制御システムの安全関連部
ISO 13849-1

第3版概要
第4版改正の動向

テュフラインランドジャパン株式会社
製品事業部　産業機器部
杉田　吉広

目次

1. ISO 13849-1とは？
   1) 適用範囲
   2) 関連規格 (引用規格）
2. ISO 13849-1 第3版概要
3. ISO 13849-1 適用例
4. 第3版対応JIS改正動向
5. 改正履歴
6. 第4版改正動向

ISO 13849-1とは？

- 適用範囲より…
- 制御システムの安全関連部（SRP/CS)の設計の原則、安全要求事項について規定。
- 安全関連部が安全機能を遂行する能力をパフォーマンスレベル（PL)とし、単位時間当たりの危険側故障発生確率（Probability of Dangerous Failure，PFH_D）で規定。

PL	単位時間当たりの危険側故障発生の平均確率（PFH_D） 1/h
a	$10^{-5} \leqq PFH_D < 10^{-4}$
b	$3\times10^{-6} \leqq PFH_D < 10^{-5}$
c	$10^{-6} \leqq PFH_D < 3\times10^{-6}$
d	$10^{-7} \leqq PFH_D < 10^{-6}$
e	$10^{-8} \leqq PFH_D < 10^{-7}$

序文より

- 達成したPLの査定を容易にするために、構造を五つに分類（カテゴリ: B, 1, 2, 3, 4）
- 適用される制御システムの安全関連部
- 保護装置（例：両手操作制御装置、インタロック装置）、電気的検知保護装置（例：ライトカーテン）、圧力検知装置
- 制御ユニット（例：制御機能の論理ユニット、データ処理、監視など）
- 動力制御要素（例：リレー、バルブなど）
- あらゆる種類の機械類に適用
- 単純な据付装置（例：小さな調理用機械、又は自動ドア及びゲート）
- 製造用の据付装置（例：包装機械、印刷機械、プレス機械）

出典；JIS B 9705-1: 2019

ISO 13849-1とは？

関連規格 (引用規格）

ISO 13849-2: 2012* - Safety of machinery – Safety-related parts of control systems – Part 2: Validation

機械類の安全性 - 制御システムの安全関連部ー第2部：妥当性確認

ISO/TR 23849: 2010** - Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery

機械類の安全関連制御システムにISO 13849-1及びIEC 62061を適用する際のガイダンス

ISO/TR 22100-2: 2013, Safety of machinery – Relationship with ISO 12100 – Part 2: How ISO 12100 relates to ISO 13849-1

機械類の安全性 – ISO12100との関係-第2部ISO 12100とISO 13849-1との関係

IEC 62061+A1+A2:2015: Safety of machinery – Functional safety of safety–related electrical, electronic and Programmable electronic control systems

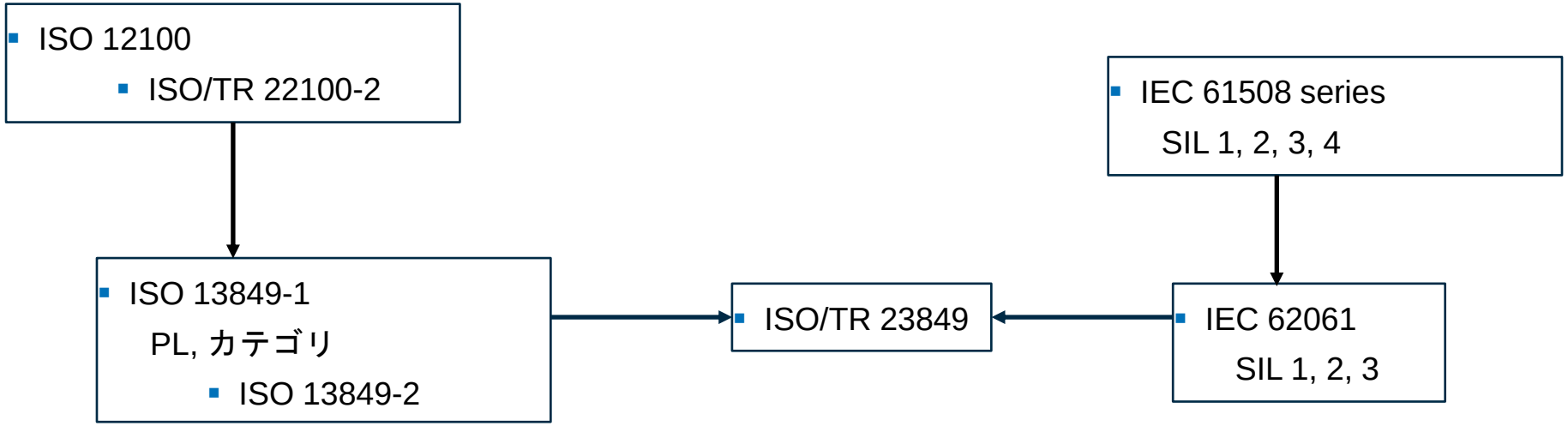
機械類の安全性 – 安全関連の電気・電子・プログラマブル電子制御システムの機能安全

IEC 61508-3/-4: Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements/Part4:Definitions and abbreviations

***: 第4版発行後改訂予定、**: 2020-04: Withdrawn**

関連規格

関連イメージ

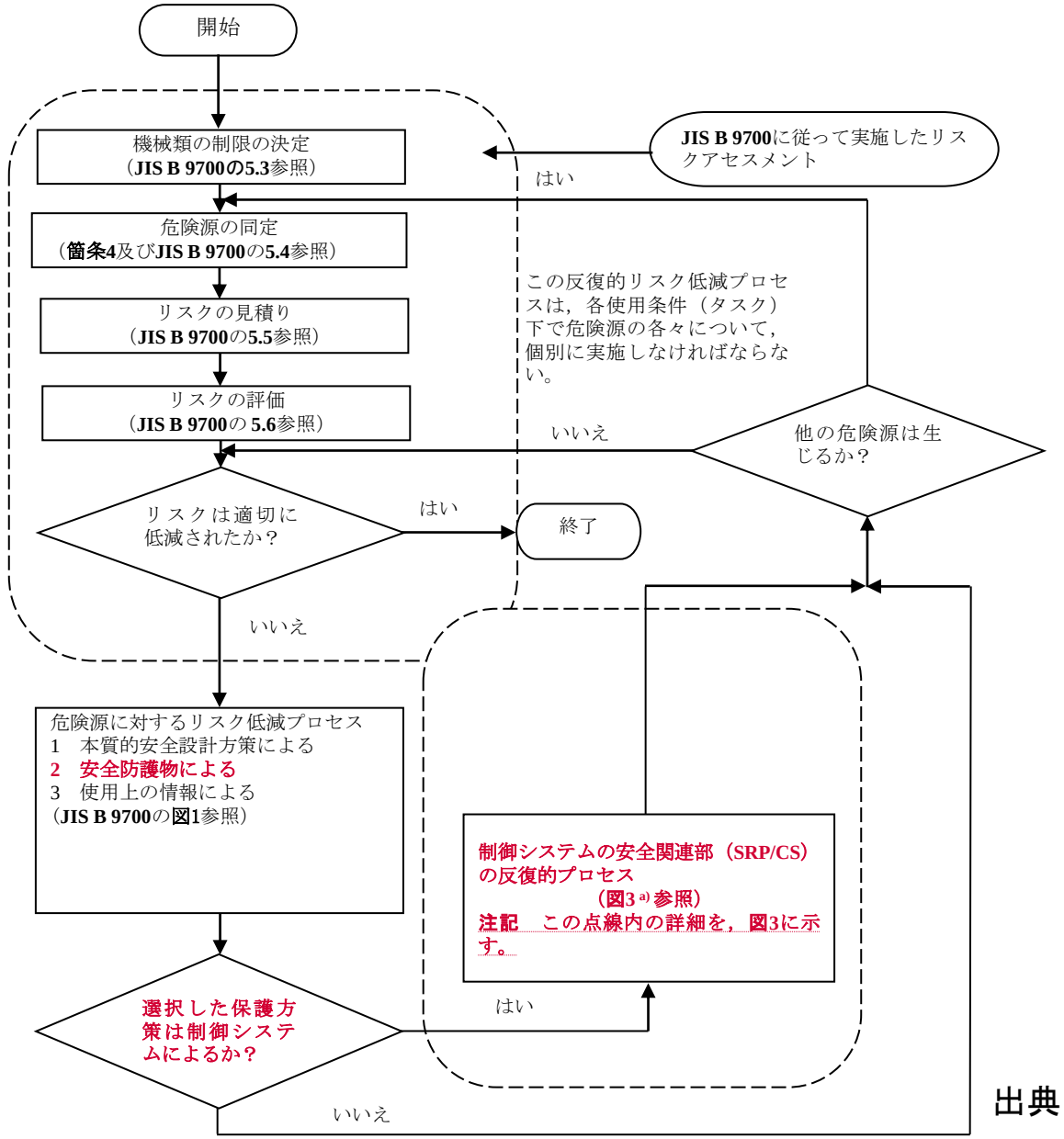


- ISO 12100: Safety of machinery-General principles for design - Risk assessment and risk reduction
- ISO/TR22100-2: Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1
- ISO 13849-2: Safety of machinery - Safety-related parts of control systems - Part 2: Validation
- ISO/TR23849: Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
- IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 62061: Safety of machinery - Functional safety of safety–related electrical, electronic and programmable electronic control systems

ISO 13849-1概要

図1　–　リスクアセスメントとリスク低減

- リスクアセスメントの結果、リスク低減を安全機能をもつ安全防護物の使用により達成する場合
- 安全機能を提供するために割り当てられる機械の制御システムの部分は，制御システムの安全関連部（SRP/CS）とし，ハードウェア及びソフトウェアで構成することができる。

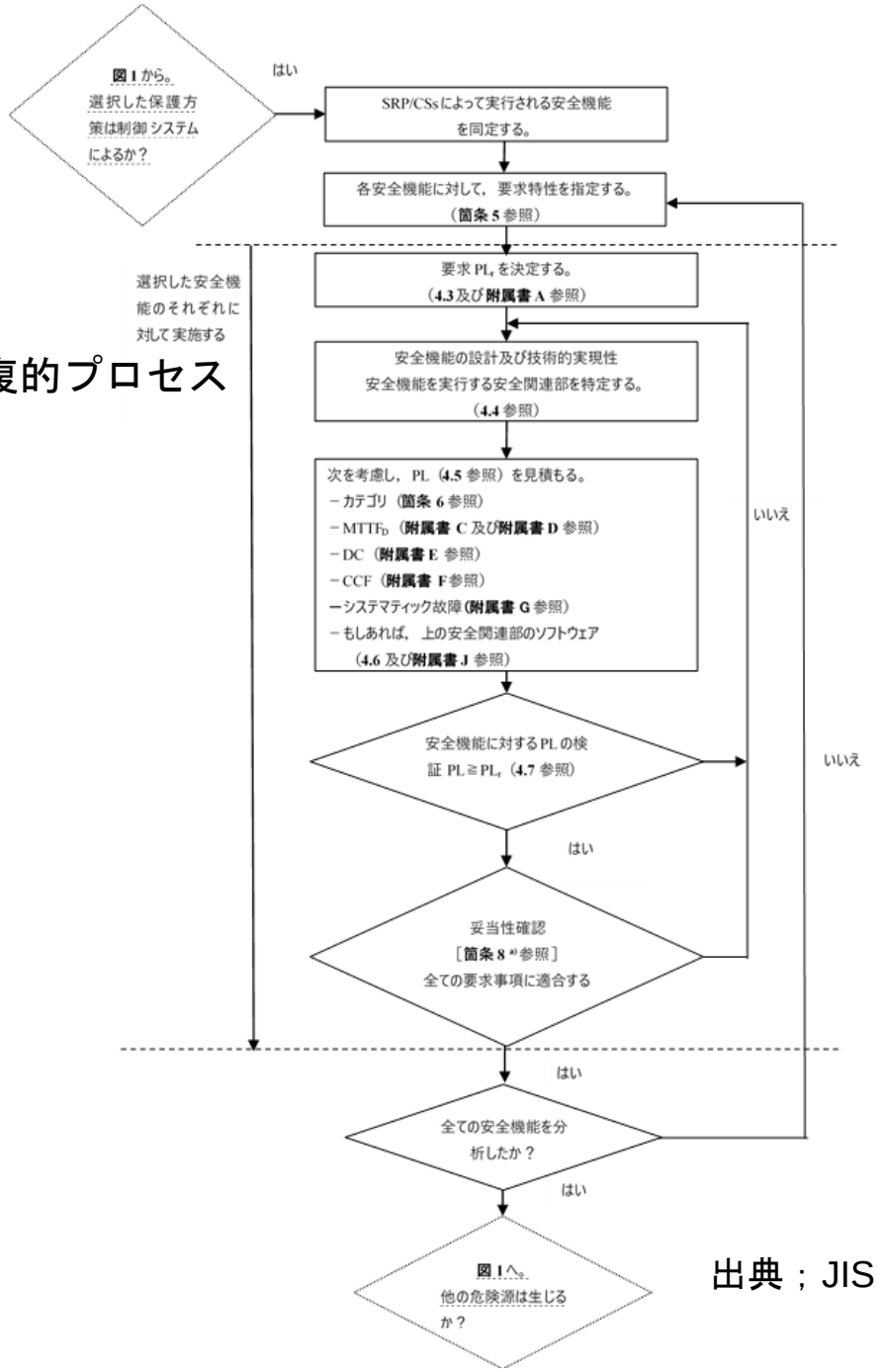


出典；JIS B 9705-1: 2019

ISO 13849-1概要

図3ー制御システムの安全関連部（SRP/CS）の設計のための反復的プロセス

- SRP/CSによって実行される安全機能の同定
- 安全機能に対する要求特性の指定（5章）
- 要求パフォーマンスレベル、PLrの決定（4.3章、附属書A)
- 安全関連部の特定(4.4章）
- PLの見積もり(4.5章)
    - カテゴリ(6章）
    - $MTTF_D$ (附属書C, D)
    - DC (附属書E)
    - CCF　(附属書F)
    - システマティック故障(附属書G)
    - ソフトウエア(使用されていれば）(4.6章、附属書J)
- PLの検証（PL≥PLr)　(4.7章）
- 妥当性確認　(8章、ISO 13849-2)



出典；JIS B 9705-1: 2019

ISO 13849-1概要

安全機能と要求特性(安全機能詳細) （5章）

3.1.20　安全機能　（Safety function):
故障がリスクの増加に直ちにつながるような機械の機能
出展:ISO 12100. 3.30

要求事項: ISO 12100 (JIS B 9700)及び
IEC 60204-1 (JIS B 9960-1)等々

表 8－典型的な機械の安全機能及びその特性に適用可能な国際規格又は JIS

安全機能，特性	要求事項		追加情報
	この規格	JIS B 9700	
安全防護物によって始動する安全関連停止機能 a)	5.2.1	3.28.8，6.2.11.3	JIS B 9960-1 の 9.2.2，9.2.3.3，9.2.3.6 JIS B 9710 JIS B 9715
手動リセット機能	5.2.2	－	JIS B 9960-1 の 9.2.3.3，9.2.3.4.3
起動及び再起動機能	5.2.3	6.2.11.3，6.2.11.4	JIS B 9960-1 の 9.2.3.2，9.2.3.1，9.2.3.2，9.2.3.7，9.2.3.8，9.2.3.9，9.2.3.10
ローカル（局所）制御機能	5.2.4	6.2.11.8，6.2.11.10	JIS B 9960-1 の 10.1.5
ミューティング機能	5.2.5	－	IEC 62046 の 5.7
ホールド・ツゥ・ラン機能		6.2.11.8 b)	JIS B 9960-1 の 9.2.3.7
イネーブル装置機能		－	JIS B 9960-1 の 9.2.3.9，10.9
予期しない起動の防止	－	6.2.11.4	JIS B 9714，JIS B 9960-1 の 5.4
捕捉された人の脱出及び救助	－	6.3.5.3	
遮断及びエネルギーの消散	－	6.3.5.4	JIS B 9714，JIS B 9960-1 の 5.3，6.3.1
制御モード及びモード選択	－	6.2.11.8，6.2.11.10	JIS B 9960-1 の 9.2.3.5，9.3.6
異なる制御システムの安全関連部間の相互作用	－	6.2.11.1 の最終文	JIS B 9960-1 の 9.3.4
安全関連入力値のパラメータ化の監視	4.6.4	－	－
非常停止機能 b)	－	6.3.5.2	JIS B 9703，JIS B 9960-1 の 9.2.3.4.3

注 a)　インターロック付きガード及び制限装置（例えば，過速度，超過温度，超過圧力）を含む。
b)　付加保護方策については，JIS B 9700 参照。

出典；JIS B 9705-1: 2019

ISO 13849-1概要

安全機能と要求特性(安全機能詳細) （5章)

5.1 安全機能仕様

- 考慮するべき点

a) 個々の危険源又は危険状態に対するリスクアセスメントの結果

b) 次を含む，機械の運転特性

- 機械の意図する使用（合理的に予見可能な誤使用を含む。）
- 運転モード［例えば，ローカル（局所）モード，自動モード，機械の一区域又は一部分に関連するモード］
- サイクルタイム
- 応答時間

c) 非常操作

d) 異なる作業プロセス及び手動作業（修理，調整，清掃，トラブルシューティングなど）での相互作用に関する記述

e) 安全機能で達成する又は回避する機械の挙動

f) 動力喪失時の機械の挙動（**5.2.8** 参照）

注記 2 幾つかの場合，動力喪失時の機械の挙動，例えば，重力による落下を回避するために垂直軸を保持することが必要な場合などを考慮する必要がある。これには，動力が供給されている場合と供給されていない場合とで二つの異なる安全機能が要求されることがある。

g) 機械が作動可能又は不可能となる条件（運転モードなど）

h) 運転頻度

i) ある機能が同時に作動した場合の優先順位

出典；JIS B 9705-1: 2019

ISO 13849-1概要

要求PLrの決定（4.3章、附属書A)

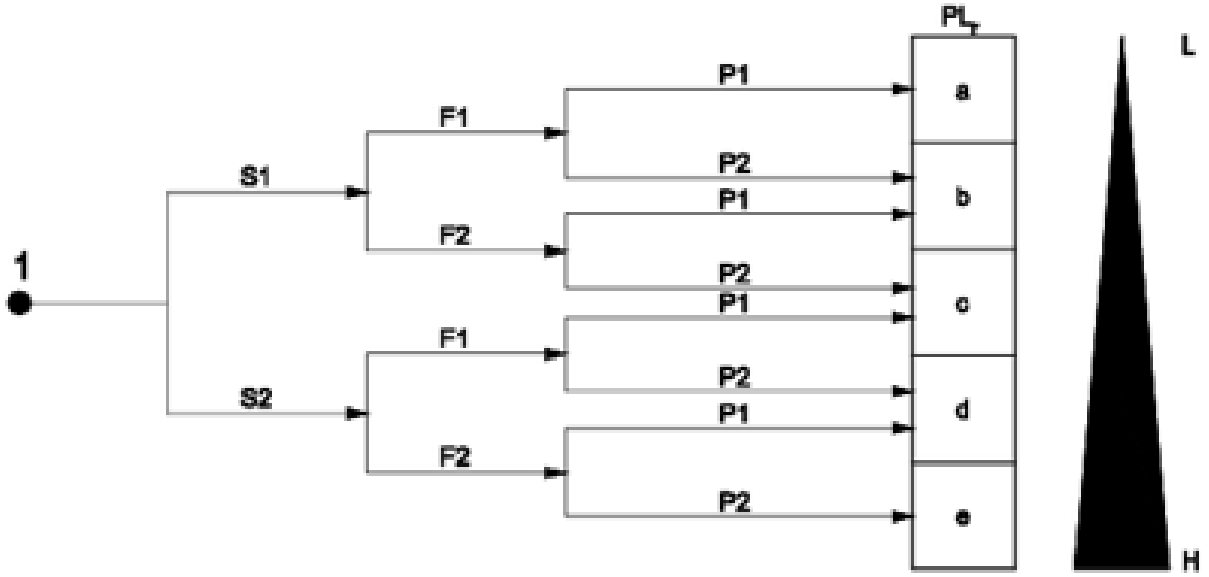
- 機械全体に対するリスクアセスメントによる安全関連PLrを決定するための指針(附属書A,　図A.1)

記号の説明

1	リスク低減に安全機能の寄与度を評価するための開始点
L	リスク低減への寄与度“低”
H	リスク低減への寄与度“高”
PL_r	要求パフォーマンスレベル

リスクパラメータ

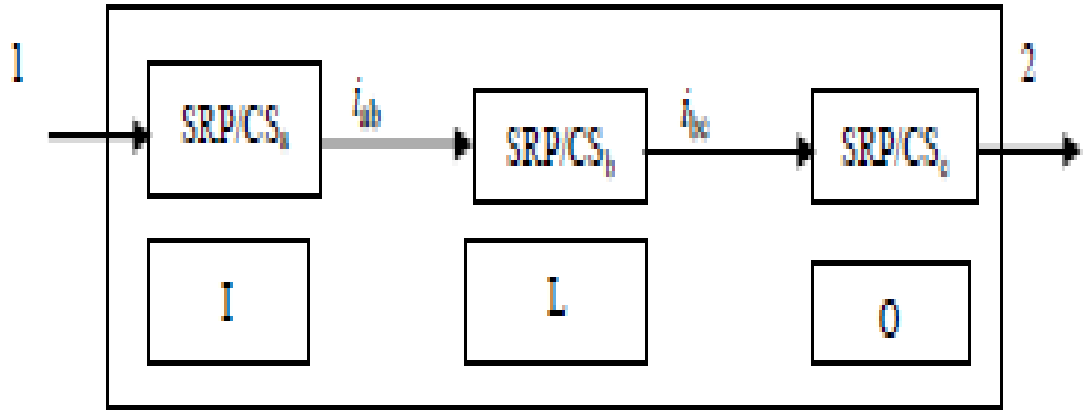
S	傷害のひどさ
S1	軽症（通常，回復可能な傷害）
S2	重傷（通常，回復不可能又は死亡）
F	危険源への暴露の頻度及び／又は時間
F1	まれ～低頻度，及び／又は暴露時間が短い
F2	高頻度～連続，及び／又は暴露時間が長い
P	危険源回避又は危害の制限の可能性
P1	特定の条件下で可能
P2	ほとんど不可能



出典；JIS B 9705-1: 2019

ISO 13849-1概要

図4－代表的な安全機能を処理するための制御システムの安全関連部の組合せに関するダイアグラム



記号の説明

I: 入力（例えば，リミットスイッチ，センサ，AOPD）

L: 論理処理

O: 出力（例えば，バルブ，接触器，電流変換器）

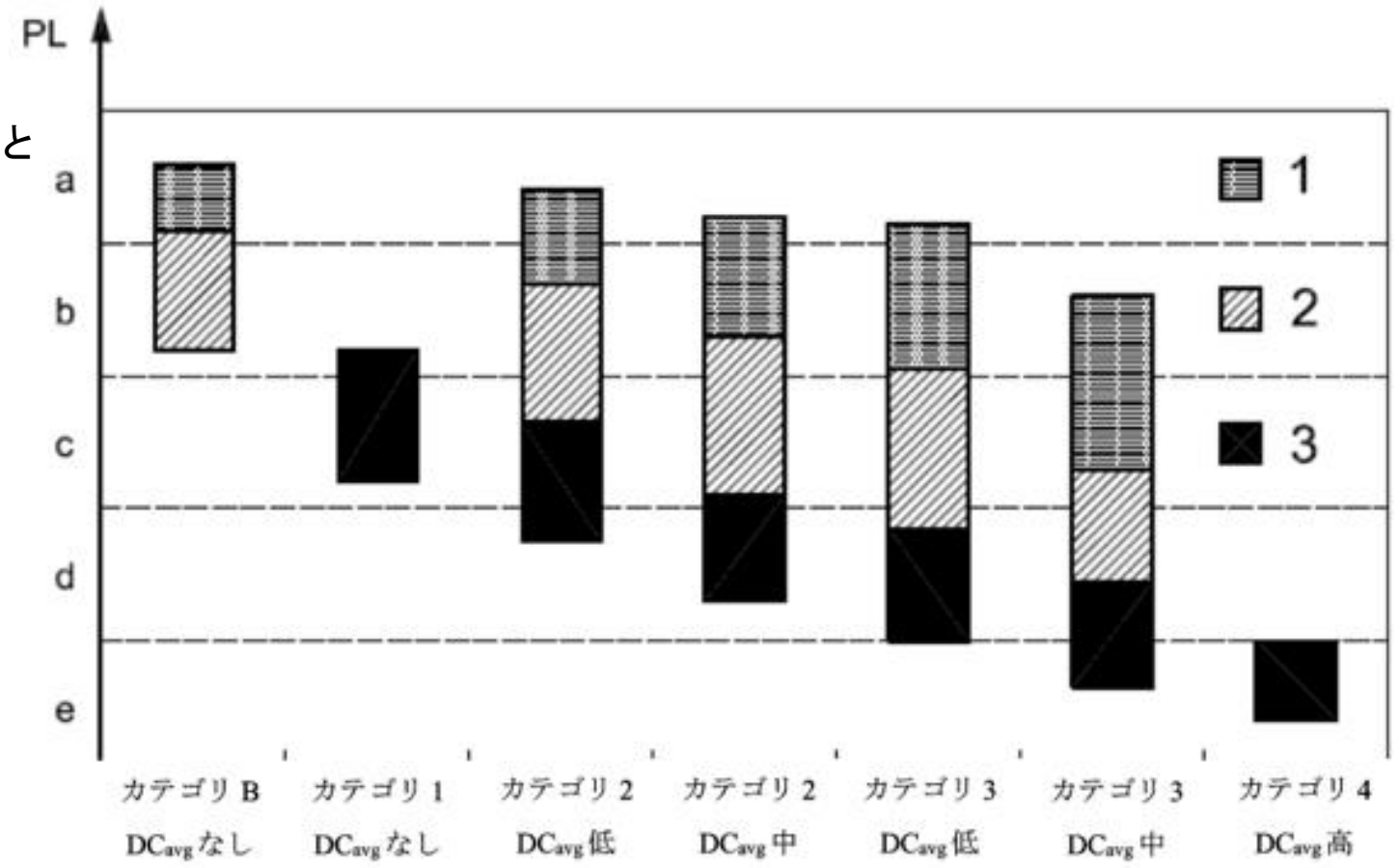
1: 開始事象［例えば，押しボタンの手動操作，ガードの開，能動的光電保護装置（AOPD）のビーム遮断］

2: 機械アクチュエータ（例えば，モータ，シリンダ）

ISO 13849-1概要

安全関連部の特定(4.4章）

図5－カテゴリ、DCAvg、各チャネルの$MTTF_D$とPLとの関係



記号の説明

PL パフォーマンスレベル
1 各チャネルの $MTTF_D$＝“低”
2 各チャネルの $MTTF_D$＝“中”
3 各チャネルの $MTTF_D$＝“高”

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

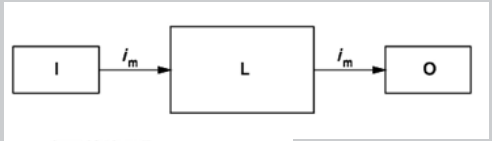
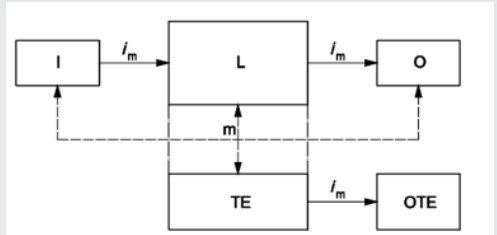
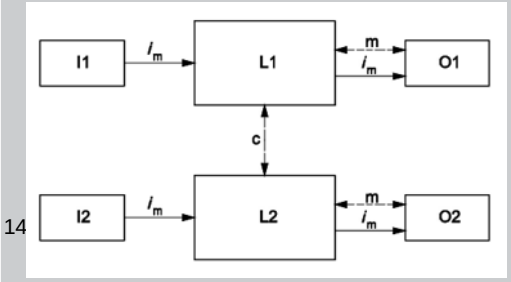
- 3.1.2 カテゴリ: 障害に対する抵抗性（フォールト・レジスタンス）、及び障害条件下におけるその後の挙動に対する制御システムの安全関連部の特性の分類であって、当該部の構造的配置、障害検出及び/又はこれらの信頼性によって達成される

カテゴリ	概要
B	基本安全原則 予想される操作ストレス（遮断容量、頻度等）に関する信頼性
1	カテゴリBに加え、 ”十分吟味されたコンポーネント”及び”十分吟味された安全原則”
2	カテゴリBに加え、 ”十分吟味された安全原則” 安全機能が適切な間隔でチェック
3	カテゴリBに加え、 ”十分吟味された安全原則” 単一障害で安全機能は喪失しない、単一障害はできる限り検出される
4	カテゴリBに加え、 ”十分吟味された安全原則” 単一障害で安全機能は喪失しない、単一障害は安全機能実行時、若しくはその前に検出。 これが不可能であれば故障の累積で安全機能を喪失しない

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

アーキテクチャ	概要	最大PL
 i_m 相互接続手段 I 入力装置。例えば，センサ L 論理 O 出力装置。例えば，主接触器	カテゴリB又はカテゴリ1 単一の障害で安全機能の喪失の可能性 カテゴリ1のMTTF$_D$はカテゴリ Bより長く安全機能の喪失の可能性はカテゴリBより少ない	B: b 1: c
 i_m 相互接続手段 I 入力装置。例えば，センサ L 論理 m 監視 O 出力装置。例えば，主接触器 TE 試験装置 OTE 試験装置の出力 破線は，合理的に実行可能な障害検出を表す。	カテゴリ2 故障が検出されない場合、運転を許可又は検出された場合、適切な制御動作を始動するための出力信号（OTE) チェック間に発生した障害により、安全機能の喪失の可能性	最大PL: d
 i_m 相互接続手段 c 相互監視 I1，I2 入力装置。例えば，センサ L1，L2 論理処理 m 監視 O1，O2 出力装置。例えば，主接触器 監視を示す破線は，合理的に実行可能な障害検出を示す。	カテゴリ3又は4 未検出の障害の蓄積で安全機能が喪失する可能性(カテゴリ3） 障害を適時検出（カテゴリ4） 未検出の障害の蓄積の考慮（カテゴリ4）	最大PL: e 出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

- 3.1.25 $MTTF_D$: Mean time to dangerous failure/平均危険側故障時間

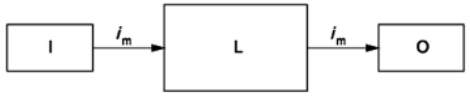
危険側故障を生じるまでの平均時間の期待値

- $MTTF_D$値により、3つのレベルに分類される

表 4－各チャネルの平均危険側故障時間

各チャネルの指定表示	$MTTF_D$ 各チャネルの範囲
“低”	3 年≦$MTTF_D$＜10 年
“中”	10 年≦$MTTF_D$＜30 年
“高”	30 年≦$MTTF_D$＜100 年

- システム（チャンネル）の$MTTF_D$を求める



- $$\frac{1}{MTTF_D}=\frac{1}{MTTF_{D\,I}}+\frac{1}{MTTF_{D\,L}}+\frac{1}{MTTF_{D\,O}}$$

- 各サブシステム、コンポーネントの$MTTF_D$のデータ選定手順

a) 製造業者のデータを使用

b) 附属書C及びDに記載する方法

c) 10年を選択

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

- 附属書C:表C.1～C.7に$MTTF_D$を記載
- $B10_D$で示されているものもある。
- $B10_D$: コンポーネントの10%が危険側に故障する（空圧式及び電気機械式コンポネント）までのサイクル数

- $B10_D$から$MTTF_D$を求める場合
- $MTTF_D = \frac{B10_D}{0.1\ x\ nop}$
  - n_{op}: 年間の平均運転回数

- $n_{op} = \frac{d_{op}\ x\ hop\ x\ 3600s/h}{t_{cycle}}$
  - h_{op}: 平均運転回数（1日当たりの時間数）
  - d_{op}: 平均運転回数（1年あたりの日数）
  - t_{cycle}: （コンポーネントの連続2サイクルでの開始と開始の間の平均運転時間（サイクル当たりの秒数）（例えば、バルブの開閉）

表 C.1－コンポーネントの $MTTF_D$ 又は B_{10D} を扱う国際規格，JIS 及び他の規格

	JIS B 9705-2 における基本安全原則及び“十分吟味された”安全原則	他の関連規格	代表値 $MTTF_D$（年） B_{10D}（サイクル）
機械式コンポーネント	表 A.1 及び表 A.2	－	$MTTF_D$＝150
液圧式コンポーネント n_{op}≧1 000 000 サイクル/年	表 C.1 及び表 C.2	JIS B 8361	$MTTF_D$＝150
液圧式コンポーネント 1 000 000＞n_{op}≧500 000 サイクル/年	表 C.1 及び表 C.2	JIS B 8361	$MTTF_D$＝300
液圧式コンポーネント 500 000＞n_{op}≧250 000 サイクル/年	表 C.1 及び表 C.2	JIS B 8361	$MTTF_D$＝600
液圧式コンポーネント 250 000 サイクル/年＞n_{op}	表 C.1 及び表 C.2	JIS B 8361	$MTTF_D$＝1 200
空圧式コンポーネント	表 B.1 及び表 B.2	JIS B 8370	B_{10D}＝20 000 000
リレー及びコンタクタ接触器リレー 低負荷	表 D.1 及び表 D.2	EN 50205 IEC 61810 規格群 JIS C 8201 規格群	B_{10D}＝20 000 000
リレー及びコンタクタ接触器リレー 定格負荷	表 D.1 及び表 D.2	EN 50205 IEC 61810 規格群 JIS C 8201 規格群	B_{10D}＝400 000
近接スイッチ 低負荷	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10D}＝20 000 000
近接スイッチ 定格負荷	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10D}＝400 000
接触器 低負荷	表 D.1 及び表 D.2	JIS C 8201 規格群	B_{10D}＝20 000 000
接触器 定格負荷	表 D.1 及び表 D.2	JIS C 8201 規格群	B_{10D}＝1 300 000 （注記 1 参照）
ポジション位置スイッチ a)	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10D}＝20 000 000
ポジション位置スイッチ （アクチュエータ分離型，施錠付き） a)	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9710	B_{10D}＝2 000 000
非常停止装置 a)	表 D.1 及び表 D.2	JIS C 8201 規格群 JIS B 9703	B_{10D}＝100 000
押しボタン （例えば，イネーブルスイッチ） a)	表 D.1 及び表 D.2	JIS C 8201 規格群	B_{10D}＝100 000
B_{10D} の定義及び使用に関しては，C.4 参照。			

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

- 3.1.26 DC（診断範囲）*：診断効果の尺度であり、検出される危険側故障率（分子）と全危険側故障率（分母）との比として決定することができる。

- 以下の通り4通りのレベルに分類される

DC	
DC の指定表示	DC の範囲
なし	DC＜60 %
“低”	60 %≦DC＜90 %
“中”	90 %≦DC＜99 %
“高”	99 %≦DC

- システムの平均診断範囲（DCavg)は、

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

出典；JIS B 9705-1: 2019

- *: DC- Diagnostic Coverageの対応訳（JIS B 9705-1)は診断範囲としているが、第4版発行後の対応JIS作成時に修正必要（IEC 62061/JIS B 9961と整合させる）：診断カバー率

ISO 13849-1概要

PLの見積もり(4.5章)

- 附属書E　DC見積もり例（一部）

表 E.1－診断範囲（DC）の見積り

方策	DC
入力装置	
入力信号の動的（ダイナミックな）変化による周期的試験	90 %
プロウザビリティ（確かさ）チェック，例えば，ノーマルオープン及びノーマルクローズの機械的結合接点使用	99 %
動的試験なしの入力装置の相互監視	適用ごとに，信号の切替頻度がどの程度頻繁に行われるかによって 0 %～99 %に変動する。
回路短絡を検出できない場合，動的試験付きの入力信号の相互監視（マルチ I/O に対して）	90 %
入力信号及び論理（処理）（L）内の中間結果の相互監視，プログラムフローの一時的及び論理的ソフトウェア監視，並びに静的障害及び回路短絡の検出（マルチ I/O に対して）	99 %
間接監視（例えば，圧力スイッチによる監視，アクチュエータの電気的位置監視）	適用によって，90 %～99 %に変動する。
直接監視（例えば，制御バルブの電気的位置監視，機械的結合接点要素による電気機械装置の監視）	99 %
処理による障害検出	適用によって，0 %～99 %に変動する。 この方策だけでは，要求パフォーマンスレベル“e”に対しては十分ではない。
センサのある種の特性監視（応答時間，アナログ信号の範囲，例えば電気抵抗，静電容量）	60 %

論理	
間接監視（例えば，圧力スイッチによる監視，アクチュエータの電気的位置監視）	適用によって，90 %～99 %に変動する。
直接監視（例えば，制御バルブの電気的位置監視，機械的結合接点要素による電気機械装置の監視）	99 %
論理の単純な一時的時間経過の監視（例えば，ウォッチドッグとしてのタイマ。論理のプログラム内にトリガ点をもつ）	60 %
ウォッチドッグによる一時的かつ論理的監視。試験装置は論理の挙動に対するプロウザビリティ（確かさ）チェック	90 %
論理（プログラム及びデータ記憶，入力／出力ポート，インタフェースなど）の部分に潜在する障害を検出するための起動時の自動試験（セルフテスト）	90 %（試験技術による。）
主チャネルによる監視装置の応答能力のチェック（例えば，ウォッチドッグ）。起動時，若しくは安全機能の動作要求時，又は外部信号が入力装置を介してそれを要求するとき。	90 %

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

- 3.1.6 共通原因故障（CCF): 単一の事象から生じる異なったアイテムの故障であって、これらの故障がお互いの結果でないもの
- 附属書F　表F.1　採点方法及びCCFに対する方策の定量化　安全関連部全体、満点又はゼロ（部分的満足はない）

No	CCF に対する方策	得点
1	分離又は隔離	
	信号経路間の物理的な分離，例えば， － 配線及び配管での分離 － 動的試験によるケーブルの短絡及び断線の検出 － 各チャネルの信号経路の個別シールド － プリント基板上での回路間の十分なクリアランス及び沿面距離	15
2	多様性（ダイバーシティ）	
	異なる技術的方式，設計又は物理的原理の使用，例えば， － 第 1 チャネルは電子又はプログラマブル電子方式で，第 2 チャネルは電気機械式のハードワイヤ方式 － 安全機能の各チャネルは異なる信号によって始動（例えば，位置，圧力，温度） 及び／又は デジタル及びアナログによる測定（例えば，距離，圧力又は温度） 及び／又は 異なる製造業者によるコンポーネント	20
3	設計，適用又は経験	
3.1	過電圧，過圧力，過電流，過熱などに対する保護	15
3.2	使用のコンポーネントは，“十分吟味されている”	5
4	査定・分析	
	制御システムの安全関連部の各部に対して，FMEA が実施されており，その結果は，設計段階において CCF を回避するために考慮されている。	5

No	CCF に対する方策	得点
5	適格性（能力），訓練	
	CCF の原因及び結果を理解できるような設計者の訓練	5
6	環境面	
6.1	電気／電子システムに対して，適切な規格（例えば，**IEC 61326-3-1**）に従った CCF に対する汚染防止及び電磁妨害の防止（EMC）。 流体システム：圧力媒体のろ過，ほこりの侵入の防止，圧縮空気の水抜き，例えば，圧力媒体の純度に関してはコンポーネント製造業者の要求事項に従う。 **注記** 流体システムと電気システムとの組合せに対しては，これらの両面を考慮することが望ましい。	25
6.2	他の影響 温度，衝撃，振動，湿度のような全ての環境関連（例えば，関連の規格で規定される）の影響に対して耐性の要求事項を考慮する。	10
	合計	最大 100

合計得点	CCF を回避するための方策 a)
65 以上	要求事項に適合
65 未満	要求事項に不適合 ⇒ 追加方策の選択

注 a) 技術方式上の方策が関連しない場合でも，この欄で算定された得点は，包括的な計算のときに考慮することができる。

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

- 3.1.7 システマティック故障: 何らかの原因に確定的に関係する故障であって、設計、製造プロセス、運転手順、文書又は他の関連要因を変更しなければ除去できない故障
- 基本安全原則及び十分に吟味された安全原則　（ISO 13849-2、附属書B参照)の適用

表 B.1－基本安全原則

基本安全原則	留意事項
適した材料及び適切な製造方法の採用	例えば，次に関する材料，製造方法，処理方法の選択。 －　応力，耐性，弾性，摩擦，摩耗，腐食，温度
正しい数値設計及び形状	例えば，次の要素を考慮する。 －　応力，ひずみ，疲労，表面粗さ，公差，及び製造方法
空圧コンポーネント及びシステムの適切な選択，組合せ，配置，組立及び据付	製造業者の適用上の留意事項，例えば，カタログ，据付指示書，仕様書，及び類似の空圧コンポーネント及びシステムにおけるグッドエンジニアリングプラクティスなどを適用する。
エネルギー解放の原則の使用	安全な状態は，全ての関連する装置からエネルギーを解放することによって得られる。停止の最初の動作は，**JIS B 9700** の **6.2.11.3** 参照。 エネルギーは，機構の動作を起動するときに供給される。 起動の最初の動作は，**JIS B 9700** の **6.2.11.3** 参照。 様々なモードについて考察する。例えば，運転モード，保全モード。 この原則は，例えば，圧力の損失が更なる危険を生じさせるような用途においては使用してはならない。
適切な留め具	ねじ留め，取付部品，接着，締付けリングの場合，製造業者の適用上の留意事項を考慮する。 過負荷は，適切なトルク管理技術を適用することで回避することができる。
圧力の制限	例えば，圧力リリーフ弁，減圧弁，制御弁である。
速度制限又は低減	例えば，流量制御弁又は絞りによるシリンダピストンの速度制限がある。
流体汚染の十分な回避	流体中の固体粒子及び水分のろ過並びに分離を考慮する。
適切な切替時間の範囲	配管長，圧力，排気容量，力，ばねの疲労，摩擦，潤滑，温度，加速・減速時の慣性，許容差の累積などを考慮する。

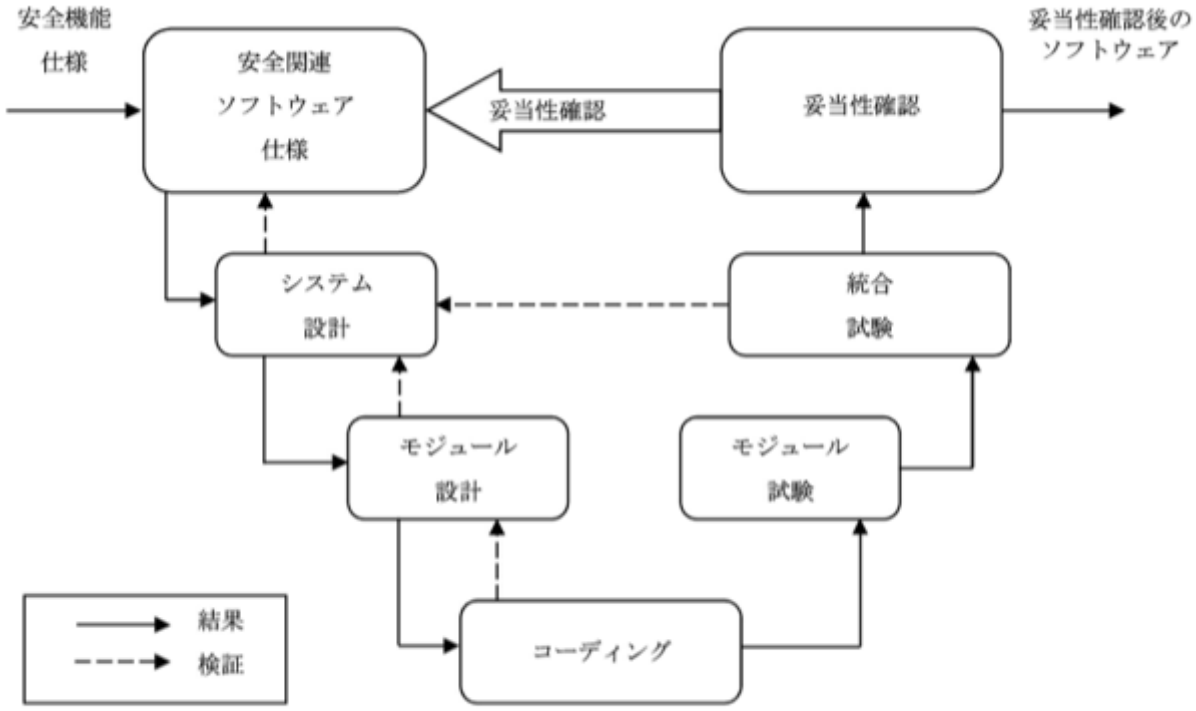
基本安全原則	留意事項
耐環境条件	全ての想定される環境において，温度，湿度，振動，汚染などの予見可能な不利な条件において作動させられるように装置を設計する。箇条 **10** 参照，及び製造業者の仕様及び適用上の留意事項を考慮する。
予期しない起動に対する保護	蓄積されたエネルギーによって生じる予期しない起動，運転モード，保全モードなどの様々なモードの動力源復帰後の予期しない起動を考慮する。 蓄積されたエネルギーの放出に特殊な装置を使用する必要があり得る（**JIS B 9714** の **5.3.1.3** 参照）。 特殊な用途，例えば，装置の保持，位置の確保にエネルギーを維持するなどは個別に考慮する必要がある。
簡素化	安全関連システムにおける不要なコンポーネントを避ける。
適切な温度範囲	システム全体について考慮する。
分離化	安全関連機能を他の機能と分離する（例えば，論理的分離）。

出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの見積もり(4.5章)

- ソフトウエア（使用していれば）
- 安全関連の組込みソフトウエア又はアプリケーションソフトウエア共に、全ライフサイクル間に生じる障害の可否を考慮しなければならない。



注記　附属書 J に，ライフサイクル活動に対して，より詳細な推奨事項を示す。

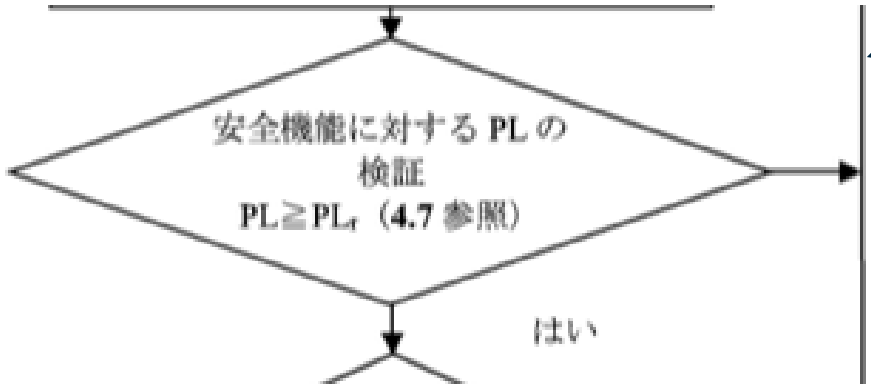
図 6－ソフトウェア安全ライフサイクルの単純化 V モデル

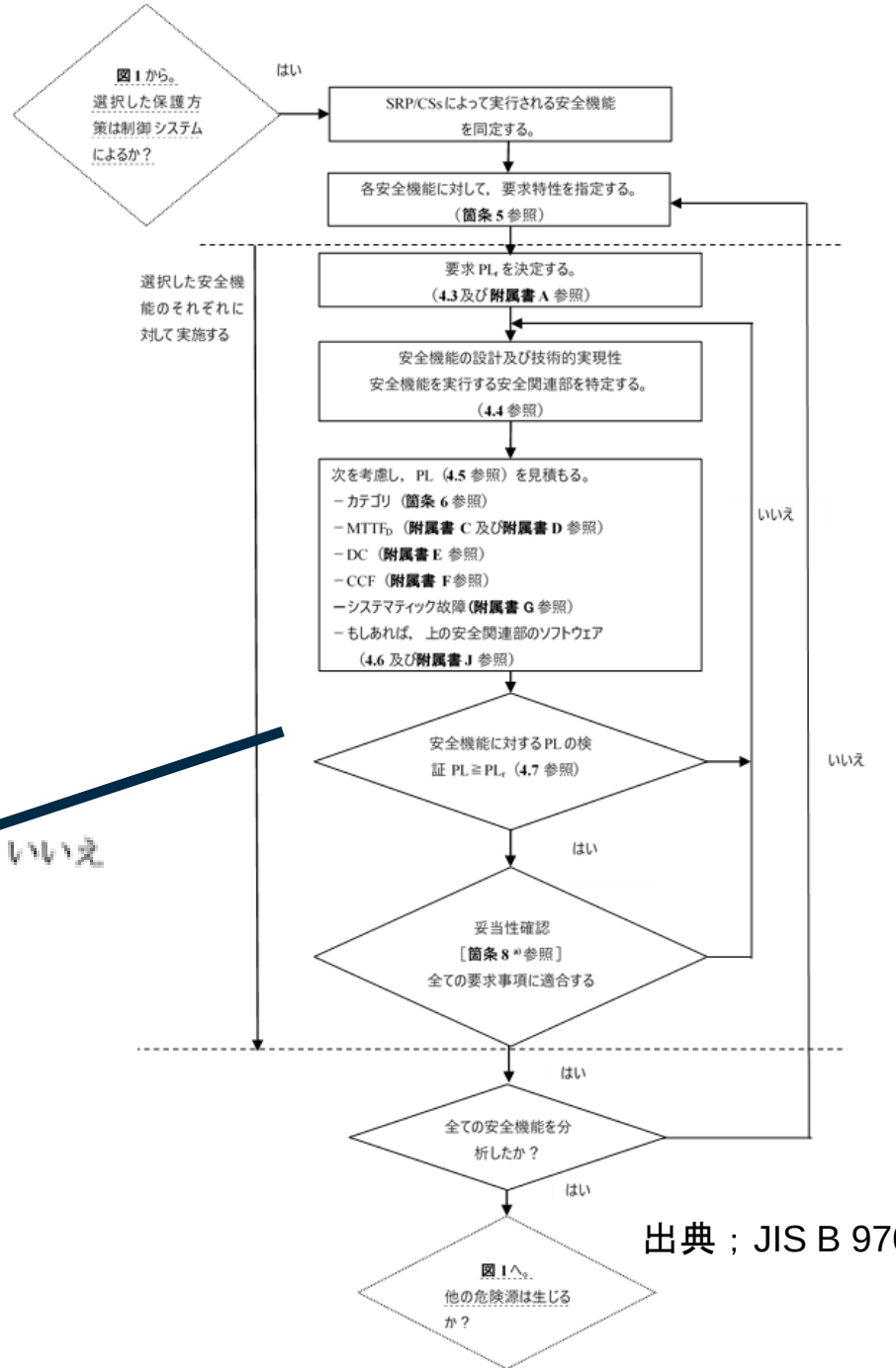
出典；JIS B 9705-1: 2019

ISO 13849-1概要

PLの検証（PL≥PLr） (4.7章）

- 安全関連部（安全機能ごと）のPLが要求PL（PLr）を満たしているか確認する。
- （PL≥PLr)





出典；JIS B 9705-1: 2019

ISO 13849-1概要

妥当性確認　(8章、ISO 13849-2)

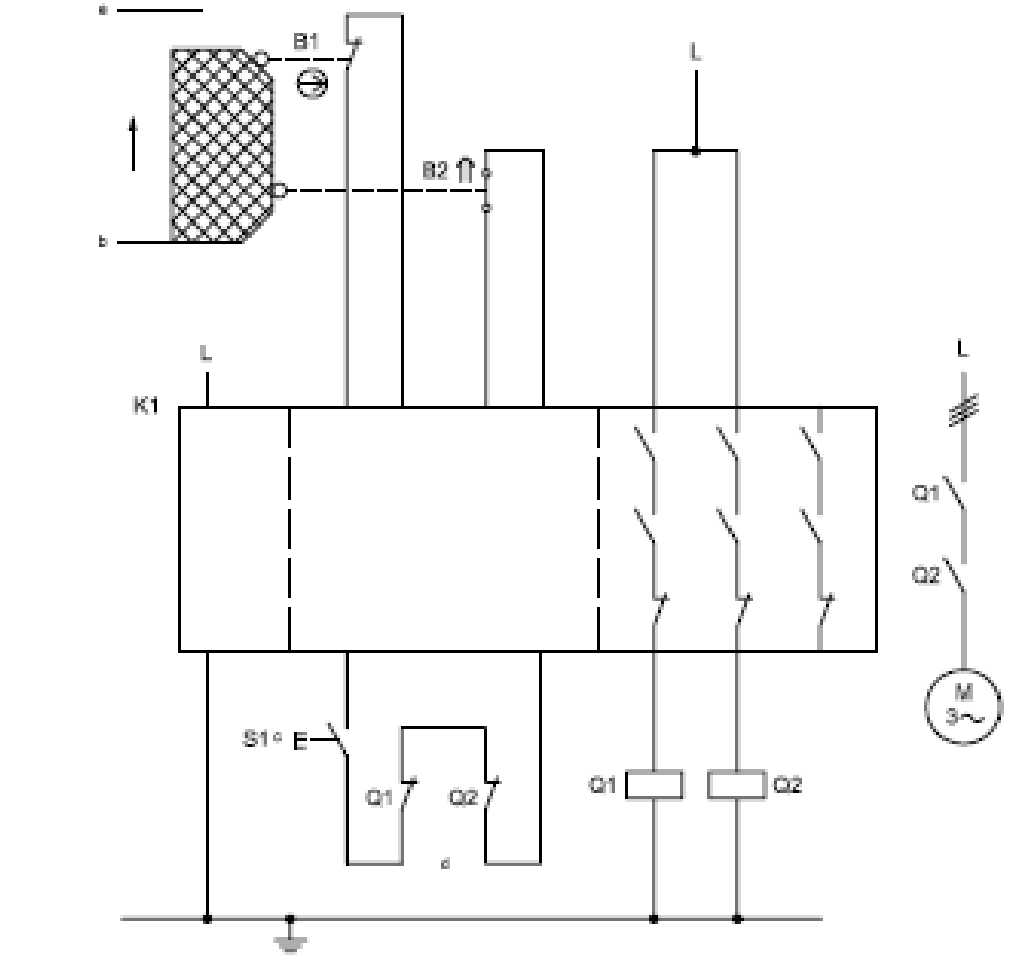
- 安全機能を実行する安全関連部がISO 13849-1の該当する要求事項を満足しているかどうかを立証する
- 詳細はISO 13849-2による。
- 安全関連部全体、カテゴリ及びソフトウエア
- 立証方法
    - 回路図を使用した故障分析
    - フォールト挿入試験（実際の回路への障害注入）
    - 障害時の制御システムの挙動シミュレーション

ISO 13849-1適用例

例　機械のインターロックガードの停止機能

I 入力（リミットスイッチ、B1, B2）
L 論理処理(安全モジュール、K1）
O 出力（コンタクタ、Q1, Q2）

安全機能：インターロックガード開でモータ停止
要求パフォーマンスレベル (PLr)：e
ハードウエア構成：カテゴリ4



shown in actuated position
a Open.
b Closed.
c START.
d Feedback circuit.

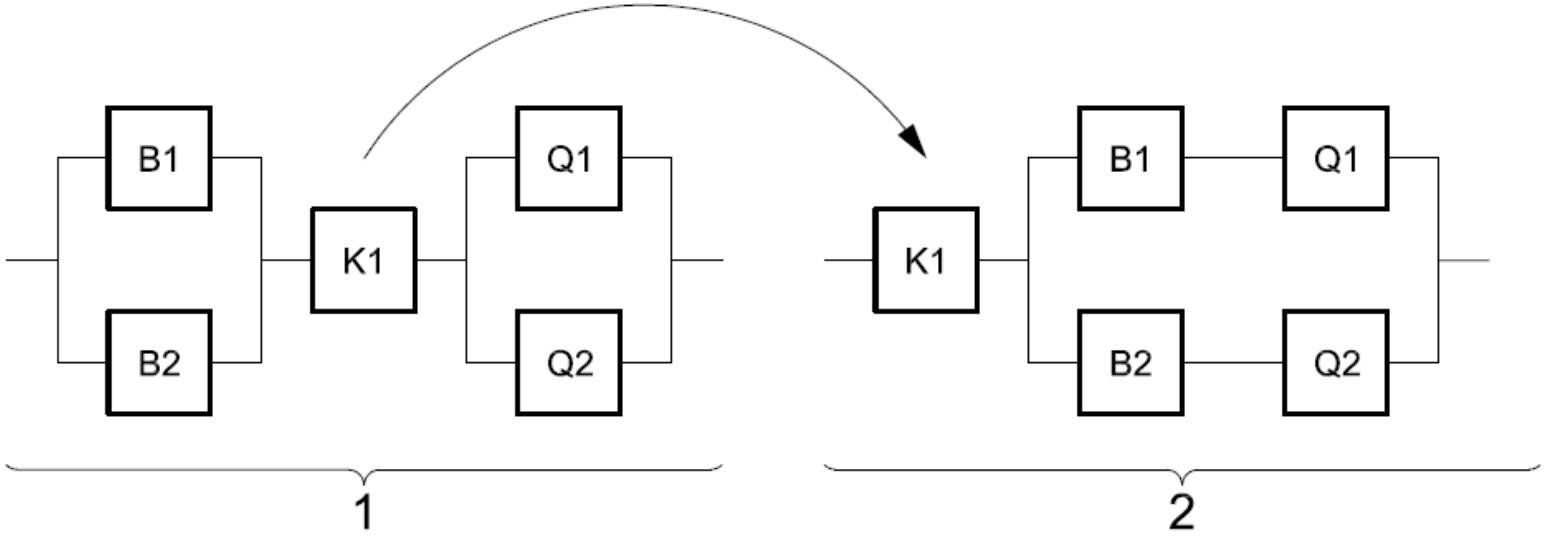
Figure 1 — Example implementation of the safety function

ISO/TR 23849　8章　図1

ISO 13849-1概要

安全機能の仕様

安全関連ブロック図に展開



安全関連部仕様(一部）

詳細設定はISO/TR 23849参照

サブシステム	仕様	備考
安全モジュール、K1	PFH_D=2.31x10-9 (1/h) カテゴリ4、PL=e	メーカー提供
リミットスイッチ、B1	B10d=1,000,000回 IEC 60947-5-1, Annex K	メーカー提供
リミットスイッチ、B2	B10d=500,000回	メーカー提供
コンタクタ、Q1, Q2	B10=1,000,000回 IEC 60947-5-1, Annex L	メーカー提供 安全側・危険側故障は同率とし B10d=2,000,000回とする

ISO 13849-1概要

機械仕様

機械仕様	仕様	備考1
年間稼働日	365日	ISO/TR 23849による
1日の稼働時間	24時間	ISO/TR 23849による
サイクルタイム	900s　(15min)	ISO/TR 23849による
年間作動回数	Nop=35,040/年	式(C.2) $n_{op} = \frac{d_{op} \times h_{op} \times 3600\ \mathrm{s/h}}{t_{cycle}}$

詳細仕様はISO/TR 23849参照

$$\frac{365\frac{\mathrm{d}}{\mathrm{y}} \cdot 24\frac{\mathrm{h}}{\mathrm{d}} \cdot 3600\frac{\mathrm{s}}{\mathrm{h}}}{900\frac{\mathrm{s}}{\mathrm{cycle}}} = 35040\frac{\mathrm{cycles}}{\mathrm{y}}$$

ISO 13849-1概要

安全関連部評価

安全関連部評価		備考1
$MTTF_D$, B1	285年	式(C.7) $MTTF_D = \frac{T_{10D}}{0,1} = \frac{B_{10D}}{0,1 \times n_{op}}$
$MTTF_D$, B2	143年	
$MTTF_D$, Q1/Q2	571年	
$1/MTTF_D$, ch1	1/190年	式（D.1） $\frac{1}{MTTF_{d,Ch1}} = \frac{1}{285\,y} + \frac{1}{571y} = \frac{1}{190\,y}$
$1/MTTF_D$, ch2	1/114年	$\frac{1}{MTTF_{d,Ch2}} = \frac{1}{143\,y} + \frac{1}{571y} = \frac{1}{114\,y}$
$MTTF_D$	154年	式（D.2)、各チャンネルの$MTTF_D$が異なるため $MTTF_D = \frac{2}{3}\left[MTTF_{D\,C1} + MTTF_{D\,C2} - \frac{1}{\frac{1}{MTTF_{DC1}} + \frac{1}{MTTF_{DC2}}}\right]$
DC, B1/B2	99%	表E.1: K1によるプラウザビリティ(確かさ）監視
DC, Q1/Q2	99%	表E.1: K1による始動時の監視
DCavg	99%=“高”	式(E.1) $DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$
CCF	70	表F.1：分離／隔離(15)、十分吟味されたコンポーネントの使用(5)、過電圧等に対する保護（15）、環境面（25+10）
Mission time (使命時間)	20年	4.5.4項

ISO 13849-1概要

(B1/B2/Q1/Q2)のPFH_D：表K.1、カテゴリ4、DCavg =”高” ：PFH_D ＝ $1.61x10^{-8}$、PL = e

安全モジュール、K1のPFH_Dを加えた安全関連部全体のPFH_D：$2.31x10^{-9}+1.61x10^{-8}=1.84x10^{-8}$ => PL=e に相当

	危険側故障の平均確率（1/h）及び対応のパフォーマンスレベルPL													
各チャネルの$MTTF_D$ 年	カテゴリB DC_{avg}=“なし”	PL	カテゴリ1 DC_{avg}=“なし”	PL	カテゴリ2 DC_{avg}=”低”	PL	カテゴリ2 DC_{avg}=”中”	PL	カテゴリ3 DC_{avg}=”低”	PL	カテゴリ3 DC_{avg}=”中”	PL	カテゴリ4 DC_{avg}=”高”	PL
36			3.17×10^{-6}	b	1.67×10^{-6}	c	9.39×10^{-7}	d	5.16×10^{-7}	d	2.01×10^{-7}	d	7.77×10^{-8}	e
39			2.93×10^{-6}	c	1.53×10^{-6}	c	8.40×10^{-7}	d	4.53×10^{-7}	d	1.78×10^{-7}	d	7.11×10^{-8}	e
43			2.65×10^{-6}	c	1.37×10^{-6}	c	7.34×10^{-7}	d	3.87×10^{-7}	d	1.54×10^{-7}	d	6.37×10^{-8}	e
47			2.43×10^{-6}	c	1.24×10^{-6}	c	6.49×10^{-7}	d	3.35×10^{-7}	d	1.34×10^{-7}	d	5.76×10^{-8}	e
51			2.24×10^{-6}	c	1.13×10^{-6}	c	5.80×10^{-7}	d	2.93×10^{-7}	d	1.19×10^{-7}	d	5.26×10^{-8}	e
56			2.04×10^{-6}	c	1.02×10^{-6}	c	5.10×10^{-7}	d	2.52×10^{-7}	d	1.03×10^{-7}	d	4.73×10^{-8}	e
62			1.84×10^{-6}	c	9.06×10^{-7}	d	4.43×10^{-7}	d	2.13×10^{-7}	d	8.84×10^{-8}	e	4.22×10^{-8}	e
68			1.68×10^{-6}	c	8.17×10^{-7}	d	3.90×10^{-7}	d	1.84×10^{-7}	d	7.68×10^{-8}	e	3.80×10^{-8}	e
75			1.52×10^{-6}	c	7.31×10^{-7}	d	3.40×10^{-7}	d	1.57×10^{-7}	d	6.62×10^{-8}	e	3.41×10^{-8}	e
82			1.39×10^{-6}	c	6.61×10^{-7}	d	3.01×10^{-7}	d	1.35×10^{-7}	d	5.79×10^{-8}	e	3.08×10^{-8}	e
91			1.25×10^{-6}	c	5.88×10^{-7}	d	2.61×10^{-7}	d	1.14×10^{-7}	d	4.94×10^{-8}	e	2.74×10^{-8}	e
100			1.14×10^{-6}	c	5.28×10^{-7}	d	2.29×10^{-7}	d	1.01×10^{-7}	d	4.29×10^{-8}	e	2.47×10^{-8}	e
110													2.23×10^{-8}	e
120													$2{,}03\times10^{-8}$	e
130													$1{,}87\times10^{-8}$	e
150													$1{,}61\times10^{-8}$	e

注：ISO/TR 23849:2010発行時は表K.1のカテゴリ4の$MTTF_D$は100年に制限されていたので、このPFH_DはTRと異なる。

第3版対応JIS改正動向

JIS B 9705-1

- 発行　2019年5月
  - JIS作成時の表記上ルール：ISO 13849-1:2015で追加された部分以外の、JIS B 9705-1: 2011 (ISO 13849-1: 2006)の部分は変更しない
  - 第4版発行後、対応のJIS作成予定

- 関連規格のJIS化
  - JIS B 9705-2
  - 発行　2019年5月
  - JIS作成時の表記上ルール：JIS B 9705-1: 2011と整合化

改正履歴

- 1999年11月　　第1版発行
- 2006年11月　　第2版発行
- 2009年9月　　正誤表（Corrigenda)発行
- 2011年4月　　追補発行を決定
- 2011年11月 第9回WGより、ISO 13849-1追補に対するコメント審議開始
- 2012年1月 追補１を発行するNWIP+CDが発行、10月に承認
  - 2013年1月 第12回WGでCDに対するコメント審議終了、DIS発行手続き
  - 2014年3月 第16回WGでDISに対するコメント審議終了、FDIS発行手続き
  - 2014年9月 追補のFDIS（ISO 13849-1 FDAM1）発行
  - 2015年10月 ISO/TC199年次大会でISO/IEC17305の開発中止が決定及びISO13849-1の更なる改定又は追補の発行を決定
- 2015年12月 第3版発行（第2版に追補1を統合）
- 2016年1月より改定に向けて作業開始（WDの作成）
- 2018年6月 CD発行
- 2018年10月 CDに対するコメント審議開始

改正履歴

- 2019年2月 2nd CD発行
- 2019年4月 2nd CDに対するコメント審議開始（2019年9月まで）
- 2020年6月 DIS発行、投票
- 2020年9月 DISに対する投票結果：否決,
  - コメント審議＝＞2nd DISを発行、開発期間の延長（9か月）することを決定
- 2021年7月 2nd DIS発行、投票
- 2021年10月 2nd DISに対する投票結果＝＞承認
  - コメント審議
    - No. 42　ミーティング：10月27－28日
    - No. 43　ミーティング：11月23－25日
    - No. 44　ミーティング：12月14－16日
- 2021年12月 FDIS案をISO CO（事務局）に送付予定
- 2022年7月 IS発行期限

第4版改正動向

2nd DIS 改正点概要

The main changes compared to the previous edition are improvements and as follows:

— specification of the safety functions (clause 5);

— software (clause 7);

— validation (clause 10);

— combination of several subsystems ;

— management of the functional safety (Annex G.5) ;

— EMC immunity (annex L);

— additional information for safety requirements specification (annex M);

— avoiding of fault avoiding measures for the design of safety related software (annex N);

— safety-related values of components or parts of the control systems (Annex O).

- 2nd DISより抜粋
- “- Avoiding of fault avoiding …”は修正予定

第3版からの主な変更点

- 安全要求仕様（箇条5）
- ソフトウエア（箇条7）
- 妥当性確認（箇条10）
- サブシステムの組み合わせ（箇条6.2、附属書H）
- 安全機能のマネジメント（附属書G.5)
- EMC イミュニティ（附属書L)
- 安全要求仕様書の追加情報（附属書M)
- 安全関連ソフトウエア設計のための障害回避手段（附属書N)
- コンポーネント又制御システムの部分の安全関連値（附属書O)

- 箇条3　定義の追加・修正あり
- 箇条4　追加、修正、箇条6への移動、図1 - 3の修正あり

第4版改正動向

2nd DIS 改正点概要

第3版構成

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

3.1.1 safety–related part of a control system

.

.

.

.

.

3.1.39 Proven in use

3.2 Symbols and abbreviated terms

Table 1 — Symbols and abbreviated terms

2nd DIS

3 Terms, definitions, symbols and abbreviated terms

3.1 Terms and definitions

3.1.1 safety–related part of a control system

.

.

.

.

.

.

3.1.58 grey box

3.2 Symbols and abbreviated terms

Table 1 — Symbols and abbreviated terms

第4版改正動向

2nd DIS 改正点概要

新規追加の定義（抜粋）

3.1.2

machine control system

system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner

Note 1 to entry: The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic and mechanical).

3.1.3

safety requirements specification

SRS

specification containing the requirements for the safety functions that have to be met by the safety-related control system in terms of characteristics of the safety functions (functional requirements) and required performance levels

[SOURCE: IEC 61508-4:2010, 3.5.11, modified, information from 3.5.12 included]

第4版改正動向

2nd DIS 改正点概要

新規追加の定義（抜粋）

3.1.49

well-tried safety principle

principles that have proved effective in the design or integration of safety-related control systems in the past, to avoid or control critical faults or failures which can influence the performance of a safety function

Note 1 to entry: Newly developed safety principles can only be considered as equivalent to well-tried if they are verified using methods which demonstrate their suitability and reliability for safety-related applications.

Note 2 to entry: Well-tried safety principles are effective not only against random hardware failures, but also against systematic failures which can creep into the product at some point in the course of the product life cycle, e.g. faults arising during product design, integration, modification or deterioration.

Note 3 to entry: Table A.2, Table B.2, Table C.2 and Table D.2 of ISO 13849-2:2012 address well-tried safety principles for different technologies.

3.1.50

well-tried component

component-successfully used in safety-related applications

Note 1 to entry: See 6.1.11 for requirements and ISO 13849-2 for a list of recognized well-tried components.

第4版改正動向

2nd DIS 改正点概要

第3版構成

4	Design considerations
4.1	Safety objectives in design
4.2	Strategy for risk reduction
4.2.2	Contribution to the risk reduction by the control system
4.3	Determination of required performance level (PLr)
4.4	Design of SRP/CS

2nd DIS

4	Overview
6	Design considerations
4.1	Risk assessment and risk reduction process at the machine
4.2	Contribution to the risk reduction
4.5	Required information
5.3	Determination of required performance level for each safety function
4.3	Design process of an SRP/CS
4.4	Methodology

第4版改正動向

2nd DIS 改正点概要

第3版構成

4.5	Evaluation of the achieved performance level PL and relationship with SIL
4.5.1	Performance level PL
4.5.2	Mean time to dangerous failure of each channel (MTTFD)
4.5.3	Diagnostic coverage (DC)
4.5.4	Simplified procedure for estimating the quantifiable aspects of PL
4.5.4	Description of the output part of the SRP/CS by category

2nd DIS

6.1	Evaluation of the achieved performance level
6.1.1	General overview of performance level
6.1.2	Correlation between performance level and safety integrity level
6.1.3	Architecture — Categories and their relation to $MTTF_D$ of each channel, average diagnostic coverage and common cause failure
6.1.4	Mean time to dangerous failure
6.1.5	Diagnostic coverage
6.1.6	Common cause failures
6.1.7	Systematic failures
6.1.8	Simplified procedure for estimating the performance level for subsystems
6.1.9	Alternative procedure to determine the performance level and PFHD without $MTTF_D$
6.1.9.1	General
6.1.9.2	Preconditions
6.1.9.3	Inputs and outputs
6.1.9.4	Logic

第4版改正動向

2nd DIS 改正点概要

第3版構成

4.6	Software safety requirements

2nd DIS

7	Software safety requirements
7.1	General
7.2	Limited variability language and full variability language
7.3	Safety-related embedded software
7.4	Safety-related application software
7.5	Software-based manual parameterization

- CD2発行後、箇条7の要求は第3版の内容に戻された。その後内容の見直し・修正

第4版改正動向

2nd DIS 改正点概要

第3版構成

4.7	Verification that achieved PL meets PLr
4.8	Ergonomic aspects of design

2nd DIS

8	Verification that achieved performance level meets required performance level
9	Ergonomic aspects of design

第4版改正動向

2nd DIS 改正点概要

- 図1 Overview of risk assessment/risk reduction

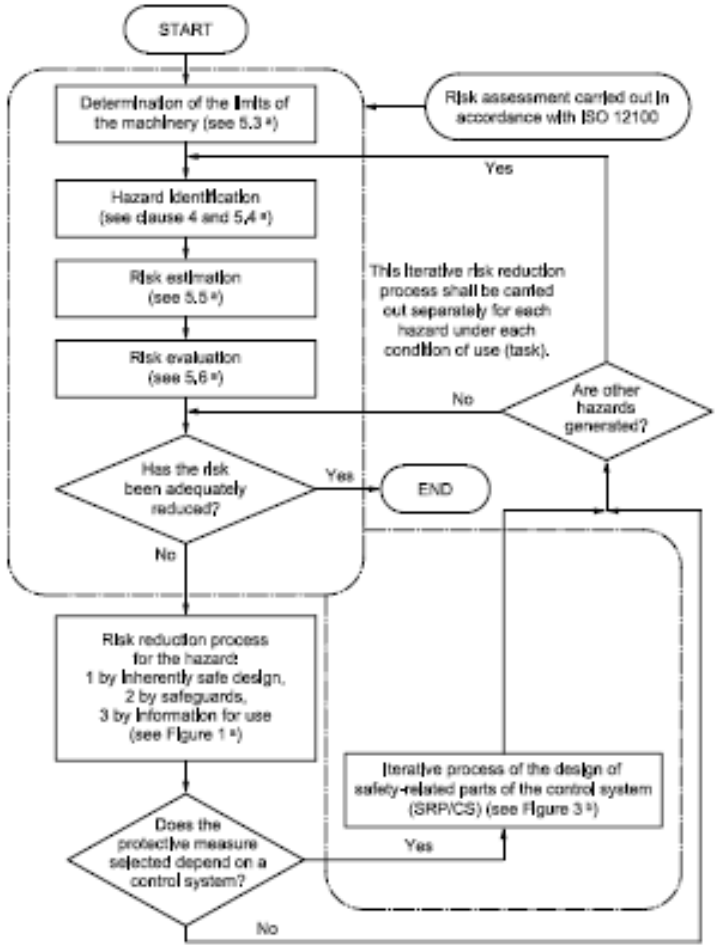
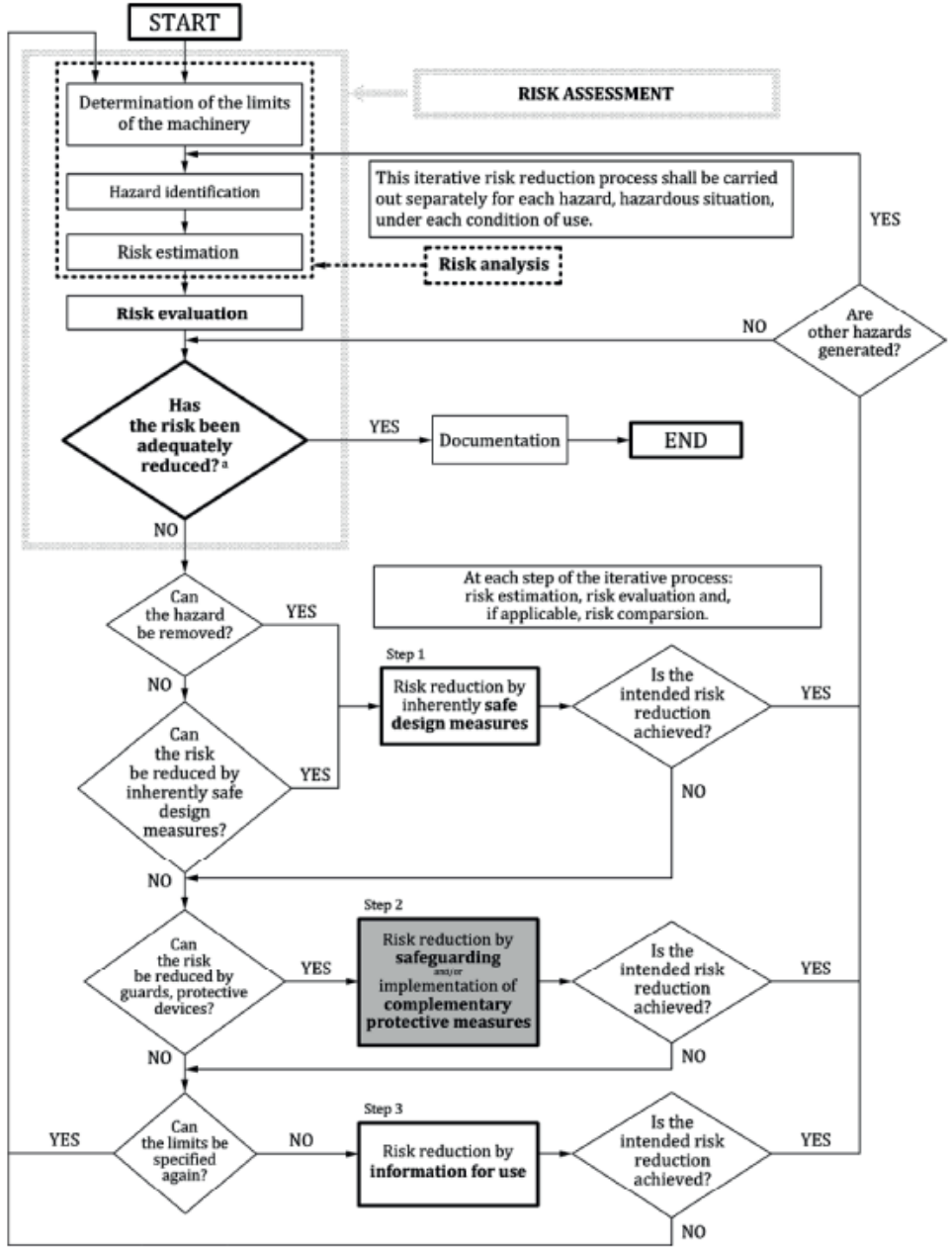


Figure 1 — Overview of risk assessment/risk reduction



- 図2 Schematic representation of risk reduction process including iterative three-step method according to ISO 12100:2010

第4版改正動向

2nd DIS 改正点概要

- 図1 Integration of ISO 13849-1 within the risk reduction process of ISO 12100

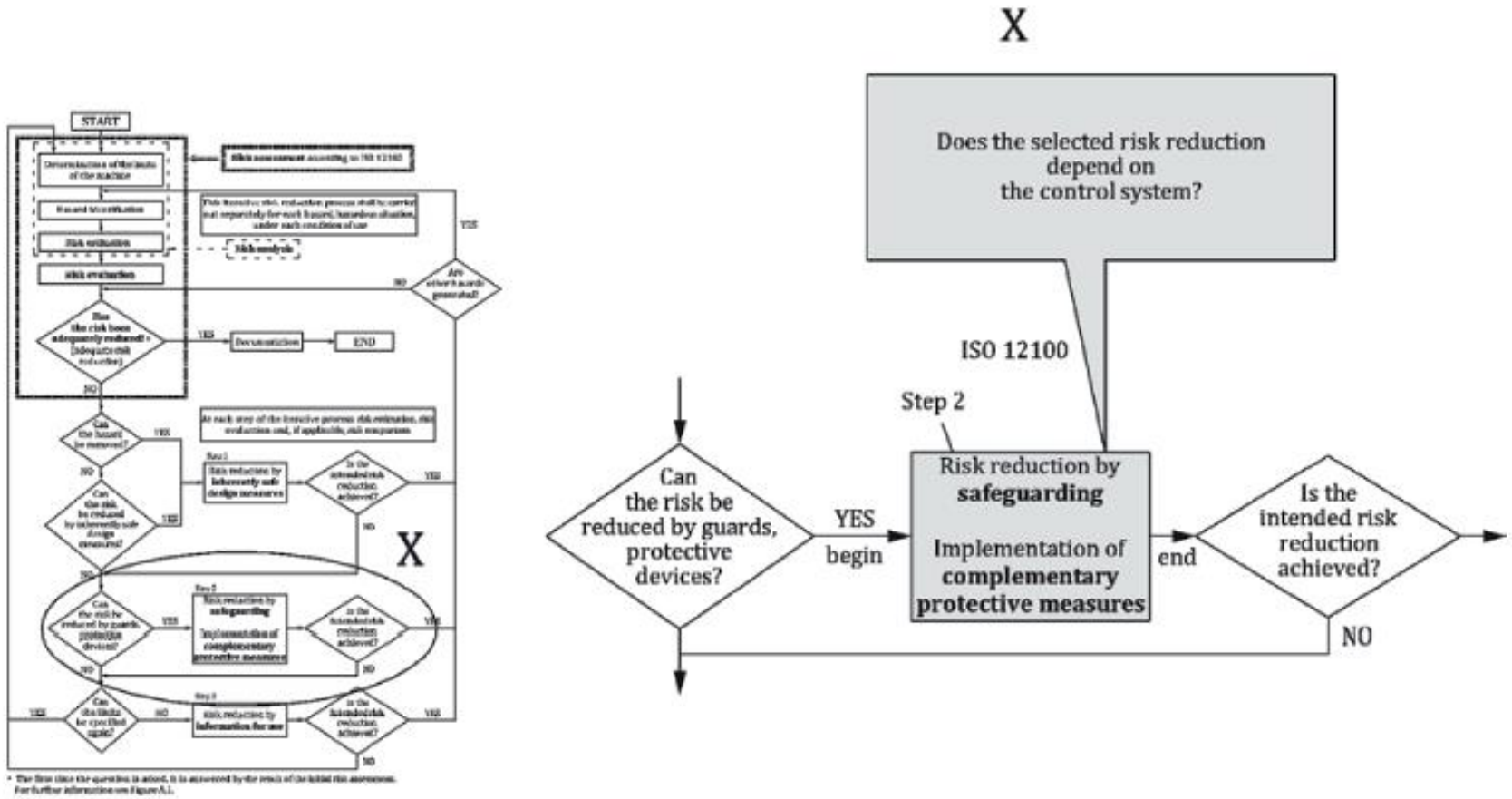
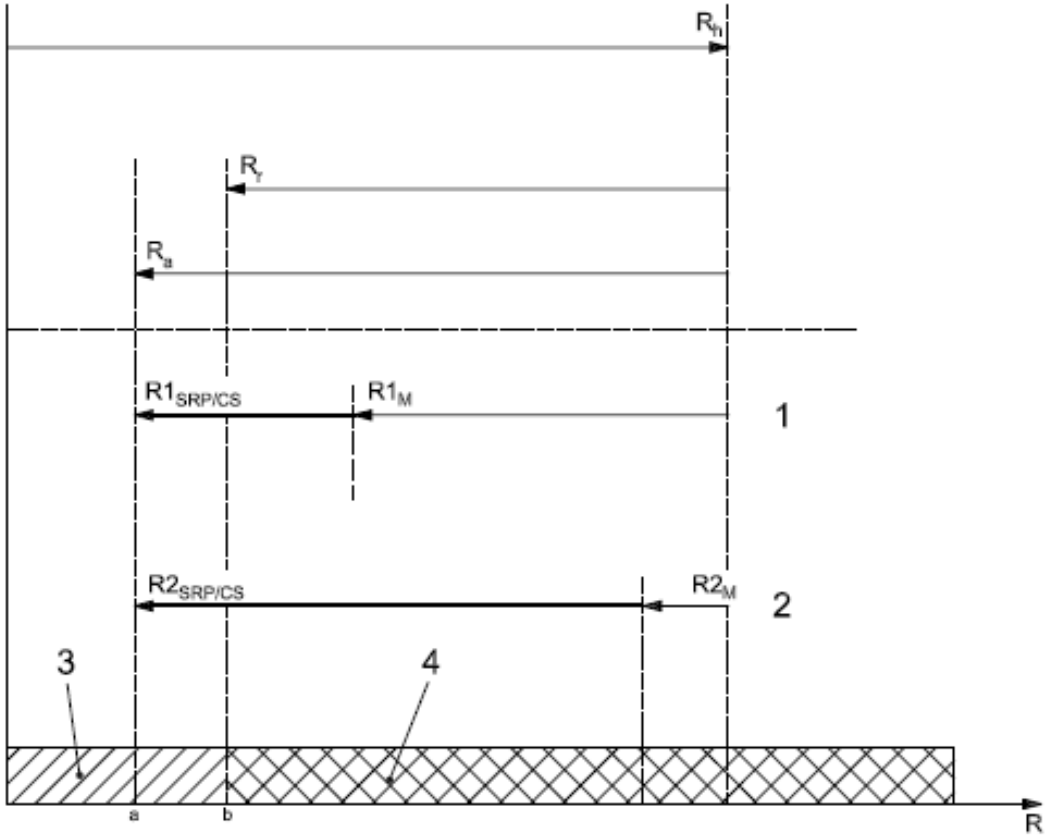


Figure 1 — Integration of ISO 13849-1 within the risk reduction process of ISO 12100

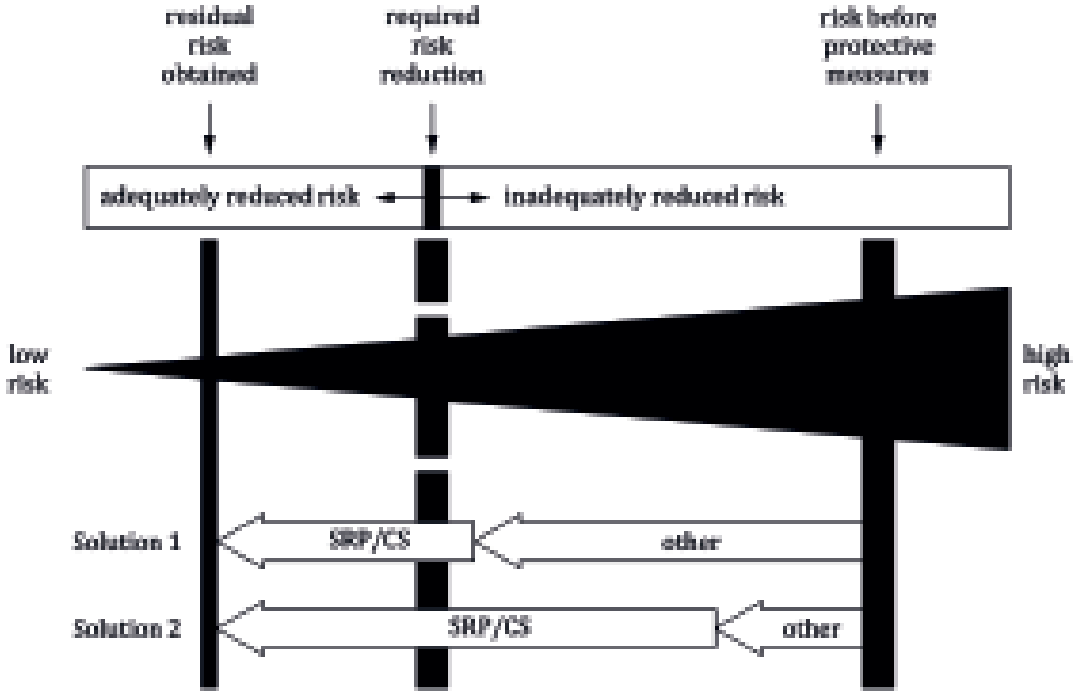
第4版改正動向

2nd DIS 改正点概要

- 図2　Overview of the risk reduction process for each hazardous situation



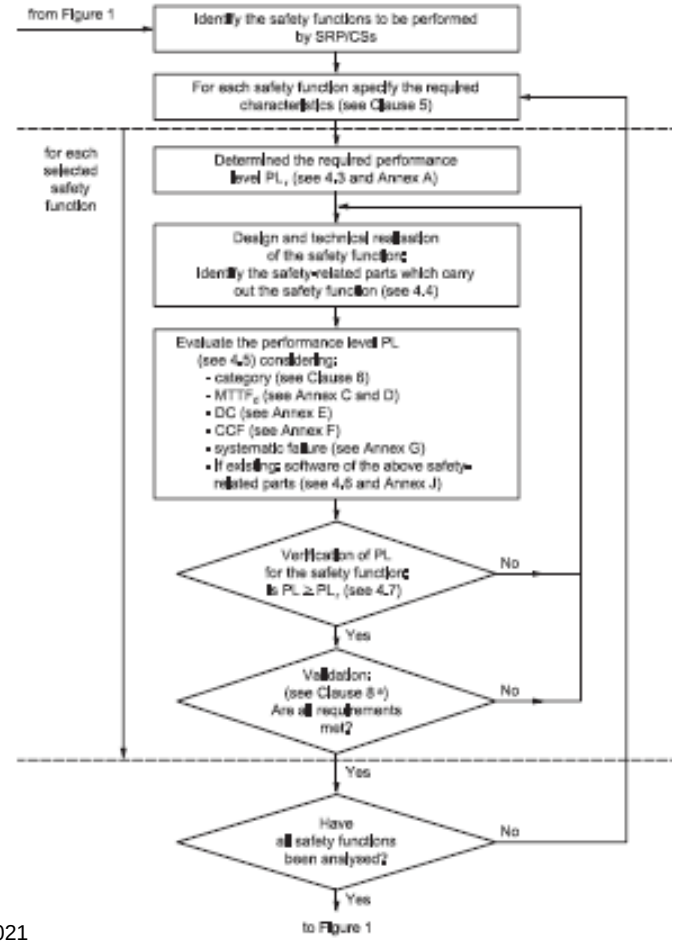
- 図3 Overview of the risk reduction process for each hazardous situation



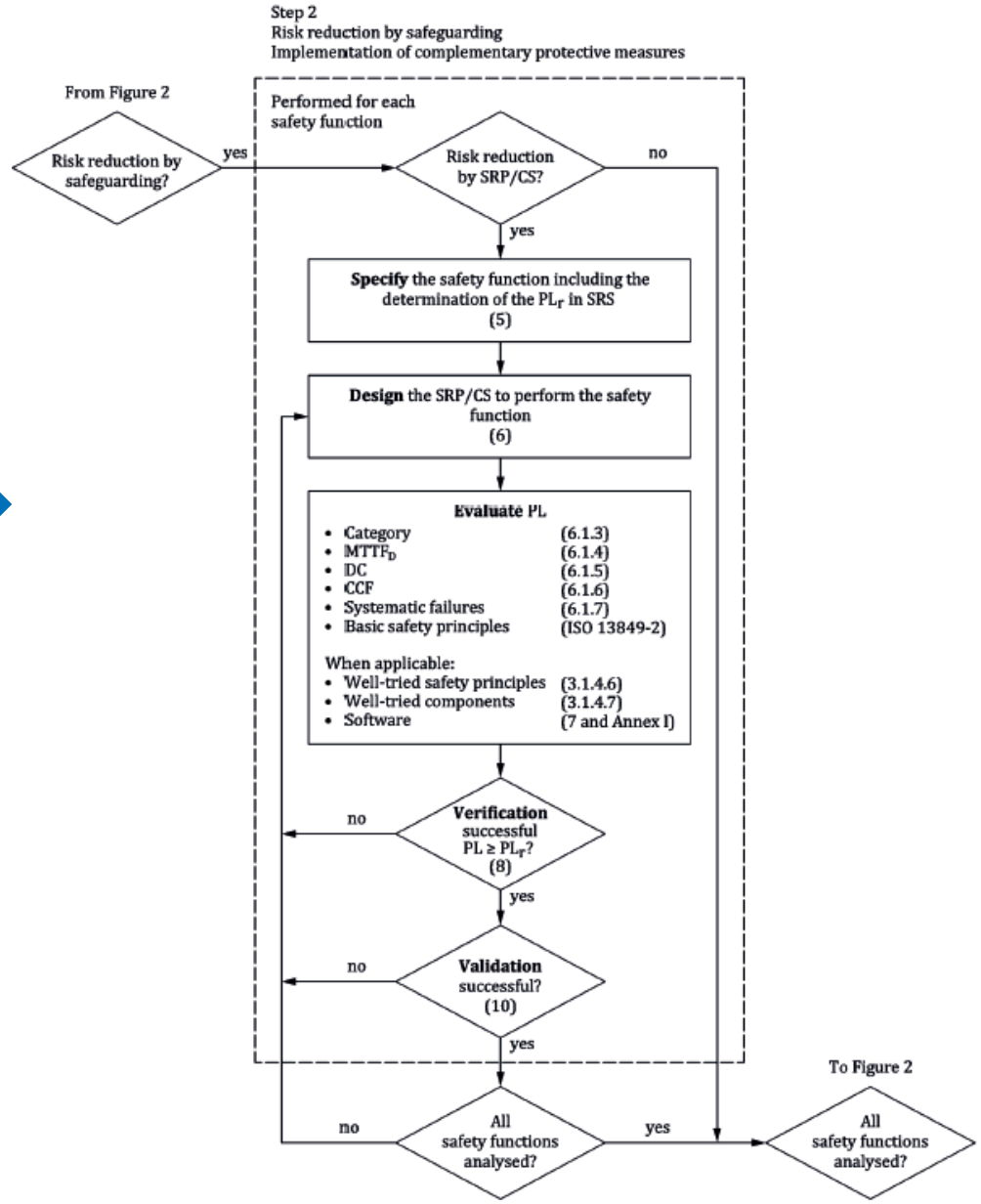
第4版改正動向

2nd DIS 改正点概要

- 図3　Iterative process for design of safety-related parts of control systems



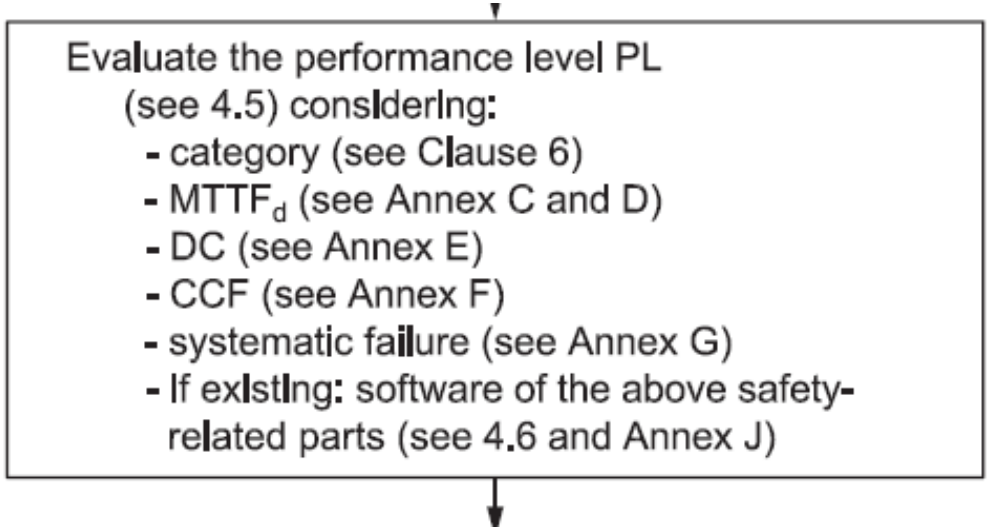
- 図4 Iterative process for design of safety-related parts of control systems



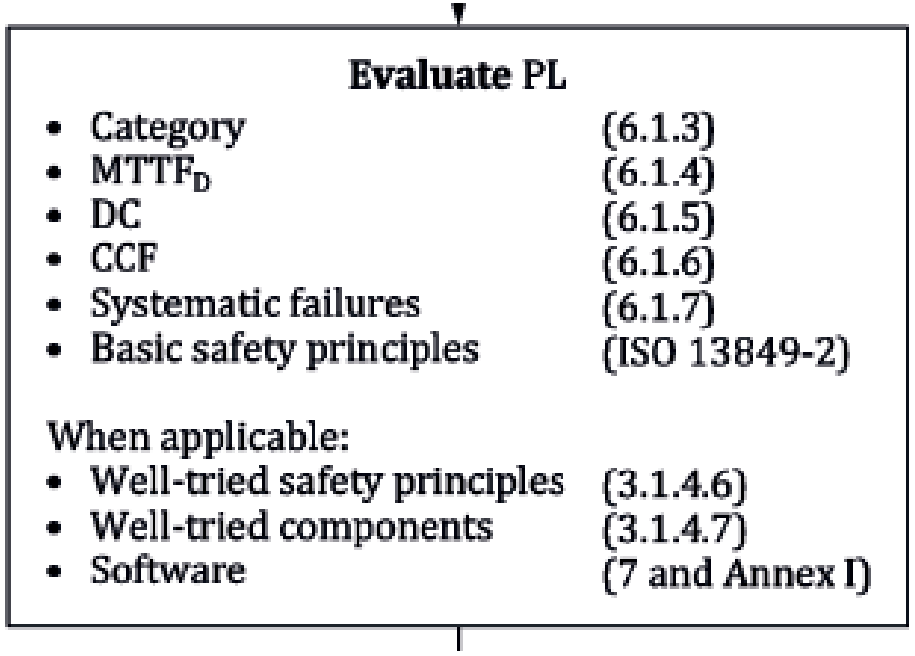
第4版改正動向

2nd DIS 改正点概要

- 図3　Iterative process for design of safety-related parts of control systems



- 図4 Iterative process for design of safety-related parts of control systems



第4版改正動向

2nd DIS 改正点概要

第3版構成

5	Safety functions
5.1	Specification of safety functions

2nd DIS

5	Specification of safety functions
5.1	Identification and general description of the safety function
5.2	Safety requirements specification
5.2.1	General requirements
5.2.1.1	General
5.2.1.2	Necessary information to produce the safety requirements specification
5.2.1.3	Specification of all safety functions in the safety requirements specification

第4版改正動向

2nd DIS 改正点概要

第3版構成

5.1 Table 8	Some International Standards applicable to typical machine safety functions and certain of their characteristics
5.1 Table 9	Some International Standards giving requirements for certain safety functions and safety-related parameters
5.2	Details of safety functions
5.2.1	Safety-related stop function
5.2.2	Manual reset function
5.2.3	Start/restart function
5.2.4	Local control function
5.2.5	Muting function
5.2.6	Response time
5.2.7	Safety–related parameters
5.2.8	Fluctuations, loss and restoration of power sources

2nd DIS

Table M.1	Examples of International Standards applicable to typical machine safety functions and certain of their characteristics
Table M.2	Examples of International Standards giving requirements for certain safety functions and safety-related parameters
5.2.2	Requirements for specific safety functions
5.2.2.1	Safety-related stop function
5.2.2.2	Manual reset function
5.2.2.3	Restart function
5.2.2.4	Local control function
5.2.2.5	Muting function
5.2.2.6	Safety-related parameters
5.2.2.7	Fluctuations, loss and restoration of power sources
5.2.2.8	Requirements for operating mode selection
5.2.2.9	Safety function(s) for maintenance tasks

第4版改正動向

2nd DIS 改正点概要

5 Specification of safety functions + Annex M

5.1 Identification and general description of the safety function

SRP/CSで実現する安全機能の要求をどのように特定するか。

5.2 Safety requirements specification

安全要求仕様は各安全機能の詳細記述

第3版の表8、9は附属書Mに移動

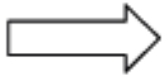
新たに、

“表3– ISO 12100に従ったリスクアセスメント/リスク低減からSRP/CS設計と評価プロセスを示す”、が追加された。

第4版改正動向

2nd DIS 改正点概要

Table 3 — Transition from the risk assessment and risk reduction process according to ISO 12100 to the SRP/CS design and evaluation process according to ISO 13849-1

Necessary information to produce the SRS (see 5.2.1.2)	Transformation	Examples of specifications of safety functions in the SRS (see 5.2.1.3)
— results of risk assessment of the machine or part of it, including hazardous parts — machine operating characteristics, e.g. intended use — emergency operation — description of the interaction of different working processes and manual activities, e.g. repairing — ergonomic aspects — limits of use in relation to environmental conditions		required safety functions (examples): 1) interlocking function — operating mode (all) — triggering event: opening of a movable guard — safety-related reaction: safe torque off (STO) of all movements — PL_r d — response time — etc. 2) safely limited speed (SLS) — operating mode (manual) — triggering event: Speed is higher than the specified limit — safety-related reaction: safe torque off (STO) of all movements — PL_r c — response time — etc.

第4版改正動向

2nd DIS 改正点概要

第3版構成

6	Categories and their relation to MTTFD of each channel, DCavg and CCF
6.1	General
6.2	Specifications of categories
6.2.1	General
6.2.2	Designated architectures
6.2.3	Category B
6.2.4	Category 1
6.2.5	Category 2
6.2.6	Category 3
6.2.7	Category 4
6.3	Combination of SRP/CS to achieve overall PL

2nd DIS

6	Design considerations
6.1.1	General overview of performance level
6.1.3	Architecture — Categories and their relation to $MTTF_D$ of each channel, average diagnostic coverage and common cause failure
6.1.3.1	General
6.1.3.2	Designated architectures — Specification of categories
6.1.3.2.1	General
6.1.3.2.2	Category B
6.1.3.2.3	Category 1
6.1.3.2.4	Category 2
6.1.3.2.5	Category 3
6.1.3.2.6	Category 4
6.2	Combination of subsystems to achieve an overall performance level of the safety function
6.2.1	General
6.2.2	Known PFH_D values
6.2.3	Unknown PFH_D values

第4版改正動向

2nd DIS 改正点概要

第3版構成

7	Fault consideration, fault exclusion
7.1	General
7.2	Fault consideration
7.3	Fault exclusion

2nd DIS

6.1.10	Fault consideration and fault exclusion
6.1.10.1	General
6.1.10.2	Fault consideration
6.1.10.3	Fault exclusion
6.1.11	Well-tried component

第4版改正動向

2nd DIS 改正点概要

第3版構成

8 Validation

詳細はISO 13849-2（JIS B 9705-2）

2nd DIS

10 Validation

10.1 Validation principles

10.2 Validation of the safety requirements specification

10.3 Validation by analysis

10.4 Validation by testing

10.5 Validation of the safety functions

10.6 Validation of the safety integrity of the SRP/CS

10.7 Validation of environmental requirements

10.8 Validation record

10.9 Validation maintenance requirements

第4版改正動向

2nd DIS 改正点概要

第3版構成

9 Maintenance

10 Technical documentation

11 Information for use

2nd DIS

11 Maintainability of SRP/CS

12 Technical documentation

13 Information for use

13.1 General

13.2 Information for SRP/CS integration

13.3 Information for user

第4版改正動向

2nd DIS 改正点概要

第3版構成

Annex A Determination of required performance level (PLr)

Annex B Block method and safety-related block diagram

Annex C Calculating or evaluating $MTTF_D$ values for single components

Annex D Simplified method for estimating $MTTF_D$ for each channel

Annex E Estimates for diagnostic coverage (DC) for functions and modules

Annex F Estimates for common cause failure (CCF)

Annex G Systematic failure

Annex H Example of combination of several safety-related parts of the control system

Annex I Examples

Annex J Software

Annex K Numerical representation of Figure 5

2nd DIS

Annex A Guideline for the determination of required performance level

Annex B Block method and safety-related block diagram

Annex C Calculating or evaluating $MTTF_D$ values for single components

Annex D Simplified method for estimating $MTTF_D$ for each channel

Annex E Estimates for diagnostic coverage for functions and subsystems

Annex F Measures against common cause failures

Annex G Systematic failure

- G.5 Management of functional safety

Annex H Example of combination of several subsystems

Annex I Examples

Annex J Example of SRESW realisation

Annex K Numerical representation of Figure 12

第4版改正動向

2nd DIS 改正点概要

第3版構成

5.1 Table 8	Some International Standards applicable to typical machine safety functions and certain of their characteristics
5.1 Table 9	Some International Standards giving requirements for certain safety functions and safety-related parameters

2nd DIS

Annex L EMC immunity

Annex M Additional information for safety requirements specification

Table M.1 Examples of International Standards applicable to typical machine safety functions and certain of their characteristics

Table M.2 Examples of International Standards giving requirements for certain safety functions and safety-related parameters

Annex N Avoiding of systematic failure in software-design

Annex O Safety-related values of components or parts of control systems

第4版改正動向

2nd DIS 改正点概要

第**3**版構成

EMC要求

6.2.3 カテゴリー**B**

Specific requirements for electromagnetic compatibility are found in the relevant product standards, e.g. IEC 61800-3 for power drive systems. For functional safety of SRP/CS in particular, the immunity requirements are relevant. If no product standard exists, at least the **immunity** requirements of **IEC 61000-6-2** should be followed.

この要求はカテゴリー**1-4**に適用される

2nd DIS

6.1.3.2.2 カテゴリー**B**

Specific requirements for electromagnetic compatibility (EMC) (immunity requirements) are found in the relevant product or generic standards. Immunity requirements are particularly relevant for subsystems. Subsystems containing active electronic components shall meet **EMC immunity requirements** based on the environment as appropriate. For practical guidance see **Annex L.**

10.7 Validation of environmental requirements

Where applicable, validation shall address

- **electromagnetic compatibility (immunity)**.
-

12 Technical documentation

When designing an SRP/CS according to this document at least the following information relevant to the safety-related part shall be documented for internal purpose:

d) environmental conditions (e.g. **EMC immunity, temperature**, vibration);

第4版改正動向

2nd DIS 改正点概要

- **附属書L　（情報）EMC immunity　12月14-16日のミーティングで最終修正予定**

The following routes provide guidance to fulfil EMC immunity measures for an SRP/CS or subsystems. At least one or more routes should be selected and fully applied:

— Route A: follow the EMC requirements of the relevant product standard (see IEC 61000-6-7:2014, 4.1, 1st sentence). Examples of product standards are IEC 61326 3 1 or 61800-5-2);

— Route B: for PL_r a and b, follow the EMC requirements of IEC 61000-6-2;

— Route C: for PL_r c, d and e implement EMC measures to achieve a score of at least 280 (of possible 400) according to Table "EMC" L.1 (see IEC 61000-6-7, 4.1, Note 1); for PL_r e, this route can only be applied if the requirements of category 4 are additionally fulfilled;

— Route D: follow IEC 61000-6-7 or other generic EMC standards for functional safety.

第4版改正動向

2nd DIS 改正点概要

- **附属書L　（情報）EMC immunity　12月14-16日のミーティングで最終修正予定**

Table L.1 — Measures to achieve EMC for safety-related components and other electrical/ electronic parts

Measures to achieve EMC	Score[a]
Safety-related sensors and their harness	
application of the measures described in Annex H of IEC 60204-1 and/or IEC 61800-3	10
analog voltage signals, angle encoder shielded and grounded and/or twisted cables for sensors and safety-related input/output-signals (cable shields are flat grounded in low impedance close to the components)	20
harnesses and wiring of low voltage DC between components is in twisted pair cabling	10
Safety-related IO system (central or decentral or integrated in the PLC)	
installed in a shielded and bonded cabinet or components in a shielded and bonded housing	20

NOTE　Redundant channels in Table L.1 means functional channel and test channel in category 2 or redundant functional channels in categories 3 and 4.

[a] Where technological measures are not relevant, scores attached to this column can be considered in the comprehensive calculation.

[b] The zones can be located inside one cabinet or separated into several cabinets.

ご清聴ありがとうございました

お問い合わせ
テュフ ラインランド ジャパン株式会社
テクノロジーセンター
杉田　吉広
〒224-0021 **横浜市都筑区北山田**4-25-2
電話: 045 914 0369
Fax: 045 914 3377
E-mail：Yoshihiro.sugita@tuv.com

www.jpn.tuv.com