7　検証及び妥当性確認

検証及び妥当性確認は、安全機能を実行する制御システムの安全関連部（SRP/CS）のレイアウト設計及び実装における不具合（障害）を回避するための品質保証手段である。本テーマは、特にISO 13849［7］の第 2 部で詳しく取り扱われる。

検証は、開発フェーズあるいは開発セグメントで達成された結果が、例えば回路レイアウトがレイアウト設計と一致しているかどうかなど、そのフェーズに関する規定要求事項が満たされていることを確認するものであり、このために実施される SRP/CS あるいはその各側面の分析及び試験を含む。

また、妥当性確認は、実際の用途に関しての適格性を証明するものであり、開発プロセスの途中もしくは終了時に実施される。つまり、ここでは、機械制御システムの安全関連部に関して仕様書で規定された安全要求事項が達成されたかどうかを審査する。

このため、SRP/CS により技術的に実現される安全機能の査定プロセスは、SRP/CS の各側面及び全体を取り扱う検証と妥当性確認の両ステップを組合せたものになる。以下の説明では、検証及び妥当性確認は V&V アクティビティということばでも表される。

7.1　手順

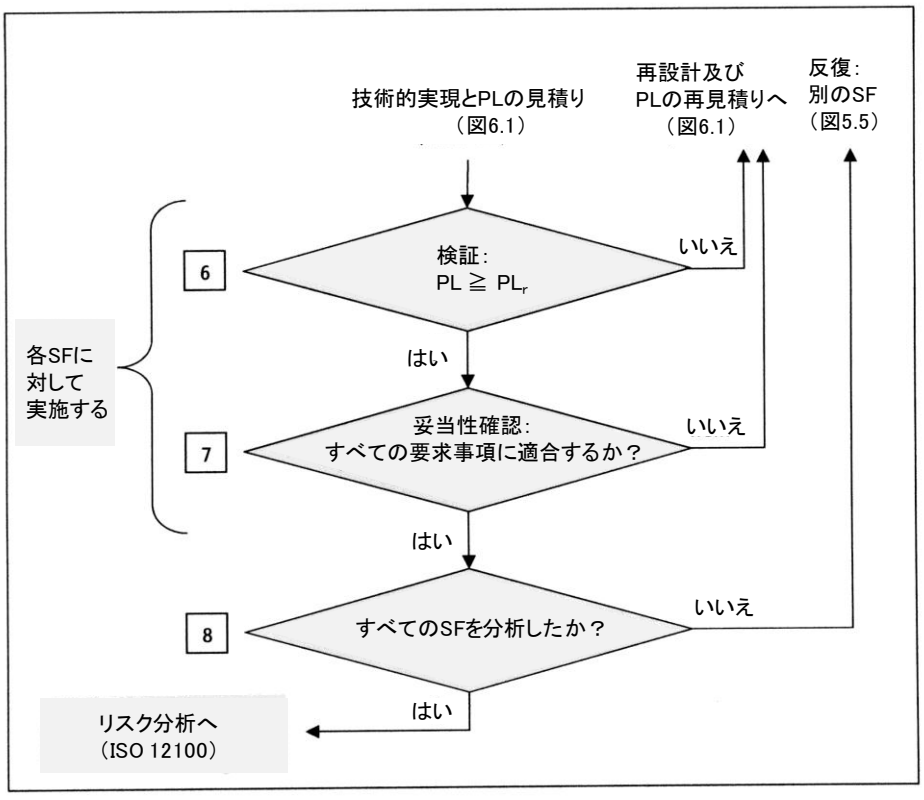

図7.1：
V&Vアクティビティ
（図4.1からの抜粋）

図 7.1 は図 4.1 からの抜粋で、検証及び妥当性確認のアクティビティに関連するブロックを示したものである。

重要な最初の試験は、本図の 1 番目のひし形ブロック（ブロック 6）のフェーズで実施される。実装された各安全機能のパフォーマンスレベル（PL）が最低でも第 5 章で決定された要求パフォーマンスレベル PL_r に達していない場合には、設計及び技術的実現のフェーズに立ち戻る必要がある。そうでない場合には、2 番目のひし形ブロック（ブロック 7）に進むことができる。

必要なステップを計画するに当たっては、図 7.2 の手順を参考にするとよい。本図は 2003 年に発行された ISO 13849 の第 2 部によるもので、V&V アクティビティがより明確に示されている。

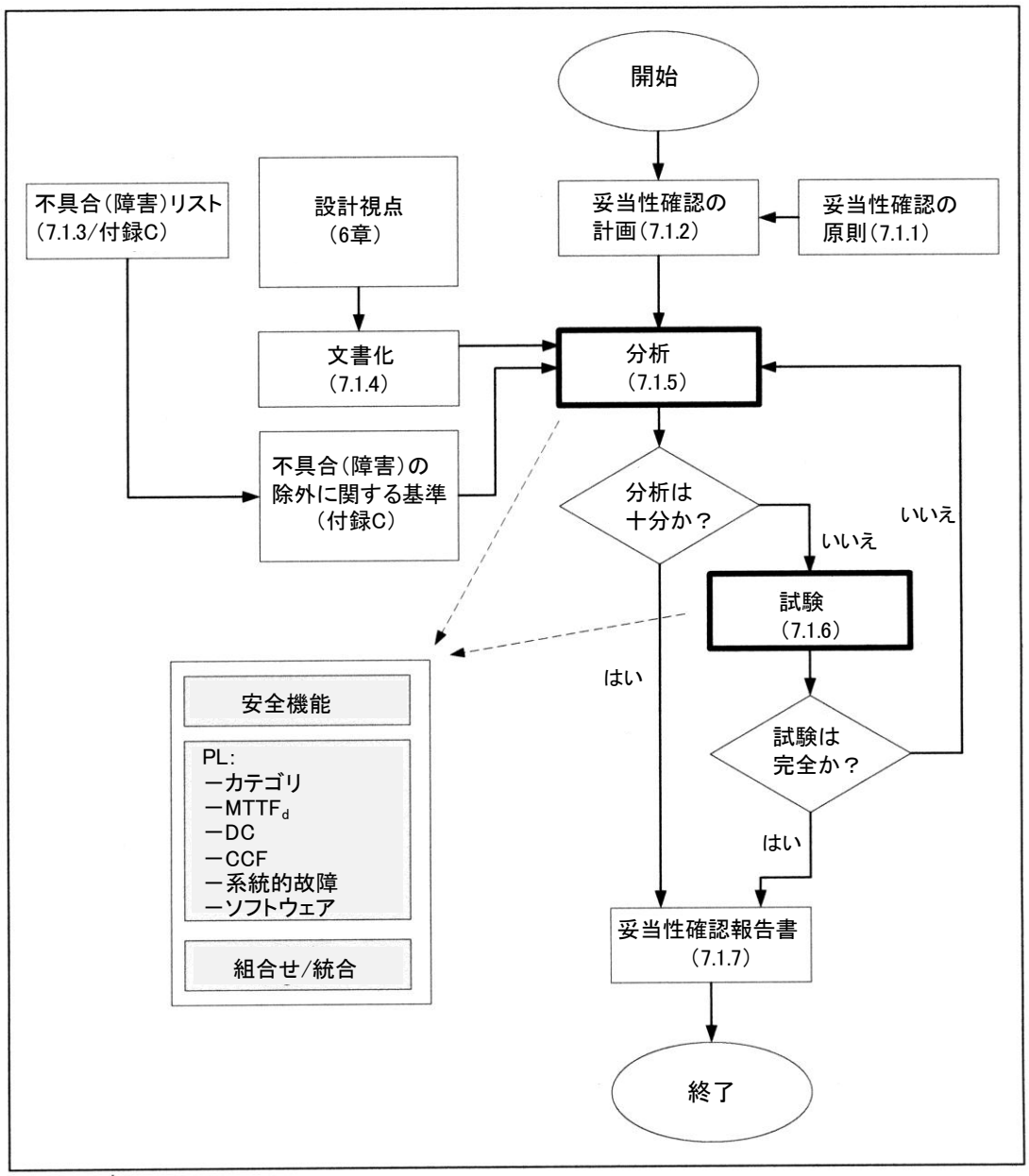

図7.2： ISO 13849-2による検証及び妥当性確認の概観

次に、検証及び妥当性確認の手順における最も重要な視点について簡単に説明する。

7.1.1 検証及び妥当性確認に関する原則

検証及び妥当性確認は、SRP/CS の設計が機械指令に適合するという確証を与えるものでなければならない。ISO 13849-1 は、機械指令の下で整合化された機械制御システムに関する安全規格であるため、V&V アクティビティにより、各安全関連部及びこれにより実行される各安全機能が ISO 13849-1 の要求事項を満たしていることを示す必要がある。このアクティビティを開発時のできるだけ早期の段階で開始することで、不具合（障害）を適時に認識し、除去することができる。試験は、できるだけ、安全関連部の設計プロセスに関与しない人／組織、つまりレイアウト設計及び実装には無関係な立場から実施されることが望ましい。組織構造的に設計部門に従属しない人員、部署、機関ということになるが、この独立性の度合いは、リスク、つまり要求パフォーマンスレベル PL_r に比例するといえる。

検証及び妥当性確認は、分析のみで、もしくは分析と試験を組み合わせて実施される。

7.1.2 検証及び妥当性確認の計画

検証及び妥当性確認の計画（V&V 計画）では、計画されるアクティビティはすべて強制的に適用されるものとして規定する必要がある。これは、次の内容を含むものとする。

- 試験される SPR/CS 製品の特定
- 対象となる SRP/CS に割り当てられる安全機能の特定
- 要求事項の記述／仕様（安全要求事項仕様書 SRS, Safety Requirements Specification）に関する文書類の一覧
- 適用する試験基準（規格）及び独自の標準、設計規則、プログラミングガイドラインなどの社内規定
- 実施すべき分析及び試験の指定、試験仕様書の特定を含む
- 適用される不具合（障害）リスト
- その他の関連文書（例：QM ハンドブック、QA 手順書）
- 分析及び試験の責任者（試験要員、部署、機関）
- 装置及びツール類の指定（記録に明記してもよい）
- 記録化の指定（作成すべき試験報告書及び記録）
- 試験の合否基準の定義、試験に合格しなかった場合の処置を含む
- リリースノートあるいは試験者署名などの形式的側面
- 製品のモディフィケーションにより再実施が必要となる V&V アクティビティ

7.1.3　不具合（障害）リスト

試験手順では、SRP/CS の故障時の挙動を考慮する必要がある。不具合（障害）の考慮に関する基本原則は、ISO 13849-2 の附属書に記載されている（本書付録 C も参照）。これらの不具合（障害）リストは長年の経験及び実績に基づくものである。

適用する不具合（障害）リスト及び不具合（障害）の除外はすべて一覧できるようにする。また、製品及び使用する技術方式に特有の不具合（障害）のリストと不具合（障害）の除外についても、同様の形式で補足しなければならない。これは特に、ISO 13849-2 の不具合（障害）リストには記載されていないコンポーネント及びアセンブリに該当する。不具合（障害）の除外はすべて、十分な根拠に基づくものでなければならない。

7.1.4　文書

図 7.2 に示されるように、V&V アクティビティには綿密な文書化が求められる。開発が進行する中でさまざまな文書が作成される。使用される技術方式によっては異なる場合もあるが、要約すると、次の内容が適切に考慮されている必要がある。

- 安全機能並びにこれらの安全機能を実行する SRP/CS に関するすべての要求事項を記述した仕様書、性能基準、実装されるすべての運転モードの一覧、詳細な機能の説明、プロセスの説明
- 意図した用途に対応した重大度（評価データ）を含む、適用される規格の運転条件及び環境条件
- SRP/CS の設計説明（使用される機械式／電気式／電子式／油圧式／空圧式コンポーネントの仕様を含む）、配線図と接続及びインターフェースの説明、回路図、組立図、コンポーネントに関する技術データ及び評価データ、データシート（該当する場合）
- 使用される不具合（障害）リストに基づいて行われる、故障モード及び影響解析（FMEA）等によるすべての重要な不具合（障害）の分析
- PL の見積りのためのデータ（定量化に関する文書）
- 完全なソフトウェアドキュメンテーション（本書 6.3 参照）
- アナログ及びデジタル回路に関する設計規則、プログラミングガイドラインなど、レイアウト設計及び実装に関して順守すべき品質保証規定
- 試験済みのコンポーネント、モジュールあるいは SRP/CS に対する試験証明書

文書は、完全な、内容的に矛盾のない、論理的に構成された、理解しやすく、検証可能なものでなければならない。各文書に関する詳細は、次の V&V アクティビティの説明に記載される。

7.1.5 分析

SRP/CS 及びその各側面に関する評価は、まず分析により行われる。ここでは、各書類を検査し、また必要に応じて、例えば回路シミュレータや、静的及び動的ソフトウェア解析、FMEA ツールなどの解析ツールを用いて、仕様書に定められた要求事項が達成されたかどうかを決定する。$MTTF_d$、DC、CCF の評価は、主に提出された資料をベースにした分析により行われる。

7.1.6 試験

分析による評価だけでは要求事項が満たされていることを十分に示すことができない場合には、試験を行う。試験は、体系的に計画され、かつ論理的な方法で実施されなければならない。一般的には、例えばプロトタイプ、機能モデル、もしくはソフトウェア・コードなどにより現実的に実行可能な開発段階で実施される。試験は、できるだけ指定された動作構成に近いかたちで行う必要がある。どのような環境条件の下で行うかは予め決定しておく。試験は手動式でも自動式でもかまわない。

試験による妥当性確認での測定の不確かさは､その適切性が説明できるものでなければならない。ISO 13849-2 には、順守すべき範囲が指示されている。

分析及び試験のアクティビティには、そのフェーズに関連するすべての書類のレビューも含まれる。試験により否定的な結果が得られた場合には、この結果を SRP/CS の開発で適切に処理するための手順及び方策をとる必要がある。

7.1.7 V&V アクティビティの文書

分析及び試験のアクティビティは、その結果（合格あるいは不合格）を含めてすべて文書化しなければならない。次節では、安全機能、SRP/CS 並びに PL、カテゴリ、$MTTF_d$、DC 及び CCF 等の各側面に関する妥当性確認のステップを説明する。

SRP/CS の仕様書に規定された要求事項がすべて満たされていない場合には､その時点で設計及び技術的実現の適切なフェーズに立ち戻る必要がある。そうでない場合には、V&V の最後のアクティビティとなる図 7.1 の 3 番目のひし形ブロック（ブロック 8）に進み、すべての安全機能が分析されたかどうかを評価する。肯定的な結果が得られれば､ISO 13849-1 による SRP/CS の評価は完了したことになる。そうでない場合には、未実施の安全機能の試験をさらに行う必要がある。

7.2 安全機能の妥当性確認

実装された安全機能が、仕様書で要求される特性及び性能基準と完全に一致していることを確認する安全機能の妥当性確認は、重要なステップである。安全機能が適切に実行に移されたかどうかを判断するに当たっては、次の質問事項を参考にするとよい。

- 安全機能は正確かつ完全に定義されているか？
- 適切な安全機能が実行に移されているか？
- 設計に対する安全機能の指定は適切か？
- 必要な運転モードはすべて考慮されているか？
- 機械の運転特性が考慮されているか（合理的に予見可能な誤使用を含む）？
- 緊急時における行動が考慮されているか？
- 安全関連の信号入力はすべて、適切に、論理的に正しく、安全指向の出力信号に処理されるか？
- 特定されたそれぞれの危険源及び危険状態に関するリスクアセスメントの結果が、安全機能の定義に取り込まれているか？

機能的要求事項が満たされたかどうかを確認するために、一般的には、次のような部分試験が実施される。

- 機能テスト（冗長システムの各チャンネルに対して実施）
- いわゆる拡張機能テストによる、通常とは異なる、予期しない、あるいは仕様書に記載されていない入力信号、操作手順、もしくはインプットにおける SRP/CS の挙動に関するテスト
- ブラックボックステスト
- 性能テスト（機能的側面）

本章で説明する V&V アクティビティでは、安全機能を実行する SRP/CS が焦点になる。しかしながら、完成品としての機械に関する安全機能の試験には、オーバーランや安全距離の測定など別の側面に関する一連の試験が含まれる。

7.3 SRP/CS の PL の妥当性確認

本節では、単独の SRP/CS の試験について説明する。1 つの安全機能に対し複数の SRP/CS を組合せた場合の試験手順は、7.5 で取り上げる。次の各項では、PL の算定に影響を及ぼす各側面の妥当性確認について述べる。これらの側面には、個々のコンポーネントの $MTTF_d$ 値、DC、CCF 及びカテゴリといった定量化できるものと、不具合（障害）発生条件による安全機能の挙動並びに安全関連ソフトウェア、系統的故障、環境条件による機能の挙動等の定性的なものが含まれる。この個々の側面の査定に続いて、PL の見積りの検証手順を説明する。

7.3.1　カテゴリの妥当性確認

カテゴリの妥当性確認の目的は、SRP/CS により技術的に実現されるカテゴリに関するすべての要求事項（本書 6.2 参照）を確認することである。このためには、特に次の文書が必要になる。

- SRP/CS の仕様書
- 設計説明書
- ブロックダイアグラム及び構造説明書
- 回路図
- 不具合（障害）リスト

要求事項が満たされたかどうかを確認するために、一般的に、次のような部分試験が実施される。

- 不具合（障害）時の SRP/CS の挙動に関するテスト、FMEA 試験又は障害注入を使用したテストを含む
- いわゆる拡張機能テストによる、入力信号の異常状態及び操作時の誤った手順／入力における SRP/CS の挙動に関するテスト

これらの部分試験は、次の分析により補足される。

- 構造／信号経路の分析
- 基本安全原則の順守に関する検査
- 十分吟味された安全原則の実行に関する検査（カテゴリ 1 以上）
- 十分吟味されたコンポーネントの使用に関する検査（カテゴリ 1 のみ）
- 不具合（障害）リストに追加される個々の不具合（除外）と許容される不具合（障害）の除外及びその十分な根拠付けに関する評価

本規格第 2 部の附属書（本書の付録 C も参照）は、この最後の 4 つの分析に関する詳細情報として利用できる。

7.3.2　$MTTF_d$ 値の妥当性確認

PL の決定に使用される $MTTF_d$ 値については、少なくとも、その尤もらしさを検証する必要がある。これには、一般的に、その値の出所に対し適切な情報源が示されているかどうかの評価も含まれる。主要なコンポーネントと、またそれ以外のコンポーネントからは無作為に抽出したものを対象として、その値の正統性を詳しくレビューする方法も推奨される。このためには、特に本書の 6.2.12 及び付録 D の記載される情報源が利用できる。

7.3.3 DC 値の妥当性確認

診断方策によりブロックに指定された診断範囲 DC は、検証可能な根拠付けがなされていなければならない。ここでも、値の出所に関する情報、つまり見積もられた値が信用するに足るものか、あるいは疑問の余地を残すものかどうかを審査するのが一般的である。$MTTF_d$ 値の場合と同様、無作為に抽出したもの、もしくは主要コンポーネントに関して、その根拠を確認することが効果的といえる。本書の付録 E に、CD 値の見積りに関する注意事項が記載される。

実現された設計に関しては、記載された診断方策が実行に移されたかどうかを審査する。このためには、開発段階で作成された文書で診断機能及び診断モジュールを特定し、その有効度を見積もることが一般的に必要である。さらに、不具合（障害）時の SRP/CS の挙動に関するテスト（FMEA 試験又は障害注入を使用したテスト）により、不具合（障害）が診断機能により適切に検出されることを示す必要がある。

7.3.4 CCF 対策の妥当性確認

共通原因故障 CCF（Common Cause Failure）に対して選択された方策の妥当性確認については、本書の付録 F に点数法による手法が記載されている。獲得された合計点数の他、採用された方策が該当文書に適切に記載されているかどうかも審査する。分析及び試験により、その方策が実際に実行に移されたことを示す必要がある。これに対する一般的な V&V アクティビティには、静的なハードウェア解析及び環境条件（境界条件）下での機能試験が含まれる。

7.3.5 系統的故障に対する方策の検証及び妥当性確認

系統的故障を回避する方策の検証として、本書 6.1.2 に記載される必要な設計方策が実行に移されたかどうかという観点から、開発文書の検査が要求される。一般的に、次の方法により立証することができる。

- 動力源ユニットに関する FMEA 試験又は障害注入を使用したテスト（例：電源、クロック信号、圧力）
- 環境影響に対する障害耐性試験又は仕様書に定められた環境条件下でのテスト
- プログラム実行監視の実装に関する分析
- データ通信システムに関して定性的に指定された特性の検査及び試験、もしくは認証されたコンポーネントが使用された場合には、その特定
- 基本安全原則及び十分吟味された安全原則の使用と、該当する場合は、多様性を採用したハードウェアなど別の方策を確認できる開発文書の検査

7.3.6　ソフトウェアの妥当性確認

ソフトウェアのレイアウト設計及びコーディングにおける検証については、本書 6.3 に詳しく説明される。

安全関連ソフトウェアの開発に関しては、下記の PL「e」での組み込み方法を例外として、簡易化された「V 字モデル」が使用される（図 6.11 参照）。この V 字モデルにおける最後の開発アクティビティが、ソフトウェアの妥当性確認である。機能の挙動に関する安全関連ソフトウェア仕様書の要求事項並びに性能基準（例えば時間関連の基準）が適切に実行に移されたかどうかが試験される。このフェーズでは、ソフトウェアの「内部動作」はもはや対象外であり、ハードウェアに統合された完成したソフトウェアのインプットの変化に応じてアウトプットされる「外部の」挙動が観察される。ここでは、ソフトウェアは「ブラックボックス」として考察される。これに対する妥当性確認が、いわゆるブラックボックステストと呼ばれるものである。

安全関連のアプリケーションソフトウェア（SRASW）については、「I/O テスト」により、安全関連の入力及び出力信号が適切に使用されるという確証を得る必要がある。PL「d」及び「e」に関しては、妥当性確認において、境界値分析をベースにした拡張テストケースを実行することも推奨される。この場合、予め分析により決定され、テストで実行される不具合（障害）ケースに対する反応も観察され、ソフトウェアによる不具合（障害）の検出及び抑制がテストされる。セーフティ・ファンクションブロックとしてすでに認証された、もしくは品質保証の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試験する必要はない。しかしながら、すでに妥当性が確認されていることを、証拠により証明しなければならない。ただし、複数のセーフティ・ファンクションブロックがプロジェクト専用に組み合わされた場合には、その結果生じる全体の安全機能について妥当性確認を行う必要が出てくる。

安全関連の組み込みソフトウェア（SRESW）による PL の達成については、ソフトウェアの実装に関し要求される設計的方策が本書 6.3 に従って正しく実行に移され、実現されたかどうかを審査する。また、PL「e」の SRP/CS に使用され、多様性をもたない 2 チャンネル用に開発された SRESW の特別なケースについては、IEC 61508-3 の 7［32］による SIL 3 の要求事項を完全に満たす必要がある。これには、そこで要求される V&V アクティビティも含まれる。

安全関連ソフトウェアを修正した場合には、適切な範囲で再度妥当性確認を行わなければならない。

7.3.7　PL の見積りの検証

各 SRP/CS に関する PL の見積りの適切性は、特に、採用した評価手法の正しい適用及び適切な算定の検証により確認される。例えば、本書の 6.2.11 及び付録 D に $MTTF_d$ を決定するための簡易的手法が説明されており、また平均診断範囲 DC_{avg} については付録 E の公式により検証することができる。

PL の見積りに簡易的手法が使用されている場合には、図 6.10 を使って、先に確認されたカテゴリあるいは $MTTF_d$ 及び DC_{avg} の値から、適切な PL が決定されたかどうかを確認することができる。

7.4 使用上の情報のレビュー

SRP/CS の安全な使用に関する重要な情報は、取扱説明書、取付／組立説明書及び銘板という形式で、使用者に提供される。総称して使用上の情報と呼ばれるこれらの文書については、規格の第 11 章に挙げられた内容がすべて含まれているかどうか、また、特に次の項目についてわかりやすく記載されているかどうか検査する必要がある。

- 意図する使用（使用及び適用範囲）
- パフォーマンスレベル及びカテゴリ情報並びに発行年が記載された規格
- 安全機能及び標準機能
- 運転モード
- 応答時間
- ミューティング（安全機能の一時的無効化）
- 運転に関する制限（周囲条件を含む）
- インターフェース
- 表示装置及び警報装置
- 安全な取付けと立ち上げ、該当する場合には安全なパラメータ化及びプログラミング
- 保全、適切なチェックリストを含む
- 保守間隔及び交換間隔
- 接近性と内部部品の交換
- 安全かつ容易な不具合（障害）発見の手段及び手順

7.5 SRP/CS の組合せと統合の妥当性確認

個々の SRP/CS は、組み合わせる前に別個に試験する必要がある。SRP/CS の組合せ及び統合における系統的故障を回避するために、次の V&V アクティビティが実施される。

- 安全機能の記載を含む設計文書の検査
- SRP/CS 間のインターフェースの特性値（例：電圧、電流、圧力、情報データ、信号レベル変換）の比較
- 組合せ及び統合に関する FMEA
- 機能テスト／ブラックボックステスト
- 拡張機能テスト

- 本書 6.4 に記載される簡易的手法により個々の SRP/CS の PL から決定された全体の PL に関する確認

7.6 検証及び妥当性確認の実施例
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」）

安全機能に関する検証及び妥当性確認の一般的説明の補足として、本節では、本書 5.7 及び 6.5 ですでに取り上げた断裁機を例に、実際の V&V アクティビティについて解説する。

7.6.1 達成される PL の検証（図 7.1 のブロック 6 参照）

リスク分析により、実行される安全機能 SF2 について要求パフォーマンスレベル PL_r「e」が決定された。定量化できる側面をすべて考慮して算定された故障確率において、この PL は達成されている。また、不具合（障害）発生条件下の安全機能の挙動、安全関連ソフトウェア、系統的故障及び環境条件下での挙動など PL「e」に対する定性的側面に関する要求事項もすべて十分に満たされている。

7.6.2 安全関連要求事項の妥当性確認（図 7.1 のブロック 7 参照）

不具合（障害）リスト

PL の決定では、ISO 13849-2［7］による不具合（障害）リストを基礎とする。

文書

すでに述べたように、回路図、部品リスト、仕様書及び機能説明書を、分析及び試験の基礎とする。

文書化

分析及び試験の結果はすべて記述し、文書化する必要がある。

安全機能の妥当性確認

安全機能に関する機能要求事項を検証するため、機能テストを実施する。さらに、入力がまれな、あるいは規定されていないケースにおける安全機能の挙動を確認するために、拡張機能テストが追加される。こうしたテストの一例として、オペレータが両手操作制御装置を操作しているときに、第三者が、そこに設置された電気的検知保護装置（ライトグリッド）を突き抜けて危険区域に介入した場合の SRP/CS の反応を確認するテストが挙げられる。機能的側面に対しては性能テストが実施される。これには、EN 574［37］による同期操作に関して順守すべき時間のテストも含まれる。2 つの手動制御器 S1 と S2 が 0.5 秒未満の時間差で操作される場合にのみ、プレスクランプ及びカッターを作動させる出力信号が発生する。前述の、仕様書に定められた安全技術特性の試験及び分析については、良好な結果が得られた。

SRP/CS の PL の妥当性確認

- カテゴリの妥当性確認

開発資料に基づき、不具合（障害）時の挙動に関するテストがプロトタイプを使って実施される。注入された障害に対する SRP/CS の反応は、仕様書に定められた反応に該当するものであることが求められる。まず分析により、そして次に試験により、例えば個々の電磁リレーが切替命令を実行できなくなった場合には何が起こるか、あるいは 2 つの手動制御器 S1 と S2 の 1 つが時間遅れで操作される、あるいはまったく操作されない場合には SRP/CS はどのように反応するかをテストする。単一の不具合（障害）が SRP/CS に注入されたときには、安全機能は常に確保されなければならない。単一の不具合（障害）は、安全機能が次に作動する時、あるいはそれ以前に検出される必要がある。不具合（障害）を検出することができない場合には、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。

基本安全原則の一例であるノーマルクローズ原理の順守は、中断事象を注入し、これに対する反応を確認することにより証明できる。例えば、供給電圧を落とした場合には、プレスクランプ及びカッターはばね力により始動位置に戻される。

尤らしさのテストは、ここでは、十分吟味された安全原則の実行に関する例として、電磁リレーについて実施される。電磁リレーK3 から K6 の強制ガイド式接点は、2 つのチャンネルによりバックチェックが行われる。バックチェックが適切に機能することをテストにより確認する。

- $MTTF_d$ 値の妥当性確認

$MTTF_d$ 値の妥当性確認の例として、ここでは、バルブ 1V3、1V4、2V2 及び 2V1 に関し、ISO 13849-1 の表 C.1［6］に従って見積もられた 150 年という値について検査する（本書の表 D.2 も参照）。適切な値が選択されており、かつ、これは信頼できる情報源によるものである。$MTTF_d$ を 150 年と仮定した場合に適用される安全原則（例えばオイル交換）が順守され、使用者には取扱説明書により情報が提供される。

設計特性

- カテゴリ B の要求事項、基本安全原則及び十分吟味された安全原則が順守される。多様冗長構造の処理チャンネル（マイクロコントローラと ASIC）により、単一の不具合（障害）により安全機能が喪失することはなく、系統的不具合（障害）は十分に回避される。
- 制御信号が除去されるたびに、安全指向の切替え位置が達成される。
- すべての電気信号は、圧力センサの信号も含め、複数チャンネルの制御システムで処理される。
- 両手操作制御装置の手動制御器 S1 と S2 は、IEC 60947-5-1 に適合する。
- K3 から K6 は IEC 60947-5-1、附属書 L［38］に適合する強制ガイド式接点要素を有する。ノーマリオープン（a 接点）を監視するためのノーマリクローズ（b 接点）はそれぞれ隣接するチャンネルで監視される。
- 信号を伝送する導線はすべて分離するか、もしくは機械的損傷に対する保護を施して敷設される。
- ソフトウェア（SRESW）のプログラミングは PL「d」（多様性の採用により 1 ランク引き下げられる）に関する要求事項及び本書 6.3 の注意事項に従って行われる。
- ASIC 開発時の不具合（障害）を回避する方策は、IEC 61508-2:2006 原案［39］の ASIC 開発ライフサイクル（V 字モデル）に準拠して実施されている。

- DC 値の妥当性確認

K1 及び K2 については、自己診断に基づき、DC = 90%であることが確認される。これには、入力信号及び中間結果（マイクロコントローラと ASIC による）の相互監視、タイミング及び論理的なプログラムシーケンスの監視と、静的な故障及び短絡の検出が含まれる。さらに、マイクロコントローラを伴うチャンネルでは CPU テストが行われる。CPU テストでは、使用されるコマンドがすべてテストされ、またランダム・アクセス・メモリ（RAM）及び読み取り専用メモリ（ROM）のテストも実施される。2 つめのチャンネル（ASIC）では、並列チャンネルの場合と定性的に比較可能なテストが行われる。試験により、記載された方策が適切なレベルで実行に移されたことを示さなければならない。

K3、K4、K5 及び K6 には、DC = 99% が指定される。これは、バックチェック機能がある電磁リレーの強制ガイド式接点に関する尤もらしさの試験に基づき、適切であると評価される。カテゴリの妥当性確認においてすでに実施された尤もらしさのテストは、ここでも、適切な機能の証明として利用できる。

- CCF に対する方策の妥当性確認

共通原因故障に対する方策に関しては、点数法において 65 点を獲得することで、最低限の要求事項は達成されたことになる。さらに、制御システムの構成部で別の方策をとることが効果的である。「信号経路の物理的分離」という方策を実行することで、15 点が考慮される。この方策の適切な実行に関しては、例えば回路図などの開発資料の分析及びハードウェアに関する試験により証明される。

- 系統的故障に対する方策の検証及び妥当性確認

基本安全原則及び十分吟味された安全原則を順守することは、系統的故障に対し非常に効果的である。カテゴリの妥当性確認のためのアクティビティにも、両安全原則の順守に関する審査が含まれる。そこで実施された分析及び試験の結果は、本項の妥当性確認に関しても用いることができる。

この試験以外に、開発と並行して、使用される基本安全原則及び十分吟味された安全原則と、本書の 6.1.2 及び規格の附属書 G による系統的故障を抑制及び回避する方策が記載された文書の検査が行われる。これは、基本原則及び方策が開発プロセスで適切に考慮されているかどうかを判断するためのものである。

系統的故障の抑制策の例として、プログラムの誤実行を検出するための、安全関連ソフトウェアのプログラムシーケンスの監視が挙げられる。プロセス監視の有効性は、障害注入によってテストされる。

仕様書に定められた環境条件に対する SRP/CS の耐性を示すために、特に温度、湿度及び電磁障害等に関して、予測及び予見可能なあらゆる不利な条件の下で試験を行う。これは、系統的故障を回避する方策に関する一例である。

- ソフトウェアの妥当性確認

ソフトウェアの検証は、本書 6.3 に詳しく説明される。ここでは、さらにソフトウェアの妥当性確認、つまり、ハードウェアに統合されたソフトウェアの機能及び応答時間に関する試験が実施される。機能テスト及び拡張機能テストを行い、安全関連の入力信号が安全関連の出力信号に適切に処理されること、そして、障害注入によるテストケースでの、マイクロコントローラ K1 のファームウェア仕様書に定められた不具合（障害）反応の妥当性を確認する。

- PL の見積りの検証

PL の見積りには、ISO 13849-1 による簡易的手法が使用された。この適用の適切性を検証する。図 6.10 の柱状グラフにより先に確認されたカテゴリ、$MTTF_d$ 及び DC_{avg} 値による PL の見積りの適切性と、また本書 6.2.11 及び付録 D による $MTTF_d$ 並びに付録 E による平均診断範囲 DC_{avg} の算定についても確認される。

- *使用上の情報のレビュー*

使用上の情報のレビューを行い、SRP/CS に関して次の内容が適切に記載されているかどうかを確認する。
意図する使用の記載・PL 及びカテゴリに関する情報（発行年が記載された規格を含む）・すべての運転モードの説明・安全防護物及び安全機能の説明、応答時間、運転に関する環境条件、外部インターフェース含む・運搬、安全な取り付け、立ち上げ、保全に関する情報及び技術データ

- *SRP/CS の組合せと統合の妥当性確認*

記載された安全機能は、1 つの SRP/CS により技術的に実現される。しかし、この SRP/CS には電子技術と油圧技術という異なる技術方式が組み合わされているため、SRP/CS を組み合わせた場合に必要となるいくつかの試験を、これらがカテゴリの妥当性確認ですでに行われたものでない限りは、実施する必要がある。この試験には、使用される技術方式間のインターフェースデータの比較、並びに機能テスト及び拡張機能テストが含まれる。

7.6.3 すべての安全機能が分析されたか、審査せよ （図 7.1 のブロック 8 参照）

本節で取り上げた SF2 に関する V&V アクティビティは、SRP/CS により実行されるすべての安全機能（SF1 から SF7）について実施される。しかしながら、これらの安全機能の多くに同一のハードウェアが起用されているため、さほど労力のかかる作業にはならない。分析及び試験により、安全機能が技術的に適切に実現されたことを示す必要がある。すべての安全機能が十分に考察されていれば、ISO 13849 の第 1 部及び第 2 部による評価は完了する。