BGIA Report 2/2008

和訳（仮訳）

BGIA Report 2/2008 の日本語版について

本日本語版は、
発行者： Deutsche Gesetzliche Unfallversicherung（DGUV:ドイツ損害保険協会）、Alte Herrstraße 111, D-53757 St.Augustin, Germany、編集 BGIA（DGUV 中央研究所）が 2008 年 2 月に発行した”BGIA Report 2/2008”, ISMB:978-3-88383-730-X の原文（独文及び英文）を基にして、日本語に翻訳したものである。

日本語訳の内容及び用語等に関して確認を要する場合には、原本である独文を参照頂きたい。

翻訳　前書き～第 7 章　NPO 安全工学研究所
第 8 章　社団法人日本印刷産業機械工業会

概要

「機械制御システムの機能安全」
― ISO 13849-　の適用 ―

ISO 13849「機械類の安全性－制御システムの安全関連部」は、制御システムの安全関連部の設計に関する規定を定めた規格である。本規格は、2007 年に大幅に改訂された。本レポートは、その主要内容を紹介すると共に、電気、流体、電子及びプログラマブル電子分野、また複合化された技術方式への具体的な適用について解説したものである。また、機械指令の必須安全要求事項との関連やリスク見積りの手法についても取り上げられている。これらの情報をベースに、制御システムの安全機能に関する要求パフォーマンスレベル PL_r の選択、そして実際に達成されるパフォーマンスレベル PL の決定が詳しく解説される。それぞれのパフォーマンスレベルを達成するための要求事項と、これに関連するカテゴリ、コンポーネントの信頼性、診断範囲、ソフトウェアの安全性、系統的故障並びに共通原因故障に対する方策が述べられ、また、要求事項を実際の制御技術で実行するに当たっての背景情報も盛り込まれている。数多くの回路例では、コンポーネントレベルまで掘り下げて、パフォーマンスレベル「a」から「e」が、カテゴリ「B」から「4」と共に、採用される技術方式でどのように達成できるかを説明している。これは、使用される安全原則と十分吟味された安全関連コンポーネントに関する情報としても利用できる。また、各ケースについてさらに深く理解したい人のために、数多くの参考文献が挙げられている。本書により、ISO 13849 の要求事項は実際の技術手法で実行できるものであることがわかる。これにより、本規格が国内及び国際レベルで統一して適用され、実施されるために、本レポートは大いに貢献するものといえよう。

1　前書き

10 年前に発行された BIA レポート 6/97「EN 954-1 による安全関連制御システムのカテゴリ」は、これまでの出荷部数がドイツ語版 12,000 部、英語版,6000 部を超えるベストセラーである。職業保険組合・労働安全研究所（BGIA: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung）のインターネットサイトからのダウンロード数はさらにこれを上回り、本書は日本語訳でも提供されている。

この 10 年の間、機械類の安全関連制御システムは、機械式、空圧式、油圧式、電気式にかかわらず、すべて EN 954-1 に従って 5 つのカテゴリに分類されてきた。しかし、プログラマブル電子システムが主流を成すにつれて抜本的見直しが必要となり、改訂に向けた準備が進められた。これは非常に困難を伴う作業であったが、それは ISO 13849-1:2007-07 の成果として多くの実りをもたらした。本規格の主要な変更は、制御システムの安全性評価及び設計に関して確率論的アプローチを取り入れたことにある。コンポーネントの故障確率に注目したこの手法は、電気装置の安全基本規格である IEC 61508 シリーズではすでに定着したものとなっている。あらゆる技術方式を適切に、そして何よりも実用的に分類できることが今後はさらに要求されることを考慮し、ISO 13849-1:2007-07 では、カテゴリはパフォーマンスレベルというより広範なコンセプトに組み入れられることになった。

後継規格となる ISO13849-1 は、取り扱う題材が非常に複雑なものであるにもかかわらず、適用における実用性を十分に考慮したものとなっている。これは、特に BGIA の経験を積んだスタッフの熱心な協力があってこそ実現できたものといえる。

本規格は 2007 年 5 月に整合規格として発行された。ドイツ機械工業連盟（VDMA）のポジションペーパー（本書 249 ページ、付録 I 参照）では、ドイツの設備及び機械製造において本規格を積極的に適用することが表明されている。これにより、機械の安全関連制御システムに関する BGIA レポートも完全改訂版として発刊すべき時期を迎えたといえる。安全技術がますます複合的・複雑になるに従い、その使用に関するアドバイス及びサポートへの期待や要求にも変化が見られる。BGIA レポート及び当 BGIA で開発されたソフトウエア「SISTEMA」は、読者並びに使用者が新たな手法をより簡単に理解し、活用できるようにする、新・旧規格の架け橋を担うものといえよう。20 名の執筆者から編制された当チームでは、読者を ISO 13849-1:2007-07 の「秘策」に一歩一歩手繰り寄せ、そして実際の適用に導くことために、何度も討論並びに検証を重ねて、文章を練り上げ、重要となる回路例を作成した。むろん、本レポートは規格の代わりをなしえるものではない。しかし、本書には、実用的な応用事例や助言をはじめ、数多くの貴重なヒントが盛り込まれている。教本及び参考図書としても十分活用いただけるものと考えている。

BGIA 所長
カールハインツ・メッフェルト（Dr. Karlheinz Meffert）

2 序文

1995 年 1 月 1 日以降、欧州経済圏内で流通する機械類にはすべて、機械指令の必須要求事項［1］を満たしていることが義務付けられた。本機械指令の第 1 条によれば、機械類とは、連結された部品または構成部品の組み合わせで、そのうち少なくとも一つは適切な機械アクチュエータ、制御及び動力回路等を備えて動くものであって、特に材料の加工、処理、移動、梱包といった特定の用途に合うように結合されたものをいう。機械指令 98/37/EC［1］では、機械類だけでなく、安全関連部品もその対象となる。安全関連部品とは、製造者が安全機能の確保を意図して市場に出荷する部品であり、その故障もしくは誤動作により、本指令の適用範囲にある機械類の作用領域にいる人の安全や健康を脅かす可能性のあるものをいう。

機械類及び安全関連部品に関する機械指令の必須要求事項は、指令附属書 I に記載される。本附属書には、安全統合の一般的基本原則をはじめ、機械類の制御装置や停止装置、また安全防護物に関する要求事項が列挙される。機械類及び安全関連部品の設計に関する必須安全要求事項により、製造者には、機械に関するすべての危険源を調査するために危険源の分析を行うことが義務付けられている。そして、個々の危険状態と結びつく災害リスクを受け入れ可能なレベルに低減するための方策として、次の 3 つの基本原則が掲げられる。

- 設計による危険源の除去もしくは最小化
- 除去できない危険源に対する必要な保護方策の実施
- 残留リスクに関するユーザーへの指導

本指令の第 5 条により、欧州整合規格に順守した製品は、機械指令の必須安全要求事に合致していると見なすことができる。機械指令の附属書 I は機械に係る労働安全を達成するための基本であり、その理念は、関連欧州規格の草案及びすでに整合された規格でさらに掘り下げられ、具現化される。ISO 12100 シリーズ［2;3］は、機械類の安全性に関する基本概念及び一般設計原則などを取り扱ったものである。また、危険源の同定並びに個々の危険状態のリスク見積りとリスク評価のための手法は、ISO 14121 の改訂原案［4］及び同技術報告書 ISO/DTR 14121-2[［5］に記載される。この 2 つの基本規格をベースに、シリーズ規格 ISO 13849-1:2007［6］及び ISO 13849-2:2003［7］により、制御システム及び安全防護物の安全関連部の設計、構造、統合において必要なリスク低減が規定される。ここでは、電気式、電子式、油圧式、空気圧式、機械式などの技術方式は問われない。本規格と共に、機械及び／又はその安全防護物の制御システムに関し、共通して適用できる体系が提示されたといえる。本規格で規定されるパフォーマンスレベルにより EN 954-1 によるカテゴリの概念が拡張され、安全アーキテクチャと共により柔軟性の高いものになった。EN 954-1 の本質的価値は、前書きでも触れたように、使用する技術方式に

は関係なく、制御システムの安全関連部を取り扱ったものであるという点にある。ISO 13849-1:2007 はこれを継承し、さらに拡張させたものといえる。パフォーマンスレベルの導入により、種々のテクノロジーを使用したさまざまな制御構造の組合せが簡単に実現できる。新規格は 100 ページにも満たないが、この中に必要な事項がすべて集約されている。そして、具体的な用途あるいは技術方式に左右されない方法論という位置付けにより、ほとんどすべての個別製品安全規格（C 規格）で引用され、また機械構造に関する国内規格等でも参考規格として挙げられる。

2009 年 12 月 29 日から新機械指令［8］が施行されることにより、本規格は整合規格としてより重要な位置を占めることになる。新機械指令の主要改正点の一つとして、制御システムの安全関連部ともいえる安全関連の論理演算機器が附属書Ⅳに新たに加えられたことが挙げられる。附属書Ⅳの製品というのは、本指令によれば、特別な取扱いを要するものをいう。今後は、この付属書Ⅳの製品に関する EC 型式試験 [1] による証明は不要となり、製造者は社内の品質管理（QC）システムを拡充し、通知機関による検定を受けることで、これらの製品を市場に流通させることができる。しかし、新指令により、制御システムの安全の重要性がクローズアップされることも十分覚悟しておかなければならない。

ISO 13849-1:2007[6]は、先に整合された ISO13849-2:2003（第 2 部）［7］と共に、EN 954-1:1997［11］の後継規格となるものである。DIN（ドイツ工業規格）版は、2007 年 2 月の初版発行後、これを若干修正したものが 2007 年 7 月に出されている。DIN では、2009 年 11 月までの 3 年間の移行期間が設けられ、その間は DIN EN 954-1:1997 が並行して適用される。つまり、撤廃時までは、使用者はこの 2 つのどちらかを選択して使用することができるわけである。旧知のカテゴリから新規格による要求パフォーマンスレベル PL_r への移行を容易にするため、本レポートの第 5 章では、そのアプローチが説明される。

本レポートは ISO 13849 の適用を解説するものであるが、特にその実際の技術的実現性を理解していただくために、数多くの設計解と共に現実的な事例を取り上げて説明することを心がけた。これらの説明や例は、ISO 13849-1 に対するドイツあるいは欧州の立場による公式の解釈というよりは、むしろ職業保険組合・労働安全研究所（BGIA: Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung ）の安全防護物及び制御システムのアセスメントにおける 30 年に及ぶ経験と、国内及び国外の当該規格委員会における長年の実績及び経験の成果ととらえていただきたい。

[1] EC 型式検定以外に、製造者は、現行の機械指令に従って、整合規格がある場合にはその整合 C 規格に従って製造したと宣言することができる。あるいは、製造者は、通知機関に書類を預けるか、もしくはそこで試験を受けて書類を保管してもらわなければならない。

第 3 章で機械及び機械設備に関する機能安全のための基本規格を取り上げ、第 4 章で ISO 13849 の適用に関する概要を示す。

制御システムの安全関連部に関する要求事項を実施するに当たって、設計者、経営者並びに労働安全専門家の皆様に本レポートを活用していただけることが、執筆者全員の願うところである。本書における規格の解釈は、実際の使用を考慮してさまざまな視点から検証されたものであり、またここで紹介する例は、すでに数多くの具体的用途において実施されているものである。

3　機械制御システムの機能安全に関する基本規格

機能安全[1]については、本レポートで取り上げる ISO 13849 の他に、選択肢となる重要な規格が存在する。それは、図 3.1 に示す IEC 61508 シリーズ規格［12］及びそこから派生した機械分野に関するセクター規格 IEC 62061［13］である。両規格とも、適用範囲は電気・電子・プログラマブル電子システムに限定される。

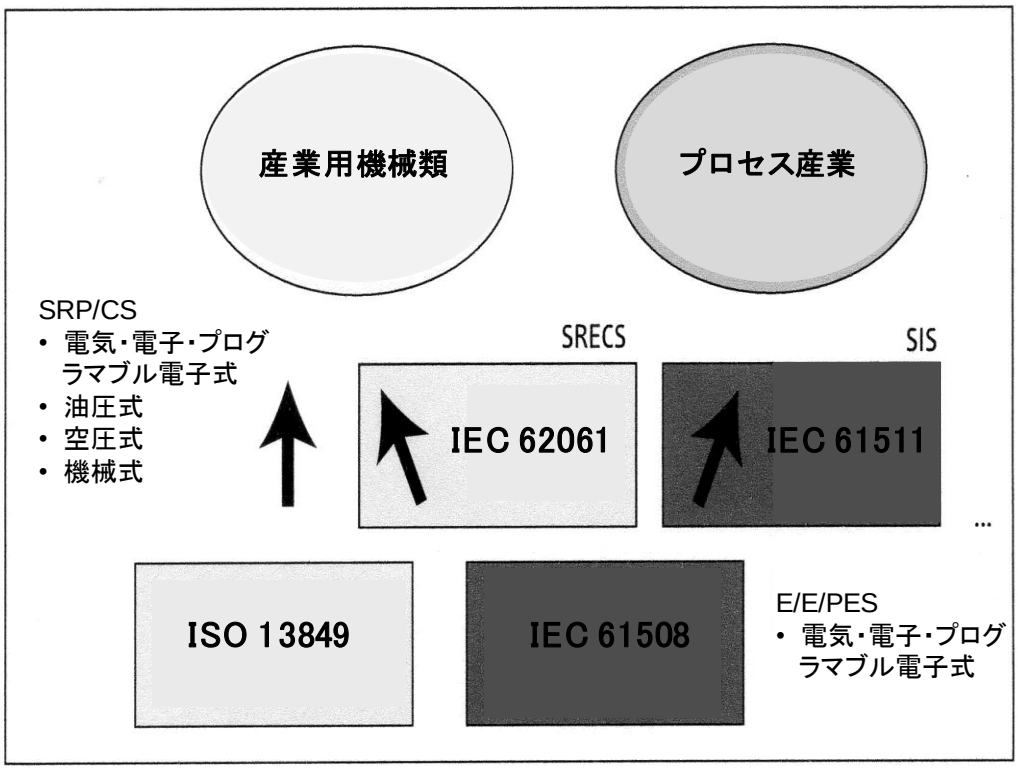

図3.1： 機能安全に関する各基本規格の適用範囲
SPR/CS：制御システムの安全関連部、SRECS：安全関連電気制御システム、
SIS：安全計装システム、E/E/PES：電気・電子・プログラマブル電子安全システム

IEC 61508 及び IEC 62061 では等級尺度として安全度水準（safety integrity level, SIL）が定義される。SIL は安全関連系の信頼性に関する指標であり、故障境界値はそれぞれ 10 の乗数で表わされる[2]。低頻度作動要求モードで算出される数値は作動要求時機能失敗平均確率 PFD（Average **P**robability of **F**ailure to Perform its Design Function on Demand）であり、一方、高頻度作動要求あるいは連続作動要求モードに関しては、単位時間当たりの危険側故障率 PFH（**P**robability of a Dangerous **F**ailure per **H**our）が定義される（詳細は［14］を参照）。機械分野及びこれに適用される IEC 62061 に関連するのは後者の定義のみであり、また高リスクを伴う SIL4 システムは機械分野での適用例はないため、IEC 62061 では考慮されない（図 3.2 参照）。

1　機能安全とは、ここでは、制御系の故障、つまり機能不良により引き起こされうる危険状態について対処することを意味する。

2　これ以外にも、それぞれのレベルで達成しなければならない、いわゆる決定論的要求がある。

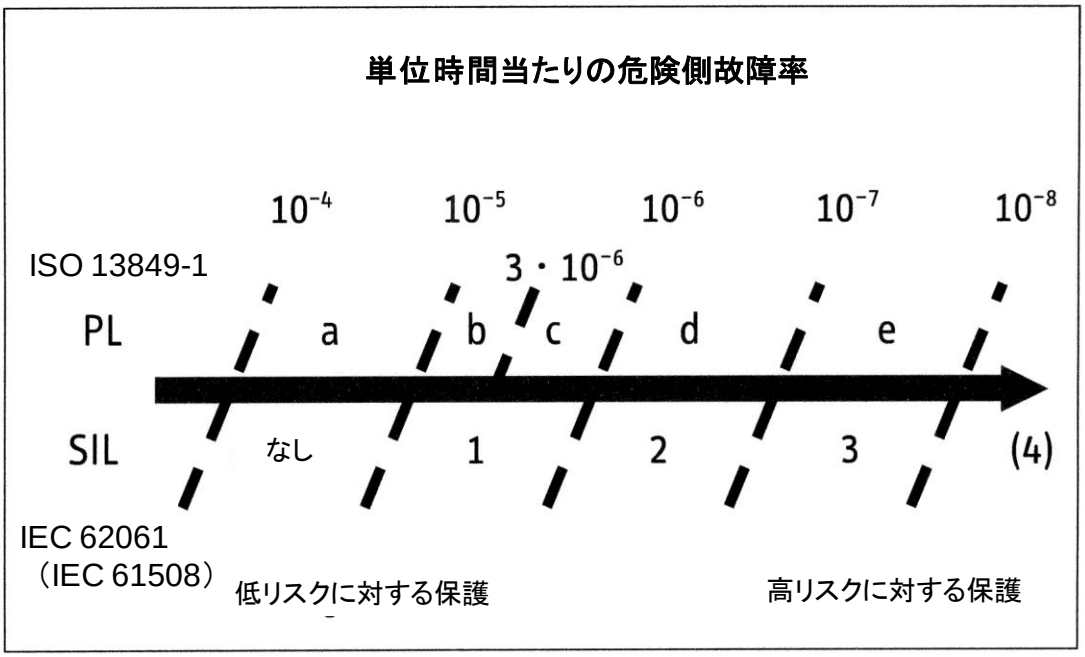

図3.2：パフォーマンスレベル（PL）と安全度水準（SIL）で表した危険側故障率

特性値として故障確率及び構造を定義したこれらの規格の基本的取組みは、一見するとより汎用性のあるものに映る。しかしながら、 ISO 13849-1 では、使用者は、センサからアクチュエータ（バルブなど）にいたるまで、それらがどのような技術方式によるものであっても、一つの規格の枠組みの中で安全機能を開発し、評価することができる。 ISO 13849 には 2003 年に発行された「妥当性確認」と題する第 2 部があり、第 1 部の改訂に合わせた修正が当然必要とされるところであるが、驚くべきことに、この第 2 部の要求事項はすでに改訂第 1 部に十分対応できるものとなっている。第 2 部の附属書 A から D には「基本安全原則」、「十分吟味された安全原則」、「十分吟味されたコンポーネント」及び「不具合（障害）リスト」に関する広範な資料が含まれており、これは改訂第 1 部にも適用される。この詳細は、本書の付録 C に記載される。

2 つの国際規格（ISO と IEC）の規定要求事項は明らかに重複したところがあり、これが、規格使用者である制御装置等の製造者には一見して分かりにくいところでもある。IEC 62061 は ISO 13849-1 と同様、機械指令に基づいた整合化規格である。一方、IEC 61508 の第 1 部から第 4 部は IEC[1] の観点からは安全の基本規格（低複雑度システムは除く）とされるが、本規格シリーズは欧州規格ではあっても、機械指令の下で整合化されることはない。このような状況から、特に次のような質問が提起される。

[1] IEC= International Electrotechnical Commission（国際電気標準会議）

- 機械指令を実行するためにはどの規格を適用すればよいのか？
- 規格の適用範囲が重複している場合、どちらの規格を使用しても同等の結果が得られるのか？
- カテゴリ、パフォーマンスレベル（PL）、安全度水準（SIL）など各規格で使用される等級尺度には互換性があるのか？
- 2 つの規格のうちの一方を考慮して開発した機器類を、安全機能の技術的実現においてもう一方の規格に則って使用することは可能か？

改訂 ISO 13849-1 では、IEC との互換性を最大限達成し、長期的視点からできるだけ両国際規格の統合を図り、さらに実績のある安全カテゴリの概念を切り捨てることなく確率論的アプローチの長所を取り入れるため、パフォーマンスレベル（PL）の定義により、従来のカテゴリの確定論的手法と安全技術の信頼性の側面を一体化する均衡策がとられている（[15] を参照）。両者の等級付けは数値的に対応させることが可能であり（図 3.2 参照）、はじめて適用する場合にも容易に見積もることができる。また、 ISO 13849-1 と IEC 62061 は共に、その原案段階で、規格委員会のメンバーにより推奨される適用案を作成し、それぞれの序文において公表しているが、これらはほぼ同じことばを使って表わされている。その中核をなすのが、各用途に適した規格を選択するために用意された一覧表である。しかし、 ISO 13849-1 に関しては、原案作成当時のものがそのまま用いられているため、これはもはや時代遅れと言わざるを得ず、ここに記載される制約は本規格の現行版には適合しない。つまり、制約は実際にはもはや存在しないといってよい。ただし、安全関連の組み込みソフトウエア（SRESW）が完全な多様性を採用していない場合は、IEC 61508-3:2002 の第 7 条に従って開発しなければならない（本書 6.3 を参照）。

本規格で指定されるアーキテクチャも、義務というよりはむしろ一つの提案（簡易的アプローチ）ではあるが、これは今後 ISO 13849 で実行されることになる確率論的アプローチの中心要素となるものであり、またこの適用は本レポートの主要観点の一つでもある。IEC 62061 については、一覧表を見ると、例えば複雑なプログラム電子系もこの規格の適用範囲に含まれるとされる。これは間違っているとは言わないが、しかしプログラマブル電子系のいわゆる SRECS（図 3.1 参照）の開発は IEC 61508 に準拠した規格の要求事項に従って行わなければならない。図 3.3 に、規格の現状況及びその適用範囲に従って推奨される「適切な適用」を示す。

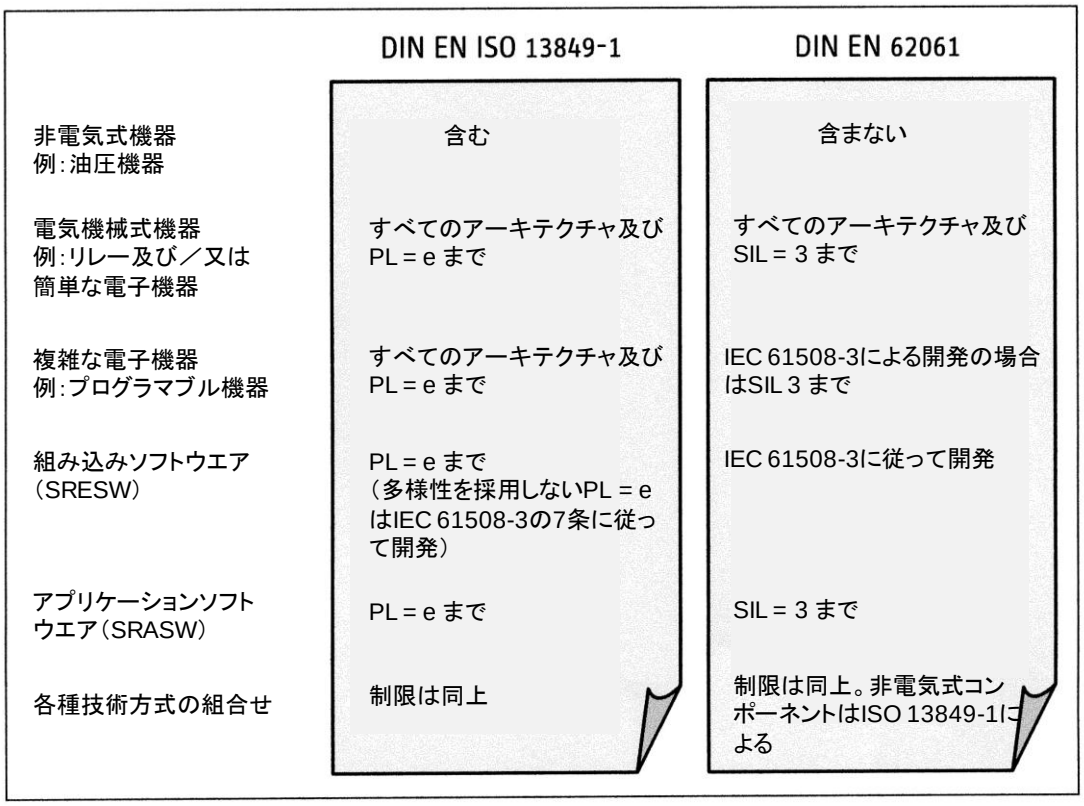

図3.3： ISO 13849-1とIEC 62061の「適切な適用」

それぞれの規格を適用した際の結果の近似性については多くの専門家が論じるところであるが、いずれにせよ、要求事項の詳細はそれぞれ全く異なったものである。IEC 62061 は IEC 61508 のセクター規格として、当然ながら「機能安全管理」の側面が特に明確に記述されている。ISO 13849-1 による組み込みソフトウエアの開発及び検証は、現在の標準として IEC 61508 にも記載される安全関連ソフトウエアに関する本質的な要求事項がベースとなる。この点の記載については複雑さを（おそらくは意識的に）避けて、「一般的には」と表現されている。しかし、両規格による要求事項を混同すべきではないという点では変わりはない。

結局のところ、機械分野の機能安全実現のためのベースとして ISO 13849 を選択する最大の理由は、ユーザーの視点からすると、技術方式全般に適用できる手法と指定のアーキテクチャによる簡易化された定量的手法にあるといえるだろう。これには、非電気式及び機械電気式コンポーネントに関する具体的な考察も含まれる。しかし、特に安全用途のプログラマブルロジックコントローラ（PLC）など大量生産される安全コンポーネントの製造者等にとっては、当然ながら機械分野以外の世界的市場もターゲットになる。このようなケースでは、 ISO 13849 だけでなく IEC 61508 も開発のベースとして考慮する必要がある。

4　ISO 13849-1 及び本レポートの概要

規格適用に関する具体的説明に入る前に、本規格及び本レポートの概要を述べる。後続の各章及び付録との関連も示してあるので、リファレンス情報としてご一読いただきたい。まず、制御システムの安全関連部を設計するための反復的プロセスの流れを図 4.1（規格の図 3 に該当）に示す。

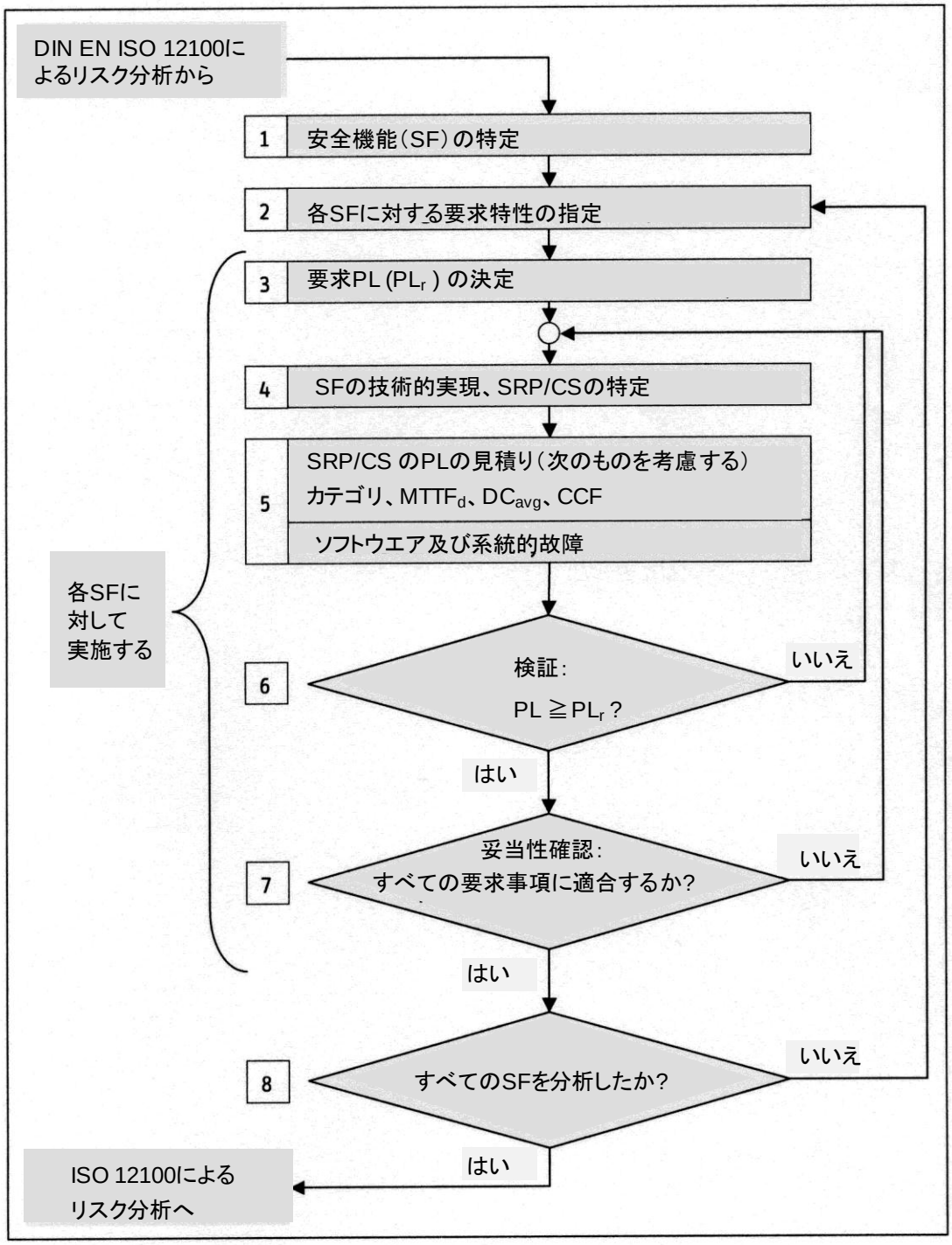

図4.1: 制御システムの安全関連部の設計のための反復的プロセス：
SF = 安全機能、PL = パフォーマンスレベル、SRP/CS = 制御システムの 安全関連部、
$MTTF_d$ = 平均危険側故障時間、DC_{avg} = 診断範囲、CCF = 共通原因故障

4.1　安全機能の特定とその要求特性の指定

制御システムの安全関連部の設計及び評価プロセスでは、最初に、十分吟味されたコンセプトとして 1 つもしくは複数の安全機能（SF）を特定する。この手順は、図 4.1 の 1 から 3 のブロックに該当するもので、詳しくは第 5 章で述べる。ここでは、「機械の危険源のリスク低減に対する制御システムの安全関連部の貢献度」がポイントになる。

機械は、第一に、使用者にとって危険な状態が発生しえない構造（本質安全設計）になっていなければならない。そして次のステップとして、さらに存在する個々の危険源／危険状態に対するリスクの低減が行われる。これは各種保護方策により達成されるが、今日では大部分が制御システムにより実現される。こうした保護方策及びこれを技術的に実行する安全防護物が、リスクに従って決められたレベルを達成するためには、リスクアセスメントが重要なステップとなる。安全防護物は制御システムの安全関連部として、単独で、あるいは部分的に関与して、安全機能を実行する。例えば、オペレータが危険区域に介入したときの予期しない起動は、安全機能により阻止することができる。安全機能は、１台の機械に、まず間違いなく複数（例えば自動運転と調整運転に対して）存在するといってよい。このため、個々の危険源及び危険状態と、これに結びつく安全機能を慎重に考察することが非常に重要である。

安全機能は、制御システムの構成部により、あるいはこれにさらに必要なコンポーネントが追加されて実行される。これらは 2 つとも、制御システムの安全関連部である。いくつかの異なる安全機能に 1 つの同じハードウェアが関与する場合でも、それぞれの安全機能（SF）に対し要求されるリスク低減のレベルは異なる可能性がある。規格では、このリスク低減のレベルが「パフォーマンスレベル」（PL）として定義される。それぞれのリスクアセスメントの結果に従って、安全機能に対し多少なりとも高めの PL 値が要求される。制御システムのレイアウト設計に対して決定されるこの基準が「要求パフォーマンスレベル」PL_r と呼ばれるものである。それでは、この PL_r はどのようにして求めればよいのだろうか？

機械の危険源のリスクは、制御システム以外に、例えば保護扉等のガード、あるいは保護めがねといった個人用保護具によっても低減することができる。そこで、まずは、制御システムが担う役割を特定する。そうすれば、「リスクグラフ」という簡単な図式を用いて要求パフォーマンスレベル PL_r を速やかに決定することができる（本書付録 A の例を参照）。傷害は回復不可能なもの（死亡、身体の一部喪失など）か、それとも回復可能なもの（打撲傷など正常時への回復が可能）か？オペレータの危険区域への介入は頻繁かつ長時間（例えば 1 時間に 1 回以上）に及ぶか、あるいはまれで短時間なものであるか？災害を回避できる可能性（例えば機械運動の速度低減による）はあるか？この 3 つの質問により PL_r は決定される。詳しくは第 5 章の 5.4 で説明する。

4.2　安全機能の設計及び技術的実現

制御システムの安全関連部に関する要求事項が確定したならば、次にレイアウト設計、続いてその技術的実現のステップへと進む。最後に、実際値 PL で表される設計の実現性（図 4.1 のブ

ロック 4 及び 5）により必要なリスク低減と目標値 PL_r が達成されえるかどうかを検証する（図 4.1 のブロック 6）。ブロック 4 及び 5 のステップについては第 6 章で詳しく説明する。定評ある BIA レポート 6/97 に倣って、本書の第 8 章でも、あらゆる制御技術及びカテゴリに関して想定される回路例を数多く取り上げた。この詳細例の他、第 5 章、6 章及び 7 章でも一般的なシステム構成図が示されている。次に説明される手法やパラメータを理解するためにも、ぜひ、これらを活用していただきたい。

制御システムの安全関連部については、まずはその安全機能が明確にされていることが前提となる。これに従って、品質基準として、使用されるコンポーネントの寿命、それらの組み合わせ（ディメンショニング）、診断の有効度（例えば自己診断）及び構造の不具合（障害）に対する耐性（フォールトトレランス）が選択され、これらのパラメータから危険側故障率と共にパフォーマンスレベル PL が決定される。改訂 ISO 13849-1 には、適用すべき算定手法については規定されていない。従って、前述のパラメータを考慮した上で、非常に複雑なマルコフモデルを利用してももちろん構わない。しかし、規格では、柱状グラフを用いた簡易的手法が説明されている（図 6.10 参照）。ここでは PL はすでにモデル化されているが、この柱状グラフの作成の仕方を詳しく知りたい方は、本書付録 G を参照いただきたい。

カテゴリは、本規格の改訂後も、PL 決定のベースとなる。カテゴリの定義については本質的に変わるところはないが、コンポーネントの品質及び診断の有効度に関する要求事項が追加され、カテゴリ 2、3、4 に関しては共通原因故障に対する十分な方策をとることが求められる（表 4.1 参照）。

カテゴリの概要については表 6.2 にまとめられており、この表の右 3 列が本規格で新しく追加された部分である。本規格で紹介される前述の簡易的手法を使用するに当たっては、いわゆる指定のアーキテクチャとして図式化される各カテゴリのブロックダイアグラムがポイントになる。

また、カテゴリには不具合（障害）の考慮（不具合（障害）の回避及び抑制）が要求されるため、個々のコンポーネントの信頼性、不具合（障害）時の挙動及び自動診断による不具合（障害）検出の視点が加わる。このベースとなるのが、不具合（障害）リスト及び基本安全原則である（本書付録 A 及び C 参照）。ISO 13849-1 では、「伝統的な」FMEA（故障モード及び影響解析）以外に、例えば「部品点数法」といった簡易的な評価方法が示されている。本テーマに関する詳細は本書の付録 B をご覧いただきたい。

故障確率に関するもっとも多い質問の 1 つとして、安全関連コンポーネントの信頼できる故障データ、すなわち $MTTF_d$（平均危険側故障時間）の入手に関する問題がある。これについては、部品あるいはコンポーネント製造者の技術データシートが他のどのような情報源よりも優先されると言ってよい。空気圧分野も含め、多くのコンポーネント製造者は、こうしたデータは今後提供できるものとしている。しかし、製造者によるデータが（現時点では）あまり多くはないにしても、参考値となる例を既成のデータ（SN 29500 や IEC/TR 62380 等）から見つけ出すことができる。規格及び本書の付録 D にも、実際例に基づく現実的な値がいくつかリストアップされている。

表 4.1：カテゴリの決定論的及び確率論的特徴：濃い灰色の欄が本規格改訂による追加項目

特徴	カテゴリ				
	B	1	2	3	4
予期される影響に耐えられるよう、関連規格に従って設計される	X	X	X	X	X
基本安全原則	X	X	X	X	X
十分吟味された安全原則		X	X	X	X
十分吟味されたコンポーネント		X			
平均危険側故障時間－$MTTF_d$	低から中	高	低から高	低から高	高
不具合（障害）の検出（診断）			X	X	X
単一不具合（障害）に対する耐性				X	X
不具合（故障）の累積の考慮					X
診断範囲－DC_{avg}	なし	なし	低から中	低から中	高
CCF 対策			X	X	X
カテゴリの特徴付け	コンポーネントの選択		構造		

診断の有効度、すなわち DC_{avg}（平均診断範囲）は非常に簡単に算定することができる。まず、各ブロックについて、そのブロックを監視する診断方策をまとめる。そして次に、各診断方策に対して、規格の表による 4 つの典型的な DC 値の中の 1 つを決定し、最終的な計算を行えばよい。詳細は本書 6.2.14 及び付録 E に記載されるので、そちらを参照いただきたい。一見すると複雑に見えるかもしれないが、実際は簡単な公式により DC_{avg} を算出することができる。

最後の CCF（Common Cause Failure、共通原因故障）についても、非常に簡単に定量化することができる（本書 6.2.15 参照）。CCF は、汚染、過剰温度、短絡などの単一の原因により、例えば 2 つの制御チャンネルが同時に機能しなくなるような、複数の不具合（障害）を次々に引き起こすものをいう。このような危険の原因を抑制するために、カテゴリ 2、3、4 のシステムについては、CCF に対して十分な方策がとられたことを証明する必要がある。これについては、主に技術的な手段による 8 つの典型的な方策に対するスコアリングにより評価する。合計点数は最低でも 65（最高は 100）に達しなければならない（本書付録 F 参照）。

故障には、構造及び故障率の改善により抑制することのできる偶発的なハードウェア故障の他に、いわゆる系統的故障と呼ばれる幅広い領域がある。この故障原因となるハードウェアのディメンショニングミス、ソフトウェアエラーあるいは論理エラーなど、設計段階からすでにシステムに内在する可能性のある不具合（障害）に対しても、これを回避あるいは抑制するための方策をとらなければならない。ここでは、ソフトウェアの不具合（障害）の占める割合が一番大きい。前書きで述べたように、安全関連のソフトウェアに関する要求事項は本規格では新しく規定されたものであるが、詳細は、関連規格によりすでに明らかにされている。具体的方策は要求される PL に従ってランク付けされる。系統的故障に関しては本書の 6.1.2、またソフトウェアに関しては 6.3 で詳しく説明する。

4.3　各安全機能に関する制御システムの検証と妥当性確認

技術的に実現されるパフォーマンスレベルの見積もりまで終えたら、制御システムにより実行される各安全機能に対し、その PL が十分なものであるかどうか確認する必要がある。これについては、PL と PL_r を比較し（図 4.1 のブロック 6 参照）、1 つの安全機能について達成される PL が PL_r より「劣る」場合には、多かれ少なかれ設計による改善（例えば、$MTTF_d$ がより高い別のコンポーネントを使用する）を行うことで、十分な PL を達成しなければならない。この検証のハードルをクリアしたら、いわゆる妥当性確認の一連のステップに進む。この妥当性確認については、ISO 13849 の第 2 部の規定が用いられる。妥当性確認とは、制御システムの安全関連部に関する機能及び性能面での要求事項がすべて達成されたことを体系的に確認することをいう（図 4.1 のブロック 7 参照）。この詳細については第 7 章で説明する。

4.4　ISO 13849-1 の今後の展開

改訂 ISO 13849-1 については 2006 年 11 月の発行後、3 年間の移行期間が設けられ、その間は前版となる EN 954-1 が並行して適用される。こうした措置をとることで、改訂により転換を強いられる開発者及び使用者の負担はいくぶんか軽減されると思われる。本改訂規格への移行がスムーズに進められるように、BGIA では、前回（BGI レポート 6/97）同様、今回もユーザーのサポートに努めていくつもりである。本書の説明及び各例の随所に記した参考文献もその一環であるが、この他にも、PL_r 及び PL の評価と文書化のためのツールとなる「SISTEMA」（Sicherheit von Steuerungen an Maschinen、機械の制御システムの安全）（本書の付録 H 参照）がフリーウエアプログラムとして用意されている。また、BGIA が考案した「パフォーマンスレベルカリキュレータ」（Performance Level Calculator）［16］もすでに無料で配布されている。この円盤型のカリキュレータは、回転させて、PL をいつでも簡単かつ正確に見積もり、表示させることができる。これらのサービス及び文献等の情報は、BGIA のインターネットサイトで公開されている。
www.dguv.de/bgia/13849

5　安全機能とリスク低減に対するその貢献度

本章では、安全機能と、機械の危険源のリスク低減に対するその貢献度を取り上げる。安全機能の構築は、安全な機械類を実現するプロセスの一部をなすものである。そこで、まず機械指令の要求事項について簡単に説明し、それから安全機能及びその要求特性について述べることにする。本章最後の 5.7 で、断裁機を例にした実際の適用を説明する。

5.1　EC 機械指令の要求事項

EC 機械指令［1］は機械類に適用される安全と健康に関する必須要求事項を規定したものであり、ドイツでは機器・製品安全法の枠組みの中で国内法に転換されている。機械指令の有する一般的性質は各規格によりはじめて具体的に表わされるが、その中で特に重要な位置を占めるのが ISO 12100 シリーズ規格［2; 3］の「機械類の安全性－基本概念、一般設計原則」である。機械設計者を主対象とした本規格には、機械類の安全を達成するために適切とされる方法が記載されており、ここで規定されるリスク低減の戦略的アプローチは、制御システムの安全関連部[1]の設計にも引き継がれる。

設計される機械に関して、EU 官報で整合規格として公示された個別製品安全規格（タイプ C 規格）が存在する場合には、この適用により、前述の安全と健康に関する必須要求事項はすでに考慮されているものと見なすことができる。この種の規格は、機械指令の要求事項との合致を前提とするため、いわゆる「適合性の推定」を伴う規格と称される。しかし、「適合性の推定」を伴う規格が存在しない場合、あるいは規格対象外である場合、または個別製品安全規格ではカバーされていない付加的側面を有する場合には、常にリスク低減戦略をとる必要がある。また、個別製品安全規格では考慮されていない状況を確認するために、次節に記載されるリスク低減プロセスの最初の 2 つのステップ、すなわち機械類の制限の決定と危険源の同定は必ず実施しなければならない。

5.2　リスク低減戦略

ISO 12100-1 で説明されるリスク低減のプロセスは、ISO 13849-1 の図 1 にも引き継がれ、本規格で具体化される局面を補足するものとなっている（本書 24 ページ、図 5.1 参照）。はじめに、リスクアセスメントを行う。ここで注意しなければならないのは、初回のリスクアセスメントは、機械には保護方策がまったくとられていないことを前提に実施するということである。最終的に、このリスク低減の全プロセスにより、採用すべき保護方策並びに安全防護物の種類及び「レベル」が決定される。

---

[1] 安全機能は特に制御システムの安全関連部により実現される。安全関連部は、例えばクラス 2 のポジションスイッチによる保護扉の位置検出による、安全関連の入力信号の認識が開始点となる。この場合、扉に取り付けられた分離型アクチュエータがすでに安全関連部であり、信号処理部に接続されて、出力信号が発生する。電磁接触器によりモータが主回路に接続される場合には、電磁接触器は制御システムの安全関連部となるが、ケーブルにより接続されるモータは安全関連部には属さない。

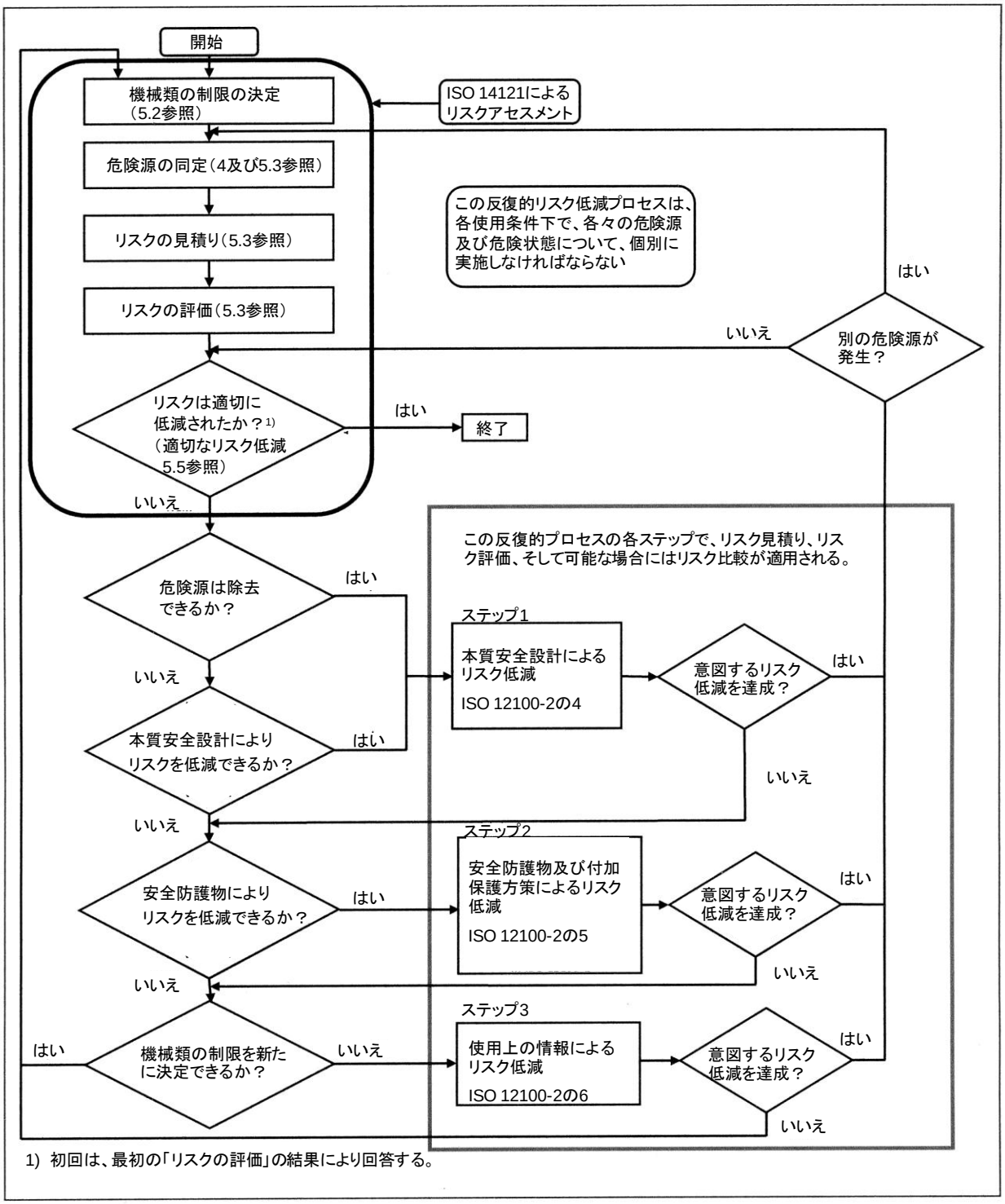

図5.1： リスク低減のための反復的プロセス

リスク低減のためのプロセスは、機械類の制限の決定が開始点となる。ここでは、機械の空間上の制限及び時間的制限の他、特に使用上の制限を考慮する必要がある。使用上の制限では、機械のすべての運転モード及びさまざまな介入の可能性などを含めた機械の意図する使用（例えば加工に使用してもよい材料）と、さらに機械の合理的に予見可能な誤使用についても考慮される。

続いて、危険源の同定を行う。これについては、機械の全ライフサイクルにわたり実施すること、そして自動運転だけでなく、特に手の介入を要する次の運転モードに注意する必要がある。

- 据え付け
- 試験
- ティーチング／プログラミング
- 立ち上げ
- 材料の供給
- 製品の取り出し
- 不具合の発見及び除去
- 清掃
- 保全

本プロセスの詳細については、ISO 12100-1 及び ISO 14121-1［4］を参照いただきたい。危険源を体系的に特定するためにはさまざまな手法があり、ISO/DTR 14121-2［5］にはそのいくつかの例が紹介されている。想定される危険源についても前述文献［4］で一覧化されており、図 5.2 はその一部を抜粋したものである（25 ページ参照）。

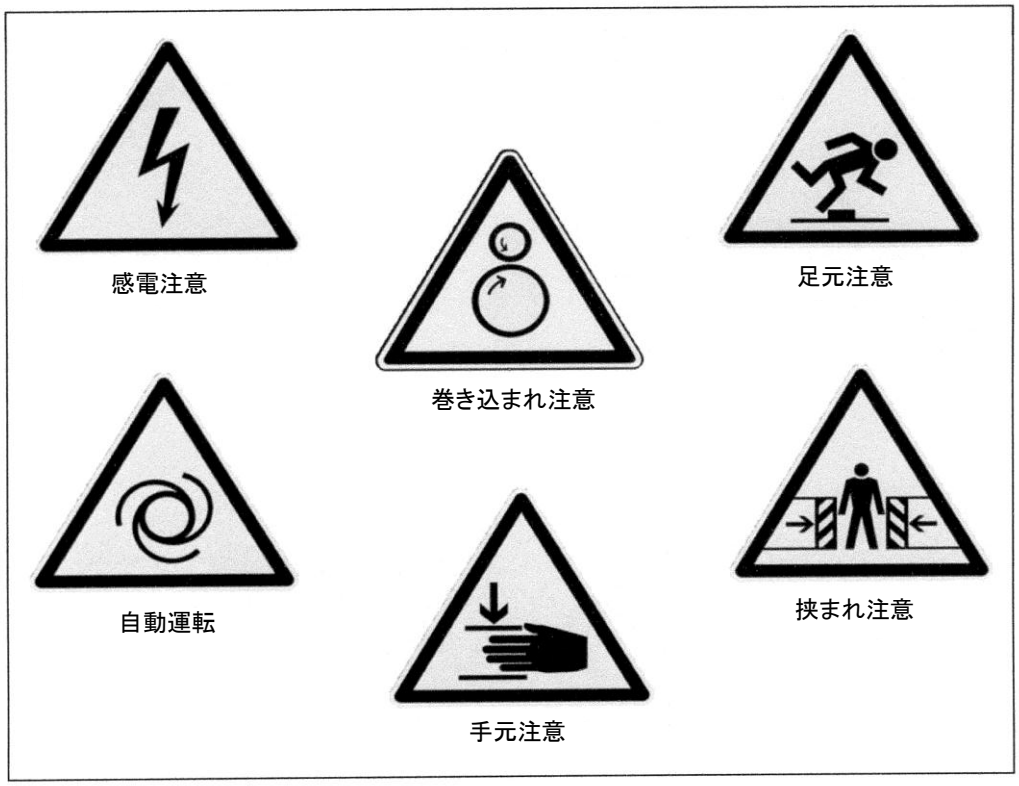

図5.2：　危険源の例　（出典：Wikipedia）

5.2.1　リスクの見積り

機械に起因する危険源をすべて調査したら、次は各危険源に対するリスクを見積もらなければならない。特定の危険状態に関連するリスクは、次のリスク要素から導くことができる。

a)　危害のひどさ

b)　危害の発生確率
　考慮すべき要素：
　－　一人又は複数の人が危険源にさらされる頻度及び時間
　－　危険事象の発生確率
　－　危害を回避又は制限する技術的あるいは人的可能性

リスクは、段階的アプローチによって受け入れ可能なレベルまで低減される。図 5.3（26 ページ参照）には、制御システムの安全関連部のリスク低減に対する貢献度が、これがない場合と比較して示されている。リスクをテーマにした詳しい情報は、BGIA ハンドブック［18］を参照いただきたい。

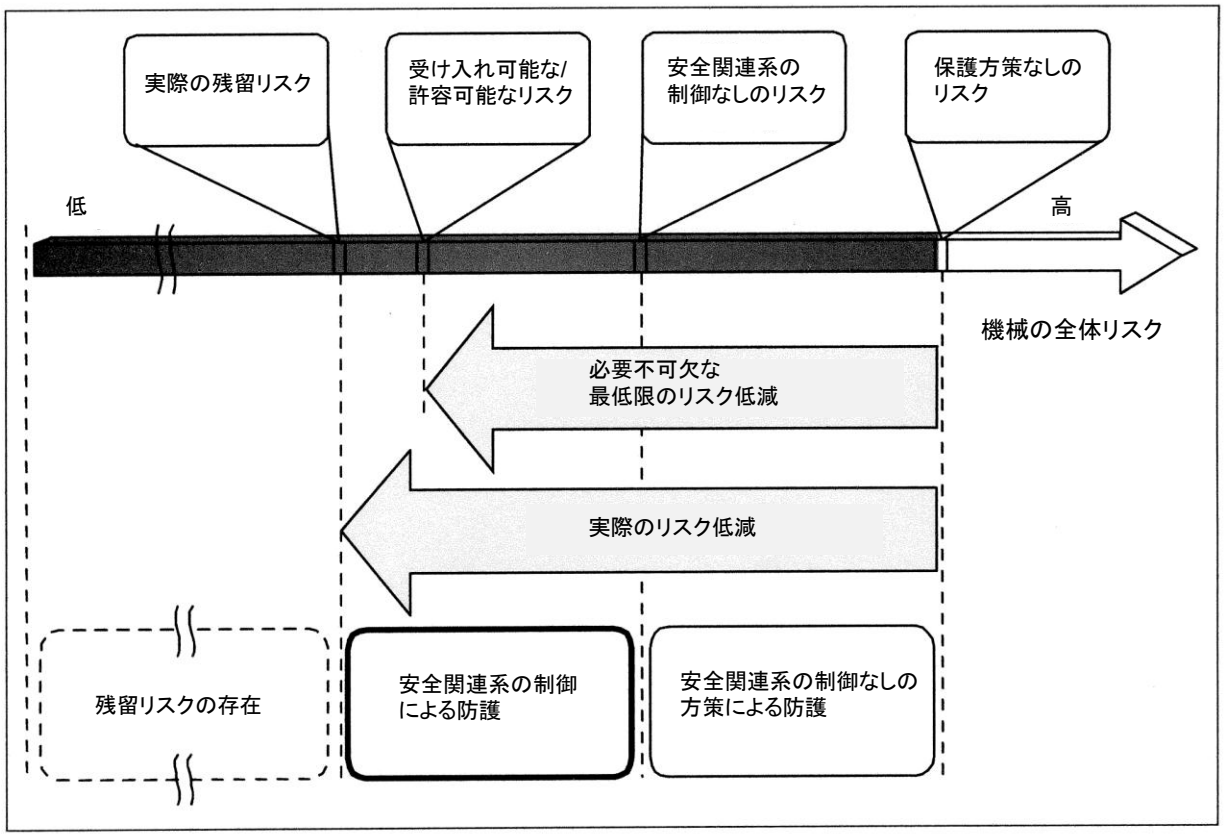

図5.3：　リスク見積りとリスク低減

5.2.2　リスクの評価

リスクの見積りに続いて、リスク低減が必要かどうか決定するためにリスクの評価を行う。適切なリスク低減に関する基準は、ISO 12100-1 で次のように定められている。

- すべての運転条件及びすべての介入方法を考慮したか？
- 危険源は適切な保護方策により除去されたか、もしくはリスクは実現可能な最も低いレベルまで低減されたか？
- 採用する方策により新たな危険源が生じないのは確かであるか？
- 使用者に残留リスクについて十分に通知し、かつ警告しているか？
- 保護方策の採用によりオペレータの作業条件及び機械の使用性が妨げられないのは確かであるか？
- 採用した保護方策は互いに支障なく成り立つか？
- 専門及び工業分野の使用のために設計された機械が非専門及び非専門工業分野で使用されるとき、それから生じえる結果について十分に配慮したか？
- 採用した方策によりオペレータの作業条件及び機械の使用性が損なわれないのは確かであるか？

5.3　必要な安全機能とその要求特性

リスクがまだ受け入れ可能なレベルには達していないと評価された場合には、適切な安全防護物を装備する必要がある。しかしながら、まずは機械の設計変更により危険源を回避（本質的安全設計)、もしくは少なくとも低減することに努めなければならない。また、原則的には、使用上の情報（組織的安全方策を含む）によるリスク低減も可能ではあるが、これは技術的保護方策によるリスク低減が経済的側面から不可能とされる場合にのみ例外的に容認されるものである。実際には、大半のケースで、安全防護物が必要になる。そして、これと関連して、制御システムの安全関連部（SRP/CS、Safety Related Parts of Control Systems）により実行される安全機能が特定される（図 5.4 参照)。

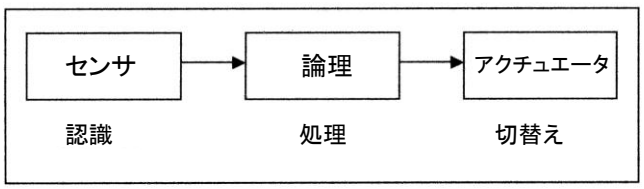

図5.4： SRP/CSによる安全機能の実行

制御システムの安全関連部の設計に関しては、[6] により反復的プロセスが規定されている（図 4.1）。図 5.5 はその中から本章で重要となる部分を抜粋したものである。

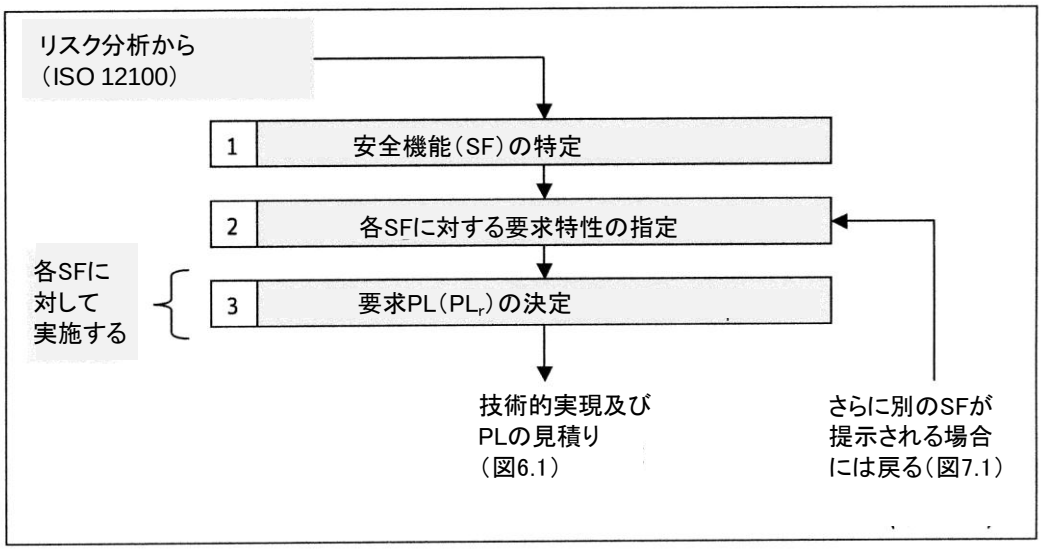

図5.5： 制御システムの安全関連部（SRP/CS）の設計のための復的プロセスからの抜粋

5.3.1 安全機能の特定

必要な安全機能は、用途だけでなく危険源によっても異なってくる。例えば、飛散物（部品や物体の飛散）が予測される場合にはライトグリッドでは不十分であり、捕捉装置（ガード）の装備が不可欠になる。安全機能とは、特定の危険源におけるリスクを、（制御技術を含む）方策によって受け入れ可能なレベルに低減する機能のことである。タイプ C 規格による規定がない限りは、安全機能は機械の設計者により決定される。

例：

a) 制御された運動の停止及び停止状態の維持

b) 機械部分の降下により生じる押しつぶし箇所の阻止

c) 目に直接さらされる切断レーザーの出力低減

d) 据え付け作業時の垂直軸の落下防止

e) 人が危険区域に侵入した時のロボットの回避行動

f) 人／身体部位の引き込まれの阻止

g) 第三者が危険区域に介入した時の両手操作制御による閉鎖運動の中断（ライトグリッドにより作動）

本章 5.7 の例（32 ページ参照）にも示されるように、安全な状態を確保するためには複数の安全機能を組み合わせて使用することが多い。例えば、運動の停止では、まず電子式制御により停止するまで減速させ、続いて機械式ブレーキにより停止状態を保つという手段がとられる。安全機能に関しては次の 2 つの表を参考にしていただきたい。表 5.1 には、ISO 13849-1 の 5.1 による代表的な安全機能と、補足としてその適用例が示されている。尚、ここで挙げられる「非常停止機能」は安全防護物の構成要素ではないが、付加保護方策を実現するために使用される（本書 5.5 参照）。表 5.2（28 ページ参照）には、さらに、IEC 61800-5-2（PDS/SR, Power Drive Systems/Safety Related、可変速電気駆動システム/安全関連部）［19］による安全な駆動制御機器に関する安全機能が示される。本規格には特に、予期しない起動の阻止 STO（Safe Torque Off、旧 SH：安全な遮断、安全な停止 SS1 及び SS2、安全な制限速度 SLS（Safely-Limited Speed、旧 SRG：安全な低減速度）に対して頻繁に使用される安全機能が含まれている。

表 5.1：ISO 13849-1 の安全機能

安全機能	適用例
安全防護物により始動される安全関連の停止機能	安全防護物の作動に対する STO、SS1 又は SS2 の実行（表 5.2）
手動リセット機能	人が危険区域内にいないことの確認
起動／再起動機能	ISO 12100-2 による制御式ガードの場合にのみ許可
ローカルコントロール機能	危険区域内にある現場での機械運動の制御
ミューティング機能	保護装置の機能の一時的中断、例）材料の搬送
ホールド・ツー・ラン制御装置（インチングスイッチ）	危険区域内にある現場での機械運動の制御、例）調整作業
イネーブル機能	危険区域内にある現場からの機械運動の制御、例）調整作業
予期しない起動の阻止	危険区域への手動介入
捕捉された人の脱出及び救助	ロールの引き離し
絶縁とエネルギー散逸機能	油圧バルブの開放による圧力の除去
制御機能と運転モードの選択	運転モード選択スイッチによる安全機能の能動化
非常停止機能	非常停止機器の操作に対する STO 又は SS1 の実行（表 5.2）

表 5.2：IEC 61800-5-2 の安全機能

略号	用語／英文	用語／和文	機能
STO	Safe Torque Off	安全トルクオフ（出力遮断）	モータに電力を供給しない：回転運動は発生しえない：EN 60204-1 の停止カテゴリ０に相当
SS1	Safe Stop 1	安全な停止 1	モータの遅延停止：減速を監視し、停止後、又は一定時間経過後 STO : EN 60204-1 の停止カテゴリ１に相当
SS2	Safe Stop 2	安全な停止 2	モータの遅延停止：減速を監視し、停止後、又は一定時間経過後 SOS : EN 60204-1 の停止カテゴリ２に相当
SOS	Safe Operating Stop	安全な運転停止	モータは停止し、かつ外力に耐えうる（停止位置からのずれを防ぐ）
SLA	Safely-Limited Acceleration	安全な加速制限	加速制限値の超過を防ぐ
SLS	Safely-Limited Speed	安全な速度制限	速度制限値の超過を防ぐ
SLT	Safely-Limited Torque	安全なトルク制限	トルク及びパワーの制限値超過を防ぐ
SLP	Safely-Limited Postion	安全な位置制限	位置制限値の超過を防ぐ
SLI	Safely-Limited Increment	安全な回転角制限	モータを指定の角度だけ回転させて、停止させる
SDI	Safe Direction	安全方向	意図しないモータの回転方向を防ぐ
SMT	Safe Motor Temperature	安全なモータ温度	モータの温度制限値超過を防ぐ
SBC	Safe Brake Control	安全なブレーキ制御	外部ブレーキの安全な制御
SCA	Safe Cam	安全なカム機構	モータ位置が指定域にある間、安全出力信号を発生する
SSM	Safe Speed Monitor	安全な速度監視	モータ回転数が指定値以下にある間、安全出力信号を発生する
SAR	Safe Acceleration Range	安全な加速範囲	モータの加速を指定制限値内に保つ

1 つの安全機能を実行するには、さまざまな方法が考えられる。このため、安全機能の選択と共にいくつかの特性を考慮して、それぞれの用途に対して個別にその方法を決定していく必要がある。安全機能特性には、次のものが含まれる。

- 異なる運転モード（自動運転、調整運転、障害の除去など）での使用
- 安全機能の応答時の反応
- 安全機能の不具合検出時の反応

- 応答時間
- 操作頻度
- 複数の安全機能が同時に作動しえる場合の、優先順位
- 安全関連パラメータの指定　例）許容最高速度
- 要求パフォーマンスレベル　PL_r

5.3.2　安全機能の定義付け　－PL の算定に及ぼす影響－

安全機能に関する単位時間当たりの危険側故障率の評価については次章で説明するが、そのベースは、安全機能の定義付けにあるといってよい。安全機能を実装するに当たっては当然ながら、これに必要なコンポーネントの種類及び量が決定される。このため、安全機能の定義付けは、安全に係る信頼性の評価に重要な影響を及ぼすものとなる。これについて、次にいくつかの例を挙げて説明する。

例 1：安全機能「保護扉開放時の停止」

保護扉の開放により、機械オペレータは危険区域に接近することができる。この危険区域では、機械部分の運動が 5 台の駆動装置により制御される。保護扉が開放されると、5 台の駆動装置はすべて速やかに（可能な限り速く）停止する。図 5.6 に、この機能ブロック図を示す。

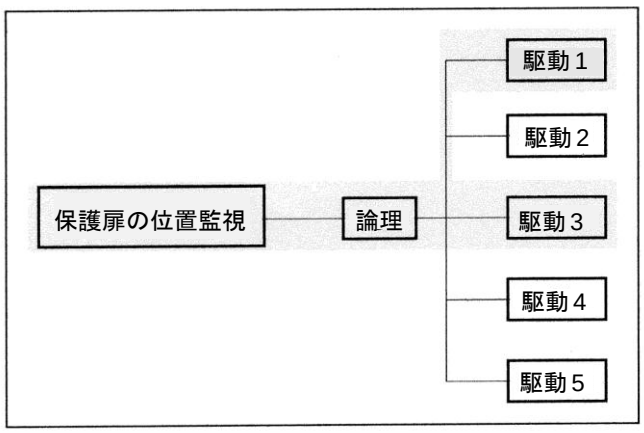

図5.6： 保護扉開放時の停止

これに従って、後で例えば表 6.6（本書第 6 章参照）を用いて安全機能の PL を評価しようとした場合、次の各ブロック[1]の PL がその決定に関与することになる。

- 機械コンポーネントを含む保護扉の位置監視

- 論理
- 駆動　x　（x = 1, 2, .., 5）

---

[1] 電気設備の不具合の可能性は、各ブロックに割り当てられる。
しかし、オペレータに対し危険な機械運動を引き起こすのは駆動装置 1 と 3 のみであり、その他の駆動装置の停止は純粋な「機能的配列」によるものだとしたら、それが考慮されていない場合には、十分な PL が達成されていないという結果につながる可能性がある。ここでは、安全機能に関しては、実際に危険源となる運動のみを考慮することがポイントになる。

例 2：安全機能「保護扉開放時の停止」

危険な機械運動はフェンスにより防護され、フェンスには 5 台の保護扉が備えられている。保護扉の 1 台が開放されることにより機械運動は停止する。後で実施する PL の評価を視野に入れ、各扉を、個別の安全機能 SF1 から SF5 のそれぞれの構成要素とする。各安全機能は次のブロックから構成される。

- 機械コンポーネントを含む保護扉 x　（x = 1, 2, .., 5）の位置監視
- 論理
- 駆動

これに関する機能ブロック及び安全機能 SF3 のブロックを、図 5.7 に示す。

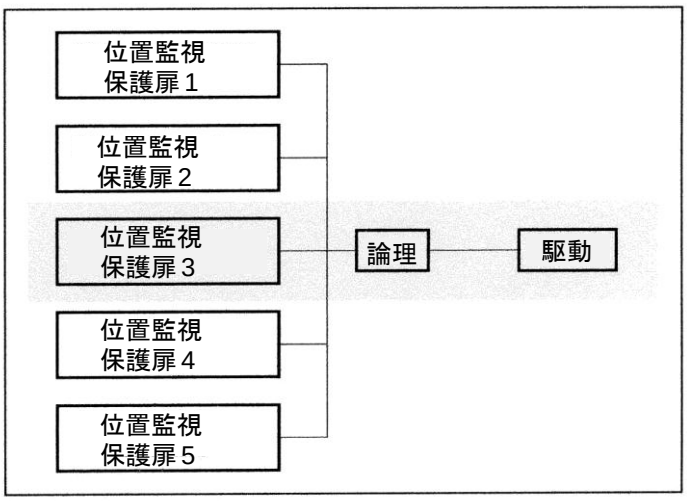

図5.7：　保護扉 3の 開放時の停止

例 3：安全機能「機械全体の非常停止」（本書 5.5 参照）

1 台の大型機械に非常停止機器が 20 台設置され、この非常停止機器の作動により 50 台の駆動装置がすべて速やかに（可能な限り速く）停止する。このようなケースでは、安全機能の実現においてどのコンポーネントを考慮すべきであろうか？この場合、20 台ある中のどの非常停止機器により安全機能が作動するか予測できない。しかし、オペレータにより操作される非常停止機器は常に 1 台とみなしてよいので、SF1 から SF20 の安全機能が定義付けされる。非常停止が作動する際には危険にさらされる人が存在するのは確かであるが、どの場所にいるのかはわからない。また、50 台の駆動装置がすべて危険源に関与しているわけではない。このような場合には、考えられるすべての状況ではなく、最も不利なケースを考察する。そして、これは最も低い PL により決定される。このため、最も好ましくない場所で危険な運動を発生させるセーフティチェーンにおける駆動装置の数とその個々の PL に、ある程度依存することになる。これに関する機能ブロック図を、図 5.8 に示す（30 ページ参照）。

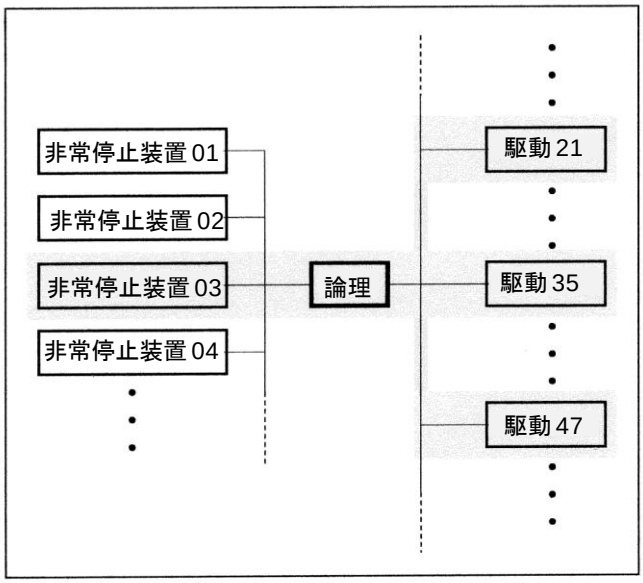

図5.8： 機械全体の非常停止、最も不利なケース

後で、例えば表 6.6 に従って安全機能の PL を決定する場合には、次の各ブロックの PL 値を考慮しなければならない。

- 非常停止機器 03
- 論理
- 駆動 21
- 駆動 35
- 駆動 47

この例では、安全機能を定義付けするに当たっては、次の視点を考慮した「局所的」見方をする方が望ましいといえる。

- 考察対象となる時点で、人はどの場所に存在するか？
- 人が存在する場所では、どのような運動が危険源になるか？
- どのような保護装置により、安全機能を作動すべきか？必要に応じて、選択肢となる複数の保護装置を考慮する。

5.4 要求パフォーマンスレベル PL_r の決定

選択されたそれぞれの安全機能に対して、要求パフォーマンスレベル PL_r [1]、つまり技術的な目標値を決定する。要求されるレベルは必要なリスク低減の結果であり、PL_r を決定するに当たっては特に、既知の災害事例を考慮する必要がある。必要なリスク低減の度合いを決定するための手法は、ISO/DTR 14121-3 にいくつか紹介されている。ISO 13849-1 で用いられるリスクグラフは、その中の 1 つである。

5.4.1 リスクグラフ

要求パフォーマンスレベル PL_r は、本規格附属書 A のリスクグラフから直接求めることができる。以下に、これについて解説する（図 5.9 参照）。尚、PL_r の決定に関する詳細例は、附属書 A を参照いただきたい。

リスクグラフの出発点から、次の 3 つのパラメータ [2] を順次評価していくことにより、要求 PL_r が決定される。

- S－傷害のひどさ
- F－危険源への暴露頻度及び／又は暴露時間
- P－危険源回避の可能性、又は危害を制限する可能性

---

[1] r（required）が付く場合には、安全機能に対する要求パフォーマンスレベル（目標値）を指すことに注意する。後で行う妥当性確認で、実際の制御システムにより達成される PL（実際値）が PL_r と同等以上（$PL \geqq PL_r$）であるかどうかチェックされる。「＞」で表わされる関係は次のとおりである。PL = e > PL = d > PL = c > PL = b > PL =a

[2] 危険事象の発生確率を確定することは、実質的にはほとんど不可能である。このため、リスクグラフでは簡易的にもっとも不利なケースが採用される。それ以外の評価は要求されない。

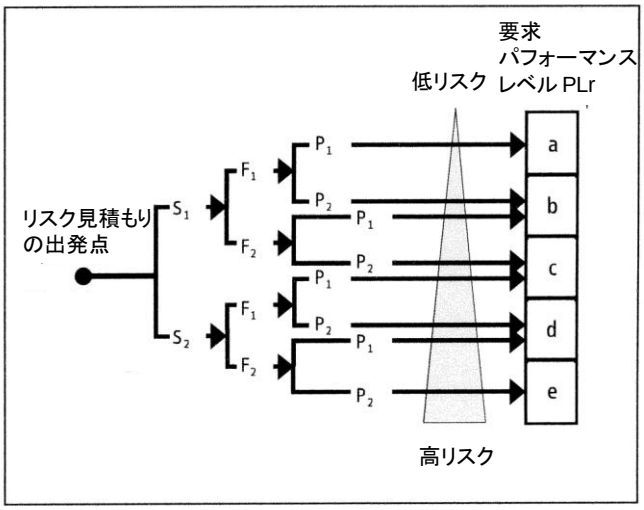

図5.9： 各安全機能に関するPL_r決定のための
リスクグラフ

この分析は、各安全機能に対して、その安全機能により達成されるリスク低減を考慮せずに行わなければならない。ただし、機械式ガードや付加的安全機能など、制御システムには依存せずに実装される他の技術方策がある場合には、PL_rの決定においてそれらの効果を前提にすることができる。

傷害のひどさ　S1 と S2

危険源の傷害のひどさに関しては、一般的にはさらに異なる分類が考えられるが、ここでは次の 2 つに大別される。

- S1－軽傷（通常回復可能とされる傷害）
- S2－重傷（死亡を含め、通常回復不可能とされる傷害）

S1 又は S2 を決定するに当たっては、事故災害の一般的結果及び通常予測される治癒プロセスが考慮される。

危険源への暴露頻度及び／又は暴露時間　F1 と F2

危険源への暴露頻度及び暴露時間は次のように評価される。

- F1－まれから低頻度及び／又は暴露時間が短い
- F2－高頻度から連続及び／又は暴露時間が長い

F1 又は F2 を決定付ける境界は、残念ながら特定することはできない。しかし、本規格には、1 時間に 1 回を超える頻度で介入する場合には F2 を選択し、それ以外は F1 を選択すべきであるという参考基準が示されており、これは、一般的に見て、実際のあらゆるケースに適用できると考えられる。危険源への暴露時間については、機械の全使用時間に対する平均値を考慮して評価すべきである。しかしながら、例えば金属加工での手送り式プレスや機械の工具間への介入が周期的に必要とされる場合には、F2 を選択すべきであるのは明らかである。反対に、調整等は年に一度しか行われず、あとは自動運転を行うマシニングセンタの場合には、間違いなく F1 が選択される。選択頻度及び時間を評価するに当たっては、危険源にさらされる人が常に同一か、あるいは異なるかにより区別してはならない。

危険源回避の可能性　P1 と P2

ここでは、危険状態を回避できる可能性を次のように評価する。

- P1－特定の条件では可能
- P2－ほとんど不可能

このパラメータを決定するに当たっては特に、機械の物理的特性とオペレータの反応が重視される。例えば速度を制限して行わなければならない調整運転の場合には、加速度は非常に小さいので、パラメータ P1 を選択するのが適切といえる。危険状態が緩やかに発生するケースでは、可動空間が十分にありさえあれば、危険区域から退避することが可能だからである。一方、速度が急激に高まる可能性があり、オペレータの退避により災害を回避できるチャンスが現実的に存在しない場合には、P2 を選択すべきである。この評価に関しては、物理的な方法による制限のみを考慮する。つまり、制御技術的要素による制限は、不具合により故障すると正常に機能しない可能性があるため、考慮すべきではない。ローラーの回転を例に挙げると、その回転方向がオペレータの手に向かったものであれば、正常な運転状態にある限りはローラー間に手が引き込まれることはないが、制御システムに不具合が生じた場合には、回転方向が変わり、最悪の事態として手が引き込まれてしまう可能性が十分考えられる。

安全機能の構築については次の第 6 章で取り上げる。

5.4.2　EN 954-1 による要求カテゴリから PL_r への移行

ISO 13849-1:2007 を適用するためには、PL_r に関する知識が必要不可欠である。前節で述べたように、PL_r を決定するためにはリスクを見積もらなければならない。もし、EN 954-1:1997 で慣れ親しんだ**要求カテゴリ**から PL_r を導くことができたとしたら、規格作成者及び機械製造者の双方に

とって事はもっと簡単に済むところであるが、残念ながらこの可能性は、一台の機械に同一のレベルのリスクを有する同一の危険源しか存在しない場合にしか認められない。それでは、新たにリスクの見積りをせずに PL_r を決定することはできないのだろうか？

EN 954-1 による要求カテゴリも、本新規格による PL_r も共に、リスクの見積りにより決定される。しかし、EN 954-1 のリスクグラフにより要求カテゴリを選択し、そこで使用したパラメータ S、F、P（5.4.1 参照）を新規格のリスクグラフに転用してみると、PL_r による区分はすべての要求カテゴリ対して必ずしも明確なものではないことがわかる。

さらに、EN 954-1 による要求カテゴリを PL_r に置き換えた場合には、SRP/CS の実現すべき構造に関する要求事項が見失われる可能性も出てくる。第 6 章で、カテゴリ 2 での診断機能やカテゴリ 3 での単一不具合（障害）に対する耐性など、カテゴリと指定のアーキテクチャの関係について説明するが、もし、EN 954-1 による要求カテゴリ 3 を PL_r 「d」に分類した場合、安全機能はカテゴリ 2 でも実現される可能性がある（図 6.10 参照）。つまり、要求カテゴリを PL_r に単純に置き換えてしまうと、従来のカテゴリ 3 による高レベルの単一不具合（障害）に対する耐性が、試験機器を備えた単一チャンネル構造によっても実現可能ということになる。

この点は、新規格により意図された自由度を示すところでもあるが、PL_r を決定するに当たっては十分に考慮する必要がある。また、要求カテゴリの選択では特に SRP/CS の不具合（障害）発生時のリスクに注意を要する（EN 954-1 の 6.3 及び ISO 13849-1 の 6.1 を参照）。この要求事項は、EN 954-1 による要求カテゴリ 3 を決定するための事例で取り上げられていたはずである。

以上の観点から、EN 954-1 による要求カテゴリを PL_r に置き換える場合には、それなりの情報を補足する必要があると考えられる。しかしながら、そのような情報は一般的にはもはや入手できるものではない。新たなリスク分析が行われない場合には、表 5.3（32 ページ参照）に示すように、PL_r と要求カテゴリを同時に決定する「ワーストケース・アプローチ」が近道になるだろう。この場合、EN 954-1 に従って「優先すべきカテゴリ」の代わりに「可能なカテゴリ」を選択するためにとられてきた追加方策を、引き続き実施することが前提条件になる。

表 5.3：
EN 954-1 による要求カテゴリを要求パフォーマンスレ

EN 954-1:1997 による 要求カテゴリ		ISO 13849-1:2007 による 要求パフォーマンスレベル及びカテゴリ
B	➔	B
1	➔	C
2	➔	d, カテゴリ 2
3	➔	d, カテゴリ 3
4	➔	e, カテゴリ 4

5.5　付加保護方策

付加保護方策に関する要求事項は、ISO 12100-2［3］の 5.5 に記載される。本レポートで取り上げる制御技術の問題に関しては、特に次の内容を理解する必要がある。

- 緊急時の停止
- 運動の逆転
- エネルギーの遮断及び消散

定義からすれば、これらは、その技術的実現に当たって特定のパフォーマンスレベルを要するような技術的方策ではない。しかしながら、技術的保護方策（ガード及び／又はガード以外の安全防護物）が故障あるいは偽操作により効果を失った場合には、こうした付加保護方策の作動が要求される。特にこのようなケースでは、非常停止機能等が実際に使用できるものであることが重要である。この点に関しては、機械の制御回路及び制御機能に関する EN 60204-1［20］の要求事項が考慮される。本規格の 9.4「故障時の制御機能」では、安全技術の性能に関し適切なレベルが要求されており、これは機械のリスク評価により決定される。結果的に、ISO 13849 の要求事項はこの付加保護方策についても適用されることになる。付加保護方策は、いかなる場合にも、安全防護物の機能及びレベルに影響を及ぼすものであってはならない。

5.6　旧型機械の取扱い

旧型機械というのは、ここでは、機械指令の発効以前にすでに市場に流通した機械をいう。本指令の要求事項は、この種の機械には適用されない。しかし、旧型機械が拡張、変更、改造などされる場合には、適用対象となる可能性がある。これについては本質的な変更があるかどうかがポイントになる。本質的な変更が認められた場合、EC 機械指令の要求事項はこの「旧型機械」にも同様に適用されることになる。これには、ISO 13849 の適用も含まれる。「本質的な変更」があるかどうか決定するに当たっては、化学工業・職業保険組合のチャート図［21］を利用するとよい。

5.7　リスク低減の実施例
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」）

次に、ISO 13849-1 の断裁機への適用例を紹介する。ここでは、全体のプロセスではなく、特定の視点について詳しく見ていくことにする。

本例における断裁機（図 5.10 参照）は、紙あるいはそれに類する材料を積み重ねたものをカッ

ターで切断するために使われる。被断裁物はほとんどの場合は手によりカッターの下に置かれる。断裁の直前に、原紙の束を固定するためにプレスクランプが大きな力を伴って降下する。カッターとプレスクランプの駆動は油圧式である。

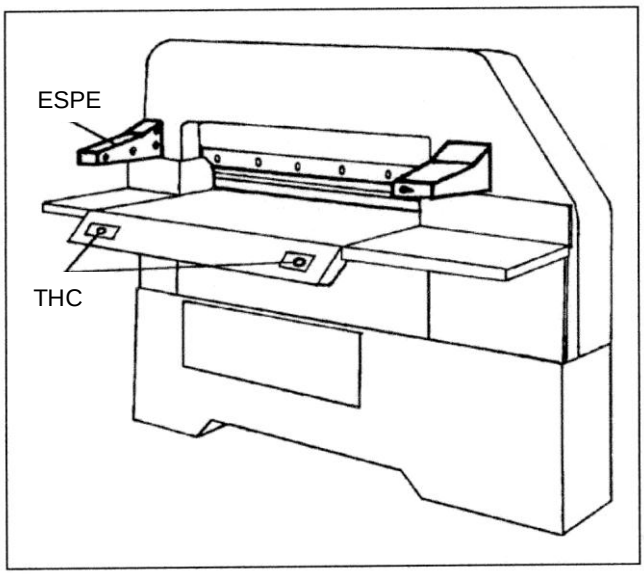

図5.10：断裁機、
両手操作制御装置（THC）及び電気的検知保護装置（ESPE）付

5.7.1 機械の制限の決定

空間上の制限

断裁機は手送り式であるため、オペレータに対し十分な運動空間を確保する共に、被断裁物の準備や、切断された紙束の搬出及び保管、紙屑の処理のためのスペースが必要になる。

時間上の制限

用途に応じて、機械はおおよそ 20 年間にわたり使用することができる。部品の摩耗により運動停止に要する時間が長くなる可能性があるため、これにより生じるオーバーランの超過を検出し、機械を停止させる必要がある。

使用上の制限

機械の意図する使用は、積み重ねた紙あるいはそれに類する材料の切断である。機械は手送り式で、一人のオペレータにより操作される。しかしながら、据え付け場所及び機械幅によっては、複数の人が周囲にいる可能性を排除することはできない。

意図された運転モード：

1. プレス

2. 手動断裁（個々の断裁）

3. 自動断裁（最初の手動断裁後の自動プロセス）

4. カッター交換

最初の 3 つの運転モードでは、断裁の位置合わせをするために、プレスクランプのみを動作させることができる。ここでは、オペレータはフットペダルを使って操作し、同時に危険区域に手を入れて紙束の位置を調整することができる。

5.7.2 危険源の同定

断裁機では、次の機械的危険源が重要である。

G1－プレスクランプによる押しつぶし

G2－断裁中のカッターによる切断

G3－静止中のカッターによる切断

リスクの見積り

プレスクランプの動的押付け力（危険源 G1）は非常に大きいため、回復不能な挫傷の他、骨折を引き起す可能性が考えられる。また、危険源 G2 については四肢の切断の可能性を想定しなければならない。危険源 G3 では、例えば紙束の位置調整を行うときに静止しているカッターで手又は前腕に損傷を負う可能性が考えられるが、これは通常は回復可能なものと考えてよい。

定常運転において周期的に危険区域に手を差し入れる必要があるため、オペレータの危険源への暴露頻度は非常に高いといえる。

プレスクランプ及びカッター（危険源 G1 及び G2）の降下速度は非常に速く、現実的に、オペレータがこれらの危険源を回避できる可能性はない。静止状態のカッター（危険源 G3）の場合には、危害を回避又は制限することは可能である。

危険事象の発生により導かれる危害の発生確率はワーストケースの結果を想定したものなので、ここでは評価されない。

リスクの評価

あらゆる運転条件及び介入の可能性を考慮すると、リスク低減が必要であると判断される。

本質安全設計

プレスクランプの動的押付け力とカッターのエネルギーを低減することは、機械の機能を制限することになるため不可能である。また、オペレータによる紙束の正確な位置調整が必要になるため、オペレータの危険区域への介入を阻止する機械の配置及び設計も不可能である。

しかしながら、次のような方策をとることは可能である。

1. 操作に必要な面を除くすべての危険区域へのアクセス面を覆う。
2. 鋭利な角部及び端部を回避する。
3. オペレータの適切な作業位置及び接近性に配慮する。
4. 機械の設計に、人間工学原則を適用する。
5. 電気的危険源を阻止する。
6. 油圧装置による危険源を回避する。

5.7.3 必要な安全機能

あらゆる運転条件及び介入の可能性を考慮すると、次の安全機能が必要になる。

SF1－予期しない起動を回避するための STO（セーフトルクオフ）

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。

SF3－ESPE（ライトグリッドなどの電気的検知保護装置）により第三者の侵入を検知し、即座に断裁を中止する。

SF4－個々の断裁及び自動断裁プロセスが終了する毎に、すべての機械運動は自動的に停止する。

SF5－「断裁位置の表示」が機能する間は、プレスクランプの動的押付け力を低減する。

SF6－断裁が中断した場合には、プレスクランプ及びカッターは自動的に開始位置に戻る。

SF7－プレスクランプによりカッターをカバーする。

安全機能の要求特性

ライトグリッドにより侵入が検知されたら、即座に断裁を中止する。このため、安全機能 SF3 は、SF2 よりも優先度が高い。SF5 については、「断裁位置の表示」におけるプレスクランプの最大許容力を指定する（EN 1010-3 参照）。

5.7.4 要求パフォーマンスレベル PL_r の決定

PL_r は、各安全機能に対して決定される。個々の安全機能が使用される状況を分析すると、安全機能 SF1 から SF6 に関しては、リスクパラメータ S、F、P は次のとおり評価される。

S2－通常は回復不可能な重篤な傷害

F2－危険区域への接近が連続的に行われる

P2－危険状態の回避はほとんど不可能

これらの評価から、図 5.9 のリスクグラフに従って要求パフォーマンスレベル PL_r「e」が決定される。図 5.11 は、ソフトウエア SISTEMA での SF1 に関する記載及びリスクグラフを示したものである。

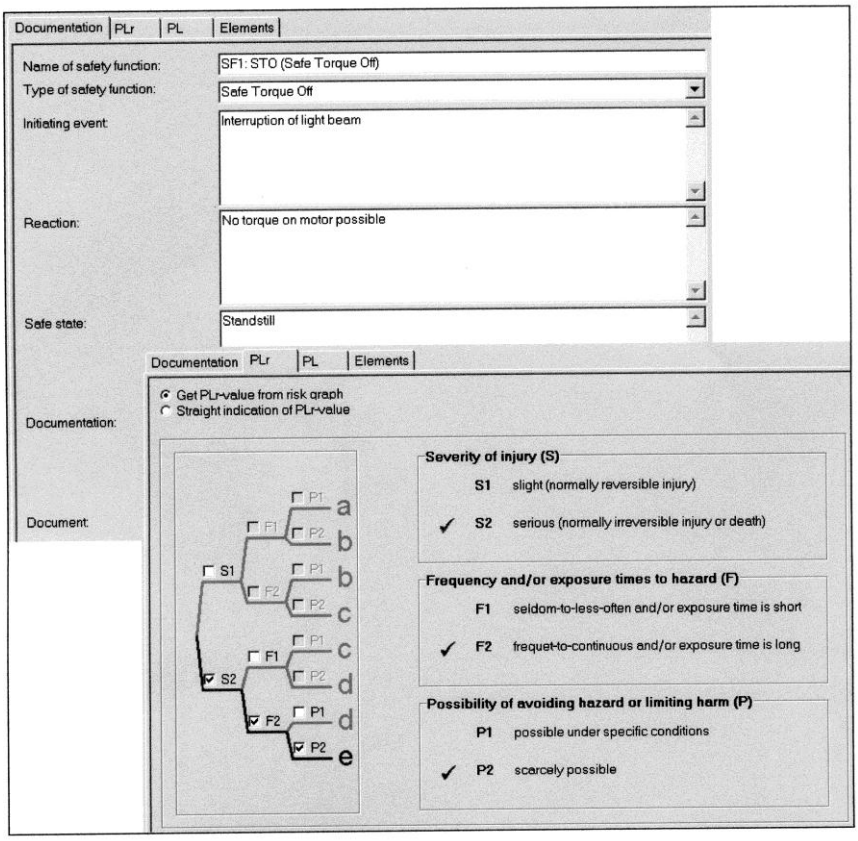

図5.11： SF1に関するドキュメント及びリスクグラフ

危険源 G3「静止中のカッターによる切断」については SF7 が指定される。これに関するリスクパラメータは、次のとおり評価される。

S1－通常は回復可能な軽微な傷害

F2－危険源への暴露時間が長い

P1－危険状態の回避は特定の条件の下で可能

これらの評価から、図 5.9 のリスクグラフに従って要求パフォーマンスレベル PL_r「b」が決定される。図 5.12 は、ソフトウエア SISTEMA での F7 に関する記載及びリスクグラフを示したものである。

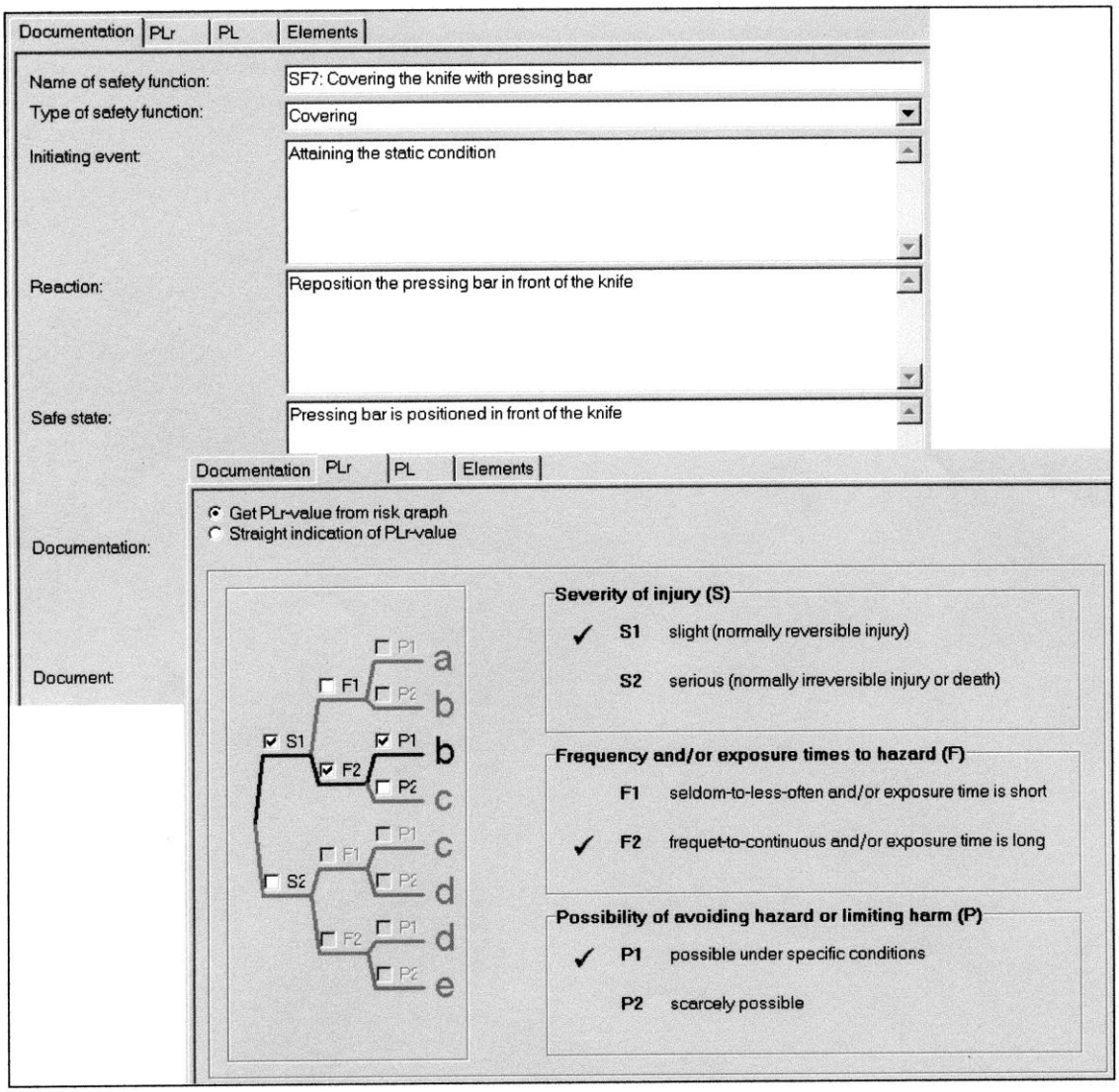

図5.12： SF7に関するドキュメント及びリスクグラフ

5.7.5　付加保護方策

次の付加保護方策が必要になる。

1. 緊急時の停止
   この機械の制御システムには、緊急停止のために用いられる PL「e」に相当する安全機能がすでに実装されている。非常停止機器の配線が 2 チャンネルであるため、緊急時の停止も PL「e」に相当する。

捕捉された人を救出するために、ばね力により実行されるカッターとプレスクランプの戻り運動が必要になる。