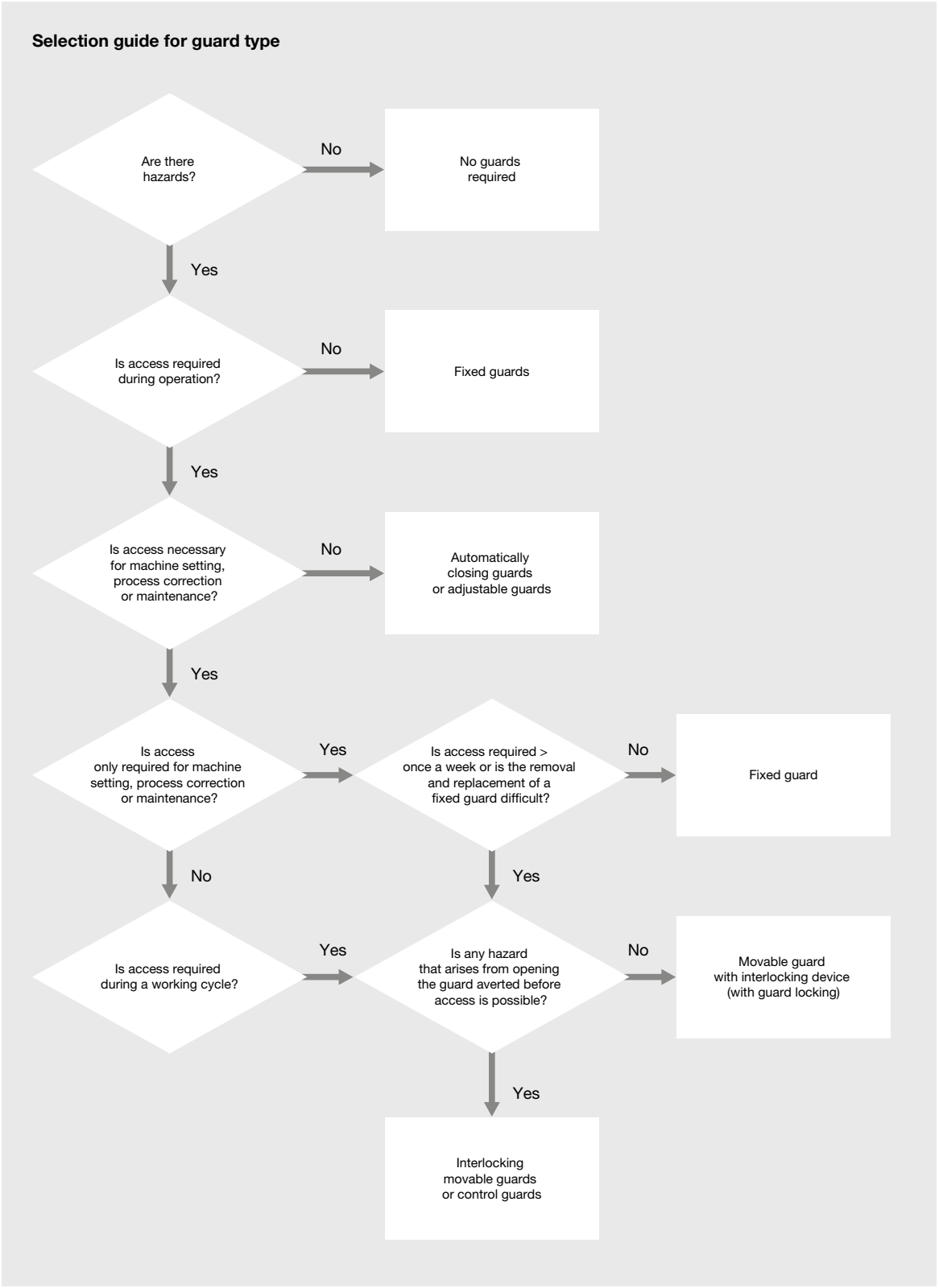
b) アクセスの頻度が低く、交換が容易で安全な作業システム内で取り外しと交換を行うことができる場合のみ、固定式ガード。

注 : この場合、「インターロック」という用語は、安全防護物の位置と停止するドライブ間における電気的な接続を意味します。安全技術では、一般的に理解されているロックを意味する機械的な「インターロック」は、「ガードロック装置」と呼ばれます。



個別診断により、1 台の評価装置で複数の安全扉を監視できます。

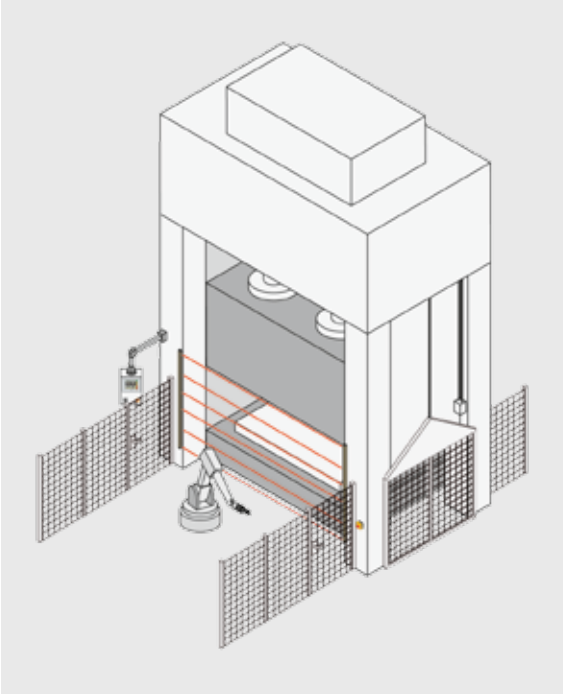
4.2 ガード



EN 14120 に適合

4.2 ガード

概要
生産モードの間に開かなければならないガードは、通常可動式ガードとして設計されています。これらは、固定式ガードとは完全に異なるものです。固定式ガードは、メンテナンスまたは修理を行うために開かれる場合など、まれにしか操作されることはありません。ガードの種類または選択によってコストが異なるため、この分類も十分な根拠に基づく必要があります。



メンテナンスまたは修理作業用の固定式ガード

4.2.3 安全防護物の設計に関するさらなる側面

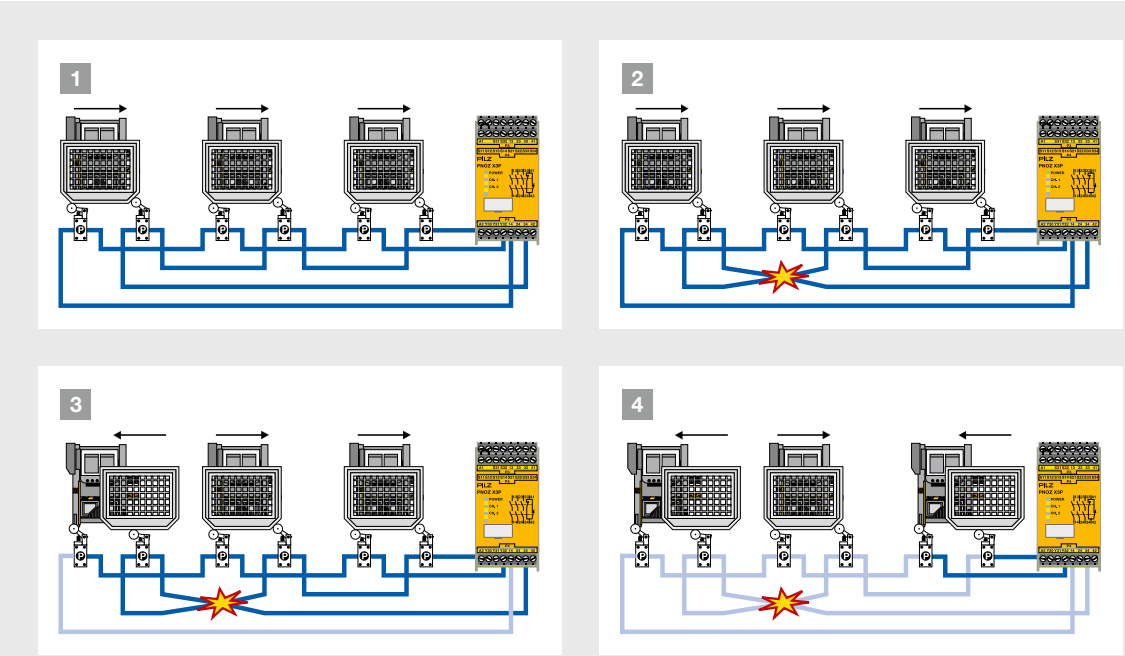
可動式ガードの使用を決定したら、次のステップとして、EN 62061 または EN ISO 13849-1 に適合した対応するインターロックの安全レベル (安全度水準 (SIL) または性能水準 (PL)) を決定します。 その後、それに対応する制御システムを設計し、妥当性を確認します。

これらの制御システムには、ガードの位置を検知するスイッチの形式によるセンサが含まれます。この検知機能を使用すると、ガードが開かれた際に危険動作を止めることができます。追加の安全機能を装備すれば、安全扉が開かれているときに、ドライブが不意に起動するのを防ぐことができます。危険動作の停止時間を考慮する必要があります。安全扉が開いているときに、停止時間の長いドライブが危険動作を引き起こすと想定できる場合、このゲートにはガードロック装置が必要になります。ガードロック装置は、能動的に解除操作を行うことにより、ロック解除する必要があります。これは、例えば、停電の結果、安全扉が意図せずに解放されることを防ぐ唯一の方法です。この場合、停電時に危険領域にいて、後方の安全扉を閉めた人を機械制御システムのロック解除コマンドでは解放できないことに注意することも重要です。このようなケースはまれであるかもしれませんが、起こり得ます。このため、機械的な解放機能を備えたバージョンのガードロック装置も存在します。但し、操作スタッフは、適切な作動ツールを用意しておくか、緊急解放の操作方法を理解しておくことが必要です。

4.2 ガード

安全扉スイッチ用の直列接続

可動式ガードをスキャンするセンサを選択する場合、そのようなセンサを評価装置に直列接続できるのかどうか、また直列接続できる場合には、何台まで接続できるのかという疑問が生じます。この質問に対する答えは、想定される異常またはこれらの異常の検知可能性のマスキングによって異なります。直列接続された以下の安全扉センサの例は、この点について説明するためのものです。



直列接続された安全扉の例

1 この例では、評価装置に直列接続された 3 枚の安全扉を示しています。最初は、すべての安全扉が閉じられており、リレーの出力が「オン」、すなわち機械を操作することができる状態です。

2 左側の安全扉で、N/C 接点を持つスイッチのラインに短絡が発生します。最初は、異常は検知されず、機械は動作を継続できます。

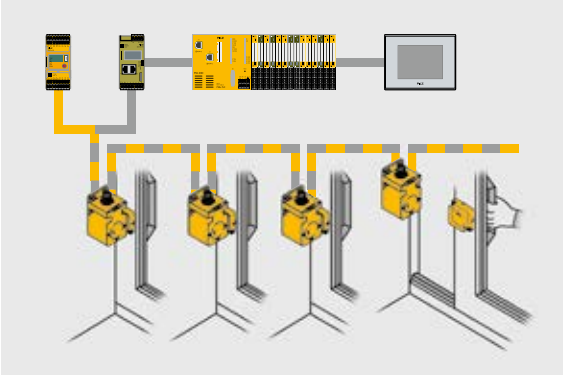
3 その次に、左側の安全扉が開かれ、左側のスイッチがリレーに信号を送ります。2 台のスイッチの動作を比較している間に、リレーは矛盾を発見し、異常状態に切り替わります。すなわち、安全扉が閉じられると、機械は再始動することができなくなります。

4 今度は、右の安全扉も開いています。これらの信号を介して、リレーは再び正常状態を検知します。異常状態がリセットされ、安全扉を再び左から右に閉じることができ、機械は再始動の準備が整います。

この例では、安全回路において検知されない異常を示しています。別の異常によって、安全扉のガード全体が故障し、危険にさらされる可能性があります。このような異常および類似の異常は、フォルトマスキングという用語で説明されます。現在の規格では、マスキングの可能性に応じて、スイッチが達成できる自己診断率 (DC) が制限されています。

4.2 ガード

この種類のフォルトマスキングの発生は、機械的スイッチと磁気近接スイッチにおいて同様に考慮する必要があります。RFID ベースのスイッチで一般的に見られるように、内部診断機能と OSSD 出力を備えたスイッチのみがこの影響を受けません。



異常検知機能を内蔵した安全スイッチ

実際には、安全リレーを介して評価される単一のスイッチのペアは、DC = 99%を達成することができます。この前提に基づいて、ISO/TR 24119 では、直列接続されたスイッチの数とその操作の頻度に基づいて、一群の相互接続されたスイッチの最大 DC が規定されています。

次のページのテーブルからわかるように、マスキングは達成可能な DC を制限し、その直接的な結果として達成可能な PL を制限します。PL e を満たすために一群の相互接続されたスイッチが必要な場合、異常検知機能を内蔵したスイッチを使用する技術的な解決策を利用できます。この場合マスキングは発生し得ないため、DC または PL を制限せずに、相互接続されたスイッチを使用することができます。

機械式スイッチ

この状況では、機械的冗長性の必要性と安全扉上の独立したスイッチの数についても問題が生じます。正しく取り付けられた場合、磁気的に操作される RFID 近接スイッチは、単独の機械的な異常が安全機能の喪失に至らないよう設計されていることが多いですが、機械的に操作されるスイッチ (リードスイッチやローラースイッチ) では、1 チャンネルの機械式アクチュエータに特に注意を払う必要があります。スイッチのマニュアルは、スイッチ自体に保証されている特性があるかどうか、ある場合にはどれかを証明するために常に慎重に確認する必要があります。これは、2 チャンネルの電気的接点が存在する場合には特に重要です。これらのスイッチの機械的部分に対する故障の除外は、意図された用途の一部としてスイッチ製造者によって明示的に示されていない場合、ユーザによって正当化される必要があります。摩耗、振動、腐食または不適切な機械的ストレスなどの影響を予測することは困難であるため、これは達成するのが不可能ではないにしても非常に困難です。このような場合、PL d または PL e を達成するには、扉ごとに機械的なスイッチを 2 台、2 チャンネルの磁気スイッチを 1 台、または OSSD 出力付きの RFID スイッチを 1 台使用する必要があります。

4.2 ガード

頻繁に使用される可動式ガードの台数[1) 2)]		追加の可動式ガードの台数[3)]	達成可能な最大自己診断率 (DC)[4)]
0	+	2 から 4	中
		5 から 30	低
		> 30	なし
1	+	1	中
		2 から 4	低
		≥ 5	なし
> 1	+	≥ 0	なし

[1)] 1 時間に 1 回の頻度を超える場合。
[2)] 独立した安全防護物を開くことができる作業者の数が 1 人を超える場合、頻繁に使用される可動式ガードの台数は 1 台増加する。
[3)] 次のいずれかの条件を満たす場合、追加の可動式ガードの台数数を 1 台減らすことができます。- 安全防護物間の最小距離が 5m を超える場合、または追加の可動式ガードのいずれにも、直接人が触れられない場合。
[4)] フォルトマスキングが確実に発生すると予測できる場合 (例えば、通常の操作またはサービスの一部として複数の可動式ガードが同時に開かれる場合)、診断範囲は「なし」に制限されます。

達成可能な最大自己診断率 (DC) (simplified)

配線タイプ、テストパルス、スイッチタイプなどの追加パラメータを考慮する場合には、テーブルに示す値を超えるさらに複雑な事項を考慮することができます。これらは、個々のケースにおいてより好ましい結果をもたらす可能性がありますが、常に最大 DC は「中」に制限されます。

また、センサとそれ自体の PL とをどのように直列接続するかいう問題もあります。この場合、診断はセンサの不可分の要素であり、直列接続によって影響を受けたり低下したりすることはありません。しかしながら、評価装置で処理する前に、チェーン内の最初のセンサのスイッチ信号は他のすべてのセンサを通って導かれる必要があります。チェーン内で別のセンサに安全に関するエラーが発生すると、転送が妨げられる可能性があります。そのため、この場合には、最初のセンサのみが検査中の安全機能に含まれる場合であっても、チェーン内のすべてのセンサのエラー確率を合計する必要があります。

4.2 ガード

磁気スイッチの評価

磁気的に操作される扉のスイッチ (リードコンタクト付き) を使用する場合、重要であると判明している問題が 1 つあります。それは、スイッチのペアと安全リレーが使用され、その相互適合性が製造業者によってテストされていない場合、機械の製造業者はスイッチ内のピーク電流が早期摩耗を起こさないようにする必要がある、ということです。これは主に、リレーベースの安全ユニットを備えたリードスイッチのペアに影響します。

これを評価するためには、発生する最大ピーク電流 I_S (式 1 参照) を決定し、これをスイッチの許容ピーク電流 I_{Smax} と比較する必要があります。直列接続のすべてのスイッチを考慮する必要があります。そのため、許容ピーク電流の最小値のすべてが、最大スイッチング電流より大きくなければなりません (式 2 を参照)。

$R_{Smin}(i)$	スイッチ i の最小内部抵抗
$I_{Smax}(i)$	スイッチ i の最大許容ピーク電流
U_{Pmax}	最大電圧
R_{Pmin}	安全リレーの最小内部抵抗
I_S	最大スイッチング電流

$$I_S = \frac{U_{max}}{R_{Pmin} + \sum_i R_{Smin}(i)}$$

式 1

$$I_S \leq \underset{i}{MIN}\,(I_{Smax}(i))$$

式 2

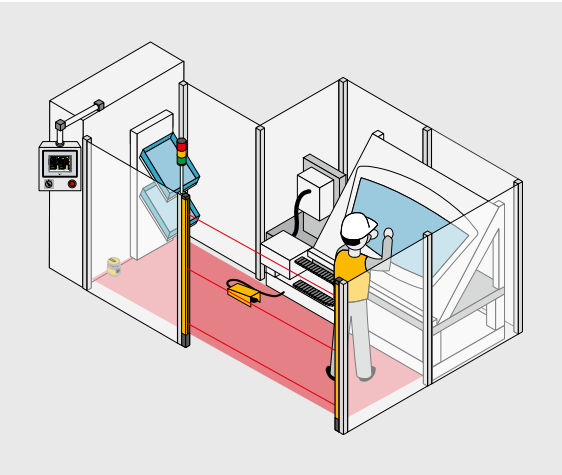
早期摩耗の問題は、機械的に操作されるスイッチおよび OSSD 出力付きのスイッチでは、通常は発生しません。これらのスイッチの摩耗は、主に平均電流および熱による挙動によって決まるためです。

可動式ガードのスイッチの検討に関して、ISO 13855 から新たに考慮すべき要素がもう 1 つあります。これには、安全フェンス内の扉が、対応する扉のスイッチが信号変化を受信することなく、開口部から危険なゾーンにアクセスできる程度に開くことができる場合に発生し得る潜在的な危険が含まれます。これはどちらかというと理論上の危険ですが、検知されないゲート開口部のサイズに比例して安全距離を長くすることで回避できます。実際には、この問題は、状況の要件を満たすように選ばれた適合する扉のスイッチを取り付けることで、そもそも発生しないはずです。

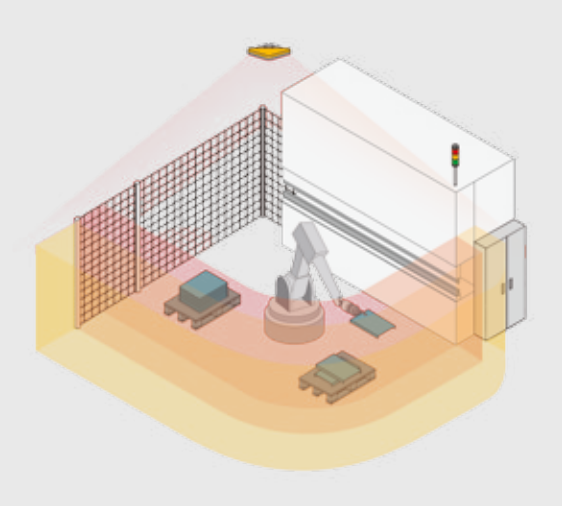
この点で、扉と危険箇所との間の実際の安全距離は、実際上の重要度が高くなります。ここで、安全フェンス内の安全扉が開いている状態で人が危険領域に入り、機械がまだ停止動作の途中である場合にどういうことが起こるかという疑問が生じます。この場合、人が十分な速度で接近し、機械の制動時間がそれに対して長い場合には、この危険領域に人が到達してしまう恐れがあります。規格によれば、ライトカーテンを使用する場合に行う計算をこの場合に使用することができます。安全距離 S は、S= (K × T) として計算されます。K は人の歩行速度 (1,600 mm/s) で、T は扉のスイッチを動作させてから機械が停止する (すなわち、安全なステータスが達成される) までの時間です。ゲートを開くのに要する時間は差し引くことができます。これは、標準的な値が提供されていないため、理論的にどれくらいかかるかを考慮するか、または実際にそれを計時することによって特定できます。

4.3 保護装置

4.3.1 能動的光電保護装置



能動的な介入が必要な生産エリアの監視



3 次元ゾーン監視用安全カメラシステム

対応する危険区域へのアクセスが特に容易になるように意図されており、機械自体から予期される危険な影響 (溶接または研削プロセスなど) がない場合には、保護装置 電気的検知保護設備、以下、ESPE と略記する) が常に使用されます。潜在的な危険を十分迅速に遮断できるようにするために、この保護装置を適切な距離に設置する必要があります。この距離、すなわち安全距離 (S) は EN ISO 13855 で定義されており、特に次の要因により決定されます。

- t_1 = 保護装置自体の応答時間
- t_2 = 機械の応答時間、すなわち保護装置からの信号に応答する機械の停止性能
- C = ビーム間の距離に応じ、ライトカーテンの 2 本のビームの間を検知されずに通って到達する場合など、保護装置によって検知されない危険領域へ接近する可能性のある距離
- K = 人体または人体部位の予想される接近速度。この係数は、歩行速度が 1,600 mm/s、手の速度が 2,000 mm/s として、EN ISO 13855 で定義されています

したがって、実施される距離は、$S = K \times (t_1 + t_2) + C$ となります

4.3 保護装置

EN ISO 13855 では、次の優先距離が定義されています。

分解能	計算式 (距離S [mm])	説明
d ≤ 40 mm	S = 2000 x T + 8 (d-14)	結果が 100 mm 未満の場合、少なくとも 100 mm の距離を維持する必要があります。
	結果が 500 mm を超える場合、 S = 1600 x T + 8 (d-14) を計算式として使用できます。	この場合、S は 500 mm 未満にはできません。
40 < d ≤ 70 mm	S = 1600 x T + 850	最も低いビームの高さ ≤ 300 mm
		最も高いビームの高さ ≥ 900 mm

複数の単一ビーム		ビームの数	ビームの高さ (mm)
マルチビーム	S = 1600 x T + 850	4	300, 600, 900, 1200
		3	300, 700, 1100
		2	400, 900
単一ビーム	S = 1600 x T + 1200	1	750
	リスクアセスメントで単一ビームの配置が許可されている場合		

ESPE が、保護を必要とするアクセス可能な領域の上に水平または傾斜した保護フィールドを形成する場合、フィールドはアプリケーションと ESPE によって予め定められている最小の高さに位置する必要があります。ここでもまた、保護されているフィールドの外縁部と保護すべき危険ポイントとの間の安全距離は、機械の停止性能を念頭に置いて、危険領域内における危険動作に起因する怪我の可能性を排除するものでなければなりません。

- ガードが慎重に設計されている場合であっても、ガードを無効化する手段はすべて考慮する必要があります。検知フィールドの上または周囲に到達する可能性は排除する必要があります。検知フィールドと隣接する安全フェンスとの間の隙間を常にカバーすることは必ずしも可能ではないため、ここでは人と危険領域との間における安全距離も遵守する必要があります。これらの距離の計算は、検知フィールドを使用する危険領域へのアクセスに適用される安全距離の計算によく似ているため、この重要な違いには、特に注意を払う必要があります。実際には、例えば、危険領域へのアクセスが垂直に設置されたライトグリッドによって保護されている場合があります。しかし、このライトグリッドは、人が届くほど高くない場合が多く、例えば、手すりによりますが、高さはわずか1,100 mm です。この場合、検知フィールドを遮ることなく、ライトグリッドのすぐ前に立つことができます。さらに、この場合、人は前方に傾き、伸ばした腕でライトグリッドの向こうの領域に手を触れることができます。この状況での危険を避けるために、危険領域とライトカーテンとの間の最小距離が定義されています。これらの最小距離は、徒歩速度と手の速度にシステムの応答時間を掛けたものと、危険領域の高さと安全防護物の高さに応じた追加値の 2 つの要素で構成されています。この付加的な値は、最大 1,200 mm になる場合があります。スペースが限られている場合、このシステムを全く使用しなくて済む可能性のある手段をすべて検討してみても良いでしょう。
- 安全マットの位置決めとサイジングに関する情報は、EN ISO 13855 の第 7 章に記載されています。ここでも同様に、よく知られた公式である S = (K x T) + C が使用されます。この場合、K は 1,600 mm/s で、これは通常の歩行速度に由来します。安全マットでは検知されない伸ばした腕や手を保護するには、C = 1,200 mm の最小距離が必要です。
- 両手操作制御装置の配置に対する安全距離 S の設計は、式 S = (K x T) + C に基づいており、この場合、C は 250 mm で、K は 1,600 mm/s です。

4.3 保護装置

4.3.2 電気的検知保護設備に関するさらに重要な側面

4.3.2.1 再起動

安全防護物が発動すると、保護されたフィールドがクリアされた後に機械が自動的に再起動しないことがあります。これは、視認により確認したうえで、危険領域の外にある制御機器でリセットすることによってのみ可能でなければなりません。

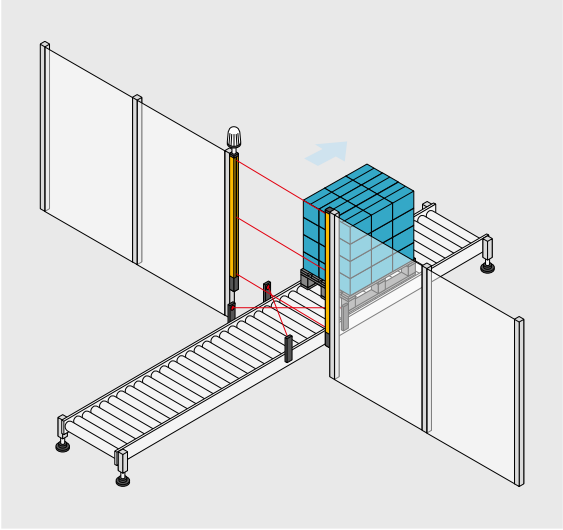
4.3.2.2 背面からの侵入

危険領域の正面の保護と同様に、装置の上、下、または周囲に手を伸ばす可能性、背面から侵入する可能性も考慮する必要があります。純粋に機械的な安全防護物や別のライトカーテンを使用して、背面からの侵入を防止することができます安全防護物が無効化される可能性がある場合は、安全防護物を守るための追加対策を講じる必要があります。

4.3.2.3 ミューティング

ミューティングは、電気的検知保護設備の一時的な自動停止であり、これによって、例えば、資材を危険領域に搬入出することができます。特別なセンサを使用して、保護されたフィールドを通って資材を搬送するときにのみミューティングコントローラがミュートサイクルを開始するようにします。このセンサは、人がミューティングセンサを有効化できないように配置する必要があります。保護区域に誰かがアクセスする必要がある場合、危険をもたらす可能性のある動作はすぐに停止されます。

業界では、特にこのような場合に対するミューティング機能を備えた特別な安全リレーを開発しています。一部のライトカーテンには、保護されたフィールドを部分的にのみミュート (ブランキング) するオプションもあります。例えば、このプロセスでは、アイテムを搬送する正確なセクションが受動的にレンダリングされます。しかし、どのような状況であっても、保護されていないフィールドのこの無効化されたセクションを介して、検知されない危険領域には誰も到達することがあってはなりません。アイテムと保護装置の間には、誰も側面から危険領域に到達できないようにするために、設計基準 (残りの自由空間のカバーなど) を使用する必要があります。



4 台のミューティングセンサによるミューティング

4.3 保護装置

4.3.3 その他のセンサベースの保護装置

4.3.3.1 レーザスキャナ

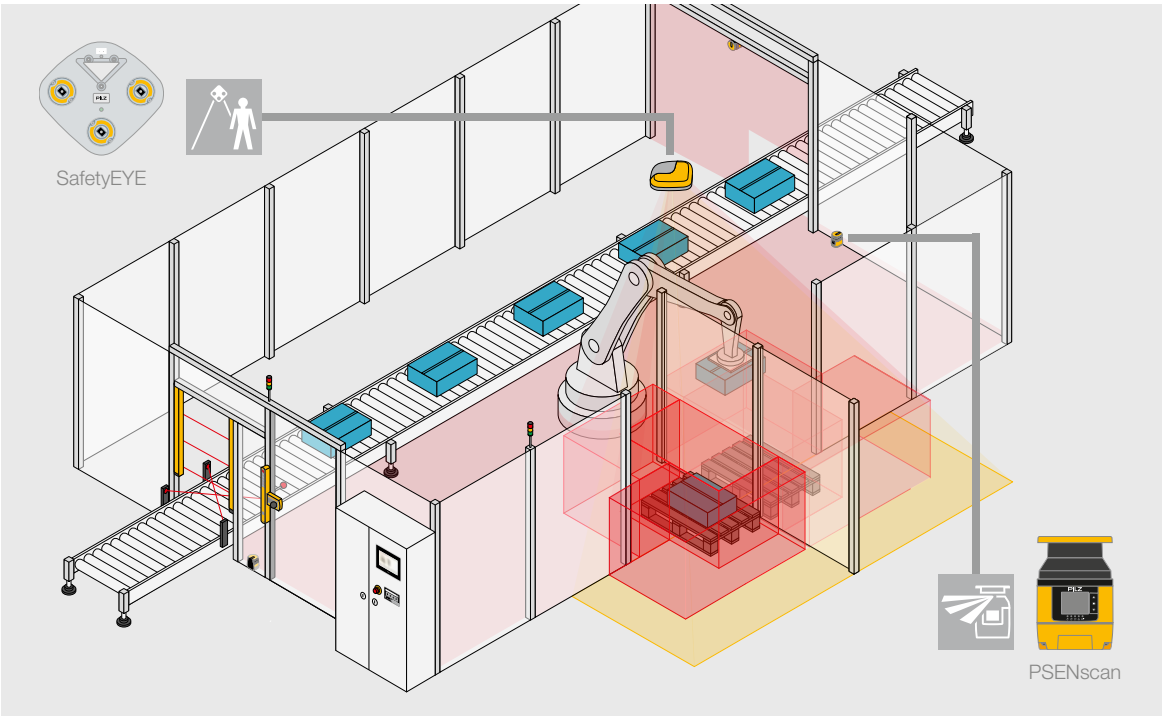
背面からの ESPE への侵入を防ぐために、水平または斜めに取り付けられた第 2 の ESPE を使用することがよありますが、これは通常、小さな領域しかカバーできません。より広いゾーンを保護するには、スキャナを使用して面からの侵入をさらに光学的に監視することができます。レーザビームが、監視対象領域を走査します。ビームが異物によって反射されると、これを検知して、危険動作が安全に停止されます。

4.3.3.2 安全カメラシステム

最近市場が拡大しているのは、自由にコンフィグレーション可能なゾーンを監視するための安全カメラシステムです。単純なセンサとは異なり、安全カメラシステムでは、監視対象ゾーン全体の詳細な情報を記録して分析することができます。これにより、危険を伴う可能性のある作業プロセスが安全に監視・制御され、人間と機械が保護されます。

4.3.3.3 安全マット

多くの圧力検知マットは、通常開の原則で動作し、特殊な評価装置の使用を必要とします。これにより、この動作原理を考慮し、適切に異常が検知されます。但し、通常閉の原則に基づいて動作する安全マットも利用可能です。これは要求される安全レベルが低く、電気的な負荷が低い場合で、これを使用してコンタクタを直接有効化することができます。



安全レーザスキャナと安全カメラシステムによる危険領域の保護

4.3 保護装置

4.3.3.4 両手操作制御装置

両手操作制御装置は、ワークステーション上で使用され、作業者の両手が操作箇所から離れないようにします。装置の操作中には、手は危険領域から離れています。様々なタイプの両手操作回路が定義されており、必要な保護レベルに合わせて適用することができます。両手操作制御装置の要件レベルは以下の通りです。

要件		種類				
	EN 574 Para.	I	II	III		
				A	B	C
両手の使用	5.1	◆	◆	◆	◆	◆
いずれかのアクチュエータが解放されると、出力信号の停止が開始されます	5.2	◆	◆	◆	◆	◆
偶発的な操作の防止	5.4	◆	◆	◆	◆	◆
保護効果が容易に無効化されてはならない	5.5	◆	◆	◆	◆	◆
両方のアクチュエータが解放された場合にのみ出力信号を再開	5.6	◆	◆	◆	◆	◆
最大 500ms 以内の同期動作直後の出力信号	5.7			◆	◆	◆
EN 954-1 に適合するカテゴリ 1 の使用	6.2	◆		◆		
EN 954-1 に適合するカテゴリ 3 の使用	6.3		◆		◆	
EN 954-1 に適合するカテゴリ 4 の使用	6.4					◆

両手操作回路の評価

EN 574 の現行版では、廃止された EN 954-1 規格を引き続き参照しています。それが EN 574 が現在改訂されている理由の 1 つです。

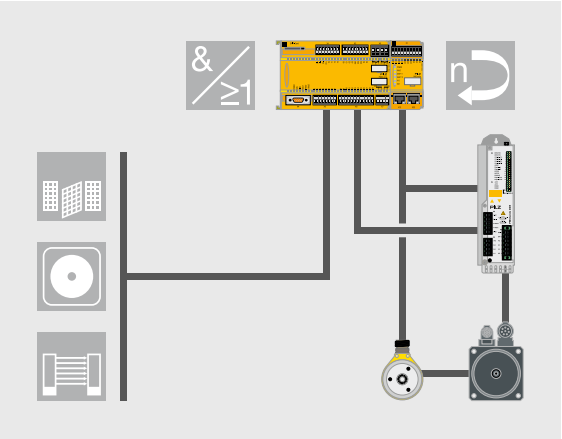
4.3 保護装置

4.3.3.5 機能的な安全防護物

EN 1037 (またはまもなく DIN EN ISO 14118) に適合した想定外の始動の回避。

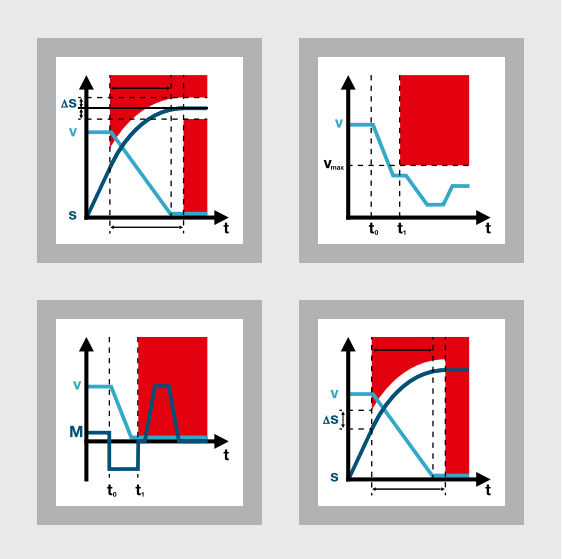
操作が進行中のときは、同じ問題が常に発生します。操作停止コマンドで停止した場合、どうやって機械が誤って再起動するのを安全に防止できるか、また、この状況でコントローラに異常が発生してドライブが不意に起動した場合にはどうなるのかという問題です。これは、「より明白な」安全防護物に関連する機能安全の検討と同様に重要な問題です。考慮すべき重要な点は、インバータ制御ドライブの問題です。これらのドライブは、「Zero Speed」や「Controller Inhibit」などの信号によって停止することがよくあります。ドライブの現在のステータスに関するデータを失わないように、電源を切るのを避けたい場合がよくあります。場合によっては、交流電源とインバータ間、またはインバータとドライブ間の接続を自発的に遮断することは、デバイスの不具合に結びつくため、考慮できないことがあります。

このような場合、機械の設計者には 2 つの選択肢があります。デバイスの不具合なしにエネルギー供給からの分離が可能で、他の危険動作を開始しない場合は、停止監視を使用できます。 インバータ制御のドライブは停止していますが、まだアクティブであるため、監視して動作しないことを確認します。万一、エラーのために何らかの動作が発生した場合は、ブランチ全体への電源供給はコンタクタを介して停止されます。このソリューションは、エラーが発生した場合に起こるわずかな駆動動作が危険を引き起こさないことを前提としています。この動作は、監視のためのセンサ技術を有効化する部分と、保護回路が反応しコンタクタが切り替わる前に発生する部分との 2 つの部分からなります。これらの影響をリスクアセスメントで検討する必要があります。



速度監視機能を備えた PNOZmulti 安全システムによる外部ドライブ監視

このような意図せぬ動きが受け入れられない場合は、安全なドライブ技術を使用する必要があります。これは、最初からこのような動作不良を防止するものです (第 7 章 : 安全なモーションコントロールも参照)。



ドライブ内蔵安全の例

4.4 安全防護物の不正操作

安全防護物とその不正操作を扱うことは、真の原因が長い間ずっとタブーになってきた問題です。マイナスのフィードバックがないため、プラントや機械の設計のどの部分からプラスの変更を加えることを開始すればよいかを知ることが困難である、という状況でした。

この状況は、今や変わりました。商取引協会連合会は、検査対象となった金属加工機械のほぼ 37%で安全装置が不正操作されていたことを示す研究を発表しています。つまり、3 分の 1 ものケースにおいて、不正操作が検出され検査されているのです。報告されていない実際の数は、それよりもいくらか高い可能性があると考えて間違いないでしょう。

残念なことに、BG の報告書が定期的に示しているように、安全防護物が不正操作された機械で発生している事故の件数には変化がありません。

4.4.1 法的立場

法的立場は明らかであり、以下の通りです。欧州法および国内法 (EC 機械指令および製品安全法 (ProdSG)) は、適切なレベルの安全性を備えた製品のみを市場に出すことが機械製造業者の責任であると規定しています。製造業者は、すべての機械における潜在的な危険をすべて事前に立証し、関連するリスクを評価する必要があります。製造業者には、リスク分析とリスクアセスメントの結果に基づき、各製品に対する安全コンセプトを開発し、そのコンセプトを実装し、関連する文書を提供する責任があります。潜在的な危険がユーザ、第三者、または環境に悪影響を与えないようにしなくてはなりません。合理的に予見可能な誤使用も含める必要があります。取扱説明書では、意図された製品の使用方法を明確に定義し、既知の不適切な使用方法を禁止する必要があります。

安全防護物を無効化する一部のいかがわしい慣習によって明らかになっているように、設計エンジニアは、機械ユーザの技術的な知識と想像力を過小評価すべきではありません。それは、信号フローチェーンの機械的構造へのおおざっぱではあるものの効果的なアクセスに始まり、タイプ 2 安全スイッチ用に巧みに仕上げられたキーにまで及ぶものです。これには、スイッチカム上のポジティブロッキングシャフト／ハブ接続を緩めること (これは発見が困難です) や、コントローラと安全スイッチ間の接続リードにおいて N/C / N/O を組み合わせた、高度な短絡とクロス回路、偽装され、巧妙に隠されているのに迅速にアクセス可能なオーバーライドスイッチなどが含まれます。これは発見された不正操作のわずかな例であって、決してすべてではありません。

4.4 安全防護物の不正操作

設計エンジニアは、機械の作業者が一般的にかなりのレベルの技術的な理解と手先の器用さを備えていること、また設計エンジニアが開発と実装にかけた時間よりもさらにかなり長い時間をかけて、間違った発想の操作／安全コンセプトに悩まされるようになり、効果的な「改善」を検討しているということを考慮すべきです。設計エンジニアは、現実的で実用的な要件を真剣に意識せず、標準的な仕様のみに頼りがちなことが非常によくあります。

したがって、事前に潜在的な不正操作を考慮するという課題には矛盾があります。設計エンジニアには、機械の作業者 (プレッシャを感じながら作業していることが多いものの、代替ソリューションを考え出すのに十分な時間とエネルギーは持っている) の想像力と意欲をシミュレーションすることが求められます。設計エンジニアには、自身の持つ専門知識を設計に取り入れ、現代の一般的な時間的制約のもとで、これを不正操作の防止となる安全対策に変換することが求められます。これは、常に簡単に解決できるとは限らない課題です。

EN ISO 14119 に含まれる、インターロック装置を無効化する動機を評価するためのチェックリストは、潜在的な不正操作を予測することに非常に役立ちます。しかし、設計エンジニアが今後ますますユーザの立場に立ち、利用可能な操作と安全に関するコンセプトをどう扱うかを正直かつ誠実に自問するようになることも望ましいでしょう。

4.4 安全防護物の不正操作

4.4.2 安全に反する行為とその意味

定義

単純な方法による無効化
多大な知的努力、手先の器用さのいずれを用いることもなく、手動により、または容易に入手可能な物体 (鉛筆、ワイヤ、ボトルオープナ、ケーブルタイ、接着テープ、金属フィルム、硬貨、釘、スクリュードライバ、ペンナイフ、ドアキー、ペンチなどの他、意図された機械の使用に必要なツール) によって動作不能状態にする (EN ISO 14119 も参照) 。

不正操作
安全技術の観点から見て、自らの利益を目的とした、機械の安全コンセプトに対する意図的、不正かつ対象を絞った隠れた介入で、ツールの使用によるもの (EN ISO 14119 も参照) 。

サボタージュ
従業員や同僚に害を与えることを目的とした、技術システムへの秘密、意図的かつ悪意のある介入。単語の起源 : 旋盤に投げ込まれた 19 世紀の農業労働者またはラダイトの木製靴 (フランス語では、サボット) 。

機械の設計および組立ての際に、製造業者は、機械に何ができるか、そして何ができなければならないかを定めます。同時に、ユーザによる機械の取り扱い方法も定めます。設計が成功するということには、実装マニュアルに記載されている生産量、および製造された製品の品質とトレランスに関して、機械が単に技術的機能を満たすということよりもさらに多くのことが含まれます。ユーザが最初から機械の機能を実行できるようにするには、一貫した安全性と操作コンセプトも備えている必要があります。この 2 つの領域は相互に関係しているため、これらが同時に連携して働くように開発し、実現する必要があります。

現在では、実用的なソリューションを提供する数多くの製品安全規格 (EN 1010 や EN 12717 など) が利用できます。とはいえ、新しい機械であっても、設計上の欠陥が未だに見受けられます。例えば、以下のような欠陥です。

- 技術的設計の不備や部品の精度などにおける不具合により、ワークフローに対する混乱が繰り返し発生している。(以下、あるプラントエンジニアによる発言を直接引用 : 「実際の健康と安全のために設計エンジニアができる最大の貢献は、販売時に約束された通りに動作する機械を設計することです。」)
- (必要なランダムサンプルの除去などを目的とした) 介入やアクセスが困難またはその機会が存在しない。
- 異常が発生した場合でも、プラント全体のシャットダウン・再起動により貴重な時間を無駄にすることなく、安全にサブセクションへのアクセスを可能とする、必要なバッファを備えたセグメント別のシャットダウン機能が欠如している。

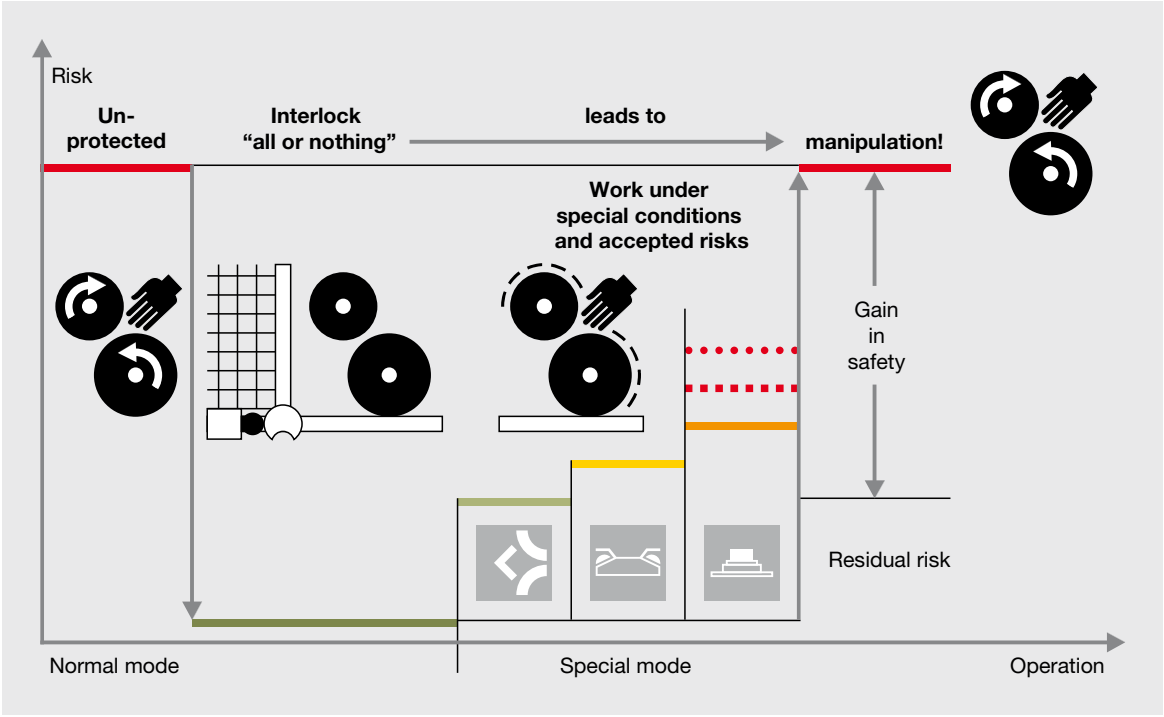
間違った発想の安全コンセプトが実践されていることが、未だにしょっちゅう見受けられます。インターロックされた安全防護物において多くのミスが犯されるのは、以下のような場合です。

- アクチュエータ、保存容器、充填孔など、危険のない、頻繁に操作される入力ファンクションが (インターロックされた) 安全防護物の背面に設置されている場合
- 安全防護物が開くと、インターロックによって危険な状況が迅速かつ確実に中断されるが、その後に機械やプロセスを続行できない、または再起動を必要とする場合

4.4 安全防護物の不正操作

設計者が自身の知識と信念を最大限に発揮して、技術的機能および人または作業者に関連する機能を設計し、実装しているということについては疑いの余地がありません。ユーザがその後に機械を使用する際に合理的かつ正しい振る舞いをすると信じ込んでいるからと言って、その設計者を責めることはできません。しかし、まさにここで注意が必要なのは、人間の行動は、日々の生活と仕事の両方において、主に利益の追求を指向するものであるということです。人は、与えられた課題、または自分自身に課した課題をできる限り迅速に、また必要に応じて最小限の労力で実行しようと努力します。

人はまた、あるプロセスが本来あるべき進行状況ほどには進んでいない場合に、そのプロセスの支援に積極的に介入しようとします。また、厄介な異常をできるだけ迅速かつ簡単に修正するためにあらゆる努力を払うものです。設計 (および取扱説明書に定められた異常修正手順) のせいでそれがかなわない場合、ユーザはインターロックの無効化などの方法を見つけ出そうとするでしょう。彼らは、余分な仕事とは、職務を円滑に行おうとしている個人に降りかかった災難であると考えることがよくあります。提供されている安全対策を無効化することで異常修正手順がずっと簡単になれば、それは成功したと見なされます。成功した行動は繰り返され、習慣として定着する傾向がありますが、困ったことに、この場合には、それは安全性に反する、非常に危険なことです。



特殊なオペレーティングモードに対するインターロックコンセプト

4.4 安全防護物の不正操作

マネジメントレベルにおいてこのようなルール違反が容認され、とがめられないことが増えると、罰を受けずにルール違反が続く確率は高くなります。不正な行為が新しい非公式のルールになってしまうのです。時間の経過とともに、リスクの認識は薄れてゆき、関係者は潜在的な危険を抜け目なく克服したと確信するようになります。しかし、リスクはまだ存在しており、攻撃の機会をうかがっているに過ぎません。

事故の引き金となる要因が、当初はその事故の影響を受けた人の行動に起因するように見える、ということは明らかです。しかし、関係者にとって大変危険な (人命を脅かしかねない) 不正を促しているのは、機械設計上のエラーなのです。このような機械は、EC 機械指令に適合していません。つまり、機械の機能性と使いやすさを保証しつつ、決定されたリスクに従って、十分なレベルの安全性を提供するように、保護対策を設計することが製造業者の責任です。結局のところ、実際の要件に合わせて調整された、緻密な安全コンセプトに基づいて計算可能かつ許容可能な残留リスクを受け入れるということの方が、不正操作を成功させて、機械の作業者を安全ではないプロセスによるリスクすべてにさらすことよりも常に望ましいのです。

4.4.3 設計者ができること

安全に関連する機械を設計するということは、ただ規制やその他の法規定を遵守すればよいということではありません。厳密に必要な安全対策のみが実施されるように、関連する規制や規格を参照して、「どこにそんなことが定められているのか？」と尊大な口調で質問してみても、安全性や人にとって正しくかつ目的にも適うソリューションを深く検討しているということにはなりません。

何よりも、設計エンジニアは、機械と安全装置の操作性に関して、作業者の実際の経験に基づく要求に対してもっと敏感でなければならず、これに対して真剣に対応する必要があります。これは、安全に関する設計をより困難にするものではなく、ユーザフレンドリな安全に関連する機械を製造するための基礎となるものです。実際の開発と設計の前に、操作上の要件を詳細かつ誠実に分析し、拘束力を持つ要件を定めた仕様書にその結果を記録するということが不可欠です。そうでない場合、機械や機械に組み込んだ安全対策が受け入れられない可能性があるという状況が起こり得ます。さらに、それによって、ユーザが「新しいアイデア」を思いつく可能性もありますが、そのほとんどは健康と安全をサポートするものではありません。これは、設計者による元々の考えからは程遠い、全く新たな一連の危険を次々に呼び起こしかねません。

とはいえ、不正操作が何もないところから起こることはまれです。これは、通常、機械と操作のコンセプトが最適ではないということを示しています。以下のような場合には、安全に反する行為の発生を常に予期しておくべきです。

- 作業慣行により、結果に直接的かつプラスの影響を与えない行動が求められている
- 作業慣行により、常に同じ作業手順の繰り返しを強いられているか、または作業目標を達成するために常に新たなアプローチが必要とされている
- 安全防護物により、業務の遂行に必要な視線や操作の余地が制限されている
- 安全防護物により、正常な作業に必要な視覚的／聴覚的なフィードバックが妨げられている、または遮断されている
- 安全防護物が開いている場合に、トラブルシューティングや異常を取り除くことができない

4.4 安全防護物の不正操作

つまり、機械の機能が制限されていること、または受け入れられない困難によって、ユーザが安全コンセプトの「改善」を実行したくなったり、実行を強いられたりするような場合には、不正操作を常に予期しておく必要があります。製造業者は、機械の機能性と操作性を許容可能なレベルの残留リスクで保証するようにするために保護対策を設計しなければなりません。つまり、将来的な不正操作の試みを予測し、それに対抗するための設計基準を使用すると同時に機械の取扱いを改善する必要があります。

製造業者の義務には、以下の 3 点が含まれます。

1. 不正操作の理由と動機を予測し、機械に対する綿密な操作／安全コンセプトを作成することにより、インターロックを無効化したいという誘惑を排除する。
2. アクセス不可能な場所に安全スイッチを設置する、ヒンジスイッチを使用する、取り外し不可能なネジを使用して安全スイッチやアクチュエータを取り付けるなど、設計によって不正操作を困難にする。
3. 製品安全法 (ProdSG) に定められている監視義務の条項に基づき、すべての作業者との厳しい製品監視によってあらゆる不具合を体系的に特定し、修正する (カスタマサービスエンジニアからの報告やスペアパーツの配送は、この点を明らかにすることに非常に有益な場合があります)

機械を発注する顧客も、機械の製造業者と協議して両当事者を拘束する実装マニュアルにその要件を誠実に定め、プロセス内の異常や不具合について率直に協議してこの情報を文書化すれば、それは不正操作に対抗することに役立ちます。

4.4.4 ユーザフレンドリなガード

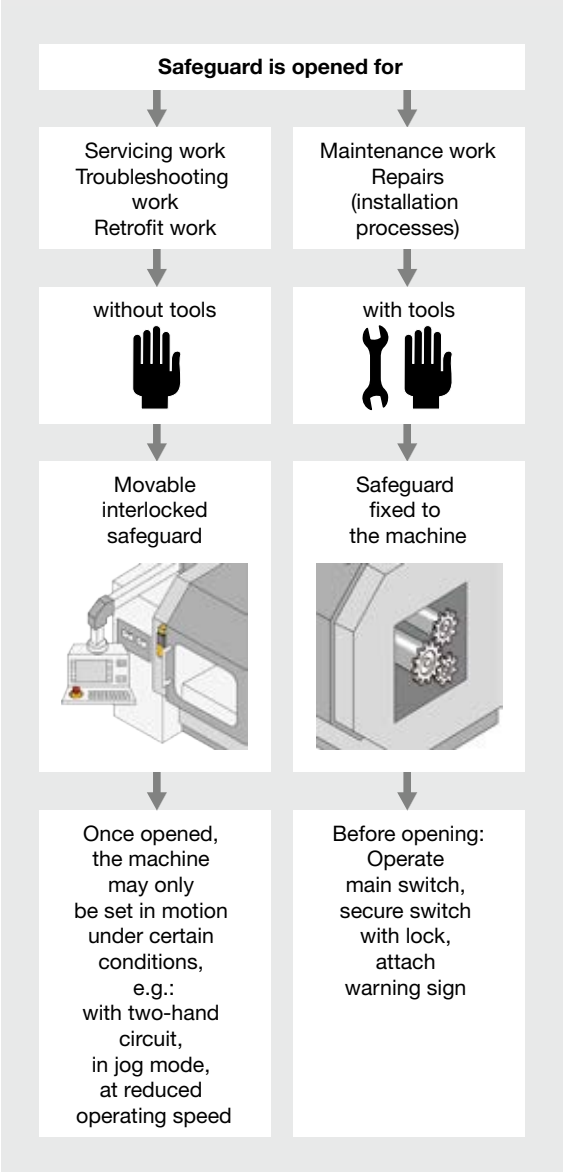
安全防護物、さらにはインターロックガードさえも、ワークフローの妨げにならず、ワークフローの実際的な支援となったり、さらにはワークフローを簡略化したりする場合には、常に積極的に受け入れられ、不正操作されないということを認識することが重要です。作業者に対して安全防護物の不正操作を強いるような安全コンセプト上の欠陥は、正真正銘の設計上の欠陥であり、状況によっては、機械の製造業者が責任を負うものです。異常のない通常の操作だけではなく、セットアップ、テスト、異常の除去、トラブルシューティングに対しても、許容可能な残留リスクを伴う安全に関連したソリューションを実施する必要があります。

技術的なレベルで不正操作の試みを困難にしても、一見問題が解決したかのように見えるだけです (EN ISO 14119 も参照)。十分なプレッシャがあれば、「ソリューション」が見つかるからです。もっと重要なことは、不正操作の理由を取り除くことです。必要なことは、(安全技術に関してでさえ) 過度な機能性ではなく、使いやすさです。安全コンセプトが適切かどうかについて疑問がある場合には、関連する雇用主の責任保険協会または安全部品の製造業者から助言を求めることを推奨します。

4.4 安全防護物の不正操作

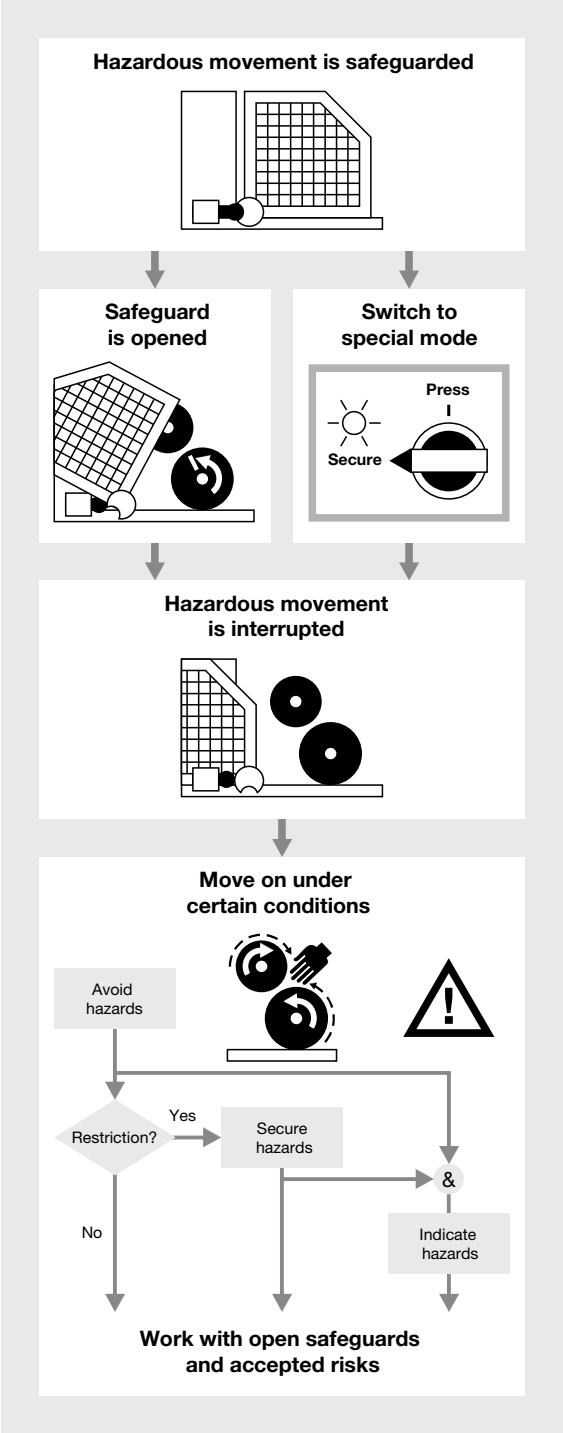
ガードは、物理的なバリヤを使用して、人や時間的および空間的に同時に発生する危険な状況を阻止するものです。その必須となる設計要件は、EN 14120 および ISO EN 14119 に定められています。材料の選択に関する問題や安定性などの機械的側面の考慮と同時に、安全に関連した、人間工学的な側面を考慮する必要があります。これらの要素は、ガードの機能の品質に関する判断だけではなく、多大な費用をかけて設定・製造された安全防護物が従業員に積極的に使用されるか、無効化されるか、さらには不正操作されるかの判断にも用いることができます。

異論はあるかもしれませんが、経験上、ほぼすべての安全防護物は、時が立てばいつかは、取り除いたり開いたりする必要が生じるものです。安全防護物が開いている場合に基本的に重要なことは、可能な限り危険が回避されていて、従業員が危険から保護されているということです。開いている理由、開いている頻度、開いている状態の安全防護物 (以下の図を参照) の背面で実施される作業に関わる実際のリスクによって、安全防護物の取り付けと監視に使用される手順が決定されます。



安全防護物を開く手順

4.4 安全防護物の不正操作



安全防護物に対するインターロックコンセプト

操作の条件として安全防護物を頻繁に開く必要がある場合、ツールを使用せずに、これが可能でなければなりません。危険な状況が発生する場合は、インターロックまたはガードロック装置の使用を保証する必要があります。結果として生じるリスクに加えてドライブ／技術条件に合わせてさらなる保護対策を調整し、安全防護物が開いている間に実施を必要とする活動が許容可能なレベルのリスクで実行されるようにしなければなりません。

4.4.5 結論

結論として、すべての設計者に対して最後に述べたいことがあります。安全防護物が開くと絶対に機械もサブセクションが動かないようにインターロックを設計することは、実際には安全性に反する行為を促し、結局のところ、事故につながります。とはいえ、設計者が戦うべき相手はその原因であり、人ではありません。機械が意図した通りに動作しない場合、ユーザは介入する以外の選択肢がないと感じます。機械がいつか事故を発生させることで、その行為に「報いる」ことはほぼ確実です。しかし、機械はそれを目的として設計されたわけではないのです。