

ISO 13849-1

# 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



チューブラインランドジャパン株式会社  
製品部  
杉田吉広

# 概要

1. ISO 13849-1とは？
2. ISO 13849-1の改定履歴
3. ISO 13849-1の関連規格
4. ISO 13849-1の構成と変更章
5. ISO 13849-1の変更点
6. まとめ

# ISO 13849-1とは？

- ソフトウェアを含み、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
- タイプB1規格 – 特定の安全面 (例えば、安全距離、表面温度、騒音) に関する規格
- 予見可能な条件下での制御システムの安全機能の遂行能力は、5通りのレベルのうちの一つに振り分けられて、それはパフォーマンスレベル PLと呼ばれる。このパフォーマンスレベルは、 $PFH_D$  (単位時間当たりの危険側故障発生確率の用語で定義される

表2 パフォーマンスレベル

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

# ISO 13849-1とは？ - 2

- 設計者を支援し、かつ、達成したPLの査定を容易にするために、この規格では、指定の設計基準及び障害条件下での指定の挙動に従った構造分類に基づく方法論を採用する。この分類は、5通りのレベルのうちの一つに振り分けられ、それはカテゴリ、B, 1, 2, 3, 4と呼ばれる
- 適用される制御システムの安全関連部
  - 保護装置（例えば、両手操作制御装置、インタロック装置）、電氣的検知保護装置（例えば、光電カーテン）、圧力検知装置
  - 制御ユニット（例えば、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（例えば、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（例えば、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（例えば、包装機械、印刷機械、プレス機械）

# ISO 13849-1の改定履歴

- 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 IEC 62061との統合を視野に入れ、第2版をよりユーザーフレンドリーにするための改定(追補発行)を決定  
(新たな技術的内容を加えないこと、理解しやすくするための追補発行で合意)
  - 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7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、CDV発行手続き
  - 2014年3月第16回WGでCDV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(ISO13849-1FDAM1)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を統合した)
  - 2016年1月より改定に向けて作業開始(WDの作成)

# ISO 13849-1の関連規格

- ISO 13849-2: 2012 Safety of machinery — Safety-related parts of control systems — Part 2: Validation
  - JIS申請中
- ISO 12100: 2010 Safety of machinery — General principles for design — Risk assessment and risk reduction
  - JIS B9700:2013
- ISO/TR 22100-2:2013, *Safety of machinery — Relationship with ISO 12100 — Part 2: How ISO 12100 relates to ISO 13849-1*
- ISO/TR 23849, *Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery*
- IEC 62061: 2012 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems
  - JIS B9961: 2008+追補1:2015
- IEC 61508 series (part 1 to 7):2010 Functional safety of electrical/electronic/programmable electronic safety-related systems
  - JIS C0508 シリーズ (パート1から7): 2012/2014/2014/2012/1999/2000/2000

# ISO 13849-1の構成と変更章

まえがき

序文

1. 適用範囲
2. 引用規格
3. 用語、定義、記号及び略号
4. 設計上での考慮事項
5. 安全機能
6. カテゴリと各チャンネルの $MTTF_D$ 、 $DC_{avg}$ 及びCCFの関係
7. 障害の考慮、障害の除外
8. 妥当性確認
9. 保全
10. 技術文書
11. 使用上の情報

当発表資料の日本語訳はJIS B9705-1:2011 (IDT: ISO 13849-1: 2006)による。

# ISO 13849-1の構成と変更章 - 2

- **附属書A (参考) 要求パフォーマンスレベルPLrの決定**
- 附属書B (参考) ブロックメソッド及び安全関連ブロックダイアグラム
- **附属書C (参考) 単一コンポーネントのMTTF<sub>D</sub>値の計算又は評価**
- 附属書D (参考) チャンネルごとのMTTF<sub>D</sub>を見積るための簡易的な方法
- 附属書E (参考) 機能及びモジュールの診断範囲(DC)の見積り
- 附属書F (参考) 共通原因故障(CCF)の見積り
- 附属書G (参考) システムティック故障
- 附属書H (参考) 制御システムにおける複数の安全関連部の組合せ例
- **附属書I (参考) 事例**
- 附属書J (参考) ソフトウェア
- **附属書K (参考) 図5の数値**



# ISO 13849-1の変更点 — 1

主に規格の廃止、改定及び新規発行による

- ISO/TR 13849-100の廃止、
  - ISO 12100:2010の発行 (ISO 12100-1, -2, ISO 14121の置き換え)、
  - ISO/TR 22100-2の発行 (ISO 12100との関係)
  - ISO/TR 23849の発行 (IEC 62061との関係)、
  - IEC 62061:2012の発行\*、
- 等々。

\*:第1.1版 IEC 62061:2005+AMD1:2012

第1.2版 IEC 62061: 2005+AMD1: 2012+ AMD2: 2015

新たな技術的内容を加えない、理解しやすくするための追補を統合した版である。

当発表資料はすべての変更点を記載しているわけではありません。

# ISO 13849-1の変更点 - 2

## 3章

### 追加された定義

- 3.1.38: high demand or continuous mode/高頻度又は連続モード
  - 出展: IEC 62061:2012, 3.2.27修正
- 3.1.39: proven in use/実績による使用
  - 出展: IEC 61508: 2010, 3.8.18修正

### 追加された記号及び略号

- 表1(旧表2)に $T_{10D}$ (コンポーネントの10%が危険側故障に至るまでの平均時間)を追加
- 附属書Cには従来から記載あり(式C.3)

Table 1 (continued)

Symbol or abbreviation	Description	Definition or occurrence
SIL	Safety integrity level	<a href="#">Table 4</a>
SRASW	Safety-related application software	<a href="#">4.6.3</a>
SRESW	Safety-related embedded software	<a href="#">4.6.2</a>
SRP	Safety-related part	General
SRP/CS	Safety-related part of a control system	<a href="#">3.1.1</a>
TE	Test equipment	<a href="#">6.2</a>
$T_M$	Mission time	<a href="#">3.1.28</a>
$T_{10D}$	Mean time until 10 % of the components fail dangerously	<a href="#">Annex C</a>

$$T_{10d} = \frac{B_{10d}}{n_{op}}$$

$B_{10D}$ : コンポーネントの10%が危険側故障を生じるまでの平均サイクル数  
 $N_{op}$ : 年間の平均運転回数

# ISO 13849-1の変更点 — 3

## 4章

- 4.5.2章  $MTTF_D$
- 表4 (旧表5)の注記1の内容を明確にするため(カテゴリ4で $MTTF_D$ を2500年までにできる場合の条件)を本文第2段落に追記

For each SRP/CS (subsystem) according to Table 5, the maximum value of  $MTTF_D$  for each channel is 100 years. For Category 4 SRP/CS (subsystems) the maximum value of  $MTTF_D$  for each channel is increased to 2 500 years

- 附属書K、表K.1に $MTTF_D$ : 110-2500年を追加

# ISO 13849-1の変更点 — 3 (2)

- 4.5.5章 新規追加 Description of the output part of the SRP/CS by category

- 6.2.2項 指定アーキテクチャーの注記の内容を明確にするために。

- 注記を削除

注記: 個々の技術的解決策から生じるか、又はタイプC規格によって決定される場合、SRP/CSの安全関連のパフォーマンスは、PLrの追加要求なしにカテゴリによってだけ要求される場合がある。

- 以下4.5.5章として追記

If for mechanical, hydraulic or pneumatic components (or components comprising a mixture of technologies) no application-specific reliability data are available, the machine manufacturer may evaluate the quantifiable aspects of the PL without any  $MTTF_D$ -calculation.

機械、油圧、空圧部品で信頼性データが無い場合、PLを $MTTF_D$ の計算無しに決定できる

- 表7の追加

# ISO 13849-1の変更点 — 3 (3)

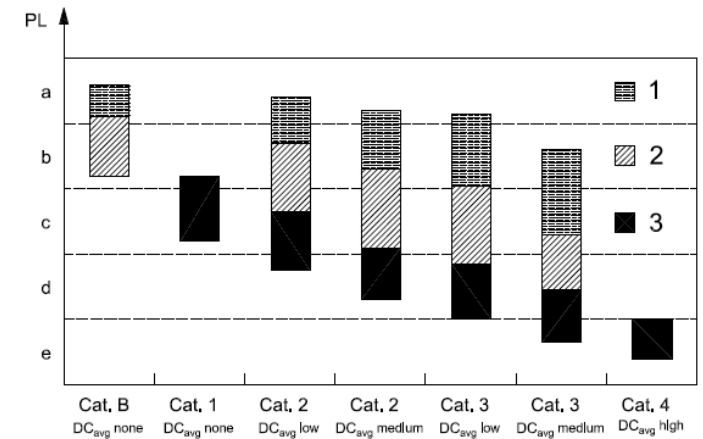
Table 7 — PL and PFH<sub>D</sub> as worst case estimation based on category, DC<sub>avg</sub>, and use of well-tried components

	PFH <sub>D</sub> (1/h)	Cat. B	Cat. 1	Cat. 2	Cat. 3	Cat. 4
PL a	2*10 <sup>-5</sup>	•	○	○	○	○
PL b	5*10 <sup>-6</sup>	•	○	○	○	○
PL c	1,7*10 <sup>-6</sup>	-	•2*	•1*	○	○
PL d	2,9*10 <sup>-7</sup>	-	-	-	•1*	○
PL e	4,7*10 <sup>-8</sup>	-	-	-	-	•1*

• Applied category is recommended.  
 ○ Applied category is optional.  
 - Category is not allowed.

1\* Proven in use (see 3.1.39) or well-tried (confirmed by the component manufacturer to be suitable for the particular application) components and well-tried safety principles must be used.  
 2\* Well-tried components and well-tried safety principles must be used.

For safety-related components that are not monitored in the process, the T10d value can be determined based on proven in use data by the machine manufacturer.



**Key**

- PL performance level
- 1 MTTFD of each channel = low
- 2 MTTFD of each channel = medium
- 3 MTTFD of each channel = high

Figure 5 — Relationship between categories, DC<sub>avg</sub>, MTTFD of each channel and PL

# ISO 13849-1の変更点 — 3 (4)

## ■ 4.6.2章 安全関連組込みソフトウェア (SRESW)

- SRESWの要求を満たしていないコンポーネントの場合の追記

For components for which SRESW requirements are not fulfilled, e.g. **PLCs without safety rating by the manufacturer**, these components may be used under the following alternative conditions:

- the SRP/CS is limited to PL **a** or **b** and uses category **B**, **2** or **3**;
- the SRP/CS is limited to PL **c** or **d** and may use multiple components for two channels in category **2** or **3**. The components of these two channels use diverse technologies

カテゴリ1には使用できない

# ISO 13849-1の変更点 — 4

## 5章 安全機能

- 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
- 表9 安全機能及び安全関連パラメータの要求事項を示す国際規格の修正（参照規格:ISO 12100-1, -2 =>ISO 12100:2010）

### 第3版

Table 8 — Some International Standards applicable to typical machine safety functions and certain of their characteristics

Safety function/ characteristic	Requirement(s)		For additional information, see:
	This part of ISO 13849	ISO 12100:2010	
Safety-related stop function initiated by safeguard <sup>a</sup>	<a href="#">5.2.1</a>	3.28.8, 6.2.11.3	IEC 60204-1:2005, 9.2.2, 9.2.5.3, 9.2.5.5 ISO 14119 ISO 13855
Manual reset function	<a href="#">5.2.2</a>	—	IEC 60204 9.2.5.4
Start/restart function	<a href="#">5.2.3</a>	6.2.11.3, 6.2.11.4	IEC 60204 9.2.5.1, 9.2.

### 第2版

Table 8 — Some International Standards applicable to typical machine safety functions and certain of their characteristics

Safety function/ characteristic	Requirement(s)			For additional information, see:
	This part of ISO 13849	ISO 12100-1:2003	ISO 12100-2:2003	
Safety-related stop function initiated by safeguard <sup>a</sup>	5.2.1	3.26.8	4.11.3	IEC 60204-1:2005, 9.2.2, 9.2.5.3, 9.2.5.5
Manual reset function	5.2.2	—	—	IEC 60204-1:2005, 9.2.5.3, 9.2.5.4
Start/restart function	5.2.3	—	4.11.3, 4.11.4	IEC 60204-1:2005, 9.2.1, 9.2.5.1, 9.2.5.2, 9.2.6
Local control function	5.2.4	—	4.11.8, 4.11.10	IEC 60204-1:2005, 10.1.5
Muting function	5.2.5	—	—	—

# ISO 13849-1の変更点 — 5

## 6章 カテゴリと各チャンネルの $MTTF_D$ 、 $DC_{avg}$ 及びCCFの関係

- 6.2.5 カテゴリ2
- 安全状態の始動に関する要求の明確化 (PLr=dとPLr=c以下により異なる要求)
- PLr=cまで:
  - 可能である場合、この出力 (OTE) は安全状態を始動しなければならない。障害が除去されるまで、安全状態を維持しなければならない
  - これが不可能な場合、出力 (OTE) は警告を発するだけで十分の場合もある
- PLr=d:
  - この出力 (OTE) は障害が除去されるまで維持される安全状態を始動しなければならない



# ISO 13849-1の変更点 — 5 (2)

- 6.2.7 カテゴリ4
- Note1(カテゴリの挙動)の修正

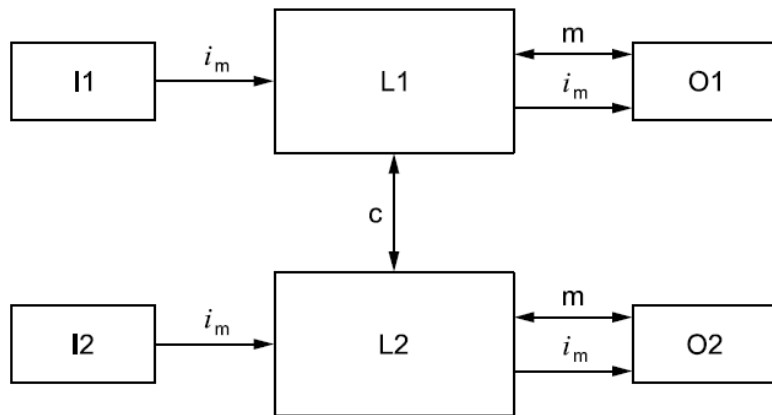
第3版	第2版	JISB9705-1
Category 4 system behaviour is characterized by	Category 4 system behaviour allows that	カテゴリ4のシステムには次の挙動が許される。
continued performance of the safety function in the presence of a single fault,	when a single fault occurs the safety function is always performed,	単一障害発生時、安全機能が常に働く。
detection of faults in time to prevent the loss of the safety function,	the faults will be detected in time to prevent the loss of the safety function,	障害は、安全機能の喪失を防止するために、適時検出される。
the accumulation of undetected faults is taken into account.	accumulation of undetected faults is taken into account.	未検出障害の蓄積を考慮する

# ISO 13849-1の変更点 — 5(3)

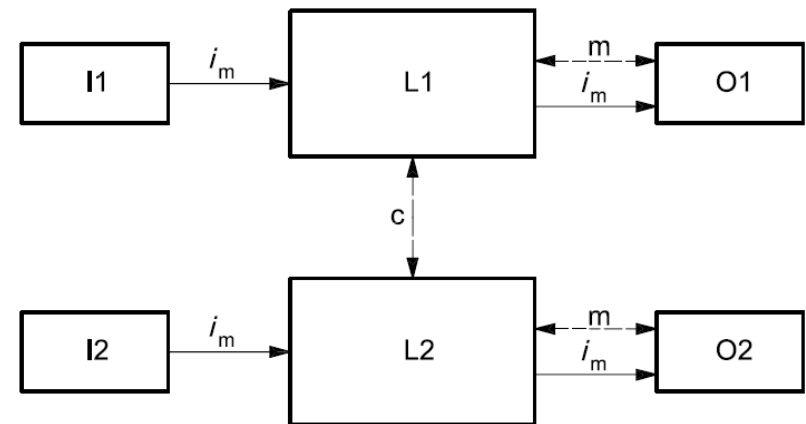
## ■ 図12の修正

- L1-O1間、L2-O2間及びL1-L2間の破線(m,c)が実線に変更(誤記訂正)
- 監視を示す実線は、カテゴリ3の指定アーキテクチャよりも高い診断範囲を表す

第3版



第2版



# ISO 13849-1の変更点 — 6

## 附属書A 要求パフォーマンスレベルPLrの決定

### ■ A.1 要求パフォーマンスレベルPLrの決定

- 第1段落に注記の追加
  - PLrを見積る方法論は強制ではない
  - C規格で要求されるPLrは図A.1で決定した場合と異なることがある
- 第2段落の修正
  - リスクアセスメントを使用していない。(‘リスクアセスメントは、意図する安全機能の設定前の状況を想定する。’の削除)
  - 図A.1の説明がリスクグラフからグラフへ変更  
但しI.2で”risk graph method (see Figure A.1)”という表記は使用されている

# ISO 13849-1の変更点 — 6(2)

- A2.2 危険源への暴露頻度及び/又は暴露時間F1及びF2
- F1/F2選択について記載された第4段落と注記を削除、以下の内容に変更
  - 頻度が15分に1回を超える=>F2が望ましい
  - 累積された暴露時間が作業時間の1/20を越えず、かつ頻度が15分に1回を超えなければF1を選んでもよい

出展: ISO/TC199/WG8 N119  
Emergency Stop Devices - (WG-2010.03 rev.2\_EN)

# ISO 13849-1の変更点 — 6(3)

## ■ A.2.3 Possibility of avoiding the hazard event P1 and P2 and probability of occurrence

=> 旧A.2.3をA.2.3.1 Possibility of avoiding the hazard とA.2.3.2 Probability of occurrence of a hazardous eventに分割

### ■ A.2.3

- A.2.3.1とA.2.3.2両方の組み合わせがパラメータ P
- P1を選択: 危険状態が発生して、事故を回避する又はその効果を顕著に軽減するための現実的機会が存在する場合だけ(変更なし)
- P2の選択条件修正
  - P2 should be selected if there is almost no chance of avoiding the hazard.
  - if there is a realistic chance of avoiding a hazard or of significantly reducing its effect; otherwise P2 should be selected.

### ■ A.2.3.1

- 旧A.2.3を修正

### ■ A.2.3.2

- 人間の挙動か技術的故障による
- 適切な発生確率は知られていない又は特定が難しい
- 信頼性データ、同等の機械でのアクシデントの履歴を含む事実をもとに見積る

# ISO 13849-1の変更点 — 6(4)

## ■ A.3 Overlapping hazards 新規追加

- 全ての危険源は特定の危険源または危険状態として考慮する
- 危険源は個別に評価することができる
- 常に同時に発生する直接リンクした危険源の組み合わせ (combination of directly linked hazards which always occur simultaneously) はリスク見積りは組み合わせて行うことが望ましい

## ■ 例

- 1. 溶接ロボット: 衝突とやけどは“combination of directly linked hazards”
- 2. 別々のロボットが稼動しているロボットセル: それぞれのロボットは別々と考える
- 3. リスクアセスメントの結果、クランピング素子を持つロータリーテーブルとクランピング素子は別と考えることができる

# ISO 13849-1の変更点 - 7

附属書C 単一コンポーネントのMTTF<sub>D</sub>値の計算又は評価

▪ 表C.1, 2, 3, 4, 5, 6, 7のMTTF<sub>D</sub>、B<sub>10D</sub>の追加・修正

- SN 29500 (all parts), Failure rates of components

第3版

Table C.1 — International Standards dealing with MTTF<sub>D</sub> or B<sub>10D</sub> for components

	Basic and well-tried safety principles according to ISO 13849-2:2012	Relevant standards	Typical values: MTTF <sub>D</sub> (years) B <sub>10D</sub> (cycles)
Mechanical components	Tables A.1 and A.2	—	MTTF <sub>D</sub> = 150
Hydraulic components with $n_{op} \geq 1\,000\,000$ cycles per year	Tables C.1 and C.2	ISO 4413	MTTF <sub>D</sub> = 150
Hydraulic components with 1 000 000 cycles per year > $n_{op} \geq 500\,000$ cycles per year	Tables C.1 and C.2	ISO 4413	MTTF <sub>D</sub> = 300

第2版

Table C.1 — International Standards dealing with MTTF<sub>d</sub> or B<sub>10d</sub> for components

	Basic and well-tried safety principles according to ISO 13849-2:2003	Other relevant standards	Typical values: MTTF <sub>d</sub> (years) B <sub>10d</sub> (cycles)
Mechanical components	Tables A.1 and A.2	—	MTTF <sub>d</sub> = 150
Hydraulic components	Tables C.1 and C.2	EN 982	MTTF <sub>d</sub> = 150
Pneumatic components	Tables B.1 and B.2	EN 983	B <sub>10d</sub> = 20 000 000
Relays and contactor relays with small load (mechanical load)	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B <sub>10d</sub> = 20 000 000

# ISO 13849-1の変更点 — 8

## 附属書D チャネルごとのMTTF<sub>D</sub>を見積るための簡易的な方法

### ■ 表D.1のMTTF<sub>Dj</sub>の修正

第3版

Table D.1 — Example of the parts list of a circuit board

<i>j</i>	Component	Units <i>n<sub>j</sub></i>	MTTF <sub>Dj</sub> typical years	1/MTTF <sub>Dj</sub> typical 1/year	<i>n<sub>j</sub></i> /MTTF <sub>Dj</sub> typical 1/year
1	Transistors, bipolar, low power (see Table C.2)	2	11 416	0,000 087 6	0,000 175 2
2	Resistor, carbon film (see Table C.5)	5	228 311	0,000 004 4	0,000 021 9
3	Capacitor, standard, no power (see Table C.4)	4	114 155	0,000 008 8	0,000 035 0
4	Relay, value given by the manufacturer ( <i>B</i> <sub>10D</sub> = 20 000 000 cycles, <i>n</i> <sub>op</sub> = 633 600 cycles per year)	4	315,7	0,003 167 6	0,012 670 3
5	Contactors, value given by the manufacturer ( <i>B</i> <sub>10D</sub> = 2 000 000 cycles, <i>n</i> <sub>op</sub> = 633 600 cycles per year)	1	31,6	0,031 645 6	0,031 645 6
$\sum(n_j / \text{MTTF}_{Dj})$					0,044 548 0
MTTF <sub>D</sub> = 1 / $\sum(n_j / \text{MTTF}_{Dj})$ [years]					22,4

第2版

Table D.1 — Example of the parts list of a circuit board

<i>j</i>	Component	Units <i>n<sub>j</sub></i>	MTTF <sub>dj</sub> Worst case years	1/MTTF <sub>dj</sub> Worst case 1/year	<i>n<sub>j</sub></i> /MTTF <sub>dj</sub> Worst case 1/year
1	Transistors, bipolar, low power (see Table C.2)	2	1 142	0,000 876	0,001 752
2	Resistor, carbon film (see Table C.5)	5	22 831	0,000 044	0,000 219
3	Capacitor, standard, no power (see Table C.4)	4	11 416	0,000 088	0,000 350
4	Relay (with small load, see C.2) ( <i>B</i> <sub>10d</sub> = 20 000 000 cycle, <i>n</i> <sub>op</sub> = 633 600)	4	315,66	0,003 168	0,012 672
5	Contactors (with nominal load, see C.2) ( <i>B</i> <sub>10d</sub> = 2 000 000 cycle, <i>n</i> <sub>op</sub> = 633 600)	1	31,57	0,031 676	0,031 676
$\sum(n_j / \text{MTTF}_{dj})$					0,046 669
MTTF <sub>d</sub> = 1 / $\sum(n_j / \text{MTTF}_{dj})$ [years]					21,43



# ISO 13849-1の変更点 — 9

- 附属書E 機能及びモジュールの診断範囲(DC)の見積り
- 表E.1の修正(出力装置の表より、第5,6行目の削除)
- 表E.1適用のための例を追加

第3版

Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %
Fault detection by the process	0 % to 99 %, depending on the application

第2版

Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 % depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Redundant shut-off path with no monitoring of the actuator	0 %
Redundant shut-off path with monitoring of one of the actuators either by logic or by test equipment	90 %
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application

# ISO 13849-1の変更点 — 10

## 附属書F 共通原因故障 (CCF)の見積り

- 表F.1の修正 (分離/隔離に例の追加)

### 第3版

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	<b>Separation/ Segregation</b>	
	Physical separation between signal paths, for example: <ul style="list-style-type: none"><li>— separation in wiring/piping;</li><li>— detection of short circuits and open circuits in cables by dynamic test;</li><li>— separate shielding for the signal path of each channel;</li><li>— sufficient clearances and creepage distances on printed-circuit boards.</li></ul>	15

### 第2版

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	<b>Separation/ Segregation</b>	
	Physical separation between signal paths: <ul style="list-style-type: none"><li>separation in wiring/piping,</li><li>sufficient clearances and creep age distances on printed-circuit boards.</li></ul>	15

# ISO 13849-1の変更点 — 11

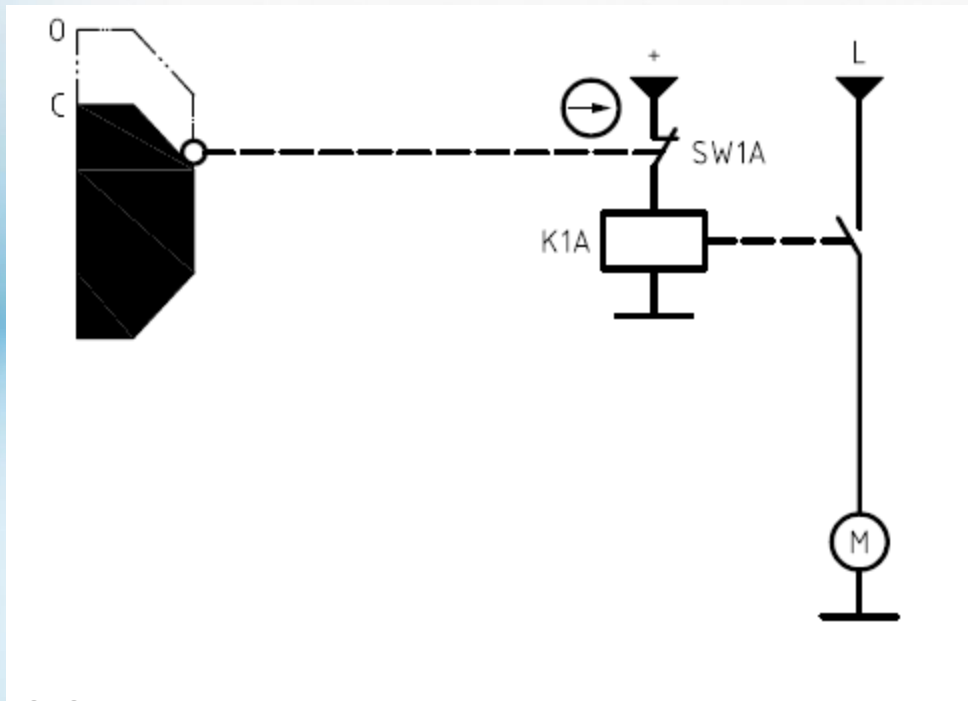
## 附属書G システムティック故障

- G.3 システムティック故障を回避する方策
- NOTE 1の追記(油空圧部品に対する定期試験の必要性)、4番目の'-'の後
- NOTE 2の追記(システムティック故障に関して、IEC 61508-2:2010、Annex Fの紹介)、一番最後

# ISO 13849-1の変更点 — 12

## 附属書I 事例

- 事例1, 2
- 回路条件、 $MTTF_D$ 再計算、DC、CCFの見直し等 (例: スイッチに直接開路動作)



# ISO 13849-1の変更点 — 13

- 附属書K 図5の数値
- 2,500年までのPFH<sub>D</sub>の追加
- NOTE 2にPFH<sub>D</sub>計算時のDCavgを記載
  - *DCavg = low calculated with 60%*
  - *DCavg = medium calculated with 90%*
  - *DCavg = high calculated with 99%*

# まとめ

- 第3版として発行されているが、第2版に追補1の内容を取り込んだもの。
  - 追補1はISO 13849-1を理解しやすくするために、技術的な内容の追加無しに作成、発行されたもの。
- 新たな改定作業が開始された(草案[WD]作成段階)。2017年2月のWGミーティング後にCDの発行予定。

*Thank you very much*



**TÜVRheinland®**

お問い合わせ

224-0021

横浜市都筑区北山田4-25-2

テクノロジーセンター

Phone: 045-470-1850 (代表)

yoshihiro.sugita@tuv.com

www.jpn.tuv.com