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
第3版対応JIS改正の動向

テュフラインランドジャパン株式会社
製品部　産業機器課
杉田　吉広

目次

ISO 13849-1とは？

適用範囲

- ソフトウエアを含み、制御システムの安全関連部（SRP/CS)の設計及び統合のための原則に関する安全要求事項及び指針について規定。
- SRP/CSに対して、安全機能を実行するために要求されるパフォーマンスレベルを含む特性について規定。
- 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 a Dangerous Failure，PFH_D）で規定する。
- 高頻度作動要求又は連続モードに適用する。

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、構造分類（カテゴリ、B, 1, 2, 3, 4の5分類）
- 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）

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

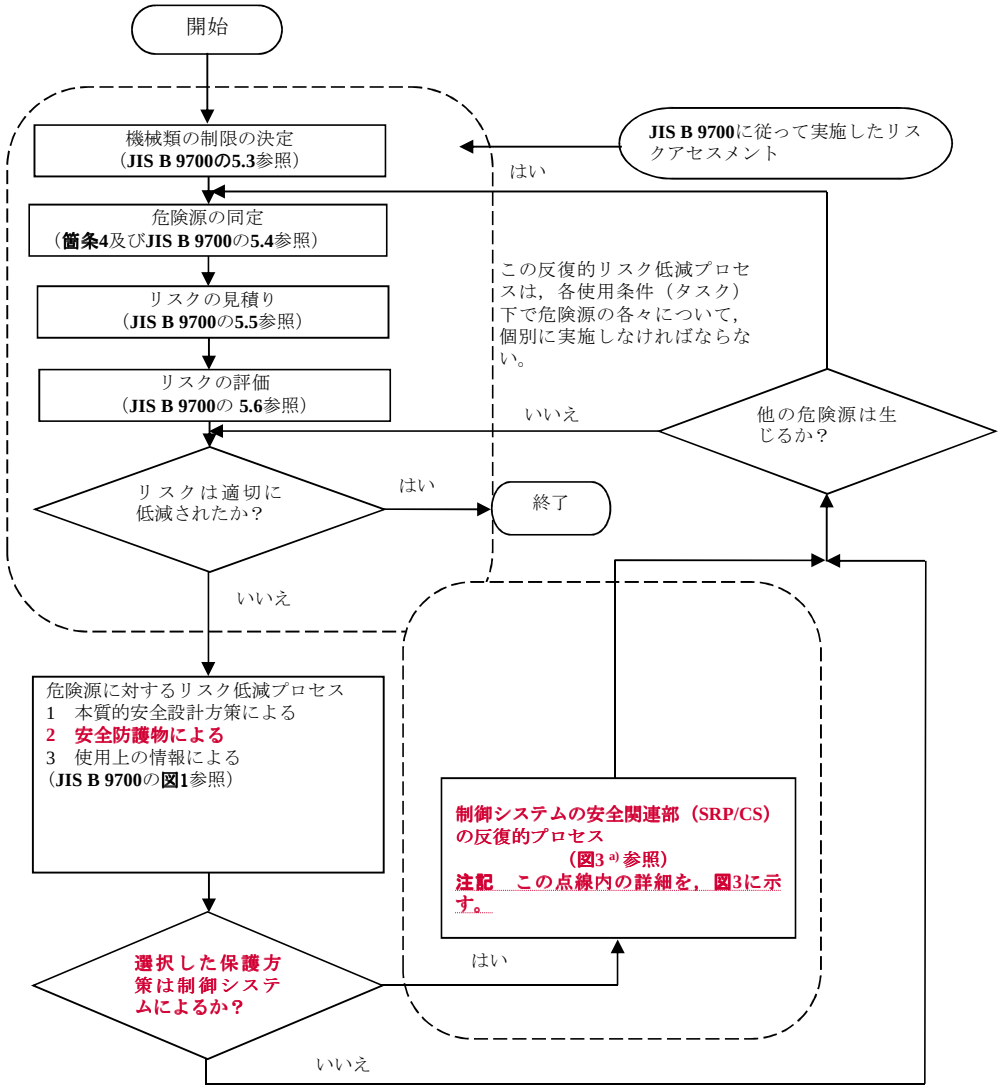
IEC 62061+A1+A2:2015: Safety of machinery - Functional safety of safety–related electrical, electronic and programmable electronic control systems

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

ISO 13849-1概要

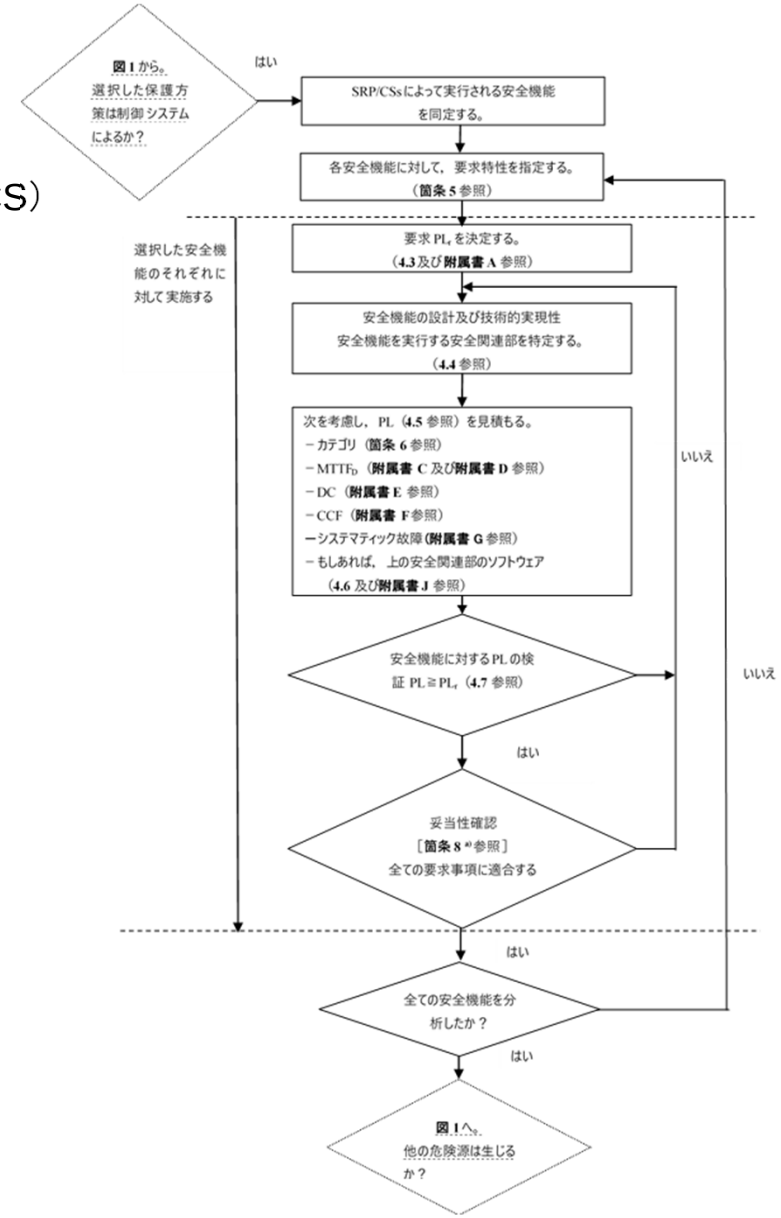
図1　–　リスクアセスメントとリスク低減



- 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。

ISO 13849-1概要

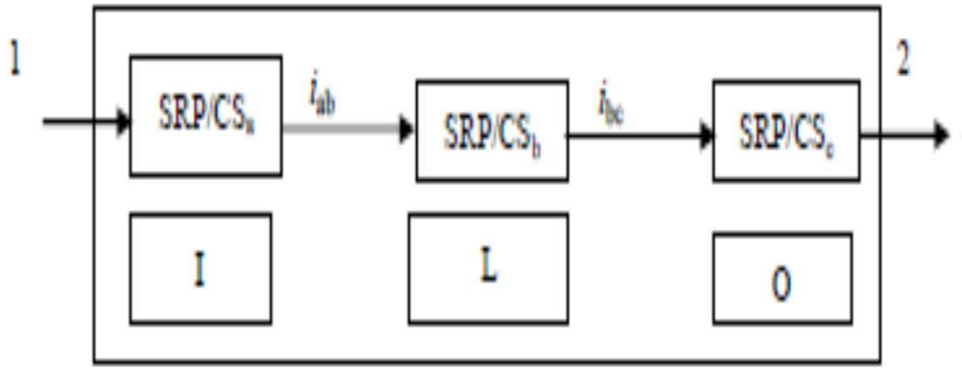
図3－制御システムの安全関連部（SRP/CS）の設計のための反復的プロセス



- 安全機能の同定
- 要求特性の指定
- 要求PLrの決定
- 安全関連部の特定
- PLの見積もり
  - カテゴリ
  - $MTTF_D$
  - DC
  - CCF
  - システマティック故障
  - ソフトウエア(使用されていれば）
- PLの検証（PL≥PLr)
- 妥当性確認

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］

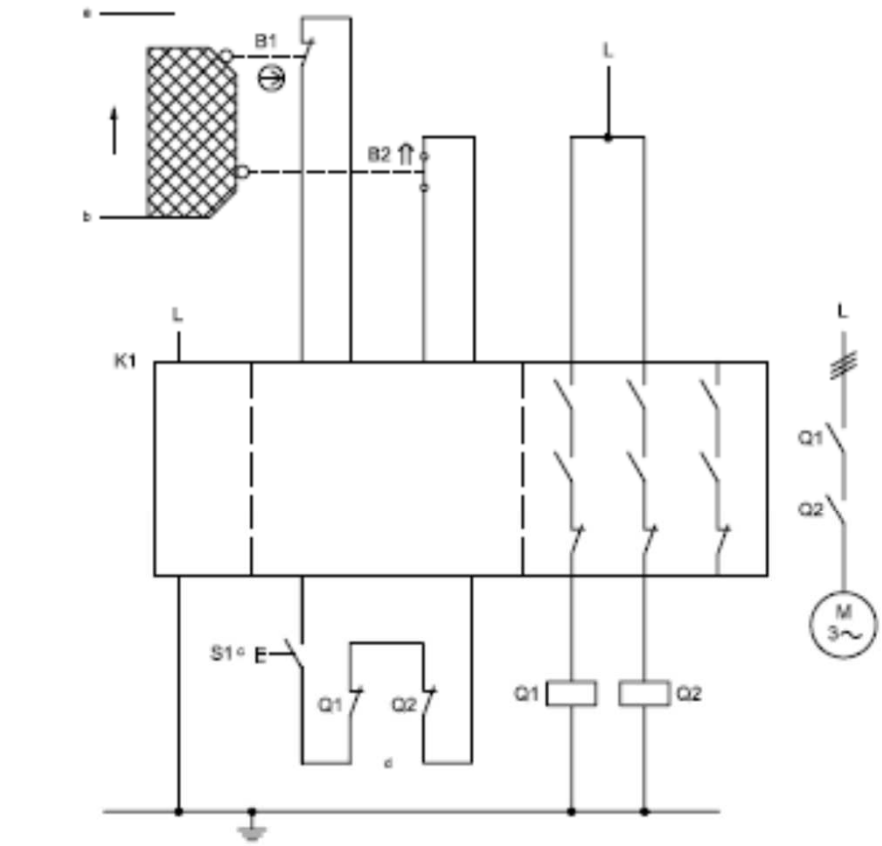
2: 機械アクチュエータ（例えば，モータ，シリンダ）

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.

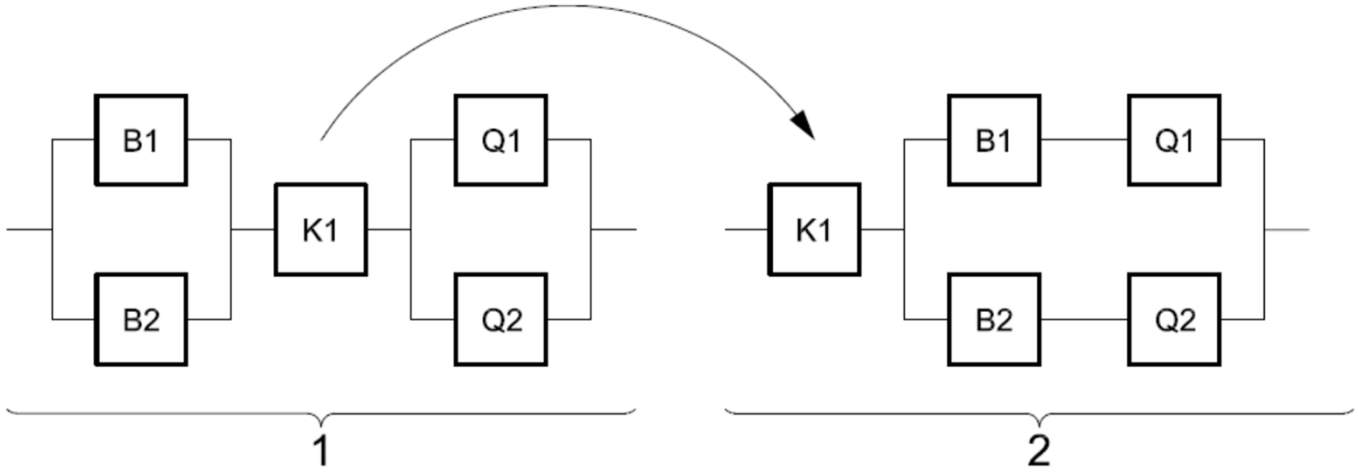
Figure 1 — Example implementation of the safety function

ISO/TR23849　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。

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
- 2019年以降 DIS、FDIS発行予定
- 2020年以降 IS発行予定

第4版改正動向

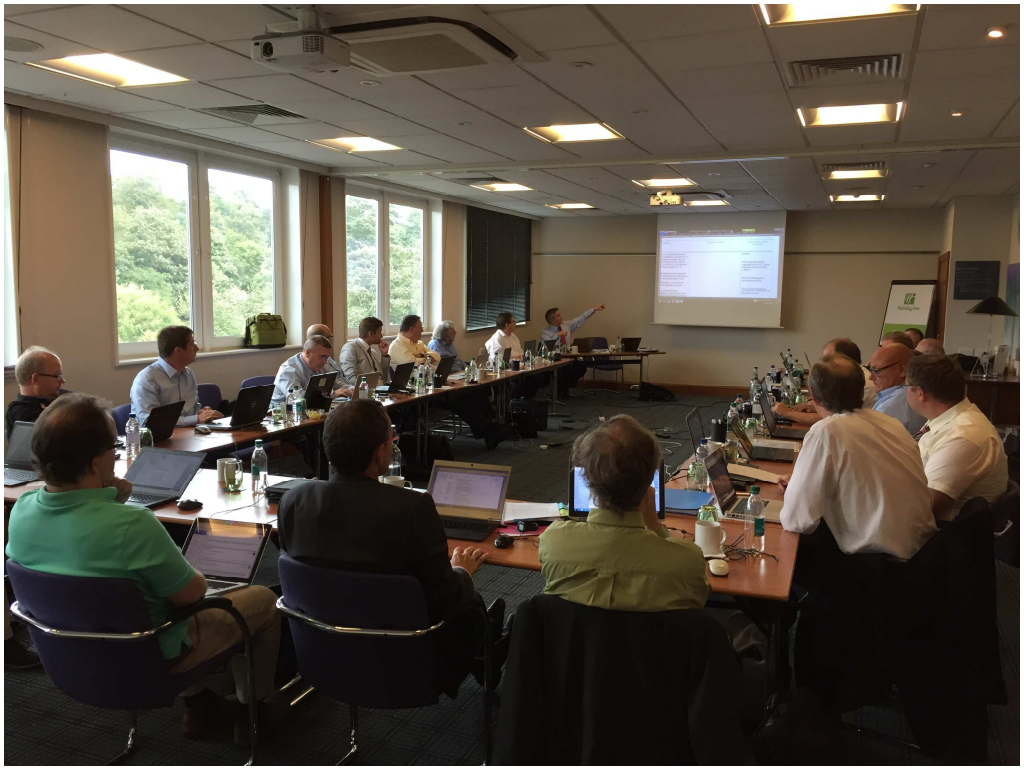
改正作業開始からWD1発行まで

期間：2016年1月 - 2017年2月

WGミーティング回数：10回

2017年2月　WD1発行

- 全体構成の見直し
- ISO/IEC 17305開発時の文書の使用
- ソフトウエア詳細要求
- Validationの詳細要求



2016年8月第21回WGミーティング

第4版改正動向

改正作業開始からWD1発行まで

2015年版構成

4 Design considerations

4.1 Safety objectives in design

4.2 Strategy for risk reduction

4.3 Determination of required performance level (PLr)

4.4 Design of SRP/CS

4.5 Evaluation of the achieved performance level PL and relationship with SIL

4.6 Software safety requirements

4.7 Verification that achieved PL meets PLr

4.8 Ergonomic aspects of design

5 Safety functions

5.1 Specification of safety functions

5.2 Details of safety functions

6 Categories and their relation to $MTTF_D$ of each channel, DC_{avg} and CCF

6.1 General　6.2 Specifications of categories

6.3 Combination of SRP/CS to achieve overall PL

WD開発時案

4 Overview [New]

Flowchart Figure 3 [updated to new organization]

Risk assessment of the machine [ISO 12100] [4.1 & Figure 1] [4.2]

Risk reduction using a SRP/CS [Bridge document ISO 22100-2]

5 Safety functions [5.1]

5.1 General

5.2 General description of the safety function

Annex of detailed safety functions [5.2]

6 Design considerations

Determination of required performance level (PLr) [4.3]

Design of SRP/CS [4.4]

Parameters (Evaluation of the achieved performance level …)[4.5]

第4版改正動向

改正作業開始からWD1発行まで

2015年版構成

7 Fault consideration, fault exclusion

8 Validation

WD開発時案

7 Software safety requirements [4.6]

7.1 General

7.2 Software safety requirements

7.3 Software safety requirements specification

7.4 Requirements for software architecture

7.5 Application software design and development

7.6 Software testing

8 Verification that achieved PL meets PLr [4.7]

9 Validation [9]

9.1 Validation principles

9.2 Validation by checking

9.3 Validation by testing

9.4 Validation of the SRP/CS

第4版改正動向

改正作業開始からWD1発行まで

2015年版構成

9 Maintenance

10 Technical documentation

11 Information for use

Annexes

WD開発時案

10 Maintenance [10]

11 Technical documentation [11]

12 Information for use [12]

Annexes

第4版改正動向

WD1発行からCD発行まで

期間：2017年6月 - 2018年5月
2017年12月　WD2発行
WGミーティング回数：5回
WD1に対するコメント数：469
WD2に対するコメント数：567
CD発行：2018年6月

2017年9月第26回WGミーティング

第4版改正動向

WD1発行からCD発行まで

WD1発行時構成

4 Overview

4.1 General approach

4.2 Contribution to the risk reduction by the control system

4.3 Risk reduction using a SRP/CS

4.4 Principle methodology

4.5 Required Information

4.6 Application level

5 Specification of safety functions

5.1 General

5.2 General description of the safety function

5.3 Detailed description of the safety function

5.4 Specification review

CD構成

4 Overview

4.1 Requirements for risk assessment and risk reductions

4.2 Contribution to the risk reduction by the control system

4.3 Risk reduction using a SRP/CS

4.4 Principle methodology

4.5 Required Information

4.6 Application level

5 Specification of safety functions

5.1 General

5.2 Safety requirements specification (SRS)

5.3 Additional requirements for safety functions

5.4 Determination of required performance level (PLr) for each safety function

5.5 Review of the safety requirement specification

第4版改正動向

WD1発行からCD発行まで

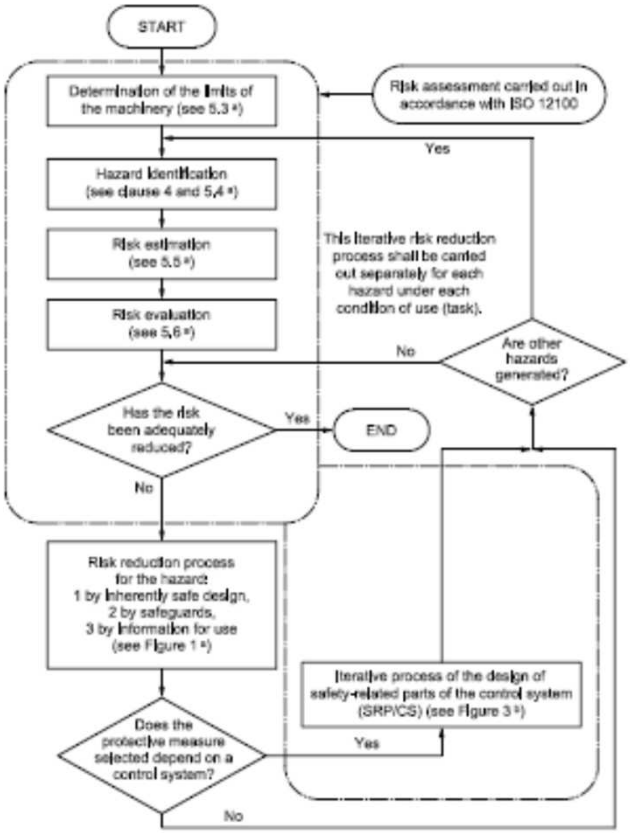


Figure 1 — Overview of risk assessment/risk reduction

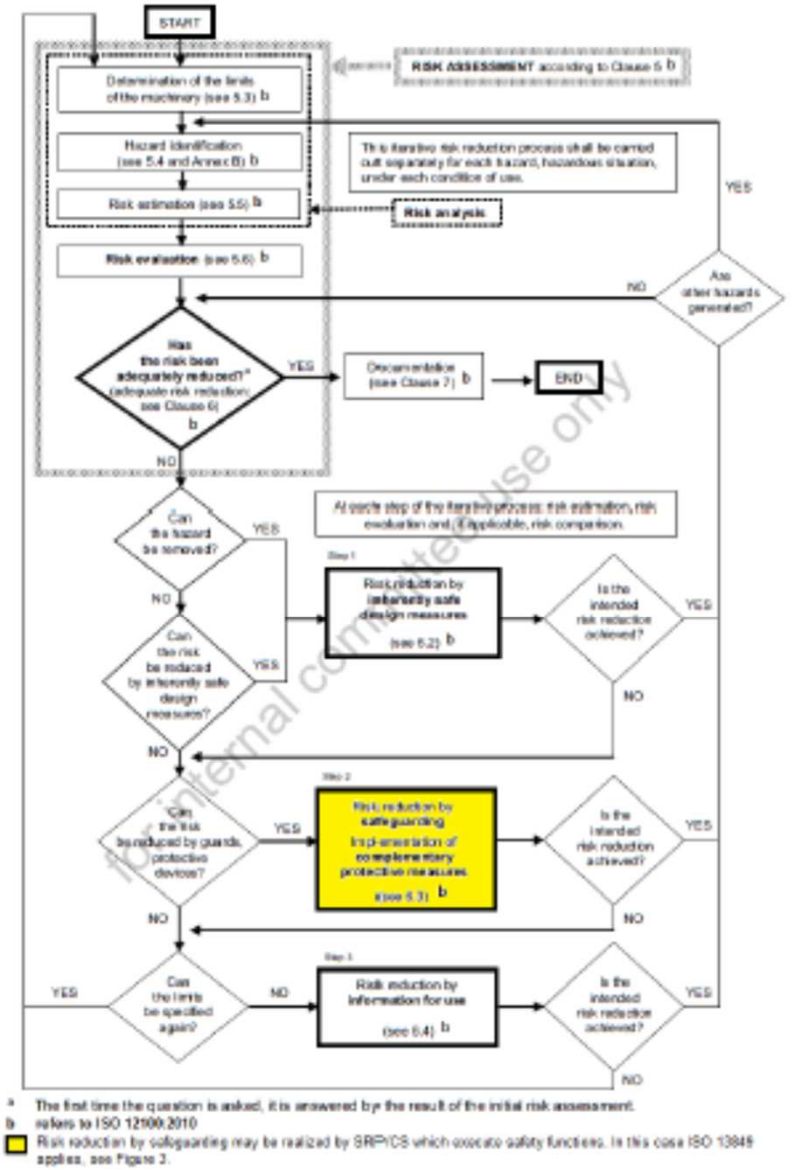


Figure 2 — Schematic representation of risk reduction process including iterative three-step method according to ISO 12100:2010

第4版改正動向

WD1発行からCD発行まで

ISO 13849-2 provides additional help for the validation.

Figure 3 — Iterative process for design of safety-related parts of control systems (SRP/CS)

ISO 13849-1: 2015

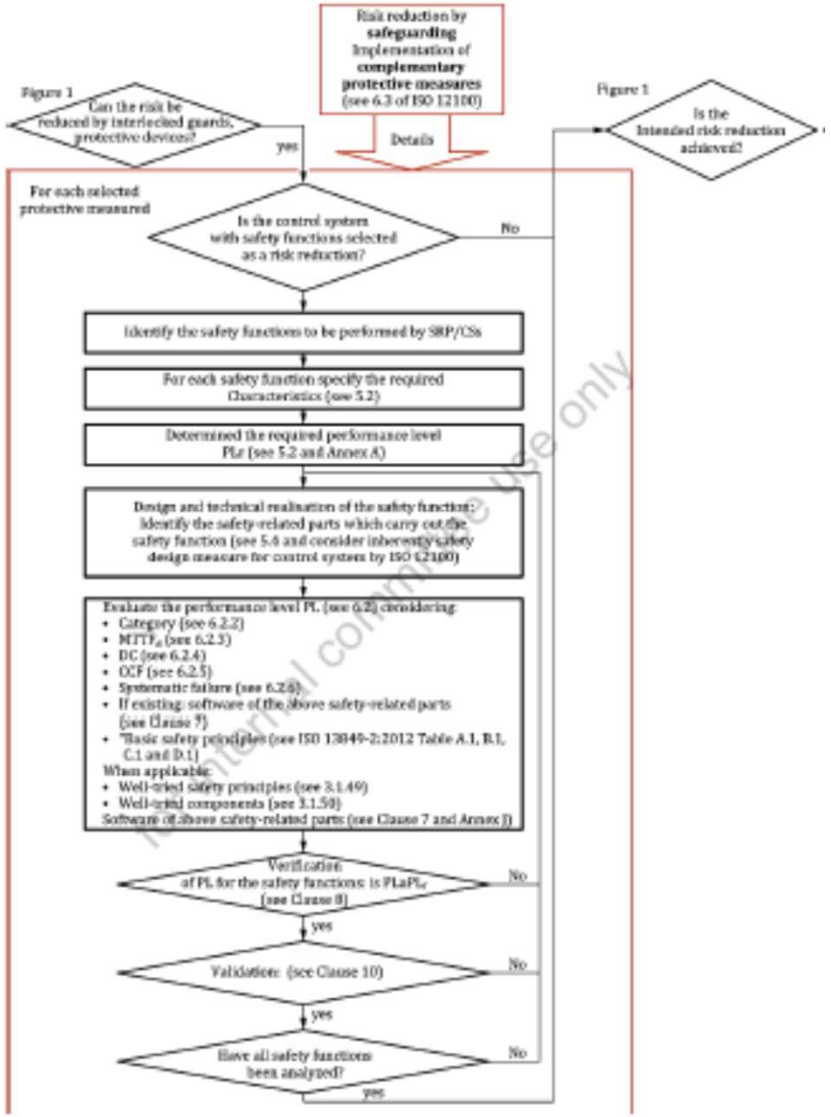


Figure 3 — Designing a SRP/CS in accordance with ISO 13849-1

第4版改正動向

WD1発行からCD発行まで

WD1発行時構成

6 Design considerations

6.1 Determination of required performance level (PLr) for each safety function

6.2 Design of SRP/CS

6.3 Evaluation of the achieved performance level PL and relationship with SIL

6.4 Combination of SRP/CS to achieve overall PL

7 Software safety requirements

7.1 General

7.2 Safety-related embedded software (SRESW)

7.3 Safety-related application software (SRASW)

7.4 Software-based parameterization

CD構成

6 Design considerations

6.1 Design of SRP/CS

6.2 Evaluation of the achieved performance level PL and relationship with SIL

6.3 Combination of SRP/CS to achieve overall PL of the safety function

6.4 Software based manual parameterization

7 Software safety requirements

7.1 General

7.2 Software levels

7.3 Software Level A

7.4 Software Level B

7.5 Software Level C

第4版改正動向

WD1発行からCD発行まで

Table 11 — Different levels of software

		HW	Embedded (SW)	Application (SW)
Level A[a]	Definition	Pre-assessed for functional safety (e.g. IEC 61508)	Pre-assessed for functional safety (e.g. IEC 61508)	LVL (SRASW)
	Requirements	According to manufacturer instruction	not applicable (embedded SW cannot be modified by the user)	LVL 7.1.3 to 7.1.10
Level B[b]	Definition	General Purpose	IEC 61131-3	LVL (SRASW)
	Requirements	Diversity required for PL c, d and e (see Table 13)	Diversity required for PL c, d and e (see Table 13)	LVL 7.1.11 to 7.1.20
Level C[c]	Definition	Application specific	LVL FVL	
	Requirements	Diversity required for PL e (see Table 17)	LVL 7.1.3 to 7.1.10 FVL 7.1.21 to 7.1.30	

a Use of a pre-assessed hardware with internal software designed for safety applications: Typically the use of module based programing which limits the inputs and outputs to a pre-defined set of values, including a combination of modules (see Figure 14). For the design of modules using LVL see Figure 15.

NOTE For the design of modules not using LVL see Software Level C.

b Use of hardware with internal software designed for the application of LVL software, but not explicitly designed for safety application.

c Use of a language other than a limited variability language (LVL). Typically in an embedded software application.

第4版改正動向

WD1発行からCD発行まで

WD1発行時構成

8 Verification that achieved PL meets PLr

9 Ergonomic aspects of design

10 Validation

10.1 Validation principles

10.2 Validation record

10.3 Validation by analysis

10.4 Validation by testing

10.5 Validation of safety requirements specification for safety functions

10.6 Validation of the safety function

10.7 Validation of the safety integrity of the SRP/CS

11 Maintenance

12 Technical documentation

13 Information for use

CD構成

8 Verification that achieved PL meets PLr

9 Ergonomic aspects of design

10 Validation

10.1 Validation principles

10.2 Validation record

10.3 Validation by analysis

10.4 Validation by testing

10.5 Validation of safety requirements specification for safety functions

10.6 Validation of the safety function

10.7 Validation of the safety integrity of the SRP/CS

11 Maintenance

12 Technical documentation

13 Information for use

13.1 General

13.2 Information for SRP/CS integrator

13.3 Information for end-user

第4版改正動向

WD1発行からCD発行まで

WD1発行時構成

Annex A (informative) Determination of required performance level (PLr)

Annex B (informative) Block method and safety-related block diagram

Annex C (informative) Calculating or evaluating MTTFD values for single components

Annex D (informative) Simplified method for estimating MTTFD for each channel

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

Annex F (normative) Measures against common cause failures (CCF)

Annex G (informative) Systematic failure

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

Annex I (informative) Examples

Annex J (informative) Software

Annex K (informative) Numerical representation of Figure 5

CD構成

Annex A (informative) Determination of required performance level (PLr)

Annex B (informative) Block method and safety-related block diagram

Annex C (informative) Calculating or evaluating MTTFD values for single components

Annex D (informative) Simplified method for estimating MTTFD for each channel

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

Annex F (normative) Measures against common cause failures (CCF)

Annex G (informative) Systematic failure

Annex H (informative) Example of combination of several subsystems

Annex I (informative) Examples

Annex J (informative) Software

Annex K (informative) Numerical representation of Figure 12

Annex L (informative) EMC immunity requirements

第4版改正動向

WD1発行からCD発行まで

Annex L EMC Immunity requirements
(Informative)

The following routes provide guidance to fulfil EMC immunity requirements for an SRP/CS:

— Route A: Follow the EMC requirements of the relevant product standard (see IEC 61000-6-7, 4.1, 1st sentence);

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

— Route C: For PL_r c and d, implement all "mandatory" EMC measures and enough other EMC measures to achieve a score of at least 70 (of possible 100) according to Table "EMC" (see IEC 61000-6-7, 4.1, Note 1);

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

第4版改正動向

CD発行後

期間：2018年10月作業開始
WGミーティング回数：　第30回10月実施
第31回11月実施予定
第32回12月実施予定

CDに対するコメント数：1,366
（テクニカルなコメントは40-50%程度）
日本からのコメント：32
DIS発行：2019年予定
IS発行：2020年??

コメント審議ポイント

- コメントは序文からAnnexまでほぼすべての章に…
- 改定中のIEC62061との関係・整合化
- 定義の見直し、追加
  - Safety sub-system
  - Well-tried component
  - Verification
  - Validation, 等々
- 図1、2、3の見直し（ISO 12100との関係）
- ソフトウエア要求事項

第3版対応JIS改正動向

JIS B 9705-1

- 2018年3月
  - 国内SWGでJIS原案作成、日本規格協会に提出

- 2018年7月
  - 日本規格協会での修正終了、審議待ち

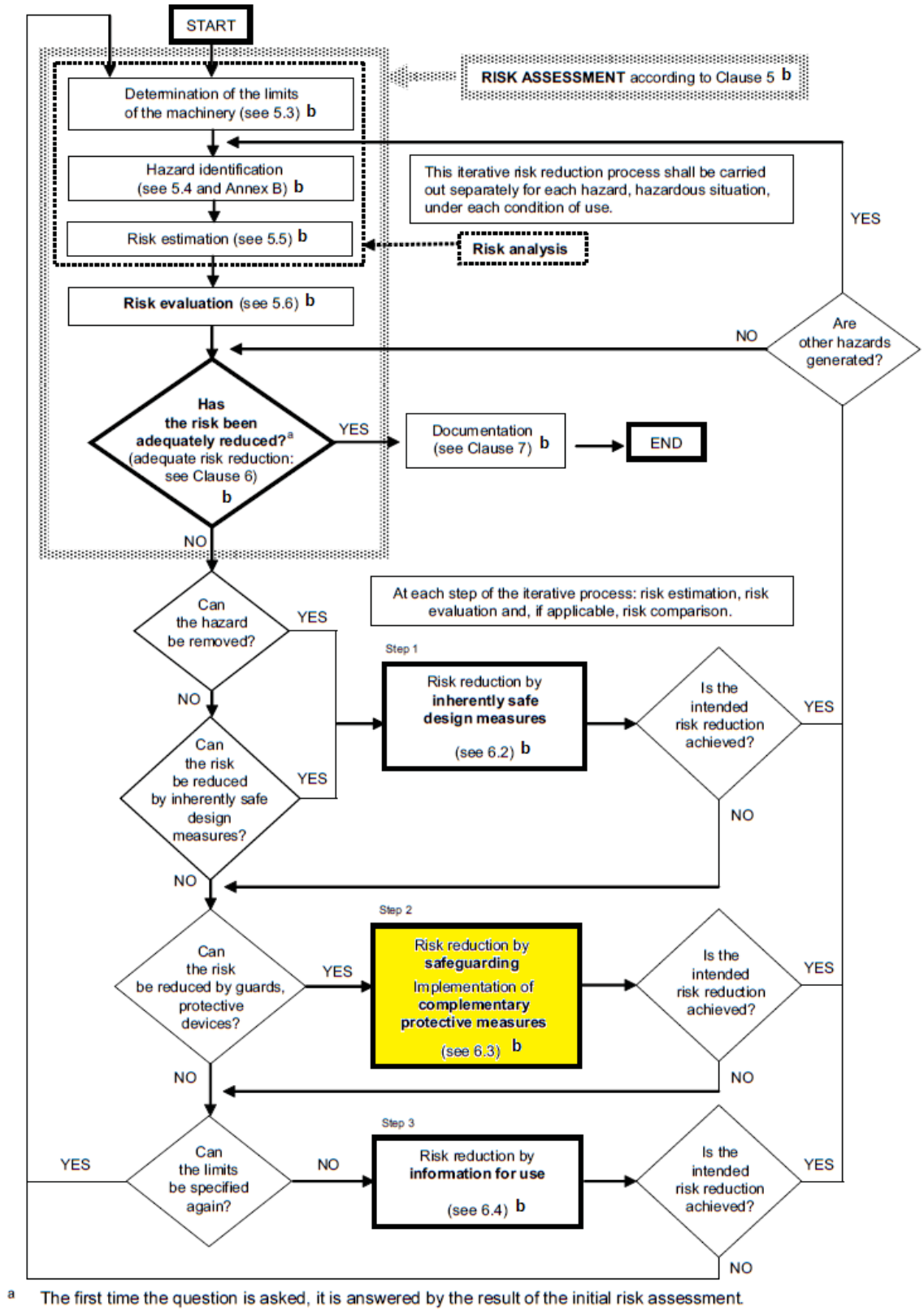
- JIS原案の表記
  - ISO 13849-1:2015で追加された部分以外は、JIS B 9705- 1 : 2011 (ISO 13849-1: 2006)と変更なし

- 関連規格のJIS化
  - ISO 13849-2のJIS化
  - JIS B 9705-2として既に最終草案作成済み
  - 日本規格協会での修正終了、審議待ち
  - 表記・用語等はJIS B 9705-1: 2011と整合化

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



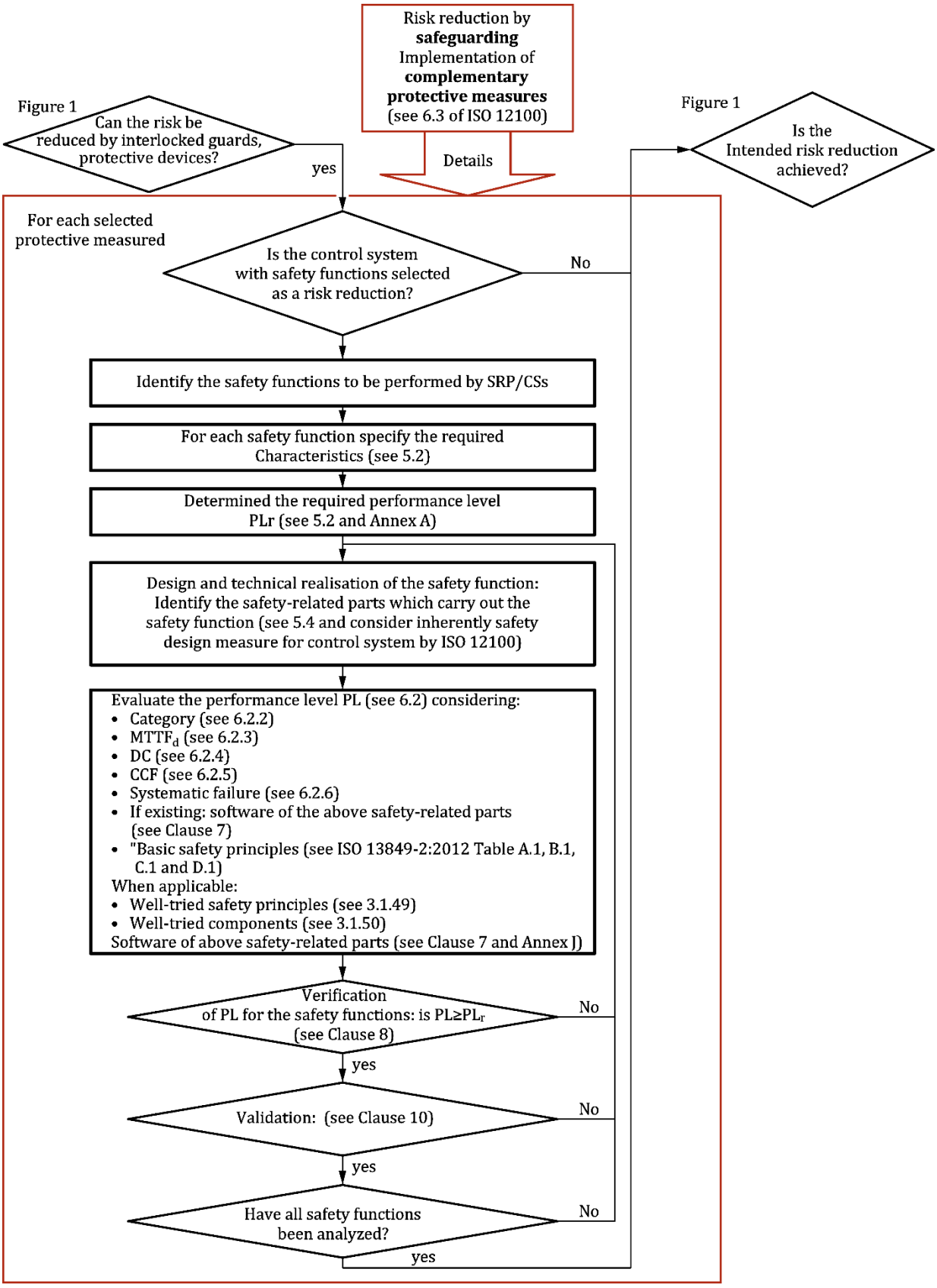
a The first time the question is asked, it is answered by the result of the initial risk assessment.

b **refers to ISO 12100:2010**

Risk reduction by safeguarding may be realized by SRP/CS which execute safety functions. In this case ISO 13849 applies, see Figure 3.

389

390 **Figure 2 — Schematic representation of risk reduction process including iterative three-step**
391 **method according to ISO 12100:2010**



402

403 **Figure 3 — Designing a SRP/CS in accordance with ISO 13849-1**