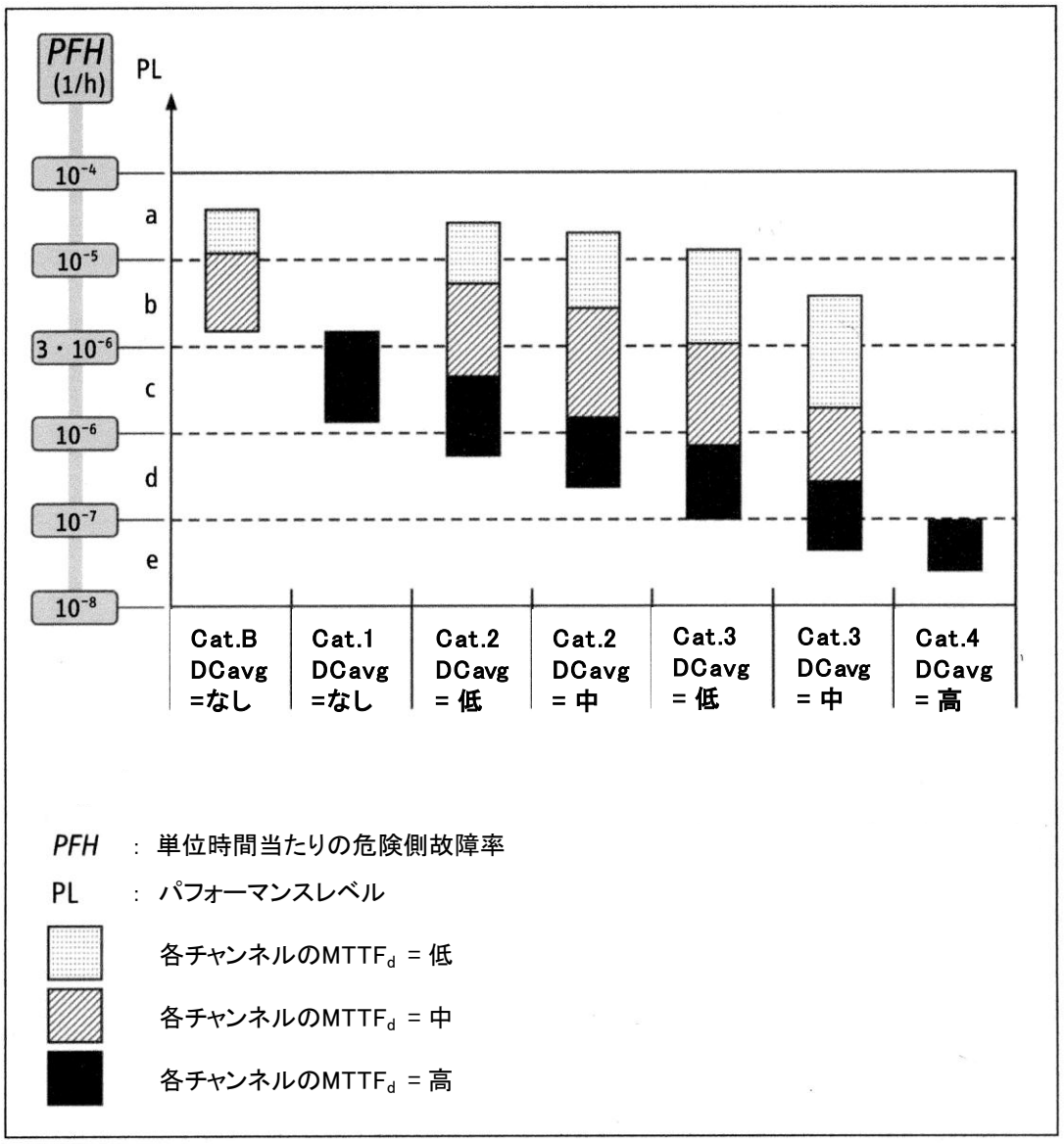

図6.10： PLを決定する簡易的手法：
カテゴリ、CCF対策、DCavg、MTTFdの組合せによる

各チャンネルの評価可能な $MTTF_d$ を 100 年に制限することにより、高い PL は特定のカテゴリでしか達成できないようになっている。これは、指定のアーキテクチャ及び柱状グラフという簡易的アプローチに関係付けられるものであるにもかかわらず、これに関連する制約は、他の手法による単位時間当たりの平均危険側故障率の算定についても適用される。すでに述べたように、いくつかのカテゴリについてはアーキテクチャによる次の制限が適用され、これによりコンポーネントの信頼性が他の影響量と比べて過大評価にならないよう配慮されている。

- カテゴリ B により達成できる PL は最高「b」とする。
- カテゴリ 1 により達成できる PL は最高「c」とする。

- カテゴリ 2 により達成できる PL は最高「d」とする。
- カテゴリ 3 もしくは 4 による場合は、PL「e」も達成可能である。

決められた PL を達成するためには、故障確率の定量的側面以外に、定性的側面にも留意しなければならない。これには系統的故障（本書 6.1.2 参照）と 6.3 で取り上げるソフトウェアの不具合（障害）が含まれる。

6.2.17　バスシステムー「結合方法」

指定のアーキテクチャの個々のブロックとなる「入力」、「論理」、「出力」のユニット間には、論理的関係のみならず、物理的結合が必要である。これについては、本規格ではいわゆる「結合方法」が定義され、SRP/CS の一部分として考察される。結合方法という呼称は、電気あるいは流体技術の専門家にしてみれば一見そぐわないものに映るかもしれないが、これは電気及び流体技術での配線あるいは配管、さらには機械的なプランジャ等に対する上位概念である。本規格のすべての要求事項はこの「結合方法」にも適用される。不具合（障害）の考察という視点からすると、例えば配線短絡は想定される不具合である。しかし、安全関連情報を伝達するバスシステムの使用についてはどのようにとらえればよいだろうか？もちろん、このような複雑なテーマを詳細に解明することは本規格の対象外である。本テーマに関しては、職業保険組合による検査ガイドライン（GS-ET-26［28］）がすでに出されており、また国際規格（IEC 61784-3 の最初の原案［29］）が目下準備中である。これらの出版物に記載される要求事項を満たしたバスシステムならば、ISO 13849-1 との関連でも、何の問題もなく使用することができる。市場にはすでに、安全技術での使用に適したバスシステムが複数出回っている。

上述の出版物の中では、安全関連のデータ伝送のためのブラックボックスチャンネルの使用を考慮するために、特殊な不具合（障害）モデルが使用される。言い換えるならば、これらの伝送ャンネル自体には、例えば不具合（障害）の検出に関する特別な要求は課されない。本モデルでは、不具合（障害）の可能性として、安全関連メッセージの反復、欠損、挿入、誤配列、改ざん、遅延と、安全関連メッセージと非安全関連メッセージの結合が想定される。さらに起こりえる不具合（障害）の局面として、メッセージを正反対にすることによってシステム的にメッセージを間違ったものにしてしまうことが考えられる。制御システムの安全関連部に実装されるいわゆるセーフティレーヤーでの方策により、伝送エラーは十分な確率で排除される。適切な方策には、例えばシーケンス番号、タイムスタンプ、タイムアウト、受信確認、送信元／受信先アドレスの同定、データの完全性の保証が含まれる。特にデータの完全性については、複雑な計算と結びつくことが多い。これを計算する目的は、いわゆる残存エラー確率 R とこれから導かれる残存エラー率 Λ（コンポーネントの低いエラー率 λ から導かれる）を決定することである。そして、この値は、安全関連メッセージの伝送に関与する分として、PL に対して求められる単位時間当たりの平均危険側故障率という視点に含めることができる。上述の 2 つの出版物では、エラー率の値は単位時間当たりの危険側故障率に対して許容される最高値の 1%に制限される。実際に製造者から従来提示されてきた値は SIL（第 3 章参照）に関するものが多いが、現実的にこれらの値は要求 PL に関して使用する場合にも互換性がある（図 3.2 参照）。1%ルールにより、結果的に単位時間当た

りの危険側故障率への貢献はほとんど無視できるものともいえるし、あるいは SRP/CS に関して算出された値に加算してもかまわない。安全関連情報を伝送するバスシステムに関しては文献［30］等で幅広く取り扱われているので、そちらを参照いただきたい。

通常、第三者機関により試験されるバスシステム及びそのコンポーネントが安全機能実現のために使用される場合には、とりわけ障害の回避という視点に基づいた使用計画と適切な実施が非常に重要になる。数多くのパラメータを設定しなければならず、このプロセスには、多かれ少なかれ、付属ツールによるサポートが必要になる。

6.3　安全関連ソフトウェアの開発

「長年の経験を有するソフトウェアプログラマはミスなどしない」というようなことばをよく耳にすることがある。しかし、これこそが、人が犯しえる最大のミスともいうべき自己過信である。ソフトウェアは一般的に複雑なものであり、このためソフトウェアエラーによる故障の数はハードウェアと比較しても増加する傾向にある。周辺機器が機能しなくなってしまい、それがドライバなど別のソフトウェアとの互換性がないソフトウェアの一部により生じたケースがいかに多いことか愕然とする「PC パワーユーザ」は少なくないだろう。これに比べると、ハードウェア障害は滅多に発生するものではない。文献［31］によれば、単純な機能に対応する単純なソフトウェアでは、コード行数 1,000 当たりおおよそ 25 のエラーがあるとされる。優れたソフトウェアの場合は、同文献によると、コード行数 1,000 当たり 2 つ 3 つ程度になり、さらにスペースシャトルで使用されるソフトウェアの場合には（NASA によると）10,000 行当たり 1 未満である。これを実際の例で見てみると、最高 200,000 のコード行数をもつ携帯電話機の場合には、最高 600 のソフトウェアエラーがあることになる。また、PC のオペレーティングシステムに 2,700 万のコード行数が含まれる場合には最高 50,000、スペースシャトルの例では最高 300、そして戦略防衛構想 SDI 向ソフトウェアでは最高 10,000 になる。こうしたエラーは製品の中に潜伏して、特定の条件及び特定の状況下で製品機能に働きかけてくる。代替技術がないため、ソフトウェアの負う責任はこれまで以上に大きく、これはプログラマについても同様のことがいえる。

EN 954-1 の適用範囲にすでに含まれているプログラマブル SRP/CS に、ソフトウェア及び開発に関する要求事項がはじめて具備されたことは、改訂 ISO 13849-1 における主要変更の一つである。まず明確にしておきたいのは、本規格の 4.6 の要求事項により、機械分野のすべての SRP/CS 及び「a」から「e」までのすべての要求パフォーマンスレベルの安全関連ソフトウェアを開発することが可能だということである。本項 4.6 は、プログラマブルロジックコントローラ（PLC）等でアプリケーション指向の言語を使って機械のための安全機能を開発するアプリケーションプログラマを主対象としている。逆に、SRESW（Safety-Related Embedded Software、安全関連の組込みソフトウェア）、つまりファームウェアあるいは電子的安全コンポーネント用のソフトウェアツールの開発者にとっては、ISO 13849-1 のこの要求事項は特に目新しいものではない。一般的に、認証済みのコンポーネント用「組込みソフトウェア」の開発は、IEC の安全基本規格 IEC 61508-3［32］（及び他 7 つのパート）による非常に複雑な要求事項に基づいて行われることが多い。

本項の基本的な考え方は、両タイプのソフトウェアに適用することができる。しかし、個々の要

求事項は、どちらかといえば SRASW（Safety-Related Application Software、安全関連のアプリケーションソフトウェア）のアプリケーションプログラマに向けた具体的な記載となっている。一方、本章 6.5 の断裁機の制御システムの例では、SRESW の開発を取り上げた。

ソフトウェア開発を管理するための要求事項は、使用されるソフトウェアタイプ（SRASW もしくは SRESW）と言語のタイプにより異なる。ソフトウェアの要求事項を含む他の現行規格同様、言語タイプは FVL（Full Variability Language、無制約可変言語）と LVL（Limited Variability Language、制約可変言語）に区別される。一般的に、SRASE は IEC 61131-3 で定義されるグラフィック言語等の LVL でプログラミングされる。これについては、ISO 13849-1 の 4.6.3 による要求事項が該当する。

しかし、SRASW が FVL（例えば一般的によく使われる C 言語を使った PLC）でプログラミングされるとなると、同規格の 4.6.2 の SRESW に関する要求事項を満たす必要が出てくる。このようなケースで、SRASW がパフォーマンスレベル「e」を達成しなければならない場合について、ISO 13849-1 の 4.6.2 では最後に一度だけ例外的に、IEC 61508-3:1998 の要求事項の参照を指示している。

6.3.1 エラーのないソフトウェア・・・

エラーの発生しないソフトウェアというのは、現実には残念ながら存在しない。ソフトウェアの障害はハードウェアの場合とは異なり、偶発的コンポーネント故障により発生するものではなく、系統的原因を有する。それだけにいっそう、リスク低減への貢献が求められる安全関連ソフトウェアを開発する際には、エラーを回避するために適切とされる方策をすべてとる必要がある。適切とされる方策は、要求パフォーマンスレベル PL_r により決定される。その一方で、運転中に故障を引き起こすまで検出されないままでいる、破壊的な作用を伴った安全に関わる障害がソフト開発の特にどのフェーズで紛れ込みやすいかは、よく知られている。それは、仕様、設計、変更のフェーズである。そのため、ISO 13849-1 の要求事項並びに本節での解説も、特にこれらのフェーズでの障害回避に重点が置かれている。残念ながら、実情としては、アプリケーションプログラミングのこれらのフェーズにあまり注意が払われないケースが多い。

安全関連ソフトウェアにおいて高い品質を獲得するためには、最新かつ実績のある「ソフトウェアエンジニアリング」開発モデルを導入することが不可欠である。安全関連システムの場合には、いわゆる「V-モデル」が引き合いに出されることが多い［32］。本文献によりよく知られた V-モデルは、本来は非常に複雑なソフトウェアに対して使用されるものであるが、ISO 13849-1 の 4.6.1 ではこの開発モデルは簡易化された形でしか要求されない（図 6.11 参照）。この簡易化は、機械分野の安全関連 SRP/CS の条件や特にそこでの SRASW の開発に関して、実用的かつ客観性のあるものとして評価できる。V-モデルの本質的な目的は、読みやすい、理解しやすい、試験しやすい、かつ保守しやすいソフトウェアを作成することにある。これらの要求事項は、通常、安全関連ソフトウェアを作成することのないプログラマにとっては骨の折れる仕事だと思われがちだが、一方で、プログラマはこれにより十分に適切なソフトウェアを開発したという確証を得ることができる。

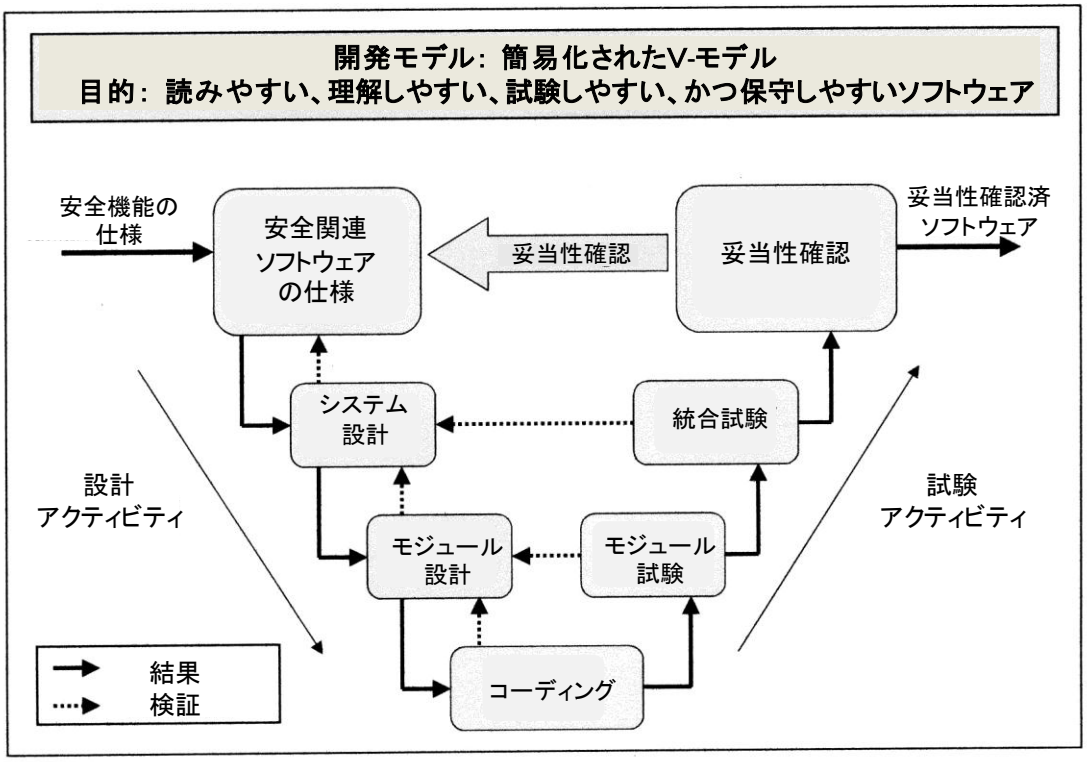

図6.11: 安全関連ソフトウェア開発のための簡易化されたV-モデル

図 6.11 にはフェーズの名称以外にも重要な用語が示されているので、まずこれらの（ソフトウェアに関しての）意味について説明する。

結果
各フェーズで作成されたもの、例えば仕様書、設計文書、コード、そして最終的結果として試験により妥当性が確認されたソフトウェア等をいう。しかし、ソフトウェアの妥当性確認を体系的に行うための試験計画書など、仕様フェーズの結果でありながらも、かなり後のフェーズにおいてはじめて必要とされるものもある。直前及びそれ以前の結果は、次のフェーズのインプットとして使用される。このことは矢印により示される。

検証
あるフェーズの結果がその前のフェーズの仕様に合致しているかどうかを試験する、品質を保証するためのアクティビティをいう。例えばコーディングフェーズの途中あるいは最後では、作成されたコードが定義されたモジュール設計を実装しているか、そしてプログラミング・ガイドラインが順守されているかどうかが検証される。

妥当性確認
ソフトウェアの妥当性確認は、ここでは、ソフトウェア全体に対して最終的に行われる特別な検証をいう。ソフトウェアの機能性に対するソフトウェア仕様書の要求事項が実装されているかどうかが試験される。

次に、簡易化した V-モデルのいくつかのフェーズと、それと同時にソフトウェア開発に関する「ロードマップ」について説明する。この開発モデル「V」の左側（降り）は設計、右側（昇り）は試験に関するアクティビティを表わす。

6.3.2 ソフトウェア仕様書 － 全体の安全性に通じるインターフェース

SPR/CS の安全機能の上位の仕様書をベースに、その中でソフトウェアにより実現しなければならない下位機能が文書で示される。また、例えば次の事項に関しても記載される。

- ハードウェアの障害を検出し、抑制する機能
- 最大応答時間等の性能特性
- 障害時の反応
- 別のシステムに接続するためのインターフェースの装備

こうした機能的な要求事項以外に、安全機能により達成すべき PL、つまり PL_r を示し、これにより障害を回避するために必要な方策（後の説明を参照）を選択できるようにする。

この仕様書（「安全関連ソフトウェアの要求仕様書」ともいう）は、例えばその作成に関与しない者によるレビューにより、検証されなければならない。検証により、第一に本要求仕様書が上位の仕様書に合致していること、第二にソフトウェア仕様書の書き方、つまり形式に関する要求事項が満たされていることを確認しなければならない。本仕様書には、後で行う妥当性確認のためのチェックリストとしても使用できるような構成と詳細が求められる。

機械及び機械設備の全体の安全性は、制御システムのすべての安全関連部及びそれらの機能（あらゆる技術方式のコンポーネント、電子機器、ソフトウェア）により保証される。従って、機械及び機械設備に関する安全性を説明するものとして仕様書の作成は不可欠である。文書は何百ページにも及ぶものである必要はなく、重要なポイントに限定されたものであってよい。わかりやすい形式で記載されていることが大切である。機械及び機械設備全体の仕様に従って、プログラマの作業量が決定される。ソフトウェア仕様書は全体のコンセプトの一部であり、このため「下請け業者」であるプログラマとの「契約書」としてとらえることができる。

ソフトウェア仕様書では、まず、ソフトウェアの設計及びコーディングに関する規定を定める。ソフトウェアでの機能の実装は、安全性に関わる他の構成要素から信頼されるに足るものでなければならない。このため、仕様書は、ソフトウェアの受け入れに関しても重要なベースになる。ソフトウェア機能の妥当性確認により、「契約」が履行されたかどうかを示さなければならない。これは、SRASW の分野では、まさしく文字通りの意味をなす。制御システムのエンジニアリング及びプログラミングは、全体の安全性に責任を負う立場の者により、他の企業あるいは事業部署に割り当てられるからである。この場合、仕様書には、外部あるいは内部の職務遂行者に対して契約的拘束力をもったインターフェースとしての役割も求められる。

6.3.3 「安全関連技術仕様書」に関するシステム設計及びモジュール設計

ソフトウェアアーキテクチャは、一般的に、オペレーティングシステムあるいは開発ツールによりすでに確定されている。設計では、さらに、仕様書で定義された安全機能を、どのような構造で、どのようなモジュールにより実現するべきかを決定する。どの既存のライブラリ機能を使用するか、また、場合によってはプロジェクト特有の新しい機能を開発する必要があるかどうかも判断しなければならない。本節で使われるソフトウェア機能及びソフトウェアモジュールという用語も常にファンクションブロックを意味するものである。

ソフトウェア設計文書は、ソフトウェアの構築及びプロセスを、ダイアグラムを用いて、外部の人間に対しても理解しやすいように記述することが要求される。プログラムが、すでに妥当性が確認され、別のどこかで文書化されているソフトウェア機能に基づくものであるほど、設計文書はコンパクトになりえる。モジュール設計では、さらに、そのプロジェクト専用に新たに作成されるソフトウェア機能及びそれに必要なインターフェースやモジュール試験のためのテストケースが明確にされる。あまり複雑ではない SRP/CS の場合には、システム設計とモジュール設計は 1 つの「安全関連ソフトウェア技術仕様書」にまとめることができる。

6.3.4 プログラミング　－　「V」の頂点

プログラマが喜ぶのは、ついに本来のコーディングの作業フェーズにたどり着いたときである。障害の回避という視点から、ここでは特に次の 3 つの点に注意する必要がある。

- 読みやすく、理解しやすいコードを書くこと。これにより、後で試験がしやすく、モディフィケーションでのエラーを防ぐことができる。強制力のあるプログラミング・ガイドラインを使用すれば、プログラムの適切なコメントや、わかりやすい変数名及びモジュール名を指定することができる。
- 防衛的プログラミング、すなわち、常に内部もしくは外部のエラーを想定し、これを検出すること。例えば、入力信号の時間的挙動がわかっていれば、これを予測するアプローチにより周辺回路の障害を検出することができる。有限状態マシンがプログラミングされる場合には、状態変数は有効な値域にあるか監視される。
- コードは静的に、つまり実行せずに解析されなければならない。低レベルの PL に関しては、コードレビューで十分であるが、PL「d」及び「e」については、データ及び制御フローも、できればツールを使用して試験されることが求められる。基本的な質問（例）：コードは、過去のソフトウェア設計と一致しているか？低レベルの PL の信号（例えば標準 PLC から）が高レベルの PL の信号に勝るポイントがあるか？どこで、そしてどのモジュールにより変数が初期化され、記述され、そして安全出力に割り当てられるか？どのソフトウェア機能が条件付きで実行されるか？

6.3.5 モジュール試験、統合試験及び妥当性確認 ― 急いては事を仕損じる

モジュール試験では、プロジェクト専用に新規に開発されたソフトウェア機能の試験及びシミュレーションを実施し、これがモジュール設計で指定されたとおりにコーディングされているか確認される。遅くとも統合試験において、例えば機械の PLC の基本動作の確認時に、ソフトウェア全体がハードウェア上で正しく動作するか（統合）、そしてシステム設計と一致しているか（検証）が試験される。両者ともまだ検証の域にある。つまり、ここでは、ソフトウェアの中身を調査しているということである。ソフトウェアによる安全関連のサブファンクションが指定されたように機能するかどうかは、すでに説明したように、ソフトウェアの妥当性確認により決定される。高レベルの PL「d」及び「e」については、広範囲にわたる機能試験が必要になる。

認証済み、あるいは品質保証対策によりすでに妥当性が確認された個々のソフトウェア機能については、再度検証する必要はない。しかし、特定のプロジェクト用に、こうした機能を複数組み合わせて安全関連のサブファンクションを実現する場合には、その妥当性を確認しなければならない。認証済みのモジュールでも、誤ったパラメータ及び誤ったロジックにより危険な系統的故障につながる可能性がある。

6.3.6 規格要求事項の構造

開発プロセスの見取り図が描けたので、次にソフトウェア自体と、使用される開発ツール並びに開発アクティビティに関する規格の要求事項について説明する。これらの要求事項も、障害の回避に貢献するものである。これに係る労力は、プログラマブル SRP/CS のハードウェアの場合と同様、それぞれ必要なリスク低減に見合ったものが要求される。このため、要求事項及びその効果は PL_r に比例して高まっていく。しかし、これに関して、ISO 13849-1 はあえて最大限の要求事項を規定することはしていない。これは、PL とは関係なく、ソフトウェア全般について、そうせざるを得ないというのが実情である。

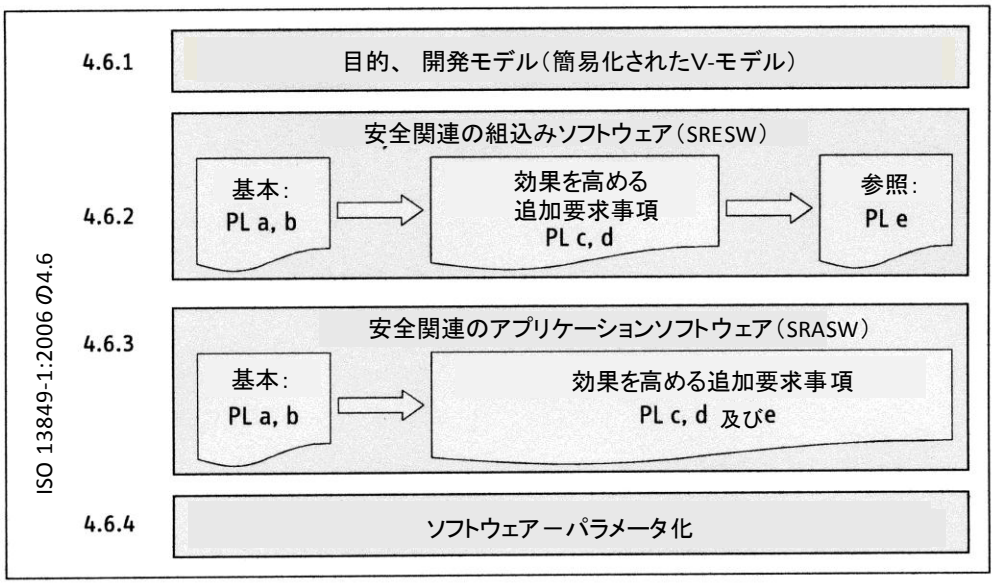

図6.12: 安全関連ソフトウェアに関する要求事項の等級付け

図 6.12 には、SRASW と SRESW の双方において、すべての PL に適用される適切な基本方策がそれぞれパッケージ化されていることが示されている。PL「a」もしくは「b」に対するソフトウェア開発に関しては、この基本方策だけで十分に対応できる。しかし、PL「c」から「e」の SRP/CS で使用されるソフトウェアについては、この基本方策以外にも、障害を回避するための追加方策が適用される。この追加方策は、PL「c」に対しては「低い」、PL「d」に対しては「中くらい」、そして PL「e」に対して「高い」効果を有するものが要求される。ソフトウェアが、任意のカテゴリの 1 つのチャンネルのみで、あるいは 2 つのチャンネルで作用するかどうかは問題にはならない。つまりこれらの要求事項に対して基準となるのは常に、実現される安全機能の PL_r だということである。

「より高い効果」というのは、障害を回避するレベルが高くなることをいう。このことは、仕様書の重要なアクティビティで説明しておくべきである。プログラマ自らが仕様書を作成し、他のプログラマがそれをレビュー（内部レビュー）するという手順は、例えば PL「c」に関するものであれば、特に差し支えはないと思われる。しかし、同じソフトウェアが PL「e」に使用されるとなると、達成すべき障害回避レベルはもっと高くなる。この場合は、仕様書は、プログラマ自身ではなく、例えば「ソフトウェアのプロジェクトマネージャ」によって書かれるべきである。また、仕様書のレビューも、プログラマだけでなくハードウェアエンジニア等の第三者も立ち会って、いっしょに行うことが望ましい。一般的には、人数が多いほど、多くのミスを発見できるものである。残念ながら、本 BGIA レポートでは、この要求事項の詳細やその効果の度合いまで論じ尽くすことはできない。このため、次のようないくつかの特別なケースについてのみ言及するにとどめる。

- 1 つの SRP/CS の統合ソフトウェアが、指定される PL_r がそれぞれ異なる複数の SFx（例：SF1 と SF2 が PL_r「c」で、SF3 が PL_r「e」）を実現するケースは少なくない。しかし、開発ライフサイクル、ツールあるいはアクティビティ（例えばモディフィケーションにおける）の効果において、PL_r の違いにより安全機能を区別することは、実際にはほとんど不可能である。そのため、このような場合には、障害回避のための要求事項は最も高い PL_r（この例では「e」）に合わせるものとする。

- 冗長構造の SRP/CS で、1 つのチャンネルのみがプログラミング可能な場合：つまり、プログラマブル電子システムが 1 つのチャンネルにしかなくても、全体の構造はカテゴリ 3 もしくは 4 に相当する場合、このカテゴリでは「d」あるいは「e」といった高い PL_r の安全機能が実現されることが多い。これに従って、ソフトウェアに関しても、最も高い PL_r の要求事項がこの 1 つのチャンネルに適用される（本書 6.3.10 参照）。

- 標準 PLC を使用する場合：本書の回路例（第 8 章、85 ページ参照）では、安全関連制御システムが、原理的には標準 PLC によっても構築できることが示されている。ただし、PL「e」に関しては、診断範囲が SRASW により実現されなければならない場合は、PLC のハードウェアが高い診断範囲（DC は最低でも 99%）を達成することは非常にむずかしい。PL「a」から「d」については、標準 PLC に関する要求事項は本書 6.3.10 で説明される。さらに、アプリケーションプログラマは、SRASW における障害回避のための要求事項（規格の 4.6.1 及び 4.6.3）を PL_r に応じて実施しなければならない。

- 多様性を採用した SRESW 場合の特例：PL_r「e」の安全機能に対する 2 チャンネル構造の SRP/CS では、両チャンネルの SRESW はそれぞれ別個に実装することができる。この多様性の度合いが大きい場合、つまりコーディング、設計、さらには仕様もそれぞれ異なって作成された場合には、このソフトウェアを ISO 13849-1 の PL「d」に関する要求事項に従って開発することもできる。この場合、SRP/CS のハードウェアチャンネルがそれぞれ異なったものであるか、あるいは 2 つとも同じであるかは、さしたる問題ではない。

6.3.7 適切なソフトウェアツール

ツールなしにはソフトウェアは作成できない：これは特に安全関連ソフトウェアについていえることである。このため、こうしたツールの選択及び品質は、障害の回避及びこれによる安全機能のレベルを決定付ける重要なファクタである。ISO 13849-1 では、次の 4 つの要素が強調されている。

- 開発ツール：
  開発には、適切かつその使用に関して実績のあるツールが要求される。SRASW については、安全コンポーネントに対し認証されたツールを使用するのが一般的である。意味論的エラーの回避及び検出、言語サブセットの順守、あるいはプログラミング・ガイドラインの監視等の機能により、プログラマは骨の折れる作業から解放され、ソフトウェアの品質を高めることができる。

- ソフトウェアライブラリ：
  システム設計では、既存の、あるいは提供されたライブラリを考慮して、妥当性がすでに確認された機能が実用的なものである限りは、それを使用するべきである。つまり、プログラムが、すでに妥当性が確認され、さらには認証された機能に基づいたものであれば、検査部門や外部機関による、あるいは独自に実施するプロジェクト専用のソフトウェアコンポーネントの妥当性確認は少なくてすむ。システムインテグレータには、反復される典型的な機能に関しては適切なユニット／モジュールを ISO 13849-1 に従って必要な労力を投じて自らが開発すること、そしてこれらが第三者からも規則通りにエラーが生じることなく繰り返し使用されえるもの、あるいはテスト可能なものであることが、十分に忠告されている。個々のライブラリ機能についても、仕様書、設計、試験計画、妥当性確認等が要求される。

- 適切なプログラミング言語
  SRASW に関しては、例えば IEC 61131-3［33］に従って、アプリケーション指向の言語が推奨される。この言語自体がすでに必要以上に広範なものであり、部分的にエラーを起こしやすい構造を含む。このため、プログラマは、その構文を限定して使用するべきである。一般的には、対応する言語のサブセットはツールにより指定される。

- プログラミング・ガイドライン
  ソフトウェア機能をコーディングするに当たっては、適切なプログラミング・ガイドラインに注意する必要がある［34, 35］。このガイドラインは、世間一般に認められた機関により承認される現行の規則でなければならない。企業自らが適切なプログラミング規則を作成するということも、その規則が実質的、あるいは理論的に確立されたものであるならば、選択肢

として認められる。プログラミング・ガイドラインには、重要な言語構造の使用、ソフトウェア機能の範囲とインターフェース、コードのフォーマットとコメント、機能及び変数の識別名等に関する規則が定められる。

これらのツール及びガイドラインは、設計文書で指示すべきである。

6.3.8 文書化と構成管理 ― やりたくない・・・、しかし重要である

製造者は、機械に対する EC 適合宣言書を発行する前に、技術文書を仕上げなければならない。安全関連ソフトウェアに関しては、まず、実現される安全機能の仕様書（要求仕様書）、設計文書（技術文書）並びに十分なコメントがあるプログラムが挙げられる。さらに、認証済みの、もしくは自らが妥当性確認を行った使用したライブラリ機能を、その識別情報（バージョン番号、作成者、日付等）と共にリスト化する必要がある。独自のプログラミング・ガイドライン及び言語サブセットの適用についても同様に文書化しなければならない。ツールにこれらがすでに含まれている場合には、それがわかるように適切に注記すれば十分である。さらに試験アクティビティに関する文書化が必要である。統合試験と安全機能の妥当性確認は、同時に実行されることが多い。これらの試験については当然ながら計画を立て、そして試験結果と共に文書化する必要がある。

構成管理とはどのようなことをいうのか？安全関連ソフトウェアの場合には特に、その開発が、関与するすべての人あるいは団体にとって、そして後で行われる試験のために透明性のあるものでなければならないのは明らかであり、構成管理はこれを要求するものといえる。

- だれが、いつ、仕様を定め、プログラミングし、指示し、検証し、妥当性を確認したか？
- 何を使って開発したか？例えば、ツール及びその設定、再利用した機能とそれらのアイデンティティ、プログラミング・ガイドライン等。
- どのプログラムバージョンがどの SRP/CS にロードされているか？

これらの要求事項をはじめ、さらに必要な情報並びに重要な開発文書は、例えば 5 年間使用した後にモディフィケーションを行う場合など先々での利用を念頭に置いて文書化し、保管する必要がある。

6.3.9 モディフィケーション ― ソフトウェアは常に流動的

経験からすると、すでに試験された SRASW でも、設備や機械の立ち上げ段階でさらに拡張や適合のための作業が続出する。この手続きが「モディフィケーション」と呼ばれるものである。モディフィケーションの規模が広がり、コーディングだけでなく、元々の仕様書が適切でなくなる場合も多い。こうなると、根本的な見直しが必要になってくる。設備や機械のある側面の安全機能の変更が、別の、さしあたって変更されない安全機能にも関わってくる可能性もある。あるいは、モディフィケーションにより安全コンセプトに亀裂が生じるかもしれない。こうした可能性をチェックする必要があり、これは V-モデルの必要なフェーズを繰り返し実行することを意味する。

しかし、実際のところ、すでに据え付けられた機械や機械設備でも、非常停止装置や保護扉を追加しなければならないケースはよくある。そして、加工プロセスも頻繁に最適化される。つまり、安全コンセプトもそれに合わせて修正されるということである。既存のソフトウェアには「モディフィケーション」は必然である。ただし、次のようなことに注意しなければならない。例えば、すでに長いことソフトウェアエラーによる故障もなく使用されてきた SRP/CS について言えば、実は「隠れた」エラーが存在し、単にまだその影響が出ていないだけなのかもしれない。しかし、モディフィケーションにより例えばソフトウェアが適切に構造化されず、そのために個々のモジュールや機能が互いに作用しない場合には、その状況が変化する可能性がある。

こうした状況の説明には、マーフィの法則がよく利用される。すなわち、次のように言い換えることができる。「このプログラムは何年も前に書かれたもので、最初にこれを書いたプログラマは現在、緊急を要する他の仕事を抱えている、あるいはすでに別の企業で働いているとする。もし、このソフトウェアが最初に述べた特性、つまり、読みやすさ、構造、わかりやすさを有し、さらに、当初の担当プログラマには依存せずにエラーを起こしにくいように簡単にモディフィケーションを行えるものならば、このケースは、機械あるいは機械設備の安全性と経済性の両方の利益に適ったものといえる」。

原則的に、モディフィケーションを行った後は、開発手順、つまり V-モデル（図 6.11 参照）の該当するフェーズを繰り返す必要がある。

例：

- コーディングを変更した場合には、モジュール試験、統合試験並びに妥当性確認を再度実施する。
- さらに仕様書も変更しなければならなかった場合には、例えば同僚がレビュー（読み合わせ）を行い、再度検証して、仕様書の別の箇所にエラーが紛れ込まないようにする。従って、すべての開発及び検証に関する方策並びに該当する安全機能の妥当性確認を再度繰り返す必要がある。

このような手順を踏むのは、モディフィケーションの安全機能に及ぼす影響を体系的に調査し、文書化するためであるのは言うまでもない。モディフィケーションは安全機能の適切な実行に大きく作用しえるため、早期の段階で、責任者の指名も含め適切な手順を決定しておくべきである。

6.3.10 SRP/CS における標準コンポーネント・ソフトウェアに関する要求事項

安全関連制御システムは、産業用途の標準コンポーネントにより実行されることが多い。規格では、SRESW 及び SRASW の実装に関する要求事項が的確に述べられているので、これらは、電子的にプログラム可能な標準コンポーネントに関しても実施される必要がある。しかしながら、検定済みの安全コンポーネントとは違って、制約がある。次のカテゴリ及びパフォーマンスレベル（PL）には、電子的にプログラム可能な標準コンポーネントを使用することはできない。

- カテゴリ 1：規格により除外。
- カテゴリ 4 及び PL「e」は、要求される診断範囲 DC が「高」であるため、標準コンポーネン

トを使用した場合は、一般的には達成することができない。個々のケースについては、それぞれ評価する必要がある。

SRESW に関する要求事項

考慮される標準コンポーネントはすべて、産業用途向けに開発されたものでなければならない。SRESW（ファームウェア、オペレーティングシステム）には、少なくとも PL「a」と「b」に関する基本方策が適用される。適用される大部分のケースでは、これを証明するために、次のいずれかの方法がとられる。

- 基本方策を実行したという、コンポーネント製造者による確認
- 品質保証プロセス（ISO 900x に準拠）に則った開発が、関連の製品規格（PLC に関する IEC 61131-2 等）に従って行われたという、コンポーネント製造者による明示。これは大部分の標準コンポーネントに対し適用される。

表 6.5： 標準コンポーネントの SRESW に関する要求事項

No.	PL	カテゴリ、冗長性	SRESW
1	a b	カテゴリ B、2、3	PL「a」及び「b」に適用される方策。選択肢は次の 2 つ： 1) 製造者による確認。 2) 関連の製品規格にしたがった、品質保証システムに則った開発が行われたことを明示。この場合は、ISO 13849-1 による要求事項の順守に関する製造者証明は不要。
2	c d	カテゴリ 2 と 3 の 2 つのチャンネルに対する 2 つのコンポーネント 多様性をもつ SRESW、もしくは多様性をもつ技術	SRESW もしくは技術の多様性による特例。PL「a」及び「b」に対する方策が適用される。選択肢は次の 2 つ： 1) 製造者による確認。 2) 関連の製品規格にしたがった、品質保証システムに則った開発が行われたことを明示。この場合は、ISO 13849-1 による要求事項の順守に関する製造者証明は不要。
3	c d	カテゴリ 2 と 3 の 2 つのチャンネルに対する 2 つのコンポーネント 同種の SRESW	多様性による特例はなし。PL「a」及び「b」に対する方策と PL「c」及び「d」に対する追加方策が適用される。ISO 13849-1 による要求事項の順守に関する製造者証明が必要。

いくつかの箇所では、「多様性をもつ SRESW」が前提条件となる。次の場合に、2 つのコンポーネントの SRESW は「多様性をもつ」とされる。

- 2 つの異なる製造者による異なったオペレーティングシステムをもつ異なったコンポーネント。
  もしくは、
- 同じ製造者の異なる製品シリーズによる異なるコンポーネント。これに関しては、製造者により、これらのコンポーネントの違いが SRESW において明白であることが確認される必要がある。例 1：1 つのコンポーネントはコンパクトな PLC（例：16 ビット CPU、独自のオペレー

ティングシステム）で、もう 1 つはモジュール型 PLC（例：32 ビット CPU、組込み用 Windows）。
例 2：1 つの PLC と、1 つのプログラム可能な切り替えリレー。

製造者が多様性を確認しない限り、他のすべてのケース（2 つの同一の PLC、あるいは同じ製造者の同じ製品シリーズによる 2 つの類似した PLC）では、2 つのコンポーネントの SRESW は多様性をもたない、つまり同種のものとして見なされる。必要な DC を達成することが必要な場合は、製造者はさらに、SRESW で実行される障害を検出／抑制する方策の DC を確認しなければならない。コンポーネントの $MTTF_d$ は、当然ながら、製造者から提供される基本データに含まれるべきものである。

別の技術方式との組合せによるカテゴリ 2 もしくは 3 で標準コンポーネントのみが使用される場合、並びに各チャンネルに対し多様性のある標準コンポーネントが使用される場合には、SRESW での系統的障害による危険側故障の確率がかなり小さいため、要求は引き下げられる。表 6.5 は、各種の組合せ及び SRESW に関する要求事項がどのように実施されるかを示したものである。

SRESW に関する要求事項をまとめると、SRP/CS における電子的にプログラム可能な標準コンポーネントの使用については、次のとおり判断される。

- PL「e」は、現在の最高技術レベルでは、ソフトウェアベースの標準コンポーネントの実装により達成することは、一般的にはできない。
- PL「c」と「d」は、多様性をもつ SRESW、もしくは 2 つのチャンネルの多様性をもつ技術方式の場合には、SRESW に関する要求を引き下げて実現することができる。本規格では、多様性の効果について明確に述べられてはいないが、その有用性は一般的に認められるところであり、予定される IEC 61508 の第 2 版でも同じような記述になるであろう。
- PL「a」と「b」は適切な標準コンポーネントにより実現することができる。

SRASW に関する要求事項

SRASW に関する要求事項は、プログラミング可能な標準コンポーネントを含むサブシステムで達成すべき PL に対応する。多様冗長構造で、1 つのチャンネルの標準コンポーネントが別のチャンネルの別の技術方式（例えば流体技術）と共に使用される場合には、SRASW での系統的障害による危険側故障の確率がかなり小さいため、SRASW に関する PL の要求は 1 ランク引き下げられる（例えば PL「d」から「c」）。

6.4 サブシステムとしての SRP/CS の組合せ

本章では、これまで、1 つのパフォーマンスレベルをもつ 1 つのカテゴリ／指定のアーキテクチャに描くことのできる全体システムとしての SRP/CS に関してのみ取り上げてきた。この場合、安全機能は、作動事象の開始から安全状態の達成に至るまですべて、1 つの制御システムだけで実行される。しかし、実際には、それぞれが安全機能の一部を実行するサブシステムであるいくつか

の SRP/CS を直列に配置しなければならないケースが多い。これらのサブシステムは、それぞれ異なる技術方式で構築され、かつ／または異なるカテゴリ及びパフォーマンスレベルを実現する場合もある。図 6.13 に示される、駆動レベル（例えばカテゴリ 1 の油圧技術）と、センサレベル及び論理レベル（例えばカテゴリ 3 の電子技術）での異なる技術方式の使用、あるいはライトグリッド、電子式制御装置、空気圧式バルブ等の調達機器の結合は頻繁に見られる例である。カテゴリを超えた PL コンセプトの大きなメリットの 1 つは、カテゴリが異なってもパフォーマンスレベルが似通ったサブシステムを組み合わせて、カテゴリの混在する 1 つの全体システムを形成し、全体の PL を決定できる点にある。実際に考えられるいくつかのシステム構成を次に説明する。

- 1 つのカテゴリの全体の制御システム。サブシステムではないもの。：このケースには、これまでに述べてきた指定のアーキテクチャなどに関する説明が当てはまる。
- 1 つのカテゴリの下位制御システム／サブシステム：このケースにも、これまでに述べてきた指定のアーキテクチャ等に関する説明が当てはまる。しかしながら、安全機能への関与と、安全機能を完全に実行するために別のサブシステムに接続させることのできるインターフェースに関して、精確に定義する必要がある（下記参照）。
- サブシステム（例えば異なるカテゴリ）の直列配置：サブシステムの特性値（PL、単位時間当たりの平均危険側故障率）から全体システムの PL を算定する方法は、以下に説明される。この場合も、安全機能への関与とインターフェースの精確な定義に注意する必要がある。
- サブシステムの並列配置や、全体の制御システムの 1 つのチャンネルでのみサブシステムが使用される場合など、特殊なケースの取り扱い。

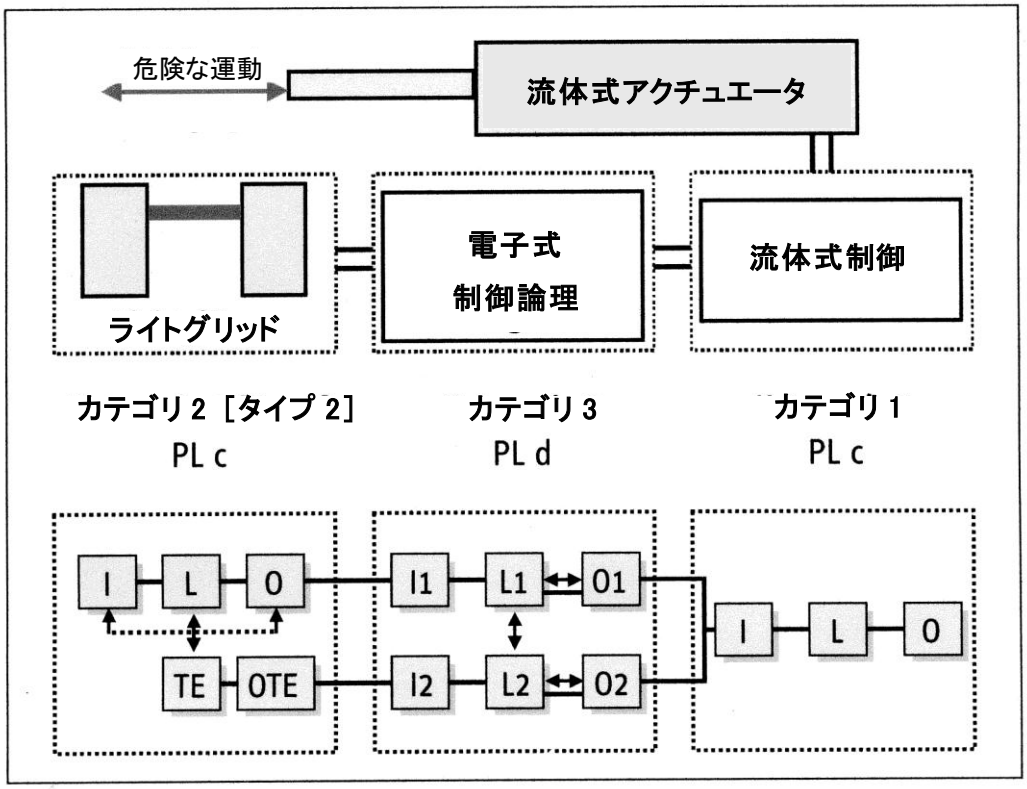

図6.13: 1つの安全機能を実行するためのサブシステムの直列配置

技術方式も異なる複数のサブシステムの直列配置について、図 6.13 に典型的な例を示す。ここでは、ライトグリッド、電子式制御装置及び空気圧式バルブが結合されて、全体で、安全機能（光線遮断時の危険な動作の停止）を実行する。空気圧式シリンダ自体は制御要素ではないので、PL 評価の対象にはならない。

1 つのチェーンの強度は常に、そのもっとも弱い構成要素の強度になる。このルールは、異なったカテゴリだけでなく、異なったパフォーマンスレベルの制御要素の結合に関しても適用される。実際の使用で確認されているように、カテゴリ 1 の液圧式制御システムはコンポーネントの $MTTF_d$ が高いため、その安全性は、DC_{avg}「中」で $MTTF_d$「低」のカテゴリ 3 の電子コンポーネントに匹敵する場合もある。$MTTF_d$ 及び DC_{avg} によるカテゴリへのプラスあるいはマイナスの付加価値は PL ですでに考慮されているため、組合せに関する PL は、個々のカテゴリではなく、直列配置における最も低い PL の出現頻度（数）に対応したものになる。制御要素の数と共に全体の故障確率も増加するため、例えばサブシステムの直列配置において、最も低い PL をもつ構成要素の数が 3 つを超える場合には、システム全体の PL は最も低いサブシステムの PL に比べてさらに 1 ランク低いものになりえる。サブシステムの PL をベースに達成される全体の PL を大まかに見積る方法として、次の ISO 13849-1 の手法が使用される。

- まず、直列に配置されるすべてのサブシステムの中で最も低い PL を確認する。これを PL_{low} とする。
- 次に、その PL_{low} がサブシステムの直列配置にいくつ存在するか確認する。この数を N_{low} とする。
- そして、表 6.6 に従って、PL_{low} と N_{low} から全体の PL を決定する。

表 6.6：サブシステムが直列配置されているときの PL の決定
－簡易的手法－

PL_{low}	N_{low}	全体の PL
a	≧4	なし、許可されない
	≦3	a
b	≧3	
	≦2	b
c	≧3	
	≦2	c
d	≧4	
	≦3	d
e	≧4	
	≦3	**e**

この簡易的手法は、サブシステムについて PL だけがわかっていて、そのベースになる単位時間当たりの平均危険側故障率が出されていない場合に、全体の PL を決定するのに利用することができる。ここでは、サブシステムに関して、故障確率はそれぞれの PL_{low} に適用される範囲のちょうど中間の値が近似値としてみなされる。

逆に、すべてのサブシステムに関して単位時間当たりの平均危険側故障率の値が出されている場合（IEC 61508［12］あるいは IEC 62061［13］による SIL 及び故障確率に関する値も適切とされる）には、加算して、全体の PL に関連する値が算出される。

$$PFH_{total} = \sum_{i=1}^{N} PFH_i = PFH_1 + PFH_2 + \ldots + PFH_N \qquad (5)$$

N = 安全機能に関与するサブシステムの数

PFHi =i 番目のサブシステムの単位時間当たりの平均危険側故障率

すべてのサブシステムの PL は、最低でも常に全体の PL と同じであるため、サブシステムの組合せでは、定量化することのできない、定性的な側面に対するすべての方策（系統的故障やソフトウェア等）が十分考慮されていることも保証される。しかしながら、ここでは、特にサブシステム間のインターフェースに注意する必要がある。

- すべての接続（コンダクタやバスシステムによるデータ通信等）は、そこに含まれるサブシステムの 1 つの PL ですでに考慮されていなければならない。もしくは、これらの接続の不具合（障害）は除外されるか、あるいは無視できるものでなければならない。
- 直列に配置されるサブシステムとそれらのインターフェースは適合したものでなければならない。つまり、安全機能の作動を指示するサブシステムの出力状態は、それ以降のサブシステムの安全状態を開始する作動事象として適切なものでなければならない。

2 チャンネルシステムを直列に配置して、サブシステムの PFH 値が加算される場合には、非安全側に対する計算エラーが生じる可能性はかなり少ない。厳密にいえば、1 つめのサブシステムの 2 つの出力は、2 つめのサブシステムの入力に組み合わせて読み取られ、比較される必要がある。しかしながら、入力情報の組合せによる二重化は、すでに入力レベルで内部的に実装されることが多い。余分なケーブル敷設作業を回避するために、PHF 値を加算する際に、PFH をやや低めに見積もっても差し支えない。

これまでに説明してきた規則に従って、サブシステムは、ISO 13849-1 改訂前のカテゴリベースによる場合と比べ、はるかに柔軟に組み合わせることができる。これらのサブシステムは、技術方式やカテゴリ等に関する特性が非常に異なる場合もあり、PL ではなく SIL をベースとした他の機械制御の安全関連部に関する規格に従って開発することもできる（図 3.2 参照）。

サブシステムの結合では、2 チャンネルと（テストされる）1 チャンネルの部分を入れ替えることもできる。図 6.14 は、2 チャンネルの入力及び出力要素に接続されている論理のサブシステム（例えば安全 PLC）の例を示したものである。安全関連ブロックダイアグラムですでにハードウェアレベルの抽象化が行われているので、サブシステムの順番は原理的に入れ替えが可能である。このため、図 6.14 に示すように、同じ構造のサブシステムをまとめることが推奨される。これにより、PL の決定はより簡単になり、また例えば 1 チャンネルの $MTTF_d$ を 100 年に制限する切り捨てを何度も行うといった余分な作業を回避することができる。

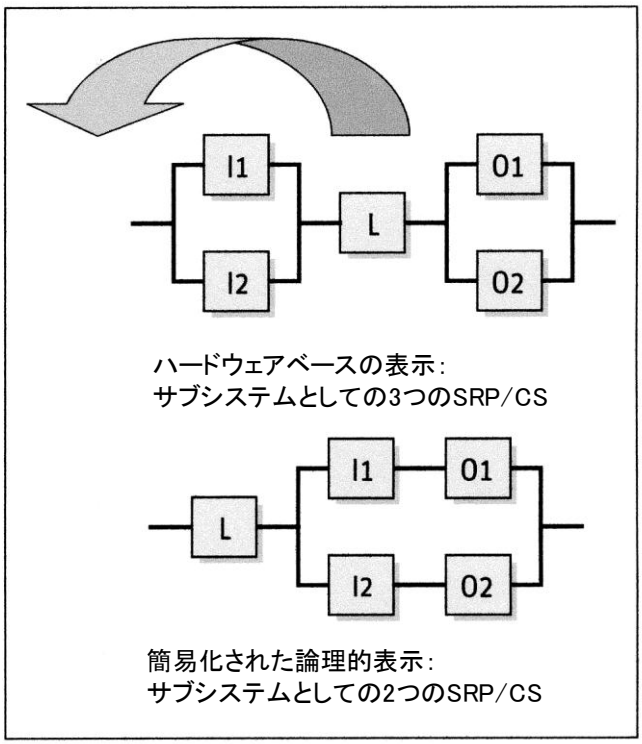

図6.14: 安全関連ブロックダイアグラムでのサブシステムの組み直し

しかし、現段階でも、非常に大まかな規則しか与えられていない特殊なケースが残っている。その一つが、サブステムの並列配置に関するものである。これについては、定量化できる側面（不具合（障害）の検出が欠けているので、カテゴリ 1 を 2 つ並べてもカテゴリ 3 にはならない）に関しても、また定性的な側面（系統的故障、ソフトウェア、共通原因故障等）に関しても、簡単な、一般的に適用される規則を策定することはできない。このため、全体システムの再評価が唯一の解決策になる。場合によっては、個々の中間結果（各ブロックの $MTTF_d$ や DC 等）を有効に利用できる可能性もある。

さらに特殊なケースとして、すでに 1 つの PL（もしくは SIL）あるいは単位時間当たりの平均危険側故障率が与えられたいくつかのサブシステムを、1 つの SRP/CS のブロックとして統合する場合が挙げられる。ここでは、サブシステムの内部構造を考慮せずに、大まかなルールとして、単位時間当たりの平均危険側故障率の逆数が、そのブロックに関する $MTTF_d$ として採用される。内部で実行されるサブシステムの診断方策のいくつかはすでに故障確率で考慮されているので、ブロ

ックの DC に関しては､外部からサブシステムに作用する追加の診断方策のみを考えればよいといえる。

さらにこれと関連して、単位時間当たりの平均危険側故障確率のデータしか与えられていないサブシムから実現された全体システムに関するカテゴリの分類が、問題になる。ここでは、内部構造に関するデータ以外に、カテゴリに応じた最小要求事項に当たる各チャンネルの $MTTF_d$ と DC_{avg} も欠けている。このため、並列配置の場合と同じことがいえる。つまり、非常に大まかに見積もる方法は唯一、可能であれば中間結果を利用して再評価するというものである。

6.5 PL の決定

例：論理制御システムに多様冗長性を採用した断裁機（カテゴリ 4－PL「e」）

本節では、一般的な説明と共に、実際に PL を決定する方法を例示する。ここで示す具体例は同時に、第 8 章への架け橋になる。第 8 章では、さまざまな PL、カテゴリ及び技術方式による回路例が数多く示される。

本節で用いられるグレーボックスの内容は、第 8 章の同スタイルで記載される箇所の要約である。その他に、第 8 章の各回路例の枠内にはおさまらない部分について説明を加える。

6.5.1 安全機能

ここでは、第 5 章の 5.7 に示した断裁機の制御例を再び使用する。すでに特定された 7 つの安全機能のうち、要求パフォーマンスレベル PL_r が「e」と決定された SF2 を例に、この実装（技術的実現）について説明する。いくつかの異なる安全機能に対し同じコンポーネントが使用される場合もあるので、実装するに当たってはすべての安全機能を考慮する必要がある。例えば、断裁機に関する製品規格 EN 1010-3 では、操作側（オペレータ）の保護に関して、両手操作制御装置（THC）に加え、例えば安全機能 SF3 を考慮した非接触式保護装置（ここでは示されていない）の使用が要求される。

安全機能（SF2）：
- 危険な運動が行われる間、オペレータの手を危険区域外に拘束する。

6.5.2 実装（技術的実現）

この安全機能は、両手操作制御装置により実現する場合、次のように説明できる。「2 つの手動制御器 S1 と S2 のうちどちらか 1 つでも解除されると、プレスクランプ及びカッターの危険な運動は中断され、カッターもプレスクランプもばね力により始動位置に戻る。再起動は、2 つの手動制御器が解除されて、両手操作制御装置により新たなサイクルが開始されるまで、阻止される。」オペレータの手を拘束するために 2 つの手動制御器が使用され、機械を起動させるためにはこれ

らを同時に操作する必要がある（偽操作防止等に関する詳細は EN 574 を参照 ）。電気信号は時間的及び論理的に評価されなければならず、これについてはプログラマブル電子システムが使用される。一般的には、これにより、プレスクランプやカッターの運動も制御される。この場合、必要とされるエネルギーが高いため、油圧式駆動が用いられる。第 5 章（5.3.2 を参照）で説明されるように、プレスクランプとカッターは共に同じ危険区域に存在するので、この 2 つのアクチュエータは安全機能に含まれる。図 6.15（68 ページ）は、安全関連の制御コンポーネントが具体的にどのように実装されるかを示した電気油圧式のシステム構成図である。第 8 章でも基本のシステム構成図として採用される本図は、概観及び概念を示すことを目的としているため、当然ながら、多くの詳細部分は除外されている。プロセス内の機械の動作に必要な大部分の機能的な制御コンポーネント以外に、保護回路（ヒューズ、EMC）あるいは「周辺機器」（電源、論理部のためのクロック信号等）のような個々の安全関連の要素も省略されている。検出されない不具合（障害）の累積に対する単一不具合（障害）耐性（フォールトトレランス）が不可欠なため、実際には、1 つのチャンネルの不具合をもった入力がもう 1 つのチャンネルにも影響を及ぼさないようにするために、例えば 2 つの論理チャンネルの結合された入力を分離する要素が必要になる。このため、このシステム構成図は、模倣して使用するための雛型ではなく、あくまで安全関連の構造を示すものとして理解していただきたい。

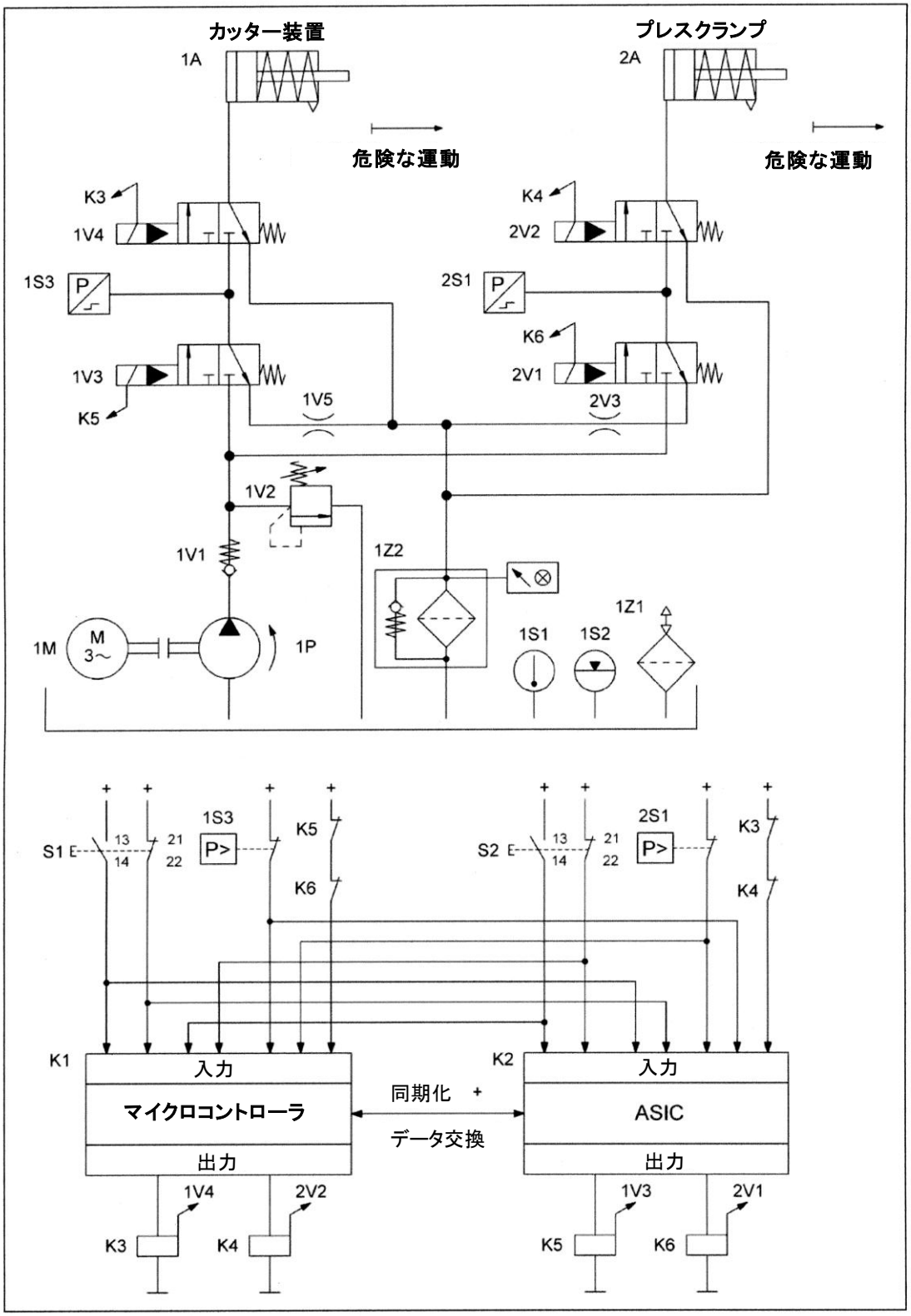

図6.15： システム構成図　－油圧式カッター装置と油圧式プレスクランプの電子的駆動システム－

6.5.3 機能の説明

このシステム構成図を理解するためには、回路構造と信号経路の説明が必要である。これにより、安全機能が実行されるとき（異なるチャンネルで実行される場合もある）のプロセスと実装される診断方策が認識できるようにする。

機能の説明：

- 両手操作制御装置の手動制御器 S1 と S2 の操作により、プレスクランプとカッターの危険な運動（処理サイクル）が開始する。このサイクルの間に両手操作制御装置の手動制御器が 1 つでも解除される、あるいは制御システムが予期しない信号変化が機械の周辺機器で発生した場合には、サイクルは中断され、機械は安全な状態に移行する。
- 手動制御器 S1 と S2 を押すことで、信号の立ち上がりエッジが 2 つの処理チャンネル K1（マイクロコントローラ）と K2（ASIC）に送り込まれる。この信号が関連規格 EN 574 による同時性を満たす場合には、2 つの処理チャンネルは適切な切断要求を出力する（電磁リレー　K3 から K6）。
- 2 つの処理チャンネルは同期動作し、また周期的信号処理の中間状態を互いに評価し合う。設定された中間状態と異なると、機械は停止する。1 つの処理チャンネルはマイクロコントローラ K1 により、そしてもう 1 つのチャンネルは ASIC K2 により構成される。K1 及び K2 により、運転中にバックグラウンドで自己診断が実行される。
- 手動制御器 S1/S2 と電磁リレー　K3 から K6（強制ガイド式バックチェック機能付き）における不具合（障害）は処理チャンネルでのクロスチェックにより検出される。
- 圧力スイッチ 1S3 と 2S1 によりバルブ 1V3／1V4 及び 2V1／2V2 の故障が検出される。
- バルブの故障、もしくは 1V4 あるいは 2V2 の開放状態の凝着は、油圧シリンダの復帰速度が非常に低下することにより検出される。この状況は、制御技術による圧力信号の適切な評価（圧力降下時間）によっても検出可能である。
- バルブの故障、もしくは 1V3 あるいは 2V1 の開放状態の凝着は、圧力スイッチ 1S3 及び 2S1 の信号変化の監視により直接、検出される。凝着が生じた場合には、圧力がかかっていないにもかかわらず、圧力を示す信号が出されるからである。
- 機械の状態はすべて、2 つの処理チャンネルにより監視される。切断サイクルの周期性により、すべてのシステム状態も周期的に発生するため、不具合（障害）を発見することができる。

6.5.4 安全関連ブロックダイアグラム

回路図に関連する回路装置の説明と、必要であればさらに別の文書（詳細な仕様書）により、制御カテゴリを決定し、実際の回路を抽象化された安全関連ブロックダイアグラムに図示することができる（図 6.16 参照）。本例では、安全機能が 2 チャンネル構造で実行されることは一目瞭然なので、カテゴリ 3 あるいは 4 が考察対象になる。さらに、不具合（障害）の組合せを抑制する高レベルの診断方策がとられるため、カテゴリ 4 が妥当だということが容易にわかる。この具体的な検証は第 7 章の妥当性確認のフェーズで行われ、$MTTF_d$、DC_{avg} 及び CCF に関する定量的な要求事項についてもチェックされる（以下参照）。安全関連ダイアグラムに置き換える際には、本章 6.2.8 及び 6.2.9 の説明に注意していただきたい。「危険な運動はどのようにして駆動され、そして阻止されるか？」をよく考えながら、アクチュエータ側を起点に、論理部を経て、終点となるセンサまでの信号経路を追跡する手順も、実績のある適切な方法である。本例では、手動制御器 S1 と S2 は冗長関係にはないことに注意が必要である。一見そのように見えても、この 2 つの押ボタンは、それぞれ独自にオペレータの片手を保護するものである。むしろ、各押ボタン内の電気的ノーマリクローズ（b 接点）とノーマリオープン（a 接点）の組合せにより冗長系がスタートするといえる。各制御チャンネルは、両手／両手動制御器を、各手動制御器の少なくとも 1 つのスイッチ接点の評価により監視する。このため、安全関連ブロックダイアグラムでは、各チャンネルに 1 つの a 接点（例：S1/13-14）と b 接点（例：S2/21-22）が含まれる。安全指向のブロックダイアグラムは、この点で、機能的な回路図とは明らかに異なる。

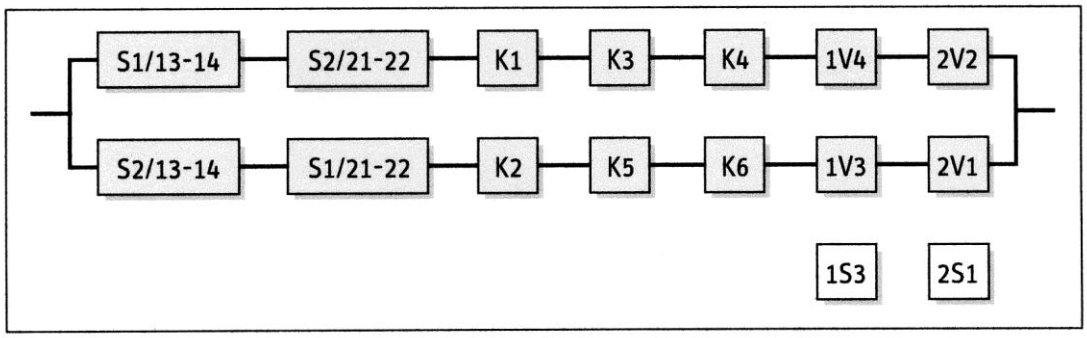

図6.16： 安全関連ブロックダイアグラム
例：断裁機での安全機能SF2に対するSRP/CS

安全機能の具体的実現により、適用に関する制約あるいは推奨が出てくる場合がある。例えば運転プロセスによる不具合（障害）の検出の効果は、当然ながら、その用途と密接に関係してくる。

注：
- 例：断裁機への適用（EN 1010-3）

6.5.5　達成される PL の定量的評価に関する入力変数

この時点では、達成される PL の評価に関するあらゆる基本情報が利用できる。カテゴリ及び安全関連ブロックダイアグラムの知識により、個々のブロックに関してまず $MTTF_d$ と DC を決定し、さらに採用された冗長系に関する CCF 対策を評価することができる。その後に、各チャンネルの $MTTF_d$、DC_{avg}、そして最終的に L を決定するための「計算」ステップが続く。

故障確率の算定：

- $MTTF_d$：年間の運転日数が 240 日で、1 日当たりの運転時間は 8 時間、サイクルタイムは 80 秒とした場合、n_{op} は年間 86,400 サイクルとなる。S1 と S2 並びに K3 から K6 に関しては、$B10_d$ 値が 2,000,000 サイクル［M］の場合、$MTTF_d$ は 232 年になる。マイクロコントローラ単体については、$MTTF_d$ は 1,142 年と算出される［D］。ASIC についても同じ値が用いられる。関連する回路構成要素を合わせて、ブロック K1 と K2 の $MTTF_d$ はそれぞれ 806 年になる。バルブ 1V3、1V4、2V1、2V2 の $MTTF_d$ はそれぞれ 150 年［S］とみなされる。これらの値から、各チャンネルの $MTTF_d$ は 31.4 年（「高」）になる。
- DC_{avg}：ISO 13849-1 の附属書 E に従って、S1／S2 の DC 値は 99%（頻繁な信号変化の動的テストを除く、入力信号の相互監視）、K1／K2 は 90%（ソフトウェアと相互監視による自己診断）、K3 から K6 は 99%（強制ガイド式接点による直接監視）、1V3／2V1 は 99%（圧力センサによる間接監視）、そして 1V4／2V2 は 99%（圧力降下時間の計測による間接監視）になる。これらの値から DC_{avg} は 98.6%（「高」）になる。
- 共通原因故障に対する十分な方策（65 点）：分離（15 点）、過負荷等に対する保護（15 点）、環境条件への耐性（25 点＋10 点）
- 制御要素の組合せは、各チャンネルの $MTTF_d$ が「高」（31.4 年）で、診断範囲「高」の DC_{avg} = 98.6%を有するカテゴリ 4 に相当する。これにより単位時間当たりの平均危険側故障確率は 9.7×10^{-8} になる。これは PL「e」に相当する。

$MTTF_d$ の算定について説明するために、まず、ブロック「K1」を考察する。システム構成図（図 6.15）にはマイクロコントローラしか示されていないが、このブロックにはさらに実際の機能に必要な要素（水晶振動子等）が含まれている。その危険側故障により、関連するチャンネルの安全機能の実行が阻止される可能性のある要素はすべて考慮しなければならない。これには、通常、減結合、バックチェック、EMC、過負荷に対する保護のための安全上重要な信号経路のすべての要素が含まれる。これらの要素は、一般的に、基本的及び十分吟味された安全原則において、あるいは DC の達成のために必要なものである。図 B.2（207 ページ参照）には、さらに簡単な例を用いて、このアプローチが示されている。要素の $MTTF_d$ をベースにブロックの $MTTF_d$ を算出するための表を使った簡易的手法として、表 6.7 の「部品点数法」が挙げられる（209 ページの図 B.3 には、故障モード及び影響解析の手法との比較が示される）。

表 6.7：ブロック K1「マイクロコントローラ」に適用される「部品点数法」
データベース SN 29500［36］から引用した故障率 λ がベースになる　（1 FIT = 1 x 10^{-9}/時間）

コンポーネント	故障率 λ SN 29500 による［FIT］	数	全体の故障率 λ ［FIT］	全体の危険側故障率 λ_d ［FIT］	年数表示による $MTTF_d$ 全体の危険側故障率 λ_d の逆数
金属皮膜抵抗器	0.2	7	1.4	0.7	163,079
コンデンサ、極性なし	1	4	4	2	57,078
汎用ダイオード	1	3	3	1.5	76,104
バイポーラ出力のオプトカプラ	15	2	30	15	7,610
マイクロコントローラ	200	1	200	100	1,142
水晶振動子	15	1	15	7.5	15,221
低消費電力バイポーラトランジスタ	20	1	20	10	11,416
プラスチックシール型補助リレー	10	1	10	5	22,831
「マイクロコントローラ」ブロック K1 に対する合計				141.7 FIT →	806 年

2 列目に記載される要素の故障率は、データベース（**D**atabase）SN 29500［35］を使用して算出された。これは、「故障確率の計算」では略称「D」で表わされる（本書 7.6 参照）。妥当性確認については、本書 7.6 で、引き続き本例を用いて詳しく説明される。同じ要素が何度も出現する可能性がある（3 列目）ため、4 列目には各要素タイプに対する全体の故障率が示されている。故障率の半分のみを危険側とする一般的近似により、5 列目の数値は 4 列目の数値の半分になる。単純合計により、最終的に、ブロック K1 に関する全体の危険側故障率が算出される。6 列目には関連する $MTTF_d$ 値が年数表示で示されている。これは危険側故障率（5 列目の数値を時間から年に換算した数値）の逆数になる。ブロック K1 については、この値は丸めると 806 年になる。使用されたデータバンクでは、マイクロコントローラと ASIC について同じ故障率が示されており、また回路は類似したものであるため、ブロック K2 についても 806 年という同じ $MTTF_d$ 値が当てはまる。

ブロック S1／S2 と K3 から K6 については、製造者のデータ（**M**anufacturers' data、略称「M」）が使用される。信頼性データは S1／S2 全体（動作機構＋b 接点**及び** a 接点）についてしか用意されていないため、各チャンネルでは動作機構以外には a 接点（例：S1／13-14）**又は** b 接点（例：S2／21-22）しか考慮されないが、それでもこれらの値は各チャンネルに関する危険側の見積りとして用いることができる。提供された B_{10d} 値は、本書付録 D に示される公式により $MTTF_d$ に換算することができる。

$$n_{op} = \frac{d_{op} \times h_{op}}{t_{cycle}} \times 3{,}600 \frac{s}{h} = \frac{240 \text{ days/year} \times 8 \text{ h/day}}{80 \text{ s/cycle}} \times 3{,}600 \frac{s}{h} = 86{,}400 \frac{\text{cycles}}{\text{year}} \quad (6)$$

$$MTTF_d = \frac{B_{10d}}{0.1 \times n_{op}} = \frac{2{,}000{,}000 \text{ cycles}}{0.1 \times 86{,}400 \text{ cycles/year}} = 231.5 \text{ years} \quad (7)$$

電気機械式コンポーネントの使用時間はいわゆる T_{10d} 値（考察されるコンポーネントの 10%が危険側故障を起こすまでの平均時間）に制限される。しかし、ここでは、この T_{10d} 値は前提とされる 20 年という使命時間を上回るので、これ以降の計算には関係しない。

$$T_{10d} = \frac{B_{10d}}{n_{op}} = \frac{2{,}000{,}000 \text{ cycles}}{86{,}400 \text{ cycles}} = 23.15 \text{ years} \quad (8)$$

バルブ 1V3、1V4、2V1 及び 2V2 に関する $MTTF_d$ 値は、本規格に記載された実用性にすぐれた技術的手法（**S**tandard、略称「S」）により算出することができる。ただし、この場合、本手法で前提とされる条件に合致している必要がある。

1 つのチャンネル（S1、S2、K1、K3、K4、1V4、2V2）に関する $MTTF_d$ は、本章の 6.2.13 に従って合計すると 31.4 年、つまり「高」と決定される。

$$\frac{1}{MTTF_d} = \frac{1}{232 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{806 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{150 \text{ years}} + \frac{1}{150 \text{ years}}$$
$$= \frac{1}{31.4 \text{ years}} \quad (9)$$

2 つめのチャンネルも同じ $MTTF_d$ になるため、通常必要な対称化の手順は省略される。

想定された DC 値の妥当性確認についても、詳しくは第 7 章で説明する。K1 及び K2 については、例えばコンピュータシステムに要求される可変メモリ及び不変メモリと処理ユニットに対する特別な方策を含む、ソフトウェアと相互監視による高レベルの自己診断が実行される。合計すると、この SRP/CS に関する DC_{avg} は、本章 6.2.14 の手順に従って 98.6%となる。許容誤差を 5%と考えれば、この値は「高」の範囲にある。

$$DC_{avg} = \frac{2 \times \left(\frac{99\%}{232 \text{ years}} + \frac{99\%}{232 \text{ years}} + \frac{90\%}{806 \text{ years}} + \frac{99\%}{232 \text{ years}} + \frac{99\%}{232 \text{ years}} + \frac{99\%}{150 \text{ years}} + \frac{99\%}{150 \text{ years}} \right)}{2 \times \left(\frac{1}{232 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{806 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{232 \text{ years}} + \frac{1}{150 \text{ years}} + \frac{1}{150 \text{ years}} \right)} = 98.6\% \quad (10)$$

本書 70 ページの左上のグレーボックスに記載された共通原因故障（CCF）対策は、一般的にわかりやすいものである。この妥当性確認についても、第 7 章で説明する。また、電気式サブシステムでは「多様性」の方策、そして液圧式サブシステムでは「十分吟味されたコンポーネント」の影響が考慮される。これについては本書付録 F を参照いただきたい。CCF、DC_{avg}「高」及び $MTTF_d$「高」に関する要求事項を満たすことで、カテゴリ 4 に対する定量的要求事項も達成される。

6.5.6　PL 決定のための定量的アプローチ

定量化できる側面をベースとした PL の決定まで、あと一歩である。カテゴリ、DC_{avg} 及び $MTTF_d$ の結果から、柱状グラフを使って PL「e」が達成されることが確認される（図 6.17 参照）。規格の附属書 K の表の値、あるいはこれに基づく BGIA の PLC ディスク（Performance Level Calculator）［16］からは次の結果が出される。

カテゴリ	CCF	DC_{avg}	$MTTF_d$	単位時間当たりの平均危険側故障率
4	OK	「高」	「高」 （丸めると 30 年）	9.54×10^{-8}/時間 （PL「e」）

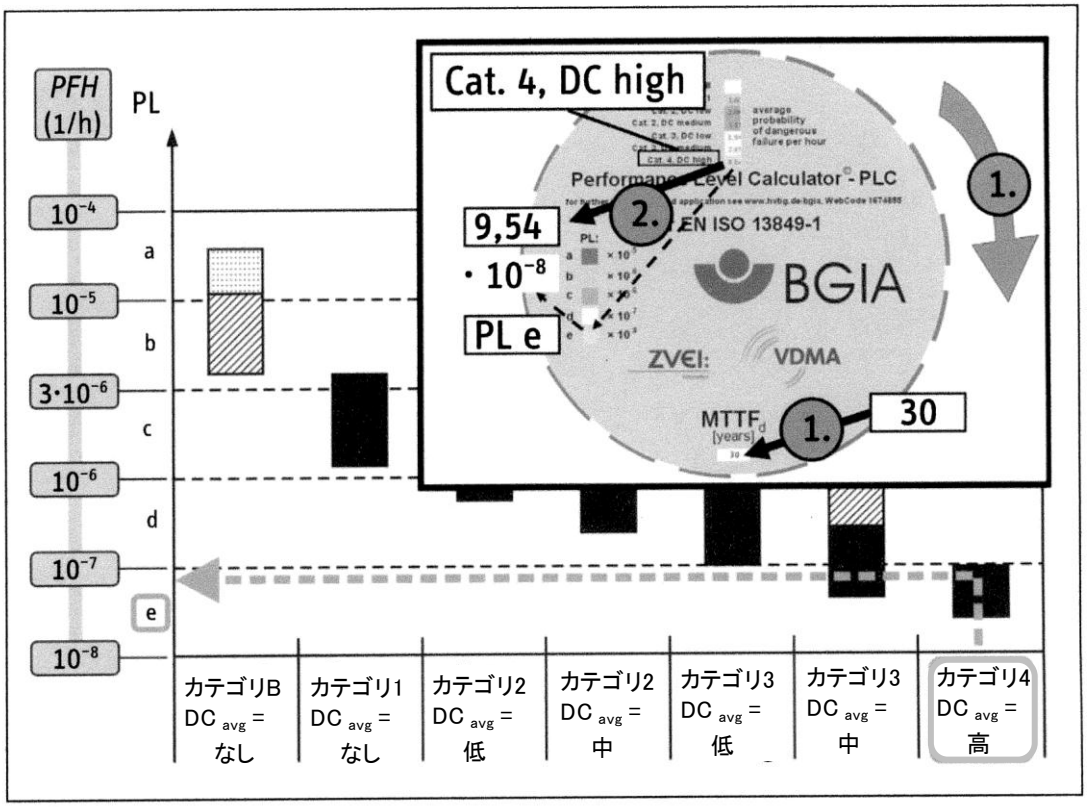

図6.17：　柱状グラフを用いたPLの決定

BGIA から無料で提供されるソフトウェア SISTEMA（本書付録 H 参照）は、管理、文書化及びあらゆる中間結果の算定において非常に便利に利用できる。SISTEMA により、これまで述べてきた PL を決定するための定量的要求事項はすべて簡単に処理され、PL の算定を含めたすべての計算ステップが自動的に行われる。特別なオプションとして、精確な DC_{avg} と $MTTF_d$ の値による算定が可能である。この場合、DC_{avg} に関しては、DC_{avg}「高」に対する許容誤差を 5%とし、かつ丸められた値である 99%を用いる代わりに（DC 及び $MTTF_d$ における許容誤差については、本規格の表 5 と 6 の注記 2 を参照)、98.6%という精確な（ここではより低い）値で計算される。許容範囲内にあってもカテゴリ 4 に対する 99%という指標を下回るため、SISTEMA からは、当然ながら警告メッセージが出される。一方、31.4 年という精確な $MTTF_d$ 値による計算は、$MTTF_d$「高」に対する 30 年という丸められた値を用いたときと比べて、若干ながらも上方修正をもたらすことになる。この結果、単位時間当たりの平均危険側故障率は 9.7×10^{-8}/時間になる。これは、上述の計算値とほとんど差異はない。

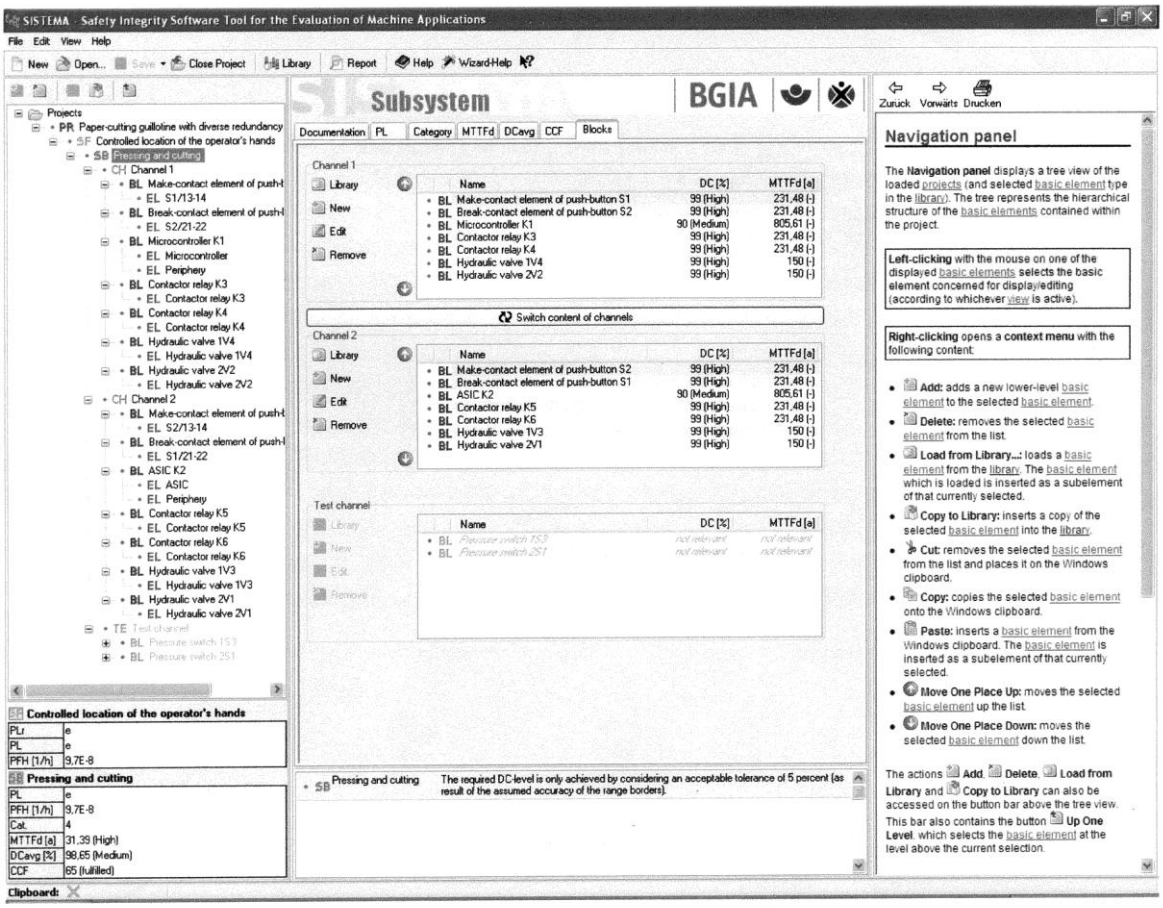

図6.18： SISTEMAによるPLの決定

次に、PL の決定において定量化できない、定性的な側面の評価について説明する。まず、系統的故障を取り上げる。

6.5.7 系統的故障

本例に関して選択された制御システムのレイアウトでは、論理制御システムに多様性手法が用いられると共に、系統的故障の影響に対して最も効果的な方策が使用される。一連の実装では、当然ながら、電圧降下、電圧変動、過電圧、不足電圧等の影響を抑制するために、さらに別の方策を実施しなければならない。必要とされる方策のうち、特に次のものについては、選択されたレイアウト設計で明白に示されている。

- ノーマルクローズ原理の使用：エネルギーがない状態では作動信号は発生しえないことが保証される（例：断線時)。
- 自動診断による故障検出 : 2 つの制御チャンネルで、それぞれ異なったテストが実行される。これにより、早期に不具合（故障）を検出でき、かつそれぞれが隣接チャンネルに依存することなく独自に安全状態を開始することができる。
- 冗長ハードウェアによるテスト：構造的多様性を用いて、さらに個々のチャンネルで異なる作用を引き起こす環境影響による不具合（障害）を抑制することができる。
- 強制ガイド式接点をもつ電磁リレーの使用：対応する接点の状態検知（バックチェック）により、電磁リレーの危険側故障及び場合によっては回路コンポーネントの危険側故障も検出することができる。
- プログラム・シーケンスの監視：マイクロコントローラのチャンネルのプログラム・シーケンスを監視するために、例えば ASIC が使用される。

系統的故障については、以下に示すように、一つは用途、もう一つはレイアウト設計のプロセスに関して特に注意する必要がある。

- 断裁機の油圧システムの設計では、紙屑のたまりを考慮しなければならない。例えば紙屑による油圧油の汚染により、断裁機の安全機能が損なわれる可能性がある。このため、特に圧力媒体の十分なろ過に注意が必要である。さらに、ピストン棒のスクレーパリングやタンクの通気フィルタ等により、紙屑の油圧システムへの侵入を阻止しなければならない。
- 規格草案 IEC 61508-2:2006 の ASIC 開発のライフサイクルにしたがった、ASIC 開発時の不具合（障害）を回避する方策。本規格草案では、ASIC の開発に関して、ソフトウェア開発でよく知られた V-モデルに準拠した V-モデルが規定されている。

6.5.8 人間工学的視点

本例には、使用者と制御システムとの間の仲立ちとなる安全関連インターフェースが 1 つ存在する。すなわち、手動制御器 S1 と S2 を備えた両手操作制御装置（THC）である。これについては、いくつかの人間工学的側面を考慮することにより、意図された使用及び合理的に予見可能な誤使用において、オペレータが、直接的要因あるいはネガティブな作業負荷の連続により危険にさら

されることがないようにしなければならない。大部分の機械に関しては、こうしたユーザインターフェースのチェックは、BG インフォメーション 5048「人間工学的視点による機械設計」の第 1 部及び第 2 部［23］を利用して行うことができる。本例では、特に次の側面が考慮される。

- オペレータに対する手動制御器の高さ及び位置
- 通常の操作場所における手の到達範囲と脚まわり
- 操作作業に適した配置と危険区域外での接近性のよさ
- THC の操作位置からの断裁プロセスの監視性
- 手動制御器の最小距離と形状（EN 574 の規定を考慮した人間工学的設計）
- 余計な力を使わないで行える容易な操作と、設計的方策による意図しない操作の回避
- 押ボタンのロバストな設計並びに適切な表示及び色
- 偽操作及び動作拘束の無効化を阻止する THC の設計

6.5.9 ソフトウェア、特に SRESW に関する要求事項

次に、マイクロコントローラ K1 の安全関連ファームウェアの実装について説明する。このソフトウェアは PL_r「e」に対応する組込みソフトウェア（SRESW）である。論理制御システムに対する多様性指向のアプローチ、つまり 2 つめのチャンネルに ASIC を用いることにより、規格の 4.6.2 の注釈「カテゴリ 3 もしくは 4 の SRP/CS の 2 つのチャンネルに対して、仕様、レイアウト設計、コーディングに多様性が採用される場合には、PL_r「e」は、PL_r「c」あるいは「d」に対する前述の方策により達成することができる」に従って、要求事項のランクを引き下げることができる。

ファームウェアに関する開発プロセスは、図 6.11 の V-モデルをベースにして、認定された製造者の品質マネジメントシステムに組み込まれる。全体の安全関連制御システムの仕様書をベースに、まずファームウェアに関するソフトウェア安全要求事項仕様書、つまり要求仕様書が書かれる。このドキュメントには、機械の安全機能へのファームウェアの関与、つまり、K1 に関し要求される応答時間、不具合（障害）検出時の反応、他のサブシステムに対するインターフェース、運転モードへの依存性等が記載される。さらに、規格の 6.3.2 に従って、PL「c」もしくは「d」に対して要求される不具合（障害）を回避する方策がすべて定められる。この仕様書については、「安全プロジェクトマネージャー」（あるいはこれに該当する立場の者）によるレビューが実施され、必要に応じて修正が加えられる。仕様書が承認されてはじめて、システム設計が開始される。

ソフトウェアアーキテクチャ：マイクロコントローラにはオペレーティングシステムが指定されない。その代わりに複数のタスクが定義され、これらは簡単なタスク管理により制御され、タイマー割り込みにより決められたインターバルで実行される。いくつかの優先度の低いタスクは断裁機の標準機能のための予備となり、先の仕様書に記述された安全関連機能は優先度の高いタスクにより実行される。このタスク呼び出しの決定性は、要求される両チャンネルの高い同期性と

短い応答時間に対して不可欠である。タスクのアイドルタイムに、偶発的ハードウェア故障を抑制するための自己診断が周期的に実行される。

ソフトウェアアーキテクチャと実装のために必要なソフトウェアモジュール及び機能の設計は、別の文書、つまりシステム及びモジュール設計のための技術文書にまとめられる。全ライフサイクルを通じて不具合（障害）を回避するためには、適切なモジュール化と、本ケースに関しては非安全関連ソフトウェアと SRESW の明確な境界付けが特に重要である。これを理解するために必要とされるソフトウェアの構造と流れは図により示される。さらに、使用されるプログラミング言語、ここではコンパイラ特有の言語拡張による ANSI C と、コンパイラ、バージョン管理、構成管理等の開発ツールに関して規定される。これらはすべて、長年にわたる実績をもつものとされる。また、プログラミング・ガイドラインと、コーディングを検証するためのツールを使った静的解析の手法が決定される。モジュール試験及び統合試験の計画についても、本技術文書で確定される。「ソフトウェア開発マネージャ」（あるいはこれに該当する立場の者）により再度レビューを行った後、本技術文書はコーディングのための仕様書として承認される。レビューでは、ソフトウェア仕様書の要求事項が満たされているかどうも検証される。

そして、メインとされるコーディング作業が、プログラミング・ガイドラインを考慮した上で開始される。プログラミング・ガイドラインには、コードをより読みやすくするため規則の他、特に重要な言語構造の使用に関する制限等が規定される。プログラミング・ガイドラインの順守は、コーディングを進める中で、適切なツールにより保証される。完成したコードの技術文書に対する意味的検証は、プログラマとその同僚によるウォークスルーにより行われる。同時に、ここでプログラムシーケンス及び重要な信号のデータフローの解析も行われる。
通常のモジュール試験では、機能及びインターフェースに関して、一つはそれが正確であること、もう一つはそれがモジュール設計と一致したものであるかどうかがチェックされる。続いて、ソフトウェアの統合と、マイクロコントローラ K1 のハードウェアと合わせてのテストが行われる。この後、両チャンネルの同期化、データ交換及び不具合（障害）の検出をいっしょにテストするために、K1 は ASIC チャンネル K2 と接続される。すべての試験は文書化される。

この統合試験において、マイクロコントローラの性能が予め想定されたほどよくないという結果が出される可能性もある。そのような場合には、ソフトウェアアーキテクチャ、具体的にはタスクの時系列的プランニングとタスクのための機能の配置も変更する必要が出てくる。ソフトウェアの安全要求事項仕様書がこれにより変更されることはなくても、システム及びモジュール設計については、仕様書との一致を順守するために、適切に変更し、再度レビューを行わなければならない。これは、開発中の必要な技術的変更が V-モデルの反復につながる可能性を示す例といってよいだろう。これにより、モディフィケーションは品質要求事項に従って実行される。モディフィケーションに対するコーディングが行われると、モジュール試験並びに統合試験が再度実施されることになる。

ファームウェアが最初の製造バッチの納品後にさらに変更を要するような場合に備えて、モディフィケーションの影響解析など適切な方策及び V-モデルによる適切な開発アクティビティを開発組織で決定しておく必要がある。

6.5.10　SRP/CS の組合せ

最初から最後まで全部の SRP/CS が 1 つのカテゴリで構築されており、サブシステムの組合せがないので、ここでは本章 6.4 による考察は不要である。しかしながら、各種のコンポーネント及び技術方式は、当然ながら、それらのインターフェースに適合したものでなければならない。統合に関する妥当性確認の視点については、第 7 章で説明する。

6.5.11　その他

本節の具体例においても、多くの安全関連の設計視点は表面的にしか取り上げることができない。このため、後で紹介される回路例に一般的に適用される説明や注意すべき要求事項を記した活用度の高い文献を以下に追記するので、参考にしていただきたい。

詳細情報を提供する参考文献

- EN 1010-3：機械類の安全性－印刷機及び紙工機の設計と構造に関する安全要求事項－第 3 部：断裁機（'02.12）。Beuth（ベルリン）、2002 年
- IEC 61508-2：電気・電子・プログラマブル電子安全関連系の機能安全－第 2 部：電気・電子・プログラマブル電子安全関連系に関する要求事項（規格草案）。Beuth（ベルリン）、2006 年
- EN 574：機械類の安全性－両手操作制御装置－機能的側面；設計原則（'97.02）。Beuth（ベルリン）、1997 年

その他、特に検証及び妥当性確認に関しては、次の第 7 章で、引き続き断裁機を例にして説明する。