ISO13849-1:2023

ISO 13849-1:2023

機械類の安全性－制御システムの安全関連部－第1部：設計のための一般原則

Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design

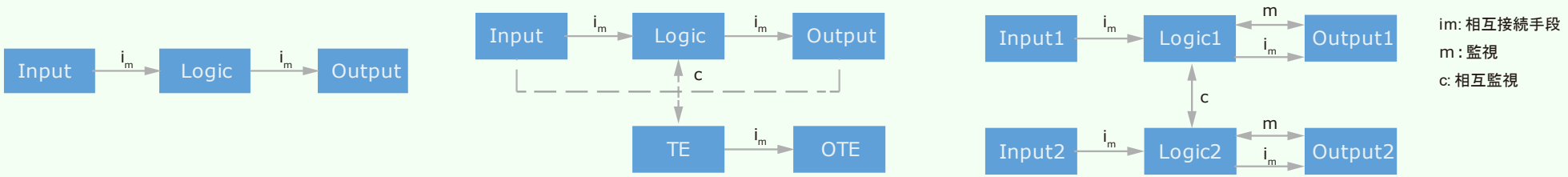
ISO13849-1の改訂版が2023年4月26日に発行された。

EN/ISO13849-1:2023は既に機械指令2006/42/ECの整合規格となっているが、旧規規格EN/ISO13849-1:2015年が、失効となるのは2026年5月31日であるので、

2026年6月1日よりEN/ISO13849-1:2023に完全移行となり、その後2027年1月20日より機械規則Regulation（EU）2023/1230の整合規格となる。

ISO13849-1:2023に基づく制御システムの安全関連部　PLにより安全性能を評価

確定的なリスク低減：制御システムの安全関連部の物理的な構造カテゴリ



＋

確率論的なリスク低減（コンポーネントの安全に関する信頼性、危険側故障の検出、設計の確かさなど）

平均危険側故障時間$MTTF_D$

危険側故障を生じるまでの平均時間の期待値

（コンポーネントの安全関信性）

診断範囲DC

検出される危険側故障率と全危険側故障率との比

（危険側故障検出の確かさ）

CCFに対する方策

単一の事象から生じる異なったアイテムの故障に対する方策

（安全設計の確かさ）

パーフォーマンスレベルPLで制御システムの安全関連部の安全性能を評価

(新設)箇条5.安全関連要求仕様(SRS)の作成

安全関連要求仕様safety requirements specification (SRS)の作成

今回の改訂により、箇条5の安全機能の仕様化を行う最初のステップとして、安全関連要求仕様の作成が要求されるようになった。

安全関連要求仕様とは、本規格において、以下のように定義されている。

3.1.3安全機能の特性(機能要求)および要求される性能レベル(PLr)(3.1.6)の観点から、制御システムの安全関連部が満たさなければならない安全機能の要求(3.1.27)を含む SRS 仕様。

安全要求仕様を作成する事で、安全機能を実現する制御システムの安全関連部の設計仕様を明確にするだけでなく、その安全性の妥当性を確認するための指標も明確化される利点がある。

5.2.1.2 安全要求 (SRS) を作成するために必要な情報を収集し、5.2.1.3 安全要求 (SRS)におけるすべての安全機能の仕様を文書化する。

(新設)5.2.1.3安全要求仕様SRSにおける全ての安全機能の仕様

5.2.1.3 安全要求仕様(SRS)におけるすべての安全機能の仕様

SRS には、特定のアプリケーションに関連する各安全機能について次の情報が含まれている必要があります。

NO	内容
a)	安全機能の簡単な説明/タイトル。 例:インターロック付き可動ガードにより始動する安全停止　例:非常停止機能
b)	安全機能をトリガーするイベント。 例:インターロック付き可動ガードが開く　例:非常停止ボタンを押す
c)	意図した安全状態に到達するために、安全機能出力によって開始される反応。
例1:	危険な動きを停止する
d)	要求されるパフォーマンスレベル PLr (5.3 を参照)。
e)	安全機能に対する要求が行われた後、機械が安全な状態に達するまでの応答時間。 ISO 13855:2010 に準拠したシステム全体の停止パフォーマンス (反応時間と停止時間の合計)。
f)	安全機能がアクティブになる動作モード。

(新設)5.2.1.3安全要求仕様SRSにおける全ての安全機能の仕様

NO	内容
g）	安全機能と機械制御システム及び他の安全機能とのインターフェース。
例2	機能チャネルに障害があり、制御された停止が不可能な場合は、即時の非制御停止を使用して障害対応を開始できる。
i）	電源喪失時の機械の動作（5.2.2.8 を参照）。
例3	重力による落下を防ぐために、垂直軸を所定の位置に保持する必要がある場合がある。 重力負荷がかかる軸など、外力が機能安全に影響を与える可能性がある場合、体系的な要求により補強(パワー要素など)が必要になる場合がある。 適切な設計ソリューションとしては、シリンダーに逆止弁を組み込むか、補助的な機械ブレーキを組み込むことが考えられる。これには、2つの別個の安全機能の設計も必要になる場合がある。 1つは電源が利用可能で、もう 1 つは電源が利用できないものとする。
j）	j）安全機能の需要率及び/または SRP/CS の動作頻度。
k）	k）同時にアクティブになり、競合する動作を引き起こす可能性がある安全機能の優先順位。

(追記)7. ソフトウェア安全要求事項図14b)

事前に評価された安全関連のハードウェアおよびソフトウェア モジュールを LVL と組み合わせて使用する場合は、図 14 b) に示す簡略化されたソフトウェア ライフサイクルが適用される。

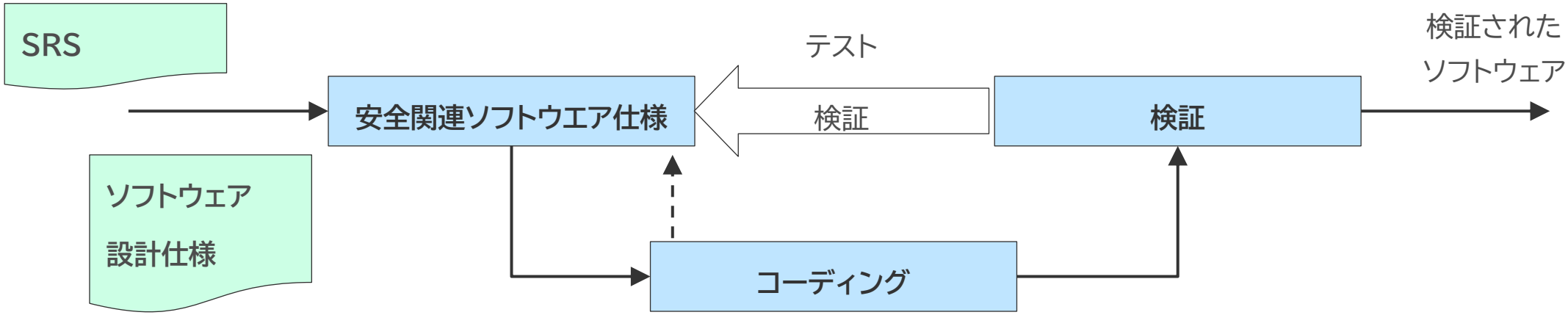


図14b) 事前検証された安全関連のハードウェア及びソフトウェアモジュールが LVL と組み合わせて使用される場合のソフトウェアの簡略化された V モデル

注記:一般的に、図 14 b) に示すソフトウェア ライフサイクルは、LVL でのモジュールベースのプログラミングの使用に適用される。このプログラミングでは、単純な相互接続のみを構成する必要があり、入力と出力はモジュールの組み合わせを含む定義済みの値のセットに制限される。

(新設) 6.1.7 システマティック故障

システマティック故障は、例えば次のようなさまざまな理由で発生する。

— 設計仕様の誤り

— 製造上の不具合

— 環境ストレスの影響 (温度、振動、EMI 耐性など)

— 運用上の不具合

— SRS、ハードウェアおよびソフトウェアの設計における人為的エラー。

体系的完全性の十分なレベルを確立するには、安全機能の設計と実装のアプローチは体系的でなければならない。

SRP/CS の要求された機能安全を達成するために必要な行動は、機能安全計画に文書化しなければならない。

機能安全計画は、誤った仕様、実装、または変更の問題を防ぐための対策を提供することを

目的としなければならない。

特に設計プロセスでは、体系的故障の制御と回避を実施しなければならない。(第 10 項および付録 G を参照)。

(追記)A3.3 危害を回避または制限する可能性P1及びP2

表 A.1 ― 5 つの要素に基づくパラメータ P の決定(リスクグラフにおけるパラメータP決定のガイドライン)

因子	C	B	A
1.機械のオペレータ		非熟練者[a]	熟練者[a]
2.危険事象を引き起こす可能性のある機械の部分の速度	速度> 1,000 mm/s、 危険源までの時間 < 1 秒、	250 mm/s＜速度≦1,000mm/s 1秒≦危険源までの時間＜ 3 秒	速度< 250 mm/s、 危険源までの時間 ≥ 3 秒、
3.危険源からの脱出可能な空間	不可能	時々/ほとんどない 50%未満の場合可能	容易に可能 50%以上の場合可能
4.危険源を認識･気づく可能性	不可能	時折/まれに危険源が認識される 50% 未満	容易に危険源を認識可能 50%以上
5.作業のために必要な人的介入の回数及び又はタイミング		中程度から高い複雑さ	複雑さの低い

(追記)付属書F CCFに対する方策

F.3.1 分離/隔離

a) 配線の分離(例:導体間に適切な絶縁を施した多軸ケーブル)

e) 別個のプリント基板上、または別個のハウジングまたはキャビネット内の冗長チャネル。など

F3.2 多様性

— チャンネル1はゴムシール付きバルブとチャンネル2は金属シール付きバルブを使用

— 可動ガード の開を検出するためにNC接点とNO接点を使用。など

F3.3.1

a)SRP/CS の入力と出力、及びロジックの電源は、潜在的な過電圧及び/または過電流のレベルから保護されていること　など

F.3.4 査定/分析

CCF の原因を特定するために故障モード及び影響分析 (FTA) が実行し、設計で CCF を回避すること　など

F.3.5 訓練

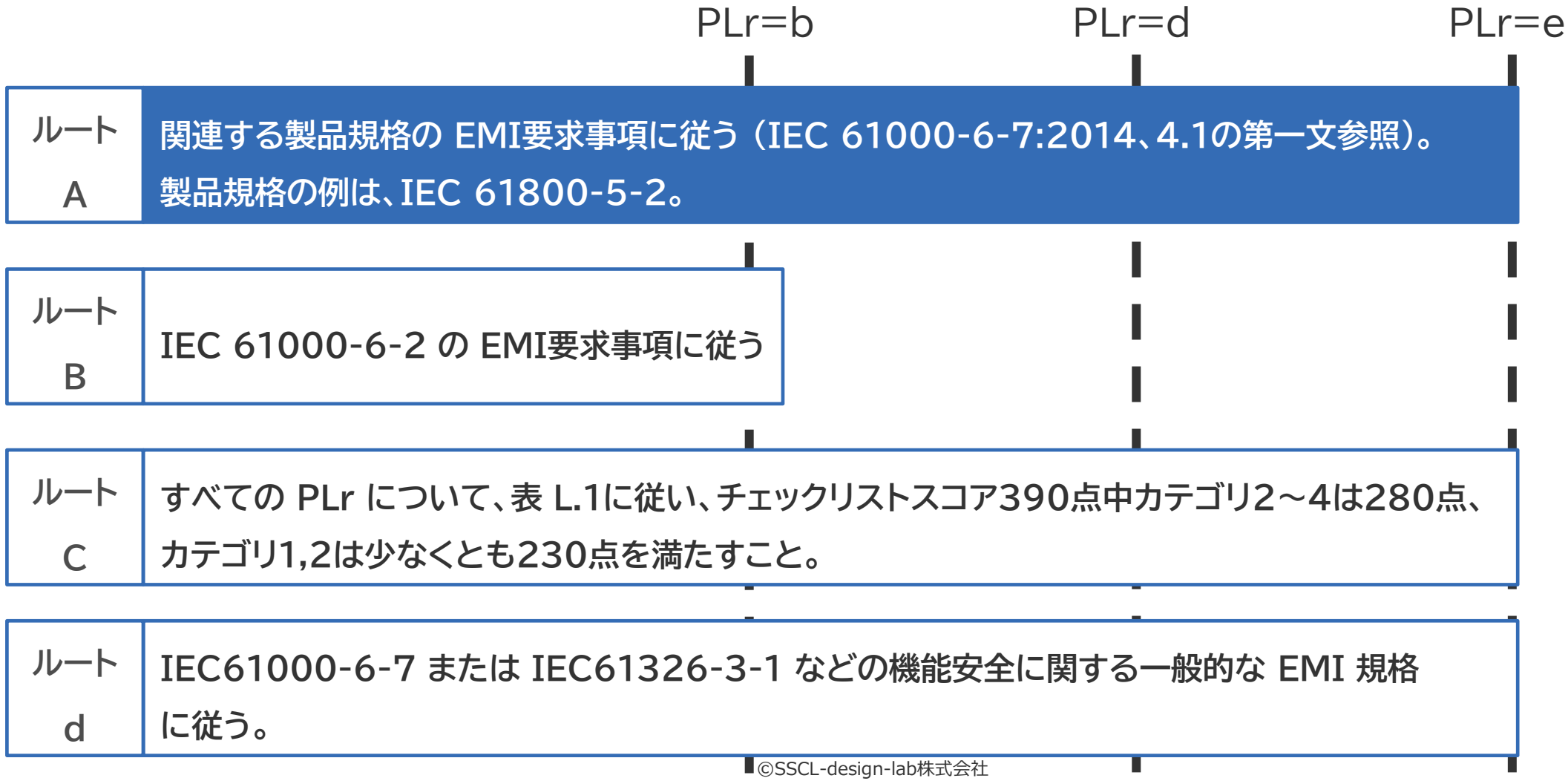
設計者は、CCF の原因と結果を理解するための訓練を受けていることを文書で照明

F.3.6.1 EMI または圧力媒体の汚染の防止

電気/電子システムの場合、適切な規格(IEC 61326-3-1、IEC 61000-6-7:2014、IEC 61000-1-2:2016、IEC 61800-5-2)従って防止　など

（新設）付属書L　電磁妨害 (EMI) イミュニティ

EMIイミュニティ方策として、少なくとも 1 つ以上のルートを選択し、完全に適用すべきである:



（新設）付属書L　表L.1　SRP/CS またはサブシステムの EMI 耐性を実現するための方策

EMI方策	スコア[a)]
SRP/CS の一部としての PLC	
シールドおよびボンディングされたキャビネット内に設置、またはシールドおよびボンディングされたハウジング内のコンポーネント	10
製造者の設置指示に従って十分な距離を保って分離された同じエンクロージャ内の多様な PLC	10 [c),d)]
異なるエンクロージャ内の冗長 PLC	20 [c),d)]
多様なチャネル（例: PLC とディスクリート ロジック）を備えた、又は安全 PLCの使用	20 [c),d)]
安全関連アクチュエータとそのワイヤーハーネス	
IEC 60204-1:2016+AMD1: 2021、付属書 H の方策の適用及び/又はIEC 61800-3の適用（hr）	20
関連する妨害レベルを持つその他のコンポーネントおよび配線	
モーター用のシールドおよびボンディングケーブルまたはモーターとインバータ間の正弦波フィルター、または該当する場合は製造元の設置手順に従った同等の方策（hr）	20
該当する場合は製造元の設置手順に従った安全関連入力信号用の RF フィルター、過電圧および過渡保護（例: フィルター、過渡電圧抑制ダイオード、オプトカプラ、フェライト）（hr）	20
電源用の EMI フィルター（製造元の設置手順に従うか、またはアプリケーション専用）（例: 過電圧過渡保護）	20
IEC 60204-1:2016+AMD1: 2021、付属書 H の方策の適用及び/又はIEC 61800-3の適用	10

(新設)附属書N N.2ソフトウェア妥当性確認の例

N.2 ソフトウェア妥当性確認の例

N.2.1 全般

妥当性確認の目的は、ソフトウェアが全体的なソフトウェア要求事項を満たしていることを確認するとである

N.2.2 コーディング ガイドライン

コーディングは、該当する場合は、ソフトウェア プラットフォームの製造元が要求するコーディング ガイドラインに従って行うべきである。

N.2.3 安全機能の仕様

アプリケーション図、ハードウェア構成図、ブロックダイヤグラムにより仕様化

N.2.4 ハードウェア設計仕様からの入力情報

配線とハードウェアドレスが正しいか検証

N.5 アプリケーションプログラム

図N.6 ファンクションブロックによるアプリケーションプログラム

N.2.6 実装されたSRASW(安全関連アプリケーションソフトウェア)の妥当性確認

FMEA とテストによる安全機能の妥当性確認

(新設)付属書N　表 N.6 非常停止の FMEA とテスト

表 N.6 非常停止の FMEA とテスト

関連する入力				
信号	I/O	Data Type	情報	備考
ES1 Channel1: IS_bES1_1 Emergency Stop	I1.4	Bool	Channel1 と Channel2 間の不一致 時間0.5秒	Emergency stop NC 強制開離動作
ES1 Channel2: IS_bES1_2 Emergency Stop	I1.5	Bool	Channel1 と Channel2 間の不一致 時間0.5秒	Emergency stop NC 強制開離動作
ACK1: I_bACK1 Reset	I1.6	Bool	NO	非常停止ES1に共通で使用されるリセット機能
関連する出力/フラグ				
信号		Data Type	情報	備考
#bES1_OK		Bool	NO	このリリースフラグは以降の処理に使用されます。
#bES1_ERROR		Bool	NO	このエラーフラグは以降の処理に使用されます。

(追記) 12 技術文書

この文書に従って SRP/CS を設計する場合、安全関連部分に関連する少なくとも次の情報を内部目的で文書化しなければならない。

NO	内容
a)	**SRS (5.2.1 を参照)。**
b)	安全関連部分が開始及び終了する正確なポイント。
c)	該当する場合、サブシステムへの分解(5.2.2 を参照)。
d)	環境条件　**(EMI 耐性、温度、振動など)。**
e)	達成されたパフォーマンスレベルとPFH値。
f)	選択されたカテゴリ (以前に検証されたサブシステムには適用できない場合があります)。
g)	信頼性 (MTTFD、DC、CCF、及び T10D) 及びミッション時間に関連するパラメータ。
h)	システマティック故障に対する方策。
i)	使用した技術方式。
j)	考慮した全ての安全関連障害

（追記）12 技術文書

NO	内容
k）	障害の除外に関する正当化の根拠（ISO 13849-2:2012 の 6.1.10.3 及びすべての付属書を参照）。
l）	該当する場合、ソフトウェア関連文書。
m）	合理的に予見可能な誤使用に対する方策。
n）	**安全関連のブロック図。**
o）	**該当する場合、関連する設計文書、試験、検証、検証記録。** **注 設計文書は一般に、製造業者の内部目的、または協力会社や外部請負業者（外部のシステム設計者、認証機関など）と製造業者の間で技術情報を交換するために使用されることを想定している。** **設計文書は法的文書要件を満たすためにも必要である。** **設計文書は機械の使用者に提示する必要はないが、その一部は使用するための適切な情報を準備するために関連する（箇条13 を参照）。**

(追記) 13.3ユーザのための情報

SRP/CS を正しく使用するために重要な情報は、機械のユーザー（オペレーターなど）に提供されなければならない。メンテナンスの情報には、次のようなタスクやアプリケーションが含まれる。

NO	内容
a)	設定。
b)	教育/プログラミング。
c)	プロセス/ツールの切り替え。
d)	洗浄。
e)	予防保全。
f)	事後保全。
g)	トラブルシューティング/障害検出。
k)	安全機能の検査の性質と頻度。
i)	技術的知識または特定のスキル、またはその両方を必要とするメンテナンス作業に関する指示。したがって、資格のある担当者（例: メンテナンススタッフ、専門家）のみが実行する必要がある。

(追記) 13.3ユーザのための情報

NO	内容
j)	特定のスキルを必要としない、したがって、機械のユーザー（例: オペレーター）が実行できるメンテナンス作業（例: 部品の交換）に関する指示。どの部品が安全にとって重要であり、元の部品または同じ安全要件を満たす部品とのみ交換する必要があることを保守スタッフに知らせる必要がある。
k)	k) 危険なエネルギーの制御(手動/その他の手段)指導、標示、装置。
l)	保守要員がタスクを実行できるようにする図面/ダイアグラム(特に、障害の原因となった状態を特定するための障害発見に関するタスク)。
m)	Tm 期間終了時または終了前のコンポーネントの交換に関する情報（空気圧、機械および電気機械コンポーネントについては、C.4.2 も参照)。

注 1 詳細については、ISO 20607:2019 及び IEC 60204-1:2016+AMD1: 2021、17.2 f を参照。
メンテナンス作業で SRP/CS の修理または変更が必要な場合は、機能試験を含む再度の妥当性確認を実行しなければならない。
注 2 関連する再度の妥当性確認の実施内容は、元のコンポーネントと置き換えるコンポーネントの間の差異の程度によって異なる。

ISO13849-1:2023主要な改訂内容まとめ

新規：SRS仕様書の作成が新規で要求事項化（箇条5.2）

追記：安全関連ソフトウエア要求事項が詳細に規定（箇条7）

新規：システマティック故障についての説明が新設（箇条6.1.7）

追記：妥当性確認について、妥当性確認のプロセスが詳細に規定（箇条10）

追記：リスクグラフによる要求PL_rの決定において、特に危険源回避の可能性についての決定方法が詳細に規定（付属書A）

追記：CCFに対する方策の判定基準が詳細に規定（付属書F）

新規：システマティック故障の抑制にG.5機能安全のマネジメントが追加（付属書G）

新規：電磁妨害（EMI）耐性（付属書L）

新規：ソフトウェア設計のシステマティック故障の抑制（付属書N）

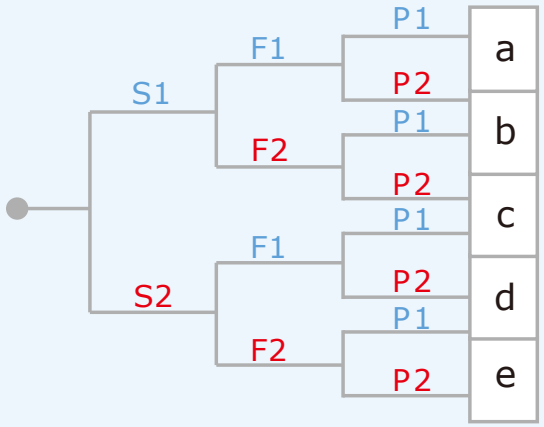
新規：SRP/CSの保全性が新規で要求事項化（箇条11）

追記：技術情報、使用上の情報の要求事項が詳細に規定（箇条12、箇条13）

ISO13849-1:2023に基づく制御システムの安全関連部の設計支援プログラム

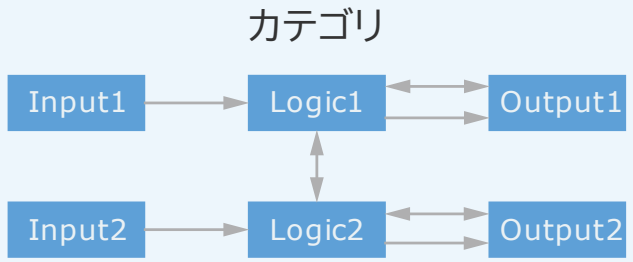
機械安全に関する国際規格のグループ安全規格(タイプB規格)の中で最も重要な規格の1つとして、制御システムの安全関連部(以下SRP/CS)の設計原則について規定したのが「ISO13849-1」です。特に欧州、北米に輸出する機械のリスク低減を制御により行う場合、リスクの大きさ(要求パフォーマンスレベルPLr)に応じて適切な性能パフォーマンスレベル(PL)を満たすSRP/CSを実装する事が要求されます。
具体的な設計評価のプロセスは下記のとおりです。

リスクグラフによる要求PLrの決定



S 傷害のひどさ	F 暴露頻度	P 危害回避の可能性
S1 回復可能な傷害	F1 15 分に一回を超えない	P1 特定条件により可能
S2 回復不能な傷害、死亡	F2 15 分に一回を超える	P2 ほとんど不可能

制御システムの安全関連部 (SRP/CS)PL見積



MTTFD

	$MTTF_D$
Low	3≦ $MTTF_D$ <10
Medium	10≦ $MTTF_D$ <30
High	30≦ $MTTF_D$ ≦ 100

DC

None	60>DC
Low	60≦ DC<90
Medium	90≦ DC<99
High	99≧DC

CCF

	項目	スコア
1	隔離と分離	15
2	多様性	20
3.1	過電圧、過圧力、過電流、過熱保護	15
3.2	"十分吟味されている"コンポーネント	5
4	査定・分析	5
5	適応性・訓練	5
6.1	環境面(EMC)	25
6.2	温度、湿度、振動などその他環境	10

安全機能に
対するPLの
検証PL≧PLr

⊕

設計者以外
の人物による
妥当性確認

⊕

技術文書
作成

ISO13849-1:2023に基づく制御システムの安全関連部の設計支援プログラムを開始

改訂されたISO13849-1:2023にお客様が設計した制御システムの安全関連部が適合できるように、

下記のような支援プログラムをオーダーメードで提供します。

①制御システムの安全関連部(SRP/CS)のPL評価代行

設計した制御システムの安全関連部のPL評価と技術レポートの作成代行(PL評価ソフトSISTEMAレポートを含む)します。

SRS仕様書、CCFに対する方策に関する根拠資料、システマティック故障に対する方策の根拠資料も作成します。

※ただし安全関連ソフトウェア妥当性については、お客様と共同で実施します。

②制御システムの安全関連部の妥当性確認

設計した制御システムの安全関連部の設計とPL評価結果の妥当性確認を行います。

③制御システムの安全関連部の設計支援

制御システムの安全関連部がPL≧PLrを達成できない場合、達成できるよう設計変更の具体的なアドバイスを実施します。

④制御システムの安全関連部の設計及び評価トレーニング

お客様がISO13849-1:2023に基づき制御システムの安全関連部を設計しPL評価を実施し、SISTEMAによるPL評価レポートを作成できるようなトレーニングを提供します。