ISO 13849-2

機械類の安全性—制御システムの安全関連部

第2部:妥当性確認

2010年12月10日＠東京

テュフラインランドジャパン株式会社

製品部

ビジネスデベロップメント　杉田　吉広

概要

- ISO 13849-2とは？
- ISO 13849-2と各国対応
- ISO 13849-2の構成
- ISO 13849-2の今後

ISO 13849-2とは？

ISO 13849シリーズのひとつ

- 第1部：設計のための一般原則
- 第2部：妥当性確認

ISO 13849-2とは？

- ISO 13849-1に基づいた、制御システムの安全関連部の
  - 安全機能
  - カテゴリ

の分析と試験による妥当性確認の手順と条件を規定

- なぜカテゴリ？
  - 現行のISO 13849-2は旧版のISO13849-1に対応

ISO 13849-2とは？

- ISO 13849シリーズの改定履歴

第1部

- 1999年　第1版発行
- 2006年　第2版発行

第2部

- 2003年　第1版発行
- 2008年　第2版のISO 13849-1に合わせた改定作業の開始

ISO 13849-2の各国対応

- **EU: EN ISO 13849-2:2008**
- **機械指令の整合規格としてリスト化**

ESO (1)	Reference and title of the harmonised standard (and reference document)	First publication OJ	Reference of superseded standard	Date of cessation of presumption of conformity of superseded standard Note 1
CEN	EN ISO 13849-1:2008 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design (ISO 13849-1:2006)	08/09/2009		31/12/2011
	EN ISO 13849-1:2008/AC:2009	08/09/2009		
CEN	EN ISO 13849-2:2008 Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2003)	08/09/2009		

ISO 13849-2の各国対応

- 中国：GB/T 16855.2-2007

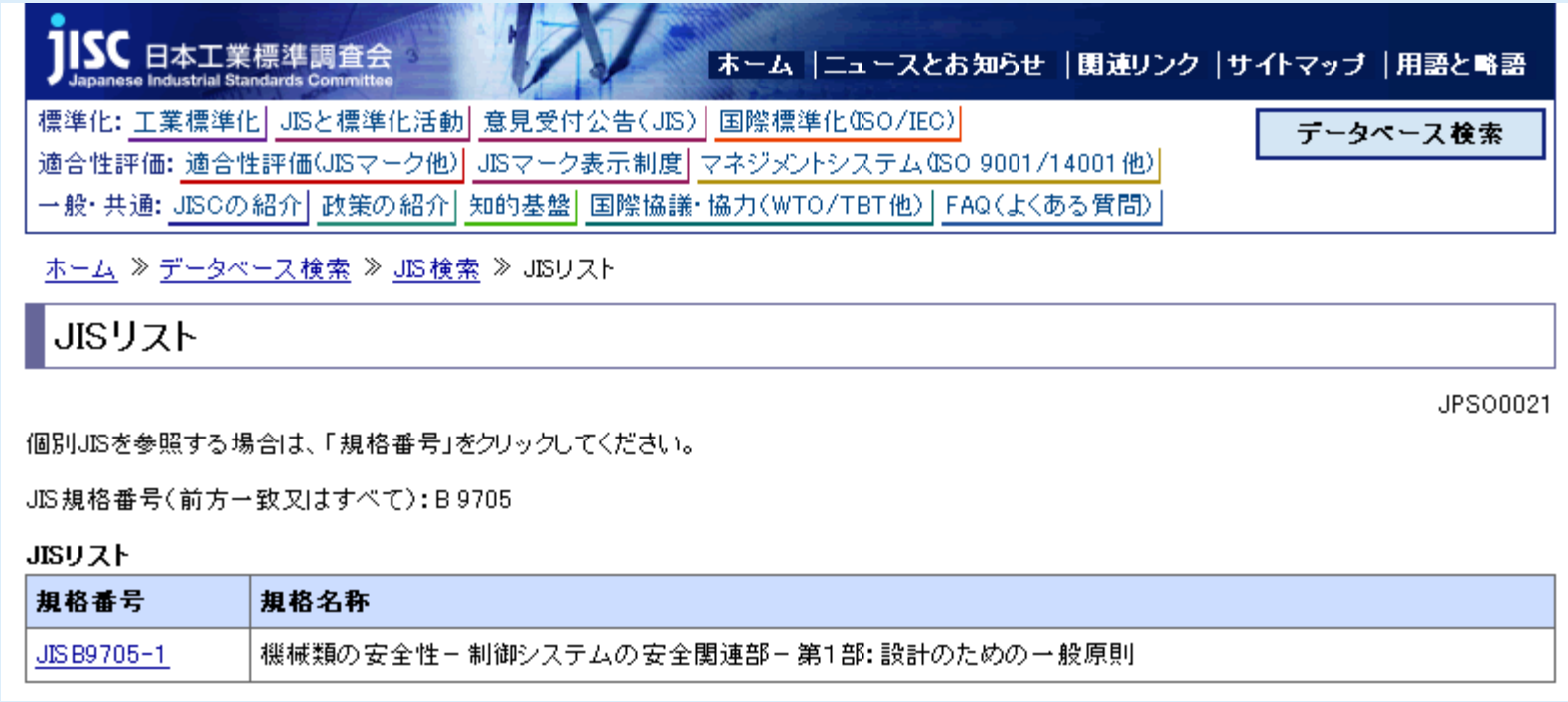
国家标准化管理委员会

国家标准查询
National Standard Query

标准号 Standard No.	GB/T 16855.2-2007				
中文标准名称 Standard Title in Chinese	机械安全 控制系统有关安全部件 第2部分：确认				
英文标准名称 Standard Title in English	Safety of machinery - Safety-related parts of control systems - Part 2: Validation				
发布日期 Issuance Date	2007-03-02	实施日期 Execute Date	2007-09-01	首次发布日期 First Issuance Date	2007-03-02
标准状态 Standard State	现行	复审确认日期 Review Affirmance Date		计划编号 Plan No.	20068087-T-469
代替国标号 Replaced Standard		被代替国标号 Replaced Standard		废止时间 Revocatory Date	
采用国际标准号 Adopted International Standard No.	ISO 13849-2: 2003				
采标名称 Adopted International Standard Name	机械安全 控制系统有关安全部件 第2部分：确认				
采用程度 Application Degree	IDT		采用国际标准 Adopted International Standard	ISO	

ISO 13849-2の各国対応

- 日本： JIS化未実施
- ISO 13849-1：1999はJIS B 9705-1: 2000としてJIS化



JISC 日本工業標準調査会
Japanese Industrial Standards Committee

ホーム | ニュースとお知らせ | 関連リンク | サイトマップ | 用語と略語

標準化: 工業標準化 | JISと標準化活動 | 意見受付公告(JIS) | 国際標準化(ISO/IEC)
適合性評価: 適合性評価(JISマーク他) | JISマーク表示制度 | マネジメントシステム(ISO 9001/14001他)
一般・共通: JISCの紹介 | 政策の紹介 | 知的基盤 | 国際協議・協力(WTO/TBT他) | FAQ(よくある質問)

データベース検索

ホーム ≫ データベース検索 ≫ JIS検索 ≫ JISリスト

JISリスト

JPSO0021

個別JISを参照する場合は、「規格番号」をクリックしてください。

JIS規格番号(前方一致又はすべて): B 9705

JISリスト

規格番号	規格名称
JIS B9705-1	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

ISO 13849-2の構成

1. 適用範囲
2. 引用規格
3. 妥当性確認プロセス
4. 分析による妥当性確認
5. 試験による妥当性確認
6. 安全機能の妥当性確認
7. カテゴリの妥当性確認
8. 環境要求の妥当性確認
9. メインテナンス要求の妥当性確認

付属書A　機械系システムの妥当性確認ツール
付属書B　空圧系システムの妥当性確認ツール
付属書C　液圧系システムの妥当性確認ツール
付属書D　電気系システムの妥当性確認ツール

ISO 13849-2の構成

3. 妥当性確認プロセス

- 安全関連部がISO13849-1の要求に合致していることを実証する
  - 安全関連部が達成しようとする規定された安全機能の特性
  - 規定されたカテゴリ
- 妥当性確認は安全関連部の設計者と独立した人間が行うことが望ましい(should)
- 注記:独立した人間は第三者試験を要求することを意味するものではない

ISO 13849-2の構成

3. 妥当性確認プロセス

- 妥当性確認はプランに沿った分析と試験（必要ならば）からなる。
- 分析はできる限り早く、そして設計と平行して開始するのが望ましい。

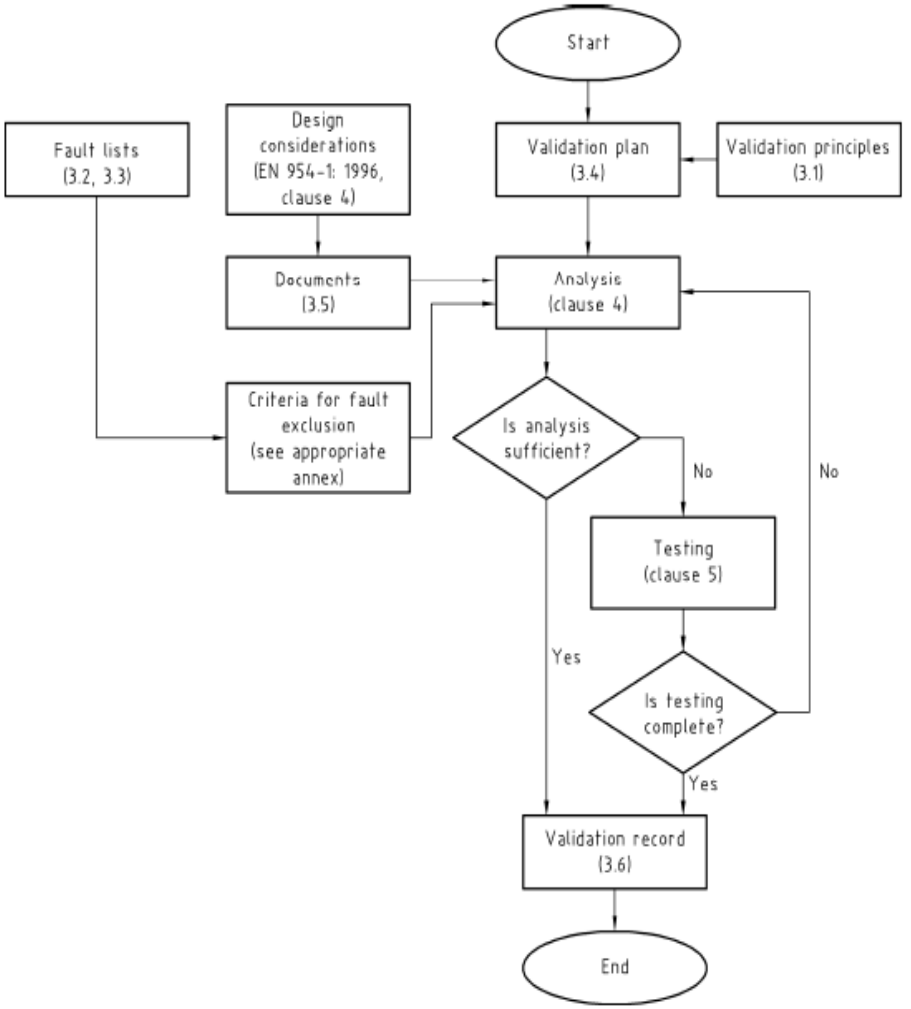


Figure 1 — Overview of the validation process

ISO 13849-2の構成

3. 妥当性確認プロセス

3.4 妥当性確認プラン

安全機能とカテゴリの妥当性確認プロセスを実行するにあたって必要な事項の記載

- 仕様書
- 使用環境条件
- 基本的安全原則
- 十分吟味された安全原則
- 十分吟味された構成部品
- 考慮すべき故障、故障除外
- 適用する分析･試験

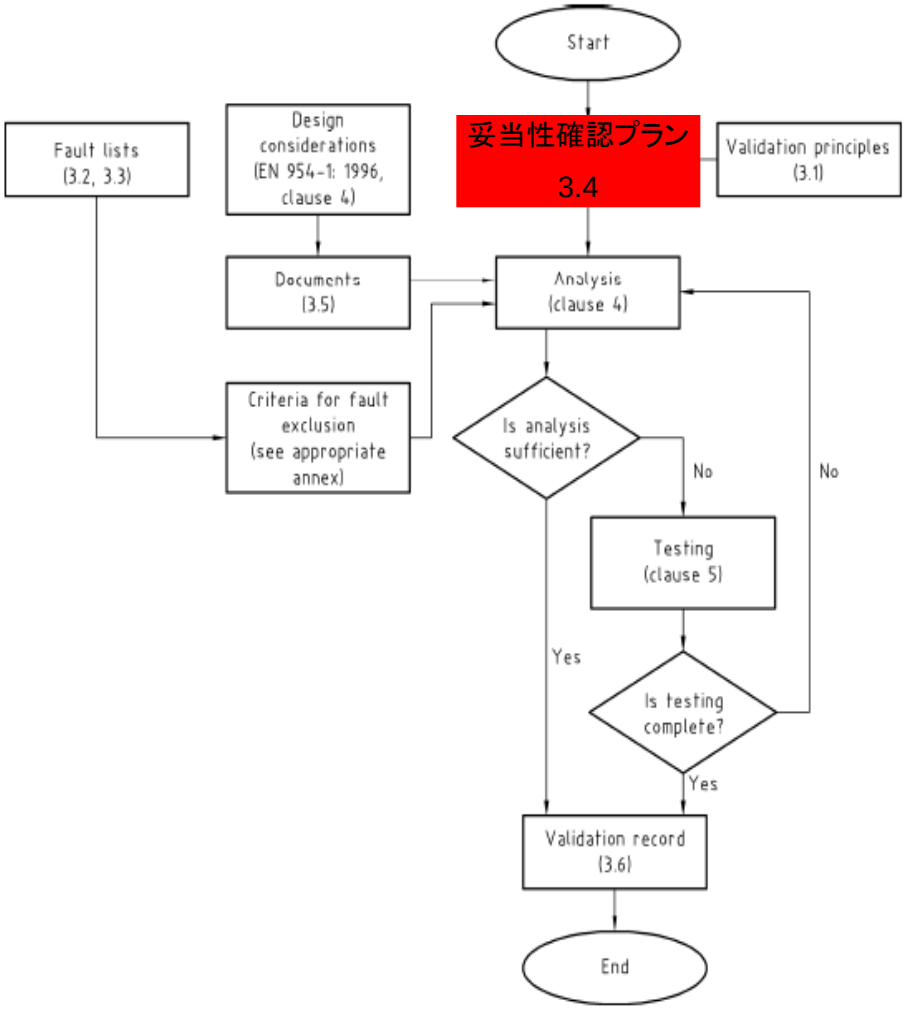


Figure 1 — Overview of the validation process

ISO 13849-2の構成

3. 妥当性確認プロセス

3.2, 3.3　一般及び特定の故障リスト

- 付属書A.5, B.5, C.5及びD.5
- 許容できる故障除外
- 恒久的な故障のみ考慮

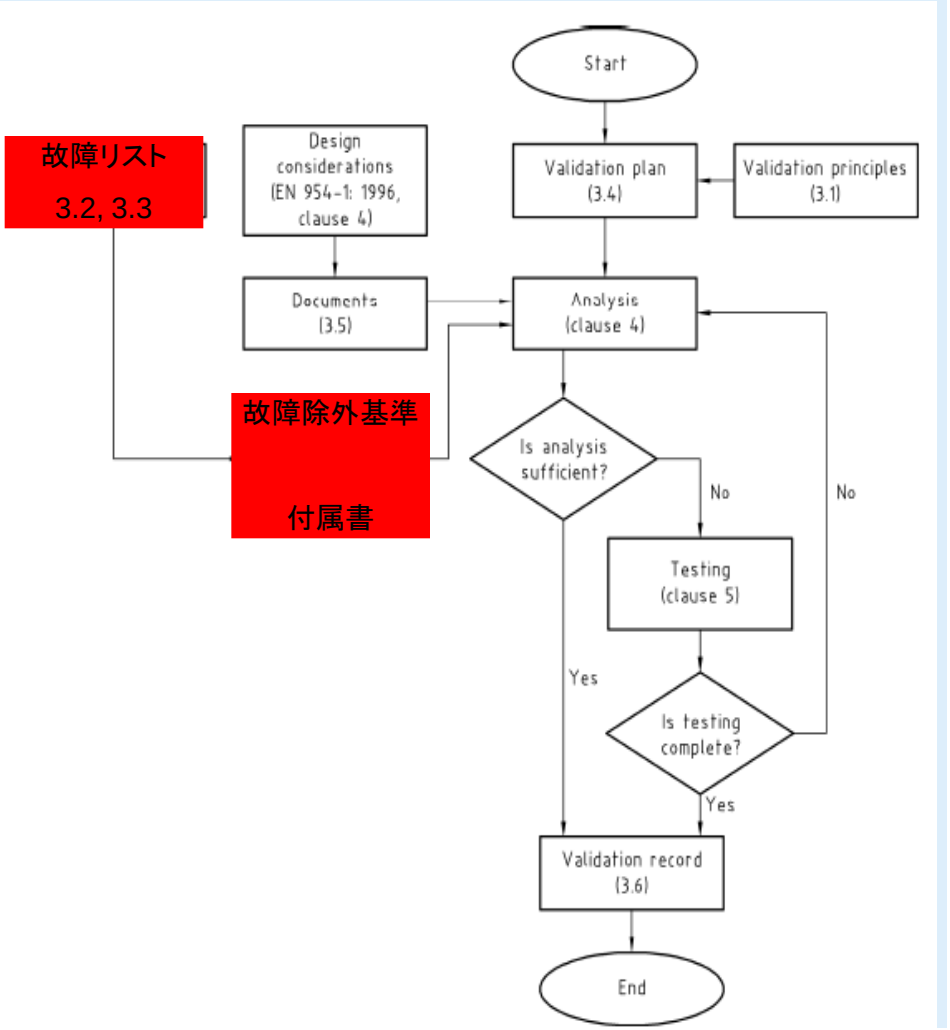


Figure 1 — Overview of the validation process

ISO 13849-2の構成

3. 妥当性確認プロセス

3.5 妥当性確認のための情報

必要な情報は使用する技術カテゴリにより異なる。

- 安全機能・カテゴリの仕様
- 図面類（機械、PCB基板、内部配線等々）
- 回路図（接続部含む）
- 回路の機能の説明
- 安全関連の信号、スイッチング素子のタイミングチャート
- 既に妥当性確認された構成部品の必要情報の記述
- 部品表（定格、故障率等々含む）
- カテゴリに固有の情報は表2
- ソフトウエア関係の情報（ソフトウエアが使用されているならば）

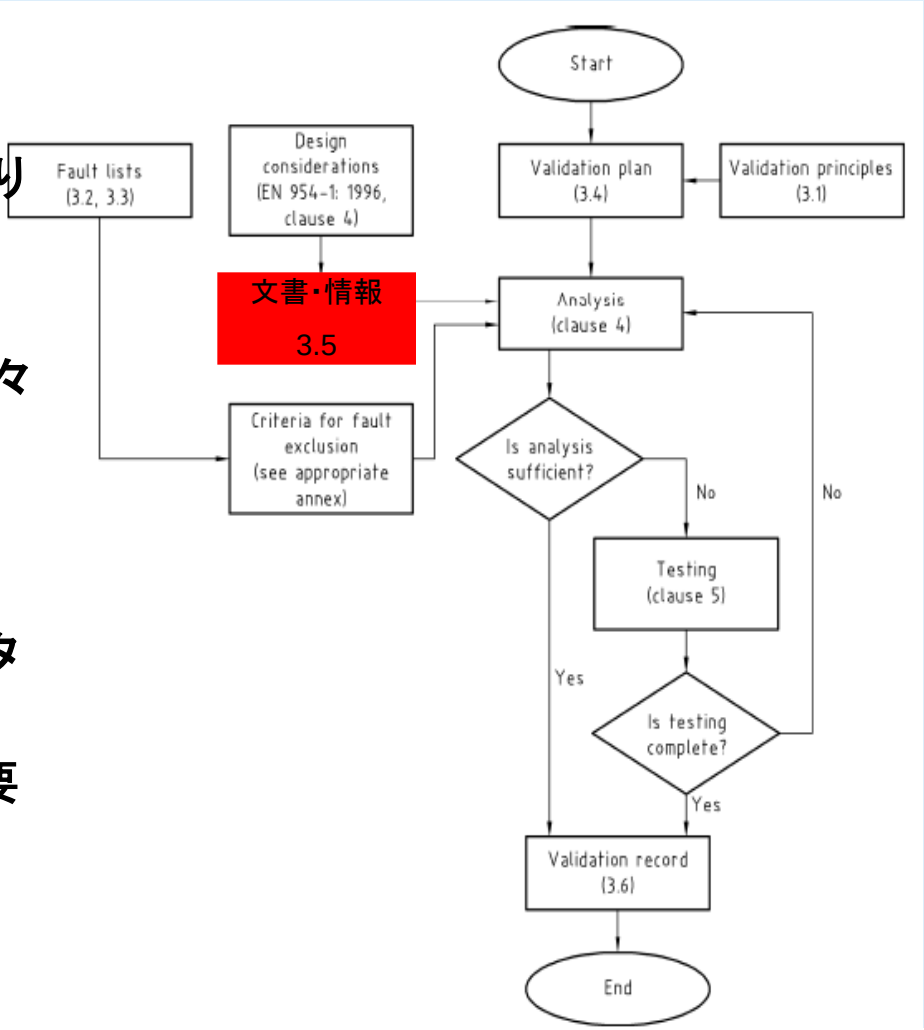


Figure 1 — Overview of the validation process

TUVRheinland®
Precisely Right.

ISO 13849-2の構成

- 表2　カテゴリに対し必要な文書

Documentation requirement	Category for which documentation is required				
	B	1	2	3	4
Basic safety principles	X	X	X	X	X
Expected operating stresses	X	X	X	X	X
Influences of processed material	X	X	X	X	X
Performance during other relevant external influences	X	X	X	X	X
Well–tried components	–	X	–	–	–
Well–tried safety principles	–	X	X	X	X
The check procedure of the safety function(s)	–	–	X	–	–
Checking intervals, when specified	–	–	X	–	–
Foreseeable, single faults considered in the design and the detection method used	–	–	x	X	X
The common mode failures identified and how prevented	–	–	–	X	X
The foreseeable, single faults excluded	–	–	–	X	X
The faults to be detected	–	–	x	X	X
The variety of accumulations of faults considered in the design	–	–	–	–	X
How the safety function is maintained in the case of each of the fault(s)	–	–	–	X	X
How the safety function is maintained for each of the combination(s) of faults	–	–	–	–	X

ISO 13849-2の構成

3. 妥当性確認プロセス

3.6 記録

- 分析･試験による妥当性確認は記録しなければならない。
- 各安全機能に対する妥当性確認プロセスを示さなければならない。
- 不適合部分の記載。

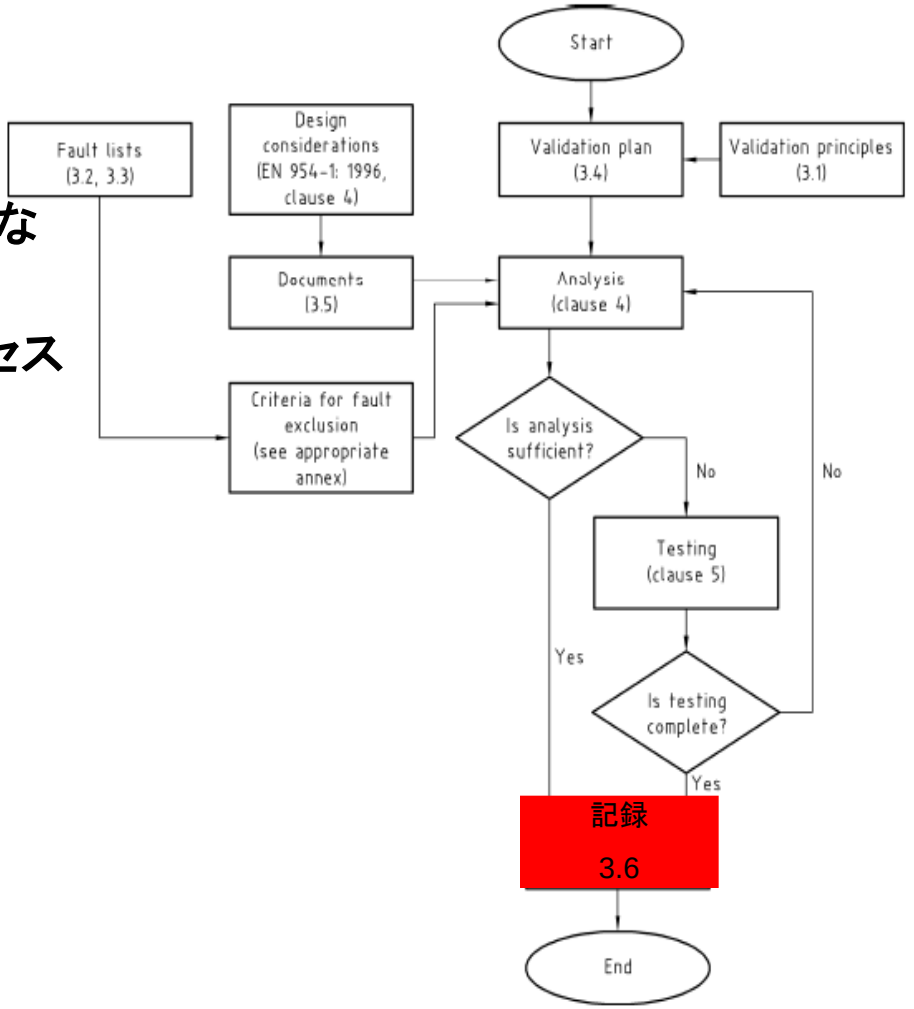


Figure 1 — Overview of the validation process

ISO 13849-2の構成

4. 分析による妥当性確認

- 分析のための情報
  - 機械危険分析中特定された危険源
  - 信頼性(ISO 13849-1, 4.2項)
  - システム構成(ISO13849-1, 4.2項)
  - システムの挙動に影響を与える定量化不可能で、定性的な側面
  - 決定論的根拠 （定性的な状況による、例として製造者の品質、故障率、使用経験など）

ISO 13849-2の構成

4. 分析による妥当性確認

- 分析テクニック
  - トップダウン:FTA　(IEC 61025参照）
    - 危険事象/トップ事象の特定。その事象につながる個々の故障の組み合わせを論理的構成によって示す（JIS B9702: 2000、付属書B.7参照）。
  - ボトムアップ：FMEA　（IEC 60812参照）
    - 構成部品の故障の頻度及び影響を評価（JIS B9702: 2000、付属書B.4参照）。

ISO 13849-2の構成

5. 試験による妥当性確認

分析による妥当性確認が不十分な時、規定した安全機能及びカテゴリの達成度を実証するため実施する。

- 試験は論理的に計画し、実施する
- 試験計画は試験実施前に作成（以下を含む）
  - 試験スペック
  - 期待される試験結果
  - 試験順序
- 試験記録を残す (以下を含む）
  - 試験者の名前
  - 試験環境条件
  - 試験手順と使用機器
  - 試験結果

ISO 13849-2の構成

6. 安全機能の妥当性確認

- 安全関連出力が正しく、かつ仕様に従い論理的に入力によって決定されることを証明
- 妥当性確認はすべての通常及び予見可能な非定常状態をカバーすることが望ましい。
- 規定された安全機能はすべての操作モードで妥当性を確認しなければならない。

ISO 13849-2の構成

7. カテゴリの妥当性確認

- カテゴリの要求項目が満たされているの実証。
- 方法として;
  - 回路図からの分析
  - 実際の回路による試験及び実施の部品の故障シミュレーション
  - 制御システムの挙動のシミュレーション

ISO 13849-2の構成

7. カテゴリの妥当性確認

- カテゴリB
  - 仕様、設計、構造、構成部品の選択がISO 13849-1の要求に従っていることを
    を実証することによって基本的安全原則に従っているか

- カテゴリ1
  - カテゴリBの要求を満たしているか、
  - 十分吟味された構成部品を使用しているか、
  - 十分吟味された安全原則を正しく実施しているか

ISO 13849-2の構成

7. カテゴリの妥当性確認

- カテゴリ2
  - カテゴリBの要求を満たしているか、
  - 十分吟味された構成部品を使用しているか、
  - 十分吟味された安全原則を正しく実施しているか
  - チェック装置はチェックプロセスの間にすべての関連する故障を検出できるか、そして適切な制御動作を起こすことができるか
  - チェックそのものが安全ではない状態に導かないか
  - チェックの開始は以下の場合であるか
    - 機械の起動時及び危険状態が発生する以前、及び
    - 運転中定期的にリスクアセスメント及び運転の性質からチェックを必要とする場合

ISO 13849-2の構成

7. カテゴリの妥当性確認

- カテゴリ3
  - カテゴリBの要求を満たしているか、
  - 十分吟味された構成部品を使用しているか、
  - 単一障害が安全機能の喪失につながっていないか
  - 単一障害（共通モード故障を含む）が論理的設計に従って検出されるか

- カテゴリ4
  - カテゴリBの要求を満たしているか、
  - 十分吟味された構成部品を使用しているか、
  - 単一障害が安全機能の喪失につながっていないか
  - 単一障害は安全機能の次の動作要求時、又はそれ以前に検出されるか
  - この検出が不可能な場合、障害の蓄積が安全機能の喪失につながっていないか

ISO 13849-2の構成

8. 環境要求の妥当性確認

- 制御システムの安全関連部の性能は制御システムの環境条件に対して妥当性を確認しなければならない。
- 妥当性確認は分析及び試験（必要ならば）による。
- 適切であれば、妥当性確認は以下を取り上げる；
  - ショック、振動、不純物の進入に対する予期できる機械的ストレス
  - 機械的耐久性
  - 電気定格及び電力供給
  - 気候条件（温度及び湿度）
  - 電磁両立性（イミュニティ）

ISO 13849-2の構成

9. メインテナンス要求の妥当性確認

- **ISO 13849-1, 9章に記載されたメインテナンスの要求を実施していること。**

9. 保全 安全関連部で指定の性能を維持するために，予防の，又は矯正の保全が通常必要である。指定の性能からの逸脱はやがて安全性の低下を引き起こすか，又は危険状態さえ招くことになる。そのような逸脱した状態を同定するために，手動による定期的検査がしばしば必要になる。

制御システムの安全関連部の保全性の規定は，ISO/DIS 12100-2 の 3.13 に従っていなければならない。保全のためのすべての情報は，ISO/DIS 12100-2 の 5.5.1e)に適合しなければならない。

ISO 13849-2の構成

付属書A　機械系システムの妥当性確認ツール
付属書B　空圧系システムの妥当性確認ツール
付属書C　液圧系システムの妥当性確認ツール
付属書D　電気系システムの妥当性確認ツール

付属書	技術	基本的安全原則	十分吟味された安全原則	十分吟味された構成部品	故障リスト及び故障の除外
A	機械的	A.2.	A.3	A.4	A.5
B	空圧	B.2	B.3	B.4	B.5
C	液圧	C.2	C.3	C.4	C.5
D	電気（電子）	D.2	D.3	D.4	D.5

ISO 13849-2の構成

付属書D　電気系システムの妥当性確認ツール

- 基本的安全原則　表D.1

基本的安全原則	見解
適切な保護ボンディング	制御回路の片側、. . . 保護ボンディング回路に接続する。(IEC 60204-1:1997、9.1.4)
予期せぬ起動の防止	予期せぬ起動の防止、例えば電源復旧後
. . .	. . .

ISO 13849-2の構成

付属書D　電気系システムの妥当性確認ツール

- 十分吟味された安全原則　表D.2

Well–tried safety principles	Remarks
Positive mechanically linked contacts	Use of positively mechanically linked contacts for, e. g. monitoring function [see EN 292–2:1991 (ISO/TR 12100-2:1992), 3.5].
Fault avoidance in cables	To avoid short circuit between two adjacent conductors: — use cable with shield connected to the protective bonding circuit on each separate conductor, or — in flat cables, use of one earthed conductor between each signal conductors.
Separation distance	Use of sufficient distance between position terminals, components and wiring to avoid unintended connections.

ISO 13849-2の構成

付属書D　電気系システムの妥当性確認ツール

- 十分吟味された構成部品　表D.3

Well–tried components	Additional conditions for "well–tried"	Standard or Specification
Switch with positive mode actuation (direct opening action), e. g.: — push–button; — position switch; — cam operated selector switch, e. g. for mode operation	—	EN 60947–5–1:1997 (IEC 60947-5-1:1997), annex K
Emergency stop device	—	EN 418 (ISO 13850)
Fuse	—	EN 60269–1 (IEC 60269-1)
Circuit breaker	—	EN 60947–2 (IEC 60947-2)

ISO 13849-2の構成

付属書D　電気系システムの妥当性確認ツール

- 故障リスト及び故障除外　表D.4 - D21

- D4: コンダクタ/ケーブル
- D5: プリント基板
- D6: ターミナルブロック
- D7: 多ピンコネクタ
- D8: 電気機械式ポジションスイッチ　(プッシュボタンなど)
- D9: 電気機械式デバイス　(リレー、コンタクタなど)
- D10: 近接スイッチ
- D11: ソレノイドバルブ

ISO 13849-2の構成

付属書D　電気系システムの妥当性確認ツール

- 故障リスト及び故障除外　表D.4 - D21

- D12: トランス
- D13: インダクタンス
- D14: 抵抗
- D15: 抵抗ネットワーク
- D16: ポテンショメータ
- D17: キャパシタ
- D18: デスクリート半導体素子
- D19: フォトカプラ
- D20: IC(プログラマブルではない)
- D21: プログラマブル/複雑なIC

ISO 13849-2の構成

付属書D　電気系システムの妥当性確認ツール

- 故障リスト及び故障除外　表D.8

Table D.8 — Electromechanical position switch, manually operated switch

(e. g. push–button, reset actuator, DIP switch, magnetically operated contacts, reed switch, pressure switch, temperature switch)

Fault considered	Fault exclusion	Remarks
Contact will not close	None	—
Contact will not open	Contacts in accordance with EN 60947–5–1:1997 (IEC 60947-5-1:1997), annex K are expected to open.	—
Short–circuit between adjacent contacts insulated from each other	Short–circuit can be excluded for switches in accordance with EN 60947–5–1 (IEC 60947-5-1) (see remark 1)).	1) Conductive parts which become loose should not be able to bridge the insulation between contacts.
Simultaneous short–circuit between three terminals of change–over contacts	Simultaneous short–circuit can be excluded for switches in accordance with EN 60947–5–1 (IEC 60947-5-1) (see remark 1)).	
NOTE The fault lists for the mechanical aspects are considered in annex A.		

ISO 13849-2の今後

ISO/TC199/WG8により現在改定作業中

- 改定作業WG
- 第1回　2008年7月22-24日
  - WDの審議
- 第2回　2009年5月26-28日
- 第3回　2009年10月19-20日
- 第4回　2010年1月28-29日
  - CDの草案作成
  - 3月　CDの発行
- 第5回　2010年11月22-24日
  - CDに対するコメントの審議
  - 300以上のコメント
- 第6回　2011年1月11-13日(予定)
  - CDに対するコメントの継続審議

ISO 13849-2の今後

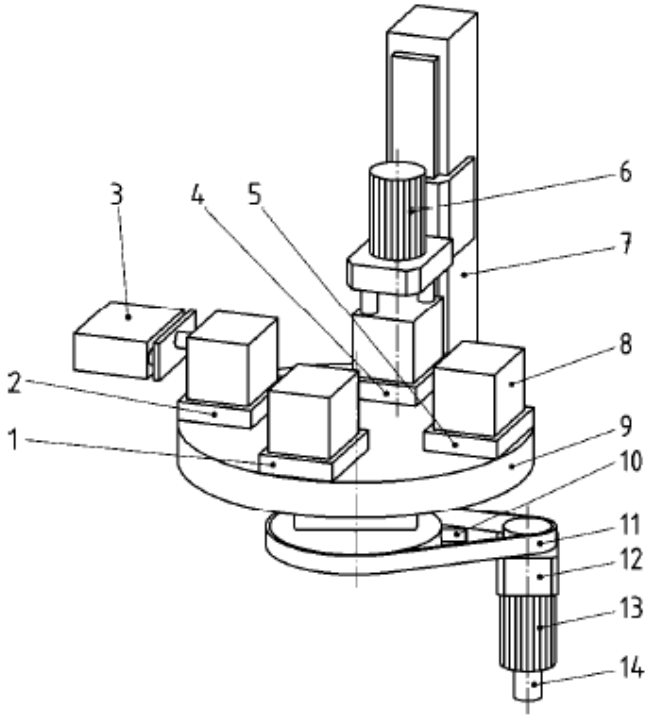
ISO 13849-2改定のポイント

- 3章を‘定義‘の章として追加。
  - 但し新規に定義した用語は無い。すべてパート1と同じ
- ISO 13849-1:2006との整合
- 妥当性確認項目の追加
  - 安全要求仕様: 7章
  - PL（パフォーマンスレベル）
    - 分析・試験：9.1章
    - 妥当性確認：9.6章
  - MTTFd、DCavg及びCCF：9.3章
  - システマティック故障：9.4章
  - 安全関連ソフトウエア：9.5章
  - 技術文書及び使用上の情報：12章

ISO 13849-2の今後

ISO 13849-2改定のポイント

- **妥当性確認例の追加**
- **空圧シリンダーを使用した機械の妥当性確認**



Key

1	loading station	8	workpiece
2	ball insertion workstation	9	rotary table
3	ball insertion cylinder (A1)	10	pulse sensor
4	screwdriving workstation	11	drive belt
5	unloading station	12	planetary gear
6	screwdriver unit (A3)	13	electric motor
7	screwdriving cylinder (A2)	14	rotation sensor

Figure E.1 — Example - automatic assembly machine

ISO 13849-2の今後

空圧シリンダーを使用した機械の妥当性確認例

- 機械の説明
- 安全機能要求仕様
  - SF1：安全関連停止　(インターロックガード)
    - SF1.1　ロータリーテーブル
    - SF1.2　ボール挿入シリンダー
    - SF1.3　ドライバーユニット
    - SF1.4　ドライバーシリンダー
  - SF2:安全制限速度
  - SF3:ホールド･トゥー･ラン　モード
- 制御システムの安全関連部の設計
  - 様々な安全機能のPLrを達成するため、カテゴリ3の選択

ISO 13849-2の今後

- 妥当性確認
  - 確認ステップ
    - 診断手段試験ユニットの特定（構成部品、ブロック）
    - 各診断回路のDC値の検証
    - システムの故障挙動の分析及び試験ケースの決定
    - 各安全関連部のDC_{AVG}の計算のチェック
    - DC値を確認するための試験の実施

ISO 13849-2の今後

- 表E.2　FMEAの例

SF 1.1: Stop function of the rotary table initiated by opening an interlocking guard and the prevention of unexpected start-up

Table E.2 — FMEA of the stop function and the prevention of unexpected start-up of the rotary table

	Systems / Characteristics	Potential faults	Fault detection	Effect / reaction	Test measure
F1	Failure of interlocking switch B1	Short-circuit; mechanical failure; electrical failure; earth fault	Is recognized by no signal change when safety function demanded (opening of the interlocking guard). Monitoring of plausibility is realized in both evaluation systems. DC = 99 %	Stop with detection; re-start prevented	A static signal at the input of both PLCs has to be applied.
F2	Failure of interlocking switch B2	Short-circuit; mechanical failure; electrical failure; earth fault	Is recognized by no signal change when safety function demanded (opening of the interlocking guard). Monitoring of plausibility is realized in both evaluation systems. DC = 99 %	Stop with detection; re-start prevented	A static signal at the input of both PLCs has to be applied.

ISO 13849-2
機械類の安全性—制御システムの安全関連部　第2部：妥当性確認

ご清聴ありがとうございました。

ご質問・お問い合わせは最寄の弊社オフィスまでご連絡ください。

新横浜本社
222-0033
横浜市港北区新横浜3-19-5 新横浜第二ｾﾝﾀｰﾋﾞﾙ
045-470-1850 (TEL)
045-473-5221 (FAX)

テクノロジーセンター
224-0021
横浜市都筑区北山田4-25-2
045-914-3888 (TEL)
045-914-3377 (FAX)

西日本地域担当オフィス
530-0044
大阪市北区東天満2-9-1 若杉ｾﾝﾀｰﾋﾞﾙ本館16F
06-6355-5777 (TEL)
06-6354-8636 (FAX)

九州オフィス
814-0001
福岡市早良区百道浜2-1-22 福岡SRPｾﾝﾀｰﾋﾞﾙ10F 1001号
092-845-5431 (TEL)
092-845-5310 (FAX)