MACHINERY SAFEBOOK 5

Allen-Bradley

Guardmaster®

機械用
安全関連制御システム

原理、規格、および実装

(Safebookシリーズリビジョン5)

LISTEN.
THINK.
SOLVE.℠

Rockwell Automation

目次

第1章: 規制

EU指令および法令

この章の目的は、機械安全、特にEUにおける防護および保護システムに関係するすべての人に指針を提供することです。産業機器の設計者やユーザを対象にしています。

すべてのEU加盟国と他の3カ国で構成される欧州経済地域(EEA)の域内における自由市場の概念を促進するため、すべての加盟国は機械とその使用に関する重要な安全要件を定義する法律を制定する必要があります。

これらの要件に適合しない機械は、EEA諸国向けにまたは域内で供給することはできません。

産業機械および機器の安全に適用できる複数の欧州指令が存在しますが、最も直接的に関連性があるのは次の2つです。

1 **機械指令(Machinery Directive)**

2 **作業者による作業現場での作業機器の使用に関する指令 (Use of Work Equipment by Workers at Work Directive)**

機械指令の必須健康安全要求事項(EHSR)が、作業機器の使用に関する指令で機器の安全性を確認するために使用できるため、この2つの指令は直接的に関連しています。

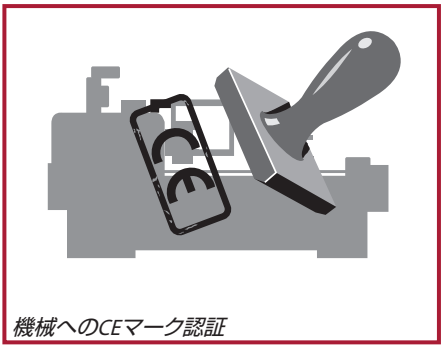
本章ではこの2つの指令の諸側面について説明し、EEAおよびその他の特定の欧州諸国向けにまたはEEA域内で産業機器の設計、供給、購入、または使用に関係するすべての人が、その要求事項を十分に理解することを強くお奨めします。これらの指令に適合しなければ、機械のサプライヤまたはユーザはこれらの国で機械を供給または稼動することは許可されません。

機械に関連する欧州指令はそれ以外にもあります。ただし、それらの多くは特定の用途に特化しているため本章では取り上げませんが、関連性がある場合は、その要求事項も満たす必要があることに注意する必要があります。例えば、EMC指令2014/30/ECやATEX指令2014/34/EUなどがこれに当たります。

機械指令

機械指令では、安全コンポーネントを含む新しい機械やその他の機器の供給が対象となります。この指令の規定および要求事項に適合しなければ、機械をEU内で供給することは違法です。

この指令で定義される最も広義の「機械」とは、人または動物の直接的な動力以外の駆動システムが取付けられ、または取付けることを意図した部品の集合であり、連結された部品またはコンポーネントによって構成され、少なくともその1つが可動部品であり、特定の用途に合わせて結合されます。



機械へのCEマーク認証

現行の機械指令(2006/42/EC)は、旧版(98/37/EC)から2009年末に置き換えられました。この指令では内容の明確化や修正が施されていますが、その「必須健康安全要求事項」(EHSR)に対する根本的な変更は行なわれていません。変更は技術や方法の変化に対応するために行なわれます。また、特定のタイプの機器(建設現場で使用されるホイストなど)に対応するためにその範囲が拡張されています。現在、適用されるEHSRを決定するためのリスクアセスメントの明確な要求事項が追加され、付属書IV「機器」の適合性評価手順が変更されています。

機械指令の定義やその他すべての側面に関する詳細情報や指針については、EUの公式ウェブサイト(*http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm*)をご覧ください。

旧版の指令(98/37/EC)の機械に関する主要な規定は、1995年1月1日に施行され、安全コンポーネントに関する主要な規定は1997年1月1日に施行されました。

現行の指令(2006/42/EC)の規定は、2009年12月29日に施行されました。供給された機器がこの指令に適合することを保証することは、その製造メーカまたは正規代理店の責任になります。これには以下が含まれます。

- 指令の付属書Iに含まれる該当するEHSRが満たされることを保証すること
- 技術ファイルを作成すること
- 適切な適合性評価を実施すること
- 「EC適合宣言書」を提出すること
- 必要に応じてCEマーキングを添付すること
- 安全使用のための取扱説明書を提供すること

必須健康安全要求事項

機械はEHSRを満たす必要がある

指令の付属書1には、必須健康安全要求事項(EHSRと呼ばれる)のリストが記載され、該当する場合、その機械はこれらの要求事項を満たす必要があります。このリストの目的は、機械が安全でその使用期間のすべての段階を通じて人員を危険にさらすことなく使用、調整、および保守できるように設計·製造されることを保証することにあります。以下に標準的な要件の概要を示しますが、付属書1に記載されたすべてのEHSRを考慮する必要があります。対象の機器に適用されるEHSRを決定するためには、リスクアセスメントを実施する必要があります。

付属書1のEHSRでは、危険を排除するために以下の階層構造からなる対策を規定します。

(1) 本質的安全設計。可能な限り、設計自体によって危険を防止します。それが不可能な場合は、**(2) 追加の保護装置**(アクセスポイントがインターロックされたガードや、ライトカーテン、セーフティマットなどの非物質的な防壁による)を使用してください。上記の方法によって対処できない残存リスクについては、次の方法で防止する必要があります。**(3) 個人用保護具またはトレーニング**。機械サプライヤは、どの方法が適切であるかを明示する必要があります。

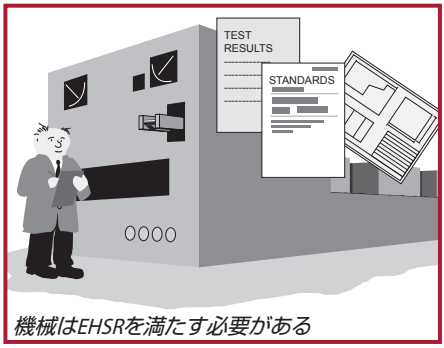
製造や稼動のために、適切な材料を使用してください。十分な照明および取扱施設を用意してください。制御および制御システムは安全で信頼できるものを使用する必要があります。機械は予期せず起動できないようにする必要があり、1つ以上の非常停止装置を取付ける必要があります。上流または下流プロセスが機械の安全に影響を及ぼす可能性がある複雑な設置には配慮する必要があります。停電または制御回路の故障が危険な状況を発生させないようにする必要があります。機械を安定した状態に保ち、予測可能な応力に十分耐えることができなければなりません。けがの原因となる鋭利な先端や表面が露出しないようにしてください。

可動部品などの危険を防止するためガードまたは保護装置を使用する必要があります。これらの保護装置は堅牢な構造を持ち、容易に通過できないものでなければなりません。固定式ガードは、工具がなければ取り外せない方法で取付ける必要があり、脱落防止機構付きの留め具を使用してください。移動式ガードはインターロックしてください。調節式ガードは、工具を使用しなくても容易に調整できるものを使用してください。

蓄積エネルギーを含む電源およびその他のエネルギー源の危険を防止する必要があります。高温、爆発、騒音、振動、粉塵、ガス、放射による傷害のリスクを最小限に抑えてください。保守および修理を適切に行なってください。十分な表示および警告装置を設置する必要があります。機械の安全な設置、使用、調整などに関する取扱説明書を提供する必要があります。

適合性評価

設計またはその他の責任企業は、EHSRへの適合性を証明する根拠を示すことができなければなりません。このファイルには、試験結果、図面、仕様などの関連するすべての情報が含まれます。



機械はEHSRを満たす必要がある

機械指令に基づきEUの官報(Official Journal of the European Union (OJ))に記載され、適合性推定の停止日に至っていない欧州整合(EN)規格は、特定のEHSRへの適合性推定を与えられます。(OJに記載されている最近の規格の多くには、その規格で対象となるEHSRを特定する相互参照が含まれます)。したがって、機器がそのような欧州整合規格に適合する場合、EHSRとの適合性を証明するタスクは大幅に簡略化され、製造メーカも法的確実性の向上による恩恵を受けることができます。これらの規格は法的には必要ありませんが、代替方法によって適合性を証明することは極めて複雑な問題となるため、これらの規格を使用することを強くお奨めします。これらの規格は機械指令をサポートし、ISOとの協力によりCEN (欧州標準化委員会)、およびIECの協力によりCENELEC (欧州電気標準化委員会)によって作成されます。

機械の潜在的なすべての危険に対処できるように、文書化された徹底的なリスクアセスメントを実施する必要があります。同様に、すべてのEHSRが欧州整合規格によって取り扱われていないものも含めて満たされるようにすることは機械製造メーカの責任です。

技術ファイル

製造メーカまたはその正規代理店は、EHSRへの適合性の証拠を提供するために技術ファイルを作成する必要があります。このファイルには、試験結果、図面、仕様などの関連するすべての情報が含まれます。

すべての情報をハードコピーとして永久的に使用できるようにする必要はありませんが、技術ファイル全体が所轄官庁(機械の適合性をモニタするためにEU加盟国によって指名された団体)からの要請により検査できるようにしておく必要はあります。

技術ファイルには少なくとも以下の文書を含める必要があります。

1. 制御回路図を含む機器のすべての図面
2. 機械のEHSRの適合性をチェックするために必要な詳細図、計算書など
3. 機械に適用される必須健康安全要求事項のリストを含むリスクアセスメント文書および実装された保護手段の説明
4 該当する必須健康安全要求事項を示す、使用されている規格およびその他の技術仕様のリスト
5 機械によって発生する危険を防止するために採用された方法の説明
6 該当する場合、試験施設またはその他の組織から取得した技術報告書または証明書
7 欧州整合規格との適合性が宣言されている場合は、試験結果を記載した技術報告書
8 機械の取扱説明書
9 必要に応じて、半完成機械類の組み込みの適合宣言書、および当該機械の関連する組立説明書
10 必要に応じて、機械に組み込まれた機械またはその他の製品のEC適合宣言書のコピー
11 EC適合宣言書のコピー

連続生産では、生産されるすべての機械の適合性を保証するための内部対策(品質システムなど)について、以下に従います。

- 製造メーカは、コンポーネント、留め具、または機械の完成品がその設計および構造により安全に設置され運転を開始できるかどうかを確認するために、これらに関する必要な調査または試験を実施する必要があります。
- 技術ファイルは、常に単一ファイルとして維持する必要はありませんが、妥当な時間内に各部を集めて利用できるようにしておく必要があります。技術ファイルは、最後のユニットが生産されてから10年間は使用できるように維持する必要があります。

機械の製造に使用されるサブアセンブリに関する詳細図面またはその他の特定情報がEHSRへの適合性を証明するために必要でない限り、技術ファイルにそれを含める必要はありません。

付属書IV機械の適合性評価

適合性評価

特定のタイプの機器は、特別な手段が必要となります。これに該当する機器は指令の付属書IVに記載されており、木工機械、プレス機、射出成形機、坑内機器、自動車修理用リフトなどの危険性の高い機械が含まれます。

また付属書IVには、人の存在を検出するように設計された保護装置(ライトカーテンなど)や安全機能を確保するためのロジックユニットなどの特定の安全コンポーネントも含まれます。

該当する欧州整合規格に完全に適合していない付属書IVの機械では、製造メーカまたはその正規代理店は以下の手続きのいずれかを実施する必要があります。

1. EC型式審査。技術ファイルを作成し、機械のサンプルをEC型式審査を行なう認定機関(試験会社)に提出する必要があります。この試験に合格すると、機械にEC型式認証書が与えられます。この認証書の有効性は、5年ごとに認定機関で再検査を受ける必要があります。

2. 完全品質保証。技術ファイルを作成し、製造メーカは設計、製造、最終検査および試験に関する承認された品質システムを使用する必要があります。品質システムは、この指令の規定への機械の適合性を保証する必要があります。品質システムは、認定機関による定期的な監査を受ける必要があります。


認定機関の検査

付属書IVに含まれない機械、または付属書IVには含まれるが該当する欧州整合規格に完全に適合していない機械については、製造メーカまたはその正規代理店は、技術文書および自己査定を作成し、機器の適合性を宣言する選択肢もあります。製造された機器が適合性を維持するように内部チェックを行なう必要があります。

認定機関

認定機関はネットワークを通じて相互に連絡を取り、EU全体で共通の基準が使用されるように協力します。認定機関は政府によって(業界によってではなく)指名されます。認定機関の資格を持つ組織については、以下のサイトをご覧ください。

http://ec.europa.eu/growth/tools-databases/nando/

EC適合宣言書の手続き

CEマーキングは、供給されるすべての機械に適用される必要があります。機械を供給するには、EC適合宣言書も必要です。

CEマークは、その機械が該当するすべての欧州指令に適合し、適切な適合性評価手続きが完了していることを示しています。関連するEHSRを満たしていない機械にCEマークを付けることは機械指令の違反になります。

EC適合宣言書には以下の情報を含む必要があります。

- 製造メーカおよび必要に応じて正規代理店の商号および正式な住所
- 技術ファイルの編纂認定者(その業界で実績のある者でなければならない)の名称および住所(EU外の製造メーカの場合、これは「正規代理店」となる)
- 一般名称、機能、モデル、タイプ、シリアル番号および商品名を含む、機械の説明および識別
- 機械がこの指令の関連するすべての規定を満たしていることを明確に宣言する文、および必要に応じて他の指令または機械が適合する関連規定への適合性を宣言する類似の文章
- 必要に応じて、使用される整合規格の参考文献
- 必要に応じて、使用されるその他の技術規格および仕様の参考文献
- (付属書IV 機械に関して) 必要に応じて、付属書IVで参照されているEC型式審査を実施した認定機関の名称、住所、および識別番号およびEC型式認証書番号
- (付属書IV 機械に関して) 必要に応じて、付属書Xで参照されている完全品質保証を承認した認定機関の名称、住所、および識別番号
- 宣言の場所および日付
- 製造メーカまたはその正規代理店のかわりに宣言書を作成する権限を付与された者の身分および署名

半完成機械類の組み込みのEC適合宣言書

後日、他の品目と組み合わせて完成機械を作るために機器が供給された場合は、その機器とともに組み込みの適合宣言書を発行する必要があります。CEマークは適用されません。この宣言書には、半完成機械類が組み込まれる機械の適合性が宣言されるまでは、機器を使用してはならないことが明記されます。技術ファイルを作成し、安全を犠牲にせずに半完成機械類を最終機械に正しく組込むために満たす必要がある条件の説明を含む情報とともに機器を供給する必要があります。

このオプションは、独立で機能する機器または機械の機能を変更する機器には使用できません。

組込みの適合宣言書には以下の情報を含める必要があります。

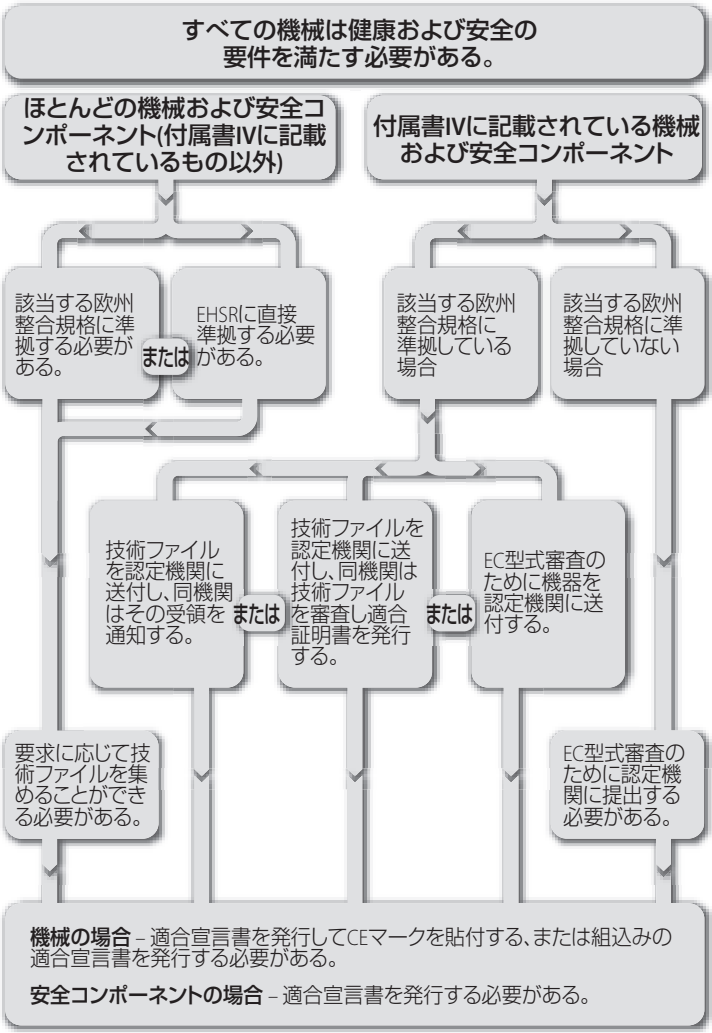
- 半完成機械類の製造メーカ、および必要に応じてその正規代理店の商号および正式な住所
- 関連する技術文書の編纂認定者(その業界で実績のある者でなければならない)の名称および住所(EU外の製造メーカの場合、これは「正規代理店」となる)
- 一般名称、機能、モデル、タイプ、シリアル番号および商品名を含む、半完成機械類の説明および識別
- この指令の重要な要件が適用され満たされていることを宣言する文、および関連する技術文書が付属書VIIのパートBに従って編纂されていることを宣言する文、および必要に応じて、半完成機械類の他の関連する指令への適合性を宣言する文章
- 国家当局の合理的な要請に対応して半完成機械類に関する情報を送信することの誓約。これには送信方法も含まれ、半完成機械類の製造メーカの知的財産権が損われることはありません。
- 必要に応じて、半完成機械類が組み込まれる最終完成機械のこの指令の規定への適合性が宣言されるまでは、半完成機械類を使用してはならないことを明記した声明
- 宣言の場所および日付
- 製造メーカまたはその正規代理店のかわりに宣言書を作成する権限を付与された者の身分および署名

EU外から供給された機械 – 正規代理店

EU (またはEEA)外の製造メーカがEU加盟国に機械を輸出する場合は、その製造メーカは正規代理店を指名する必要があります。

正規代理店とは、機械指令に関連する義務および手続きのすべてまたは一部を製造メーカにかわって実行することを製造メーカから書面で委任を受けた欧州共同体内に所在する自然人または法人を意味します。

作業機器の使用に関するEU指令(U.W.E.指令)



機械指令がサプライヤに向けたものであるのに対して、この指令(2009/104/EC)は機械のユーザに向けたものです。この指令は全産業分野に適用され、雇用主に対して作業機器の安全性に関する最小限の要件を含む一般的な義務を課します。すべてのEU加盟国は、この指令を実施するためにそれぞれ固有の法律を制定しています。

例えば、英国ではProvision and Use of Work Equipment Regulations (作業機器提供･使用規則)(略称P.U.W.E.R.)という名称で実施されています。実施形式は各国により異なりますが、指令の効力には変わりありません。

指令の条文には、指令が適用される機器のタイプと作業場所の詳細が説明されています。

また、条文には作業に向けた安全システムの導入や適切に維持する必要がある適切で安全な機器の提供などの雇用主の一般的な義務も規定されています。機械オペレータに対しては、機械の安全使用に関する適切な情報とトレーニングを提供する必要があります。

1993年1月1日以降に提供された新しい機械(およびEU外からの中古機械)は、機械指令(過渡的な措置に従う)などの関連する製品指令を満たす必要があります。作業場所に初めて導入されたEU内からの中古機器は、U.W.E.指令の付属書に規定された最小要求事項を直ちに満たす必要があります。

注: 全面的な分解修理または大幅に改造された既存または中古機械類は新しい機器に分類され、これらの機器に対する作業は(社内使用の場合であっても)機械指令に適合するように実施する必要があります。

作業機器の適合性は指令の重要な要件であり、リスクアセスメントの適切なプロセスを実施する雇用主の責任を強調しています。

機械類の適切な保守は必要不可欠です。つまり、日常的および計画的な予防保守スケジュールを実施する必要があります。実施された保守作業を記録し、常に更新することを推奨します。機器の保守およびチェックが保護装置またはシステムの継続的な安全性に寄与する場合、このことは特に重要です。

U.W.E.指令の付属書では、作業機器に適用される一般的最小要件が規定されています。

機器が機械指令などの該当する製品指令に適合する場合、その機器は付属書の最小要件に規定されている対応する機械設計要件に自動的に適合します。

加盟国は、U.W.E.指令の最小要件以上の作業機器の使用に関する法律を制定することができます。

作業機器の使用に関する指令については、EUの公式ウェブサイト(*https://osha.europa.eu/en/legislation/directives/3*)をご覧ください。

米国の規制

ここでは、米国におけるいくつかの産業機械安全保護規制について説明しますが、これは開始点にすぎません。ユーザは特定のアプリケーションの要件についてさらに調査し、機械の設計、使用および保守手順および慣行が自身の必要性に合致するとともに、国家および地域の法律および規制に適合することを保証するための対策を講じる必要があります。

米国には産業安全を推進する多くの組織があります。これらの組織には以下が含まれます。

1. 確立した要件を使用し、その会社固有の内部要件を確立している企業
2. 労働安全衛生局(OSHA)
3. 全国防火協会(NFPA)、ロボット工業会(RIA)、および製造技術協会(AMT)などの産業組織、ANSI(広く認められている規格一覧を発行)、およびロックウェル・オートメーションなどの安全製品およびソリューションのサプライヤ

OSHA (米国労働安全衛生局)

米国では、産業安全を推進する主要な組織の1つに労働安全衛生局(OSHA)があります。OSHAは、米国議会の決議により1971年に設立されました。設立の目的は安全で健全な作業環境を提供し、人的資源を保護することにあります。同法により、労働長官は州際通商に影響を及ぼす事業に義務的に適用される労働安全衛生基準を設定することを認められています。同法は、州、コロンビア特別区、米領プエルトリコ、バージン諸島、米領サモア、グアム、大平洋諸島信託統治領、ウェーク島、領海外大陸棚法で定義された領海外大陸棚、ジョンストン島、およびパナマ運河地帯の職場で実施される雇用に対して適用されます。

同法5条は基本的要件を定めています。雇用主は各従業員に対して、従業員の死亡または重大な身体的危害の原因となる、またはその可能性があると認識されている危険が存在しない仕事および職場を提供しなければなりません。また、雇用主は同法に基づいて公布された労働安全衛生基準を遵守する必要があります。

また同法5条では、各従業員もその行動および行為に適用される労働安全衛生基準および同法に従って発行されたすべての規則、規制、および命令を遵守すべきことを示しています。

OSHA法(労働安全衛生法)は、雇用主および被雇用者の双方に責任を課しています。このことは、危険がない機械を市場に供給することをサプライヤに要求する機械指令とは大きく異なります。米国では、サプライヤは何の安全保護手段も施されていない機械でも販売することができます。ユーザは、機械を安全に使用するために安全防護対策を追加する必要があります。これは同法が承認された当時は一般的な慣行でしたが、設計段階から機械に安全を組込むことは、機械を設計・製造した後に安全保護装置を追加するより遙かにコスト効率が良いため、現在ではサプライヤが安全防護を取付けた機械を提供するのが主流となっています。規格を通じてサプライヤとユーザが安全防護の要件について連絡を取り合い、機械の安全だけでなく生産性も向上させる試みが現在進められています。

労働長官は、当該規格の公布が特に指定された被雇用者の安全衛生の改善をもたらさない場合を除き、国家コンセンサス規格および制定された連邦規格を労働安全衛生規格として公布する権限を有します。

OSHAは、連邦規則集タイトル29 (29 CFR)の規制を発行することによってこの課題を達成します。産業機械に関する29 CFRのパート1910の規格は、OSHAによって発行されました。これらの規格は、OSHAのウェブサイト(www.osha.gov)で自由に利用できます。ほとんどの規格が任意規格(自主基準)であるのに対して、OSHA規格は法律です。

機械安全に関する重要部分には以下が含まれます。

A – 総則
B – 制定された連邦規格の採択および拡張
C – 一般安全衛生規定
H – 危険物
I – 個人用保護具
J – 一般的環境規制(ロックアウト/タグアウトを含む)
O – 機械類および機械防護
R – 特殊産業
S – 電気

一部のOSHA規格では、任意規格が参照されています。参照による編入の法的効力は、連邦公報でその資料の全文が発行された場合と同様に取り扱われます。国家コンセンサス規格がサブパートの一つに参照参照文書として組み込まれている場合、その規格は「法的拘束力」を持ちます。

例えば、NFPA 70 (米国電気工事規程として知られる任意規格)が、サブパートSで参照されています。これによって、NFPA70規格の要件は強制規格になります。

サブパートJの29 CFR 1910.147では、危険なエネルギーの管理が対象になります。これは、ロックアウト/タグアウト規格として一般的に知られています。これに相当する任意規格がANSI Z244.1です。基本的に、この規格では修理チェックまたは保守を行なう際は機械の電源をロックアウトすることを要求しています。その目的は、従業員の傷害の原因となる機械の予期しない通電または始動を防止することにあります。

従業員は、ロックアウトおよびタグアウトプログラムを確立し、適切なロックアウト装置またはタグアウト装置エネルギー分離装置に取付けるための手順を用いる必要があり、予期しない通電、始動または蓄積されたエネルギーの放出を防止して従業員の傷害を防止するため、機械または機器を無効にするその他の方法を用いる必要があります。

通常の生産作業中に行なわれるわずかな工具の変更および調整、およびその他の小規模な修理チェック作業は、それらの作業が日常的に繰返し実行する必要があり、生産のための機器の使用と不可分である場合は、ANSI Z244「代替手段」の規定が適用されますが、ただしそのような場合は、有効な保護を提供する代替手段を使用して作業することが条件となります。これはOSHAによって直接サポートされています(「OSHA小規模サービス除外」)。代替手段とは、ライトカーテンやセーフティマット、ゲートインターロック、および安全システムに接続されたその他の類似のデバイスなどの安全保護装置を指します。機械設計者とユーザにとって困った問題は、何が「小規模」で何が「日常的に繰返され、不可分」であるかを判断することです。これは、リスクアセスメントに含めることができます。

サブパートOは、「機械類および機械防護」について規定しています。このサブパートには、すべての機械の一般的な要件と一部の特定の機械の要件が記載されています。OSHAは、1971年に発足したときに多くの既存のANSI規格を採用しました。例えば、機械式パワープレスに関するB11.1は、1910.217として採用されました。

1910.212は、機械に関する一般的なOSHA規格です。この規格では、機械領域のオペレータおよびその他の作業員を作業点、巻き込み点、回転部品、飛散する切り屑、スパークなどによって発生する危険から保護するために機械防護のための1つ以上の方法を提供することが義務づけられています。ガードは、可能であれば機械に取付け、何らかの理由で機械への取付けが不可能な場合はそれ以外の場所に取付ける必要があります。ガードは、それ自体が偶発的危険にならないようなものを使用する必要があります。また、ガードを取り外す必要がある場合は、取り外し用の工具も必要となります。

「作業点(ポイント·オブ·オペレーション)」とは、処理中の材料に対して作業が実際に実行されている機械の領域のことです。機械の作業点は、その動作によって作業員を怪我の危険にさらすことになるため、防護しなければなりません。この保護装置は該当する規格に適合する必要があり、該当する特定の規格が存在しない場合は、動作サイクル中にオペレータの身体のいかなる部分も危険領域に入ることを防止するように設計·製造する必要があります。

サブパートS (1910.399)では、OSHA電気要件が規定されています。設備または機器は、労働次官補によって受理され、国家承認試験研究所(NRTL)によって安全であることを承認、認証、リストに記載、ラベル表示、またはその他の方法で確認された場合は、このサブパートSの意図する範囲内で承認されます。

「機器」という用語は次のように定義されます。電気設備の一部としてまたはこれに接続して使用される材料、取付具、装置、器具、固定具等を含む総称。

「リストに記載」という用語は次のように定義されます。機器は、次のようなリストに記載された場合に「リストに記載」されたと見なされます。(a) そのような機器の生産の定期的な検査を実施する国家承認試験研究所(NRTL)によって発行されたもの、(b) 国家承認規格に適合する機器であること、または特定の方法で試験され使用の安全が確認されたことを正式に示すもの。

2009年8月以降、以下の会社がNRTLとしてOSHAによって承認されています。

- カナダ規格協会(Canadian Standards Association) (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- サウスウエスト･リサーチ･インスティテュート (Southwest Research Institute) (SWRI)
- TÜV SÜD America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TÜV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

要求事項に関する最終決定権は規制当局(AHJ)にあります。例えば、ニューヨーク州、カリフォルニア州、イリノイ州などの州では追加要件があります。

一部の州では、州独自のOSHAを採用し、米国/連邦OSHA要件に対して要件が追加される場合があります。24州、プエルトリコ、およびバージン諸島には、OSHA承認の州計画があり、州独自の規格および実施方針があります。これらの州は、大部分は連邦OSHAと同一の規格を採用しています。ただし、一部の州ではこの問題に関して異なる規格および異なる実施方針を採用しています。雇用者はOSHAにインシデント発生履歴を報告する必要があります。OSHAは、インシデント発生率を集計し、この情報を地方事務所に送信し、この情報を使用して検査の優先順位を決定します。検査の重要な要因は以下の通りです。

- 差し迫った危険
- 大惨事および死亡事故
- 従業員の告発
- 非常に危険な産業
- 地域計画検査
- 追跡調査
- 連邦および地域特定プログラム

OSHA規格を違反すると罰金が課せられる場合があります。以下に罰金の一覧を示します。

- 重大な違反: 違反1件につき最大7000ドル
- 重大ではない違反: 自由裁量(7000ドルを超えない範囲)
- 再犯: 違反1件につき最大70,000ドル
- 故意の違反: 違反1件につき最大70,000ドル
- 違反による死亡事故: 追徴金
- 危険低減の改善なし: 1日ごとに7000ドル

カナダの規制

カナダでは、産業安全は州レベルで管理されています。各州では独自の規制が維持され実施されています。例えば、オンタリオ州では労働安全衛生法が制定され、同法は職場のすべての当事者の権利と義務を規定しています。同法の主要目的は、業務上の安全衛生に関する危険から従業員を保護することにあります。同法は職場の危険に対処する手順を制定し、規制が自主的に遵守されない場合の法律の執行を規定しています。

同法に含まれるものとして、「開始前健康安全審査」について定めた規制851、セクション7があります。このレビューはオンタリオ州内での新品、再構築または改修された機械に対して要求され、専門エンジニアによって報告書を作成する必要があります。

第2章: 規格

この章では、機械安全に関連する代表的な国際および国家規格のいくつかを取り上げます。ここでは包括的なリストを作成することが目的ではなく、標準化の対象となる機械安全の問題について洞察を与えることにを主要な目的としています。この章をお読みになるときは、「規制」の章も合わせてお読みください。

世界の国々は、規格の国際的な調和に向けて取り組んでいます。このことは特に、機械安全の領域で顕著に現れています。国際的な機械類の安全規格は、ISOとIECという2つの団体によって管理されています。各地域および国家の規格は今なお存在し、地域の要件に継続して対応していますが、多くの国ではISOとIECによって作成された国際規格の使用に向けた移行が行なわれています。

例えば、EN (European Norm) 規格はEEA諸国全体を通じて使用されています。すべての新しいEN規格は、ISOおよびIEC規格と足並みを揃え、ほとんどの場合、同一の本文が含まれています。現在、米国でもIECおよびISO規格がしばしば参照されます。

IECは電気技術分野を受け持ち、ISOはその他すべての分野を対象としています。ほとんどの先進工業国は、IECおよびISOの加盟国です。機械安全規格は、世界の多くの先進工業国の専門家で構成される作業部会によって起草されます。

ほとんどの国では、規格は任意と見なされますが、規制は法的強制力があります。しかしながら、規格は通常、規制の現実的な解釈として使用されています。したがって、規格と規制の世界は密接に関連し合っています。

ISO (国際標準化機構)

ISOは世界のほとんどの国(本書の発行時には157ヶ国)の国家規格団体で構成される非政府組織です。スイス、ジュネーブにある中央事務局が組織を統括しています。ISOは、より効率的で安全、清潔な機械類の設計、製造、および使用に関する規格を作成しています。これらの規格によって国家間の貿易もさらに簡単で公正なものになります。ISO規格は、規格名に含まれるISOの3文字によって識別できます。

ISO機械規格は、EN規格と同じようにタイプA、B、およびCの3階層で構成されています(EN欧州整合規格に関する後のセクションを参照)。

詳細は、ISOのウェブサイト(*www.iso.org*)をご覧ください。

IEC (国際電気標準会議)

IECは、電気、電子、および関連技術に関する国際規格を策定し発行します。IECは、その会員を通じて電気電子技術分野における標準化のすべての問題および電気電子規格への適合性評価などの関連事項に関する国際協力を促進します。

詳細は、IECのウェブサイト(*www.iec.ch*)をご覧ください。

EN欧州整合規格

これらの規格は、すべてのEEA諸国に共通して適用され、欧州標準化委員会(CEN)およびCENELECによって作成されます。その使用は任意ですが、これらの規格に従って機器を設計および製造することは、機械指令のEHSRへの適合性を証明するための最も直接的な方法です。

これらの規格はA、BおよびC規格の3つのタイプに分類されます。

タイプA規格: すべてのタイプの機械に適用される側面を対象にします。

タイプB規格: 2つのグループに細分されます。

タイプB1規格: 機械の特定の安全および人間工学的な側面を対象にします。

タイプB2規格: 安全コンポーネントおよび保護装置を対象にします。

タイプC規格: 特定のタイプまたはグループの機械を対象にします。

C規格への適合は、当該規格が対象とするEHSRへの適合を暗黙の前提としていますので注意してください。適切なC規格が存在しない場合は、該当するセクションへの準拠を指し示すことにより、AおよびB規格がEHSR適合性の部分的または完全な証明として使用できます。

CEN/CENELECと、ISOやIECなどの機関間の協力に関して合意に至りました。これによって最終的に世界共通の規格が実現すると考えられています。ほとんど場合、EN規格にはIECまたはISOの規格に対応する規格が存在します。一般的に、両者の本文は同じものであり、地域的な相違が規格の序文に示されます。

EN機械安全規格の完全なリストについては、以下のウェブサイトをご覧ください。

http://ec.europa.eu/growth/single-market/european-standards/

米国の規格

OSHA規格

可能な場合、OSHAは国家コンセンサス規格または確立した連邦規格を安全規格として公布します。参照文書として組み込まれている規格の強制的な規定(例えば、「～なければならない」という言葉は必須であることを意味する)は、パート1910に記載された規格と同等の効力と影響力を持っています。例えば、国家コンセンサス規格であるNFPA 70は、CFRのパート1910のサブパートS「電気」の付属書Aに参考文書として記載されています。NFPA 70は、全国防火協会(NFPA)によって作成された任意規格です。NFPA 70は、米国電気工事規程(NEC)としても知られています。組み込みによって、NECの必須要件はすべてOSHAの必須になります。

ANSI規格

米国規格協会(ANSI)は、米国内の民間部門の自主的な標準化システムの管理者および調整団体としての役割を果たしています。ANSIは、民間および公共部門のさまざまな後援者によって支持されている非営利の会員制民間団体です。

ANSI自体は規格の作成は行なわず、公認された団体間のコンセンサスを確立することによって規格の開発を促進しています。また、ANSIは公認団体がコンセンサスの基本理念、適正手続き、および公開性に必ず従うように監督しています。

これらの規格は、適用規格または構造規格のいずれかに分類されています。適用規格は、安全保護手段を機械に適用する方法を定義します。その例としては、ANSI B11.1ではパワープレス機での機械防護の使用に関する情報を提供し、ANSI/RIA R15.06ではロボット保護のための安全保護手段の使用を概説しています。

全国防火協会

全国防火協会(NFPA)は1896年に組織されました。同協会の使命は、火災および関連する安全問題に関する科学的根拠に基づいた法令や規格、調査・研究および教育を提言することにより、QOL (生活の質)の見地から火災の負担を低減することにあります。NFPAは多くの規格を援助し、その使命を達成することを支援します。産業安全および安全防護に関連する2つの非常に重要な規格には、米国電気工事規程(NEC)と産業機械用電気規格があります。

全国防火協会は、1911年以来、NECの後援団体として活動しています。最初の規約書は、さまざまな保険、電気、建築、および提携業者が結束した取り組みの結果として1897年に作成されました。NECはそれ以降も何度となく更新され、約3年ごとに改訂が行なわれています。

NECの670条では、産業機械に関するいくつかの問題を詳細に取り上げ、産業機械用電気規格、NFPA 79について言及しています。

NFPA 79は、産業機械の電気/電子設備、装置、またはシステムに適用されます。NFPA 79の目的は、生命および財産に対する安全を促進する産業機械の一部として供給される電気/電子設備、装置、またはシステムの詳細な情報を提供することです。NFPA 79は、1962年にANSIによって公式に採択され、IEC 60204-1規格の内容に非常に類似しています。

特定のOSHA規格によって取り扱われていない機械は、死亡まは重傷事故の原因となることが広く認められている危険を防止する必要があります。これらの機械は、適用される産業規格の要件を達成または超過するように設計および維持される必要があります。NFPA 79は、OSHA規格で特に規定されていない機械に適用される規格です。

カナダの規格

CSA規格は、製造メーカ、消費者、小売業者、組合、および職能団体を含む、生産者およびユーザの全国的な合意が反映されています。この規格は商工業分野で広く使用されており、市役所、州政府、および連邦政府でもその規制にしばしば採用されています。特に、保健、安全、ビルや建築物、および環境の分野で使用されています。

カナダ国内の個人、企業、および団体は、CSA協会の作業にボランティアとして時間とスキルを提供したり、協会の継続会員として存在することで協会の目的を支持することにより、CSAの規格開発への支援を表明しています。7000名を超える協会ボランティアと2000名の継続会員の合計がCSAの会員全体を構成しています。

カナダ規格審査会(SCC:Standards Council of Canada)は、国益に資する自発的標準化のさらなる開発および改善に向けた全国的規格システム、独立連合、自律的組織の調整機関です。

オーストラリアの規格

これらの規格のほとんどは、同等のISO/IEC/EN規格と密接に連携しています。

Standards Australia Limited

286 Sussex Street, Sydney, NSW 2001

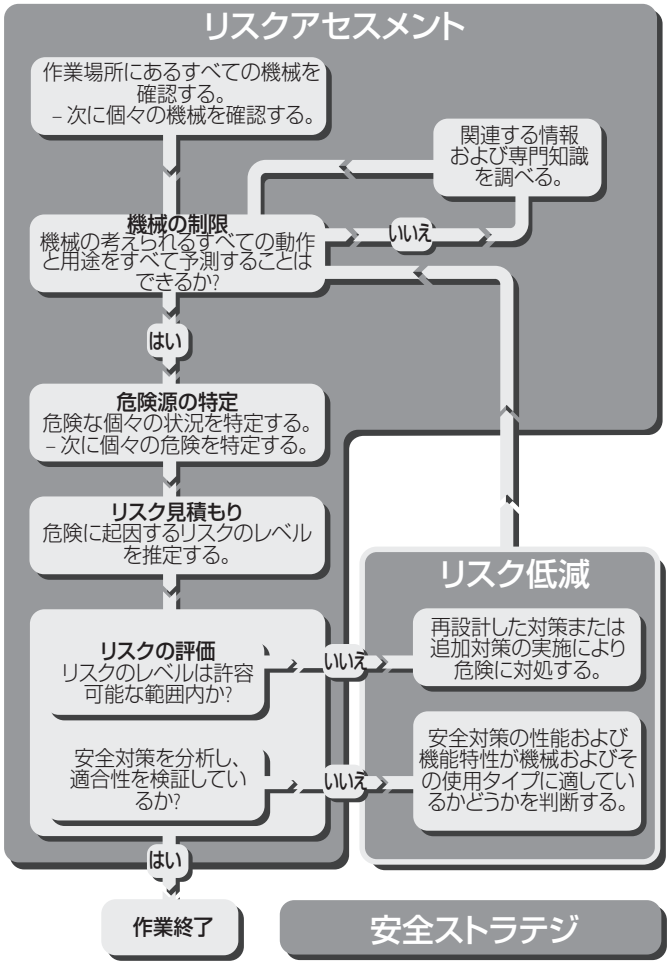
電話: +61 2 8206 6000

電子メール: mail@standards.org.au – Webサイト: *www.standards.org.au*

第3章: 安全ストラテジ

純粋に機能的な観点から見れば、機械は材料を処理するタスクをより効率的に実行するほど優れていると言えます。ただし、機械が機能し続けるためには安全でなければなりません。安全は最重要検討事項と見なさなければなりません。

適切な安全ストラテジを考案するには、下図に示すように相互に連携する2つの重要なステップが存在することが必要です。



リスクアセスメントは、機械の制限および機能、さらに機械がその寿命全体を通して実行する必要のあるタスクの明確な理解に基づいて行なう必要があります。

リスク低減は、リスクアセスメント段階から導き出された情報に基づいて、必要な安全対策が選択された場合に実行されます。これを実行する方法が、機械の安全ストラテジの基礎となります。

これに従った体系的アプローチによって、すべての側面が考慮され、最重要な原則が細部に進むにつれて失われないことが保証されます。そのプロセス全体は文書に記録する必要があります。これによってさらに完璧な仕事が保証されるだけでなく、その結果を他の当事者がチェックのために利用できるようになります。

このセクションの内容は、機械の製造メーカとユーザの両方に適用されます。製造メーカは自社が製造する機械が安全に使用できることを保証する必要があります。リスクアセスメントは、機械の設計段階から始まり、機械で実行する必要がある予測可能なすべてのタスクを考慮する必要があります。リスクアセスメントの初期ループでのこのタスクベースのアプローチは非常に重要です。例えば、機械の可動部品を定期的に調整しなければならない場合があります。設計段階では、このプロセスを安全に実施する対策を施した上で、設計できるようにしてください。初期段階でこれを実施しないと、後の段階で実施することは困難または不可能になる場合があります。その結果、可動部品の調整を実行するにしても、危険または非効率的な方法(またはその両方)で実施しなければならなくなる可能性があります。リスクアセスメントの段階ですべてのタスクを考慮した機械は、より安全でより効率的な機械になります。

ユーザ(または雇用者)は、機械が作業環境で安全であることを確認する必要があります。たとえ製造メーカによって機械が安全であると宣言されている場合でも、機械のユーザはリスクアセスメントを実行し、ユーザの環境でその機器が安全であるかどうかを判断する必要があります。機械は、しばしば製造メーカによって予見できない状況で使用されます。例えば、学校の工作室で使用されるフライス盤は、産業用工場で使用される同じ機械に対してよりも考慮すべき事柄を追加する必要があります。また、それぞれは安全な機械も組み合わせる方法によっては危険になる可能性もあります。

ユーザ企業が2台以上の独立した機械を取得し、それらを1つのプロセスに統合した場合、この企業が最終的に結合された機械の製造メーカとなることも忘れてはなりません。

それでは適切な安全ストラテジを実現するために不可欠のステップについて検討して行きたいと思います。以下の事柄は、既存の工場設備にも、または単体の新しい機械にも適用できます。

リスクアセスメント

リスクアセスメントを負担と見なすことは間違っています。リスクアセスメントは、不可欠な情報をもたらし、ユーザまたは設計者に安全を達成する方法に関する論理的決定を下す能力を与える有益なプロセスです。

この問題に関してはさまざまな規格が存在します。(EN) ISO 12100 機械類の安全 – 設計の一般原則 – リスクアセスメントおよびリスク低減には、世界的に最も適用されている指針が記載されています。ISO技術報告: ISO/TR 14121-2も利用できます。この資料には、リスクアセスメントに関する実用的な指針と方法の例が記載されています。

どのテクニックを使用してリスクアセスメントを実施するにしても、一般的に複数メンバーで構成される機能横断型チームのほうが1人の個人よりも広範囲でバランスの取れた結果を生み出します。

リスクアセスメントは反復プロセスであり、機械のライフサイクルのさまざまな段階で実行されます。利用可能な情報は、ライフサイクルの段階によって異なります。例えば、機械メーカによって実施されるリスクアセスメントは、機械のメカニズムや構成材料に関してあらゆる詳細までアクセスできますが、機械の最終的な動作環境については、おそらく大まかな仮定にすぎません。機械ユーザによって実施されるリスクアセスメントは、必ずしも掘り下げた技術的詳細にアクセスできるとは限りませんが、機械の動作環境のあらゆる詳細までアクセスできます。1つの反復ループの出力が、次の反復ループの入力になるのが理想的です。

機械の制限の決定

これには機械の部品やメカニズム、機能に関する情報の収集や分析が必要になります。また、機械および機械が動作する環境と人間のタスクとのあらゆるタイプの相互作用も考慮する必要があります。その目的は、機械とその使用に関する明確な理解を得ることにあります。

個々の機械が機械的にまたは制御システムによって相互に連結されている場合、適切な保護手段によって「区分」されていない限り、これらは単一の機械として考慮する必要があります。

設置、立上げ、保守、廃棄、適切な使用、運転、ならびに合理的に予測可能な誤用または誤動作を含む、機械の寿命のすべての限界および段階を考慮する必要があります。

タスクおよび危険源の特定

機械のすべての危険源を特定し、その性質および位置に関して記載する必要があります。危険源のタイプには、粉砕、切断、巻き込み、部品の射出、煙、放射、毒物、熱、騒音などが含まれます。

タスク分析の結果は、危険源の特定の結果と比較する必要があります。これは危険源と個人の収束の可能性、すなわち危険な状況の可能性がどこに存在するかを示します。すべての危険な状況が記載される必要があります。個人またはタスクの性質に応じて、同一の危険源が異なるタイプの危険な状況を生み出す可能性もあります。例えば、熟練した技術を持ち、訓練された保守技術者の存在のほうが、機械の専門知識を持たない非熟練の清掃者の存在よりもさまざまな問題を含む場合があります。この状況においては、各ケースがリストアップされ個別に対処されている場合は、保守技術者に対してのほうが清掃者よりもさまざまな保護手段が正当化される可能性があります。各ケースがリストアップされておらず個別に対処されていない場合は、ワーストケースを使用する必要があり、保守技術者と清掃者の両方が同じ保護手段によって保護されます。

場合によっては、既に保護手段が施されている既存の機械(インターロック付き防護ドアによって保護された危険な可動部品を含む機械など)に関する一般的なリスクアセスメントを実施してみる必要があります。危険な可動部品は、インターロックシステムが故障した場合に実際の危険になり得る潜在的な危険源の一例です。インターロックシステムの妥当性が(リスクアセスメントや該当する規格に準拠した設計などによって)既に確認されている場合を除いて、その存在を考慮に入れるべきではありません。

リスク見積もり

これは、リスクアセスメントの最も根本的な側面の一つです。この問題に取り組む多くの方法が存在し、以下のページではその基本的な原理について説明します。

危険な状況につながる潜在性を有するあらゆる機械類は、危険な事象(すなわち損害)のリスクであることを示しています。リスクの量が多くなるほど、それに関して対策することはますます重要になります。ある一つの危険源ではリスクは許容され受容可能なほど小さい可能性がありますが、別の危険源ではリスクはそれに対して最高度の保護手段が必要になるほど大きい可能性があります。したがって、「リスクに関してどのような場合に何をすべきか」という意思決定を行なうためには、それを定量化できることが必要です。

リスクは多くの場合、事故における傷害の重大度という観点だけから語られています。リスクの存在量を推定するには、潜在的危険の重大度および事故の発生確率の両方の側面を考慮に入れる必要があります。

ISO TR 14121-2「リスクアセスメント – 実用的な指針と方法の例」では、リスク定量化のためのさまざまな方法が示されています。用語やスコアリングシステムには相違がありますが、すべての方法は(EN) ISO 12100で提示された原則に関わっています。以下のテキストでは、基本的なリスク定量化の原則を概説し、どの方法論を使用するかに関わらず役に立つ情報を提供することを意図しています。ほとんどの場合、ISO TR 14121-2の6.5条の「ハイブリッドツール」で規定されたパラメータに従っています。

以下の要因について考慮してください。

- 潜在的な傷害の重大度
- 事故が発生する確率

事故の発生確率には、少なくとも次の2つの要因が含まれます。

- 危険にさらされる頻度
- 傷害の確率

確率因子自体は、しばしば次のような他の要因に分けられます。

- 発生の確率
- 回避の可能性

利用可能なあらゆるデータおよび専門知識を活用します。機械の寿命のすべての段階を取り扱うことから、複雑になり過ぎないようにするために、各要因のワーストケースに基づいて決定を行ないます。常識を保持することも重要です。決定には、実現可能性、現実性、および妥当性を考慮することが必要です。ここでは機能横断型チームのアプローチが役に立ちます。

この段階では通常、既存の保護システムを考慮する必要はありません。このリスク見積もりによって保護システムが必要であると確認できた場合は、必要な特性を決定するために使用できる方法論について本章の中で後から説明します。

潜在的な傷害の重大度

本考察では、事故または事件が発生したことを前提としています。危険を十分に考慮することにより、考えられる最も重大な傷害が明らかになります。

注意事項: 本考察では、傷害が不可避であることを前提とし、その重大度のみを検討します。オペレータが危険な動きまたはプロセスにさらされていることを前提とします。傷害の重大度は、選択された方法論に従って評価されます。

以下に例を示します。

- 死亡、眼球または腕の喪失
- 永続的影響、手指の喪失など
- 可逆的影響かつ医療を要する
- 可逆的影響かつ応急処置を要する

危険にさらされる頻度

この係数は、オペレータまたは保守作業員が危険にさらされる頻度を示しています。危険にさらされる頻度は、選択された方法論で規定された係数に従って分類できます。

以下に例を示します。

- 1時間当たり1回より高い頻度
- 1時間当たり1回と1日当たり1回の間
- 1日当たり1回と2週当たり1回の間
- 2週当たり1回と1年当たり1回の間
- 1年当たり1回よりも低い頻度

傷害の確率

オペレータが危険な動きまたはプロセスにさらされていることを前提とします。危険な事象の発生確率は、選択された方法論で規定された係数に従って分類できます。機械の特性を考慮することにより、期待される人間行動および発生確率が分類できるその他の係数が導かれます。

以下に例を示します。

- 無視できる
- まれ
- 可能
- 可能性が高い
- 非常に高い

危険防止の可能性

作業員が機械を操作する方法やモーションが起動する速度などのその他の特性を考慮することにより、傷害防止の可能性は、選択された方法論で規定された係数に従って分類できます。

以下に例を示します。

- 可能性が高い
- 可能
- 不可能

すべての項目をチェックした後に、リスク定量化に使用されるグラフまたは表に結果が入力されます。これにより、機械のさまざまな危険に関して何らかの形式でのリスクの定量化された推定を得ることができます。次にこの情報は、安全の許容可能レベルを達成するために低減する必要があるリスクを決定するために使用できます。

リスク低減

ここで各機械およびその個々のリスクを順次検討し、そのすべての危険に対処する手段を講じる必要があります。

リスク低減のための手段の階層

考慮すべき基本的方法には3つあり、以下の順序で使用されます。

1. 可能な限りリスクを排除または低減します(本質的安全機械設計および構造)。
2. 設計によって排除できないリスクに関連して、安全防護および補足的保護手段を設置します。
3. 警告標識および信号を含む、安全使用のための情報を提供します。また、残存リスクに関する情報や特定のトレーニングまたは個人用保護具の必要性に関する情報も提供します。

階層のそれぞれの手段は一番上の階層から検討していき、可能であれば使用します。このようにすることで、通常は複数の手段を組み合わせて使用することになります。

リスクの排除(本質的安全設計)

機械の設計段階では、材料、アクセス要件、高温面、伝送方式、トラップポイント、電圧レベルなどの要因を慎重に考慮するだけでも考えられる多くの危険を防止することが可能になります。

例えば、危険領域へのアクセスが必要でない場合は、機械の本体内に安全防護を施したり、またはある種の固定式包囲ガードを使用することよって解決することができます。

保護手段およびシステム

アクセスが必要な場合は、解決は少し難しくなります。機械が安全状態のときのみアクセスが得られるように保証する必要があります。インターロック付き防護ドアやトリップシステムなどの保護手段が必要になります。保護装置またはシステムの選択は、機械の動作特性によって大きく影響を受けます。機械の効率性を損なうシステムは、それ自体が不正な取り外しや侵入を受けやすくなるため、このことは極めて重大です。

人間と機械の間の最も複雑で全面的な相互作用の一つが、保守やトラブルシューティング、修理のときに発生します。日常的で小規模な介入の場合は、安全関連システムベースの保護手段(後述の説明を参照)を使用して安全を確保することが可能な場合もあります。しかし、すべての規制にわたって、大規模な保守や修理、分解、または電源回路の作業などのいかなる介入においても、機械のエネルギー(重力を含む場合もある)の遮断および消失を保証する機器の提供と使用の両方が必要になることは極めて明白です。この方法で、予期しない始動およびエネルギー源にさらされるリスクをなくすことができます。この方法は、さまざまな多くの規制および規格で取り上げられています。例えば、「ロックアウト/タグアウト」の規制および規格を説明した「米国の規制」の前述のテキストを参照してください。欧州およびISO規格EN 1037およびISO 14118規格「予期しない始動の防止」でも要件が規定されています。電気技術については、IEC/EN 60204-1およびNFPA 79も指針および要件を記載しています。

もちろん、すべての正しい手順に従うことを保証する適切な作業システムは必要不可欠です。

以下のセクションでは、いくつかの代表的な実装について説明します。

予期しない始動の防止

予期しない始動の防止は、多くの規格で取り上げられています。そのような例には、ISO14118、EN1037、ISO12100、OSHA 1910.147、ANSI Z244-1、CSA Z460-05、およびAS 4024.1603などが含まれます。これらの規格には、予期しない始動を防止する第一の手段は、システムからエネルギーを遮断し、システムをオフの状態にロックするという共通のテーマがあります。その目的は、作業員が安全に機械の危険領域に立ち入ることができるようにすることです。

ロックアウト/タグアウト

新たに製造される機械には、ロック可能なエネルギー分離装置を搭載して製造する必要があります。このデバイスは、電気、油圧、空気圧、重力、およびレーザを含む、あらゆるタイプのエネルギーに適用されます。ロックアウトとは、エネルギー分離装置にロックをかけることを示します。このロックは、制御状態でオーナまたはスーパーバイザによってのみ解除できるようにする必要があります。複数の作業員が同じ機械で作業する必要がある場合は、エネルギー分離装置へのロックは、各作業員がそれぞれかける必要があります。各ロックは、そのオーナを識別できなければなりません。

米国では、タグアウトは、ロック可能なデバイスを取付けることができない旧式の機械でのロックアウトの代替方法として使用されています。この場合、機械がオフになってタグが適用され、タグ保持者が機械で作業をしている間は機械を始動しないようにすべての作業員に警告を発します。1990年以降、変更された機械は、ロック可能なエネルギー分離装置を組込むためにアップグレードする必要があります。

エネルギー分離装置は、エネルギーの伝送または放出を物理的に防止する機械式デバイスです。これらのデバイスは、サーキットブレーカやディスコネクトスイッチ、手動式スイッチ、プラグ/ソケットの組み合わせ、または手動式バルブの形態を取る場合があります。電気絶縁デバイスは、接地されていない電源の導線を切換える必要があり、どの電極も独立して動作できません。

ロックアウトおよびタグアウトの目的は、機械の予期しない始動を防止することです。予期しない始動が発生する原因には、制御システムの故障、始動スイッチ、センサ、コンタクタ、またはバルブの不適切な動作、電源遮断後の電源復旧、またはその他の何らかの内部的または外部的影響などのさまざまな原因があります。ロックアウトまたはタグアウトプロセスの完了後に、エネルギーの消失を確認する必要があります。

安全絶縁システム

安全絶縁システムは、機械の秩序あるシャットダウンを実行し、機械への電源をオフの状態でロックする簡単な方法も提供します。このアプローチは、大型の機械や製造システムに効果的で、特に複数のエネルギー源が中2階または離れた場所に配置されている場合に適しています。

ロードディスコネクト

電気デバイスのローカル絶縁には、絶縁およびロックアウトする必要のあるデバイスの直前にスイッチを配置することができます。Bulletin 194Eロードスイッチは、絶縁およびロックアウトの両方が可能な製品の一例です。

トラップ・キー・システム

トラップ・キー・システムは、ロックアウトシステムを実現するもう一つの方法です。多くのトラップ・キー・システムは、エネルギー分離装置から動作を開始します。スイッチが「一次」キーによってオフになると、機械への電気エネルギーが未接地のすべての電源コンダクタから同時に遮断されます。一次キーはその後に取り外して、機械へのアクセスが必要な場所に持っていくことができます。さらに複雑なロックアウトの配置に対応するために、さまざまなコンポーネントを追加することができます。

ロックアウトの代替手段

機械の修理または保守の実施中は、ロックアウトおよびタグアウトを使用する必要があります。通常の生産作業中の機械への介入は、ガード·ドア·インターロック·システムなどの保護手段によって実行されます。修理/保守作業と通常の生産作業との区別は必ずしも常に明確ではありません。

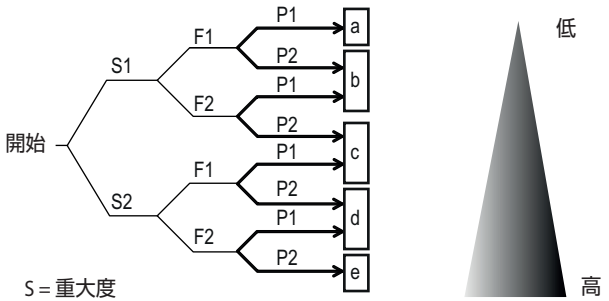
通常の生産作業中に行なわれるある程度小規模な調整や修理作業では、必ずしも機械をロックアウトする必要はありません。材料の積み降ろし、わずかな工具の変更および調整、潤滑レベルのチェック、および廃材の除去などがこの例に含まれます。これらのタスクは、日常的に繰返し実行する必要があり、生産のための機器の使用と不可分であり、効果的な保護を提供する安全防護などの代替手段を使用して作業が実行されます。安全保護装置には、インターロック付きガードやライトカーテン、セーフティマットなどのデバイスが含まれます。適切な安全定格のロジックおよび出力デバイスとともに使用され、オペレータは通常の生産作業や小規模の介入時に機械の危険領域に安全にアクセスできます。

この場合の機械の安全は、障害発生時であっても保護システムの適切な適用と正しい操作に依存します。そのため、システムの正しい操作を考慮する必要があります。各タイプには、障害のモニタ、検出、または防止の性能レベルが異なる技術が選択される可能性があります。

理想的な世界であれば、すべての保護システムは危険な状況に対して故障する可能性が絶対になく完璧に作動するかもしれません。しかし現実の世界では、知識や材料の現在の限界によって常に制約を受けます。そしてもう一つの非常に現実的な制約がコストです。これらの要因に基づくなら、リスク見積もり段階で得られたリスクレベルに見合った範囲に関係する保護手段を何らかの方法で備える必要があることは明白です。

どのタイプの保護装置を選択する場合でも、「安全関連システム」には、保護装置や配線、電源切換え装置、および場合によっては機械の運転管理システムの一部を含む、多くの要素が含まれていることを忘れてはなりません。システムのこれらのすべての要素(ガード、土台、配線などを含む)は、それらの設計原則やテクノロジに関連性のある適切な性能特性を持つ必要があります。IEC/EN 62061および(EN) ISO 13849-1は、制御システムの安全関連部分の性能階層レベルを分類し、付属書でリスクアセスメント方法を規定して保護システムの整合性要件を決定しています。

(EN) ISO 13849-1:2015では、付属書Aに拡張されたリスクグラフが記載されています。



安全機能ごとに判定が必要です!

IEC 62061でも、以下に示す形式で付属書Aに方法が記載されています。

リスクアセスメントおよび安全対策

文書番号:
パート:

☐ プレ・リスク・アセスメント
☐ 中間リスクアセスメント
☐ フォローアップ・リスク・アセスメント

製品:
発行者:
日付:

黒い領域 = 要求される安全対策
灰色の領域 = 推奨される安全対策

影響(Consequence)	重大度 Se	クラス Cl					頻度および継続期間 (Fr)		危険事象の発生確率(Pr)		回避 (Av)	
		3–4	5–7	8–10	11–13	14–15						
死亡、眼球または腕の喪失		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1時間	5	共通	5		
永久的、手指の喪失			OM	SIL 1	SIL 2	SIL 3	> 1時間 – <=日	5	可能性が高い	4		
可逆的、医療				OM	SIL 1	SIL 2	>1日 – <= 2週	4	可能	3	不可能	5
可逆的、救急処置					OM	SIL 1	> 2週 – <= 1年	3	まれ	2	可能	3
							> 1年	2	無視できる	1	可能性が高い	1

シリアル番号	危険番号	危険源	Se	Fr	Pr	Av	Ci	安全対策	安全

コメント

上記のどちらの方法を使用しても、同等の結果が得られなければなりません。それぞれの方法は、それが含まれている規格の詳細な内容を説明することを目的としています。

どちらの場合でも、その規格の中で示されている指針を使用することが極めて重要です。これらのリスクグラフや表は、対応する規格と切り離して、または過度に単純化して使用してはなりません。

評価

保護手段を選択した後にそれを実装する前に、リスク見積もりを繰返し実行する必要があります。これは見過ごされてしまうことが多い手順です。保護手段を設置すると、オペレータは元の想定されたリスクから完全に保護されていると感じてしまう可能性があります。

元の危機意識がなくなっているため、オペレータは違う方法で機械に介入しようとする場合があります。以前より頻繁に危険にさらされる可能性や、もっと先まで機械に立ち入ろうとする場合があります。つまり、保護手段が故障した場合、以前に想定されたより大きなリスクに直面することになります。これはあらかじめ考えておく必要がある実際のリスクです。したがってリスク見積もりでは、作業員が機械に介入する方法の予測可能な変化を折に触れて繰返し考慮する必要があります。この活動の結果は、提案された保護手段が実際に適切であるかどうかをチェックするために使用されます。詳細は、IEC/EN 62061の付属書Aを参照してください。

トレーニング、個人用保護具など

オペレータは機械の安全な作業方法に関する必要なトレーニングを受けることが重要です。これはその他の手段を省略しても良いことを意味しません。単に危険領域の近くに行ってはならないとオペレータに命令することは許されません(ガードするかわりに)。

また、オペレータは専用手袋、ゴーグル、保護マスクなどの器具を使用することも必要です。機械設計者はどのような種類の保護具が必要であるかを指定する必要があります。通常、個人用保護具の使用は主要な安全防護方法にはなりませんが、上記の手段を補足することはできます。また、一般的に残存リスクに対する認識を高めるための標識やマーキングの必要もあります。

第4章: 保護手段の導入

リスクアセスメントによって機械またはプロセスに傷害のリスクがあることが示された場合、危険をなくす、または抑制する必要があります。これを達成する方法は、機械および危険の性質に依存します。防護装置と併用される安全制御システム保護手段は、危険へのアクセスを防止するか、または危険源へのアクセスが可能な場合は危険な動きを防止します。安全制御システム保護手段の代表的な例については後述します(インターロック付きガード、ライトカーテン、セーフティマット、両手用制御、およびイネーブルスイッチを含む)。

非常停止装置およびシステムは、安全関連制御システムと関係がありますが、これらは直接的な保護システムではなく、補助的保護手段と見なされます。

固定式包囲ガードによるアクセス防止

危険源がアクセスする必要のない機械の部分である場合は、ガードを機械から取り外せないように固定します。これらのタイプのガードを取り外すには工具が必要です。固定式ガードには以下のことが要求されます。
1) 動作環境に耐えること。
2) 必要に応じて危険物の飛散を防止できること。
3) 鋭い先端などの危険源を形成しないこと。
固定式ガードは、金網タイプの囲いを使用するため、ガードが機械または開口部に合わさる部分に開口部が設けられる場合があります。

ウィンドウは、機械のパフォーマンスをモニタするために便利な方法を提供します。切削液との化学的相互作用や紫外線、単純な経年劣化等の原因によりウィンドウの材料が時間経過と共に劣化する可能性があるため、使用する材料には注意する必要があります。

開口部の大きさは、危険源にオペレータが達することを防止する必要があります。
U.S. OHSA 1910.217 (f) (4)の表O-10、ISO 13854、ANSI B11.19の表D-1、CSA Z432の表3、およびAS4024.1は、特定の開口部を危険源から離す必要がある適切な距離を規定しています。

接近の検出

危険源へのアクセスを検出するために保護手段を使用できます。リスク低減の方法として検出が選択された場合、設計者は完全な安全システムを使用する必要があること、安全保護装置はそれ自体では必要なリスク低減もたらさないことを理解している必要があります。この安全システムは、一般的に次の3つのブロックから構成されます。
1) 危険源へのアクセスを検知する入力デバイス、
2) 検知装置からの信号を処理し、安全システムのステータスをチェックし、出力デバイスのオンとオフを切換えるロジックデバイス、
3) アクチュエータを制御する出力デバイス(例えばモータ)。

検出デバイス

人員が危険領域に入ったり、危険領域内にいる人員の存在を検出する検出デバイスには多くの代替装置が使用できます。特定のアプリケーションに対する最適な選択は、次のような数多くの要因に依存します。

- 検出器の信頼性に影響を及ぼす環境要因
- アクセス頻度
- 危険の停止時間
- 機械サイクル完了の重要性
- 投射物体、液体、霧、気化ガスなど

適切に選択された可動式ガードは、投射物体、液体、霧、およびその他の危険からの保護を提供するためにインターロックを形成でき、危険源へのアクセス頻度が低い場合にしばしば使用されます。また、機械が完全に停止状態に達する時間まで、または望ましくないサイクルの途中で機械を停止する場合に、インターロック付きガードもロックされてアクセスを防止できます。

ライトカーテン、マット、レーザスキャナなどの存在検知装置は、危険領域への迅速かつ容易なアクセスを提供し、オペレータが危険領域に頻繁にアクセスする必要がある場合にしばしば選択されます。これらのタイプのデバイスは、投射物体、霧、液体、またはその他のタイプの危険源に対する保護を提供しません。

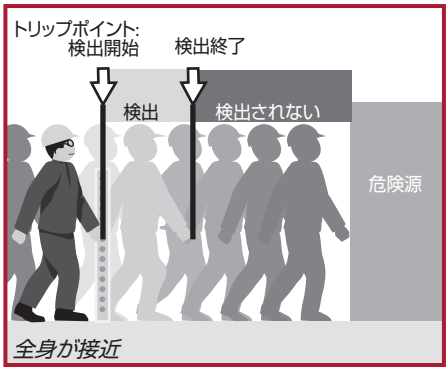
保護手段の最適な選択は、最大限の保護を通常の機械動作の妨げを最小限にして提供できるデバイスまたはシステムです。経験が示すように使用が困難なシステムは取り外されたり回避されたりしやすくなるため、機械使用のあらゆる側面を考慮する必要があります。

存在検知装置

IEC 62046は、存在検知装置の適用に関する有用な指針を提供します。この規格は、存在検知装置の使用を推奨しています。区域または領域を保護する方法を決定する場合、正確にどの安全機能が必要であるかを明確に理解していることが重要です。一般的に、少なくとも2つの機能が使用されます。

- 危険領域に人が入ったら、電源のスイッチを切る、または無効にする機能
- 危険領域に人がいる間は、電源のスイッチを入れたり、有効にできないようにする機能

一見すると、これらは同じ1つのものであるように思われるかもしれませんが(明らかに相互に関連し、しばしば同一の機器によって実現されることも事実ですが)、実際には両者は2つの別個の安全機能です。第一の機能を実現するには、ある種のトリップ装置を使用する必要があります。言い換えると、人体の一部があるポイントを越えたことを検出し、電源を切るための信号を送信するデバイスが必要になります。さらに、人がトリップポイントを過ぎてもそのまま進むことができ、その存在がもはや検出されなくなった場合、第二の機能(電源のスイッチが入るのを回避する)は実現できないかもしれません。



上図に、全身が接近する場合のこのような特性を持つ装置の例としてトリップ装置として垂直に取付けられたライトカーテンの例を示します。インターロック付き防護ドアも、検出領域に入った後にドアが閉じることを回避する手段がないため、通常はトリップするだけの装置と見なされます。

全身が接近する可能性がないため、人がトリップポイントを越えて進むことができない場合は、その存在は常に検出されており、第二の機能(電源のスイッチが入るのを回避する)は実現されています。体の一部が接近するタイプのアプリケーションでは、同じタイプのデバイスがトリップ機能と存在検知機能を実行します。唯一の違いはその使用形態です。

存在検知装置は、人の存在を検出するために使用されます。このタイプの装置としては、セーフティ・ライト・カーテン、シングル・ビーム・セーフティ・バリア、セーフティ・レーザ・スキャナおよびセーフティマットなどがあります。すべての存在検知装置において、検出ゾーンのサイズとデバイスの位置は、必要な安全距離を考慮に入れる必要があります。

セーフティ・ライト・カーテン

セーフティ・ライト・カーテンは、簡単に言えば光電センサであり、危険な機械動作から作業員を守るために特別に設計されています。ライトカーテンは、AOPD (能動的光電保護装置)またはESPE (電気的検知保護設備)とも呼ばれ、最適な安全を保証すると同時に、生産性の向上にも貢献します。ライトカーテンは、作業員が頻繁に、かつ容易に作業上危険な箇所にアクセスしなければならない場合に最適です。

ライトカーテンは、IEC 61496-1およびIEC 61496-2に適合するように設計され、テストされています。

セーフティ・レーザ・スキャナ

セーフティ・レーザ・スキャナは回転する鏡を使用し、光パルスを鏡の曲面で屈折させて検知面を作り出します。対象物の位置は、鏡の回転角によって特定されます。レーザスキャナは、不可視光線の反射ビームによる「タイム・オブ・フライト(飛行時間)」技術を使用し、スキャナと対象物までの距離を測定することもできます。測定された距離と対象物の位置を使用して、レーザスキャナは対象物の正確な位置を特定します。

感圧式セーフティマット

機械周辺のフロアをガードするために使用されます。格子状に相互接続されたマットが危険領域の周囲に配置され、マットに圧力がかかる(オペレータが足で踏むなど)と、マット・コントローラ・ユニットが危険源への電源をオフにします。感圧式マットは、複数の機械やフレキシブルな製造システム、ロボットセルなどが設置された閉鎖領域でよく使用されます。セルへのアクセスが必要な場合(例えば、ロボットの設定や「ティーチ」のため)に、オペレータが安全領域からからそれるか、装置の一部の背後に回らなければならないときに、感圧式マットが危険な動きを防止します。マットを正しくしっかりと固定することにより、マットが動かないようすることが重要です。

感圧式エッジ

身体がぶつかったりはさまれたり、切断のおそれがある工作台や電動ドアなどの可動部品の端に取付ける縁が柔軟な帯状のデバイスです。

可動部品がオペレータに接触すると(またはその逆の場合も)、柔軟な感圧式エッジが押し下げられ、危険源の電源をオフにするコマンドが起動されます。感圧式エッジは、オペレータが巻き込まれるおそれがある機械をガードするためにも使用できます。オペレータが機械に巻き込まれると、感圧式エッジの接点が機械の電源を切断します。

ライトカーテン、スキャナ、フロアマット、および感圧式エッジは、「トリップ装置」にも分類されています。これらのデバイスは実際にアクセスを阻止するのではなく、それを「感知」するだけであり、安全を提供するために感知とスイッチの2つの機能に全面的に頼っています。一般的に、これらのデバイスを適用できるのは、電源のスイッチを切るとすぐに停止する機械だけです。オペレータは、危険領域内に直接踏み込んだり触れたりできるため、動きが停止するのにかかる時間が、デバイスがトリップしてからオペレータが危険源に到達するのに要する時間よりも短くなければならないことは明らかです。

セーフティスイッチ

機械にアクセスする頻度が低い場合や、部品が飛び出す可能性がある場合は、可動式(開閉可能な)保護ガードが適しています。このガードは、防護ドアが閉じられていないときは必ず危険源の電源のスイッチが確実に切られているように危険源の電源とインターロックされています。

このアプローチでは、防護ドアに取付けられたインターロックスイッチが使用されます。危険源の電源の制御は、ユニットのスイッチ部分を使用して行なわれます。この電源には通常、電気が使用されますが、空気圧や油圧が使用される場合もあります。防護ドアの動き(開く)が検出されると、インターロックスイッチが危険源の電源を遮断するコマンドを直接的にまたは電源コンタクタ(またはバルブ)を介して起動します。

インターロックスイッチの中には、防護ドアを閉じた状態でロックして機械が安全状態になるまで解除しないロック装置が組み込まれているものもあります。

大多数のアプリケーションでは、可動式ガードとガードロック機能ありまたはなしのインターロックスイッチの組合わせが最も信頼性が高く、コスト効率の良いソリューションとなります。(EN) ISO 14119では、あらゆるタイプのガード機能付きインターロック装置に関する役に立つ指針が提供されています。この規格は、存在検知装置の使用を推奨しています。

以下を含めて、幅広いセーフティスイッチのオプションがあります。

- **タング式インターロックスイッチ** - これらのデバイスには、スイッチに挿入されたり、引き抜かれたりするタング型アクチュエータが必要です。
- **ヒンジ型インターロックスイッチ** - これらのデバイスは、防護ドアのヒンジピンに設置され、ガードが開くことで起動します。
- **ガードロック機能付きスイッチ** - アプリケーションによっては、ガードを閉じた状態でロックしたり、ガードが開くのを遅らせたりすることが必要となる場合があります。この要件に適したデバイスは、ガードロック機能付きインターロックスイッチと呼ばれ、ランダウン(じょじょに停止する)特性を持つ機械に適していますが、ほとんどのタイプの機械でも保護レベルを大幅に向上させることができます。
- **非接触型インターロックスイッチ** - これらのデバイスの動作には物理的な接点は必要ありません。一部のバージョンではコーディング機能が組み込まれ、不正操作に対する耐性が向上しています。
- **位置(リミットスイッチ)インターロック** - カム作動式は通常、ポジティブ・モード・リミット(または位置)スイッチと、リニアカムまたはロータリカムで構成され、一般的にスライド式ガードで使用されます。
- **トラップ・キー・インターロック** - トラップ・キーは、電源インターロックだけでなく制御インターロックも実行できます。「制御インターロック」を実行すると、インターロック装置は中間装置に対して停止コマンドを指令し、それによって後続の装置がオフになり、アクチュエータからエネルギーを切り離します。「電源インターロック」を実行すると、停止コマンドは機械のアクチュエータへのエネルギー供給を直ちに遮断します。

オペレータインターフェイス装置

停止機能 - 米国、カナダ、欧州、および国際的なレベルで、機械または製造システム向けの停止カテゴリの説明に関して規格の整合化が行なわれています。

注: これらのカテゴリは、ISO 13849-1のカテゴリとは異なります。詳細は、NFPA79およびIEC/EN 60204-1規格を参照してください。停止は次の3つのカテゴリに分類されます。

カテゴリ0では、機械のアクチュエータへの電力を直ちに取り除くことにより停止を実現します。これは非制御停止と見なされます。電源を遮断すると、電源を必要とするブレーキング作用が無効になります。これにより、モータは空回りするようになり、自然に停止するまで長時間かかります。その他のケースとして、材料を保持するために電力を必要とする機械の保持固定具の場合は材料が落下する可能性があります。電力を必要としない機械的な停止手段(ブレーキ)も、カテゴリ0の停止と合わせて使用されることもあります。カテゴリ0の停止は、カテゴリ1またはカテゴリ2の停止より優先されます。

カテゴリ1は、停止を実現する機械のアクチュエータに電源を使用できる制御停止です。機械が停止した時点で、アクチュエータから電力が取り除かれます。このカテゴリの停止では、電動ブレーキを使用して危険な動きを迅速に止めることができ、その後でアクチュエータから電力を取り除くことができます。このタイプの停止は、より高速で制御された停止を実現することができ、停止状態からの再起動も短時間で可能になります。
注: IEC/EN 60204-1の2016年版ではカテゴリ1の停止のタイプが拡張されます。

カテゴリ2は、機械のアクチュエータで電源を使用可能にした状態で実行される制御停止です。通常の生産で使用される停止はカテゴリ2の停止と見なされます。

これらの停止カテゴリは停止機能ごとに適用する必要があります。各停止機能は、制御システムの安全関連部分が入力に応答して行なわれる動作であり、カテゴリ0または1を使用する必要があります。停止機能は、関連する始動機能をオーバライドする必要があります。各停止機能での停止カテゴリの選択は、リスクアセスメントによって決定する必要があります。

非常停止機能

非常停止機能は、リスクアセスメントによる決定に従ってカテゴリ0またはカテゴリ1のいずれかの停止として動作する必要があります。非常停止機能は、人の1つの動作で起動しなければなりません。非常停止機能が起動されたら、他のすべての機能および機械の動作モードをオーバライドする必要があります。その目的は、さらに他の危険を引き起こすことなく、できるだけ速やかに電力を取り除くことです。オペレータが機械でトラブルに巻き込まれる危険が存在するあらゆる場所に、非常停止装置に素早くアクセスできる設備を配置する必要があります。非常停止装置は、連続して操作可能でいつでも使用可能であることが必要です。オペレータパネルには少なくとも1つの非常停止装置が装備されていなければなりません。必要に応じて、別の場所に追加の非常停止装置を使用することもできます。非常停止装置にはさまざまな形態があります。押しボタンおよびロープ式スイッチが最も一般的なタイプのデバイスです。

最近まで、非常停止回路にはハード配線された電気機械式コンポーネントを使用する必要がありました。IEC 60204-1やNFPA 79などの規格の最近の変更によって、IEC61508などの規格の要件に適合するセーフティPLCやその他の形態の電子ロジックが非常停止回路に使用できるようになりました。

非常停止装置は、補足的な安全保護装置と考えられます。これらの装置は、危険源へのアクセス防止も危険源へのアクセスの検出も実行しないため、主要な安全保護装置とは見なされません。これらは人の操作に依存しています。

非常停止装置については、ISO/EN13850、IEC 60947-5-5、NFPA79、およびIEC60204-1、AS4024.1、Z432-94を参照してください。

非常停止押しボタン

押しボタンが非常停止装置として使用される場合は、台が黄色で赤色のマッシュルーム型押しボタンを使用する必要があります。非常停止装置は、作動された時点でラッチしなければならず、ラッチできなかった場合は停止コマンドを生成できないようにする必要があります。非常停止装置のリセットによって危険な状態を引き起こすことは許されません。機械を再起動するには、別の意図的な処置を使用する必要があります。

非常停止採用されている最新の技術の1つに自己モニタ技術があります。非常停止装置の背面に接点が追加され、パネル構成部品の背面がまだ存在しているかどうかをモニタします。これは自己モニタ用接点ブロックと呼ばれます。この技術は、接点ブロックがパネルの所定の位置にはめ込まれると接点が閉じるように設計されたスプリング駆動式接点で構成されます。

ロープ式スイッチ

コンベアなどの機械の場合、非常停止装置として危険領域に沿ってロープ式の装置を設置すると便利で効果的である場合が少なくありません。これらの装置では、プルスイッチをラッチするために鋼線ロープを使用しているため、その全長でどの位置からでも、どの方向にでもロープを引っ張るとスイッチがトリップし、機械の電源を遮断できます。

ロープ式スイッチは、ロープが引っ張られたときと、たるんだときの両方を検知する必要があります。たるみの検知により、ロープが切断されずにいつでも使用できる状態であることをモニタします。

このスイッチの性能は、ロープの距離に影響されます。距離が短い場合は、セーフティスイッチをロープの一方の端に取付け、反対側の端にはテンションスプリングを取付けます。距離が長い場合は、オペレータの1つの動作で停止コマンドが確実に起動するように、セーフティスイッチをロープの両端に取付ける必要があります。ロープの支持とガイドのために、適切な位置にアイボルトを使用することが不可欠です。ロープの引くために必要な力は200N (45ポンド)を超えないこと、または2つのアイボルト間の中央の位置で400mm (15.75インチ)を超えないようにしてください。適切な動作性能を実現するためには製造メーカの取扱説明書に従うことが重要です。

両手用制御

両手用制御(バイマニュアル制御とも呼ばれる)の使用は、機械が危険な状態のときに機械に接近することを防ぐ一般的な方法です。機械を始動するには、2つのスイッチを同時に(相互に0.5秒以内に)操作する必要があります。これにより、オペレータの両手が安全な位置(すなわち制御ユニット)に置かれているため、危険な領域にはないことを確認できます。制御は、危険な状況にあっても動作を継続する必要があります。機械の動作は、制御ユニットのいずれか一方を開放すると停止し、一方を開放した場合は、機械を再起動できるようになるにはもう一方の制御ユニットも開放する必要があります。このことは「アンチ·タイ·ダウン」を実現し、両手用制御を片手用制御に不正に変更することを防止します。

両手用制御システムは、障害を検出する制御およびモニタシステムの整合性に大きく依存するため、この側面を適切な仕様に従って設計することが重要です。両手用安全制御システムの性能は、ISO 13851 (EN 574)によるタイプに分類され、ISO 13849-1のカテゴリに関連付けられています。機械安全で最も一般的に使用されているタイプはIIIBおよびIIICです。以下の表に、これらのタイプと安全性能のカテゴリとの関係を示します。

要件	タイプ				
	I	II	III		
			A	B	C
同期作動			X	X	X
カテゴリ1の使用(ISO 13849-1)	X		X		
カテゴリ3の使用(ISO 13849-1)		X		X	
カテゴリ4の使用(ISO 13849-1)					X

ISO 13851の要件の表

物理的な設計では、不適切な操作(例えば、手と肘を使うなど)を回避する必要があります。これは距離をとるかまたはシールドすることで可能です。両方のボタンを開放してから、再度押さない限り、機械が1つのサイクルからもう1つのサイクルに移行することはできません。これにより「アンチリピート」を実現し、両方のボタンをブロックする可能性を回避し、機械を連続して動作することを防ぎます。いずれか一方のボタンを開放すると、必然的に機械の停止を引き起こします。

両手用制御機器を使用すると、通常、一部対応しきれない危険が残る場合が多いので、十分な検討が必要です。両手用制御は、それを使用する人のみを保護します。両手用制御で保護されているオペレータは、他の作業員が保護されていない可能性があるため、危険源へのあらゆるアクセスを監視できなければなりません。

ISO 13851 (EN574)は、両手用制御に関する追加の指針を提供しています。

イネーブルスイッチ

イネーブルスイッチは、危険源のモータが安全速度で動作中で、かつオペレータがイネーブルスイッチを動作位置に保持している場合のみ、オペレータが危険領域に立ち入ることを許可する許容ストラテジの一部として使用される場合があります。イネーブルスイッチには、2点式スイッチまたは3点式スイッチを使用します。2点式スイッチは、アクチュエータが動作していないときはオフになり、アクチュエータが動作しているときはオンになります。3点式スイッチは、アクチュエータが動作していないときはオフになり(1の位置)、中央の位置にあるときはオンになり(2の位置)、アクチュエータが中央を越える位置に動かされるとオフになります(3の位置)。さらに、3の位置から1の位置に戻すときは、2の位置を通過するときは出力回路は閉じてはなりません。

イネーブルスイッチは、他の安全関連機能と組み合わせて使用する必要があります。代表的な使用例としては、制御された安全低速モードの動きで使用されます。イネーブルスイッチを使用する場合は、イネーブルスイッチがアクティブであることを信号によって示す必要があります。

ロジックデバイス

ロジックデバイスは、制御システムの安全関連部分の中心的な役割を果たします。ロジックデバイスは安全システムのチェックとモニタを実行し、機械を始動を許可したり、機械を停止するコマンドを実行することができます。

機械に要求される複雑さや機能に対応する安全アーキテクチャを作成できるように、幅広いロジックデバイスがそろっています。小型のハード配線されたモニタ·セーフティ·リレーは、安全機能の実行に専用のロジックデバイスを必要とする小型機械にとって最も経済的です。モジュール式の構成可能なモニタ·セーフティ·リレーは、多数かつ多様な安全保護装置と最小限のゾーン制御を必要とする環境に理想的です。中型から大型のより複雑な機械では、分散I/Oを使用したプログラム可能な安全システムを選択することをお奨めします。

モニタ·セーフティ·リレー(MSR)

モニタ·セーフティ·リレー(MSR)モジュールは多くの安全システムで重要な役割を果たします。これらのモジュールは通常、安全機能の実行を保証するための追加回路を備えた2つ以上の強制開離式リレーで構成されています。

強制開離式リレーは、通常閉接点と通常開接点が同時に閉じることがないように設計されています。一部のモニタ·セーフティ·リレーは、安全関連のソリッドステート出力を備えています。

モニタ·セーフティ·リレーは、安全システムで多くのチェックを実行します。電源投入と同時にリレー内部コンポーネントの自己チェックを実行します。入力デバイスが有効になると、MSRは冗長入力の結果を比較します。問題がなければ、MSRはその出力に接続されている外部アクチュエータをチェックします。これが正常な場合、MSRはリセット信号を待ってから、出力を有効にします。したがって、正しく選択され構成されたMSRは、接続された入力および出力デバイスをチェックすることによりシステム障害を検出できます。また、始動/再始動インターロックも提供できます。

適切なセーフティリレーは、モニタする装置のタイプ、リセットのタイプ、出力の数とタイプなど、多くの要因に基づいて選択します。

モニタ·セーフティ·リレー(MSR)への入力のタイプ

タイプの異なる安全保護装置は、モニタ·セーフティ·リレーに異なるタイプの入力を供給するため、互換性を確認することが重要です。考えられる入力タイプと要求されるクロスフォルト検出特性の概要を以下に示します。

電気機械式インターロック、一部の非接触型インターロックおよび非常停止: 1つの通常閉接点があるシングルチャネルまたは、2つの通常閉接点があるデュアルチャネルの機械的な接点。MSRは、シングルまたはデュアルチャネルに対応可能であることが必要で、デュアルチャネル構成でクロスフォルト検出を提供可能である必要があります。

一部の非接触型インターロックおよび非常停止: 1つの通常開接点と1つの通常閉接点があるデュアルチャネルの機械的な接点。MSRは多様な入力を処理可能である必要があります。

ソリッドステート出力を備えたデバイス: ライトカーテン、レーザスキャナ、および一部の非接触型ガードインターロックには、2つのソース出力があり、自動的にクロスフォルト検出を実行します。MSRは、デバイスのクロスフォルト検出方法を無視できなければなりません。

感圧式マット: マットは2つのチャネル間で短絡を発生します。MSRは、このアプリケーション専用に設計されているか、または設定できなければなりません。

感圧式エッジ: エッジには、4線式マットと同じように設計されているものがあります。また、抵抗の変化を発生する2線式デバイスのものもあります。MSRは、短絡または抵抗の変化を検出できなければなりません。

モータ動作検知: 停止中のモータのバックEMFを測定します。MSRは、高電圧に耐えられるだけではなく、モータのスピンダウンに伴う電圧低下を検出できなければなりません。

停止動作: MSRは多様な冗長センサからのパルスストリームを検出する必要があります。

両手用制御: MSRは、通常開および通常閉のさまざまな入力を検出するとともに、0.5秒を計時して、ロジックを処理できなければなりません。

モニタ・セーフティ・リレーは、これらの異なる電気特性をもつ各タイプのデバイスに接続するために特別に設計されているか、または構成可能でなければなりません。異なるタイプのデバイスに対して完全に構成可能なMSRもあります。また、MSRによっては数種類の入力に接続できても、いったんデバイスを選択すると、そのMSRはそのデバイス以外には接続できないものもあります。システム設計者は、入力デバイスと互換性のあるMSRを選択するか、または入力デバイスに合わせて構成する必要があります。

入力インピーダンス

モニタ・セーフティ・リレーの入力インピーダンスによって、リレーに接続できる入力デバイスの数と入力デバイスを設置できる距離が決まります。例えば、セーフティリレーの許容可能な最大入力インピーダンスが500Ωであるとします。入力インピーダンスが500Ωを超えた場合は、その出力はオンになりません。ユーザは、入力インピーダンスが最大仕様未満に収まっているように注意する必要があります。使用するワイヤの長さ、サイズ、およびタイプが入力インピーダンスに影響します。

入力デバイスの数

モニタ・セーフティ・リレー(MSR)のユニットに接続する入力デバイスの数と入力デバイスをチェックする頻度を決定するために、リスクアセスメントが実施されます。非常停止とゲートインターロックを常に操作可能な状態に保つには、リスクアセスメントで決められた間隔で定期的に動作をチェックする必要があります。例えば、マシンサイクルごと(1日当たり数回など)に開く必要があるインターロック式ゲートに接続されたデュアルチャネル入力MSRは、チェックする必要がありません。これは、ガードを開くとMSRが自己チェックを行ない、入力および出力(構成により異なる)に単一のフォルトがないか確認するためです。ガードが開く頻度が高くなれば、チェック処理の整合性が高くなります。

もう一つの例は、非常停止です。通常、非常停止は緊急時にのみ使用されるため、この機能が使用されることはめったにありません。したがって、定期的に非常停止を実行して、効果を確認するプログラムを確立する必要があります。このように安全システムを作動させることは、機能テストと呼ばれます。第3の例は機械調整用のアクセスドアですが、これも非常停止と同じで、めったに使用されることはありません。ここでもまた、定期的に機能をチェックするためのプログラムを確立する必要があります。

リスクアセスメントは、入力デバイスをチェックする必要があるかどうか、どのくらいの頻度でチェックすればよいかを決定するために役立ちます。リスクのレベルが高ければ高いほど、チェック処理に求められる整合性が高くなります。また、「自動」チェックの頻度が低くなれば、その分だけ頻繁に「手動」チェックを実施する必要があります。

入力クロスフォルト検出

デュアル·チャネル·システムでは、入力デバイスのチャネル間の短絡フォルト(「クロスフォルト」とも呼ばれる)を安全システムによって検出する必要があります。これは、検知装置すなわちモニタ·セーフティ·リレーによって遂行されます。

ライトカーテン、レーザスキャナ、および高度な非接触型センサなどのモニタ·セーフティ·リレーをベースにしたマイクロプロセッサは、これらの短絡をさまざまな方法で検出します。クロスフォルトを検出する一般的な方法の1つは、パルステストを使用することです。MSRへの信号入力は、非常に高速なパルスによって行ないます。チャネル1のパルスは、チャネル2のパルスからオフセットされています。短絡が発生すると、これらのパルスが同時に発生し、このデバイスによって検出されます。

電気機械式のモニタ·セーフティ·リレーでは異なるダイバーシティ技術が用いられています。その1つがプルアップ入力であり、もう1つがプルダウン入力です。チャネル1からチャネル2との間の短絡は、過電流保護装置をアクティブにし、安全システムをシャットダウンします。

出力

MSRの出力の数は決まっていません。出力のタイプで、特定のアプリケーションで使用するMSRを選択することができます。

ほとんどのMSRには、直ちに動作する安全出力が少なくとも2つあります。MSRの安全出力は、通常開の特性を持っています。これらの出力は冗長性と内部チェック機能を持つため、安全と定格されています。2番目のタイプの出力は、遅延出力です。遅延オフ出力は、通常、カテゴリ1の停止で使用されます。カテゴリ1の停止では、危険領域へのアクセスを許可する前に、機械が停止機能を実行するために時間がかかります。また、MSRには補助出力もあります。一般的に、補助出力は通常閉と見なされます。

出力定格

出力定格は、安全保護装置が負荷を切換える能力を表します。一般的に、産業用装置の定格は抵抗負荷または電磁負荷で表されます。抵抗負荷は、ヒータタイプの素子である場合があります。電磁負荷は、一般的にリレー、コンタクタ、またはソレノイドであり、負荷の誘導特性が大きくなります。IEC 60947-5-1の付属書Aに負荷の定格が記載されています。

表示記号: この記号は、A300などのように数字の前に付けられるアルファベット文字です。この記号は従来の密閉型熱電流を示し、その電流が直流(DC)か交流(AC)かを示します。例えば、Aは10A交流電流(AC)を示します。数字は、定格絶縁電圧を表します。例えば、300は300Vを表します。

用途:「用途」とは、そのデバイスが切換えるように設計されている負荷のタイプを示します。IEC 60947-5に関連する用途を、以下の表に示します。

用途	負荷の説明
AC-12	オプトカプラで絶縁された抵抗負荷およびソリッドステート負荷の制御
AC-13	トランス絶縁によるソリッドステート負荷の制御
AC-14	小容量の電磁負荷(72VA未満)の制御
AC-15	72VAを超える電磁負荷の制御
DC-12	オプトカプラで絶縁された抵抗負荷およびソリッドステート負荷の制御
DC-13	電磁の制御
DC-14	回路にエコノミレジスタがある電磁負荷の制御

熱電流(Ith): 従来の密閉型熱電流は、指定したエンクロージャに設置された機器の温度上昇試験に使用される電流値です。

定格動作電圧(Ue)および定格動作電流(Ie): 定格動作電流および電圧は、通常の動作条件におけるスイッチング素子のメイクおよびブレークの容量を指定します。一般的にAllen-BradleyのGuardmaster製品の定格は、AC125V、AC250V、およびDC24Vです。

VA: VA (電圧 x 電流値)定格は、回路をメイクするときと、回路をブレークするときのスイッチング素子の定格を示します。

例1: A150、AC-15という定格は、接点が7200VAの回路をメイクできることを示します。AC120Vでは、接点は60Aの突入回路をメイクできます。AC-15が電磁負荷であるため、60Aは短期間(電磁負荷の突入電流)のみに限られます。電磁負荷の定常電流は定格動作電流である6Aであるため、回路のブレークは720VAだけです。

例2: N150、DC-13という定格は、接点が275VAの回路をメイクできることを示します。AC125Vでは、接点は2.2Aの回路をメイクできます。DC電磁負荷では、AC電磁負荷のような突入電流は発生しません。電磁負荷の定常電流が定格動作電流である2.2Aであるため、回路のブレークも275VAになります。

機械の再起動

例えば、稼働中の機械でインターロック付きガードが開いた場合、セーフティ・インターロック・スイッチがこの機械を停止します。ほとんどの状況では、ガードが閉じたときに機械がすぐに再起動しないことが必須です。これを実現する一般的な方法は、ラッチ機能付きのコンタクタの始動処理を使用することです。

始動ボタンを押してから離すと、電源接点を閉じているコンタクタの制御コイルがすぐに出力状態になります。電源接点に電力が流れている間は、電源接点に機械的にリンクされたコンタクタの補助接点によって、制御コイルは出力状態(電気的にラッチされた状態)に保たれます。主電源または制御電源が遮断されると、コイルがオフ状態になり、主電源と補助接点が開きます。ガードインターロックは、コンタクタ制御回路に配線されています。つまり、ガードを閉じてから通常の始動ボタンを「オン」することによってのみ再起動できます。この操作によってコンタクタがリセットされ、機械が起動します。

通常のインターロック状況における要件は、ISO 12100に明記されています(抜粋)。

「ガードが閉じているときに、ガードによって保護されている機械の危険な機能は動作可能であるが、ガードを閉じる行為そのもので機械の動作が開始されることはない。」

多くの機械には、上記のように動作する1つまたは2つのコンタクタ(または同等の結果を実現するシステム)が既に搭載されています。既存の機械にインターロックを取付ける場合は、電源制御の配置がこの要件に適合していることを確認し、必要に応じて追加措置を講じる必要があります。

リセット機能

Allen BradleyのGuardmasterモニタ・セーフティ・リレーは、モニタ付き手動リセットまたは自動/手動リセットのいずれかと併用するように設計されています。

モニタ付き手動リセット

モニタ付き手動リセットは、ゲートが閉じた後、または非常停止がリセットされた後にリセット回路の状態を変更する必要があります。機械的にリンクされた電源切換えコンタクタの通常閉の補助接点は、モメンタリ式押しボタンと直列に接続されています。ガードが開いてから再び閉じた後、セーフティリレーはリセットボタンを押してから離すまで、機械を再起動できないようにします。これは、(EN) ISO 13849-1に規定された追加の手動リセット要件の意図に従うものであり、リセット機能は両方のコンタクタがオフになっていて、かつ両方のインターロック回路(そして、それに伴ってガード)が閉じており、また(状態の変化が必要であるため)、リセットアクチュエータがどのような形でもバイパスされないか、またはブロックされないことを保証します。これらのチェックに合格して初めて、機械は通常の制御から再起動できます。
(EN) ISO 13849-1では、オン状態からオフするには状態の変化(「立下がりエッジ」)を必要とすることが言及されています。

リセットスイッチは、危険な状態をすぐに発見できる場所に設置し、オペレータが操作前にその領域に障害がないことをチェックできるようにする必要があります。

自動/手動リセット

一部のセーフティリレーには自動/手動リセットを備えているものもあります。手動リセットモードではモニタは行なわれず、ボタンを押したときにリセットが実行されます。リセットスイッチが短絡やジャムしていても検出されません。このモードでは、追加の手段を使用しない限り、(EN) ISO 13849-1で規定された要件を満たすことはできません。

そのかわり、リセットラインをジャンパして自動リセットを可能にすることもできます。その場合、ユーザはゲートが閉じたときに機械が起動しないようにするために、別の機構を取付ける必要があります。

自動リセット装置は手動によるスイッチ操作は必要ありませんが、動作を止めた後、システムをリセットする前に必ずシステム整合性チェックを実行します。自動リセットシステムについて、リセット機能が搭載されていないデバイスと混同しないように注意してください。後者では、安全システムは動作を止めた後、直ちに有効になり、システム整合性チェックは行なわれません。

リセットスイッチは、危険な状態をすぐに発見できる場所に設置し、オペレータが操作前にその領域に障害がないことをチェックできるようにする必要があります。

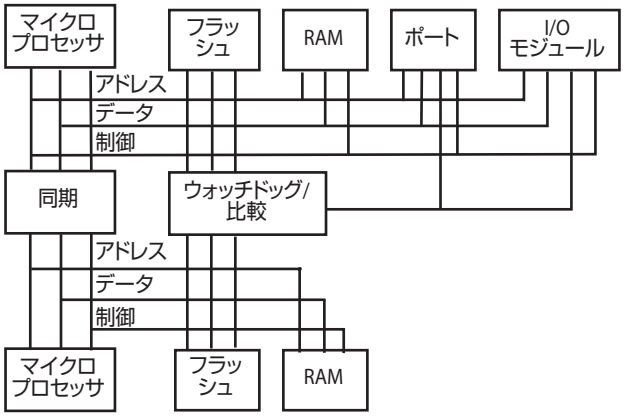
制御ガード

制御ガードは、ガードが開くと機械を停止し、ガードが閉じると直ちに機械を再び始動します。制御ガードの使用は、予期しない始動または停止不能は極めて危険な状況を発生するため、特定の厳格な条件下でのみ使用することが認められています。インターロック式システムは、可能な限り高いレベルの信頼性が必要です(通常はガードロックの使用を推奨する)。制御ガードの使用を検討できるのは、ガードが閉じているときにオペレータの身体またはその一部が危険領域内に留まったり、危険領域に近づいたりする可能性のない機械の場合だけです。制御ガードは、危険領域に接近できる唯一の経路となるようにする必要があります。

セーフティ・プログラマブル・ロジック・コントローラ

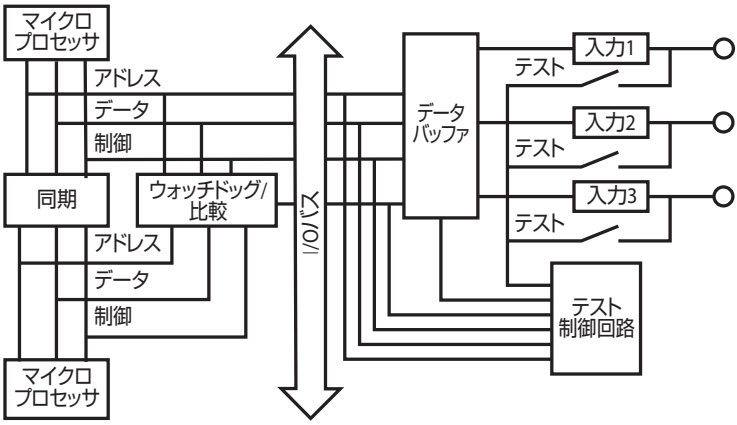
柔軟でスケーラブルな安全アプリケーションに対する要望が、セーフティPLC/コントローラの開発を後押ししています。プログラマブル・セーフティ・コントローラは、ユーザが使い慣れている標準のプログラマブルコントローラと同じくらい自由な制御を可能にします。ただし、標準PLCとセーフティPLCには大きな違いがあります。セーフティPLCには、より複雑な安全システムのスケーラビリティ、機能的および統合要件に対応するために多様なプラットフォームが用意されています。

I/O、メモリ、および安全通信を処理するために複数のマイクロプロセッサが使用されています。ウォッチドッグ回路が診断分析を実行します。2つのマイクロプロセッサのいずれか1つが安全機能を実行し、両方のマイクロプロセッサの確実に同期をとって動作するように拡張診断が実行されるため、このタイプの構造は1oo2Dと呼ばれています。



1oo2Dアーキテクチャ

また、各入力回路は1秒間に何回も内部的にテストされ、正しく動作していることが確認されます。非常停止ボタンを月に1回押すだけでも、内部回路は継続的にテストされています。



安全入力モジュールのブロックダイアグラム

セーフティPLC出力は、電気機械式または安全定格のソリッドステートです。入力回路と同様に、出力回路も1秒間に何回もテストされ、出力をオフにできることが確認されます。3つの回路の1つが故障した場合は、他の2つの回路によって出力がオフにされ、内部モニタ回路によってフォルトが報告されます。

機械的な接点を含む安全デバイス(非常停止、ゲートスイッチなど)を使用しているときは、ユーザはパルステスト信号を適用してクロスフォルトを検出できます。

ソフトウェア

セーフティPLCは標準PLCとほとんど同じようにプログラムできます。前述の追加された診断およびエラーチェック機能は、すべてオペレーティングシステムによって実行されるため、プログラマはそれが実際に行なわれていることを意識する必要はありません。ほとんどのセーフティPLCには、安全システム用のプログラムを作成するために使用される特殊な命令があり、これらの命令はセーフティリレーの機能に似ています。例えば、非常停止命令はMSRとほとんど同じように動作します。これらの命令の背後にあるロジックが複雑であっても、プログラマはこれらのブロックを相互に接続するだけで済むため、比較的簡単に安全プログラムを使用することができます。これらの命令は、他の論理、計算、データ操作などの命令と組み合わせると、その動作が適用される規格に確実に適合することが第三者機関によって保証されます。

ファンクションブロックは、安全機能をプログラミングするために広く使用されている方法です。ファンクションブロックやラダーロジックだけでなく、セーフティPLCでは認定された安全アプリケーション命令を使用できます。認定済みの安全命令によりアプリケーション固有の動作が可能になります。

認定済みのファンクションブロックは、ほとんどすべての安全デバイスと接続できます。この中に含まれないものとして、抵抗技術を使用するセーフティエッジがあります。

セーフティPLCは、変更の有無を追跡する機能を提供する「署名」を生成します。この署名は、通常、プログラム、I/O構成、およびタイムスタンプ を組み合わせて作成されます。プログラムが最終的に完成し妥当性が確認されると、ユーザは後で参照できるようにこの署名を妥当性確認の結果の一部として記録しておく必要があります。プログラムに変更が必要になった場合は、再度妥当性確認が必要となり、新しい署名を記録する必要があります。また、プログラムは不正な変更を防ぐためにパスワードを使用してロックすることができます。

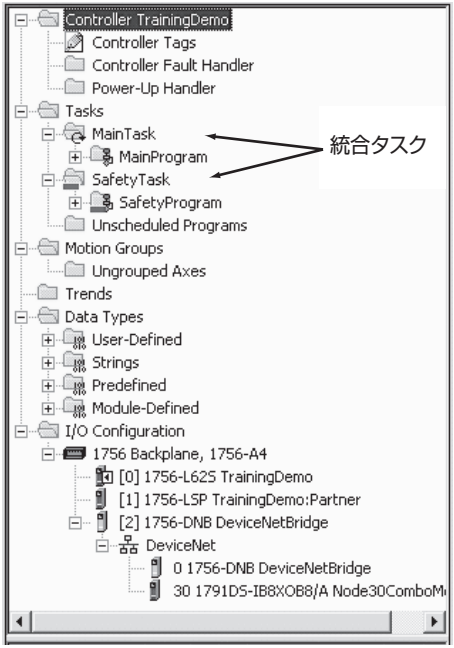
配線は、モニタ·セーフティ·リレーと比較するとプログラマブル·ロジック·システムによって単純化されています。モニタ·セーフティ·リレーが特定の端子に接続されるのとは異なり、入力デバイスは任意の安全入力端子に接続され、出力デバイスは任意の安全出力端子に接続されています。接続後に、各端子はソフトウェアによって割付けられます。

統合セーフティコントローラ

安全制御ソリューションは、安全および制御機能が組み込まれて連携して動作する単一の制御アーキテクチャ内に完全に統合されます。モーション、ドライブ、プロセス、バッチ、高速シーケンシャル、およびSIL 3安全を1台のコントローラで実行できることは、非常に大きな恩恵をもたらします。安全および標準制御の統合は、共通のツールとテクノロジを活用できる機会を提供し、これにより設計、設置、立上げ、メンテナンスに関連するコストを削減できます。共通の制御ハードウェア、分散安全I/OまたはデバイスをEtherNet/IP、ControlNetまたはDeviceNetで接続されたGuardLogixコントローラとの間でやり取りできます。安全タグデータは、外部デバイスやヒューマン·マシン·インターフェース(HMI)、パーソナルコンピュータ(PC)またはその他のコントローラを使用して直接読取ることができます。

以下の図に、制御と安全の統合の例を示します。安全関連ではない標準の制御機能は、メインタスクに組み込まれます。安全関連の機能は、安全タスクに組み込まれます。

標準機能と安全関連の機能は、すべて互いに分離されています。例えば、安全タグは標準ロジックで直接読取ることができます。安全タグは、



1. 標準タグおよびロジックは、ControlLogixと同様に動作します。
2. 標準タグデータ(プログラム用またはコントローラ用)、および外部デバイス、HMI、PC、その他のコントローラなど。
3. 統合コントローラであるGuardLogixは、安全タスク内で使用するために標準タグデータを安全タグに移動する(マップする)ことができます。これによって、ユーザはGuardLogixの標準側からステータス情報を読取ることができるようになります。このデータは、安全出力を直接制御するために使用してはなりません。
4. 安全タグは、標準ロジックで直接読取ることができます。
5. 安全タグは、安全ロジックで読み書きできます。
6. 安全タグは、EtherNet/IPを介してGuardLogixコントローラ間でやり取りできます。
7. 安全タグデータ(プログラム用またはコントローラ用)は、外部デバイス、HMI、PC、その他のコントローラなどで読取ることができます。このデータが安全タスク外でいったん利用されると、それは安全データではなく標準データとみなされることに注意してください。

安全ネットワーク

これまで、プラントフロアの通信ネットワークは、柔軟性を向上させ、診断機能を改善し、距離を伸ばし、設置および配線コストを削減し、保守性を高め、製造作業の全般的な生産性を向上させる能力を製造メーカに提供してきました。上記と同じ理由から、産業安全ネットワークの導入も進んでいます。これらの安全ネットワークにより、製造メーカは安全と標準I/O通信の両方に1本のネットワークケーブルを使用して安全I/Oや安全デバイスを機械の周辺に分散して配置することができるため、設置コストを削減するとともに診断機能を改善し、より複雑な安全システムを実現することができます。また、セーフティPLC/コントローラ間の安全な通信を実現し、複数のインテリジェントなシステムに安全制御を分散させることができるようになります。

安全ネットワークは、通信エラーを検出し、適切な障害応答機能を開始するように設計されています。検出される通信エラーには、メッセージ挿入、メッセージ損失、メッセージ破損、メッセージ遅延、メッセージ反復、および不正なメッセージシーケンスなどがあります。

ほとんどのアプリケーションではエラーが検出されると、デバイスは一般的に「安全状態」と呼ばれる既知の電源が絶たれた状態になります。安全入力または出力通信モジュールが、これらの通信エラーを検出し、必要に応じて安全状態に移行する役割を果たします。

初期の安全ネットワークは特定のメディアタイプやメディアアクセス方式に縛られていたため、製造メーカは安全機能の一部になる特別なケーブル、ネットワーク・インターフェイス・カード、ルータ、ブリッジなどを使用する必要がありました。これらのネットワークでは、安全デバイス間の通信しか対応しないという制限もありました。

つまり、製造メーカは機械を制御するために2つ以上のネットワーク(1つは標準制御用で、もう1つは安全関連制御用)を使用する必要があり、設置、トレーニングおよびスペアパーツに多くのコストがかかっていました。

最新の安全ネットワークでは、1本のネットワークケーブルで安全および標準制御デバイスの通信が可能になります。CIP (Common Industrial Protocol:共通の産業プロトコル) Safetyは、ODVA (Open DeviceNet Vendors Association)によって公開されているオープン規格のプロトコルで、DeviceNet、ControlNetおよびEtherNet/IPネットワーク上の安全デバイス間の安全通信に使用できます。CIP Safetyは標準のCIPプロトコルを拡張したプロトコルで、安全デバイスと標準デバイスをすべて同じネットワーク上に配置することができます。また、安全デバイスを含むネットワーク間をブリッジすることが可能であるため、安全デバイスをさらに分割して安全応答時間を微調整したり、簡単に安全デバイスを分散することもできます。安全プロトコルはエンドデバイス(セーフティPLC/コントローラ、安全I/Oモジュール、安全コンポーネント)のみを管理するため、標準のケーブル、ネットワーク・インターフェイス・カード、ブリッジ、およびルータが使用され、特別なネットワークハードウェアは必要なく、これらのデバイスに安全機能を持たせる必要はありません。

出力デバイス

セーフティ制御リレーおよびセーフティコンタクタ

制御リレーおよびコンタクタは、アクチュエータから電力を取り除くために使用されます。安全に使用するために、制御リレーとコンタクタに特殊機能が追加されています。

機械的にリンクされた補助接点を使用して、制御リレーおよびコンタクタのステータスを、モニタするロジックデバイスにフィードバックします。機械的にリンクされた接点を使用すると、安全機能を確保できます。機械的にリンクされた接点の要件を満たすには、通常開接点と通常閉接点を同時に閉じた状態にすることはできません。IEC 60947-4-1は、機械的にリンクされた接点の要件を規定しています。通常開接点が溶着した場合、通常閉接点は少なくとも0.5mm開いたままになります。逆に、通常閉接点が溶着した場合、通常開接点が開いたままになります。

安全システムは、特定の位置からのみ開始されなければなりません。標準定格の制御リレーおよびコンタクタは、アマチャを押し下げて通常開接点を閉じることができます。安全定格デバイスでは、予期しない起動の危険を緩和するためアマチャが手動制御されないように保護されています。

セーフティ制御リレーでは、通常閉接点はメインスパナによって駆動されます。セーフティコンタクタはアダーデッキを使用して、機械的にリンクされた接点の場所を確認します。接点ブロックがベースから脱落した場合は、機械的にリンクされた接点は閉じたままになります。機械的にリンクされた接点は、セーフティ制御リレーまたはセーフティコンタクタに取り外せないように固定されています。大型のコンタクタでは、幅の広いスパナのステータスを正確に反映させるには1つのアダーデッキでは不十分です。ミラー接点がコンタクタの片側に配置されます。

制御リレーまたはコンタクタのドロップアウト時間が、安全距離の計算に関わってきます。多くの場合、コイルを駆動する接点の寿命を向上させるためにサージサプレッサがコイルに取付けられます。AC電源用コイルでは、ドロップアウト時間は影響を受けません。DC電源用コイルでは、ドロップアウト時間が増加します。増加量は選択した抑制のタイプによって変わります。

制御リレーおよびコンタクタは、0.5Aから100Aを超える大きな電流負荷を切換えるように設計されています。安全システムは低電流で動作します。安全システムのロジックデバイスによって生成されるフィードバック信号は、通常DC24Vで数mAから数十mAの範囲でオンになります。セーフティ制御リレーおよびセーフティコンタクタは、金めっきされた分岐接点を使用して、より低い電流切換えの信頼性を向上させます。

過負荷保護

電気規格によりモータの過負荷保護が要求されます。過負荷保護デバイスの診断機能により、機器の安全だけでなくオペレータの安全も向上します。現在使用可能なテクノロジでは、過負荷、欠相、地絡、ストール、ジャム、負荷不足、電流不均衡、および過熱などのフォルト状態を検出できます。トリップが発生する前に異常な状態を検出し通知することは、生産稼動時間を増やし、オペレータや保守要員が予期しない危険な状態になることを防ぐために役立ちます。

ドライブおよびサーボ

安全定格ドライブおよびサーボは、回転エネルギーが流出するのを防いで、非常停止だけでなく安全停止を実行するためにも使用されます。

ACドライブは、冗長チャネルを備えた安全定格を実現し、ゲート制御回路から電力を除去します。冗長チャネルは、ドライブのタイプによって外部または内部ロジックのいずれかによってモニタされます。この冗長方式により、コンタクタを必要とせずに安全定格ドライブを非常停止回路に適用することができます。

サーボは、安全機能「安全トルクオフ」を実現するために使用される冗長安全信号を使用して、ACドライブと同様の結果を実現します。

接続システム

接続システムは、安全システムの設置および保守コストを低減するという付加価値があります。設計時には、シングルチャネル、デュアルチャネル、表示付きデュアルチャネル、およびさまざまなタイプのデバイスを考慮する必要があります。

デュアル·チャネル·インターロックを直列に接続する必要がある場合は、配電ブロックを使用すると簡単に設置できます。保護定格IP67では、これらのタイプのボックスを離れた場所にある機械に取付けることができます。多種多様なデバイスを組み合わせて使用する場合は、ArmorBlock Guard I/Oボックスを使用できます。入力はソフトウェアを使用して、さまざまなタイプのデバイスに対応できるように構成できます。

第5章: 安全距離の計算

危険源は、オペレータが到達する前に安全な状態になっていなければなりません。安全距離の計算に関しては、2つのグループの規格があります。これらの規格は、次のようにグループに分けられていいます。

ISO EN: (EN ISO 13855)

米国/カナダ(ANSI B11.19, ANSI RIA R15.06およびCAN/CSA Z434-03)

計算式

最小安全距離は、停止コマンドの処理に必要な時間と、検出されるまでにオペレータが検出領域に侵入できる距離で決まります。世界中で使用される計算式には、同じ形式と要件が使用されます。ただし、変数を表すために使用される記号と測定の単位が異なる場合があります。

以下の式を使用します。

ISO EN: S = K x T + C

米国/カナダ: Ds = K x (Ts + Tc + Tr + Tbm) + Dpf

この式のDsとSは、危険領域から最も近い検出ポイントまでの最小安全距離です。

接近する方向

ライトカーテンやエリアスキャナを使用した安全距離の計算を検討する場合は、検出デバイスに接近する角度を考慮に入れる必要があります。接近方法として以下の3タイプが考えられます。

通常 – 検出面に垂直方向から接近する。

水平 – 検出面と平行に接近する。

斜め – 検出領域に斜めの方向から接近する。

速度定数

Kは速度定数です。速度定数の値は、オペレータの動き(手の速度、歩く速度、歩幅など)によって異なります。このパラメータは、調査データに基づいて、オペレータの身体が静止しているときの手の速度は1600mm/sec (63インチ/sec)と想定するのが妥当であるとされています。実際のアプリケーションの状況を考慮に入れる必要があります。一般的なガイドラインとして、接近速度は1600～2500mm/sec (63～100インチ/sec)の範囲で変化します。適切な速度定数は、リスクアセスメントによって決定する必要があります。

停止時間

Tは、システムが完全に止まるまでの時間です。つまり、停止信号の開始から危険が解消するまでの合計時間を秒(sec)で表します。この時間は、分析しやすくするためにその増加部分(Ts、Tc、Tr、およびTbm)に細分化します。Tsは、期待する最低限の機械/機器の停止時間です。Tcは、期待する最低限の制御システムの停止時間です。Trは、インターフェイスを含む安全保護装置の応答時間です。Tbmは、エンドユーザがあらかじめ設定した停止時間の制限を超えたことをブレーキモニタが劣化として検出するまでに猶予される追加の停止時間です。Tbmは、部分回転機械式プレスに使用されます。Ts + Tc + Trの値がわからない場合、通常は停止時間測定デバイスを使って測定されます。

奥行侵入係数

奥行侵入係数は、CおよびDpfという記号で表されます。これは、安全保護装置によって検出されるまでに危険源に向かう最大移動距離です。奥行侵入係数は、デバイスのタイプとアプリケーションによって異なります。最適な奥行侵入係数を決定するには、適切な規格を確認する必要があります。ライトカーテンまたはエリアスキャナへの垂直方向からの接近の場合に、対象物感度が64mm (2.5インチ)未満のときは、ANSIおよびカナダ規格では次の式を使用します。

Dpf = 3.4 x (**対象物感度** – 6.875mm) (ただし、負の数でない)

ライトカーテンまたはエリアスキャナへの垂直方向からの接近の場合に、対象物感度が40mm (1.57インチ)未満のときは、ISOおよびEN規格では次の式を使用します。

C = 8 x (**対象物感度** – 14mm) (ただし、負の数でない)

これらの2つの式では、19.3mmで交差します。対象物感度が19mm未満の場合は、ライトカーテンまたはエリアスキャナは危険源からかなり遠ざける必要があるため、米国/カナダの方法では接近により厳しく制限が課せられます。対象物感度が19.3mmを超える場合は、ISO EN規格はより多くの制限を課します。世界中で使用される機械を製造するメーカは、両方の式における最悪の条件を考慮する必要があります。

通り抜けアプリケーション

比較的大きな対象物感度を使用する場合は、米国/カナダとISO EN規格では、奥行侵入係数と対象物感度が若干異なります。ISO EN値が850mmである場合に、米国/カナダの値は900mmです。両方の規格では、対象物感度も異なります。

手を伸ばすアプリケーション

どちらの規格も最下段ビームの高さは最低でも300mm以上でなければならないことで一致していますが、最上段ビームの最低の高さについては見解が異なります。ISO ENでは900mmに規定されているのに対して、米国/カナダでは1200mmに規定されています。最上段ビームの値については議論の余地があると考えられています。これを通り抜けアプリケーションで考えると、最上段ビームの高さは、オペレータが立った状態で十分に通れる高さが必要です。オペレータが検知面の上に手を伸ばすことができる場合は、部分検知基準が適用されます。

シングルまたはマルチビーム

シングルまたはマルチの個別のビームについては、ISO EN規格で詳細に定義されています。以下の図に、床からのマルチビームの「実用的」な高さを示します。ほとんどの場合、奥行侵入は850mmで、シングルビームの場合は1200mmを使用します。これに比べて、米国/カナダでは、これを通り抜けの要件として考慮しています。シングルおよびマルチビームの上、下、または側面からの接近についてを常に考慮する必要があります。

ビーム数	床からの高さ: mm (インチ)	C: mm (インチ)
1	750 (29.5)	1200 (47.2)
2	400 (5.7), 900 (35.4)	850 (33.4)
3	300 (11.8), 700 (27.5), 1100 (43.3)	850 (33.4)
4	300 (11.8), 600 (23.6), 900 (35.4), 1200 (47.2)	850 (33.4)

距離の計算

ライトカーテンへの垂直方向からの接近の場合は、ISO ENと米国/カナダでの安全距離の計算はよく似ていますが、相違点もあります。垂直に取付けられた対象物感度が最大40mmのライトカーテンに垂直方向から接近する場合、ISO ENの接近方法では2段階の手順が必要です。最初に、速度定数に2000を使用してSを計算します。

S = 2000 x T + 8 x (d -1 4)

Sの最小距離は100mmです。

2番目の手順は、距離が500mmより大きい場合に使用されます。
その場合、Kの値を1600に減じます。K=1600を使用する場合は、Sの最小値は500mmです。

米国/カナダの接近方法では、1段階の手順で実行されます。
Ds = 1600 x T * Dpf

この式では、応答時間が560msec未満の場合は、規格間で5%を超える違いが出ます。

斜めからの接近

ほとんどのアプリケーションでライトカーテンおよびスキャナは、垂直(垂直方向からの接近)または水平(平行方向からの接近)に取付けられています。取付けの角度が±5°以内の意図的な設計であれば、角度があるとは見なされません。角度が±5°を超えた場合は、接近についてリスクの可能性(距離が短すぎるなど)を考慮する必要があります。一般的に、基準面(床など)との角度が30°を超えると垂直と考えられ、30°未満の場合は水平と考えられます。

セーフティマット

セーフティマットの場合、オペレータは歩いて接近し、セーフティマットは床に設置されていると仮定して、安全距離にはオペレータの速度と歩幅を考慮する必要があります。マット上の上のオペレータの1歩目は、1200mm (48インチ)になります。オペレータが壇上に上る場合は、段の高さの40%だけ奥行侵入係数を減らすことができます。マットが動かないようにしっかりと固定することが重要です。

例

例: オペレータが14mmのライトカーテンに対して垂直方向からの接近するものとします。ライトカーテンはモニタ·セーフティ·リレーに接続され、モニタ·セーフティ·リレーはダイオードサプレッサが付いたDC電源コンタクタに接続されています。安全システムの応答時間(Tr)は、20 + 15 + 95 = 130msecです。機械の停止時間(Ts + Tc)は、170msecです。ブレーキモニタは使用しません。Dpfの値は1インチで、Cの値は0です。
この場合、以下のように計算します。

Dpf = 3.4 (14 – 6.875) = 1**インチ**(24.2mm)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf

Ds = 63 x (0.17 + 0.13 + 0) + 1

Ds = 63 x (0.3) + 1

Ds = 18.9 + 1

Ds = 19.9**インチ**(505mm)

C = 8 (14-14) = 0

S = K x T + C

S = 1600 x (0,3) + 0

S = 480mm (18.9**インチ**)

そのため、世界中で使用される機械の場合、セーフティ·ライト·カーテンを取付ける危険源からの最小安全距離は508mm (20インチ)になります。

第6章: 安全関連制御システム

はじめに

安全関連制御システム(SRCS)とは、危険な状況の発生を回避する機械制御システムの一部です。安全関連制御システムは独立した専用システムのこともあれば、標準の機械制御システムに統合されている場合もあります。

その複雑さは、電源コンタクタの制御巻線に直列で接続された防護ドアのインターロックスイッチや非常停止スイッチのような単純なシステムから、ソフトウェアおよびハードウェアを介して通信する単純なデバイスと複雑なデバイスの両方で構成される複合的なシステムまでさまざまです。

安全関連制御システムは、安全機能を実行するように設計されています。SRCSは、予想されるあらゆる状況で正常な動作を継続できる必要があります。それ内容は、安全機能とは何か、これを達成するためのシステムの設計方法は、およびそれをいつ行なったか、どのように示すか?です。

安全機能

安全機能は、特定の危険や一連の危険に際して機械制御システムの安全関連部分によって実行され、制御対象の装置を安全な状態に保持できるようにする機能です。安全機能が故障すると、装置の使用に関わる危険性が急に高くなります。すなわち、危険な状況になります。

「危険な状況」とは、人が危険にさらされたときに発生します。危険な状況が直接人に危害を及ぼすわけではありません。危険にさらされた人が危険を認識できれば、傷害を避けることができます。危険にさらされた人が危険に気づかない場合や、予期しない始動によって危険な状況が発生する場合もあります。安全システムの設計者の主な作業は、危険な状況や予期しない始動を回避することです。

安全機能は、通常、複数部分に分かれた要件で説明されています。例えば、インターロック付きガードによって起動される安全機能は、以下の3つの部分から構成されています。

1. ガードで保護された危険源は、ガードが閉じられるまで動作できません。
2. ガードが開くと、危険源がその時点で動作していた場合は停止されます。
3. ガードが閉じたとしても、ガードで保護された危険源は再始動しません。

特定のアプリケーションに対する安全機能を規定する場合は、「危険源」という言葉はその特定の危険に置き換える必要があります。危険源と危険による結果を混同してはなりません。身体を挟まれたり、切り傷、火傷などを負うことは危険の結果です。危険源の例としては、モータ、ラム、ナイフ、トーチ、ポンプ、レーザ、ロボット、エンドエフェクタ、ソレノイド、バルブ、その他のタイプのアクチュエータ、または重力に関連する機械的な危険源などがあります。

安全システムについて説明する場合、「安全機能に次の要求を出す時または次の要求の前に」という言い回しが使われます。安全機能に対する要求とは何でしょうか? 安全機能に対する要求の例としては、インターロック付きガードを開くことや、ライトカーテンを遮る、セーフティマットを踏む、非常停止ボタンを押すなどがあります。オペレータは、危険源を停止するか、すでに停止している場合は停止した状態を保持するように要求します。

機械制御システムの安全関連部分が、安全機能を実行します。安全機能は、1つの装置、例えばガードだけでは実行されません。ガードのインターロックがロジックデバイスにコマンドを送信し、それによってアクチュエータが無効になります。安全機能はコマンドで起動されて、実行後に終了します。

安全システムは、機械のリスクにつりあう安全度水準に設計する必要があります。リスクが高くなればなるほど、安全機能の性能を保証するためにより高い安全度水準が必要になります。機械安全システムは、その設計意図と安全機能の性能確保能力、つまり機能安全度水準によって分類できます。

制御システムの機能安全

機能安全とは何か?

機能安全とは全体的な安全要件の一部であり、その入力に応えてプロセスまたは機器が適切に機能することに依存します。IEC TR 61508-0には、機能安全の意味を明確化すために以下の例を示しています。「例えば、過熱防止装置は機能安全の一例です。これは電気モータの巻線内の温度センサを使用して、モータが過熱する前にモータの電源を遮断します。ただし、高温に耐えるための専用断熱材は機能安全の例ではありません(それでも、これは安全装置の一つで、まったく同じ危険源から保護することができる)。」

他の例として、ハードガードとインターロック付きガードを比べてみます。ハードガードは、インターロック式ドアと同様に危険源へのアクセスを防止できますが、「機能安全」とは認められません。インターロック式ドアは機能安全の一つです。ガードが開いているときは、インターロックが安全状態を実現するシステムへの「入力」として機能します。同様に、個人用保護具(PPE)が作業員の安全性を高めるための保護手段として使用されます。PPEは、機能安全とは認められません。

機能安全は、IEC 61508:1998で導入された用語です。それ以降、この用語はしばしばプログラム可能な安全システムにのみ関連付けられてきましたが、これは誤解です。機能安全は、安全システムを構築するために使用される幅広い範囲のデバイスが対象となります。インターロック、ライトカーテン、セーフティリレー、セーフティPLC、セーフティコンタクタ、および安全ドライブなどのデバイスは相互接続されて安全システムを構成し、特定の安全関連機能を実行します。これが機能安全です。

したがって、電気制御システムの機能安全は、機械の可動部に起因する危険源の制御に大いに関連しています。

機能安全を実現するには、以下の2つのタイプの要件が必要になります。

- 安全機能
- 安全整合性

リスクアセスメントは、機能安全要件の開発で重要な役割を果たします。タスクと危険を分析することで、安全のための機能的要件(例えば、安全機能)を知ることができます。リスクを定量化することで、安全整合性の要件(例えば、安全度水準または安全遂行レベル)を求めることができます。

機械に関する最も重要な制御システムの機能安全規格は、以下の4つです。

1. IEC/EN 61508「安全関連の電気、電子およびプログラマブル電子制御システムの機能安全」

   この規格には、複雑な電子およびプログラマブルシステムおよびサブシステムに適用される要件および規定が含まれています。この規格は一般的なもので、機械分野だけに限定されません。

2. IEC/EN 62061「機械類の安全性 – 安全関連の電気、電子およびプログラマブル電子制御システムの機能安全」

   この規格は、IEC/EN 61508を機械専用の要件に特化したものです。すべてのタイプの機械の安全関連の電気制御システムや複雑ではないサブシステムまたはデバイスの設計にも適用される要件を規定しています。複雑またはプログラム可能なサブシステムは、IEC/EN 61508の要件を満たす必要があります。

3. (EN) ISO 13849-1「機械類の安全性 – 制御システムの安全関連部分」

   この規格は、旧規格EN 954-1のカテゴリから直接移行するための指針を提供することを意図しています。

4. IEC 61511「機能安全 –プロセス産業分野の安全計装システム」

   この規格は、IEC/EN 61508をプロセス分野専用の要件に特化したものです。

機能安全規格は、従来のISO 13849-1:1999 (EN 954-1:1996)における「制御信頼性」や「カテゴリ」体系など、よく知られている既存の要件から大幅に進化しています。

カテゴリは完全になくなるわけではなく、現行の(EN) ISO 13849-1にも使用されています。

IEC/EN 62061および(EN) ISO 13849-1

IEC/EN 62061および(EN) ISO 13849-1は、どちらも安全関連の電気制御システムを対象にしています。これらは最終的に共通の用語を使用する1つの規格に統一されると考えられています。どちらの規格も同じ結果をもたらしますが、使用する方法は異なります。どちらの規格も、ユーザの状況に最も適した選択肢を提供することを目的としています。ユーザはいずれかの規格を使用するか選択して、欧州の機械指令の元で両方を統合します。

両方の規格の結果は、安全性能または整合性のレベルは同等です。それぞれの規格は、対象とするユーザに合わせて異なる方法を採用しています。

IEC/EN 62061の方法は、以前の慣例に従わないシステムアーキテクチャによって実施されている複雑な安全機能に対応することを目的としています。(EN) ISO 13849-1の方法は、従来のシステムアーキテクチャによって実施されているより旧式の安全機能のために、より直接的であまり複雑でない手段を提供することを目的としています。

これらの2つの規格の重要な違いは、各種多様なテクノロジに対する適用範囲です。IEC/EN 62061は、電気システムに適しています。(EN) ISO 13849-1は、電気システムだけでなく空気圧、油圧、機械式システムにも適用できます。

IEC/EN 62061および(EN) ISO 13849-1の共同技術報告

両方の規格のユーザを支援するために、IECとISO内で共同報告書が準備されました。

この報告書では、2つの規格の関係を説明し、(EN) ISO 13849-1のPL(安全遂行レベル)とIEC/EN 62061のSIL(安全度水準)の間でシステムとサブシステムレベルの両面でバランスをとる方法について説明しています。

両方の規格が同等の結果をもたらすことを示すために、同報告書では両方の規格の方法に従って計算された安全システムの例を示しています。同報告書はまた、さまざまに解釈されてきた数多くの問題を明確化しています。おそらく最も重要な問題の一つが、フォルト排除の観点です。

一般的に、安全関連制御システムによって安全機能を実現するためにPLeが必要とされる場合は、この安全遂行レベルを実現するためにフォルト排除のみに頼ることは適切ではありません。これは、使用されるテクノロジと対象となる動作環境によって左右されます。したがって、設計者はPL要件が高ければ高いほど、フォルト排除の使用に対してより一層の注意を払う必要があります。

一般的に、安全関連制御システムの設計でPLeを達成するためには、フォルト排除の使用は電気機械式の位置スイッチの機械的な側面には適用されません。特定の機械的な故障状態(摩耗/腐食、破断など)に適用できるフォルト排除は、ISO 13849-2の表A.4に記載されています。

例えば、PLeを達成する必要があるドア·インターロック·システムは、この安全遂行レベルを実現するために最小フォルトトレランスのレベル1 (2つの従来型の機械式の位置スイッチなど)を組み込む必要があります。これは、破損したスイッチアクチュエータなどのフォルトを排除するために、これが妥当だとは通常認められないためです。ただし、該当する規格に準拠して設計された制御パネル内の配線の短絡などのフォルトを排除するために、これを許容できる場合があります。

SILおよびIEC/EN 62061

IEC/EN 62061では、リスク低減の度合いとそのリスクを低減する制御システムの能力をSIL (安全度水準)という用語で説明しています。機械分野では、3段階のSILが使用され、SIL 1が最低で、SIL 3が最高の安全度水準です。

SILという用語は、石油化学、発電、および鉄道などの他の産業分野でも同じ方法で適用されるため、これらの産業分野で機械が使用されるときにIEC/EN 62061は非常に役に立ちます。プロセス産業などの他の産業分野では重大なリスクが発生する可能性があり、この理由からIEC 61508およびプロセス産業分野固有の規格IEC 61511にはSIL 4が含まれています。

SILは安全機能に適用されます。安全機能が組み込まれたシステムを構成しているサブシステムは、適切なSIL性能を備える必要があります。これは、SIL付与制限(SIL CL)と呼ばれます。IEC/EN 62061を正しく適用するには、この規格を徹底的に詳しく検討する必要があります。

PLおよび(EN) ISO 13849-1

(EN) ISO 13849-1ではSILという用語は使用されず、そのかわり、PL (安全遂行レベル)という用語が使用されます。多くの点で、PLはSILと関連しています。安全遂行レベルには5段階あり、PLaが最低レベルで、PLeが最高レベルです。

PLとSILの比較

以下の表に、標準的な回路構造に適用された場合のPLとSILのおおよその関係を示します。

PL (安全遂行レベル)	PFH_D (単位時間当たりの危険側故障発生確率)	SIL (安全度水準)
a	$\geqq 10^{-5} \sim < 10^{-4}$	なし
b	$\geqq 3 \times 10^{-6} \sim < 10^{-5}$	1
c	$\geqq 10^{-6} \sim < 3 \times 10^{-6}$	1
d	$\geqq 10^{-7} \sim < 10^{-6}$	2
e	$\geqq 10^{-8} \sim < 10^{-7}$	3

PLとSILのおおよその対応

重要: 上記の表は一般的な指針であり、変換のために使用してはなりません。両方の規格の完全な要件については、それぞれの規格を参照する必要があります。付属書Kの表に詳細な情報が記載されています。

第7章: (EN) ISO 13849に準拠したシステム設計

(EN) ISO 13849-1を正しく適用するには、この規格を徹底的に詳しく検討する必要があります。以下にこの規格の概要を示します。

この規格は、一部のソフトウェアの側面を含む制御システムの安全関連部分の設計と統合の要件を規定します。規格は安全関連システムに適用されますが、システムのコンポーネント部品にも適用されます。

SISTEMAソフトウェアPL計算ツール

SISTEMAは、(EN) ISO 13849-1の実装に使用されるソフトウェアツールです。このツールを使用すると、規格実装の定量化および計算面を大幅に簡略化できます。

SISTEMAは、「Safety Integrity Software Tool for the Evaluation of Machine Applications (機械アプリケーションの評価用安全保全ソフトウェアツール)」を表し、IFAによって定期的に見直され更新されています。このツールには、後で説明するように、さまざまなタイプの機能安全データを入力する必要があります。データは手作業で入力することも、製造メーカのSISTEMAデータライブラリを使用して自動的に入力することもできます。

ロックウェル・オートメーションのSISTEMAデータライブラリは、SISTEMAダウンロードサイトのリンクからダウンロードできます。
*www.rockwellautomation.com*にアクセスしてから、Solutions & Services→Safety Solutionsを順番に選択して表示したページ

(EN) ISO 13849-1の概要

以下に、(EN) ISO 13849-1の基本的な規定の概要を記載します。また、この説明には2106年の初めに発行された改訂についても言及されています。規格自体を綿密に検討することが重要です。

この規格には広い適用性があり、電気、油圧、空気圧、および機械システムを含むすべてのテクノロジに適用されます。ISO 13849-1は複雑なシステムに適用できるだけでなく、複雑なソフトウェアが組み込まれたコンポーネント向けのIEC 61508にも言及されています。

ISO 13849-1の出力は、安全遂行レベル [PL a、b、c、dまたはe]です。旧規格の「カテゴリ」の概念は残されていますが、システムのPLを主張するには追加要件を満たす必要があります。

この要件は、以下の基本形式で示されます。

- システムのアーキテクチャ。これは基本的に、カテゴリとして私たちが慣れていた概念に相当します。
- システムの構成要素として信頼性データが必要です。
- システムの自己診断率[DC]が必要です。これはシステムにおけるフォルトモニタの有効性を表します。
- 共通原因故障に対する保護
- 系統的障害に対する保護
- 必要に応じて、ソフトウェア固有の要件

この後、各要因について詳しく見ていきますが、それを行なう前に、規格全体の基本的な目的および原則について検討してみます。この段階で他にも知るべきことが多く存在するのは確かですが、規格が実現しようとしていることとその理由をいったん理解してから細部を知るほうが役に立ちます。

まず、なぜ新しい規格が必要になったのでしょうか。機械安全システムに使用されているテクノロジが過去10年間で飛躍的に進歩し変化していることは明らかです。比較的最近まで、安全システムは予知や予測が非常に容易な故障モードのある「シンプルな」機器に依存していました。しかし最近では、より複雑な電気式のプログラミング可能なデバイスが安全システムで使用されるようになってきました。このことはコストや柔軟性、互換性に関しては利点になりますが、既存の規格では対応しきれなくなったことも意味します。安全システムが十分に適切であるか否かを知るためには、安全システムについてもっとよく知る必要があります。これが機能安全規格に関するより多くの情報が求められている理由です。安全システムは、事前認証されたサブシステムを統合することにより、より「ブラックボックス」的な手法を採用するにつれて、規格に適合していることをより重視するようになってきました。したがって、これらの規格には適切にテクノロジを調査することができる能力が必要になります。規格はこれを実現するために、信頼性や障害検出、アーキテクチャと系統的な整合性に関する基本的な要因について論じる必要があります。これが(EN) ISO 13849-1の目的です。

規格全体を通して論理的に理解するために、安全関連サブシステムの設計者と安全関連システムの設計者という2つの根本的に異なるユーザタイプを考慮する必要があります。一般的に、サブシステムの設計者[通常は、安全コンポーネントの製造メーカ]は、より高いレベルの厳格性が求められます。サブシステムの設計者は、サブシステムがシステムに対して十分な整合性を持つことをシステムの設計者が確認できるように必要なデータを提供する必要があります。これは、通常、一定のテスト、分析および計算が必要です。その結果は、規格によって要求されるデータの形式で表されます。

システムの設計者(通常は、機械設計者またはインテグレータ)は、システムの全体的な安全遂行レベル(PL)を決定するために、サブシステムのデータを使用して比較的単純な計算を行ないます。

安全機能の決定

どのような安全機能にするのかを決める必要があります。安全機能が作業にとって適正なものになる必要があるのは明らかですが、どの程度保証すればよいのでしょうか。この規格はどのように役立つのでしょうか?

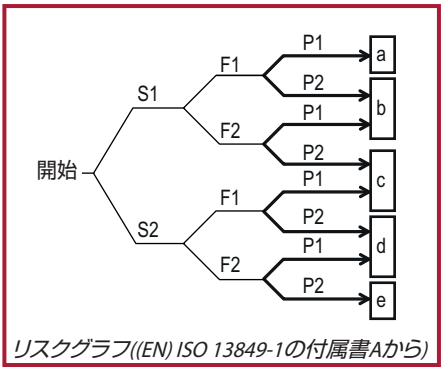
必要な機能は、実際の用途で一般的な特性を考慮することでのみ決定できるということを理解することが重要です。これは、安全概念の設計段階と見なすことができます。この規格は特定の用途の全特性について把握しているわけではないので、この規格ですべてを網羅することはできません。このことは、機械を製造しているもの、使用される正確な条件を必ずしも理解していない機械メーカにもしばしば当てはまります。

この規格は、一般的に使用される多くの安全機能(安全装置による安全関連停止機能、ミューティング機能、始動/再起動機能など)についてリストアップし、一般的に関連のある要件を定めることで便宜を図っています。この段階では、(EN) ISO 12100に関する考察:「基本設計原則およびリスクアセスメント」を使用することをお奨めします。ISO TR 22100-2は、ISO 12100に規定されている機械リスクアセスメントプロセスと(EN) ISO 13849-1のPL割付けプロセスの間の関係について有益な指針を提供します。また、特定の機械向けの安全機能要件が規定された機械固有の規格も幅広く用意されています。欧州のEN規格内では、これらの規格はCタイプの規格と呼ばれており、その一部はISO規格とまったく同じです。ISO TR 22100-1は、ISO 12100とC規格の関係に関する詳細な情報を提供します。

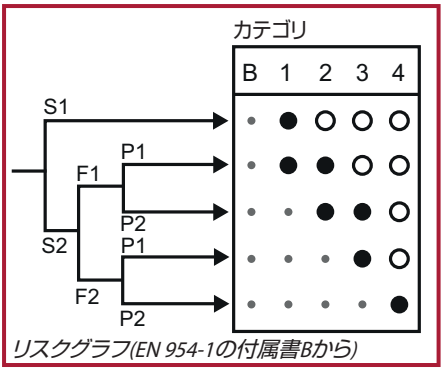
安全概念の設計段階は、機械の種類と使用されている用途と環境の特性にも依存していることがお分かりかと思います。機械メーカは、安全概念を設計できるようにするために、これらの要因を予測しておく必要があります。意図した(つまり予測される)使用条件を、ユーザーズマニュアルに記載しておく必要があります。機械のユーザは、それが実際の使用条件に合っていることをチェックする必要があります。

PLrは、安全機能で要求される安全遂行レベルを示すために使用され、リスクアセスメントでこれが決定されます。PLrを決定するためのリスクグラフが用意されており、この規格は傷害の程度(重大性)や危険にさらされる頻度、および危険回避の可能性についてのアプリケーション要素を入力します。

出力がPLrになります。旧規格であるEN 954-1のユーザはこの手法に慣れていますが、(EN) ISO 13849-1ではS1線が分岐していて、古いリスクグラフでは分岐していないことに注意してください。2015年版では、予測可能な発生確率に基づいて特定の状況ではPLrを1レベル引き下げる可能性が示されています。



リスクグラフ((EN) ISO 13849-1の付属書Aから)



リスクグラフ(EN 954-1の付属書Bから)

ここでは、安全機能を実装するために使用される制御システム[SRP/CS]の安全関連部分の安全機能と要求される安全遂行レベル(PLr)について説明します。私たちはここでシステムを設計し、PLrに適合していることを検証する必要があります。

(EN) ISO 13849-1またはEN/IEC 62061のどちらの規格を使用するか決定するための重要な要因の一つは、安全機能の複雑さです。ほとんどの場合、機械向けの安全機能は比較的単純であるため、(EN) ISO 13849-1が最適な選択となります。信頼性データ、自己診断率(DC)、システムアーキテクチャ[カテゴリ]、共通原因故障、および該当する場合はソフトウェアの要件がPLの評価に使用されます。

これは、概要を把握するための単純化された説明です。この規格の本文に指定されたすべての条項を適用する必要があることを理解してください。ただし、いつでも支援を利用できますので心配ありません。SISTEMAソフトウェアツールは文書化や計算の支援に利用できます。また、このツールは技術ファイルも作成します。

SISTEMAでは、ドイツ語や英語を初めとした多くの言語が利用できます。SISTEMAの開発元であるIFAは、ドイツに拠点を置く、信頼性の高い研究およびテスト機関です。主に、ドイツにおける法定事故保険や予防の観点から安全に関連する科学的および技術的問題の解決に取り組んでいます。この機関は20カ国以上の労働安全衛生局と協力して作業に当たっています。

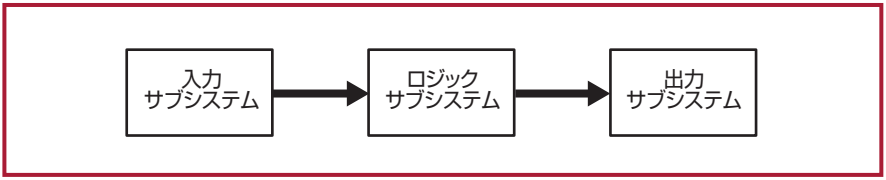
IFAの専門家は、彼らを後方支援する同僚らと共に(EN) ISO 13849-1およびIEC/EN 62061の両方の規格の起草にも大きく貢献しています。

SISTEMAで使用するロックウェル・オートメーションの安全コンポーネントデータの「ライブラリ」は、以下のページから入手できます。
*www.rockwellautomation.com*にアクセスしてから、Solutions & Services→Safety Solutionsの順番に選択して表示したページ

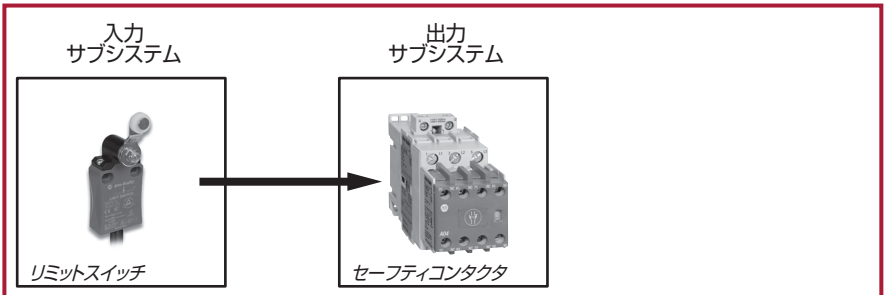
どの方法でPLの計算を行なう場合でも、適切な基礎から開始することが重要です。この規格と同じ方法でシステムを検討することが必要になるため、まず規格の説明からはじめてください。

システム構造

どのようなシステムも基本システムコンポーネント、すなわち「サブシステム」に分割できます。各サブシステムには、それぞれ独自の機能があります。ほとんどのシステムは、入力、ロジック解決、および作動の3つの基本機能に分割できます(一部の単純なシステムの中にはロジック解決機能のないものもある)。

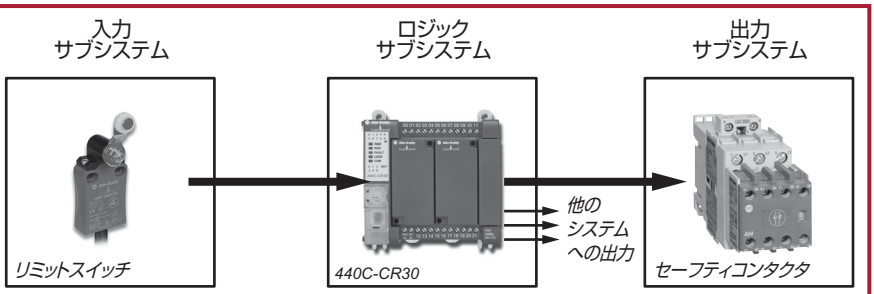


これらの機能を実装しているコンポーネントグループがサブシステムです。



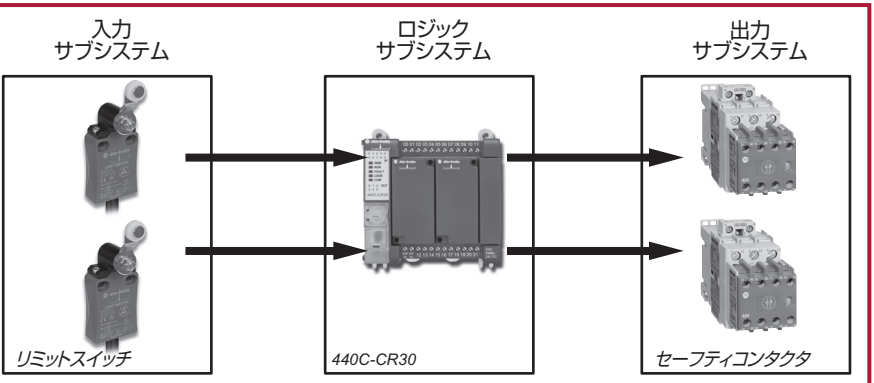
インターロックスイッチおよびセーフティコンタクタ

上図に、単純なシングルチャネル電気システムの例を示します。このシステムは、入力および出力サブシステムのみで構成されています。



インターロックスイッチ、セーフティコントローラおよびセーフティコンタクタ

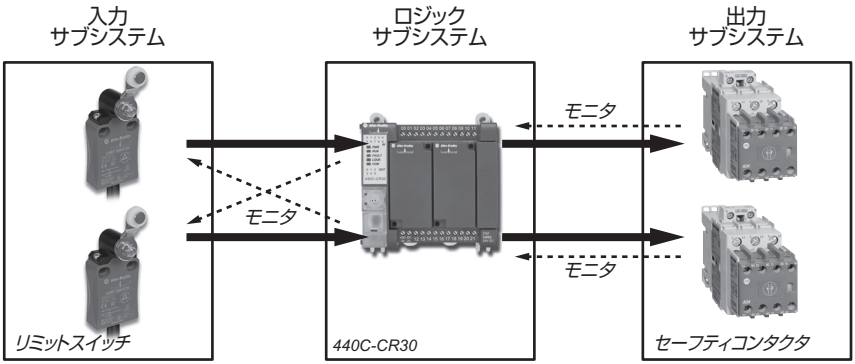
上図のシステムはもう少し複雑で、いくつかの論理演算が必要になります。セーフティコントローラ自体は内部にフォルトトレランス(つまりデュアルチャネルなど)を備えていますが、システム全体は単一のリミットスイッチおよび単一のコンタクタのサブシステムであるため、ステータスはシングルチャネルに制限されたままです。シングル・チャネル・システムは、シングルチャネルの1つが故障するとシステム全体も故障するため、「フォルトトレランス」ではありません。



デュアルチャンネル安全システム

上図は、デュアルチャネル(冗長または「フォルトトレランス」とも呼ばれる)システムです。各サブシステムには2つのチャネルがあり、単一のフォルトが発生しても耐えることができ、安全機能を提供できます。この安全機能では、サブシステムの故障、つまりシステムの故障が発生するには、各チャネルに1つずつ、合計2つの障害が発生する必要があります。明らかにデュアル・チャネル・システムはシングル・チャネル・システムに比べて、危険な状況に対して故障が発生しにくくなります。しかし、フォルト(障害)検出のための診断手順を含めることで、より一層(安全機能に関して)信頼性を高めることができます。もちろん、フォルトが検出された場合には、それに対応してシステムを安全な状態にする必要があります。

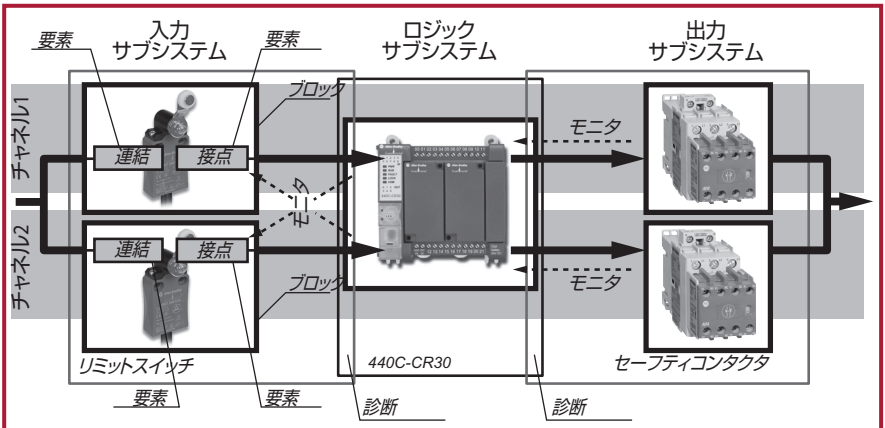
以下の図に、モニタ技術によって実現された診断手順が含まれている例を示します。



デュアルチャネル安全システムの診断

必ずではありませんが、以下の図に示すように、すべてに2つのチャネルがあるサブシステムでシステムが構成されていることが一般的です。したがって、この場合は各サブシステムに2つの「サブチャネル」があることが分かります。規格ではこれらを「ブロック」と表現しています。2つのチャネルを持つサブシステムは、少なくとも2つのブロックを持ち、シングル·チャネル·サブシステムは少なくとも1つのブロックを持ちます。デュアルチャネルのブロックとシングルチャネルのブロックの組み合わせてシステムを構成することも可能です。

このシステムをより深く検討したい場合、ブロックのコンポーネントに目を向ける必要があります。SISTEMAツールでは、これらのコンポーネント部品のことを示すために「要素」という用語を使用します。



診断付きのデュアルチャネル安全システムで、分割されたシステム

リミットスイッチのサブシステムは、要素レベルにまで細分化されていることが分かります。出力コンタクタサブシステムはブロックレベルまで細分化されていますが、ロジックサブシステムは既に製造メーカによって所定のPLが認証され検証されているため、まったく細分化されていません。リミットスイッチおよびコンタクタのモニタ機能は、両方ともロジックコントローラによって実行されます。したがって、リミットスイッチおよびコンタクタサブシステムを表すボックスは、ロジックサブシステムのボックスと部分的に重なり合っています。

このシステム細分化の原則は、(EN) ISO 13849-1に規定された方法論やSISTEMAツールの基本システム構造原則で認識できます。ただし、これらにはわずかな違いが存在することにも注意する必要があります。規格では手法に特に制限はありませんが、PLを評価するための簡略化された方法では、通常、最初にシステム全体がチャネルに分解され、次に各チャネル内でブロックに分解されます。SISTEMAを使用すると、さらに簡単にシステムをサブシステムに分割し、各サブシステムをブロックに分割することができます。この規格ではサブシステムの概念を明確に記述していませんが、SISTEMAではより理解可能で直感的な手法でサブシステムの概念を使用しています。もちろん、最終的な計算には影響しません。SISTEMAとこの規格では、いずれも同じ原則と式を使用しています。また、興味深いことに、サブシステムの手法はEN/IEC 62061でも使用されています。

本書で例として使用しているシステムは、規格が明示されているシステムアーキテクチャの5つの基本タイプの1つにすぎません。カテゴリシステムをよく理解しているかたであれば、この例はカテゴリ3または4に相当するとお分かりでしょう。

この規格は、旧規格EN 954から元の5つのカテゴリを使用しています。これらは指定アーキテクチャカテゴリと呼ばれます。これらのカテゴリの要件は、EN 954-1で規定されたカテゴリの要件と完全ではないものほぼ同じです。指定アーキテクチャカテゴリは、以下の図のように表されます。これらのカテゴリがシステム全体またはサブシステムのいずれかに適用できることに注意する必要があります。これらの図は、そのまま物理構造としてとらえるべきではなく、概念的な要件をグラフィカルに表したものです。

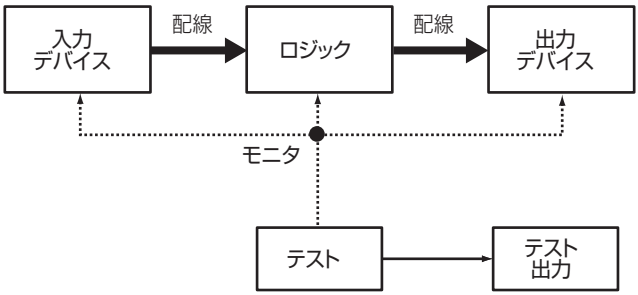
指定アーキテクチャのカテゴリB

指定アーキテクチャカテゴリBは、基本的な安全原理((EN) ISO 13849-2の付属書を参照)を使用する必要があります。単一のフォルトが発生すると、システムまたはサブシステムが故障する可能性があります。

完全な要件については、(EN) ISO 13849-1を参照してください。

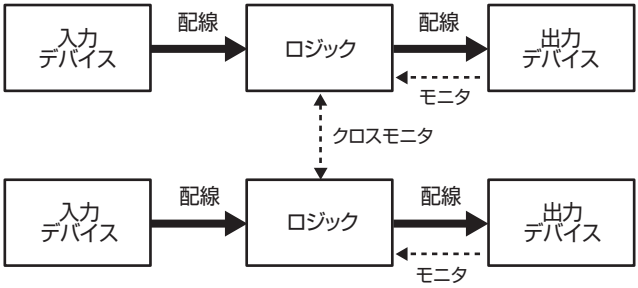
指定アーキテクチャのカテゴリ1

指定アーキテクチャカテゴリ1はカテゴリBと同じ構造で、単一のフォルトが発生すると故障する可能性があります。ただし、十分に検証された安全原理((EN) ISO 13849-2の付属書を参照)を使用する必要もあるため、故障発生の可能性はカテゴリBよりも低くなります。完全な要件については、(EN) ISO 13849-1を参照してください。



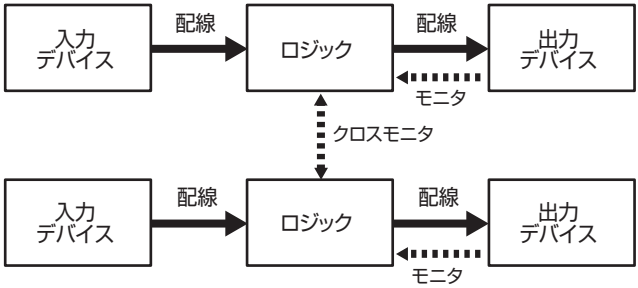
指定アーキテクチャのカテゴリ2

指定アーキテクチャカテゴリ2は、基本的な安全原理((EN) ISO 13849-2の付属書を参照)を使用する必要があります。また、システムまたはサブシステムの機能テストによる診断モニタも実行する必要があります。これは起動時に実施する必要があり、その後は、安全機能に対する各要求に対して少なくとも100回のテストに相当する頻度で定期的に実施する必要があります。2015年の修正では、プロセス安全時間になる前に安全状態に移行する安全機能に関する代替要件が許可されました。各機能テストの間に単一のフォルトが発生した場合、システムまたはサブシステムは故障する可能性がありますが、故障発生の可能性は通常、カテゴリ1よりも低くなります。PLdに使用されるカテゴリ2では、障害が検出された場合にテスト出力が安全状態を開始する必要があるため、2つの信号出力デバイスを使用する必要があることに注意してください。完全な要件については、(EN) ISO 13849-1を参照してください。



指定アーキテクチャのカテゴリ3

指定アーキテクチャカテゴリ3は、基本的な安全原理((EN) ISO 13849-2の付属書を参照)を使用する必要があります。システム/サブシステムは、単一のフォルトが発生しても故障してはならないという要件もあります。このことは、当該システムは安全機能に関してシングル·フォルト·トレランス(単一のフォルトに対する耐性)を有する必要があることを意味します。この要件を達成するための最も一般的な方法は、上図に示すようなデュアル·チャネル·アーキテクチャを採用することです。これに加えて、可能な限り単一のフォルトを検出することも求められます。この要件は、EN 954-1のカテゴリ3の元の要件と同じです。そのような状況では、「可能な限り」という表現の意味は多少問題であることが分かります。これでは、カテゴリ3には、冗長性を備えているものフォルト検出はできないシステム(しばしば「愚かなる冗長性」と説明的に描写される)から、単一のフォルトをすべて検出できる冗長システムまでが含まれていることになります。(EN) ISO 13849-1では、自己診断率(DC)の品質を評価するための要件でこの問題を解決しています。システムの信頼性($MTTF_D$)が高ければ高いほど、必要とされるDCが低くなることが分かります。ただし、いかなる場合でも、カテゴリ3のアーキテクチャでのDCは60%以上であることが必要です。)



指定アーキテクチャのカテゴリ4

指定アーキテクチャカテゴリ4は、基本的な安全原理((EN) ISO 13849-2の付属書を参照)を使用する必要があります。このカテゴリは、カテゴリ3の要件の図に似ていますが、より多くのモニタ、すなわち高い自己診断率が求められています。これは、モニタ機能を示す点線が太くなっていることで表されます。カテゴリ3とカテゴリ4の基本的な違いは、カテゴリ3ではほとんどのフォルトを検出する必要があるのに対して、カテゴリ4ではすべての危険な単一のフォルトおよび危険なフォルトの組み合わせを検出する必要があることです。実際には、通常、高度の診断によってこれが達成され、すべての関連するフォルトの累積が可能になる前に確実に検出されます。DCは99%以上であることが求められます。

信頼性データ

(EN) ISO 13849-1では、制御システムの安全関連部分によって達成されるPLの計算の一部として定量的信頼性データが使用されます。これで最初に浮かぶのは、「データはどこから取得するのか?」という疑問です。一般に認められている信頼性ハンドブックのデータを使用することもできますが、この規格には望ましい情報源は製造メーカであることが明記されています。このため、ロックウェル·オートメーションではSISTEMA用にデータライブラリの形式で関連データを提供しています。

さらに先に進む前に、どのようなタイプのデータが必要なのかを検討し、またそのデータはどのようにして作成されるかについても理解する必要があります。

この規格(およびSISTEMA)におけるPLの評価の一環として必要になる最終的なデータのタイプは、PFH (単位時間当たりの危険側故障確率)です。これは、IEC 61508で使用されているものと同じデータであり、IEC/EN 62061で使用されているPFH_Dという略語で表されます。

PL (安全遂行レベル)	PFH_D (単位時間当たりの危険側故障発生確率)	SIL (安全度水準)
a	$\geqq 10^{-5} \sim < 10^{-4}$	なし
b	$\geqq 3 \times 10^{-6} \sim < 10^{-5}$	1
c	$\geqq 10^{-6} \sim < 3 \times 10^{-6}$	1
d	$\geqq 10^{-7} \sim < 10^{-6}$	2
e	$\geqq 10^{-8} \sim < 10^{-7}$	3

上記の表は、PFH_D とPLとSILの関係を示します。一部のサブシステムでは、PFH_Dは製造メーカから入手できるます。これにより、計算の手間をかなり省くことができます。製造メーカは通常、サブシステムをユーザに提供するために比較的複雑な計算やテストを実施する必要があります。このデータを入手できない場合、(EN) ISO13849-1ではシングルチャネルの平均$MTTF_D$(平均危険側故障間隔)に基づく簡略化された代替方法を推奨しています。この代替方法では、この規格で定められている手法と式を使用して、システムまたはサブシステムのPL (およびPFH_D)を計算できます。SISTEMAを使用すれば、さらに簡単に計算を行なうことができます。

注: デュアル·チャネル·システム(診断付きまたはなし)では、1/PFH_Dを使用して、(EN) ISO 13849-1で要求されるMTTF$_D$を決定することは誤りであることを理解しておく必要があります。この規格では、シングルチャネルのMTTF$_D$が必要とされています。これは、2つのチャネルサブシステムの両方のチャネルの組み合わせと、MTTF$_D$の値ははまったく違う値です。2つのチャネルサブシステムのPFH_Dがわかっている場合は、それをSISTEMAに直接入力できます。

シングルチャネルのMTTF$_D$

これは、安全機能の故障につながる可能性のあるフォルト(故障)が発生するまでの平均時間です。この値は年単位で示され、各チャネルの「ブロック」のMTTF$_D$の平均値であり、システムまたはサブシステムのいずれかに適用できます。この規格では、シングルチャネルまたはサブシステムで使用される各要素のすべてのMTTF$_D$の平均値を計算するために使用する以下の式を規定しています。

この段階で、SISTEMAの値が明らかになります。これらの作業はソフトウェアによって実行されるため、ユーザは時間のかかる表の参照や式の計算をせずに済みます。最終結果は、複数ページのレポート形式でプリントアウトできます。

$$\frac{1}{\mathrm{MTTF_d}} = \sum_{i=1}^{\tilde{N}} \frac{1}{\mathrm{MTTF_{di}}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{\mathrm{MTTF_{dj}}}$$

(EN) ISO 13849-1からの式D1

ほとんどのデュアル·チャネル·システムでは、両方のチャネルが同じであるため、式の結果はいずれのチャネルにも当てはまります。

システム/サブシステムのチャネルが異なる場合は、この規格ではこれに対応する式を利用できます。

$$\mathrm{MTTF_d} = \frac{2}{3}\left[\mathrm{MTTF_{dC1}} + \mathrm{MTTF_{dC2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{dC1}}} + \frac{1}{\mathrm{MTTF_{dC2}}}}\right]$$

これは実際には2つの平均値の平均です。単純化のために、ワーストケースのチャネル値を使用することも許容されています。

この規格では、$MTTF_D$ を以下の表に示すように3つの範囲にグループ分けしています。

各チャネルの$MTTF_D$の表示	各チャネルの$MTTF_D$の範囲
低	3年 ≦ $MTTF_D$ < 10年
中	10年 ≦ $MTTF_D$ < 30年
高	30年 ≦ $MTTF_D$ < 100年

$MTTF_D$のレベル

(EN) ISO 13849-1では、導き出された実際の値がどれほど大きなものであっても、サブシステムのシングルチャネルの使用可能な$MTTF_D$を最大100年に制限していることに注意してください。

後で説明するように、次に$MTTF_D$平均の達成範囲を、指定アーキテクチャカテゴリと自己診断率(DC)と組み合わせと、暫定的なPLL評価値が得られます。ここで「暫定的」という用語を使用しているのは、システムの整合性や共通原因故障への対策など他の要件も必要に応じて満たさなければならないためです。

データ評価の手法

製造メーカが*PFH_D*または$MTTF_D$のいずれかの形式でデータを評価する方法について、もう少し詳しく検討する必要があります。コンポーネントは、以下の3つの基本タイプに分類できます。

- 機械的(電気機械式、機械、空気圧、油圧など)
- 電子的(ソリッドステートなど)
- ソフトウェア

これらの3つのテクノロジタイプの共通故障メカニズムには根本的な違いが存在します。基本的には、次のように要約できます。

機械的テクノロジ:

故障は、固有の信頼性と使用量の両方に比例します。使用量が多ければ多いほど、コンポーネント部品のいずれかが品質低下して故障する可能性が高くなります。これだけが故障の理由とはなりませんが、運転時間/サイクルが制限されている場合を除いて、主要な故障原因となります。10秒ごとに1回のサイクルを持つコンタクタのほうが、1日につき1回のサイクルで動作する同じコンタクタよりも信頼性がある状態で動作する期間がはるかに短いのは自明の理です。

一般的に、物理テクノロジデバイスは、それぞれが特定の用途向けに個別に設計されたコンポーネントで構成されています。これらのコンポーネントは、成形、金型、鋳造、機械加工などの方法で製造され、連結、スプリング、磁石、電気巻線などと組み合わされてメカニズムを形成します。一般的に、これらのコンポーネント部品は他の用途に使用されたことがないため、既存の信頼性データを入手できません。当該メカニズムのPFH_Dまたは$MTTF_D$の評価は、通常、テストに基づいて行なわれます。EN/IEC 62061および(EN) ISO 13849-1は、いずれも$B10_D$テストと呼ばれるテストプロセスを推奨しています。

$B10_D$テストでは、数多くの(通常、10以上の)サンプルデバイスを適切な一般的な条件のもとでテストされます。サンプルの10%が故障して危険な状況が陥るまでの動作サイクルの平均数が、B10d値と呼ばれるものです。実際には、すべてのサンプルが故障しても安全状態になることもよくありますが、その場合、この規格はB10d (危険)値をB10値の2倍とすることができるとこの規格には明記されています。

電子的なテクノロジ:

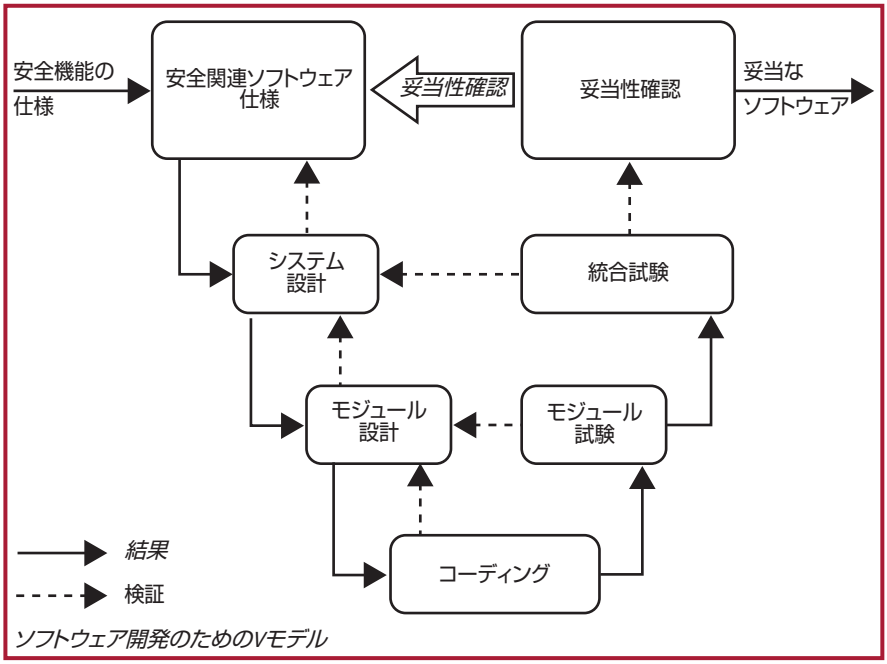
物理的な磨耗が生じる可動部がありません。動作環境が特定の電気的および温度特性に見合っていると仮定すると、電子回路の主な故障は、回路を構成するコンポーネントの固有の信頼性(または信頼性の欠如)に比例します。個々のコンポーネントの故障には、製造時の欠陥や過度の電力サージ、機械的な接続の問題など、さまざまな原因が存在します。一般的に、電子コンポーネントの故障は、負荷や時間、温度条件によって発生する可能性がありますが、分析による予測は困難であり、本質的にランダムに発生しているように見えます。したがって、テスト環境下で電子機器をテストしても、代表的な長期的故障パターンは必ずしも明らかになりません。

電子機器の信頼性を評価するには、分析と計算を使用するのが一般的です。個々のコンポーネントに関する有用なデータは、信頼性データハンドブックにも記載されています。どのコンポーネント故障モードが危険であるかは、分析によって判断できます。平均してコンポーネント故障モードの50%が安全で、50%が危険であるというのが許容可能で一般的です。通常、この方法では比較的控えめなデータになります。

IEC 61508には、デバイス、すなわちサブシステムの全体的な危険側故障確率(PFHまたはPFD)の計算に使用できる式が定められています。この計算式はかなり複雑であり、(必要に応じて)コンポーネントの信頼性、共通原因故障の可能性(ベータ係数)、自己診断率(DC)、機能テストの間隔、プルーフテストの間隔も考慮してください。幸いなことに、この複雑な計算は通常、デバイス製造メーカによって実施されています。EN/IEC 62061および(EN) ISO 13849-1は、どちらもIEC 61508に準拠したこの方法で計算されたサブシステムを認めています。この計算で得られたPFH_Dは、(EN) ISO 13849-1の付属書KまたはSISTEMA計算ツールのいずれかで直接使用できます。

ソフトウェア:

ソフトウェアの故障は、本質的に系統的な性質のものです。その原因は、ソフトウェアがどのように考案、記述、またはコンパイルされたかに起因します。したがって、すべての故障の原因は、ソフトウェアの使用ではなく、製造元となったシステムにあります。そのため、故障を抑制するには、システムを制御する必要があります。IEC 61508と(EN) ISO 13849-1には、どちらにもそのための要件と手法が定められています。ここでは詳細を説明する必要はないので、両方の規格が古典的なVモデルを使用していることを述べるだけにとどめます。組み込みソフトウェアは、デバイスの設計者にとって問題となります。一般的な手法としては、IEC 61508パート3で規定された正式の方法に従って組み込みソフトウェアを開発します。ユーザとのインターフェイスを受け持つソフトウェアであるアプリケーションコードに関しては、ほとんどのプログラム可能な安全デバイスに「認定済み」のファンクションブロックまたはルーチンが提供されています。これを利用することで、アプリケーションコードの検証作業が簡略化されますが、完成したアプリケーションプログラムの妥当性確認が必要であることは忘れてはなりません。ブロックをリンクしてパラメータ化する方法は、目的の作業に対して適切かつ妥当であることが実証されていなければなりません。(EN) ISO 13849-1とIEC/EN 62061は、どちらもこのプロセスに関するガイドラインを規定しています。



ソフトウェア開発のためのVモデル

自己診断率(DC)

これについては、指定アーキテクチャカテゴリ2、3および4について検討した際に既に触れました。これらのカテゴリでは、なんらかの形式の診断テストを実施して安全機能が正常に動作していることを確認する必要があります。「自己診断率」(通常、DCと略記)という用語は、このテストの有効性を示すために使用されます。DCは、危険な故障の可能性があるコンポーネント数だけに基づくものではないことを理解する必要があります。DCでは全体的な危険側故障率も考慮されています。「故障率」を表すために記号λが使用されます。DCは、以下の2つのタイプの危険側故障の発生率の関係を示します。

検出危険側故障[λdd] 安全機能の喪失の原因となる、またはそれにつながる故障ではあるが、既に検出されている故障。検出後に、故障応答機能によってデバイスまたはシステムは安全状態に移行します。

危険側故障[λd] 潜在的に安全機能の喪失の原因となる、またはそれにつながる可能性のあるすべての故障。これには、検出された故障も検出されていない故障の両方が含まれます。もちろん本当に危険な故障は、未検出の危険側故障(λduで示される)です。

DCは、以下の式で表されます。

DC = λdd/λd (割合(%)で示す)。

DCという用語の意味は、(EN) ISO 13849-1とEN/IEC 62061で共通しています。ただし、それを導き出す方法が異なります。後者の規格は、故障モード分析に基づいた計算の使用を推奨していますが、(EN) ISO 13849-1に規定されたルックアップテーブル形式での簡略化された方法の使用も許容されています。各種の一般的な診断方法が、その使用により達成されると考えられるDCの割合(%)と共に記載されています。場合によっては、依然として推理的な判断が必要なものもあります。例えば、一部の技法では、得られるDCはテストの実施頻度に比例します。この手法は不確実すぎるという意見もありますが、DCの評価は多くの異なる変数要素に依存しているため、いずれの技法を使用しても、通常の結果は概算値で表すことしかできません。

また、(EN) ISO 13849-1の表はIFAによって実施された幅広い調査に基づいていて、実際の用途で使用されている既知の実際の診断技法で得られた結果になっていることも理解する必要があります。この規格では、簡略化のためにDCを以下の4つの基本範囲に分けています。

60%未満 = なし
60〜90% = 低
90〜99% = 中
99%以上 = 高

個々の割合(%)の値ではなく範囲を使用するこの手法は、実際の精度の面では十分に現実的であると見なすことができます。SISTEMAツールは、この規格と同じルックアップテーブルを使用します。安全関連デバイスでの複雑な電子部品の使用が増加するにつれて、DCはますます重要な要素になってきています。各規格における今後の作業では、この問題の明確化がさらに検討されると考えられています。それまでの間、DCの範囲の適切な選択には工学的および常識的な判断を使用すれば十分です。

共通原因故障(CCF)

ほとんどのデュアルチャネル(つまりシングル・フォルト・トレランス)のシステムまたはサブシステムにおいて、診断の仕組みは両方のチャネルで危険な故障が同時に発生することはないという前提に基づいています。「同時に」という用語を正確に表現すると、「同じ診断テスト間隔で」となります。診断テスト間隔が適度に短い場合(8時間未満)、2つの独立した関連性のない故障がその時間内に発生する確率はきわめて低いと仮定するのが合理的です。ただし、この規格ではその故障が本当に独立した無関係のものであるかどうか慎重に検討すべきである点を明確にしています。例えば、1つのコンポーネントの故障が他のコンポーネントの故障につながることが予測できる場合は、故障全体は単一フォルトであると考えられます。

また、1つのコンポーネントの故障の原因となる事象が、他のコンポーネントの故障の原因になる可能性もあります。これは「共通原因故障」と呼ばれ、通常、CCFという略語が使用されます。CCFが発生する傾向の度合いは、通常、ベータ(β)係数として説明されます。サブシステムおよびシステムの設計者がCCFの可能性を認識していることは非常に重要です。さまざまなタイプのCCFが存在し、それに応じて回避方法も数多く存在します。(EN) ISO 13849-1では、複雑すぎでも単純すぎでもない合理的な方法が規定されています。EN/IEC 62061と同様に、この規格では本質的に定性的な手法が採用されています。この規格は、CCFを回避するために効果的と認められている対策のリストを提供しています。

番号	CCFの対策	スコア
1	隔離/分離	15
2	ダイバーシティ(多様性)	20
3	設計/アプリケーション/経験	20
4	評価/分析	5
5	能力/トレーニング	5
6	環境	35

共通原因故障(CCF)のスコアリング

システムやサブシステムを設計する際に、このリストの中から十分な数の対策を導入する必要があります。このリストを使用するだけではすべてのCCFの可能性を回避することはできなという主張にも、ある程度正当な理由があります。しかしながら、リストの趣旨を正しく考えるなら、この要件の真意は、設計者がCCFの可能性を分析し、テクノロジの種類と対象用途の特性に基づいて適切な回避策を導入できるようにすることです。リストを使用することによって、多様な故障モードや設計能力などの最も基本的で効果的な技法の一部を検討することができます。IFA SISTEMAツールでも、この規格のCCFルックアップテーブルの導入が必要で、使いやすい形式で利用できるようにしています。

系統的故障

すでに、$MTTF_D$の形式の定量化された安全信頼性データや危険側故障確率について議論してきましたが、これはそれだけで終わる話ではありません。それらの用語について言及する際には、ランダムな性質と思われる故障について検討しました。実際に、IEC/EN 62061では、PFH_Dという略語はランダムなハードウェア故障発生確率を指しています。しかし、設計プロセスや製造プロセスでのエラーに起因する種類の故障も存在し、「系統的障害」と総称されています。この代表的な例が、ソフトウェアコードのエラーです。この規格では、付属書Gに、これらのエラー(およびそれに伴う故障)を回避するための対策を定めています。これらの対策には、適切な素材および製造技術、レビュー、分析、およびコンピュータシミュレーションの利用などの対応が含まれています。また、動作環境では、結果を制御しなければ故障の原因となる予測可能な事象や特性も発生します。付属書Gには、これを回避するための対策も定められています。例えば、偶発的に電力の損失が発生することは容易に予測できます。したがって、コンポーネントの電源が切断されても、システムは安全な状態を維持できるようにする必要があります。このような対策は単に常識と思われがちで、実際にそうですが、極めて重要なことです。系統的故障の抑制や回避に対して適切な考慮を払わない場合、この規格の他のすべての要件は無意味なものとなります。これは、自動診断テストや冗長ハードウェアなど、必要なPFH_Dを達成するために、ランダムなハードウェア故障の抑制に使用されるものと同等の対策が求められる場合もあります。

フォルト排除

故障分析は、安全システムの主要な分析ツールの1つです。設計者とユーザは、フォルトが存在する場合に安全システムがどのように動作するかを理解する必要があります。この分析を実行するためにさまざまな技法を使用できます。例として、フォルトツリー解析、故障モード、影響および致命度解析、イベントツリー解析、および負荷強度検査などがあります。

分析中に、特定のフォルトを発見できないこともあります。これは、費用を節減した自動診断テストでは検出できないためです。さらに、これらのフォルトが発生する確率は、設計、構造およびテスト方法の軽減策を講じることによって極めて低くなる場合があります。このような状況では、さらに検討することによりフォルトを排除できる可能性もあります。フォルト排除とは、SRCSの特定の故障に関してその発生確率が無視できるほど低いためにそのフォルトの発生を排除することです。

(EN) ISO13849-1では、技術的に発生しそうにないこと、一般に認められている技術的な経験、およびアプリケーションに関連する技術的要件に基づいたフォルト排除を認めています。(EN) ISO13849-2では、電気、空気圧、油圧および機械システムにおける特定のフォルトを排除するための例やその正当な理由も記載されています。フォルト排除は、正当性を詳細に示した上で、技術文書で宣言する必要があります。

特定のフォルトを排除することができなければ、安全関連制御システムを評価することは常に可能であるわけではありません。フォルト排除については、ISO 13849-2を参照してください。

リスクレベルが高くなればなるほど、フォルト排除のための正当化はより厳しくなります。一般的に、安全関連制御システムによって実現される安全機能のためにPLeが要求される場合、この安全遂行レベルを実現するためにフォルト排除のみに頼ることは通常ありません。これは、使用されるテクノロジと対象となる動作環境によって左右されます。そのため、PL要件が高くなればなるほど、設計者はフォルト排除の使用に関してより多くの注意を払う必要があります。

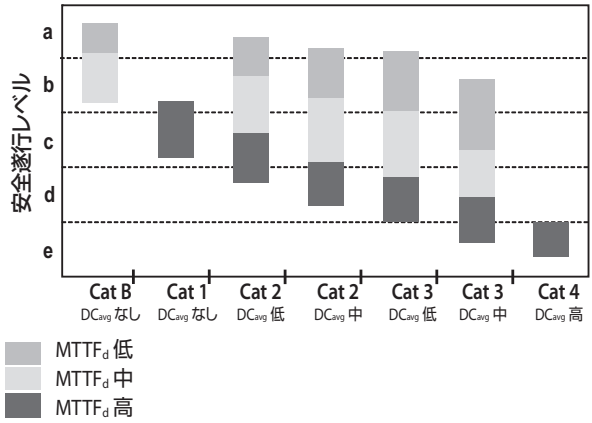
安全遂行レベル(PL)

安全遂行レベルは、制御システムの安全関連部分が安全機能を実行する能力を規定する個別のレベルです。

指定された5つのアーキテクチャのいずれかを実装することによって達成されるPLを評価するために、システム(またはサブシステム)には以下のデータが必要になります。

- $MTTF_D$ (各チャネルの危険側故障発生までの平均時間)
- DC (自己診断率)
- アーキテクチャ(カテゴリ)

以下の図に、これらの要因を組み合わせてPLを評価する方法を示します。付属書Kの表は、この図に基づいて作成されたさまざまなマルコフモデルの結果を表形式で示しています。より正確な判断が必要な場合は、この表を参照してください。



PLのグラフィカルな決定

要求されるPLを達成するためには、その他の要因も理解する必要があります。これらの要件には、共通原因故障や系統的故障、環境条件、およびミッション時間などが含まれます。システムまたはサブシステムのPFH_Dがわかっている場合は、付属書Kの表を使用してPLを特定することができます。

サブシステムの設計と組み合わせ

PLに準拠したサブシステムは、以下に示す表を使用してシステムに統合できます。

PLlow	Nlow	PL
a	>3	許可されない
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

直列に組み合わせたサブシステムのPL計算

この規格のこの表の使用は必須項目ではありません。この表は、*PFH*d値がわからない場合に非常に簡単な最悪の場合の代替方法を提供することを意図しています。システムのPLは、SISTEMAを含むその他の方法によって計算できます。この表の論理的根拠は明白です。第一に、システムはその最も弱いサブシステムと同じ性能しか得ることができません。第二に、多くのサブシステムがあればあるほど、故障の可能性は高くなります。

以下の図に示すシステムでは、最も低い安全遂行レベルはサブシステム1および2であり、両方ともPLbです。そのため、この表を使用すると、PLlow列がbでNlow列が2となる行を探せば、PL列から達成されるシステムのPLがbであることが分かります。3つのサブシステムがすべてPLbである場合は、達成されるPLはPLaとなります。

連続するサブシステムがPLbシステムとなる組合わせ

妥当性確認

安全機能の妥当性確認には、達成される安全遂行レベルの妥当性確認が含まれ、さらにそれ以上が要求されます。その目的は、実装された安全機能が実際に機械の全体的な安全要求事項に適合していることを検証することにあります。妥当性確認は、安全システムの開発および立上げプロセス全体を通じて重要な役割を果たします。ISO/EN 13849-2:2012では、妥当性確認の要件が設定されています。妥当性確認では、妥当性確認の計画が要求され、フォルトツリー解析や故障モード、影響および致命度解析などのテストや分析技法が検討しています。これらの要件のほとんどは、サブシステムのユーザではなく、サブシステムの製造メーカに適用されます。

機械の立上げ

システムまたは機械の立上げ段階では、安全機能の妥当性確認はすべての動作モードで実施する必要があり、すべての正常な状態と予想される異常な状態を網羅しなければなりません。入力の組み合わせや動作の順序も、考慮しなければなりません。この手順が重要なのは、システムが実際の動作および環境特性に適していることを確認することが常に必要となるためです。これらの特性の中には、設計段階の予想とは異なるものもあります。

第8章: IEC/EN 62061に準拠したシステム設計

IEC/EN 62061「機械類の安全 – 安全関連の電気、電子およびプログラマブル電子制御システムの機能安全」は、IEC/EN 61508規格を機械分野固有の要件に特化したものです。この規格は、すべてのタイプの機械の安全関連の電気制御システムや複雑ではないサブシステムまたはデバイスの設計にも適用される要件を規定しています。

リスクアセスメントからリスク低減ストラテジが決定され、そこから安全関連制御機能の必要性を特定することができます。これらの機能を文書化し、以下の内容を含める必要があります。

- 機能要求の仕様
- 安全整合性の要件の仕様

機能要件には、動作の頻度、要求される応答時間、動作モード、デューティサイクル、動作環境、およびフォルト応答機能などの詳細が含まれます。安全整合性要件は、安全度水準(SIL)と呼ばれるレベルで表されます。システムの複雑さに従って、以下の表の一部またはすべての要素を考慮して、システム設計が必要なSILを満たしているかを確認する必要があります。

SILの検討項目	シンボル
単位時間当たりの危険側故障確率	PFH_D
ハードウェア·フォルト·トレランス	HFT
安全側故障割合	SFF
プルーフテスト間隔	T_1
診断テスト間隔	T_2
共通原因故障(CCF)に対する影響	β
自己診断率(DC)	DC

SILの検討項目

サブシステム

IEC/EN 62061規格では、「サブシステム」という用語は特別な意味を持っています。サブシステムは、システムを細分化した場合の最上位の単位であり、サブシステムで発生した故障は安全機能の故障の原因になります。したがって、1つのシステム内で2つの冗長スイッチを使用している場合には、どちらのスイッチも単独ではサブシステムになりません。サブシステムは、両方のスイッチと、関連する障害診断機能で構成されます。

単位時間当たりの危険側故障確率(PFH_D)

IEC/EN 62061では、(EN) ISO 13849-1のセクションで説明したのと同じ基本的な方法を使用してコンポーネントレベルの故障発生確率を判断できます。同じ対策と方法が、「機械的」および電子的コンポーネントに適用されます。IEC/EN 62061では、年単位の$MTTF_D$を考慮していません。単位時間当たりの故障発生確率(λ)は、直接計算するか、または以下の計算式を使用してB10値から導かれます。

$\lambda = 0.1 \times C/B10$ (この場合は、C = 単位時間当たりの動作サイクル数)

サブシステムまたはシステムのPFH_Dの合計を判断する方法については、規格ごとに大きな違いがあります。サブシステムの故障発生確率を判断するには、コンポーネントの分析を行なう必要があります。共通するサブシステムのアーキテクチャの計算のために、簡略化した式を提供します(後述)。これらの計算式が適用されない場合は、マルコフモデルなどのより複雑な計算方法を使用する必要があります。次に、各サブシステムの危険側故障確率(PFH_D)を合計して、システム全体の合計のPFH_Dを決定します。次に、この規格の表3を使用して、そのPFH_Dの範囲がどの安全度水準(SIL)が対応しているかを判断できます。

SIL (安全度水準)	PFH_D (単位時間当たりの危険側故障発生確率)
3	$\geqq 10^{-8} \sim < 10^{-7}$
2	$\geqq 10^{-7} \sim < 10^{-6}$
1	$\geqq 10^{-6} \sim < 10^{-5}$

SILに対応する危険側故障確率

サブシステムのPFH_Dデータは、通常、製造メーカによって提供されます。ロックウェル・オートメーションの安全コンポーネントおよびサブシステムのデータは、以下のページから入手できます。
*www.rockwellautomation.com*にアクセスしてから、Solutions & Services→Safety Solutionsを選択して表示したページ

また、IEC/EN 62061では、必要に応じて信頼性データハンドブックも使用できることが明記されています。

あまり複雑ではない電気機械式のデバイスでは、故障が発生するメカニズムは、通常、時間だけではなく、作動の回数と頻度に関連するのが普通です。そのため、これらのコンポーネントでは、データは何らかの寿命テスト((EN) ISO 13849-1に関する章で説明されているB10テストなど)から得られます。次に、B10dまたは同様のデータをPFH_Dに変換するために、予測年間作動回数などのアプリケーションベースの情報が必要です。

注: 一般的に、次の式が当てはまります(年を時間に換算する係数を考慮する)。

$PFH_D = 1/MTTF_D$

ただし、デュアル・チャネル・システム(診断機能付きまたはなし)では、1/PFH_Dを使用して(EN) ISO 13849-1で要求されるMTTF$_D$を判断することは正しくないことを理解しておく必要があります。この規格は、シングルチャネルのMTTF$_D$用です。これは、自己診断率(DC)の効果を含む2チャネルサブシステムの両方のチャネルを組み合わせたMTTF$_D$とはまったく異なる値です。

アーキテクチャによる制約

IEC/EN 62061の重要な特性は、安全システムをサブシステムに分割することです。サブシステムに付与できるハードウェア安全度水準は、PFH_Dだけでは制限できませんが、ハードウェア・フォルト・トレランスやサブシステムの安全側故障割合によって制限されます。ハードウェア・フォルト・トレランスは、単一のフォルトが存在しているときにシステムが機能を実行できる能力です。フォルトトレランスが0というのは、単一フォルトが発生した場合、機能が実行されないことを意味します。フォルトトレランスが1のとき、サブシステムは単一フォルトが発生していても機能を実行できます。安全側故障割合(SFF)は、全体的な故障率の中で、危険な故障につながらない故障の割合です。この2つの要素を組み合わせたものが、いわゆるアーキテクチャによる制約で、SIL付与制限(SIL CL)と表されます。以下の表に、アーキテクチャによる制約とSIL CLの関係を示します。サブシステム(およびそのシステム)は、この規格やその他の関連する条項と共に、PFH_D要件とアーキテクチャによる制約の両方を満たす必要があります。

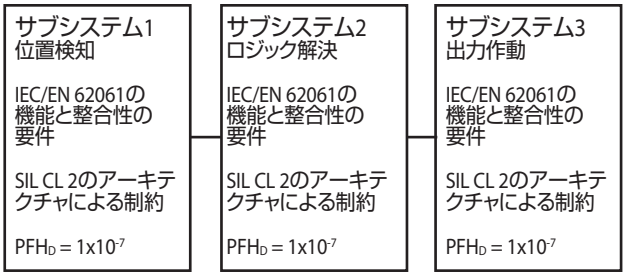
安全側故障割合 (SFF)	ハードウェア・フォルト・トレランス		
	0	1	2
60%未満	特定の例外事項を適用しない限り、許可されない	SIL1	SIL2
60～90%	SIL1	SIL2	SIL3
90～99%	SIL2	SIL3	SIL3
99%以上	SIL3	SIL3	SIL3

アーキテクチャによる制約とSIL CLの関係

例えば、シングル・フォルト・トレランスを備えて、安全側故障割合が75%のサブシステムアーキテクチャは、危険側故障確率に関係なく、SIL2定格以下に制限されます。サブシステムを組み合わせているときは、SRCSに適合するSILは、安全関連制御機能に関与するサブシステムの最も低いSIL CL以下に制限されます。

システムの実現

危険側故障の発生確率を計算するには、各安全機能をファンクションブロックに分割する必要があり、これがサブシステムになります。多くの安全機能のシステム設計では、検知装置をロジックデバイスに接続し、そのロジックデバイスをアクチュエータに接続しています。これで、サブシステムが直列に配置されます。これまで見てきたように、サブシステムごとに危険側故障確率を決定でき、SIL CLがわかっている場合、システムの故障の発生確率は、サブシステムの故障の発生確率を加算するだけで簡単に計算できます。以下の図にこの概念を示します。



$= PFH_D^1$ $+ PFH_D^2$ $+ PFH_D^3$
$= 1x10^{-7}$ $+ 1x10^{-7}$ $+ 1x10^{-7}$
$= 3x10^{-7}$ (SIL2に適合)

例えば、SIL 2に適合したい場合、各サブシステムには最低でもSIL 2のSIL付与制限(SIL CL)を持つ必要があり、システムのPFH_Dは、「SILの危険側故障確率」を示す前記の表で許容可能な制限を超えてはなりません。

サブシステムの設計 – IEC/EN 62061

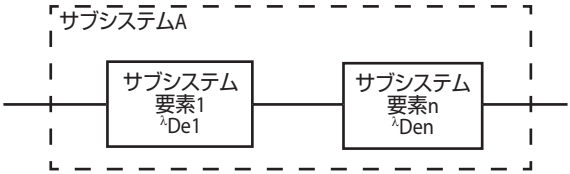
システム設計者がIEC/EN 62061に従ってあらかじめサブシステムに「パッケージ化」されたコンポーネントを使用すると、サブシステム設計に関する特定の要件を適用せずに済むため、作業はかなり簡単になります。これらの要件は、通常、デバイス(サブシステム)の製造メーカによって実施され、システムレベルの設計に要求されるものよりもはるかに複雑になっています。

IEC/EN 62061は、セーフティPLCなどの複雑なサブシステムがIEC 61508またはその他の該当する規格に適合することを要求しています。つまり、複雑な電子的またはプログラム可能なコンポーネントを使用するデバイスについては、IEC 61508の厳格さがすべてに適用されることを意味します。これは非常に困難で、複雑な工程になる可能性があります。例えば、複雑なサブシステムによって達成されたPFH_Dの評価は、マルコフモデルや信頼性ブロックダイアグラム、フォルトツリー解析などの手法を使用する非常に複雑なプロセスとなる可能性があります。

IEC/EN 62061は、それほど複雑ではないサブシステムの設計に対する要件を規定しています。これには、通常、インターロックスイッチや電気機械式のモニタ・セーフティ・リレーなどの比較的単純な電気コンポーネントが含まれます。この要件にはIEC 61508の要件のような関係性はありませんが、それでもかなり複雑です。

IEC/EN 62061は、あまり複雑ではないサブシステムによって実現されるPFH_Dを評価するために使用できる式が付属する4つのサブシステム論理アーキテクチャを提供しています。これらのアーキテクチャは純粋に論理的な表現であり、物理構造とは考えないでください。4つのサブシステム論理アーキテクチャとそれに付属する式を、以下の4つの図に示します。

以下の図に示す基本的なサブシステムアーキテクチャでは、危険側故障確率は合計するだけで求めることができます。

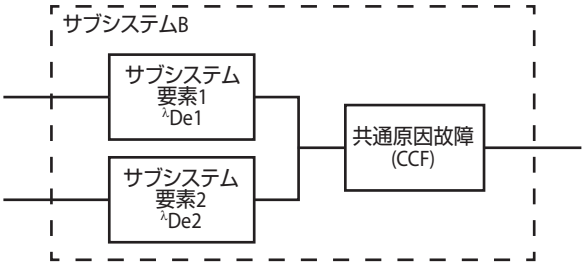


サブシステムの論理アーキテクチャA

$\lambda DssA = \lambda De1 + \cdots + \lambda Den$
$PFHDssA = \lambda DssA$

λ (ラムダ)は、故障の発生確率を指定するために使用されます。故障の発生確率の単位は、単位時間当たりの故障発生回数です。λDは、危険側故障発生確率です。$\lambda DssA$は、サブシステムλの危険側故障発生確率です。これは、個別の要素e1、e2、e3から最大enまでの故障の発生確率の合計です。危険側故障発生確率に1時間を掛けると、1時間当たりの故障発生確率になります。

以下の図に、診断機能を持たないシングル・フォルト・トレラント・システムを示します。アーキテクチャにシングル・フォルト・トレランスが組み込まれている場合、共通原因故障の可能性があるので考慮する必要があります。共通原因故障の派生については、この章の後半で詳しく説明します。



サブシステムの論理アーキテクチャB

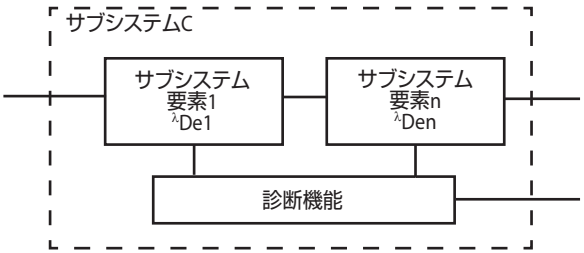
$DssB = (1-\beta)^2 \times \lambda De1 \times \lambda De2 \times T1 + \beta \times (\lambda De1 + \lambda De2)/2$
$PFHDssB = \lambda DssB$

このアーキテクチャの式では、サブシステム要素の並列配置を考慮するため、前の表「SIL検討項目」から以下の2つの要素が追加されています。

β - 共通故障原因(CCF)に対する影響

T1 - プルーフテスト間隔または寿命のうちいずれか小さい方。プルーフテストは、フォルトと安全サブシステムの劣化を検出するように設計されています。これによって、サブシステムを動作可能な状態に回復させることができます。実際には、通常、これは交換時期を意味します((EN) ISO 13849-1の「ミッション時間」の用語と同等)。

以下の図に、診断機能を備えた0のフォルト・トレランス・システムの機能を説明します。自己診断率(DC)は、危険側ハードウェア故障発生確率を低下させるために使用されます。診断テストは自動的に実行されます。自己診断率の定義は、(EN) ISO 13849-1での定義と同じで、すべての危険側故障確率に対する検出された危険側故障確率の比率を示します。

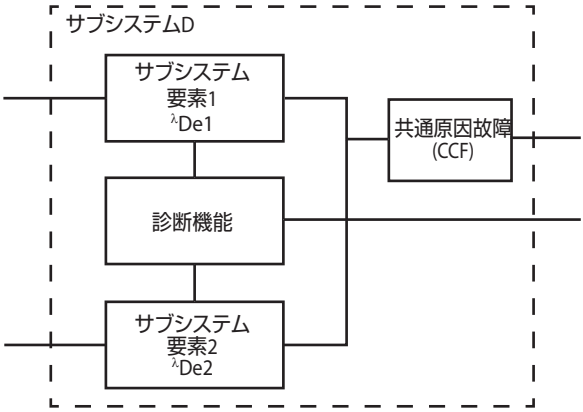


サブシステムの論理アーキテクチャC

$\lambda DssC = \lambda De1\ (1\text{-}DC1) + \cdots + \lambda Den\ (1\text{-}DCn)$
$PFHDssC = \lambda DssC$

これらの式には、サブシステムの要素ごとの自己診断率(DC)が組み込まれています。各サブシステムの故障の発生確率は、各サブシステムの自己診断率によって低減されます。

以下に、サブシステムのアーキテクチャの4番目の例を示します。このサブシステムはシングル·フォルト·トレラントで、診断機能を備えています。シングル·フォルト·トレラント·システムでは、共通原因故障の発生確率も考慮する必要があります。



サブシステムの論理アーキテクチャD

サブシステムの要素が異なる場合は、以下の式を使用します。

$\lambda DssD = (1-\beta)2\{[\lambda De1 \times \lambda De2 \times (DC1+DC2)] \times T2/2 + [\lambda De1 \times \lambda De2 \times (2-DC1-DC2)] \times T1/2\} + \beta \times (\lambda De1 + \lambda De2)/2$
$PFHDssD = \lambda DssD$

サブシステムの要素が同じ場合は、以下の式を使用します。

$ADssD = (1-\beta)^2\{[\lambda De^2 \times 2 \times DC] \times T2/2 + [\lambda De^2 \times (1-DC)] \times T1\} + \beta \times \lambda De$
$PFHDssD = \lambda DssD$

両方の式に、1つの追加のパラメータT2(診断テストの間隔)が使用されていることに注意してください。これは機能の定期的チェックだけを行なう、プルーフテストより範囲が広くないテストです。

サブシステムの要素が同じ場合の例として、例えば以下の値を想定しています。

$\beta = 0.05$

$\lambda De = 1 \times 10^{-6}$ 故障/時間

T1 = 87600時間(10年)

T2 = 2時間

DC = 90%

$PFHDssD = 5.790E\text{-}8$ 単位時間当たりの危険側故障発生確率 これは、SIL3に要求される範囲内にあります。

プルーフテスト間隔の影響

IEC/EN 62061は、プルーフテストの間隔(PTI)を20年にすることを推奨しています(必須ではない)。プルーフテストの間隔がシステムに及ぼす影響を見てみましょう。20年のときにT1で式を再計算すると、結果はPFHDssD = 6.581E-08になります。これでもまだSIL 3に要求される範囲内です。設計者が、全体の危険側故障の発生確率を計算するには、このサブシステムと他のサブシステムを組み合わせる必要があることを常に注意してください。

共通原因故障の影響の分析

共通原因故障がシステムに及ぼす影響を見てみましょう。プルーフテストの間隔を20年のままにして、追加対策を講じてβ (ベータ)の値が1% (0.01)に改善したと仮定します。危険側故障の発生確率が2.71E-8に向上し、これでサブシステムがSIL 3システムに適合できるようになりました。

共通原因故障(CCF)

共通原因故障とは、1つの原因から複数のフォルトが発生し、危険な故障につながることを意味します。CCFに関する情報が必要になるのは、サブシステム設計者(通常、製造メーカ)だけです。この情報は、サブシステムのPFH_Dの評価に使用される式の一部として使用されます。通常、システム設計レベルでは必要ありません。

IEC/EN62061の付属書Fには、CCFを推定するための簡単な方法が記載されています。以下の表に、スコアリングプロセスの概要を示します。

番号	CCFの対策	スコア
1	隔離/分離	25
2	ダイバーシティ(多様性)	38
3	設計/アプリケーション/経験	2
4	評価/分析	18
5	能力/トレーニング	4
6	環境	18

共通原因故障防止(CCF)に対する対策のスコアリング

特定のCCF対策を採用するとポイントが与えられます。スコアを合計して、共通原因故障(β)の係数を決定します。以下の表に、この係数を示します。β係数はサブシステムモデルで使用され、故障の発生確率を「調整」します。

全体のスコア	共通原因故障の係数(β)
35未満	10% (0,1)
35～65	5% (0,05)
65～85	2% (0,02)
85～100	1% (0,01)

共通原因故障のベータ係数

自己診断率(DC)

自動診断テストは、危険側ハードウェア故障発生確率を減少させるために使用されます。危険側ハードウェア故障をすべて検出できることが理想ですが、実際には最大値は99%に設定されています(これは0.99とも表現される)。

自己診断率は、すべての危険側故障発生確率に対する検出された危険側故障発生確率の比率です。

$$DC = \frac{\text{検出された危険側故障発生確率}(\lambda)_{DD}}{\text{すべての危険側故障発生確率}(\lambda)_{Dtotal}}$$

自己診断率の値の範囲は、0～99%です。

ハードウェア・フォルト・トレランス

ハードウェア・フォルト・トレランスは、危険側故障を引き起こす前にサブシステムが耐えることができるフォルトの数を表します。例えば、ハードウェア・フォルト・トレランスが1であると、フォルトが2つあると安全関連制御機能の損失につながりますが、フォルトが1つなら安全関連制御機能を失わないことを意味します。

機能安全の管理

規格には、安全関連電気制御システムの機能安全を実現するために必要な管理の制御および技術活動に関する要件が規定されています。

プルーフテスト間隔

プルーフテスト間隔とは、「新品同様」の状態にしておくために全面的なチェックまたは交換が必要になる間隔を表します。実際には、機械分野では交換時期を意味します。そのため、プルーフテスト間隔は、通常、製品の寿命と同義になります。(EN) ISO 13849-1では、この時間はミッション時間ともいいます。

プルーフテストとはSRCSのフォルトおよび劣化を検出するチェックのことで、これによってSRCSをできる限り「新品同様」に近い状態に回復させることができます。プルーフテストは、診断機能(存在する場合)を含むすべての危険側障害を100%検出する必要があります。個々のチャネルは個別にテストする必要があります。

自動的に行なわれる診断テストとは異なり、プルーフテストは通常、手作業によりオフラインで実行されます。自動で行なわれる診断テストは頻繁に実行されますが、それに比べるとプルーフテストはあまり頻繁には行なわれません。例えば、ガード上のインターロックスイッチにつながる回路は、診断テスト(パルスなど)によって短絡や開回路状態を自動的にテストすることができます。

プルーフテストの間隔は、製造メーカが明示しなければなりません。場合によっては、製造メーカがさまざまなプルーフテスト間隔を示すことがあります。実際にプルーフテストを実行するより、サブシステムを新しいものに交換するほうが一般的です。

安全側故障割合(SFF)

安全側故障割合は自己診断率(DC)に似ていますが、本来安全な状態に終わる傾向のある故障も考慮に入れています。例えば、ヒューズが飛んだ場合、故障は存在しますが、その故障はほぼ確実に開回路であるため、ほとんどの場合は安全な故障であるのは確実です。SFFは、(安全側故障の発生確率と検出できる危険側故障の発生確率の合計)を、(安全側故障の発生確率と検出·未検出を合わせた危険側故障の発生確率の合計)で割って計算します。安全機能に何らかの影響を与えるタイプの障害だけを考慮していることに注意してください。

通常、SFF値はそれが適切であれば製造メーカによって明示されます。

安全側故障割合(SFF)は、以下の式を使用して計算できます。

$$SFF = (\Sigma\lambda S + (\Sigma\lambda DD)/((\Sigma\lambda S + (\Sigma\lambda D)$$

この場合、以下のようになります。

$\sum S$ = 安全側故障の発生確率

$\sum\lambda S + \sum\lambda D$ = 全体の故障の発生確率

λDD = 検出された危険側故障の発生確率

λD = 危険側故障の発生確率

系統的故障

規格には、系統的故障の制御および回避に関する要件が記載されています。系統的故障は、ランダムハードウェア故障とは異なります。ランダムハードウェア故障は、一般的にハードウェア部品の何らかの劣化が原因で時間的に無秩序に発生する故障です。考えられる系統的故障の一般的なタイプは、ソフトウェア設計エラー、ハードウェア設計エラー、要件仕様エラー、操作手順などです。系統的故障を回避するために必要な対策の例を、以下に示します。

- コンポーネントの適切な選択、組み合わせ、配置、組立て、および設置
- 優れた技術的手法を使用
- 製造メーカの仕様および取付け手順に従う
- コンポーネント間の互換性を確認
- 環境条件への耐性を考慮
- 適切な材質を使用

第9章: 安全関連制御システムの構造に関する注意事項

概要

この章では、安全関連制御システムを設計する際に考慮すべき一般的な構造的な注意事項と原理について説明します。

制御システムのカテゴリ

制御システムの「カテゴリ」が使用されるようになったのは、旧規格EN 954-1:1996 (ISO13849-1:1999)からです。ただし、この用語は安全制御システムの構造を説明するために現在でもしばしば使用されており、指定アーキテクチャとして(EN) ISO13849-1の不可欠な部分として存続しています。カテゴリの説明と要件については、本書の「(EN) ISO 13849-1の概要」で説明しています。この章では、カテゴリ構造の実装方法に関する簡略で実用的な指針を記さしています。

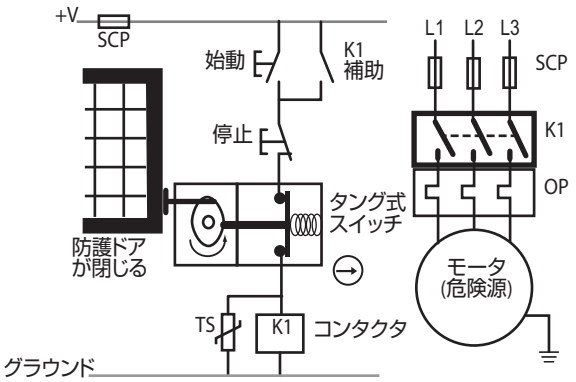
カテゴリB

カテゴリBは、その他すべてのカテゴリが構築される基礎と見なされます。(EN) ISO 13849-2の付属書A～Dに規定された基本的な安全原理以外の特別ないかなる規定または構造もありません。これらは設計および材質の選択における優れた一般的な慣行を示しています。

カテゴリ1

カテゴリ1は、十分に検証されたコンポーネントおよび十分に検証された安全原理を求めています。

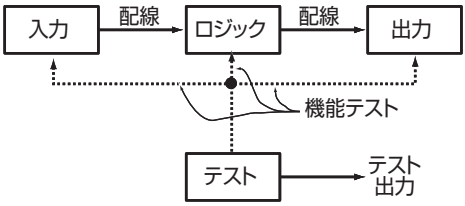
カテゴリ1を実現するための標準的なシステムを以下に示します。インターロックとコンタクタは、危険源にアクセスする必要がある場合にモータからエネルギーを除去するために重要な役割を果たします。タング式インターロック(円の中に矢印の記号で示す)は、IEC 60947-5-1の直接開動作接点に関する要件を満たします。十分に検証されたコンポーネントを使用することにより、カテゴリ1ではカテゴリBよりもエネルギーが除去される確率が高くなります。十分に検証されたコンポーネントを使用すれば、安全機能の損失の可能性を最小限に抑えることができますが、それでも単一のフォルトが安全機能の損失を引き起こす可能性がゼロではないことに注意してください。



単純なカテゴリ1の安全システム

カテゴリ1は、信頼性の高いコンポーネントを用いた単純な設計を使用することにより故障を防止することを意図しています。このタイプの防止策だけでは十分なリスク低減をもたらさない場合は、フォルト検出を使用する必要があります。カテゴリ2、3および4は故障またはフォルト検出に基づき、より厳格な要件によってさらに高いレベルのリスク低減を実現します。

カテゴリ2



カテゴリBの要件を満たし十分に検証された安全原理を使用することに加えて、安全システムはカテゴリ2を満たすための適合テストを受ける必要があります。このテストは、制御システムの安全関連部分のフォルトを検出するように設計する必要があります。フォルトが検出されなければ、その機械は実行を許可されます。フォルトが検出された場合は、フォルト対応機能によって機械を確実に安全状態に維持する必要があります。

このテストを実行する機器は、安全システムの不可分の一部である場合も、別の機器である場合もあります。

このテストは以下のときに実行する必要があります。

- 機械が最初に電源を投入したとき
- 危険な作業を開始する前
- リスクアセスメントによって必要と判断された場合は定期的に実行

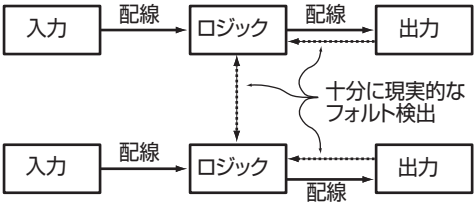
注: (EN) ISO 138491-1では、安全機能の需要割当が100:1のテスト、またはフォルトを検出し、機械が危険源に到達するより短い時間内に機械を停止する能力を備えた安全機能の要求に対応するテストを想定しています。

本質的に、安全システムまたはサブシステムは、その安全機能が正しく機能しているかをテストするために実行する必要があります。このことは機械的な特性を持つテクノロジを用いて実現することは困難または不可能となる場合があることを意味します。通常、カテゴリ2の手法は電子技術に対してより適切に使用されます。PLdについては、フォルトが検出された場合に安全状態を起動することが可能なテスト出力が存在しなければなりません。

カテゴリ3

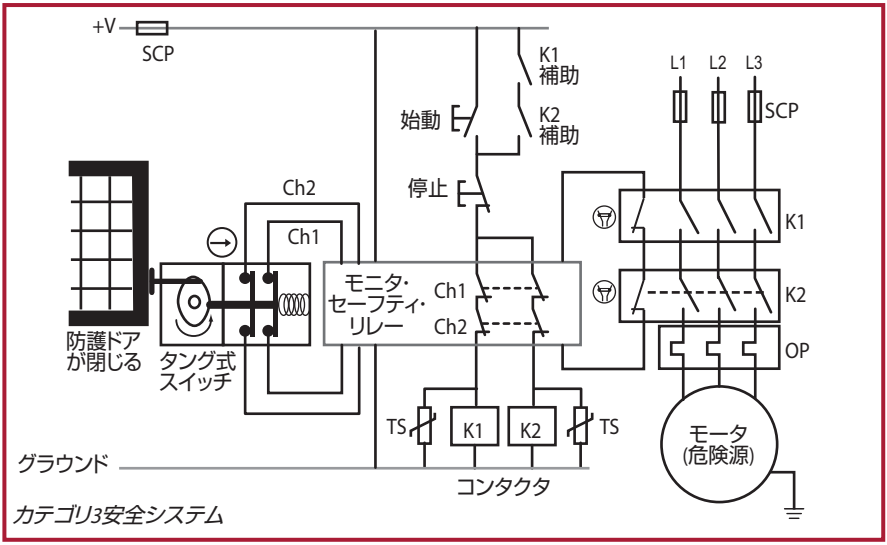
カテゴリBの要件を満たし十分に検証された安全原理を使用することに加えて、カテゴリ3は単一のフォルトが存在しても安全機能が正常に実行できることが要求されます。安全機能に次の要求が出されたとき、または要求が出される前に、可能な限りフォルトの検出を行なう必要があります。

クロスフォルトなど、直ちに安全機能を失う原因とはならない一部のフォルトは、検出されない場合があります。つまり、カテゴリ3では未検出フォルトの累積が安全機能の損失をつながる可能性があります。



これは、カテゴリ3のシステムの原理を説明するブロックダイアグラムです。冗長にクロスモニタと出力モニタを組み合わせて使用すると、安全機能を確実に実行できるようになります。

安全関連制御システムの構造に関する注意事項



カテゴリ3安全システム

上の図は、カテゴリ3のシステムの例です。タング式インターロックスイッチには、接点の冗長セットがあります。内部的に、モニタ·セーフティ·リレー(MSR)には相互にクロスモニタを行なう冗長回路が含まれています。コンタクタの冗長セットがモータから電力を除去します。これらのコンタクタは、機械的にリンクされた接点を介してMSRによってモニタされます。

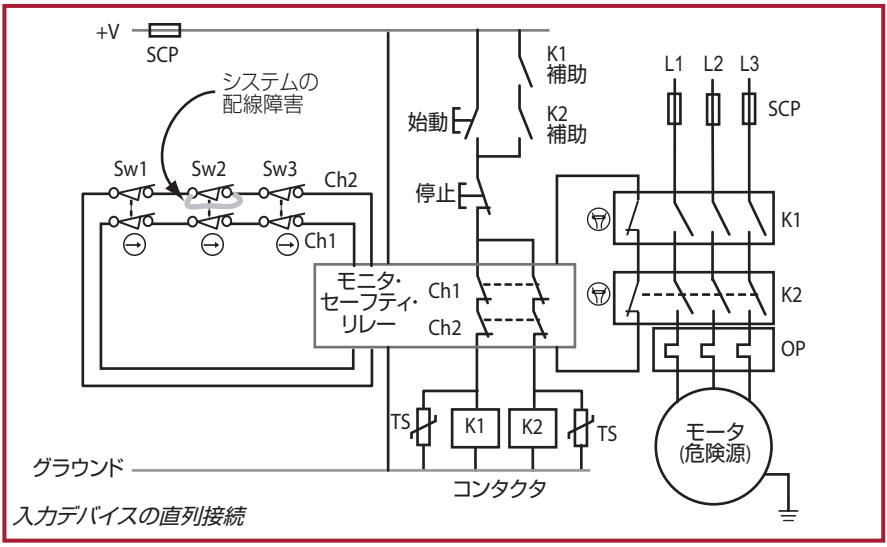
フォルト検出は、安全システムの各部分で考慮する必要があります。デュアル·チャネル·タング式スイッチの故障モードとはどのようなものか? MSRの故障モードとはどのようなものか? コンタクタK1およびK2の故障モードとはどのようなものか? 配線の故障モードとはどのようなものか?

カテゴリ3の回路では、冗長電気接点セットを備えた1つのタング式インターロックスイッチを使用することが一般的です。このことは、作動リンケージ内の単一コンポーネントのフォルトを排除する必要がある可能性を意味します。このフォルトが排除できない場合は、単一のフォルトが安全機能を損失する原因になる可能性を意味します。あらゆるフォルト排除が完全に正当化されることが極めて重要になります。

モニタ·セーフティ·リレー(MSR)は、タング式インターロックスイッチやコンタクタにフォルト診断機能を提供します。また、MSRは手動リセットなどのその他の機能も支援できます。内部アーキテクチャの観点から、モニタ·セーフティ·リレーは通常、PLeまたはSIL3に相当します。

2つのコンタクタは、過負荷保護および短絡保護を備える必要があります。接点溶着によってコンタクタが故障する可能性は小さくなりますが、可能性がないわけではありません。コンタクタは、アマチャの固着によって電源切換え接点が閉じた場合も故障することがあります。1つ目のコンタクタが故障して危険な状態になっても、2つ目のコンタクタが正常に動作を続け、モータから電力を除去します。MSRは、次のマシンサイクルでフォルトが発生したコンタクタを検出します。ゲートが閉じられているときに始動ボタンが押されると、故障したコンタクタの機械的にリンクされた接点が開いたままになり、MSRは安全接点を閉じることができず、それによってフォルトが明らかになります。

検出されないフォルト



入力デバイスの直列接続

カテゴリ3のシステム構造を使用すると、検出はできないけれどもそれ自体では安全機能の損失を引き起こさないフォルトが発生する場合があります。フォルトが検出できる場合は、特定の状況で、システム構造内の他のデバイスの動作によって覆い隠されたり、または意図せずにクリアされることがあるかを知っておく必要があります。

上の図に、複数のデバイスをモニタ・セーフティ・リレーに接続するために広く使用されている方法を示します。各デバイスには、2つの通常閉の直接開動作接点が組み込まれています。この方法では、入力デバイスはデイジーチェーン接続されるため配線コストを節約できます。上図のSw2の接点の1つで短絡フォルトが発生していると仮定します。このフォルトは検出できるでしょうか?

スイッチSw1(またはSw3)が開いている場合、Ch1およびCh2の両方が回路を開き、MSRが危険源から電力を除去します。その後、Sw3が開いてから再び閉じても、MSRのステータスが変わっていない(Ch1およびCh2の両方が開いたままになっている)ため、その接点のフォルトは検出されません。Sw1(またはSw3)が閉じると、始動ボタンを押して危険源を再起動できます。これらの状況では、フォルトによって安全機能が失われることはありませんが、検出されずシステム内にフォルトが存在するままになり、その後のフォルト(Sw2の2番目の接点での短絡)によって安全機能が失われることになります。

Sw2だけが開くいてから閉じて、他のスイッチが動作しない場合、Ch1は開いて、Ch2が閉じたままになります。MSRは、Ch1が開いたため、危険源の電力を除去します。Sw2が閉じると、Ch2が開いていないため、始動ボタンを押してもモータを起動できません。フォルトが検出されます。ただし、何らかの理由でSw1(またはSw3)が開いてから閉じると、Ch1およびCh2の両方が開いてから回路を閉じます。このシーケンスはフォルトのクリアに似ていて、MSRで意図しないリセットが起こることがあります。

このことは、(EN) ISO 13849-1またはIEC 62061を使用しているときに、この構造内で個々のスイッチに関してDCは何を求めるかという問題を提起します。ISO TR 24119 (2015年11月: Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts (ガードに関連するインターロック装置のフォルトを隠蔽する無電圧接点での直列接続に関する評価))が発行されるまでは、このことに関して特に決定的な指針も存在せず、フォルトを発見するために適切な時期にスイッチが個別にテストされるという条件で60%のDCが一般的に想定されていました。スイッチの1つ(または複数)が個別にテストされていないことが予測できるときは、そのDCが0であるべきかを検討できます。ISO TR 24119では、直列に接続された無電圧接点を使用するガードインターロック装置のDCの決定に関する詳細な指針が規定されています。以下の表に、基本的な概要を示します。特定のアーキテクチャおよびアプリケーションに関する実際の最大許容DCを決定するには、この規格の資料を十分に調査することが不可欠です。

頻繁に使用される可動式ガードの数[1]	追加の可動式ガードの数	隠蔽される可能性	自己診断率 (DC)	達成可能な最大のPL
0	2〜4	低	中	PL d
	5〜30	中	低	PL d
	30を超える	高	なし	PL c
1	1	低	中	PL d
	2〜4	中	低	PL d
	≥5	高	なし	PL c
1を超える	--	高	なし	PL c

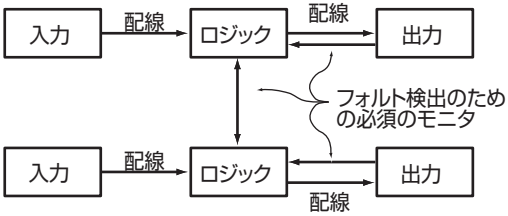
[1] 切換え頻度は1時間に1回より多い

電気機械的な接点の直列接続は最大PLdに制限され、特定の場合は、最大PLcに制限することができます。いずれの場合でも、フォルトの隠蔽が発生することが予測される場合は(複数の可動式ガードが通常の動作または修理の一部として同時に開く場合など)、DCは0に制限されることに注意してください。

興味深いのは、カテゴリ3構造のこれらの特性は常に考慮を必要としますが、これらが機能安全規格によって詳しく解明されていることです。

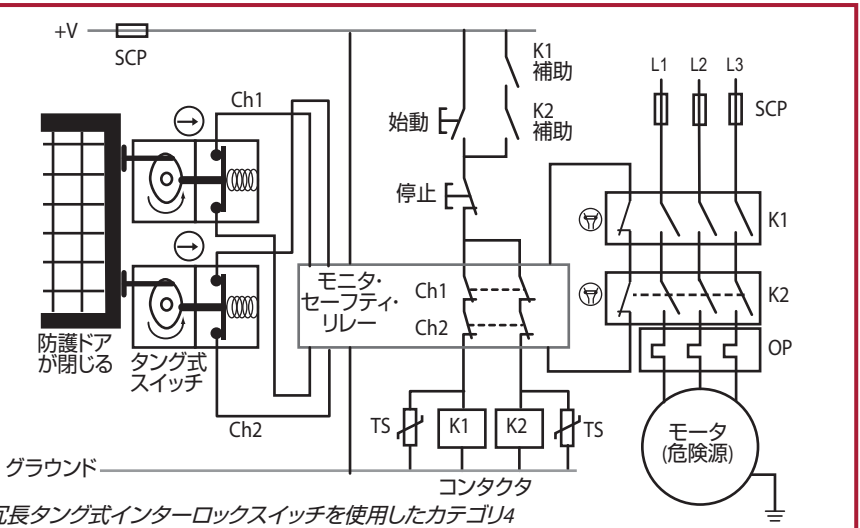
カテゴリ4

カテゴリ3と同様に、カテゴリ4は安全システムがカテゴリBの要件を満たし十分に検証された安全原理を使用し、単一のフォルトが存在しても安全機能が正常に実行されることを求めています。フォルトの累積が安全機能の損失につながる可能性があるカテゴリ3とは異なり、カテゴリ4はフォルトが累積した状態であっても安全機能が正常に実行できることが要求されます。実際には、通常、高度の診断によってこれが達成され、すべての関連するフォルトの累積が可能になる前に確実に検出されます。理論的なフォルトの累積を考慮する場合は2つのフォルトを考慮すれば十分ですが、設計によっては3つのフォルトを考慮することが必要になる場合もあります。



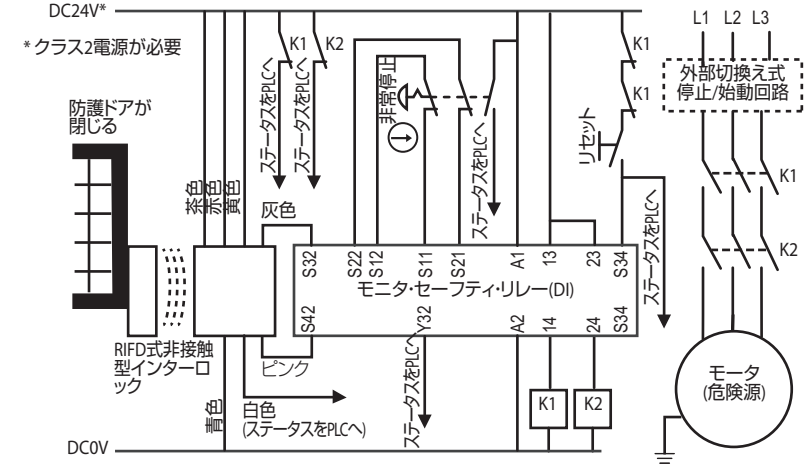
上の図は、カテゴリ4のブロックダイアグラムを示しています。両方の出力デバイスのモニタおよびクロスモニタが必要です。カテゴリ4は、カテゴリ3よりも高い自己診断率(DC)となります。比較的最近まで、2つの電気チャネルを備えた単一のタング式インターロックスイッチは、カテゴリ4の回路での使用が考慮されてきました。

安全関連制御システムの構造に関する注意事項



冗長タング式インターロックスイッチを使用したカテゴリ4

デュアルチャネル回路で1つのタング式インターロックを使用するには、機械作動式タングとスイッチのリンケージでの考えられる単一のフォルト故障点を除外する必要があります。ただし、『Joint Technical Report ISO TR 23849』では、このタイプのフォルト排除はPLeまたはSIL 3システムでは使用すべきではないと明記されています。安全システムの設計者がタング式インターロックを使用したい場合には、2つの個別のスイッチを使用してカテゴリ4の要件を満たすことができます。最新技術では、カテゴリ4 (およびPLe / SIL 3)のアーキテクチャを実現するために別の方法が採用されています。



RFID式電子非接触型インターロックを使用したカテゴリ4

複雑な電子部品を使用することによって、フォルトトレランスや高レベルの自己診断率を1つのデバイスにコスト効率良く組み込むことができるようになりました。図に示すインターロック装置はカテゴリ4を達成するだけでなく、RFIDコーディングの使用により極めて高度な不正操作(オーバライド)防止機能も提供します。また、カテゴリや自己診断率を低下させることなく、他のよく似たデバイスと直列に接続することもできます。

コンポーネントのPL (安全遂行レベル)およびシステム定格

(EN) ISO 13849の指定アーキテクチャ(カテゴリ)は、システムのPL定格だけでなく安全コンポーネント(デバイス)のPL定格の一部としても使用できます。これによって生じる多少の混乱は、コンポーネントとその機能を理解することで解明できます。前記の例を詳しく調べることによって、カテゴリ1に定格されたインターロックスイッチなどのコンポーネントは、そのままでカテゴリ1のシステムで使用できることが分かります。

これらのコンポーネントの2つをモニタ・セーフティ・リレーによって提供される診断機能と組合わせて使用すると、カテゴリ3または4のシステムの一部を形成することもできます。

モニタ・セーフティ・リレーやプログラマブル・セーフティ・コントローラなどの一部のコンポーネントには独自の内部診断機能があり、自己チェックを実行して適切な動作を保証します。したがって、これらは安全コンポーネントとして定格され、特に対策を追加しなくてもカテゴリ2、3または4を満たします。

フォルトに関する注意事項およびフォルト排除

安全分析には、幅広いフォルトの分析だけでなく、フォルトが存在するときの安全システムの動作について完全に理解していることが必要です。ISO 13849-1およびISO 13849-2には、フォルトの注意事項およびフォルト排除に関する詳細が規定されています。

1つのフォルトがその後に続くコンポーネントの故障を引き起こした場合は、最初のフォルトとそれに続くすべてのフォルトは単一のフォルトであると見なされます。

1つの原因の結果として複数のフォルトが発生する場合、そのフォルトは1つのフォルトであると見なされます。これは共通原因故障と呼ばれます。

2つ以上の個別のフォルトが同時に発生することはほとんどあり得ないので、この分析では考慮されません。

フォルト排除

(EN) ISO 13849-1およびIEC 62061では、安全システムの分類を決定する場合に、フォルトが発生する確率が極めて低いことが確認できれば、フォルト排除の使用が認められています。フォルト排除が使用されている場合は、その排除が適切に妥当であることと安全システムの計画されたライフタイムに対して排除が有効であることを把握しておくことは重要です。安全システムによって保護されるリスクのレベルが高ければ高いほど、フォルト排除で求められる妥当性は厳格になります。これは、特定のタイプのフォルト排除がいつ使用できるかできないかについて、何らかの混乱を生ずる原因となります。この章で説明してきたように、最近の規格と指針の文書ではこの問題のいくつかの側面について明確にしています。

一般的に、安全システムによって実現される安全機能にPLeまたはSIL3が要求される場合、ISO TR 23849では、このレベルの安全遂行レベルを達成するためにフォルト排除だけに頼ることことは一般的ではありません。これは、使用されるテクノロジと対象となる動作環境によって左右されます。したがって、PLまたはSILの定格が上がるにつれて、設計者はフォルト排除により一層の注意を払う必要があります。例えば、フォルト排除の使用は、PLeまたはSIL3のシステムを実現するために、電気機械式の位置スイッチおよび手動作動スイッチ(非常停止装置など)の機械的側面には適用されません。特定の機械的障害状態(摩耗/腐食、破壊など)に適用できるフォルト排除については、ISO 13849-2の表A.4に記載されています。したがって、PLeまたはSIL3を達成する必要があるガード・インターロック・システムでは、通常、スイッチアクチュエータの破損などのフォルトを排除することは妥当とは認められないため、この安全遂行レベルを達成するために少なくとも1のフォルトトレランス(2つの従来型の機械式位置スイッチなど)を組込む必要があります。ただし、該当する規格に準拠して設計された制御パネル内の配線の短絡などのフォルトを排除するために、これを許容できる場合があります。

IEC/EN 60204-1およびNFPA 79に準拠した停止カテゴリ

安全関連制御システムに関連する「カテゴリ」という用語には2つの異なる意味があるために、不運と混乱をまねくことがあります。もともとは、EN 954-1でカテゴリについて説明しています。カテゴリは、フォルト状態での安全システムの性能を分類したものです。

また、もとのIEC/EN 60204-1およびNFPA 79では「停止カテゴリ」と呼ばれる分類もあります。停止カテゴリには以下の3つがあります。

停止カテゴリ0では、アクチュエータへの電力供給をすぐに遮断する必要があります。一部の環境では、モータは惰性で回転し続けるため、動作が停止するのにある程度の時間がかかるため、モータは停止するまで惰性で回転するため、これは非制御停止と見なされることがあります。

停止カテゴリ1では、ブレーキを作動させるため停止するまでアクチュエータへの電力供給を継続させる必要があり、停止後にアクチュエータへの電力供給を遮断します。
注: 停止カテゴリ1aおよび1bについては、IEC 60204-1を参照してください。

停止カテゴリ2では、アクチュエータから電力供給を遮断する必要はありません。

非常停止としては、停止カテゴリ0または1しか使用できないことに注意してください。2つのカテゴリのうちどちらを使用すべきかは、リスクアセスメントによって決定します。

この章に示すすべての回路図の例には、停止カテゴリ0が使用されています。停止カテゴリ1は、最終的な電力供給の停止による時間遅延出力によって停止します。ガードロック付きのインターロックガードには、しばしばカテゴリ1の停止システムがついていることがあります。これにより、機械が安全(つまり停止)状態になるまでガードが閉じた状態にロックされます。

プログラマブルコントローラについて十分に検討しないまま機械を停止すると、再起動に影響を及ぼしたり、ツールや機械に深刻な損傷が発生することがあります。標準PLC (セーフティPLC以外)は、安全関連の停止作業には関わらないので、他の方法を考える必要があります。

以下に、カテゴリ1の停止のために考えられる2つのソリューションを示します。

1. 時間遅延オーバライドコマンド付きセーフティリレー

即時作動式と遅延作動式の両方の出力を備えたセーフティリレーが使用されます。即時作動式の出力は、プログラム可能なデバイス(PLCまたはドライブの「イネーブル」)の入力に接続され、遅延作動式の出力はメインコンタクタに接続されます。ガード·インターロック·スイッチが作動すると、セーフティ·リレー·スイッチが直ちに出力します。これで、プログラム可能なシステムに正しいシーケンスで停止を行なうために信号が送られます。このプロセスを行なうために十分な時間が経過してから、セーフティリレーの遅延出力がオンになり、メインコンタクタを遮断します。

注: 全体的な停止時間を判断するための計算では、セーフティリレー出力遅延期間も考慮する必要があります。安全距離の計算に従って装置の位置を決定するためにこの要素を使用する場合は、これが特に重要になります。

2. セーフティPLC

GuardLogixなどのセーフティPLCを使用することにより、必要なロジックおよび計時機能を簡単に実装できます。

米国の安全制御システムの要件

制御信頼性

米国およびカナダのロボット規格での最高レベルのリスク低減は、信頼できる制御の要件を満たす安全関連制御システムによって実現されます。制御信頼性の要件を満たす安全関連制御システムは、モニタ機能を備えたデュアル・チャネル・アーキテクチャです。ロボットの停止機能は、モニタ機能も含めて、いかなる単一コンポーネントの故障によっても妨げられてはなりません。

モニタ機能は、フォルト検出時に停止コマンドを生成します。動作が停止した後も危険が残る場合は、警告信号を送る必要があります。安全システムは、フォルトが解消されるまで安全な状態を保つ必要があります。できれば、フォルトが起きた時点で検出されることが望まれます。これが実現できない場合には、安全システムに次の要求が出された時点で障害が検出されなければなりません。同様の障害が発生する可能性が大きい場合は、コモンモード故障と考える必要があります。

カナダでの要件は、米国の要件に2つの追加要件が加わります。1つは、安全関連制御システムが通常のプログラム制御システムから独立していることです。もう1つは、安全システムは気づかれることなく簡単に無効化されたり、バイパスされてはいけないということです。

制御信頼性に関するコメント

制御信頼性の最も基本的なものは、シングル・フォルト・トレランスとモニタ(フォルト検出)です。この要件は、「1つの単一のフォルト」、「任意の単一のフォルト」、または「任意の単一コンポーネントの故障」が存在する場合に、どのように対応すべきかを規定しています。

フォルトに関して、以下の3つの非常に重要な概念を考慮する必要があります。
(1) すべてのフォルトを検出できるとは限らない。
(2) 「コンポーネント」という言葉が加わると、配線の問題が発生する。
(3) 配線は安全システムに不可欠な要素であり、配線障害は、安全機能の損失につながる可能性がある。

制御信頼性の目的は、フォルトが存在するときに安全機能を実行することであるのは明らかです。フォルトが検出された場合、安全システムは安全措置を実行し、フォルトを通知して、フォルトが解決されるまで機械が動作を続けないようにする必要があります。フォルトが検出されなかった場合でも、要求があれば、安全機能を実行する必要があります。

第10章: アプリケーション例

概要 – 機械用のエンジニアリング済みの安全機能

機械類の安全機能 – 非常停止であれ、ガード、または存在検知機能であれ、センサまたは入力デバイス、ロジックデバイス、および出力デバイスなどの複数の要素が必要となります。これらの要素を組み合わせて、(EN) ISO 13849-1で概説されている安全遂行レベルによって計算された保護レベルを提供します。

この章では、ロックウェル·オートメーションが開発した機械用の多くのエンジニアリング済みの安全機能の中から1つを選択しました。これらの安全機能の個々の説明書では、セットアップや配線、構成、検証および妥当性確認計画、および安全遂行レベルの計算などを含む機能要件、機器の選択、要求された安全遂行レベルに基づいた特定の安全機能に関する指針を記載しています。

エンジニアリング済みの安全機能は、ロックウェル·オートメーションのウェブサイトから無料でダウンロードできます。
*www.rockwellautomation.com*にアクセスしてから、Solutions & Services→Safety Solutionsを順番に選択して表示したページ

以下のエンジニアリング済みの安全機能は、構成可能なセーフティリレーを備えたドア·モニタ·インターロック·スイッチに基づいています。これには次の製品が使用されています。Guardmaster 440C-CR30構成可能セーフティリレーに接続されたSensaGuard RFID式非接触型安全インターロックスイッチ 使用されている出力デバイスは、100S-Cセーフティコンタクタです。

エンジニアリング済みの安全機能によって達成される安全定格は、(EN) ISO 13849-1のカテゴリ4、PLeです。

オリジナル資料のパブリケーション番号は、SAFETY-AT133C-EN-Pです。

機能安全の説明

作業員は固定式バリアによって危険な動きから保護されます。危険エリアへのアクセスは、必要な場合に、スイングドアを通じて行ないます。このドアは、440C-CR30構成可能セーフティリレーの入力に接続されたSensaGuard非接触型インターロックによってモニタされます。440C-CR30リレーは、危険な動きを駆動するモータへの電力を制御する、直列に接続された2つの100S-Cセーフティコンタクタを制御します。このモニタされたドアが開く場合は、必ず、安全システムがモータへの電力を遮断します。モータおよびモータが駆動する危険な動きは完全に停止するまで惰性で動作します(停止カテゴリ0)。モータはモニタされているドアが開いている間は再起動できません。ドアが閉じれば、リセットボタンを押してから開放することにより440C-CR30リレーをリセットし、次に外部始動を開始して100S-Cコンタクタによって制御されるモータ電源を復旧することによりモータを再起動できます。

SensaGuardスイッチはドアのステータス(開または閉)をモニタします。またSensaGuardスイッチは、2つのOSSD出力でフォルトもモニタします。440C-CR30リレーは、SensaGuardスイッチからの入力で障害をモニタし、100S-Cコンタクタからのリセット信号とフィードバック信号もモニタします。このリレーは、自己の出力でもフォルトをモニタします。これらの出力は100S-Cコンタクタを制御します。440C-CR30リレーは、フォルトが検出されると出力をオフにし、モータへの電力を遮断します。フォルトが解消されるまではリセットされません。

部品表

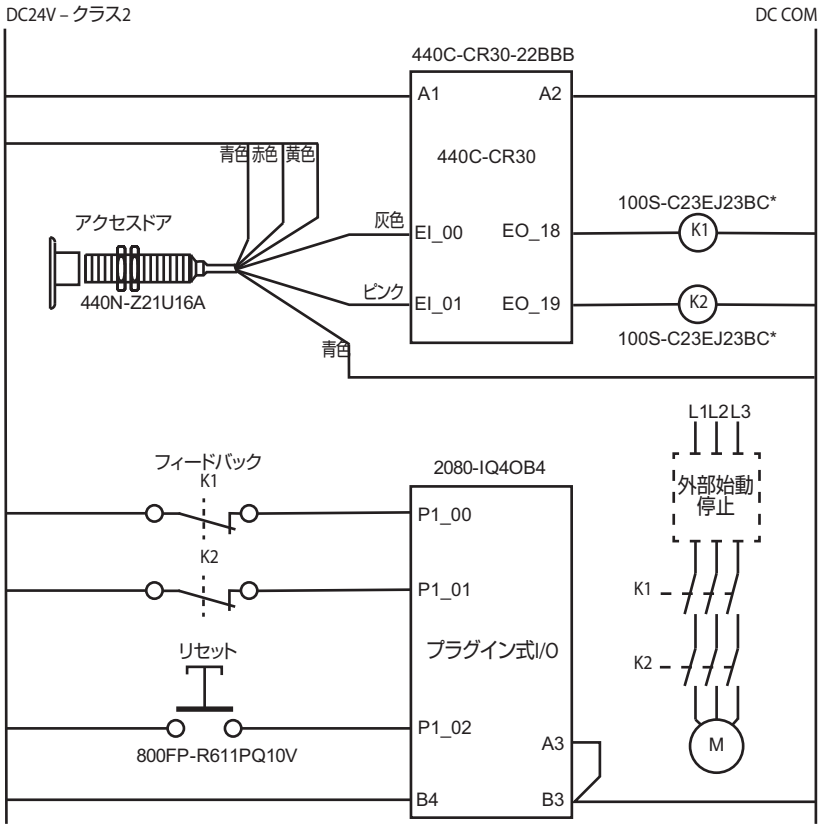
このアプリケーションでは以下の製品が使用されます。

カタログ番号	説明	数量
440N-Z21S16B	SensaGuardスイッチ、18mmプラスチック、2 x PNP、最大0.2A、安全出力、10mケーブル	1
800FP-R611	800Fリセット、丸型プラスチック(タイプ4/4X/13、IP66)、青、R、標準パック	1
2080-IQ4OB4	4チャネルデジタルI/O組合せモジュール	1
1761-CBL-PM02	440C-CR30構成可能セーフティリレーとパーソナルコンピュータを接続するケーブル、プリンタケーブル	1
440C-CR30-22BBB	Guardmaster 440C-CR30ソフトウェアで構成されるセーフティリレー、PLe SIL 3、22の安全I/O、シリアルポートを搭載、USBプログラミングポート、2プラグインスロット、DC24.0V	1
100S-C23EJ23BC	MCS 100S-Cセーフティコンタクタ、23A、DC24V (電気コイル付き)、分岐接点	2

システムの概要

SensaGuardインターロックスイッチは、防護ドアが安全で閉じた状態であることを確認するために使用されます。このドアが閉じていないときは常に、危険な動きを停止するか、または防止します。防護ドアの状態をモニタするのに加え、SensaGuardスイッチはその出力ですべてのフォルト状態をモニタします。440C-CR30構成可能セーフティリレーは、ワイヤ開状態フォルト、シングル·チャネル·フォルト、またはSensaGuardスイッチ入力での0Vへの短絡も検出します。

440C-CR30構成可能セーフティリレーは、セーフティコンタクタのコイルを駆動するパルステスト出力ですべてのフォルト状態をモニタします。セーフティコンタクタK1およびK2の適切で安全な状態は、起動時にSMF2でフィードバック信号をモニタする440C-CR30構成可能セーフティリレーによって確認されます。



** ISO 13849-2では、基本的な安全原理として負荷全体に一時的抑制を行なうことを要求しています。「EJ」電子コイルは適切な抑制を提供します。*

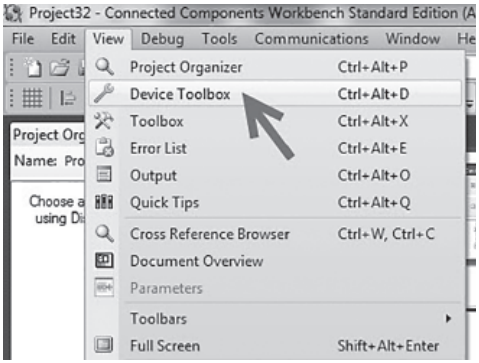
構成

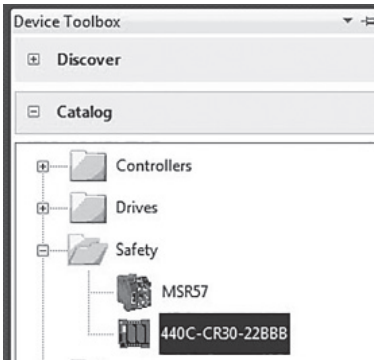
440C-CR30リレーは、Connected Components Workbench™ソフトウェア、リリース6.01以降を使用して構成されます。各手順の詳細な説明は、本書では割愛します。Connected Components Workbenchソフトウェアの知識があることを前提にして説明します。

440C-CR30リレーの構成

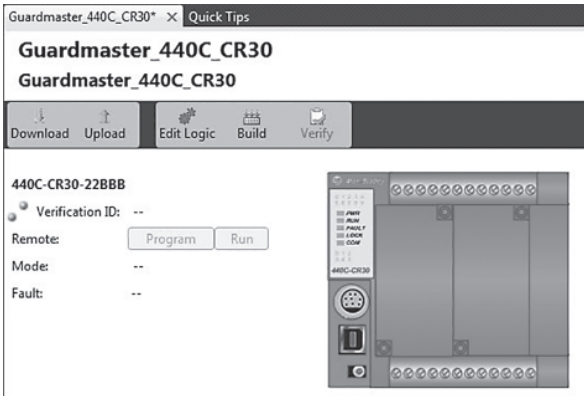
以下の手順に従って、Connected Components Workbenchソフトウェアで Guardmaster 440C-CR30リレーを構成してください。

1. Connected Components Workbenchソフトウェアで、View→Device Toolboxを順番に選択します。Device Toolboxで、440C-CR30-22BBBを選択します。

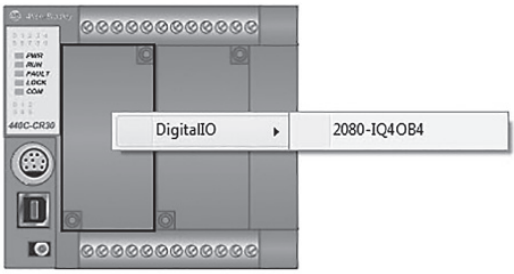


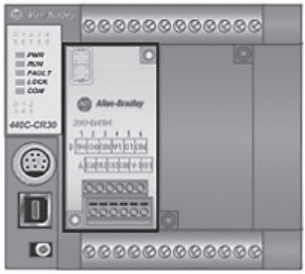


2. Project Organizerで、Guardmaster_400C_CR30 *をダブルクリックします。



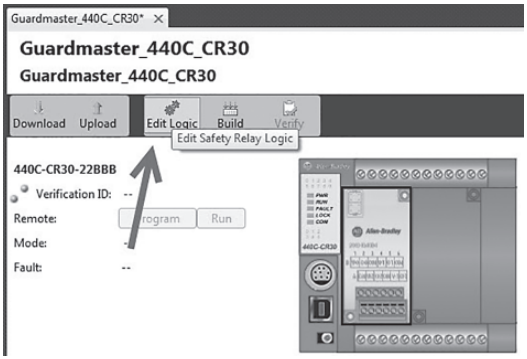
3. この回路で必要なプラグイン式I/Oモジュールを追加するには、左側のプラグイン式モジュールのスペースを右クリックして2080-IQ4OB4モジュールを選択します。



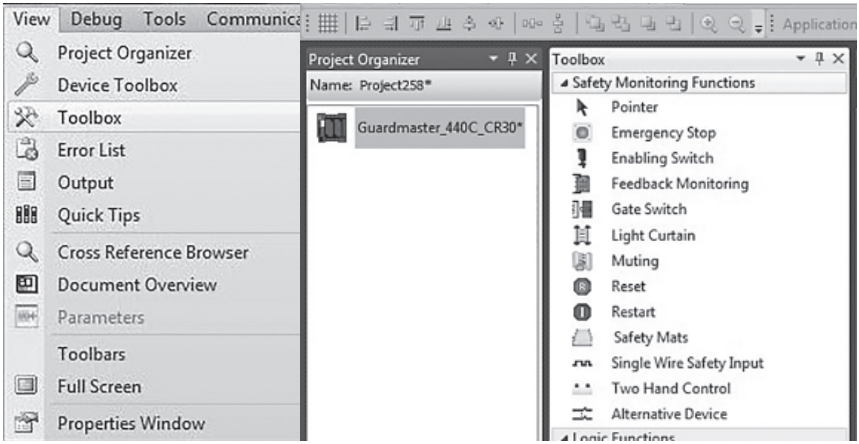


ヒント: このI/Oモジュールは安全I/Oモジュールではないため、標準の灰色で表示されます。安全信号の接続に使用されないため、このアプリケーションでは許容されます。フィードバックやリセットボタンなどの入力は、厳密な安全信号とは見なされません。これらの非安全信号に標準I/Oを使用することにより、限られた数の安全入力および出力を本当の安全信号のために残しておくことができます。

4. Edit Logicボタンをクリックして、Connected Components Workbenchワークスペースを開きます。空白のワークスペースが表示されます。



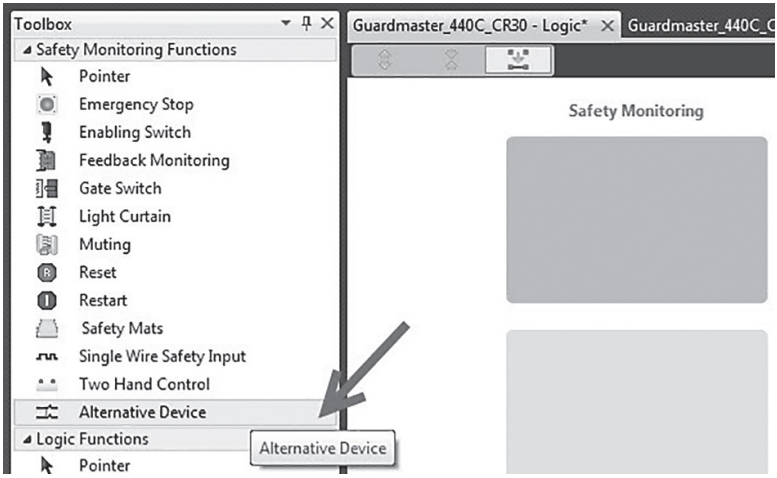
5. Viewプルダウンメニューから、Toolboxを選択します。Toolboxが表示されます。



入力の構成

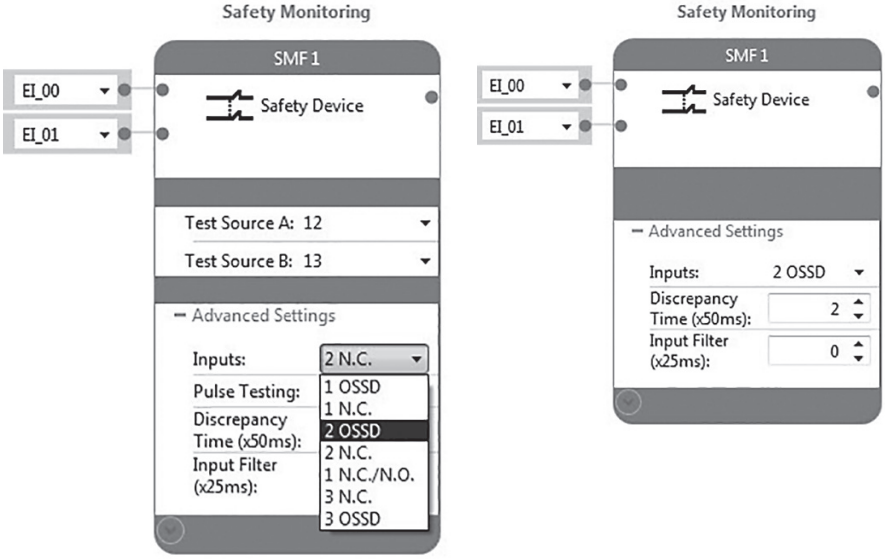
Toolboxには、SensaGuard Safety Monitoring Functionのリストは表示されません。以下の手順に従って、入力を構成してください。

1. Alternative Deviceを選択します。Safety Monitoring列の緑色のブロックにこれをドラッグして放します。

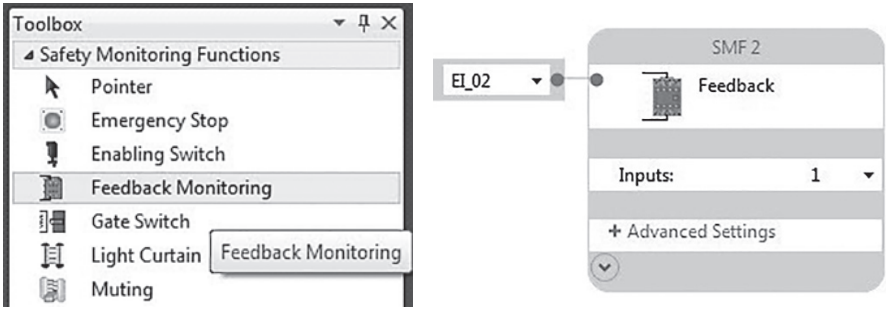


Connected Components Workbenchソフトウェアは、最初の2つの使用可能な入力EI_00およびEI_01をデバイスに自動的に割付けます。割付けられた入力をそのままにしておきます。Connected Components Workbenchソフトウェアは、このブロックにファンクション名SMF 1を自動的に割付けます。ソフトウェアは、デフォルトで電気機械式デバイスを前提としてTest Sourcesを割付けます。SensaGuardスイッチには2つのOSSD出力があり、Test Sourcesは必要ありません。

2. ブロックを適切に構成するには、Advanced Settingsを開き、Inputsプルダウンメニューから2 OSSDを選択します。下図に示すように選択されたブロックが表示されます。

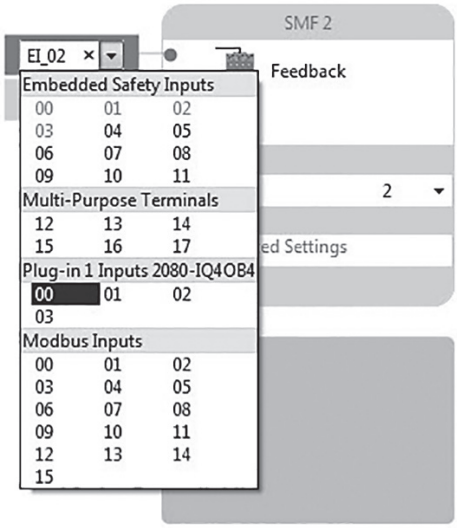


3. Feedback Monitoring Safety Monitoringファンクションをクリックし、ワークスペースのSensaGuardブロックの下のSafety Monitoringブロックにドラッグして放します。

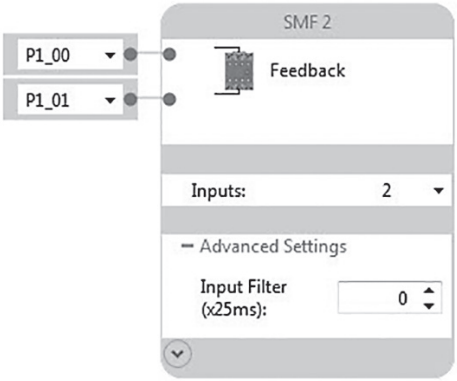


Connected Components Workbenchソフトウェアは、次に使用可能なSafety Input端子である入力端子EI_02にこれを割付けることに注意してください。ソフトウェアはこれが信号入力であることを前提として、このブロックにファンクション名SMF 2を自動的に割付けます。

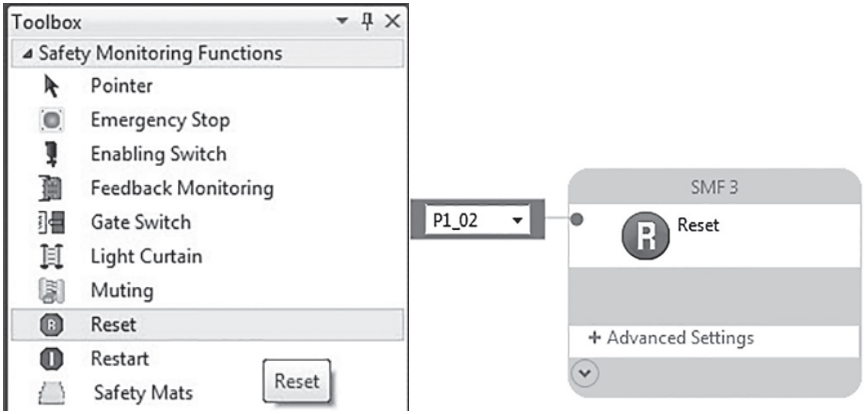
4. この回路は各コンタクタから1つずつ2つの入力を必要とするため、入力数を2に変更します(それぞれの100Sコンタクタから通常閉接点を1つずつ)。



5. 入力をPlug-In端子PI_00およびPI_01に割付けます。これにより、フィードバック信号に安全入力を無駄に使用することを防ぎます。



6. Reset安全モニタ機能をクリックし、ワークスペースのFeedback Monitoringブロックの下のSafety Monitoringブロックにドラッグして放します。

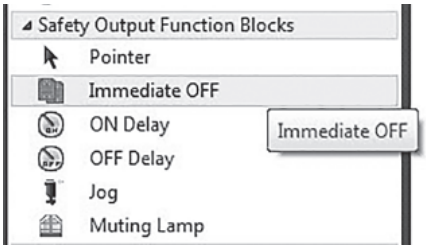


Connected Components Workbenchソフトウェアは、このブロックにファンクション名SMF 3を自動的に割付けます。Reset入力をPlug-In端子PI_02に再度割付けます。

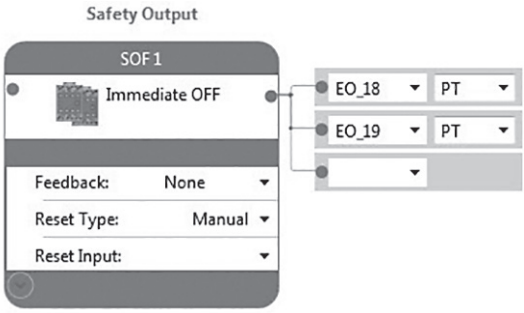
出力の構成

以下の手順に従って、出力を構成してください。

1. ToolboxのSafety Output Function BlocksセクションからImmediate OFFをクリックしてドラッグします。

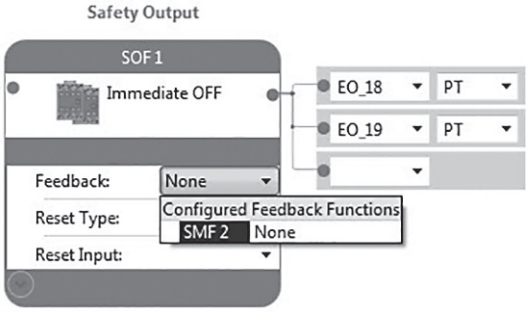


2. ワークスペースのSafety Output列の一番上のブロックで放します。

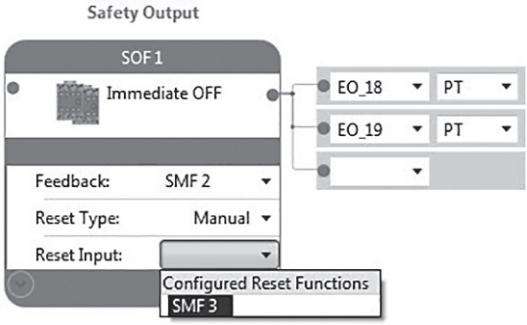


Connected Components Workbenchソフトウェアは、出力端子EO_18およびEO_19を自動的に割付けます。デフォルトでこれらの端子はPulse Testingに割付けられます。デフォルトのReset TypeはManualです。これらの設定をデフォルトのままにしておきます。

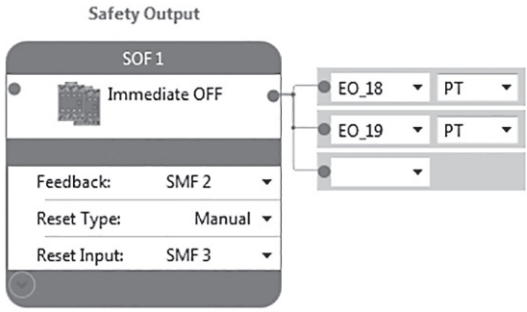
3. FeedbackプルダウンメニューからSMF 2を選択します。



4. Reset InputプルダウンメニューからSMF 3を選択します。



安全出力の構成が完了します。

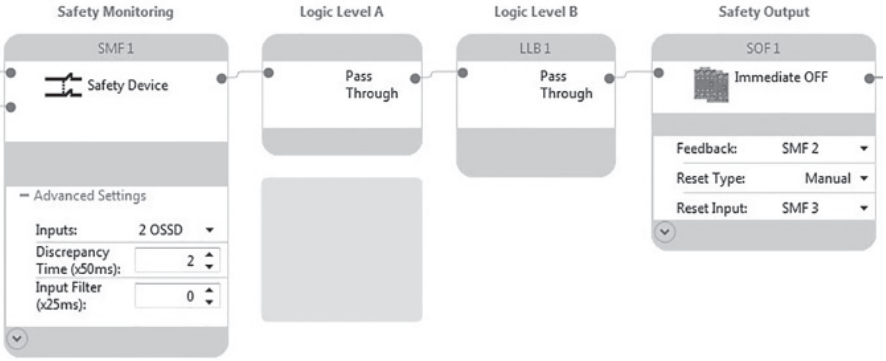


ロジックの構成

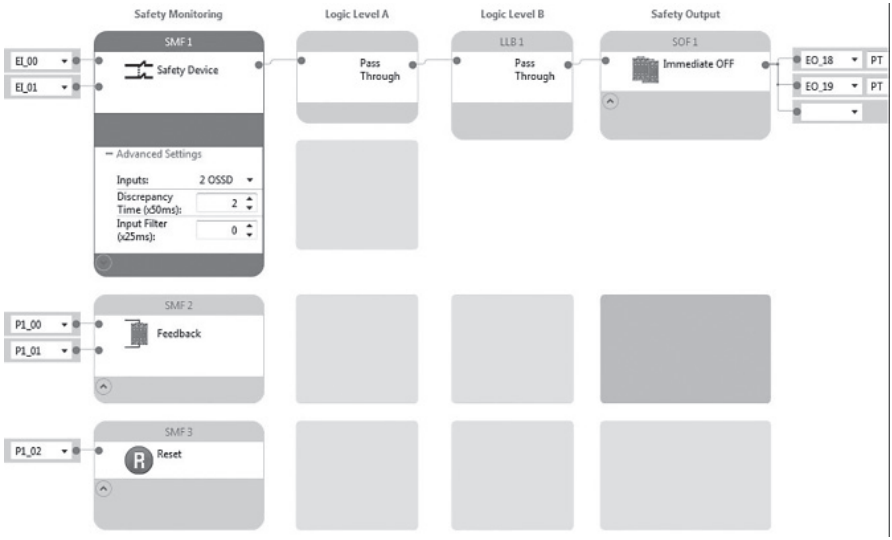
Logicセクションでは、安全出力が安全モニタ入力にどのように応答するかを決定します。この場合では、安全出力は安全モニタ入力のすぐ後に続きます。

1. SensaGuard Safety Monitoring入力ブロックの右側にある青色の点をクリックします。色が灰色に変わります。

2. Safety Outputブロックの左側にある青色の点をクリックして、ロジックを接続します。

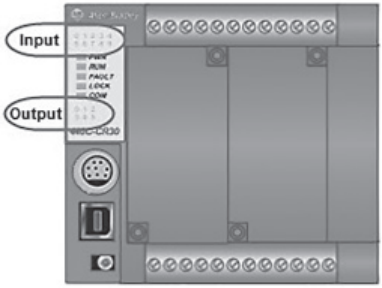


接続が完了したロジックは下図のように表示されます。

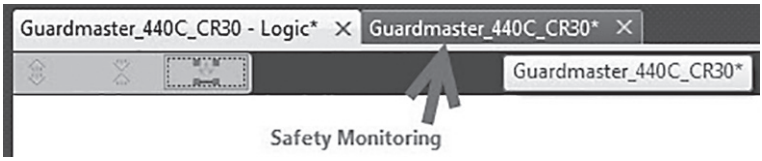


ステータスインジケータの構成

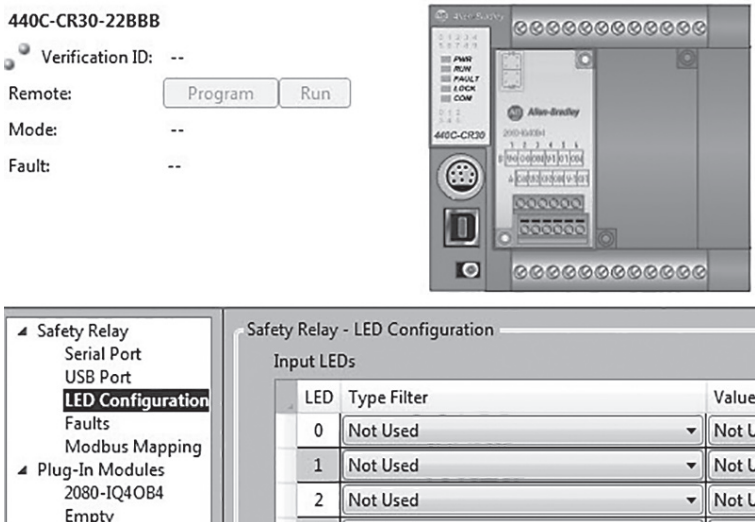
440C-CR30構成可能セーフティリレーには、10個のユーザ構成可能入力ステータスインジケータLEDと6個のユーザ構成可能出力ステータスインジケータLEDがあります。多くの場合、ステータスインジケータは設置や立上げ、モニタ、および440C-CR30構成可能セーフティリレーのシステムのトラブルシューティングに非常に役に立ちます。ステータスインジケータはシステムの動作には何ら影響を及ぼさず、特に構成する必要はありませんが、簡単に構成できるので、使用することをお奨めします。



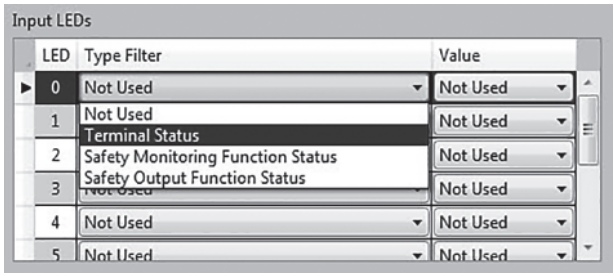
1. Guardmaster_440C_CR30*をクリックします。



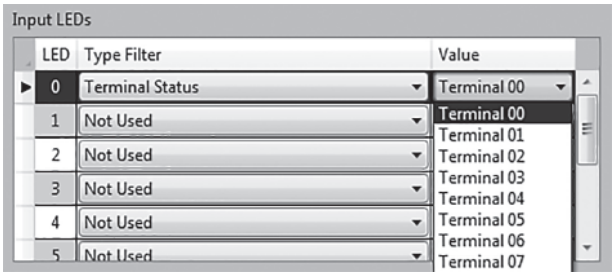
2. LED Configurationを選択します。



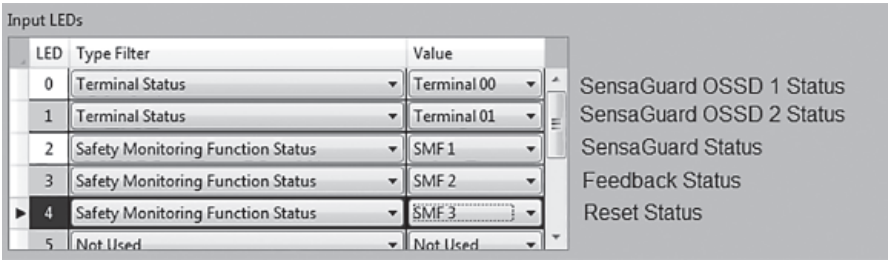
3. LED 0のType FilterでTerminal Statusを選択します。



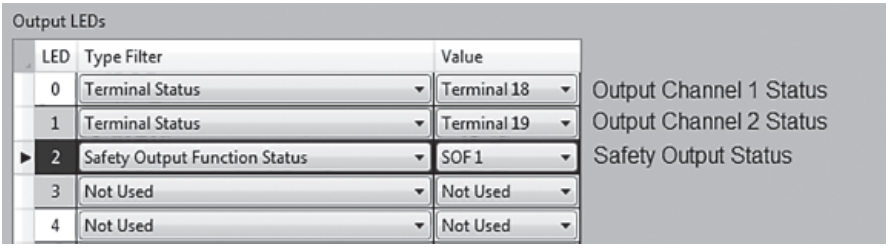
4. LED 0のValueプルダウンメニューからTerminal 00を選択します。ステータスインジケータLED 0が構成され、端子00のステータスが表示されます。



5. 次の4つの入力LED (1～4)を同じ手順で割付けます。これで入力ステータスインジケータLEDの構成が完了します。



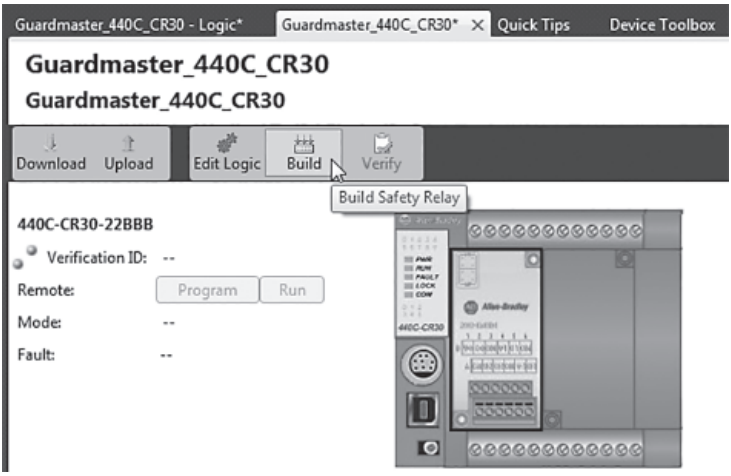
6. 下図のように3個の出力LEDを割付けます。



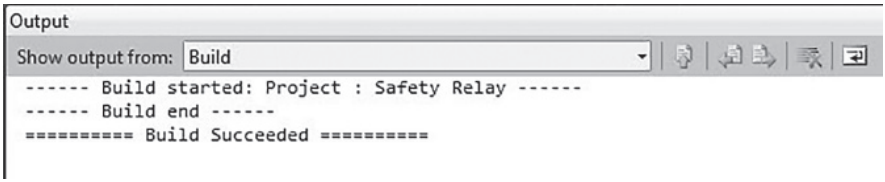
ビルドの妥当性確認

以下の手順に従って、Connected Components Workbenchソフトウェアでビルド機能を使用して、ロジックの妥当性を確認してください。

1. ワークスペースの上のバーでGuardmaster_440C_CR30をクリックします。
2. Buildをクリックします。



Build Succeededメッセージで構成が有効であることが確認できます。



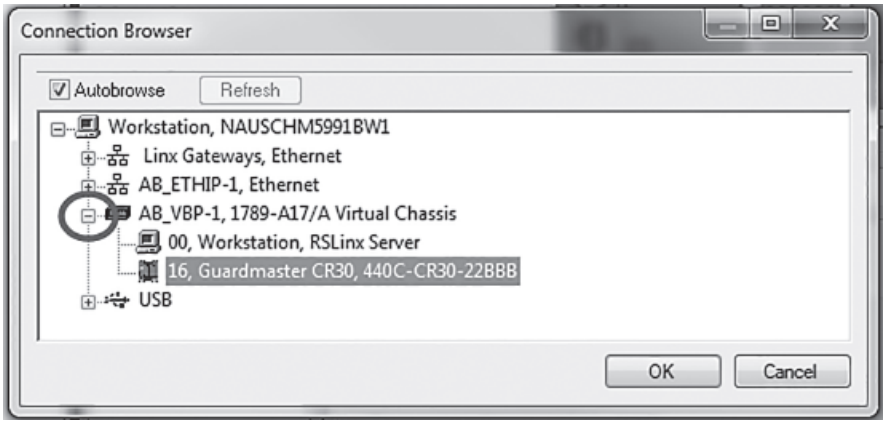
ビルド中にエラーまたは漏れが発見された場合は、修正できるようにエラーの詳細を示すメッセージが表示されます。エラーの修正後に、再度構築を実行する必要があります。

プロジェクトの保存およびダウンロード

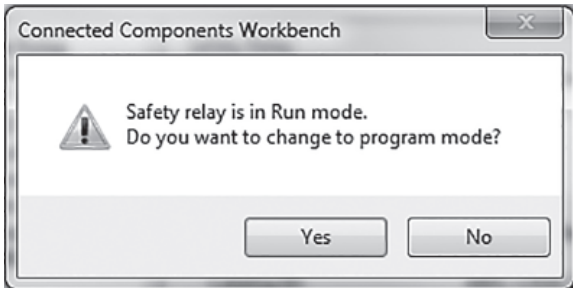
以下の手順に従って、プロジェクトを保存してダウンロードしてください。

1. Fileメニューから、プロジェクトを保存するためにSaveを選択します。
2. Project Organizerウィンドウで、Guardmaster_440C_CR30をダブルクリックしてワークスペースを開きます。
3. 440C-CR30セーフティリレーの電源を投入します。
4. USBケーブルを440C-CR30リレーに接続します。
5. Downloadをクリックします。

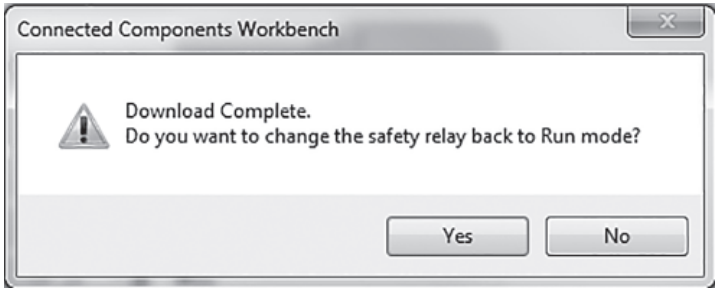
6. Connection Browserで、AB_VBP-1 Virtual Chassisを展開し、Guardmaster 440C-CR30-22BBBを選択します。OKをクリックします。



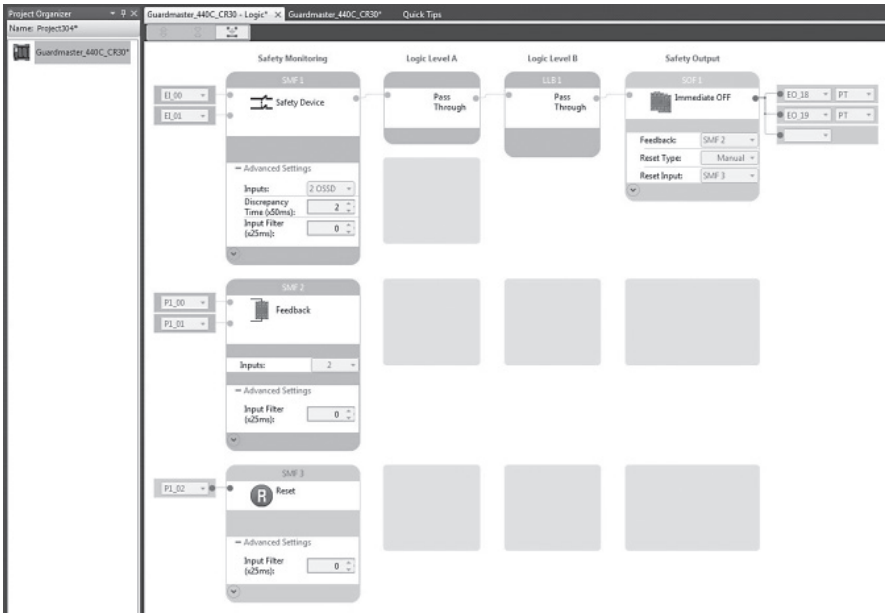
7. Yesをクリックして、ランモードからプログラムモードに変更します。



8. ダウンロードが完了すると、Yesをクリックしてプログラムモードからランモードに変更します。



9. Edit Logicをクリックして、オンライン診断を表示します。

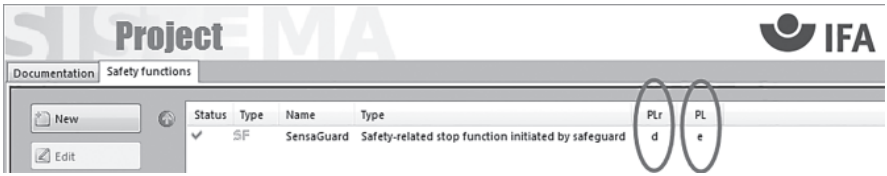


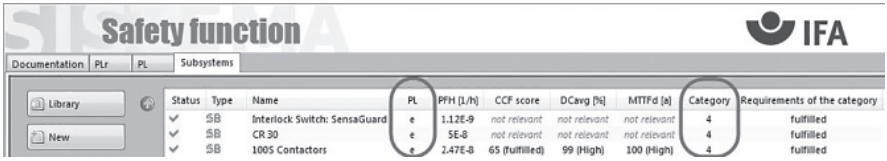
緑色はブロックがTrueであること、または入力または出力端子がオンであることを示します。緑色のインジケータの点滅は、Safety Output Functionをリセットする準備ができていることを示します。440C-CR30リレーのオンライン診断モードは、検証プロセスで非常に役に立ちます。

10. 構成の検証を実行する前に、安全遂行レベルの計算や検証および妥当性確認計画を見直します。

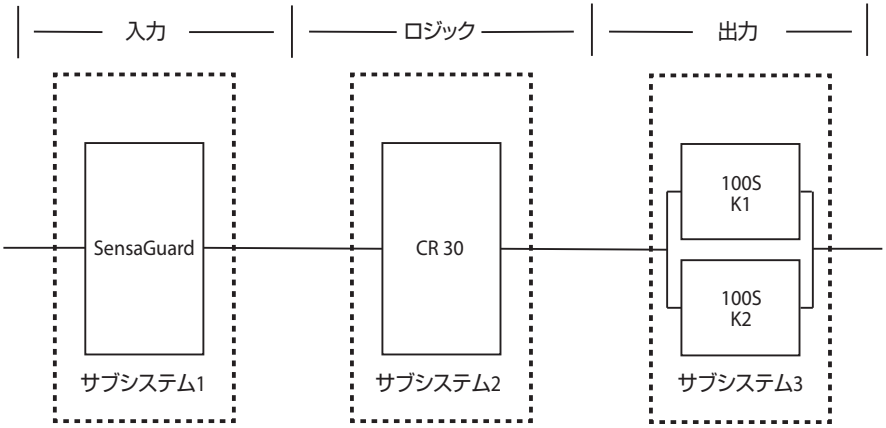
安全遂行レベルの計算

適切に実装されている場合、この安全関連停止機能は、SISTEMAソフトウェアPL計算ツールを使用して計算した通りに、ISO 13849-1: 2008に準拠したカテゴリ4、安全遂行レベルe (CAT. 4、PLe)の安全定格を実現することができます。この安全機能のリスクアセスメントから要求される最小安全遂行レベル(PLr)はPLdです。





安全保護機能によって開始されるこの安全関連停止は、以下の図のようにモデル化されます。



これらは電気機械式デバイスであるため、セーフティコンタクタのデータには以下が含まれています。

- 危険側故障発生までの平均時間($MTTF_D$)
- 自己診断率(DCavg)
- 共通原因故障(CCF)

電気機械式デバイスの機能安全の評価には以下が含まれています。

- 動作頻度
- 効果的にフォルトをモニタしているか
- 適切に指定され、設置されているか

SISTEMAは、SISTEMAプロジェクトの作成時に入力される推定使用頻度とともにコンタクタに関して提供されるB10dデータを使用することによりMTTFdを計算します。

コンタクタのDCavg (99%)は、ISO 13849-1の付属書E「直接モニタ」の「出力デバイス」表から選択されます。

CCF値は、ISO 13849-1の付属書Fに概説されているスコアリングプロセスを使用して生成されます。実際にアプリケーションを実装する場合は、完全なCCFスコアリングプロセスを実施する必要があります。最低でも65のスコアを達成する必要があります。

検証および妥当性確認計画

検証および妥当性確認は、安全システムの設計および開発プロセス全体を通じて障害の防止に重要な役割を果たします。ISO 13849-2は、検証および妥当性確認の要件を規定します。この規格は、すべての安全機能要件が満たされていることを確認するために文書化された計画を要求しています。

検証では、開発された安全制御システムを分析します。安全制御システムの安全遂行レベル(PL)を計算し、そのシステムが仕様で要求される安全遂行レベル(PLr)を満たしているか確認します。計算を実行するためにSISTEMAソフトウェアが一般的に使用され、ISO 13849-1の要件を満たすことを支援します。

妥当性確認では、安全制御システムの機能テストを実施し、システムが安全機能の仕様の要件を満たしていることを立証します。安全制御システムの試験では、すべての安全関連出力がそれに対応する安全関連入力に適切に応答することを確認します。機能テストには、故障モードの潜在的障害注入に加えて、通常の動作条件が含まれます。チェックリストは通常、安全制御システムの妥当性確認を記録するために使用します。

システムの妥当性確認を実施する前に、Guardmaster 440C-CR30構成可能セーフティリレーがインストレーションインストラクション(取付け手順書)に従って配線され構成されていることを確認します。

検証および妥当性確認チェックリスト

一般的な機械情報	
機械名/型番	
機械のシリアル番号	
顧客名	
試験日	
試験者の氏名	
計画図番号	
入力デバイス	440N-Z21S16B
構成可能なセーフティリレー	440C-CR30-22BBB
可変周波数ドライブ	
セーフティコンタクタ	100S-C23EJ23BC

安全配線およびリレー構成			
テスト手順	検証	合格/不合格	変更/修正
1	すべてのコンポーネントの仕様が当該アプリケーションに適していることを確認します。ISO 13849-2の基本的な安全原理および十分に検証された安全原理を参照します。		
2	セーフティリレー回路を目視チェックし、回路図に記載されている通りに配線されていることを確認します。		
3	440C-CR30構成可能セーフティリレーが適切に意図通りに構成されていることを確認します。		

通常動作の検証 - 通常のすべての始動、停止、リセット、非常停止、およびSensaGuardスイッチ入力に対して、安全システムが適切に応答することを確認します。			
テスト手順	検証	合格/不合格	変更/修正
1	防護領域に誰もいないことを確認します。		
2	危険な動きが停止していることを確認します。		
3	ドアが閉じていることを確認します。		
4	安全システムの電源を投入します。		
5	440C-CR30セーフティリレーの端子00、端子01、およびSMF1入力のステータスインジケータLEDが緑色になっていることを確認します。すべての出力ステータスインジケータが消灯していることを確認します。PowerおよびRunステータスインジケータLEDが緑色になっていることを確認します。Connected Components Workbenchソフトウェアを使用して、440C-CR30セーフティリレーのステータスが適切であるかをモニタします。		
6	440C-CR30セーフティリレーのリセットボタンを押してから放します。端子18、端子19、およびSOF1出力ステータスインジケータLEDが緑色になっていることを確認します。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		

7	電源投入時に危険な動きが開始していないことを確認します。		
8	ドライブの始動ボタンを押してから放します。危険な動きが開始し、機械が動作を開始したことを確認します。		
9	外部の停止ボタンを押します。機械は通常の構成された方法で停止する必要があります。安全システムは応答してはなりません。		
10	外部の始動ボタンを押してから放します。危険な動きが開始し、機械が動作を開始したことを確認します。		
11	防護ドアを開きます。安全システムはトリップする必要があります。危険な動きは0.7秒未満で停止する必要があります。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
12	440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30構成可能セーフティリレーは応答してはなりません。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
13	防護ドアを閉じます。機械は起動してはなりません。440C-CR30セーフティリレーは応答してはなりません。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
14	440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30セーフティリレーのSOF1が励磁する必要があります。危険な動きは開始してはなりません。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
15	外部の始動ボタンを押してから放します。モータが起動し、機械が動作を開始することを確認します。		

異常な動作に対する安全な応答の妥当性確認 – 安全システムが対応する診断により予測可能なすべてのフォルトに対して適切に応答していることを確認します。			
SensaGuardおよび440C-CR30構成可能セーフティリレーのテスト			
テスト手順	**検証**	**合格/不合格**	**変更/修正**
1	防護ドアを閉じたままにします。危険な動きが動作を続ける間、440C-CR30セーフティリレーの端子EI_00に接続されたSensaGuard OSSD1のワイヤを取り外します。440C-CR30セーフティリレーは直ちにトリップする必要があります。リレーの赤色のフォルト·ステータス·インジケータLEDが点滅する必要があります。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
2	ワイヤをE1_00に再接続します。440C-CR30セーフティリレーは応答してはなりません。440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30セーフティリレーは応答してはなりません。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		

3	防護ドアを開いて閉じます。赤色のフォルトステータスLEDは消灯する必要があります。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
4	440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30リレーのSOF 1出力が励磁する必要があります。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
5	外部始動ボタンを押します。機械は動作を開始する必要があります。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。以下のSensaGuard妥当性確認テスト(手順6～27)では、この手順はオプションです。		
6	防護ドアを閉じた状態で、OSSD 1をDC24Vに接続します。約40秒後に、SensaGuardスイッチがトリップします。440C-CR30セーフティリレーがトリップします。440C-CR30セーフティリレーの赤色のフォルト・ステータス・インジケータLEDが点滅する必要があります。SensaGuardスイッチのステータスインジケータが赤色に点滅します。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
7	OSSD 1をDC24Vから切り離します。SensaGuardスイッチも440C-CR30セーフティリレーもいずれも応答しません。440C-CR30セーフティリレーの再起動ボタンを押してから放します。SensaGuardスイッチも440C-CR30セーフティリレーもいずれも応答しません。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
8	SensaGuardスイッチの電源を切断してから再投入します。SensaGuardスイッチへの電源が復旧してから約5秒後に、ステータスLEDが緑色に点灯します。440C-CR30セーフティリレーの赤色に点滅するフォルト・ステータス・インジケータLEDが消灯します。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
9	440C-CR30セーフティリレーのリセットボタンを押してから放します。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
10	OSSD 1をDC COMに接続します。440C-CR30セーフティリレーが直ちにトリップします。赤色のSafe Stopスタックライトが点灯します。黄色のGate 1スタックライトが点灯します。440C-CR30セーフティリレーの赤いフォルト・ステータス・インジケータLEDが点滅する必要があります。SensaGuardスイッチのステータスインジケータが赤色に点滅します。		

11	OSSD1をDC COMから切り離します。SensaGuardスイッチも440C-CR30セーフティリレーもいずれも応答しません。440C-CR30セーフティリレーの再起動ボタンを押してから放します。SensaGuardスイッチも440C-CR30セーフティリレーもいずれも応答しません。		
12	SensaGuardスイッチの電源を切断してから再投入します。SensaGuardスイッチへの電源が復旧してから約5秒後に、ステータスインジケータLEDが緑色に常時点灯します。黄色のGate 1スタックライトが消灯します。赤色のSafe Offスタックライトが点灯したままになります。440C-CR30セーフティリレーの点滅中の赤いフォルト・ステータス・インジケータLEDが消灯します。		
13	440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30セーフティリレーのSOF 1がコンタクタを励磁する必要があります。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
14～27	EI_00のかわりにEI_01を、OSSD 1のかわりにOSSD 2を使用して、ステップ1～13を繰返します。		
28	OSSD 1をOSSD 2に(端子EI_00を端子EI_01に)接続します。約50秒後に、SensaGuardスイッチがトリップします。440C-CR30セーフティリレーがトリップします。SensaGuardスイッチのステータスインジケータが赤色に点滅します。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
29	OSSD 1をOSSD 2から切り離します。SensaGuardスイッチも440C-CR30セーフティリレーもいずれも応答しません。440C-CR30セーフティリレーの再起動ボタンを押してから放します。SensaGuardスイッチも440C-CR30セーフティリレーもいずれも応答しません。		
30	SensaGuardスイッチの電源を切断してから再投入します。SensaGuardスイッチへの電源が復旧してから約5秒後に、ステータスLEDが緑色に点灯します。440C-CR30セーフティリレーの赤色に点滅するフォルト・ステータス・インジケータLEDが消灯します。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		
31	440C-CR30セーフティリレーのリセットボタンを押してから放します。赤色のSafe Stopスタックライトが消灯する必要があります。440C-CR30セーフティリレーのSOF1出力がコンタクタを励磁する必要があります。適切に動作しているかすべてのステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30セーフティリレーが適切なステータスであるかモニタします。		

異常な動作に対する安全な応答の妥当性確認 – 安全システムが対応する診断により予測可能なすべてのフォルトに対して適切に応答していることを確認します。			
コンタクタ – 440C-CR30構成可能セーフティリレーのテスト			
テスト手順	検証	合格/不合格	変更/修正
1	機械が動作を続ける間、440C-CR30構成可能セーフティリレーの端子EO_18およびK1コイルのA1端子の間の接続を切り離します。危険な動きは惰走停止する必要があります。		
2	外部の停止ボタンを押します。接続を復旧します。外部始動ボタンを押して、危険な動きを再開します。		
3	危険な動きが動作を続ける間、K1コイルのA1端子をDC24Vに接続します。約18秒後に、440C-CR30セーフティリレーがトリップする必要があります。K2をオフする必要があります。危険な動きが惰走停止します。440C-CR30セーフティリレーの赤色のフォルト・ステータス・インジケータLEDが点灯します。		
4	K1コイルのA1端子をDC24Vから切り離します。440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30セーフティリレーは応答してはなりません。		
5	440C-CR30セーフティリレーの電源を切断してから再投入します。セーフティリレーが応答します。440C-CR30セーフティリレーのフォルト・ステータス・インジケータLEDが消灯します。		
6	440C-CR30セーフティリレーのリセットボタンを押してから放します。外部始動ボタンを押します。危険な動きが再開する必要があります。		
7	機械が動作を続ける間、K1コイルのA1端子をDC COMに短絡させます。440C- CR30セーフティリレーがトリップする必要があります。440C-CR30セーフティリレーの赤色のフォルト・ステータス・インジケータLEDが点灯します。		
8	K1コイルのA1端子をDC COMから切り離します。440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30セーフティリレーは応答してはなりません。		
9	440C-CR30セーフティリレーの電源を切断してから再投入します。440C-CR30セーフティリレーが応答します。440C-CR30セーフティリレーのフォルト・ステータス・インジケータLEDが消灯します。		
10	440C-CR30セーフティリレーのリセットボタンを押してから放します。外部始動ボタンを押します。危険な動きが再開します。		
11～21	EO_18のかわりにEO_19を、K 1のかわりにK 2を使用して、手順1～10を繰返します。		
22	K1のA1端子をK2のA1端子に接続します。約18秒後に、440C-CR30セーフティリレーがトリップする必要があります。危険な動きが惰走停止します。440C-CR30セーフティリレーの赤色のフォルト・ステータス・インジケータLEDが点灯します。		
23	K1のA1端子をK2のA1端子から切り離します。440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30セーフティリレーは応答してはなりません。		
24	440C-CR30セーフティリレーの電源を切断してから再投入します。セーフティリレーが応答します。440C-CR30セーフティリレーのフォルト・ステータス・インジケータLEDが消灯します。		
25	440C-CR30セーフティリレーのリセットボタンを押してから放します。外部始動ボタンを押します。危険な動きが再開する必要があります。		

異常な動作に対する安全な応答の妥当性確認 – 安全システムが対応する診断により予測可能なすべてのフォルトに対して適切に応答していることを確認します。			
コンタクタのフィードバック – 440C-CR30構成可能セーフティリレーのテスト			
テスト手順	検証	合格/不合格	変更/修正
1	機械が動作を続ける間、端子P1_00のK1フィードバック接続を取り外します。機械は動作を続ける必要があります。		
2	防護ドアを開きます。安全システムはトリップする必要があります。危険な動きは0.7秒未満で停止する必要があります。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30リレーが適切なステータスであるかモニタします。		
3	防護ドアを閉じます。機械は起動してはなりません。440C-CR30リレーは応答してはなりません。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30リレーが適切なステータスであるかモニタします。		
4	440C-CR30セーフティリレーのリセットボタンを押してから放します。440C-CR30リレーは応答してはなりません。適切に動作しているかステータスインジケータLEDをモニタし、Connected Components Workbenchソフトウェアを使用して440C-CR30リレーが適切なステータスであるかモニタします。		
5	P1_00の接続を元に戻します。440C-CR30リレーの電源を切断してから再投入します。440C-CR30リレーのリセットボタンを押します。440C-CR30リレー出力が励磁する必要があります。外部の始動ボタンを押してから放します。モータが起動し、機械が動作を開始することを確認します。		
6	端子P1_01のK2フィードバック接続を使用して、手順1～5を繰返します。		

構成の検証

システムは、Verifyコマンドを使用して個々のアプリケーションの構成を検証する必要があります。440C-CR30構成可能セーフティリレーが検証されていない場合、24時間の動作後にフォルトが発生します。

注意: 検証プロセスは、安全システムの技術ファイルに記録してください。

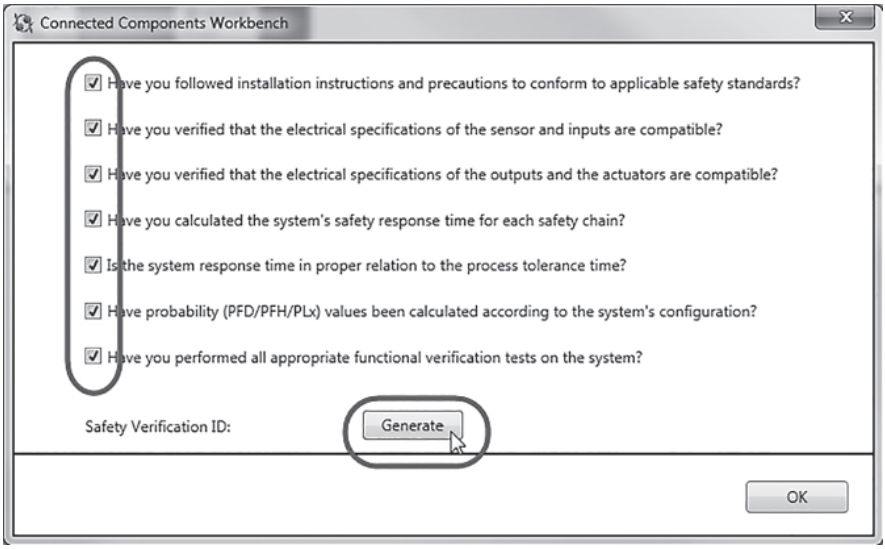
以下の手順に従って、構成をダウンロードして検証してください。

1. 440C-CR30リレーに電源が投入され、USBケーブルを介してワークステーションに接続されていることを確認します。

2. 440C-CR30リレーが接続されていることが、Connected Components Workbench Projectタブの右上隅に表示されていることを確認します。表示されていない場合は、Connect to Deviceをクリックして、ソフトウェアのコネクションを確立します。

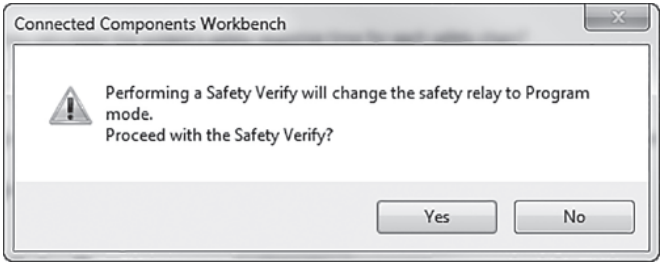
3. Verifyをクリックします。

4. すべての質問に回答し、完了したら各ボックスをチェックします。Generateをクリックします。



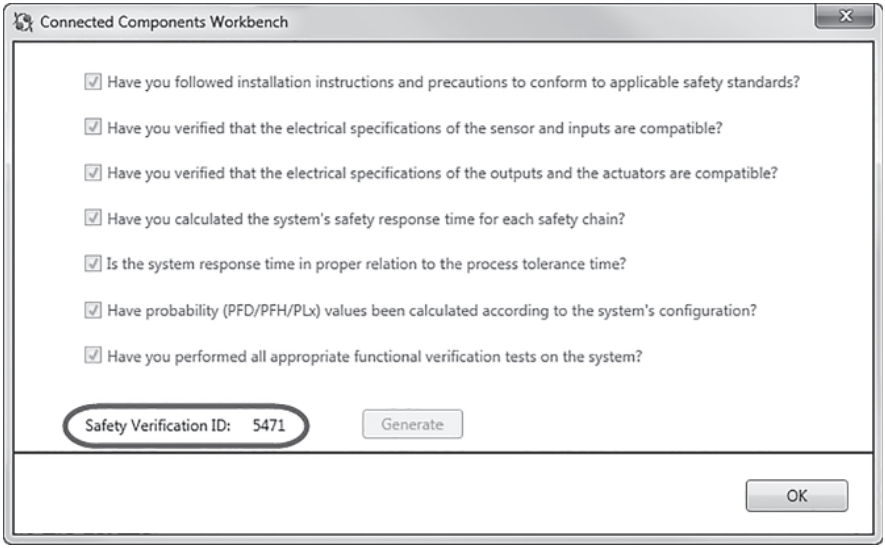
重要: Verification IDを生成するには、すべてのボックスがチェックされていなければなりません。

6. Yesをクリックして、検証を開始します。



7. Yesをクリックして、ランモードに変更します。

8. 機械の資料にSafety Verification IDを記録します。



このプロセスは、システムの検証および妥当性確認が完了したことを440C-CR30リレーにフィードバックするためのものです。固有の検証IDを使用して、構成ファイルに変更が行なわれたどうかをチェックできます。構成に何らかの変更があれば、Safety Verification IDは削除されます。その後に検証作業を実行することにより、別の検証IDが生成されます。Safety Verification IDは、440C-CR30リレーに接続しているときのみ、Connected Components Workbenchソフトウェアに表示されます。

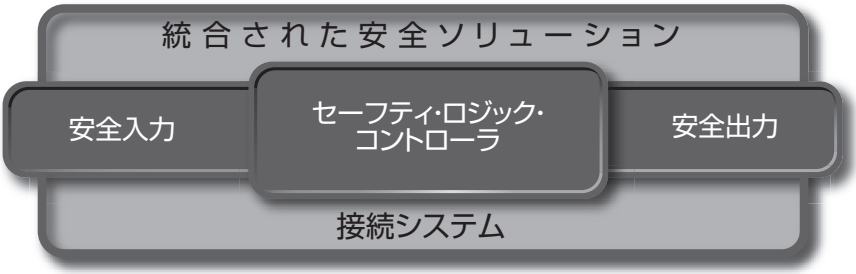
第11章: 製品、ツールおよびサービス

概要

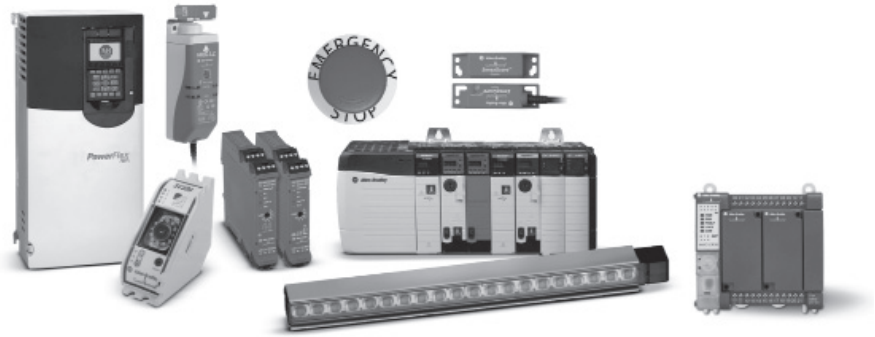
ロックウェル・オートメーションは、産業用電源、制御および情報ソリューションをグローバルに提供するリーディングカンパニーであり、創業以来100年以上にもわたりさまざまな産業分野のお客様をサポートしています。当社の産業オートメーション製品ラインには、総合的な機械安全テクノロジやツールおよびサービスが含まれます。

お客様のアプリケーションに対応した製品およびテクノロジ

ロックウェル・オートメーションは、最大の品揃えを誇る機械安全ソリューションのサプライヤであり、安全システムを構成する3つの要素(入力デバイス、ロジック制御および最終的なパワー要素)をすべて提供しています。



当社が提供する製品およびテクノロジには次のようなものがあります。



安全入力デバイス

- **存在検知安全装置**
  存在検知安全装置は、危険領域の近くにある物体または作業員の位置を検出します。これには、セーフティ・ライト・カーテン、セーフティ・レーザ・スキャナ、手検出セーフティセンサ、感圧式マットおよびエッジなどがあります。

- **セーフティ・インターロック・スイッチ**
  セーフティスイッチは、高い信頼性と安定性そして高品質が求められる国際規格に合わせて設計および構築されています。セーフティスイッチには、リミットスイッチやインターロックスイッチ、非常停止スイッチがあります。

- **非常停止/トリップ装置**
  非常停止スイッチには、強制開離式接点が搭載されたさまざまなマッシュルーム型押しボタン装置があります。イネーブルスイッチやロープ式スイッチは、アプリケーション各所に緊急機能を提供し、または安全アプリケーション内でオペレータが移動できるようにロープなどでつながれています。

- **オペレータインターフェイス**
  オペレータインターフェイス装置は、オペレータがアプリケーションを対話的操作することを可能にし、追加の専用安全機能を提供します。

セーフティ・ロジック・コントローラ

- **セーフティリレー(単一機能または構成可能)**
  セーフティリレーは、安全システムを確認およびモニタし、機械を始動したり、機械を停止するコマンドを実行することができます。単一機能セーフティリレーは、安全機能の実行に専用のロジックデバイスを必要とする小型機械にとって最も経済的なソリューションです。モジュール式の構成可能なモニタ・セーフティ・リレーは、多数かつ多様な安全保護装置と最小限のゾーン制御を必要とする環境に理想的です。

- **統合セーフティコントローラ**
  セーフティPLCは、安全状態への自動化プロセスをもたらすために一般的に必要とされるハード配線のリレーシステムを置き換え、従来のPLCシステムの利点を安全アプリケーションにもたらします。セーフティPLCにより、標準および安全関連プログラムが単一コントローラシャーシ内に共存でき、プログラミングに柔軟性を与えるだけでなく、プログラマが慣れ親しんだ使いやすい環境を提供します。セーフティ・コントローラ・ソリューションは、機械の安全と資産の保護を保証するオープンで統合された制御を提供します。

- **安全I/Oデバイス**
  Guard I/O™ 安全製品は、安全システム用に設計されていますが、従来の分散I/Oのあらゆるメリットを安全システムもたらすものです。これらの製品により、機械およびセルの配線コストを低減でき、スタートアップ時間を短縮できます。Guard I/O安全製品は、さまざまな機能を備え、In-CabinetアプリケーションおよびOn-Machineアプリケーションに対応しています。

安全アクチュエータ

- **セーフティコンタクタおよびスタータ**
  ArmorStart®分散モータコントローラはカテゴリ4の安全機能を達成しながら、DeviceNet™ On-Machine™安全装置に統合された安全ソリューションを実現できます。IECセーフティコンタクタおよび制御リレーを使用することで、予期しないマシンの起動や安全機能の損失を防ぎ、作業員を保護できます。

- **PowerFlex® ACドライブ**
  PowerFlexドライブでは安全機能が利用できます。PowerFlex 525 ACドライブには、安全機能として安全トルクオフが組み込まれています。安全トルクオフは、PowerFlex 40P、70、700H、700S、および750シリーズACドライブのオプション機能で、安全速度モニタ機能もサポートされています。

- **Kinetix®統合モーション**
  Kinetix 300、6000、6200、6500および7000サーボドライブにはすべて、安全機能が組み込まれています。安全トルクオフによって、ドライブ出力が無効になり、機械全体の電力供給を停止することなくモータトルクを除去できます。安全速度モニタでは、アプリケーションの速度を落としてモニタすることができるため、機械を完全に停止することなく、オペレータが一定の種類の作業を安全に実施することができます。

接続システム/ネットワーク

- **「クイックコネクト」接続システム**
  Guardmaster® 安全Tポート/スプリッタと配電ボックス、短絡プラグは、機械の安全保護に特化したクイック・ディスコネクト・システムの一部です。

- **GuardLink™**
  GuardLinkは安全に基づいた、トランク&ドロップトポロジでのプラグ&プレイコネクション付きの標準的な配線を使用する通信プロトコルです。シングルケーブルでリモートリセットやロックコマンドなどの安全装置の診断および制御のための通信が可能になります。最大32のデバイスを最長1,000mのケーブル距離で接続できます。GuardLinkテクノロジが搭載されたAllen-Bradleyの安全装置を使用すると、安全システムの情報にEtherNet/IPを介してアクセスできます。GuardLinkはシステム構成を簡略化し、配線を削減し、保守や操作に役立つ診断情報が増加します。

- **Safety over EtherNet/IP**
  EtherNet/IP™ネットワークを使用することで、業界標準のオープンネットワーク技術を利用した、工場全体をカバーできるネットワークシステムを構築できます。ディスクリート、連続プロセス、バッチ、安全、ドライブ、モーション、高可用性などさまざまなアプリケーションで、リアルタイムでの制御と情報の流通を可能にします。EtherNet/IPネットワークでは、モータスタータやセンサなどの装置をコントローラやHMI装置に接続し、さらに企業の基幹ネットワークにつなげることができます。つまり、非産業用通信と産業用通信の両方を単一の共通ネットワークインフラ基盤上で行なうことができます。

便利なツールの利用

安全規格への適合をサポートし、人身事故のリスクを軽減し、生産性を向上させる豊富なツールを揃えています。

Safety Automation Builder

Safety Automation Builderは、機械安全の設計と検証を簡易化し、時間とコストを節約するのに役立つ無料のソフトウェアツールです。RASWinリスク·アセスメント·ソフトウェアとの統合により、機能安全ライフサイクルを一貫した、信頼性の高い、文書化された形で管理できます。Safety Automation Builderは、安全システムのレイアウト、製品選択、安全分析を含む安全システムの開発全体を通じてユーザをガイドすることにより安全システムの設計を合理化し、国際規格である(EN) ISO 13849-1によって規定された機械安全の安全遂行レベル(PL)の達成を支援するとともに、コンプライアンスを向上させコストを削減します。

RASWin

RASWinソフトウェアは、機能安全ライフサイクル全体を通じた進行をユーザが管理することを支援し、プロセスおよび機械の妥当性確認の各ステップから得られた情報を整理します。RASWinは、安全機能の仕様、要求される安全遂行レベル(PLr)の割付けとPLrの計算、安全回路の妥当性確認、および文書化を含む安全ライフサイクルの各ステップを結び付けます。

SISTEMA Performance Level Calculator

SISTEMAツールは、ドイツ法的損害保険の試験研究機関(IFA)の労働安全衛生研究所によって開発され、(EN) ISO 13849-1に従って機械制御システムの安全関連部分が達成する安全遂行レベルの計算を自動化します。ロックウェル·オートメーションの機械安全製品のデータは、SISTEMA計算ツールで使用できるライブラリの形式で入手できます。この2つの組み合わせにより、機械およびシステム設計者は、(EN) ISO 13849-1に従った安全評価の総合的なサポートが得られ、時間を節約することができます。Safety Automation Builderからのエクスポート機能により、要求安全遂行レベルの第三者による検証を受けるために、安全システムの設計を簡単にSISTEMAにインポートできます。

機械のエンジニアリング済みの安全機能

機械安全機能には、センサや入力デバイス、ロジックデバイス、出力デバイスなどの多くの要素が必要です。これらの要素を組み合わせることにより、(EN) ISO 13849-1に規定された安全遂行レベルによって計算された水準の保護が得られます。ロックウェル·オートメーションは、数多くの安全機能の文書を作成し、それぞれの文書は、機能要件、機器の選択、および要求安全遂行レベルに基づいた特定の安全機能の指針を提供します。これらの内容には、セットアップや配線、構成、検証および妥当性確認計画、および安全遂行レベルの計算が含まれます。

Safety Maturity Index (安全成熟度指数)ツール

Safety Maturity Index™ (安全成熟度指数)は、安全文化、コンプライアンスプロセスおよび手続き、および安全テクノロジへの資本投資などにおけるパフォーマンスの総合的な測定基準です。このツールにより、各企業は現在の自社の安全遂行レベルを理解し、安全および収益性を改善するために使用できる手段が分かります。

サービスと経験によりお客様をサポート

世界最大の産業安全プロバイダとして、ロックウェル·オートメーションは怪我のリスクとコストを低減しながら、安全ライフサイクルのあらゆる局面で生産性を向上させるためのサポートを行なっています。

当社の安全サービスは、経験豊富で安全資格(その多くはTÜV Rheinlandの機械安全認定)を有するスタッフによって提供されます。ロックウェル·オートメーションでは、TÜV機能安全エキスパートの有資格者やエンジニア、技術者を雇用し、お客様の安全ライフサイクルを総合的にサポートします。

安全ライフサイクルは明確に定義されたプロセスであり、機械リスクを評価し軽減するために必要なステップを特定することにより生産性を最大化し、安全を向上させます。安全ライフサイクルについては、本書を参照してください。関連サイトから資料をダウンロードすることもできます。

提供されるサービスには以下が含まれます。

- **安全の評価**
  工場リスクの評価を支援し、十分に情報を得た意思決定をサポートすることにより従業員および機械安全を向上させるためのサービスを提供します。
- **設計サービス**
  総合的な回路設計やデバイスの正しい適用および設計レビューにより全体的な安全の向上をサポートします。
- **設置および妥当性確認サービス**
  システムが定義されたパラメータおよび規格に従って動作していることを検証します。
- **安全トレーニング**
  業界トップのエキスパートが提供する総合的なトレーニングプログラムです。
- **カスタマイズサービス**
  お客様固有のアプリケーション、テクノロジ、プラットフォーム、および構成を網羅しています。

ロックウェル･オートメーションを選択する理由

機器の設計および試験、設置および立上げから運転および保守、さらに最新化や廃棄までの製造プロセスの多くのステージで安全をオートメーションに統合することによって生産性の向上を実現できます。あらゆるステージが適切に導入される安全ソリューションを通じて最適化できます。

ロックウェル･オートメーションは、産業オートメーションおよび安全分野のグローバルリーダ、テクノロジイノベータとして、より効率的で安全な生産性の高いお客様の製造ソリューション開発をサポートする理想的なパートナです。

オートメーションおよび安全分野における長年の経験、アプリケーションの専門知識、およびISO 12000、(EN) ISO 13849-1およびIEC 62061などの安全規格の最先端の基本理念の適用を通じて、ロックウェル･オートメーションは、機械安全、プロセス安全および電気安全ソリューションの選択、統合、トレーニングおよびサポートによりお客様の成功をお手伝いします。

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

ロックウェル オートメーション ジャパン株式会社
本社営業部 〒104-0033 東京都中央区新川1-3-17 Tel (03) 3206-2786 Fax (03) 3206-2796
関西支店 〒532-0003 大阪市淀川区宮原4-1-14 Tel (06) 6397-1020 Fax (06) 6397-1090
中部支店 〒460-0003 名古屋市中区錦1-6-5 Tel (052) 222-7060 Fax (052) 222-7065

Publication: SAFEBK-RM002C-JA-P - November 2016