# 6 安全な制御システムの設計

## 6.1 序

詳細な安全機能及び要求されるリスク低減が $PL_r$ という形で決定されたら、次に安全機能を実行する制御システム安全関連部（SRP/CS）の具体的設計に着手する。図 6.1 は、ISO 13849-1 の反復的設計プロセスから本章に関連する部分を抜粋したものである。

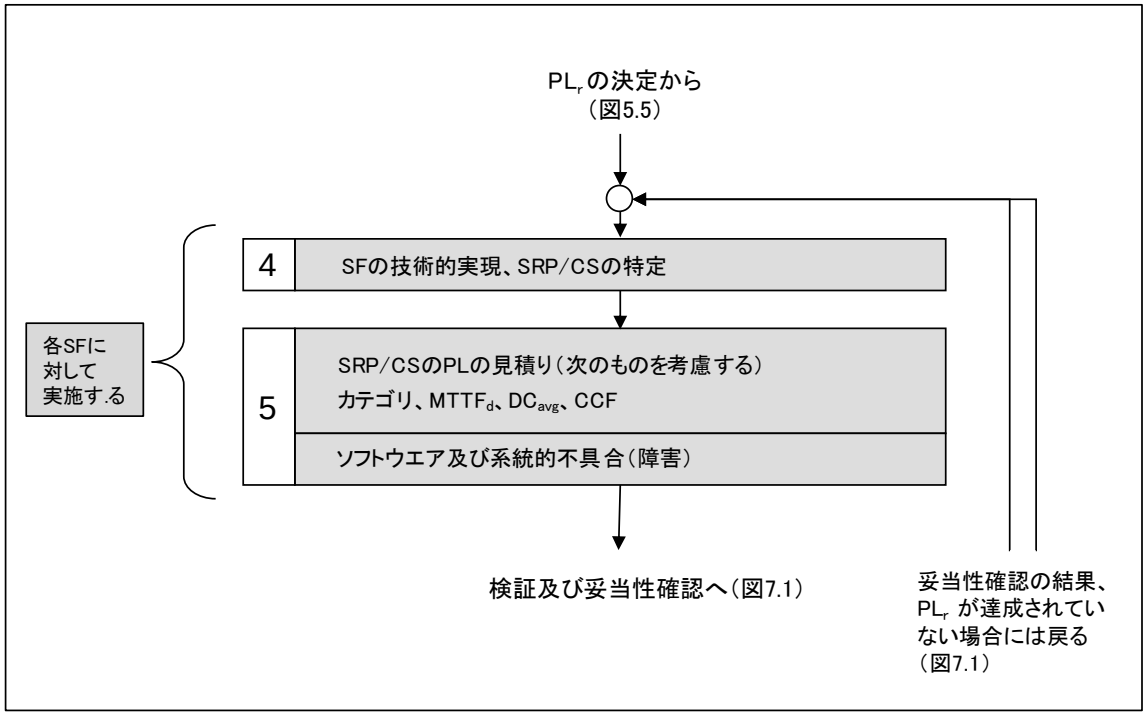


図6.1: SRP/CSの技術的実現ステップで達成されるPLの見積り
図4.1の反復的プロセスからの抜粋

SRP/CS の安全技術の品質は、5 段階に分類されるパフォーマンスレベル（PL）で表わされる。各 PL には、それぞれ該当する単位時間当たりの危険側故障率（PFH: Probability of a Dangerous Failure per Hour）の範囲が割り当てられる（表 6.1）。この単位時間当たり危険側故障率以外にも、適切な PL を達成するためには、さらにソフトウェアのロバスト性の強化や系統的故障対策等の方策が必要になってくる。

故障確率を証明する方法（例：マルコフ型評価、ペトリネット手法）については特に規定されてはいないが、いずれの場合も、次の基準を考慮しなければならない。

- 定量的な側面（構造、コンポーネントの信頼性、自己診断機能、共通原因故障）
- 定量化できない、SRP/CS の挙動に影響を及ぼす定性的な側面（不具合（障害）発生時の安全機能の挙動、安全関連ソフトウェア、系統的故障及び環境条件）

表 6.1:
パフォーマンスレベルと故障率

| パフォーマンス<br>レベル<br>(PL) | 単位時間当たりの<br>危険側故障率（PFH）<br>1/h |
|---|---|
| a | $10^{-5}$≦から＜$10^{-4}$ |
| b | 3 x $10^{-6}$≦から＜$10^{-5}$ |
| c | $10^{-6}$≦から＜3 x $10^{-6}$ |
| d | $10^{-7}$≦から $10^{-6}$ |
| e | $10^{-8}$≦から $10^{-7}$ |

構築された PL をこの 2 つの側面から科学的に適切に評価できるようにするため、ISO 13849-1 では実用的手法が提案されている。各側面に関する調査は、それぞれ必要に応じてある程度大まかに、あるいは細かくなっても構わず、これにより迅速に見積もることも、また綿密に証明することも可能である。

まず本章 6.1.1 の開発手順で、SRP/CS のライフサイクルで要求される仕様書及び文書化等について説明する。続いて、系統的故障の抑制に必要な方策（6.1.2）、設計における人間工学的視点（6.1.3）について述べる。6.2 では、カテゴリと、これをベースにした定量的側面を評価するための簡易的手法について説明し、6.3 では、ソフトウェアに関する要求事項を取り上げる。さらに 6.4 で、SRP/CS の組み合わせにおいて注意すべき定量的側面について述べる。図 6.2 は、本節の必要性を示したものである。

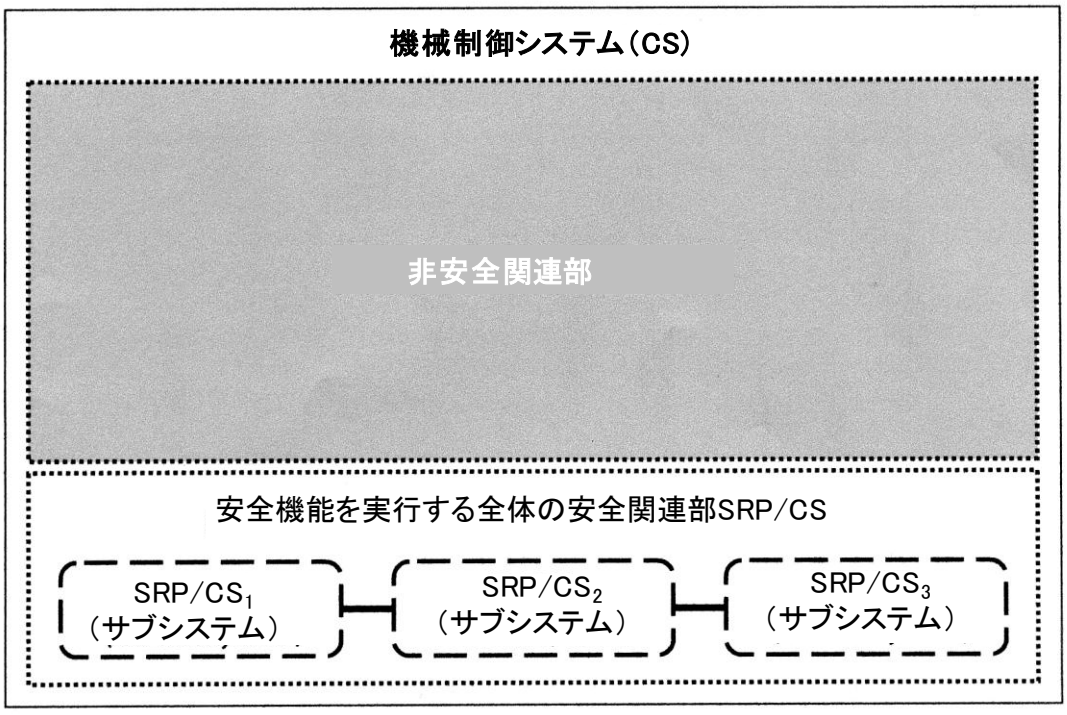


図6.2: 機械制御システム内のSRP/CS及びサブシステム

機械全体の制御システム CS（Control System）は、安全関連部（SRP/CS）と、通常の運転機能にのみ関与する非安全関連部に分けられる。一般的には、非安全関連部の占める範囲の方が大きくなることは明らかである。制御システムの安全関連部の組み合わせは、安全関連の信号が発生する場所（ポジションスイッチのアクチュエータ等を含む）で始まり、パワー制御要素の出力側（電磁接触器の主接点等を含む）で終わる。エネルギーがない状態では危険状態が発生しない（ノーマルクローズ原理）場合には、モータやシリンダ等の動力要素は SRP/CS には該当しない。しかし、もし外力が（例えば垂直軸に）作用する場合には、この動力要素は SRP/CS として考察する必要がある。本章最後の 6.5 では、すでに 5.7 で取り上げた断裁機の制御システムを例に、実際の適用について解説する。

### 6.1.1 開発手順

制御システムの安全関連部の構築及び統合（規格の適用範囲）における各々のアクティビティは、できるだけ不具合のない、要件に合致した製品を開発し、これを意図したとおりに使用してもらうことを目的としたものでなければならない。最終的な目標は、人の健康と災害の回避にある。開発プロセスにおける**構造化と適切な文書化**は、このために掲げられるモットーである。

ISO 12100-1 によるリスク低減のプロセスは、図 6.3 に示すように、機械の全ライフサイクルを網羅するものでなければならない。規格では明言されてはいないものの、単独または複数の SRP/CS の構築及び統合についても、そのアクティビティを適切に構造化するに当たってはライフサイクルの考え方が採用される。本規格の制御システムの安全関連部設計のための反復的プロセスにおいて、個々のフェーズに細分化されるプロセスが重要な意味をもつことは、第 4 章の規格の説明からも明らかであろう。妥当性確認のフェーズでは、図 6.3 からも見てとれるように、独自の構造化された手順が示される。これについては第 7 章で詳しく説明する。ライフサイクルフェーズへの構造化は、安全関連ソフトウェアの作成で使用される V-モデルにより、その特徴が示される。これについては本章 6.3 で取り上げる。また、保全フェーズは SRP/CS の設計プロセスには明記されていないが、「使用上の情報」で要求される項目に含まれる。

SRP/CS は機械の一部であるため、機械のライフサイクルの各フェーズに関する要求事項はほとんどすべて、SPR/CS にも影響を及ぼすといってよい。このため、安全機能の特定及び要求特性の指定においては、機械のライフサイクルの全フェーズを考慮しなければならない。このプロセスをできるだけ包括的かつ検証可能なものとして具体化するために、まずそれぞれの安全機能を明確にする。特に、機械の制御システムのために特別に開発されたものではない SRP/CS、例えばライトグリットや安全 PLC 等については、適正な使用であることを保証するために、その特性値及びインターフェースを正確に記述する必要がある。

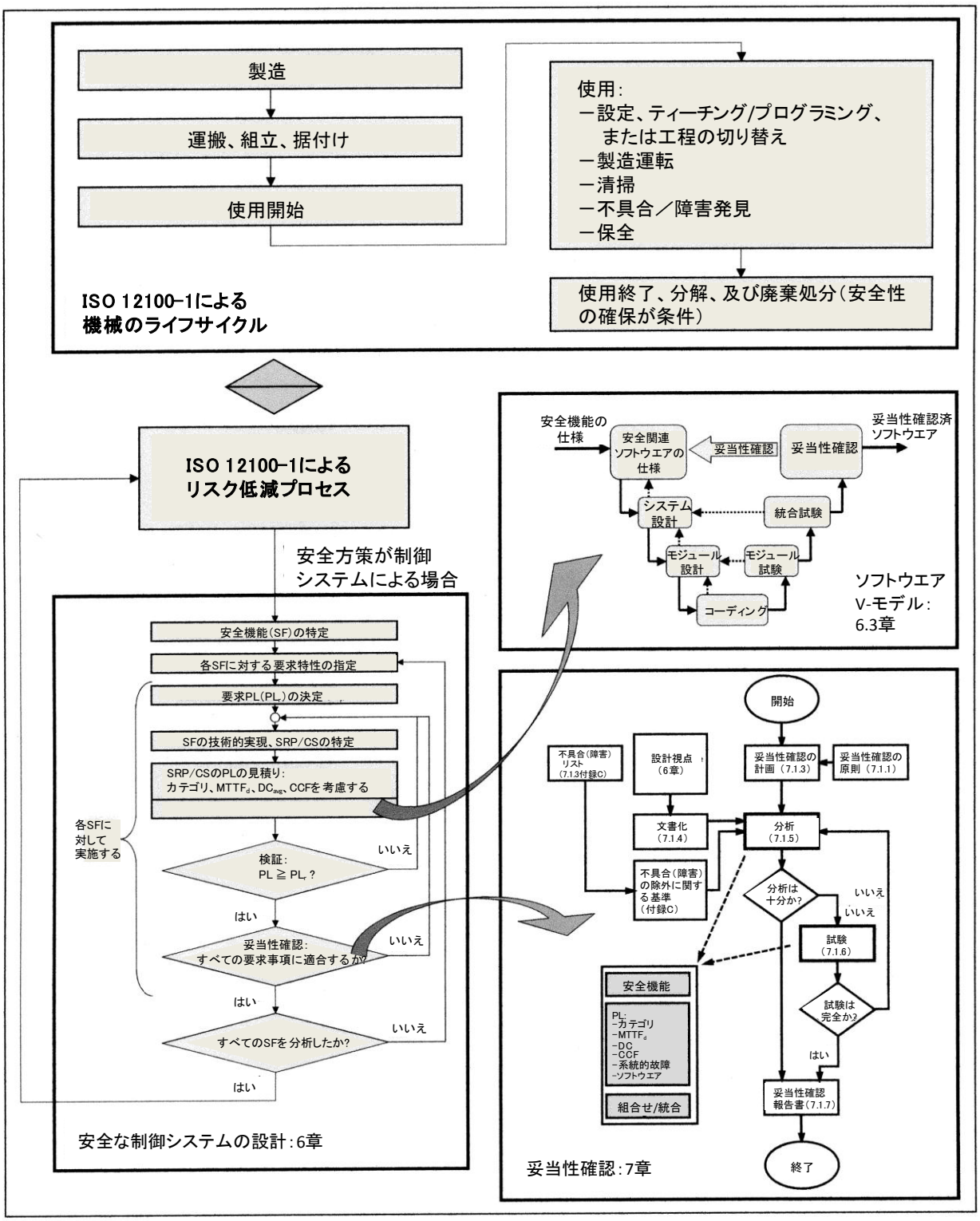


図6.3: 機械及びSRP/CS のライフサイクル

安全機能の仕様書により、SPR/CS のライフサイクルがスタートする。ISO 13849-1 では、各種安全機能の個別事項だけでなく、本仕様書に最低限含むべき一般的事項についてもリスト化している。

この仕様書により、開発プロセス開始時の関係者すべてに適用される基本条件が決定される。いわゆる要求仕様書であり、開発後に作成される製品記述書を意味するものではない。1 つの安全機能は SRP/CS により技術的に実現される。この SRP/CS は機械制御システムの構成部であり、さらに別の SRP/CS 及び機能制御システムに対するインターフェースが装備される。このため、仕様書の作成が不可欠である。ボックス 6.1 に、安全要求事項仕様書の一般的構成を示す。ここには安全機能の仕様も含まれる。この構成例は安全機能全体を実行する SRP/CS に関するものであるが、サブシステムとしての SPR/CS にも適用される。

ボックス 6.1:
安全要求事項仕様書の一般的構成

**1 製品及びプロジェクトに関する一般的記載**

1.1 製品の同定
1.2 作成者、バージョン、日付、文書名称、ファイル名称
1.3 目次
1.4 用語、定義、関連語彙
1.5 バージョン履歴及び変更の注記
1.6 開発に関連する重要な指令、規格及び技術規則

**2 機械の機能に関する記載（安全技術上重要なもの）**

2.1 意図する使用及び合理的に予見可能な誤使用／誤操作
2.2 プロセス記述（運転機能）
2.3 運転モード（セットアップ、自動運転、機械の局所的あるいは部分的な運転）
2.4 特性値　例：サイクル時間、応答時間、オーバーラン距離
2.5 その他の機械特性
2.7 プロセス間の相互作用（2.2 参照）及び手による作業（修理、調整、清掃、不具合発見等）
2.8 緊急時の操作

**3 要求パフォーマンスレベル（$PL_r$）**

3.1 機械の危険源分析及びリスクアセスメントのための既存文書、参考資料
3.2 同定された各危険源もしくは危険状態に関するリスクアセスメントの結果とそれぞれのリスク低減に必要な安全機能の決定

ボックス 6.1:（前ページからの続き）

**4　安全機能（各安全機能に適用される記載）**

- 機能の説明（「検出」－「処理」－「出力」）、すべての機能特性を含む（表 5.1 及び 5.2 を参照）
- 作動／非作動条件もしくは事象（例：機械の運転モード）
- 安全機能作動時の機械の挙動
- 考慮すべき再起動条件
- 性能基準／性能データ
- 応答時間を伴う安全機能のプロセス（時間的挙動）
- 作動頻度（作動要求頻度）、要求後の復帰時間
- その他のデータ
- 調整可能なパラメータ（指定されている場合）
- 複数の安全機能が同時に作動及び要求される場合の優先順位
- 非安全機能及び他の安全機能からの分離、あるいはこれらに対する非依存／非応答に関する機能コンセプト

**5　SRP/CS のレイアウト設計に関する要件**

5.1　安全機能を実現する SRP/CS 及び技術方式の指定、予定される装置／設備

5.2　カテゴリの選択、安全関連ブロックダイアグラムで示される指定のアーキテクチャ（構造）

5.3　インターフェースの記述（プロセスインターフェース、内部インターフェース、操作及び表示機器等）

5.4　作動時の挙動、起動及び再起動時に必要とされる挙動

5.5　性能データ：サイクルタイム、応答時間等

5.6　コンポーネントの故障及び不具合（障害）における時間挙動を含む SRP/CS の挙動（安全状態の達成と維持）

5.7　コンポーネント、モジュールあるいはブロックの考慮すべき故障率と、該当する場合には不具合（障害）の除外の理由付け

5.8　偶発的故障及び系統的故障の検出及び抑制を実行するためのコンセプト（自己診断、テスト回路、監視、比較、尤らしさのチェック、プロセス実行中の故障検出等）

5.9　定量的側面

ボックス 6.1:（前ページからの続き）

5.9.1 $MTTF_d$ 及び $DC_{avg}$ の目標値
5.9.2 摩耗するコンポーネントの動作頻度
5.9.3 不具合（障害）を検出する方策の頻度
5.9.4 耐用年数（指定のアーキテクチャの算定ベース（20 年）と異なる場合）
5.10 運転データ及び最大定格（運転温度及び保管温度レンジ、湿度、IP 保護等級、衝撃耐性、振動耐性、EMC-電磁両立性、電源許容誤差等）（IP=International Protection、EMC=Electromagnetic Compatibility）

5.11 設計（設備、感電／人体への危険な電流の作用に対する保護、環境条件に対する耐性等）に適用される基本規格
5.12 安全関連パラメータ及び SRP/CS の機能特性へのアクセス防止（無効化防止、接近防止、プログラム及びデータ保護）及び非定常運転モード等での権限を与えられていない者による操作の防止（キースイッチ、コード化等）に関する技術的及び組織的方策
5.13 一般的な技術条件と、立ち上げ、試験、受け入れ、保守・点検に関する組織的な基本条件

次の開発ステップに進む前に、仕様書の妥当性を確認するための検証が行われる。ここでは、必要事項がすべて記載されているか、正確であるか、理解しやすいものか、矛盾はないか、が重要なポイントになる。言うまでもないが、この検証はプロジェクトの当事者以外の者により実施されるのが望ましい。安全関連ソフトウェアを使用する場合には、この安全要求事項仕様書からさらにソフトウェア独自の仕様書を作成しなければならない（本書 6.3.2 参照）。

安全要求事項仕様書は、SRP/CS の設計プロセスにおける最初のドキュメントである。文書化は、開発を追跡できるものにするという意味で、基本的に非常に重要である。1 つの製品には開発当事者以外の者も後から関わってくることに留意するべきである。SRP/CS の反復的設計プロセスで必要とされる文書化の詳細は 6.3.8 のソフトウェアに関する項及び 7.1.4 等で説明するが、文書というのは一義的に特定できるものでなければならない。従って、いわゆるバージョン管理システムが必須になってくる。また、安全機能が正しく実現されるためには、使用上の情報が特に重要である。ISO 13849-1 では、第 11 章に、この使用上の情報が含むべき最低限の情報がリスト化されている。また、SRP/CS に関する製造業者の社内技術文書の内容については本規格の第 10 章でリスト化されており、さらに立法機関においても文書化に係る要求事項が策定されている。ボックス 6.2（本書 42 ページ参照）に、2009 年 12 月 29 日から施行される新欧州機械指令 2006/42/EC［8］による機械類に関して必要となる技術資料の内容を示す。

ボックス 6.2:
機械に関する技術資料：新機械指令（2006/42/EC）附属書Ⅶ、A からの抜粋

1. 技術資料：
   a) 次の記載及び資料を伴う技術文書
      - 機械の一般的記述
      - 機械の基本設計図、制御回路の接続図並びに機械の動作方式を理解するために必要な記述及び説明
      - 完全な詳細図面。必要に応じて当該機械が安全と健康に関する必須要求事項に合致することを証明するために必要な評価、試験結果及び記述等を付す。
      - リスクアセスメントに関する資料。これにより、どのような方法を用いたかわかるようにする。これには、次のものが含まれる。
        i) 当該機械に適用される安全と健康に関する必須要求事項の一覧
        ii) 同定された危険源の回避もしくはリスク低減のためにとられる保護方策の記述と、該当する場合には機械から生じる残留リスクに関する記載
      - 適用される規格と、それらの規格で扱われる安全と健康に関する必須要求事項の記載に基づくその他の技術仕様
      - 製造者自ら、もしくは製造者又はその代理人が選択した機関により実施された試験の結果を含むすべての技術報告書
      - 機械の取扱説明書の見本
      - 該当する場合には、完成品でない機械に関する組込み宣言書及び組立説明書
      - 該当する場合には、当該機械に組み込まれる他の機械又は製品に関する EC 適合宣言書の写し
      - EC 適合宣言書の写し

   b) ライン生産の場合には、製造されたすべての機械が本指令の規定に合致していることを保証するための社内方策の一覧

### 6.1.2 系統的故障

系統的故障は、コンポーネントの偶発的故障とは異なり、設計や製造プロセス、運用手順、文書化等を変更しない限り、その原因を除去することはできない。系統的故障は、仕様書の作成やレイアウト設計、あるいは SRP/CS の変更等の誤りにより、製品ライフサイクルのどこかある時点で発生する。複数チャンネル構造の技術的実現とコンポーネントの故障確率の考察は、安全設計の重要な要素ではある。しかし、基本的視点が十分に考慮されていなかったならば、故障確率において最高のレベルが達成できたとしても、それは何の意味もなさないだろう。例えば、ある製品が正しく使用されていない、あるいは不適切な環境で利用された場合には、系統的故障が発生する恐れがある。ISO 13849-1 が本規格の第 2 部と共に、PL の達成に関して想定される系統的故障を

考慮することを要求しているのは、こうした事実に鑑みた措置である。基本安全原則及び十分吟味された安全原則の多くは、基本的には、系統的故障に対し効果を発揮するものといえよう（本書付録 C）。本規格の附属書 G により補足されるこの系統的故障については、ISO 13849-2 に従って考慮する必要がある。

ISO 13849-1 の参考情報である附属書 G には、系統的故障に対する方策と、間接的ではあるが考察すべき影響がリスト化されている。方策は、故障を回避するためのもの（G.3 及び G.4）と、故障を抑制するためのもの（G.2）に分類される。図 6.4 に、その概要を示す。故障を回避するための方策は、製品の全ライフサイクルに通用するものでなければならない。このため、本書第 7 章でも、妥当性確認の視点からこれについて言及している。明記されているわけではないが、変更、不具合（障害）の除去、保全には、特に注意が必要である。これらのフェーズになると、開発時の詳細情報の存在は薄れがちである。このため、故障を抑制するための方策を製品に取り入れて、使用中にその効果が発揮されなければならない。本規格には、基本的要求事項以外にも選択肢となる方策がリストアップされており、SRP/CS の複雑性及び PL を考慮して、その中の 1 つあるいは複数の方策を使用することが求められる（図 6.4 では「付加的」と表わされている）。

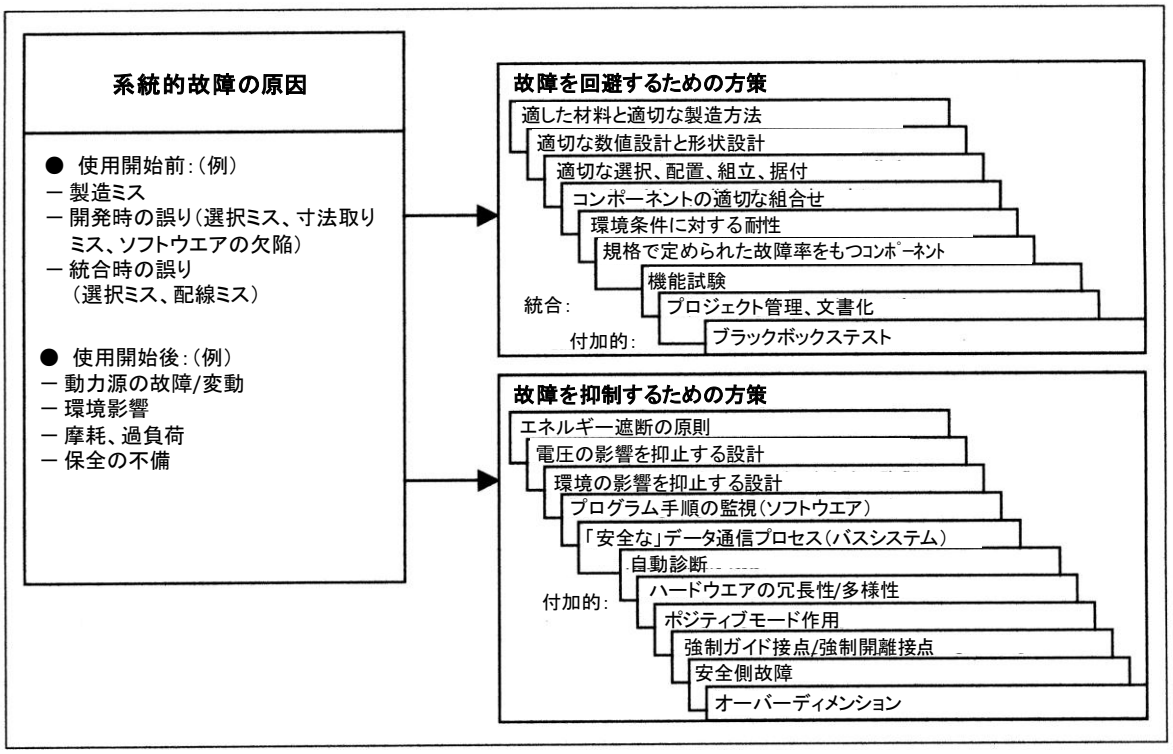


図6.4: 規格附属書Gによる系統的故障に対する方策

これらの方策に関する規格の説明は、かなり簡略化されている。まず、ここで補足しておきたいのは、図 6.4 では、多様性（ダイバーシティ）はハードウェアを対象としたものとなってるが、これは BGIA の経験からしても、実際には広範囲で使用されるものだということである。これについては、本書 6.3.10 のソフトウェアに関する要求事項も参照いただきたい。

本レポートを丹念に読み進めると、共通原因故障（CCF、本書 6.2.15 参照）に対する方策との違いはどこにあるのかという疑問を持たれることだろう。共通原因故障はもちろん、系統的故障としても見なすことができる。しかしながら、CCF の考察は、複数のチャンネル、あるいは少なくとも試験機器を有する構造（カテゴリ 2、3、4）のみが対象となる。さらに、CCF の側面は「努めて」定量的に考察されるが、本規格の附属書 G による考察は純粋に定性的なものであるという点でも異なる。附属書 G の系統的故障に対する適切な方策と基本安全原則及び十分吟味された安全原則に留意すれば、共通原因故障（CCF）対策の要求事項を実行することは特に難しいことではないはずである。

具体的な要求事項は、用途及び技術方式特有のものもあるため、場合により一般要求事項の解釈が必要になる。これについては以下に例を挙げて説明する。

*例 1：動力源の故障の影響を抑制するための方策*

制御システムの安全関連部を設計するに当たっては、動力源（電圧、空圧、油圧）の故障も考慮しなければならない（本書 5.2.8 及び規格の附属書 G 参照）。電圧降下、電圧変動、過電圧及び不足電圧は、機械の安全な状態を脅かしかねない。これは、特に電気駆動及び油圧駆動（垂直軸駆動）による荷の吊り上げについていえる。この種の故障が SRP/CS 内のコンポーネントの不具合が原因で発生しえる場合は、パフォーマンスレベルに対するその影響が検証において考慮される。しかしながら、原因が動力供給装置にある場合、あるいは機械の断路器（メインスイッチ）が作動してしまう場合には、これらの事象は定量的分析の範囲外に置かれ、系統的故障としてのみ考察される。中には単なる運転状態としてしか見なされないものある。これらについては SRP/CS による抑制が必要であり、これにより安全な状態を達成し、かつ／又は維持しなければならない。例えば、動力源の故障がまれにしか起こらないからといって、要求事項をより低い $PL_r$ に引き下げることは許されない。リスクアセスメントに関わる重要なパラメータ S、F、P は、動力源の故障を考慮することで変更されるものではないからである。

*例 2：空圧弁及び油圧弁の故障*

ISO 13849-2 の表 B.1「空圧システムの基本安全原則」及び表 B.2「空圧システムの十分吟味された安全原則」では、空圧コンポーネントの設計及び製造における留意点として*「適切な材料と製造方法」*と*「圧縮空気の汚染の適切な防止」が挙げられている*。ここでは特に応力、耐久性、摩擦、摩耗、腐食等を考慮した材料、製造及び処理方法の選択と、圧縮空気の高精度濾過／固液分離に考慮することが要求される。さらに、表 C.1「油圧システムの基本安全原則」では、「適切な数値設計と形状設計」も油圧コンポーネント設計の留意点として挙げられている。ここでは、特に応力、引張ひずみ、疲労、表面粗さ、各種耐性及び製造方法に対する考慮が求められる。

しかしながら、こうした流体システムの構成要素がたまにしか作動しないものである場合には、さらに構造上の特徴（弁体と弁箱のすきま）により付着力が高まる恐れがある。

- 空圧弁にソフトシールが使用されている場合、長期間切り替えが行われずに同じ位置にあると、ソフトシールが潤滑剤（コンプレッサー、給油機器、あるいは初期潤滑により送り込まれる圧縮空気内の合成オイル）の化学的作用によりふやけてしまったり、あるいは潤滑膜がシールエッジの圧力によりつぶされて、これにより付着力が高まる可能性がある。

- 油圧弁については、長期間切り替えが行われずに同じ位置にあると、いわゆるシルティングが発生する可能性がある。そうなると、次に作動するまでの間にシールのすきまに細かい汚染粒子が沈積して、これが原因で弁体が動かなくなる恐れがある。

  このような理由から、一般的に、弁体が「安全な切り替え位置」に復帰するための大きな力の蓄え（例えばばね力）が構造上必要とされる。非機械式ばねの場合には、適切な方策をとることで、復帰機能が確実に保持されるようにする。さらに、切り替えサイクル及び試験サイクルを、例えば 8 時間を限度とした適切な周期で行うことにより、上述の影響を阻止することが重要である。

*例 3：安全機能と他の機能の分離*

機能安全規格に共通するテーマとして、安全機能と他の機能（非安全機能）の分離が挙げられる。ISO 13849-2 においても同様に、「不具合（障害）の可能性の低減」をキーワードに、電気設備に関する十分吟味された安全原則等が示されている。この要求事項は、ハードウェアだけでなくソフトウェアにも適用される。しかしながら、いくつかの理由から完全な分離が有効的とはいえない場合もある。このようなケースでは、機能的及び技術的に明確に定義されたインターフェースにより安全関連部に対する影響を回避あるいは抑制することが、最低限必要になる。

これについては、アプリケーションソフトウェアの作成を例に挙げると理解しやすいだろう。標準のアプリケーションソフトウェアと安全関連ソフトウェア（SRASW、本書 6.3 参照）を分離する最良の方法は、これらを別のプログラミングシステム（いわゆるエンジニアリングスイート）で作成し、かつ別の PLC（プログラマブルロジックコントローラ）で実行させることであるのは言うまでもない。しかしながら、とりわけ経済的理由から、全アプリケーションソフトウェアを 1 つのプログラミングシステムを使って、またできれば共通のエンジニアリングプロセスで作成したいケースもある。この場合には、当然ながらさまざまな側面を考慮しなければならない。例えば、安全関連系の変数、結果あるいはアウトプットがソフトウェアの非安全関連部（プログラム、ファンクションブロック、機能／命令等）により上書きされてはならないということが要求される。両者の環境がリンクすることは許されるが、ただし、これは取り決めが守られている場合に限られる。安全関連信号及び機能は常に優先されなければならず、従って、例えば「OR」演算によるリンクはいかなる場合にも許可されない。近頃ではソフトウェア開発ツールによりこのようなアプローチはサポートされており、（エディターとコンパイラで）設定された機能と自動チェッ

クルールが実行される。このようにして、予期しない操作状況でしか効果が現れない、あるいは受け入れ／立ち上げ時にある程度の労力を費やしても検出できないような論理演算上のエラーは阻止することができ、非常にユーザフレンドリーなものといえる。

制御システムの標準機能部品が安全関連部に及ぼす影響、またついでながら言うと安全機能の相互間の影響についても同様であるが、設計者はこれらの分析を完璧に行わなくてはならない。しかし、前述の開発ツールを使用することで、どこで（表面上）、どのような（機能上）影響が生じえるか解析することは、はるかに容易かつ迅速に実施できるようになった。「確認された影響をどのように除去（回避あるいは抑止）するべきか？」というさらに重要な問題にまでは、場合にもよるが、あえて立ち入る必要はない。

### 6.1.3 人間工学

欧州機械指令 98/37/EC の附属書 I、1.1.2d により、機械製造者には、機械オペレータが被る不便、疲労、精神的負荷を、人間工学原則に基づいて機械設計の段階ですでに最小レベルにまで軽減することが要求される。このことは機械／機械設備のオペレータと SRP/CS 間のインターフェースについても適用される。ここで言うインターフェースには、ポジションスイッチ付保護扉等の具体的な安全防護物だけでなく、安全機能の操作に使用される押ボタンスイッチ、さらにはグラフィカルユーザインターフェース等も含まれる。

人間工学原則が SRP/CS にとっていかに重要なものであるか、また SRP/CS の意図しない使用あるいは予見可能な誤使用を機械の設計段階で考慮しなければならないことは、HVBG（ドイツ職業保険組合連盟）レポート「機械の安全防護物の無効化」［22］で指摘されている。

このため、 ISO 13849-1 でも人間工学の原則を用いることが要求され、本規格の 4.8 にこれに関連する規格群がリストアップされている。機械設計者が、SRP/CS のマン・マシン・インターフェースの設計を査定できるように、BGIA では、「人間工学設計」チェックリストを開発した。このチェックリスト並びに新情報は、2006 年 10 月に、BG インフォメーション BGI 5048-1 及び BGI 5048-2 で公表されており［23］、ここでは特にキーボード、押ボタン、入力機器等の手動制御器や、視覚危険信号等のディスプレイ及び表示器、そしてユーザインターフェースに関するソフトウェアエルゴノミクスが具体的に取り上げられている。また、機械の操作システムに関するユーザ指向の設計の手引き書として、VDI/VDE 指針 3850［24］を参考文献に挙げておきたい。

### 6.2　故障確率の定量化

PL を見積もるために規格で要求される故障確率の数値規定は、（他の規格においても同様）単純に「定量化」と呼ばれることが多いが、厳密に言えば、この数値は決して精確なものではなく、統計的手法あるいは他の見積りを利用して出された近似値にすぎない。この「規定」には考慮すべき主要影響量は挙げられているものの、それらの影響量から故障確率を見積もる手法については指示されていない。基本的に、信頼性ブロックダイアグラム、フォールト・ツリー手法、マルコフモデルあるいはペトリネットなど定評ある手法はどれでも認められる。故障確率を決定するのは、制御システムメーカー、機械のユーザ、あるいは試験機関であるが、それぞれの状況により各種手法に対する好みや経験が異なるため、適切な手法であればいずれを採用してもよいと明言されている。

一方、これまで故障確率の定量化を行ったことがない者にとっては、ISO 13849-1 によるサポートが多かれ少なかれ必要になるのも事実である。科学的に確立されたベース（マルコフモデル）があるにもかかわらず、簡単な定量化の方法を段階的に示した簡易的アプローチを開発したのは、これを考慮したためである。このアプローチは、いくつかの点で、安全側の見積りには問題があり、より精確な手法によるものと比べて故障確率の見積り数値が大きくなる可能性があると指摘される。しかしながら、この手法は数学者でない者にとっても実行可能であり、その手順は非常に明快であり、立証性のあるものといえる。この簡易的方法については、実際の計算例と共に後で詳しく説明する（本書 6.5 参照）。

#### 6.2.1　指定のアーキテクチャ・・・

安全制御システムの構造あるいはアーキテクチャは、不具合（障害）に対する耐性（フォールトトレランス）を決定付けるベースであり、これを土台に他のあらゆる定量可能な側面が組み立てられ、最終的に制御システム安全関連部の PL が構築される。1985 年以来、当産業分野に携わってきた BGIA の経験から言っても、機械の安全制御システムの基本型というのは限られており、実現されるすべての制御システムの大半はこの基本型（あるいはこの基本型の組み合わせ）に属するといってよい。これらをスペクトルで表すと、スペクトルの一端には信頼性の異なる複数のコンポーネントから構成されるテストの行われない単一チャンネルのシステムがあり、そしてスペクトルの中央部に行くほどテスト機能によりレベルアップされ、最終的にスペクトルのもう一端には 2 チャンネル構造の高レベルの診断機能を備えたシステムが存在する。3 チャンネル以上の複数のチャンネル、あるいは「特殊な」構造をもつシステムというのは機械構造では非常にまれであり、また簡易的方法では条件付でしか評価することはできない。しかし、3 チャンネル以上であったとしても、通常は 2 つの最も信頼性の高いチャンネルを考慮すれば、指定のアーキテクチャという簡易的方法で PL を十分正確に見積もることができる。このため、3 チャンネル以上の複数チャンネルによるシステムは、ISO 13849-1 では取り扱われない。各種機能チャンネルあるいはテストチャンネルへの「水平的」区分に加え、センサレベル（入力機器「Ｉ」）、処理レベル（論理演算機器「Ｌ」）そしてアクチュエータレベル（出力機器「Ｏ」）への「垂直的」区分も、多くのケースでは効率的手段になるといえる。

機械製造分野及び関連規格で確立された EN 954-1 のカテゴリについては、その継続が全面的に支持されて、ISO 13849-1 でも同じように 5 つの構造がカテゴリとして定義されている。ただし、ISO 13849-1 では、旧カテゴリの定義に、コンポーネントの信頼性（$MTTF_d$）、診断範囲（$DC_{avg}$）、共通原因故障（CCF）に対する耐性といった定量的要求が若干ながら追加され、さらにカテゴリは 5 つの構造基本型、つまり指定のアーキテクチャとして図式化される。同じカテゴリのものでも細部の構造についてはさまざまな形をとりえるが、しかし、指定のアーキテクチャへの図式化による一般化は、簡易的アプローチにおいてなお近似性を有すると見なしてよい。例えば 1 つのチャンネルの「垂直的」区分となるブロック（入力、論理、出力）の数は、通常、数学的及び安全技術的観点から見て、PL の決定にはほとんど影響を及ぼすものではない。

より複雑な安全機能の場合には、全体のセーフティチェーンを上記の 5 つの基本型のいずれを使ってもそれだけでは図式化できない可能性がある。そのような場合には、セーフティチェーンを複数のセグメントに分解し、その個々のセグメントを指定のアーキテクチャに図式化するという手法をとるのが一般的である。これらのセグメントをどのように再構築し、個々のパフォーマンスレベルから全体値を決定すればよいかについては、本章の 6.4 で詳しく説明する。次項で説明する仕様は、サブシステムに分解せずに 1 つのカテゴリに分類することのできる制御システム（SRP/CS）を対象としたものである。

### 6.2.2 ・・・カテゴリ

カテゴリは、制御システムの安全関連部（SRP/CS）を、不具合（障害）に対するその耐性及び発生時の挙動に関して、コンポーネントの信頼性及び／又は構造的配置に基づき等級付けするものである（表 6.2 参照）。不具合（障害）に対する耐性が高いほど、リスク低減の可能性は高くなる。カテゴリは故障確率及び PL を決定するためのバックボーンであり、コンポーネントの信頼性（$MTTF_d$）、診断機能（$DC_{avg}$）及び共通原因故障耐性（CCF）により補足される。

カテゴリ B は、基本となるカテゴリであり、これに関する要求事項はその他のカテゴリにおいても順守される。カテゴリ B 及びカテゴリ 1 では、不具合（障害）に対する耐性は主に適切なコンポーネントの選択と使用により達成される。不具合（障害）発生時には、安全機能を喪失する可能性がある。カテゴリ 1 は、特に安全技術的に十分吟味されたコンポーネント及び安全原則の使用により、カテゴリ B よりも高い耐性を有する。

カテゴリ 2、3、4 では、指定された安全機能に関する性能はより高いものとなる。これは主に構造的な方策により達成される。カテゴリ 2 では、通常、安全機能の実行性は技術的手段（試験機器 TE）により自動監視される。しかしながら、次のテストが行われる間に不具合（障害）が発生すると、安全機能を喪失する可能性がある。カテゴリ 2 を使用した場合には、適切なテスト間隔を選択することで、適切なリスク低減が達成される。カテゴリ 3 及び 4 では、単一の不具合（障害）の発生により安全機能の喪失を招くことはない。カテゴリ 4、また合理的に実行可能な場合にはカテゴリ 3 においても、単一の不具合（障害）は自動的に検出される。カテゴリ 4 では、さらに、検出されない不具合（障害）の累積に対する耐性が備えられる。

表 6.2:　カテゴリの要求事項の要約：右 3 列が旧規格のカテゴリの定義に対する主要変更事項

| カテゴリ | 要求事項の要約 | システムの挙動 | 安全性達成のための原則 | 各チャンネルの $MTTF_d$ | $CD_{avg}$ | CCF |
|---|---|---|---|---|---|---|
| B | SRP/CS 及び／又はその安全防護物並びにコンポーネントは、予期される影響に耐えうるように、関連規格に従って設計、製造、選択、組立、組合せされていること。基本安全原則を使用すること。 | 不具合（障害）発生時、安全機能の喪失を招くことがある。 | 主にコンポーネントの選択により特徴づけられる。 | 低から中 | なし | 関連なし |
| 1 | B の要求事項を適用すること。十分吟味したコンポーネント及び安全原則を使用すること。 | 不具合（障害）発生時、安全機能の喪失を招くことがあるが、発生の確率はカテゴリ B より低い。 | 主にコンポーネントの選択により特徴づけられる。 | 高 | なし | 関連なし |
| 2 | B の要求事項を適用し、かつ十分吟味された安全原則を使用すること。安全機能は機械の制御システムにより適切な間隔でテストされること。 | テスト間の不具合（障害）の発生が安全機能の喪失を招くことがある。安全機能の喪失はテストにより検出される。 | 主に構造により特徴づけられる。 | 低から高 | 低から中 | 方策が必要、附属書 F 参照。 |
| 3 | B の要求事項を適用し、かつ十分吟味された安全原則を使用すること。安全関連部は次のように設計されていること：<br>－いずれの部分の単一の不具合（障害）も安全機能の喪失を招かない。<br>－合理的に実行可能な場合は常に単一の不具合（障害）は検出される。 | 単一の不具合（障害）発生時、安全機能は常に動作する。すべてではないが、いくつかの不具合／障害は検出される。検出されない不具合／障害の累積により安全機能の喪失を招くことがある。 | 主に構造により特徴づけられる。 | 低から高 | 低から中 | 方策が必要、附属書 F 参照。 |
| 4 | B の要求事項を適用し、かつ十分吟味された安全原則を使用すること。安全関連部は次のように設計されていること：<br>－いずれの部分の単一の不具合（障害）も安全機能の喪失を招かない。かつ<br>－単一の不具合（障害）は、次の安全機能作動要求時、又はそれ以前に検出される。検出が不可能でも、検出されない不具合（障害）の累積により安全機能の喪失を招かない。 | 単一の不具合（障害）発生時、安全機能は常に動作する。<br>不具合（障害）の累積の検出により安全機能の喪失確率は低減する（高い $DC_{avg}$）。安全機能の喪失を防止するため、不具合（障害）は適時に検出される。 | 主に構造により特徴づけられる。 | 高 | 高<br>不具合（障害）の累積を含む | 方策が必要、附属書 F 参照。 |

不具合（障害）を考慮するに当たっては、想定すべきコンポーネントの不具合（障害）と、妥当なものとして除外できる不具合（障害）について慎重に検討しなければならない。これに関する注意事項は本書付録 C に記載される。

カテゴリ 3 及び 4 では、複数のチャンネルで同時故障を引き起こす可能性のある共通原因故障についても十分に抑制する必要がある。このことはカテゴリ 2 についても同様のことがいえる。というのは、独自の遮断経路をもつ試験機器により 2 チャンネル構造のシステムになるからである。基本安全原則及び十分吟味された安全原則の多くは、根本的に、偶発的ハードウェア故障に対してだけでなく、製品ライフサイクルのある時点、例えばレイアウト設計や変更時に製品に潜入する可能性のある系統的故障に対しても効果を発揮するものといってよいだろう。

### 6.2.3 カテゴリ B

SRP/CS は、関連規格に従って特定の用途に適用される基本安全原則に基づき、次のような影響に耐えられるよう設計、製造、選択、組立て及び組み合わせる必要がある。

- 予期される使用応力（例：遮断容量や開閉頻度に関する信頼性）
- 作業工程で使用される材料の影響（例：刺激性のある化学物質、粉塵、切り屑）
- 他の重要な外的作用（例：機械的振動、電磁妨害、動力源の中断あるいは障害）

本書付録 C の基本安全原則では、これらの一般原則が、共通原則または技術原則として示されている。共通の基本安全原則はすべて、あらゆる技術方式に適用される。一方、技術原則はそれぞれの技術方式に関して補足的に必要とされる。カテゴリ B は他のすべてのカテゴリに対する基本のカテゴリであるため（表 6.2 参照）、この基本安全原則は制御システム及び／又は安全防護物の安全関連部の設計一般に適用されなければならない。

カテゴリ B に使用されるコンポーネントに関しては、さらに特別な安全技術的方策は要求されない。このため、各チャンネルの $MTTF_d$ は「低」から「中」となる（「低」及び「中」の定義については後で説明する）。コンポーネント故障が生じると、安全機能の喪失を招く可能性がある。監視方策は要求されないので、$DC_{avg}$ は「なし」となる。また共通原因故障は単一チャンネルの制御システムでは考えられないため、CCF に関する要求も示されていない。

カテゴリ B の故障耐性は非常に低いため、基本的に、本カテゴリのシステムで達成しえる PL は最高でも「b」に制限される。

図 6.5 のカテゴリ B に適用される指定のアーキテクチャは、入力装置（I）、論理（L）、出力（O）からなる単一チャンネルシステムに対応する。

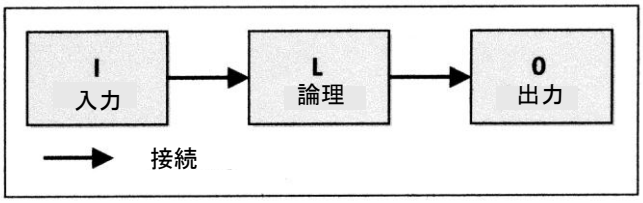


図6.5： カテゴリB及びカテゴリ1に適用される
アーキテクチャ

### 6.2.4 カテゴリ 1

カテゴリ 1 の SRP/CS については、カテゴリ B の要求事項（基本安全原則の使用等）を適用した上で、さらに安全技術的に十分吟味されたコンポーネント及び原則を用いて設計し、製造することが求められる。

安全関連用途での十分吟味されたコンポーネントとは、次のいずれかのものをいう。

- 過去に類似の用途で成功し、広く使用されているもの
- 安全関連の用途への適性及び信頼性示す原則を用いて製作され、検証されているもの

各種技術の十分吟味されたコンポーネントの概要は、本書付録 C に記載される。

新規に開発されるコンポーネント及び安全原則の適用は、それが、上記 2 つめの条件を満たしている場合には、「十分吟味された」ものとして見なすことができる。あるコンポーネントを十分吟味されたものとして受け入れるかどうかは、用途に依存する。例えばプログラマブルロジックコントローラ（PLC）、マイクロプロセッサ、もしくはある特定用途のために設計／製造される集積回路（ASIC）等の複雑な電子コンポーネントは、十分吟味されたコンポーネントとして見なすことはできない。結論から言えば、トランジスタ、ダイオード等の単純な電子コンポーネントは十分吟味されたものとして判断することができる。

コンポーネントの「十分吟味された」信頼性は、その用途に依存して、危険側故障が起こりそうにないということを意味するものでしかない。予期される危険側故障率は 0 よりも大きい適切な数値であり、これは $MTTF_d$ として PL の決定に組み入れられる。それとは反対に、不具合（障害）の除外（本書 6.2.10 参照）を採用する場合には、「限りなく高い」$MTTF_d$ が想定され、考慮対象外となる。

カテゴリ 1 では、予期されるコンポーネントの信頼性は高いため、単一チャンネルの $MTTF_d$ は高くなければならない。しかし、カテゴリ B 同様、$DC_{avg}$ 及び CCF に関する要求は存在しない。また、不具合（障害）の発生により安全機能の喪失を招く可能性がある。しかしながら、カテゴリ 1 のチャンネルの $MTTF_d$ はカテゴリ B よりも高い。従って安全機能が喪失する可能性はより少なく、カテゴリ 1 で達成できる PL は最高「c」になる。

カテゴリ 1 に対する指定のアーキテクチャは、カテゴリ B と同じものが適用される（表 6.5 参照）。両者の違いはコンポーネントの信頼性にあり、構造自体は同じである。

### 6.2.5 カテゴリ 2

カテゴリ 2 の SRP/CS については、カテゴリ B の要求事項（基本安全原則の使用等）を適用した上で、十分吟味された安全原則を使用し、かつ安全機能が適切な周期で機械の制御システムによりテストされることが求められる。安全機能（単独もしくは複数）のテストは、次のときに実行されなければならない。

- 機械の起動時
- 新たなサイクルの開始、別の動作の開始など危険状態が始動する前と、リスクアセスメント及び運転モードにより必要とされる場合には運転中／周期的

こうしたテストは自動的に実行することができる。安全機能の診断により、次のいずれかが実行されなければならない。

- 不具合（障害）が検出されなかったときには運転を許可する。
- 不具合（障害）が検出されたときには、適切な制御方策を開始するための出力を発生させる。この出力は、可能な場合は常に安全状態を導くものでなければならず、かつその安全状態は不具合（障害）が除去されるまで維持されなければならない。安全状態に導くことができない場合（開閉機器の接点溶着等により）には、この出力は危険状態を警告できるものでなければならない。

カテゴリ 2 に適用されるアーキテクチャ（図 6.6）の場合、$MTTF_d$ 及び $DC_{avg}$ の算定で考慮されるのは機能チャンネルのブロック（つまり I、L、O）のみであり、テストチャンネルのブロック（つまり TE 及び OTE）の $MTTF_d$ は間接的にしか考慮されない。機能チャンネルの $MTTF_d$ については「低から高」まで認められる。$DC_{avg}$ は少なくとも「低」が要求される。また、CCF に対する十分な方策をとる必要がある（本書 6.2.15 及び付録 F を参照）。

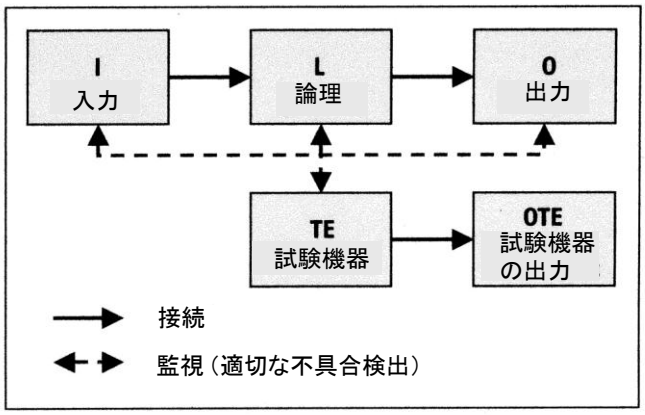


図6.6： カテゴリ2に適用されるアーキテクチャ：
点線は合理的に実施可能な不具合（障害）検出

テストを行う試験機器自体が、危険な状況を引き起こすことがあってはならない（例えば応答時間の遅れ等による）。試験機器は機能チャンネルの構成部として、あるいはそれとは分離して装備される。安全機能のテストはすべてのコンポーネントでは実施されるわけではないので、いくつかのケースではカテゴリ 2 は適用することができない。次のテストが実施されるまでに検出されずに安全機能が故障する可能性があるので、テスト頻度は重要なパラメータになる。さらに、試験機器自体が機能チャンネルよりも早く故障してしまうことも考えられる。このため、指定のアーキテクチャと柱状グラフ（図 6.10）を用いた PL の簡易的な定量化では、次のことが前提条件となる。

- 試験機器の $MTTF_d$ 値は論理（論理演算機器）の $MTTF_d$ 値の半分未満である（本書付録 E の最終ページ参照）。
- テスト頻度は、最低でも安全機能の平均作動要求頻度の 100 倍を超える（6.2.14 参照）。

これらの条件により、また外部の試験機器による指定のアーキテクチャでは実際には 90%を超える $DC_{avg}$ を達成することは難しいため、検出されない最初の不具合（障害）により安全機能の喪失を招く可能性がある。このような理由から、カテゴリ 2 で達成することのできる PL は最高でも「d」に制限される。

### 6.2.6 カテゴリ 3

カテゴリ 3 の SRP/CS については、カテゴリ B の要求事項（基本安全原則の使用等）を適用した上で、十分吟味された安全原則を使用し、かつ単一の不具合（障害）が安全機能の喪失を招かないように設計することが求められる。適切な方法で実施可能な場合は常に、単一の不具合（障害）は次の安全機能作動要求時、もしくはその前に検出されなければならない。

いずれのチャンネルの $MTTF_d$ についても、「低」から「高」まで選択できる。不具合（障害）をすべて検出することは要求されず、また検出されない危険側故障の累積により危険状態を引き起こす可能性があるため、$DC_{avg}$ は最低「低」である。共通原因故障（CCF）に対する十分な方策をとる必要がある。

危険側故障が潜在しない（フェールセーフデザイン）単一チャンネルのコンポーネントも単一不具合（障害）に対する耐性があるといえるので、単一不具合（障害）耐性の要求は必ずしも 2 チャンネルシステムの実現を意味するものではない。同じことが、独自の遮断経路により不具合（障害）に迅速に対応し、危険状態を回避することのできる高レベルの監視付システムについてもいえる。それにもかかわらず、カテゴリ 3 のシステムは 2 チャンネル構造で実現されるケースが圧倒的に多い。このため、カテゴリ 3 に適用される指定のアーキテクチャもこれに対応して選択された（図 6.7 参照）。なお、単一チャンネルのハードウェア上に冗長ソフトウェアを使用するような純粋に「論理的な 2 チャンネル構造」は、当然ながら、一般的にはハードウェア故障に対する単一不具合（障害）耐性を有するものとは見なされない。

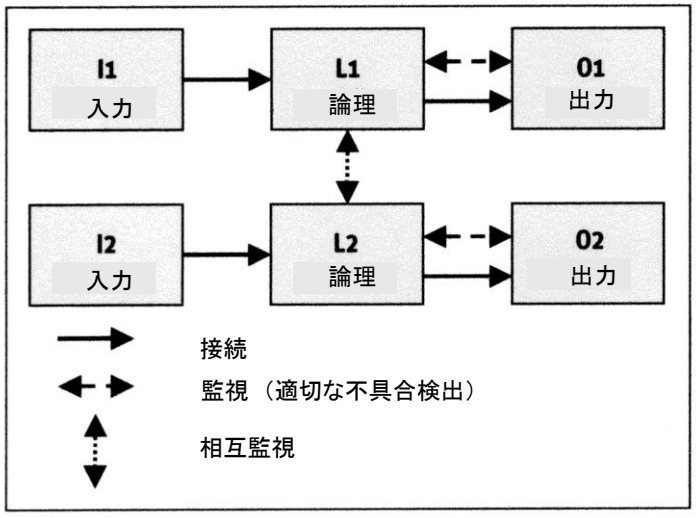


図6.7: カテゴリ3に適用されるアーキテクチャ：
点線は合理的に実施可能な不具合（障害）検出

### 6.2.7 カテゴリ 4

カテゴリ 4 の SRP/CS については、カテゴリ B の要求事項（基本安全原則の使用等）を適用した上で、十分吟味された安全原則を使用し、かつ次のように構築することが求められる。

- 単一の不具合（障害）は安全機能の喪失を招かない。
- 単一の不具合（障害）は次の安全機能作動要求時、もしくはその前の、例えば機械サイクルの開始あるいは終了時に検出される。このような検出が不可能な場合には、検出されない不具合（障害）の累積により安全機能の喪失を招くことがあってはならない（実際には、2 つの不具合に関する不具合の組合せを考察すれば十分といえる）。

このカテゴリは最も高い不具合（障害）耐性（リスク低減への最高度の貢献）を有するものとなるため、各チャンネルの $MTTF_d$ 並びに $DC_{avg}$ も「高」でなければならず、CCF に対しても十分な方策をとる必要がある。

カテゴリ 3 との違いは主に $MTTF_d$ と $DC_{avg}$ にあるので、カテゴリ 4 に対し指定されるアーキテクチャ（図 6.8）はカテゴリ 3 のものと類似する。しかし、監視を表す線種により、より高い $DC_{avg}$ であることがわかる。

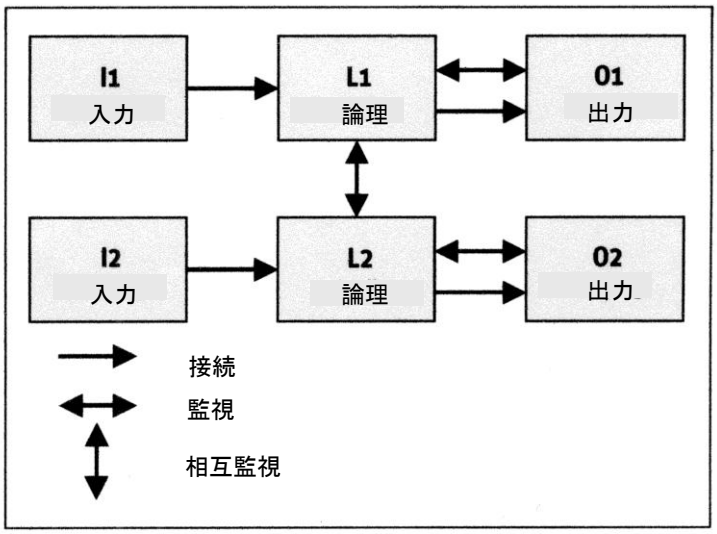


図6.8: カテゴリ4に適用されるアーキテクチャ

### 6.2.8 ブロックとチャンネル

故障確率を簡易的に定量化するために、安全関連制御部を抽象化したブロックとチャンネルで表す手法が活用される。本件で使われる「ブロック」の定義は固有のものであり、ここでは、直列及び並列で配置された比較的小さなユニットで安全機能を実行する機能ブロックを意味する。ハードウェアの構造を安全関連ブロックダイアグラムで図示するに当たっては、次のルールが適用される。

- ブロックは、安全機能の実行に関係するすべての制御要素を抽象化した形で表すこと。
- 安全機能が複数の冗長チャンネルで実行される場合には、それらのブロックは別々に示すこと。これにより、1 つのブロックが故障しても別のチャンネルのブロックによる安全機能の実行には支障をきたさないということが表わされる。
- 1 つのチャンネル内のブロックの割り当ては、むしろ任意に指定されるものといってよい。ISO 13849-1 では、1 チャンネルごとに 3 つのブロック（入力 Ｉ、論理 Ｌ、出力 Ｏ）を指定することが提案されてはいるが、これは理解しやすいように用いられたものといえる。「Ｉ」、「Ｌ」、「Ｏ」間の正確な境界及び 1 つのチャンネルにおけるブロックの数はいずれも PL の形で算定される故障確率に重要な影響を及ぼすものではない。

- 安全関連の各ハードウェアユニットに関して、所属するブロックを明白に（例えば部品リストとして）定めること。これにより、あるブロックに属するハードウェアユニットの平均危険側故障時間（$MTTF_d$）をベースにして、そのブロックの $MTT_d$ が算定できる（例えば故障モード及び影響解析 FMEA あるいは「部品点数」法による、本書 6.2.13 参照）。
- その故障がそれぞれのチャンネルにおける安全機能の実行に直接影響を及ぼしえない、純粋にテストを目的として使用されるハードウェアユニットは、追加されるテストチャンネルの別のブロックとしてグループ化される。

本規格は、カテゴリ 3 及び 4 については、外部の試験機器の信頼性に関する要求事項を直接的には定めてはいないが、カテゴリ 2 に基づいて言うならば、試験機器に要求される $MTTF_d$ は最低でも個々の（対称化された）チャンネルの $MTTF_d$ の半分である。また、ここでは系統的故障及び CCF についても考慮する必要がある。

### 6.2.9 安全関連ブロックダイアグラム

安全関連ブロックダイアグラムは、比較的よく知られている信頼性ブロックダイアグラム［25］をベースとしている。両ダイアグラムには、左から右に流れる機能結合線に沿ったブロックチェーンが、各ブロックが危険側故障に陥ることなく存在する限り、機能（安全機能）は実行されえるという原則が共通して適用される。しかし、安全関連ダイアグラムの方には、冗長チャンネルの相互監視、あるいは分離された試験ユニットによるテスト等の診断メカニズムが追加される。安全関連ブロックダイアグラムの一般的な例を図 6.9 に示す。

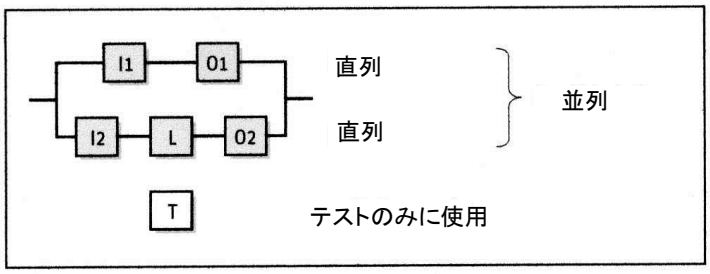


図6.9: 安全関連ブロックダイアグラムの一般的な例;
I1及びO1が1番目のチャンネルを構成（直列）し、
I2、L、O2が2番目のチャンネルを構成（直列）
する。 2つのチャンネルにより安全機能は冗長構造
（並列）となる。Tはテストのみに使用される。

この定義に従って安全制御システムを安全関連ブロックダイアグラムで図示するためには、次のようなルールが作成される。

いわゆる「チャンネル」を構成するブロックの直列配置（例：Ｉ、Ｌ、Ｏ）は、1 つのブロックの故障によりチェーン全体の故障を招く可能性があることを示すものである。例えば、1 つのチャンネルの 1 つのハードウェアユニットが危険側故障に陥ると、全体のチャンネルは安全機能を実行することができなくなる。

- ブロック及びチャンネルの並列配置は、安全機能あるいはその該当するコンポーネントの多重冗長構造を象徴的に示すものである。例えば複数のチャンネルにより実行される安全機能は、少なくとも 1 つのチャンネルが故障しない限り維持される。
- その故障がそれぞれのチャンネルにおける安全機能の実行に直接影響を及ぼしえない、テストのみを目的として使用されるブロックは、分離されたテストチャンネルとして示すことができる。診断機能の故障によりシステムの信頼性は総合的に低下するが、このことは、個々のチャンネルでの純粋な安全機能の実行が保証されている限りはわずかな影響しか及ぼさない。

ブロック及びチャンネルの定義付はカテゴリの決定と同調するものであり、PL の定量的決定における最初のステップになる。PL の定量的決定には、さらに、コンポーネントの信頼性の評価（$MTTF_d$）、診断の特性値（$DC_{avg}$）及び共通原因故障（CCF）に対する方策が考慮される。

### 6.2.10　不具合（障害）の考察と除外

実際の制御システムでは、理論的に可能な不具合（障害）の数はほとんど無限であるといってよい。このため、評価を行うに当たっては重要な不具合に限定する必要がある。特定の不具合は、次のことを考慮した上で除外することができる。

- その発生は技術的にありえそうにない（他の想定される不具合及び達成すべきリスク低減と比べ合わせるとその確率及び程度はわずかである）
- 考察される用途には依存しない、一般的に認められる技術的な経験
- 用途及び特定の危険源に関する技術的要求事項

どのようなコンポーネントの不具合（障害）が発生しえるかは、ISO 13849-2 で説明される。これについては、次の点に留意する必要がある。

- 不具合（障害）リストは単に選択肢を示すものである。このため、新規コンポーネント等の場合には新たな不具合（障害）モデル（新規コンポーネント等の場合）を作成したり、あるいはそれぞれの用途に従ってその他の不具合（障害）のタイプを考慮しなければならないケースもある。これは、例えば FMEA に基づいて行われる。
- 続発する不具合（障害）は、共通原因を有する複数の不具合（共通原因故障 CCF）と同様、それを誘発した最初の不具合（障害）といっしょに単一の不具合（障害）として評価する。

不具合（障害）の除外に関しては、本書付録 C 及び ISO 13849 の第 2 部で詳しく説明される。除外の理由がすぐにわかるようなものではない場合（例：正確に寸法決めされた回路基板のレイアウトの配線パターンがはがれる）は、技術文書でその除外に対する根拠を正確に示す必要がある。

不具合（障害）の除外は、前提となる条件が適切な場合には、電気機械式ポジションスイッチ、非常停止機器のノーマリクローズ（ブレーク接点）、機械アクチュエータ等のコンポーネントについても可能である。このようなコンポーネントに関しては、不具合（障害）の除外において故障率（$MTTF_d$）及び診断方策（DC）を考慮する必要はない。

### 6.2.11　平均危険側故障時間－$MTTF_d$

制御システムを構成する個々のコンポーネントの信頼性により、システム全体の信頼性が決定される。このため、いわゆる平均危険側故障時間 $MTTF_d$（Maen Time to Dangerous Failure）が信頼性データとして PL に考慮される。故障とは、ここでは、指定された機能をもはや実行できなくなるコンポーネントの欠陥のことをいうのは明らかである。以下に、「平均危険側故障時間」を構成するその他の用語についても説明しておく。

- 「平均」とは、統計上の平均値を指す。これは個々のコンポーネントに関するものではなく、典型的なコンポーネントの平均寿命の期待値として定義される。この場合、個々のコンポーネントの期待値は同タイプの数多くのコンポーネントの平均値と同等と見なすことができる。つまり、故障のない期間という意味での保証された最低限の寿命のことではない。この平均値の考え方は、コンポーネントがその決められた使用条件内で使用される限り、通常、その寿命値は使用条件（例：負荷、温度、雰囲気）に合ったものではないという事実にも反映されている。つまり、ある機器のある使用における高い負荷は、その機器の別の使用における低い負荷により平均化されていることが一般的に想定される。もちろん、すべての使用において負荷が高まる（例えば極端な温度により）ことが予測されるならば、こうした条件は $MTTF_d$ を決定する際に考慮されなければならない。

- 「時間」は、信頼性が寿命という意味の時間で表わされることを示すことばである。一般的には、$MTTF_d$ は年（略称「a」）で表わされる。$MTTF_d$ に換算することのできる他の表記形式によるものとして、例えば故障率あるいは切り替え頻度が挙げられる。故障率は、通常、ギリシャ文字の小文字「λ」で表わされ、単位は「FIT」（= $10^{-9}$/h、つまり 10 億個出荷されたコンポーネントのうち 1 時間当たり 1 個の故障）が用いられる。$\lambda_d$ と $MTTF_d$ の関係は、平均寿命にわたる一定の故障率を $\lambda_d$ とした場合には、$MTTF_d = 1/\lambda_d$ となる。ここでは、当然ながら時間の年への換算を考慮に入れる必要がある。主に機械的な操作により摩耗が生じるコンポーネントの場合には、信頼性は、$B_{10d}$、つまり 10%のコンポーネント（サンプル）が危険側故障に至るまでの平均サイクル数等の切り替え頻度で示されるのが一般的である。この場合には、使用において期待される 1 年間の平均操作回数 $n_{op}$（Number of Operations）を算入することで、$MTTF_d$ に換算することができる。これに関する詳細は、本書付録 D を参照いただきたい。

- 「危険側」は、安全機能を実行する能力が損なわれ、最終的に PL に影響するような故障（非安全側故障）を明確にすることばである。これとは反対に、非危険側故障では安全な状態に誘導される（運転抑止）。機械の稼働率及び生産性を低下させる可能性はあるものの、この場合には安全機能がさらに有効に働く、あるいは安全状態が導かれて維持される状況が発生する。冗長構造では、「危険側」という属性は当然ながら個々のチャンネルそれぞれに関わってくる。1 つのチャンネルの故障が安全機能の失効を招く場合には、仮に別のチャンネルにより安全機能を続行できるとしても、この故障は危険側故障と呼ばれる。

トランジスタ、バルブ、コンタクタ等の個々のコンポーネントと同様、1 つのブロック、チャンネル、あるいは制御システム全体についても 1 つの $MTTF_d$ を考察することができる。全体の $MTTF_d$ は、複数のチャンネルの場合には対称化して、SRP/CS に関与するすべてのコンポーネントの $MTTF_d$ をベースとした 1 つのチャンネルに対する値として解釈される。ボトムアップ方式により、考察されるユニット（単位）は順次拡大していく。労力を最小限に抑えるには、その故障が安全機能の実行に直接あるいは間接的に悪影響を及ぼしえる安全関連コンポーネントのみを考察するのが一般的には効率的といえる。さらに、負担を軽減するためには、特定の故障は極めて発生しそうになく、全体の信頼性へのその貢献度は無視してもよいほど小さなものであるということを根拠に、不具合（障害）の除外を行うこともできる。もちろん、不具合の除外を採用するに当たっては、ISO 13849-2 における詳細な規定及び本書 6.2.10 で説明される条件が関係してくる。これに従って、特定の条件の下で、配線の短絡あるいは特定の機械的故障等を設計上の理由から除外することが可能である。

### 6.2.12　個々のコンポーネントのデータ

定量化の関連でもっともよく出される質問の 1 つとして、安全関連コンポーネント（セーフティコンポーネント）に関する信頼できる故障データの入手が挙げられる。この場合もっとも優先すべき情報源は、メーカーの技術データシートである。電気機械あるいは油圧分野等のコンポーネントメーカーの多くは、今後こうしたデータは提供可能であると話しているが、（さしあたって）メーカーによるデータがなかったとしても、典型的なサンプル値は既成のデータ集から探し出すことができる（本書付録 D 参照）。もちろん、こうした資料では、非危険側故障と危険側故障の区別はほとんどなされていないが、概算すると、平均的には全故障の半数のみが危険側であると想定される。信頼性データの入手性を意識して、ISO 13849-1 では典型的な値をリスト化している。しかし、これらは非常に保守的な見積りとなっているため、前述の情報源が用意されていない場合にのみ使用することをお勧めする。付録 D には、機械、油圧及び電子コンポーネントの $MTTF_d$ 値だけでなく、空圧及び電気機械コンポーネントの $B_{10d}$ の値も挙げられている。詳細については、そちらを参照いただきたい。

### 6.2.13　FMEA と「部品点数」法

すべての安全関連コンポーネントの $MTTF_d$ 値がそろっていれば、そこから、いくつかの簡単なルールに則り制御システムの $MTTF_d$ 特性を算定することができる。その際、2 つの異なる手法が利用

できる。1 つは、精確ではあるが労力を要する FMEA（Failure Mode and Effects Analysis、故障モード及び影響解析）であり、もう 1 つは、安全側に対する数少ない見積もりにより迅速かつ簡単に行うことのできる「部品点数」法と呼ばれる手法である。両者の違いは、すでに、次のような MTTF と $MTTF_d$ との小さな違いに見ることができる。

ある構成要素の危険側故障率はどのくらいになるか？労力を要する FMEA 手法では、想定されるすべての故障モードがリスト化され、それぞれ「非危険側」もしくは「危険側」として評価され、その故障の原因の頻度が見積もられる。1 つのコンポーネント故障がそのブロックに及ぼす影響は、安全側もしくは非安全側かにその故障の方向性が決定されるので、ある故障により引き起こされる影響について詳細な分析が必要になる場合もある。しかし、これにより、ISO 13849-1 で提案されるような簡易的評価による場合よりも多くの故障モードが「安全側」とされる可能性もある。一方、「部品点数」法の場合には、保守的なアプローチにより、全体として、非危険側及び危険側への関与が相殺されることが前提となる。このため、$MTTF_d$ は、より精確なデータがない限りは常に、MTTF の 2 倍になる。ここでも、統計学上の平均値の原則がベースになる。つまり、ある構成要素の過度に有利な評価と別の構成要素の過度に不利な評価は、互いに補填し合い、相殺されるということである。「部品点数」法と FMEA を組み合わせることももちろん可能である。「部品点数」法のみで適切な（十分に小さい）PFH が導き出される場合には、FMEA を行う必要はない。しかしそうでない場合には、特に低い $MTTF_d$ 値を示すコンポーネントに関しては、例えば部分的に FMEA を実施することにより故障の方向性を調査するのが、有効的アプローチといえる。本テーマに関する詳細は本書付録 B を参照いただきたい。

他の定量化の手法と同様、ISO 13849-1 による評価においても、すべての $MTTF_d$ 値は、コンポーネントの使命時間の期間内における故障率が一定であることを前提としている。これは、例えば摩耗の激しいコンポーネントについてはその故障挙動に直接対応したものとはいえないが、それでも、安全側の見積もりにより決定される $MTTF_d$ は近似値として、そのコンポーネントの使命時間にわたって適用される。初期故障については無視するのが一般的である。というのは、初期故障が顕著なコンポーネントは機械の制御システムに関する稼働率の要求に適ったものとはいえず、そのため市場で有用されることはほとんどないからである。この評価手順の便利さは、$MTTF_d$ が常にこれに関連する危険側故障率 $\lambda_d$ の逆数に等しいという点にある。1 つのブロックのコンポーネントの危険側故障率 $\lambda_d$ は簡単に合算できるので、関与するコンポーネント（インデックス i の n 個のコンポーネント）の $MTTF_d$ 値から次の式によりブロックの $MTTF_d$ を算出することができる。

$$\lambda_d = \sum_{i=1}^{N} \lambda_{di} \quad \text{すなわち} \quad \frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}} \qquad (1)$$

同様の関係が、ブロックの $MTTF_d$ 値からそのブロックが属する各チャンネルの $MTTF_d$ を求めるときにも適用される。そして、各チャンネルの $MTTF_d$ が決定されたら、等級一覧表という形でさらに簡易化される。決定された値は 3 つの等級に分類される（表 6.3 参照）。

表 6.3： 各チャンネルの $MTTF_d$ の等級付け

| 各チャンネルの $MTTF_d$ | |
|---|---|
| 表記 | 範囲 |
| 適切ではない | 0 年 ≦ $MTTF_d$ ＜ 3 年 |
| 低 | 3 年 ≦ $MTTF_d$ ＜ 10 年 |
| 中 | 10 年 ≦ $MTTF_d$ ＜ 30 年 |
| 高 | 30 年 ≦ $MTTF_d$ ＜ 100 年 |
| 許容されない | 100 年 ＜ $MTTF_d$ |

平均寿命（保証されたものではない!）が 3 年未満のものは、安全関連のコンポーネントについては適切でないと見なされる。また、100 年を超えるものは、構造やテストなど他の重要な影響量との比較考量においてコンポーネントの信頼性を過大評価しないために、考慮に入れることはできない。実際に 1 つのチャンネルに関して 3 年未満となる場合には、コンポーネントをより信頼性の高いものと取り替えるべきである。そうしなければ、PL「a」ですら達成することはできない。また、100 年を超える平均寿命が一般的に存在しないというわけではないが、コンポーネントの信頼性ではすでに 100 年が最高値とされているので、この「上限」を超える場合には PL に貢献するものとして認められない。1 つの制御システムに複数のチャンネルが含まれる場合には、システム全体に対する値をどのように求めるべきかということがまず問題になる。このようなケースでは、慎重を期するならば、当然小さい方の値をとるのが常に確実といえるだろう。しかし、次式による平均化（C1 と C2 はここでは対称化される 2 つのチャンネルを表わす）によりさらに適切な結果を導くことができる。

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}}\right] \qquad (2)$$

チャンネル同士のバランスがとれている場合には、このように算出された $MTTF_d$ 値は 1 つのチャンネルの $MTTF_d$ に相当する。バランスがとれていない場合には、より高い値の最低 3 分の 2 となる平均 $MTTF_d$ 値が算出されることになる。さらに、この場合は、より高い $MTTF_d$ 値は前もって上限 100 年に制限されるので、これにより対称化される値は常に 100 年未満になるという筋書きができているともいえる。このため、一般的には、できるだけ信頼性のバランスのとれた複数チャンネルを実現するのが望ましい。いずれにせよ、この手法による結果は、チャンネルの数及び仕様とは無関係に、制御システムにわたって平均化された単一の制御チャンネルに関する $MTTF_d$ 値として、コンポーネントの信頼性レベルを示すものである。

### 6.2.14　テスト及び監視方策による診断範囲　－DC

さらに、PL に対し大きな影響を及ぼすパラメータの 1 つとして、SRP/CS のテスト（自己診断）と監視方策がある。効果的なテストにより、例えばコンポーネントの低い信頼性を部分的に補償することができる。診断の有効度は、ISO 13849-1 では、いわゆる診断範囲 DC（Diagnostic Coverage）により評価される。DC は、想定されるすべての危険側故障に対する検出された危険側故障の割合として定義され、1 つのコンポーネント、ブロック、あるいは SRP/CS 全体がその定量化対象となりえる。SRP/CS 全体の場合には平均診断範囲 $DC_{avg}$（average）となり、柱状グラフにより PL を決定する際に重要な役割を担う。

本規格の随所に見られるように、この $DC_{avg}$ を決定するに当たっても、より精確ではあるが労力を要する手法と、安全側に対する一連の見積りを実行する簡易的手法が挙げられる。前者の方法は、故障モード及び影響解析（FMEA）により進められ、DC の定義に対応したものといえる。この場合、各コンポーネントに対して、検出可能な危険側 dd（dangerous detectable）故障モード及び検出不可能な危険側 du（dangerous undetectable）故障モードと、コンポーネントの全故障率に対するその比率が決定される。最終的に、足し算及び分数により、考察される単位の DC 値が算出される。

$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \sum \lambda_{du}} = \frac{\sum \lambda_{dd}}{\sum \lambda_{d}} \qquad (3)$$

ISO 13849-1 で推奨される方法は、コンポーネントあるいはブロックレベルをベースとして保守的な DC の見積もりを行い、さらにそれらの個々の DC 値から平均値を算出する公式により $DC_{avg}$ を算定するものである。多くの診断方法は典型的ないくつかの標準方策に整理することができ、方策に応じた DC の参考値が本規格の附属書 E にリスト化されている。これらの方策は 4 つの指標値（0%、60%、90%、99%）による大まかなパターンに分類される。本規格で扱われる典型的な診断方策の詳細については本書付録 E のリストを参照いただきたい。また、この適用については断裁機を例に別途説明する（本書 6.5 参照）。

1 つのコンポーネントあるいはブロックの DC を決定するに当たっては、種々の周辺条件に留意する必要がある。

- 危険側故障の検出は、スタートにすぎない。テストを有効に終了するためには、危険状態がもはや存在しない安全状態が開始される必要がある。これには効果的な遮断経路も含まれ、例えば単一チャンネルの診断システム（カテゴリ 2）の場合には、2 つめの停止要素が必要になってくる。これは、テストにより正規の遮断要素（安全関連ダイアグラムにおけるブロック「O」）の故障が確認された場合に、安全な状態に導き、これを維持するために必要とされる。
- テストの作動及び実施だけでなく、必要な停止（遮断）も、SRP/CS により優先的に自動的に実行されることが求められる。ここでは、機械オペレータ等を頼りにした手動介入は、例外的ケースを除いてお勧めできない。残念な実態ではあるが、手間をかけたくない、時間的余

裕がない、あるいは情報や組織が不完全であるといった理由により、必要な方策が十分に実行されないことが多いからである。手動テストを効果的に実行するためには、しっかりとした組織的取り組みや規律が欠かせない。しかし、そうであるにもかかわらず、2 チャンネル構造のシステムに関する DC の決定では、安全機能作動要求時の不具合（障害）検出が考慮される。すなわち、プログラマブル電子機器システムで自動的に作動するテストのみが考察されるわけではない。リレーやコンタクタ等の電気機械コンポーネントでは、「遮断できない」という不具合は、通常、安全機能の作動要求時にしか検出することができない。不具合（障害）の検出が安全機能作動要求時に行われるものについては、その作動要求頻度を考慮に入れる必要がある。

- さらに、必要なテスト頻度の問題が挙げられる。非常にまれにしか実行されないようなテストは、危険事象の発生に遅れをとり、見せかけの安全性を提供するものでしかない。テスト頻度に関しては、大まかには次のことがいえよう。テスト頻度は常に何かしら別の頻度と競合する。そのため、一般的に適切な頻度と言えるものはない。カテゴリ 3 及び 4 の 2 チャンネル構造のシステムでは、テスト頻度は 2 つめの危険側故障の発生頻度と競合するといえる。というのは、テストにより 1 つめのチャンネル故障が認められる前に、2 つめのチャンネルが故障してはじめて、安全機能が実行されないという危険が存在するからである。さらに、カテゴリ 4 のシステムは、その定義に従って、検出されない不具合（障害）の累積にも耐えられるものである。2 チャンネル構造のシステムでは、1 シフトにつき 1 回というテスト頻度が適切なものとして実証されている。一方、カテゴリ 2 のテスト機能付単一チャンネルの場合には、次の安全機能の作動要求が起こる前、つまり潜在的危険源が実現される前に、テストが有効に行われる必要がある。この場合は、テスト頻度は安全機能の作動要求頻度と競合関係にあるといえる。両ケースともに、適切なテスト頻度はファクター100、つまり、危険側故障率 $\lambda_d$ (= 1/$MTTF_d$)（カテゴリ 3 と 4 の場合）もしくは安全機能の平均作動要求頻度（カテゴリ 2 の場合）の少なくとも 100 倍とされる。反対に、ファクターが 25 まで下がると、故障確率は最高約 10%増加する。このレベルを下回った場合には、そのテストが有効なものかどうかは、本質的には、作動要求とテストの同期化に依存する。テスト機能付単一チャンネルシステムでは、危険源が生じる前にテストが速やかに実行され、安全状態が達成されるならば、テスト頻度に関する条件は課せられない。

- 次のポイントは、試験機器自体の信頼性である。試験機器は、基本的に、それにより監視されるコンポーネントよりも先に故障するべきではない。しかし一方で、試験機器の信頼性に、本来の安全機能を実行する安全機器に対してよりも多く投資することは現実的とはいえない。このため、ISO 13849-1 の試験機器の信頼性に関する要求は控えめである。カテゴリ 3 及び 4 では、安全機能が実行されなくなるまでに試験機器の故障を含めて合計 3 つの危険側故障が必要なので、単一の不具合（故障）に対する耐性が頼りにされる。3 つの危険側故障が検出されずに発生するというのは極めてありえそうにないため、このことはさしたる問題にはならない。しかし、カテゴリ 2 の場合には、少なくとも柱状グラフによる簡易的な PL の決定では、「カテゴリ 2 の柱」を算定するために設定された付随条件がある。そこでは、試験機器の危険側故障率が、これにより監視されるコンポーネントの危険側故障率の 2 倍を超えないことが要求される。この比較をチャンネルベースで行うのかは定かではないが、結果的に、テストチャンネル全体の $MTTF_d$ 値は、機能チャンネルの $MTTF_d$ 値の半分以上であることが求められる。

- 例えばプロセスによる不具合（障害）の検出など特定の診断方策の有効性は、用途により非常に大きく左右され、DC は 0%から 99%まで可能である。診断指標の選択には、特に細心の注意が必要である。
- コンポーネントあるいはブロックが複数の方法により監視される、あるいは各種構成部にさまざまな診断方法が作用して、そこからコンポーネントあるいはブロックに対する全体の DC を算出しなければならない場合も生じる。本書付録 E には、こうした質問に対する参考情報が記載される。
- プログラマブル電子システムの場合には特に数多くの複合化された不具合（障害）が考えられ、診断方法の複合性に関してもこれに対応した要求事項が示される。ISO 13849-1 では、（プログラマブルあるいは複合的）演算論理に関して 60%よりも高い DC が要求される場合には、可変メモリ、不変メモリ及び処理ユニット（該当する場合）に対し少なくとも 1 つの方策をとることが要求され、それぞれ最低でも DC 60%であることが求められる。

最終的に、すべてのブロックの DC 値が出されたならば、システムに対する $DC_{avg}$ が近似式（4）により算出される。ここでは、個々の DC は関連する $MTTF_d$ とともに評価される。というのは、非常に信頼性の高い構成部（高 $MTTF_d$）は、信頼性の低い構成部よりも有効度の高い診断に依存する必要がないからである。（分子及び分母の足し算は、システム全体を構成する N 個のブロックが対象となる）。

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_N}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}} \qquad (4)$$

$DC_{avg}$ という平均値の算出により、SRP/CS 全体の診断及び監視方策の品質レベルを表わす特性値が準備されたことになる。この値は、カテゴリ（5 つの等級）及び各チャンネルの $MTTF_d$（3 つの等級）と同様、PL の簡易的定量化に組み入れる前に、表 6.4 の 4 つの等級に分類される。

表 6.4： ISO 13849-1 の簡易的アプローチによる診断範囲の分類

| DC（診断範囲） | |
|---|---|
| 表記 | 範囲 |
| なし | DC ＜ 60% |
| 低 | 60% ≦ DC ＜ 90% |
| 中 | 90% ≦ DC ＜ 99% |
| 高 | 99% ≦ DC |

次に、この $DC_{avg}$ を柱状グラフによる簡易的な定量化（6.2.16 章参照）に適用する際には、$DC_{avg}$ 等級のそれぞれ低い方の指標値（0%、60%、90%、99%）しか用いられない。つまり、安全側に対する見積りに基づき、さらに簡略化されるわけである。

しかしながら、個々のケースでは、この簡易化された大まかなパターンに当てはめると、例えば SRP/CS に関して平均値を上回る DC を有する信頼性のあまり高くないコンポーネントを、信頼性の高いコンポーネントに置き換えた場合には、矛盾が生じる可能性がある（詳細は本書付録 G の最後を参照）。

### 6.2.15　共通原因故障に対する方策－CCF

簡易的定量化において故障確率に関わる最後のパラメータとなるのが、共通原因故障 CCF（Common Cause Failure）である。例えば、冗長構造をとる SRP/CS の 2 つのチャンネルに関連する単一の原因に起因した危険側故障がこれに当たる。故障原因としては、制御システムの設計において十分な考慮がなされなかったことによる不適切な環境条件や過負荷等が挙げられる。チャンネルの分離が不十分である場合には、意図された単一不具合（障害）耐性の効力が失われる、あるいは二次故障を招くといった恐れがある。具体的なシステムにおけるこの影響の重要性は、定量的に評価することが難しい（本書付録 F 参照）。これについては、IEC 61608-6［27］の附属書 D に、共通原因故障の 1 つのチャンネルの危険側故障率 $\lambda_d$ に対する割合を $\beta$ x $\lambda_d$ としたいわゆるベータ・ファクタ・モデルが示されている。しかしながら、精確な FMEA なしでは、$\beta$ は実際の SRP/CS についてはあくまでも推定値でしかありえない。ISO 13849-1 では、CCF 対策については、5 点から 25 点で評価される重要な 8 項目を含んだチェックリストが用意されている。

- 異なるチャンネルの信号経路の物理的分離（15 点）
- チャンネルの技術方式、設計、物理原則の多様性（20 点）
- 想定される過負荷に対する保護（15 点）と十分吟味されたコンポーネントの使用（5 点）
- 潜在的共通原因故障を発見するための開発段階での故障モード及び影響解析（5 点）
- CCF とその回避に関する設計者／保守作業者の訓練（5 点）
- 汚染（機械及び流体システム）、電磁妨害（電気システム）により引き起こされる共通原因故障に対する保護（25 点）
- 不適切な環境条件により引き起こされる共通原因故障に対する保護（10 点）

1 つの対策についての評価は、上記の与えられた点数による満点、もしくは 0 点のどちらかになる。また、これらの方策が「半分しか実行されない」場合は、この点数評価の対象にはならない。しかし、もちろんサブシステムレベルでは、さまざまな方策の組合せは効果的だといえる。8 項目すべての対策が実行される場合には、合計点数は最高 100 点になるが、ISO 13849-1 で要求される最低合計点数は 65 点である。CCF 対策はカテゴリ 2、3、4 の SRP/CS にのみ要求されるものであ

る。カテゴリ 2 のシステムの場合には、危険な不具合（障害）が検出されないために発生する可能性のあるテストチャンネル及び機能チャンネルでの共通原因による危険側故障を回避することが重要である。簡易的定量化に用いられる柱状グラフを作成するに当たって、チェックリストによる 65 点は、ベータ・ファクタ 2%以下と同等に扱われた。ここでは、5 つのカテゴリ、3 つないしは 4 つに分類される $MTTF_d$ 及び $DC_{avg}$ 等級と比べても区分がさらに単純化されて、指標値に対して Yes/No の判定しかなされない。冗長構造のメリットは、ベータ・ファクタが 10%の場合にはほとんど完全に抹殺されてしまうことになるが、一方で、ベータ・ファクタが 2%以下であることにより共通原因故障の重要性は許容可能なレベルに低減される。

### 6.2.16　柱状グラフによる PL 決定の簡易的手法

故障確率を算定するための 4 つの主要な定量的パラメータが決定されていても、これにより SRP/CS に関して達成される算出することは決して簡単な作業ではない。基本的には、適切な手法であればどれを採用してもかまわないとされるが、ISO 13849-1 は、安全側に対する複雑な計算及び見積もりをベースにした簡単な図表、いわゆる柱状グラフによる方法を提案している（図 6.10 参照）。

本グラフは、カテゴリに適用される指定のアーキテクチャをベースに、マルコフモデルにより作成されたものである。詳細は、本書付録 G を参照いただきたい。この柱状グラフを適用する場合、まず、達成されるカテゴリと $DC_{avg}$ 等級を組み合わせて、該当する横軸上の柱を指定する。なお、カテゴリ 2、3、4 については、CCF に対する十分な方策がとられていなければならない。そして、選択された柱上の SRP/CS により達成される $MTTF_d$ の高さから該当する PL を縦軸から読み取ることができる。この手法により、精確な定量的データがなくても、達成される PL の定性的見積もりを迅速に行うことができる。例えば PL だけでなく単位時間当たりの平均危険側故障率の正確な値が問われる場合には、本規格の附属書 K にある表を利用することができる。同様に、BGIA ソフトウェア SISTEMA（本書付録 H 参照）を使ってもこの柱状グラフを定量的に分析することができる。

この柱状グラフを作成するに当たっては、指定のアーキテクチャが考慮されただけでなく、本グラフの適用において留意されるべき条件が次のとおり設定された。

- SRP/CS の使命時間は 20 年とし、その間のコンポーネントの信頼性は一定の故障率により説明／見積もられる。ただし、摩耗の激しいコンポーネント（本書付録 D の $T_{10d}$ の値を参照）の使用、あるいは他の理由から、実際の使命時間が 20 年を下回る可能性がある。その場合には、該当するコンポーネントもしくは SRP/CS の交換を予め配慮することにより、柱状グラフの適用は正当化される。これらに関する情報は、使用者情報や SRP/CS への表示等により、使用者に適切に伝える必要がある。
- カテゴリ 2 に対応する柱については、テスト頻度は少なくとも安全機能の平均作動要求頻度の 100 倍を超え、さらに試験機器は少なくとも論理演算機器の半分の信頼性を有することが前提条件とされる（本書付録 E も参照）。