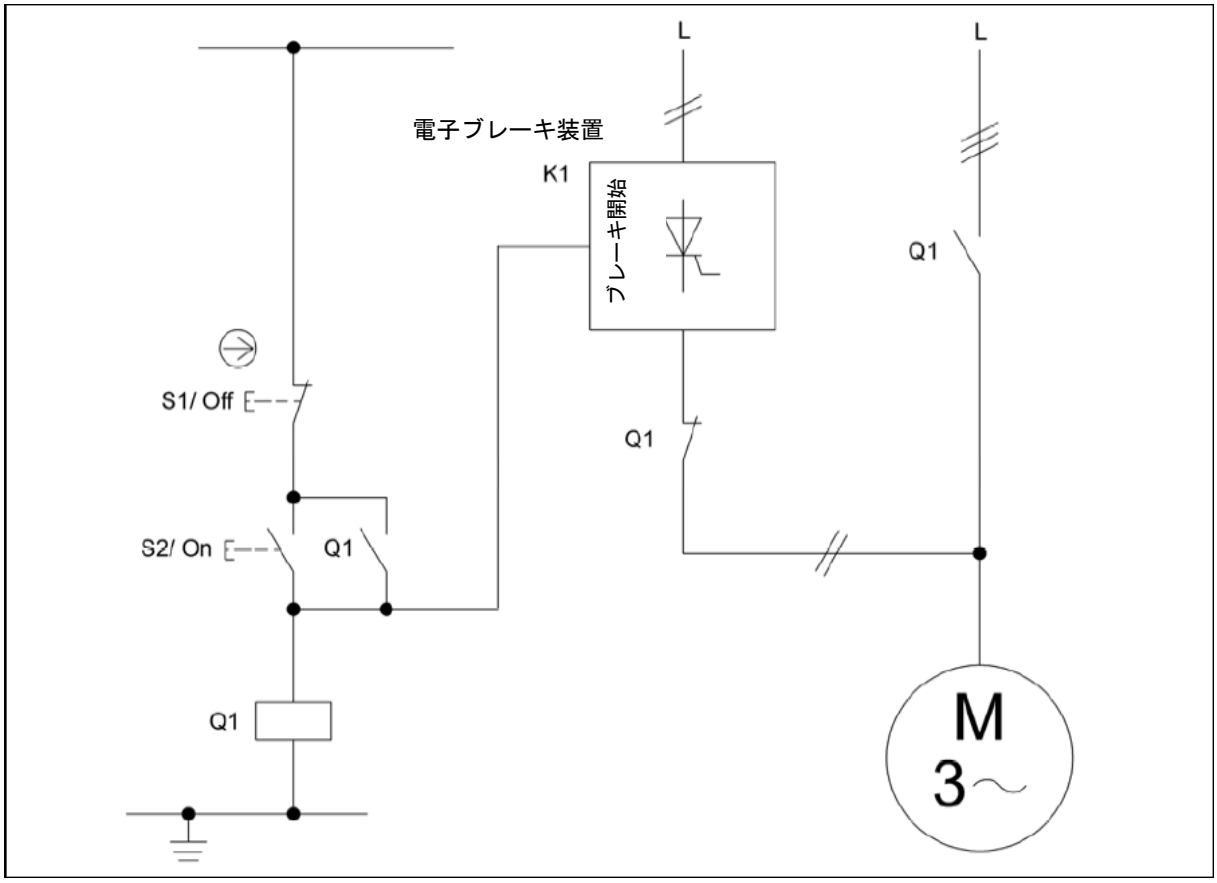
### 8.2.4　木工機械の停止　－　カテゴリー1　－　PL c（例 4）

図 8.9：木工機械停止用の電気機械制御機器と単純電子ブレーキ装置の組み合わせ

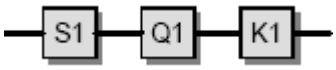



**安全機能**

- Off ボタンの作動は、SS1（安全停止 1）、最大許容時間内でのモータの制御停止、につながる。

**機能の説明**

- モータの停止はOffボタンS1の作動によって始まる。モータ接触器Q1はドロップアウトし、ブレーキ機能が開始する。位相角制御を用いたサイリスタによってブレーキユニット K1 内に発生され、モータ巻線にブレーキトルクを生じさせる直流により、モータにブレーキがかかる。
- 遅動時間は最大値（例えば 10 秒）を超えてはならない。
  このために必要なブレーキ電流のレベルは、ブレーキユニットのポテンショメータで設定できる。




- 最大ブレーキ時間の終了と同時に、サイリスタへの制御信号は停止し、ブレーキ電流用の電路は遮断される。停止プロセスは、EN 60204-1 によるカテゴリー1 停止に相当する。
- 安全機能は全ての構成部品の故障に対して維持できるわけではなく、構成部品の信頼性に依存する。
- フォールト（故障）検出方策は実施されない。

**設計特性**

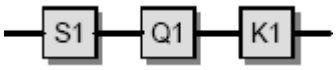
- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。基本安全原則として遮断原則（閉回路電流）を採用する。電源復旧時の予期しない起動に対する保護として、制御システムに Q1 でのラッチインを備える。
- S1 は、IEC 60947-5-1　付属書 K（直接開動作）の正作動モード付き押しボタンである。そのため、S1 は十分に実証済みの構成部品と見なされる。
- EN ISO 13849-2 の表 D.4 に従った追加条件が守られていれば、接触器 Q1 は十分に実証済みの構成部品である。
- ブレーキユニット K1 は、十分に実証済みの構成部品と見なされるトランジスタ、コンデンサ、ダイオード、レジスタおよびサイリスタなどの単純電子構成部品のみで設計されている。安全関連ブレーキ機能の無故障性能は、構成部品の選択によって特徴づけられる。故障検出に対する内部対策は実施されない。EN ISO 13849-1 の 6.2.4 項によって十分に実証済みの構成部品と同等であるとは考えられていない複雑な電子構成部品（例えばマイクロプロセッサ）は採用しない。

**適用**

- 木工機械や同様の機械で、ブレーキをかけない停止では危険な工具動作の許容できないほど長い遅動が起きる可能性があるもの。制御システムは、少なくとも PL b に達するように設計しなければならない。（木工機械用試験原則　GS-HO-01）

**故障確率計算**

- S1 は、IEC 60947-5-1　付属書 K（直接開動作）の正作動モード付き押しボタンである。この種の押しボタンが制御装置として採用されていれば、押しボタン内の機械的構成部品を含む電気接点が開かない故障によるフォールト（故障）を排除することが可能である。
- $MTTF_d$ : 2,000,000 回の開閉操作の $B_{10d}$ 値[S]を接触器 Q1 の定格負荷で想定する。稼働日 300 日、稼働時間 8 時間、サイクル時間が 2 分の場合、$n_{op}$ は 1 年に 72,000 サイクルで、$MTTF_d$ は 277 年となる。



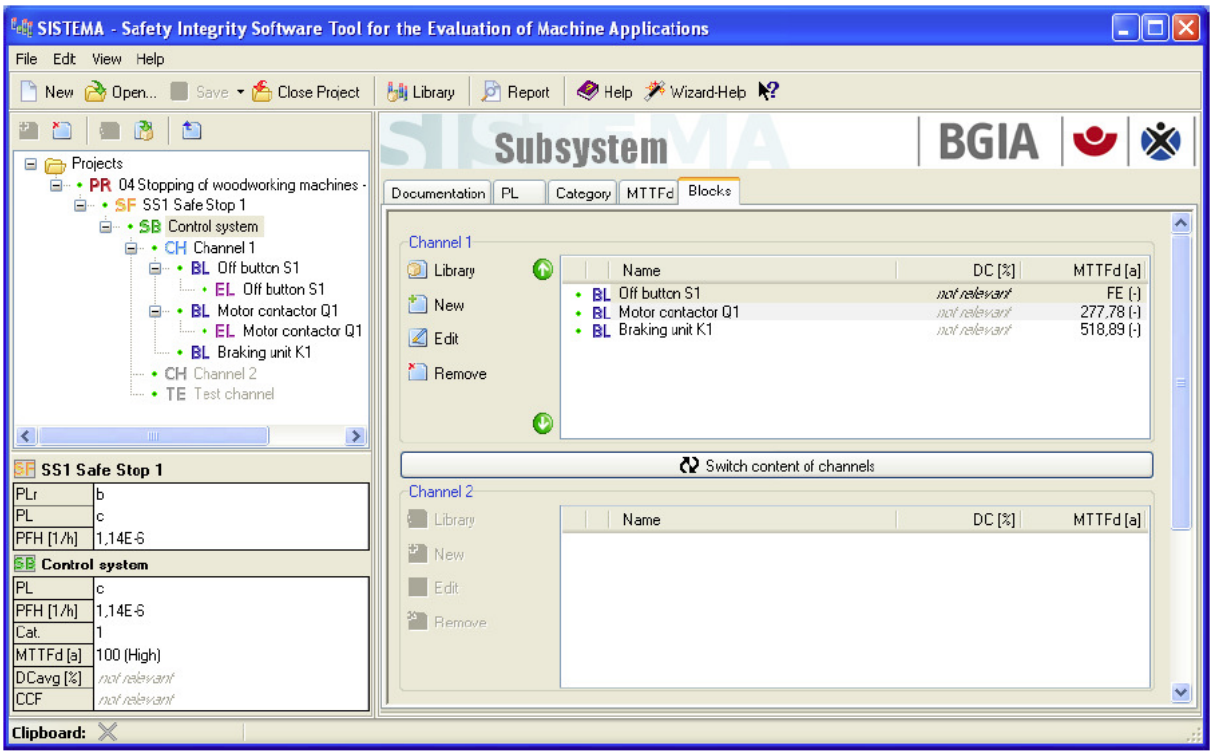

ブレーキユニット K1 の $MTTF_d$ は部品カウント法により決定される。パーツリストからのパーツ情報と SN 29500 データベース[36]からの値で、$MTTF_d$ は 518 年[D]となる。Q1 と K1 の組み合わせで、そのチャンネルの $MTTF_d$ は 180 年となり、上限の 100 年（「高」）に達する。

- カテゴリー1 では、$DC_{avg}$ と共通原因故障に対する対策は関係しない。
- 電気機械制御システムは、高い $MTTF_d$（100 年）のカテゴリー1 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.14 \times 10^{-6}$ となる。これは PL c に相当し、そのため、b の $PL_r$ を超える。

**より詳細な参考文献**

- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01 (12/2007).
  www.dguv.de, Webcode d14898

図 8.10：SISTEMA による PL の決定



### 8.2.5　可動式ガードの位置監視　－　カテゴリー1　－　PL c（例 5）

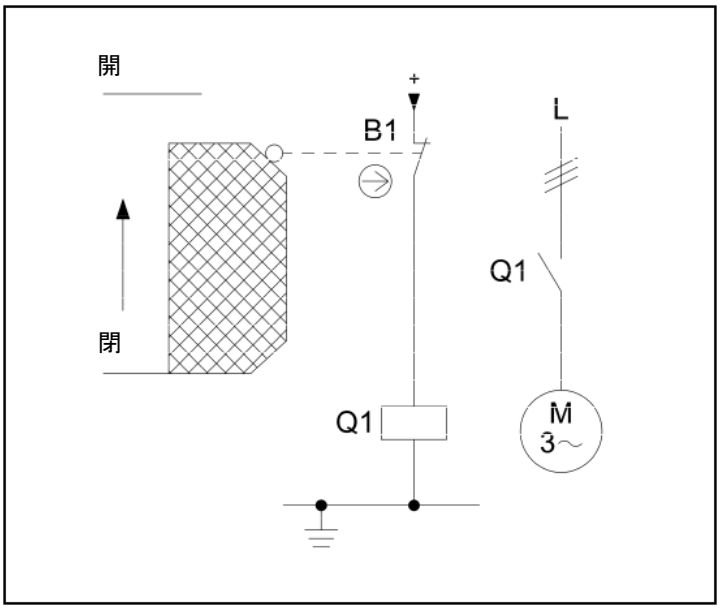



図 8.11：
危険動作防止のための可動式ガードの位置監視
（STO－安全トルクオフ）

**安全機能**

- 保護装置によって起動する安全関連停止機能：可動式ガードが開くことで安全機能 STO－安全トルクオフが起動する。

**機能の説明**

- 可動式ガード（例えば安全ガード）の開動作は、接触器 Q1 を作動させる直接開動作付き位置スイッチ B1 が検知する。Q1 のドロップアウトにより、危険な動作や状態が遮断または防止される。
- 安全機能は全ての構成部品の故障に対して維持できるわけではなく、構成部品の信頼性に依存する。
- フォールト（故障）検出方策は実施されない。
- 保護装置の取り外しは検知されない。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。基本安全原則として閉回路電流原則を採用する。制御回路の接地は十分に実証済みの安全原則と見なされる。

- スイッチ B1 は、IEC 60947-5-1　付属書 K による直接開動作付き位置スイッチであり、そのため、十分に実証済みの構成部品と見なされる。保護装置が安全な位置から外れると、常時閉接点が直接、機械的に回路を遮断する。
- EN ISO 13849-2 の表 D.4 に従った追加条件が守られていれば、接触器 Q1 は十分に実証済みの構成部品である。
- 位置監視用に位置スイッチを採用する。位置スイッチの作動のために保護装置の安定した配置を確保する。位置スイッチの作動要素は移動できないように保護される。剛性の機械的部品のみ（アクチュエータと接点の間にはバネ要素なし）を採用する。
- 位置スイッチの作動ストロークは、メーカの仕様に従う。

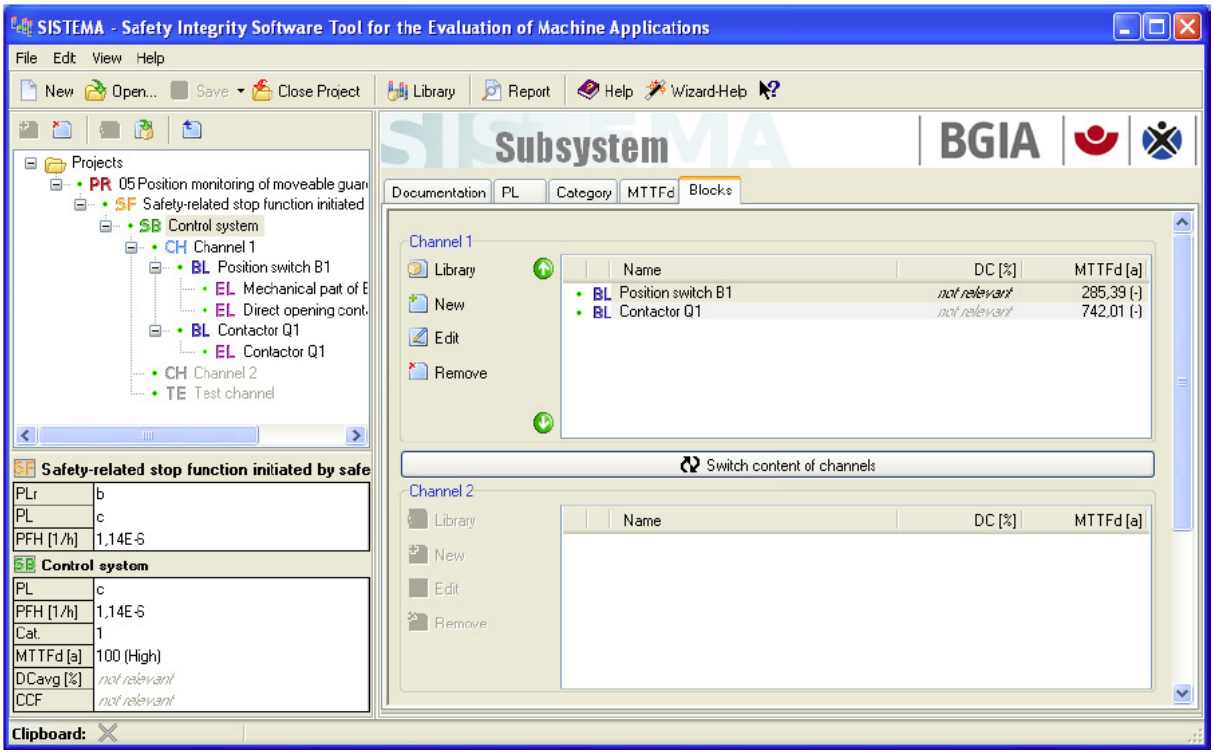
**故障確率計算**

- $MTTF_d$：B1 に対し直接開電気接点のフォールト（故障）を排除することが可能である。1,000,000 サイクルの $B_{10d}$ 値[M]が、B1 の機械的部品について提示されている。稼働日 365 日、稼働時間 16 時間/日、サイクル時間が 10 分の場合、$n_{op}$ は 1 年に 35,045 サイクルで、これらの構成部品の $MTTF_d$ は 285 年となる。接触器 Q1 では、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,300,000 回の開閉サイクル[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。上記 $n_{op}$ の想定値から、Q1 の $MTTF_d$ は 742 年となる。B1 と Q1 の組み合わせで、そのチャンネルの $MTTF_d$ は 206 年となり、上限の 100 年（「高」）に達する。
- カテゴリー1 では、$DC_{avg}$ と共通原因故障に対する対策は関係しない。
- 電気機械制御システムは、高い $MTTF_d$（100 年）のカテゴリー1 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.14 \times 10^{-6}$ となる。これは PL c に相当し、そのため、b の $PL_r$ を超える。

**より詳細な参考文献**

- IEC 60947-5-1: Low-voltage switchgear and controlgear – Part 5-1: Control circuit devices and switching elements – Electromechanical control circuit devices (11.03)

図 8.12： SISTEMA による PL の決定



### 8.2.6　非常停止装置付き起動/停止設備　－　カテゴリー1　－　PL c（例 6）

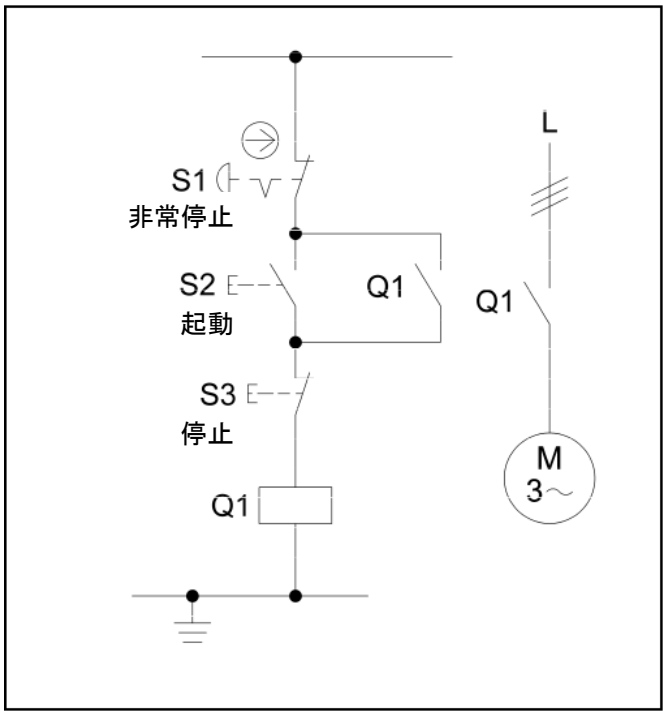



図 8.13：
非常停止装置付き起動/停止複合設備

**安全機能**

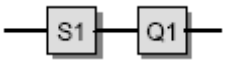
・　非常停止機能、非常停止装置の作動による STO－安全トルクオフ

**機能の説明**

・　非常停止装置 S1 が作動すると、接触器 Q1 の制御電圧の遮断により危険な動作や状態が遮断される。
・　安全機能は全ての構成部品の故障に対して維持できるわけではなく、構成部品の信頼性に依存する。
・　フォールト（故障）検出方策は実施されない。

**設計特性**

・　基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。基本安全原則として閉回路電流原則を採用する。制御回路もまた、十分に実証済みの安全原則として接地する。




- 非常停止装置 S1 は、IEC 60947-5-1　付属書 K による直接作動モード付きスイッチであり、そのため、EN ISO 13849-2 の表 D.4 に従った十分に実証済みの構成部品である。
- 信号は接触器によって処理される。（EN 60204-1 の停止カテゴリー0）
- EN ISO 13849-2 の表 D.4 に従った追加条件が守られていれば、接触器 Q1 は十分に実証済みの構成部品である。

**備考**

- 非常停止機能は、危険区域の安全防護対策のために安全機能を補完する保護対策である。

**故障確率計算**

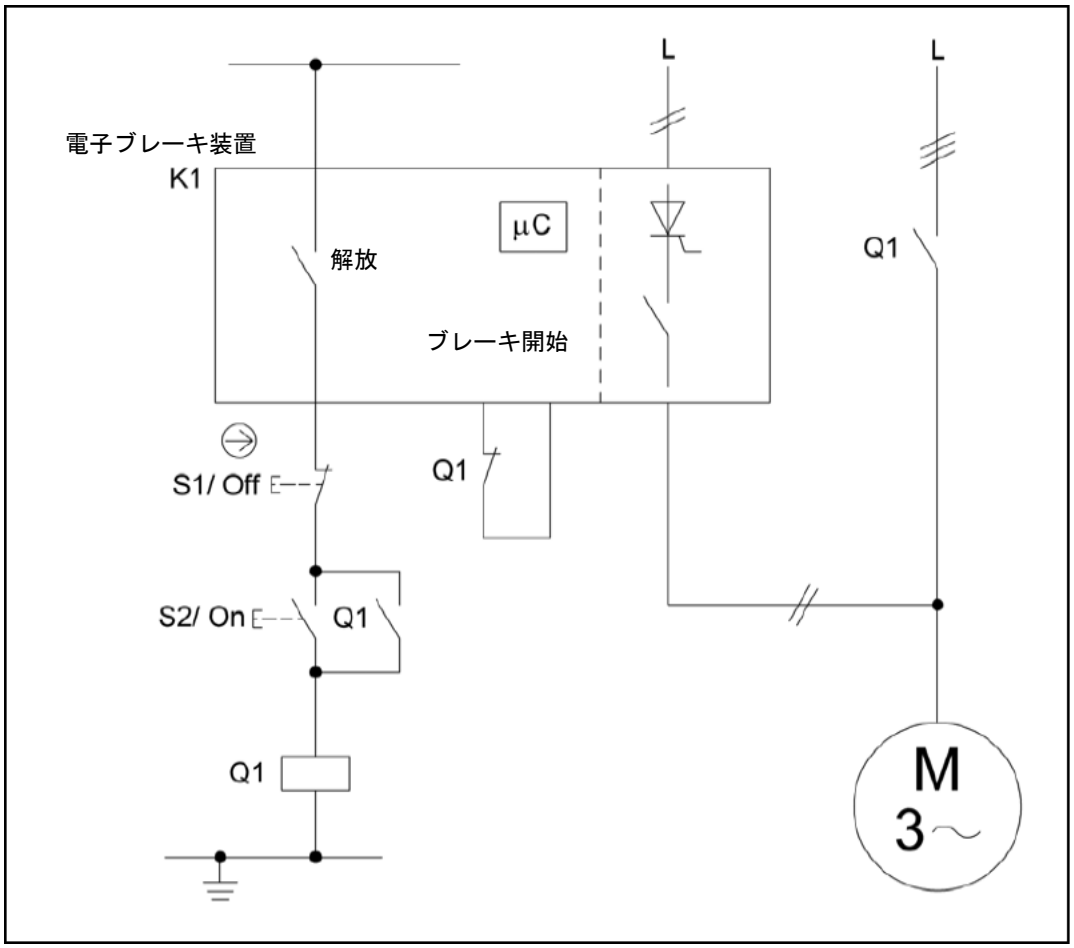
- $MTTF_d$：S1 は EN ISO13850 の標準非常停止装置である。本レポートの表 D.2 に記載の操作回数を超えなければ、フォールト（故障）の排除が直接開接点および機械的要素に適用される。接触器 Q1 では、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,300,000 回の開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。起動/停止設備が稼働日 365 日で 1 日に 2 回作動し、非常停止装置が 1 年に 3 回作動すると仮定すると、1 年あたり 733 サイクルの $n_{op}$ で、Q1 の $MTTF_d$ は 35,470 年となる。これはまたチャンネルの $MTTF_d$ であり、上限の 100 年（「高」）に達する。
- カテゴリー1 では、$DC_{avg}$ と共通原因故障に対する対策は関係しない。
- 電気機械制御システムは、高い $MTTF_d$（100 年）のカテゴリー1 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.14 \times 10^{-6}$ となる。これは PL c に相当する。

**より詳細な参考文献**

- EN ISO 13850: Safety of machinery – Emergency stop – Principles for design (11.06)
- EN 60204-1: Safety of machinery – Electrical equipment of machines. Part 1: General requirements (06.06)

### 8.2.8　木工機械の停止　－　カテゴリー1　－　PL c（例 8）

図 8.15：木工機械停止用の電気機械制御機器とプログラマブル電子ブレーキ装置の組み合わせ




**安全機能**

- Off ボタンの作動は、SS1（安全停止 1）、最大許容時間内でのモータの制御停止、につながる。

**機能の説明**

- モータの停止はOffボタンS1の作動によって始まる。モータ接触器Q1はドロップアウトし、ブレーキ機能が開始する。位相角制御を用いたサイリスタによってブレーキユニット K1 内に発生され、内部リレーによってモータ巻線に接続された直流により、モータにブレーキがかかる。
- 遅動時間は最大値（例えば 10 秒）を超えてはならない。
  所望の遅動時間およびその他の必要なパラメータ（例えばブレーキ電流、ゼロ速度検知用閾値）は、ブレーキ装置で設定できる。

- モータの静止または最大ブレーキ時間の終了と同時に、ブレーキ装置はブレーキ電流を切り、モータを電源から再度遮断する。停止プロセスは、EN 60204-1 によるカテゴリー1 停止に相当する。
- 安全機能は全ての構成部品の故障に対して維持できるわけではなく、構成部品の信頼性に依存する。
- ブレーキ機能がフォールト（故障）していない状態は、ブレーキ装置 K1 によって定期的に監視される。最大許容ブレーキ時間を超えるなどのフォールト（故障）が検出されると、装置の解放接点がモータの再起動を防止する。S1 や Q1 にはフォールト（故障）検出に対する対策は実施されない。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。基本安全原則として遮断原則（閉回路電流）を採用する。電源復旧時の予期しない起動に対する保護として、制御システムに Q1 でのラッチインを備える。
- S1 は、IEC 60947-5-1　付属書 K（直接開動作）の直接作動モード付き押しボタンである。そのため、S1 は十分に実証済みの構成部品と見なされる。
- EN ISO 13849-2 の表 D.4 に従った追加条件が守られていれば、接触器 Q1 は十分に実証済みの構成部品である。
- ブレーキ装置 K1 はマイクロコントローラで制御され、カテゴリー2 および PL c の全ての要求事項を満たす。安全関連機能は定期的に試験される。マイクロコントローラのプログラムシーケンスタイミングは、別のウオッチドッグによって監視される。

**適用**

- 木工機械や同様の機械で、ブレーキをかけない停止では危険な工具動作の許容できないほど長い遅動が起きる可能性があるもの。制御システムは、少なくとも性能レベル b に達するように設計しなければならない。（木工機械用試験原則　GS-HO-01）

**故障確率計算**

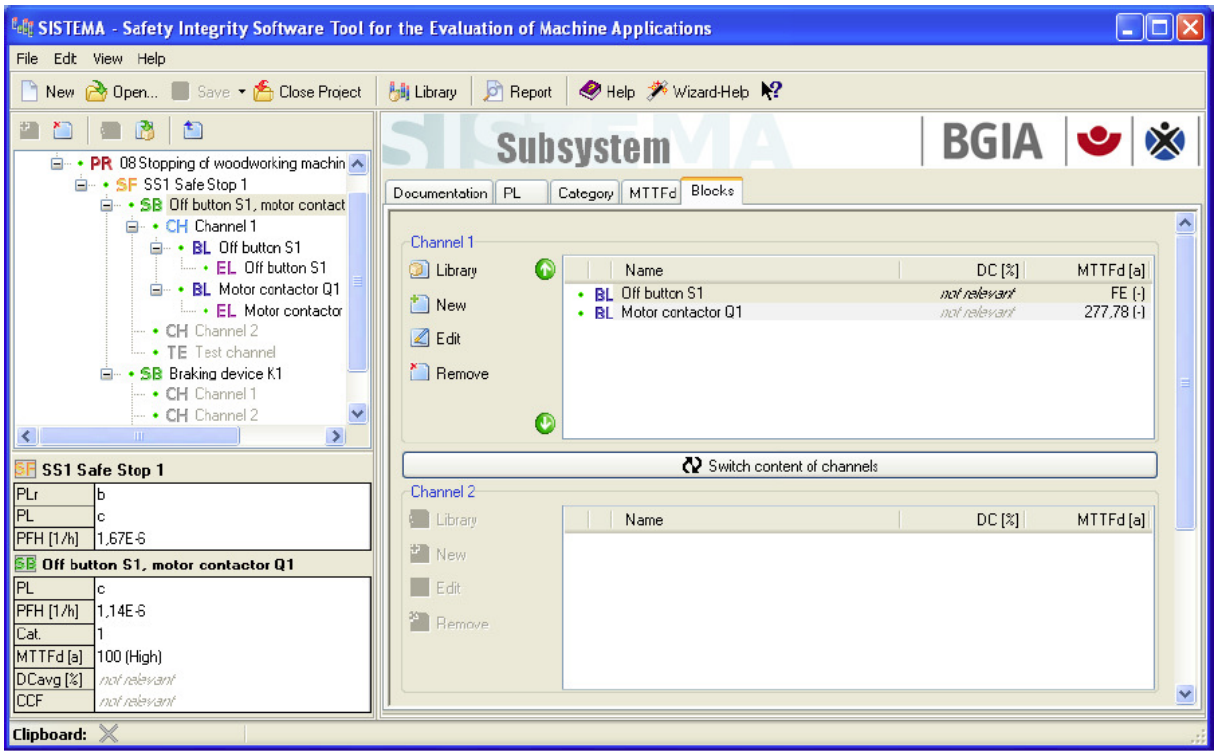
- 電子ブレーキ装置 K1 には標準モジュールが採用されているため、故障の確率（$5.28 \times 10^{-7}$/hr [M]）が SISTEMA による下記の計算に追加される。制御システムの残りの部分については、故障確率を下記の通り計算する。
- S1 は、IEC 60947-5-1　付属書 K（直接開動作）の直接作動モード付き押しボタンである。この種の押しボタンが制御装置として採用されていれば、押しボタン内の機械的構成部品を含む電気接点が開かない故障によるフォールト（故障）を排除することが可能である。

- $MTTF_d$：定格負荷での 2,000,000 回の開閉操作の $B_{10d}$ 値[S]を接触器 Q1 に対して想定する。稼働日 300 日、稼働時間 8 時間、サイクル時間が 2 分の場合、$n_{op}$ は 1 年に 72,000 サイクルで、$MTTF_d$ は 277 年となる。これはまたチャンネルの $MTTF_d$ であり、上限の 100 年（「高」）に達する。
- カテゴリー1 では、$DC_{avg}$ と共通原因故障に対する対策は関係しない。
- S1 および Q1 からなる電気機械制御システムは、高い $MTTF_d$（100 年）のカテゴリー1 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.14 \times 10^{-6}$ となる。サブシステム K1 の追加により、危険側故障の平均確率は 1 時間あたり $1.67 \times 10^{-6}$ となる。これは PL c に相当し、そのため、b の $PL_r$ を超える。

**より詳細な参考文献**

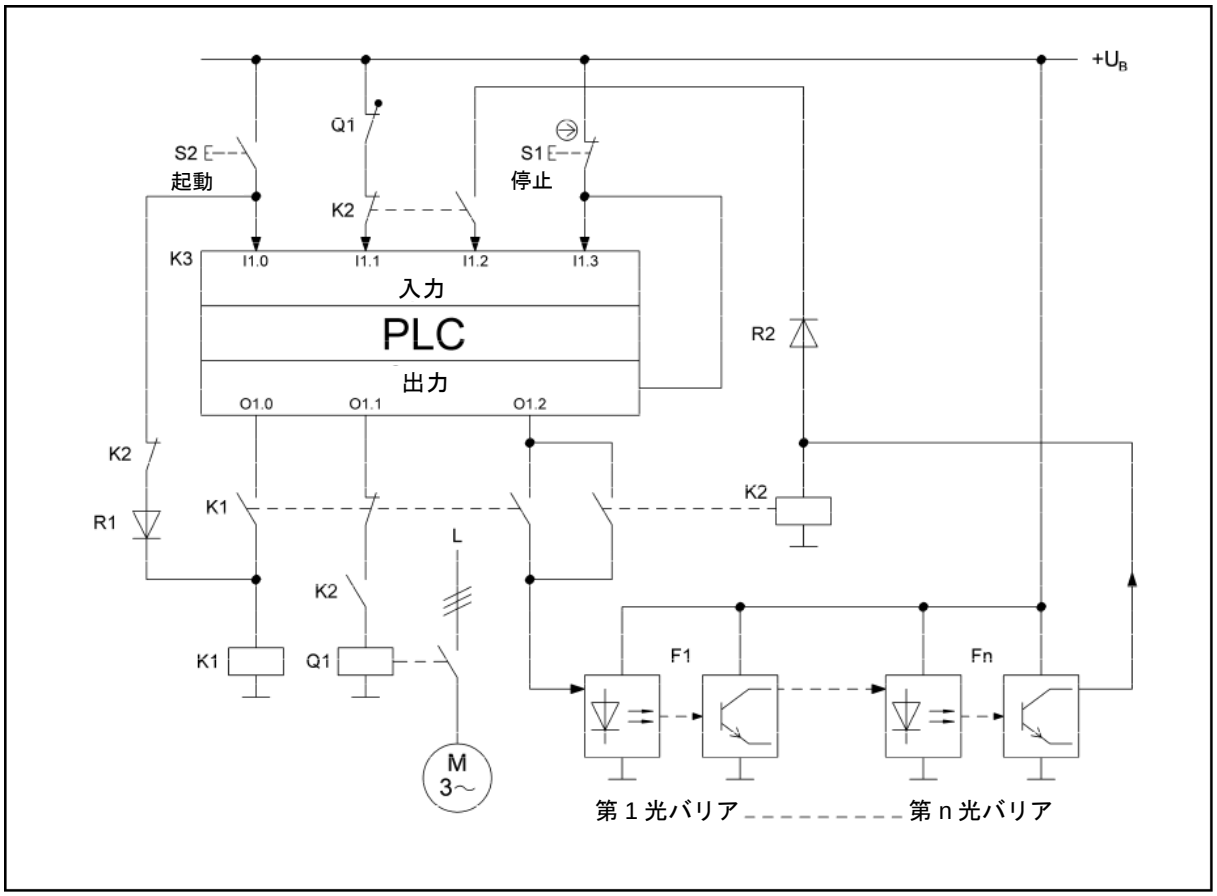
- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01 (12/2007). www.dguv.de, Webcode d14898

図 8.16：SISTEMA による PL の決定



### 8.2.9　試験済み光バリア　－　カテゴリー2　－　下流カテゴリー1 出力信号開閉装置付き PL c（例 9）

図 8.17：標準 PLC 付き光バリアの試験

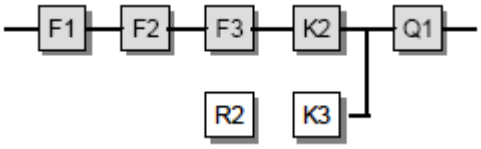



**安全機能**

- 保護装置によって起動する安全関連停止機能：光ビームが遮断されると、危険動作が停止する。（STO－安全トルクオフ）

**機能の説明**

- F1 から Fn の、カスケード接続された n 個の光バリアの光ビームが遮断されると、リレー、および接触器リレーK2 の遮断により、試験チャンネルの PLC 出力（O1.1）を通して遮断指令が始動する。その後、接触器 Q1 によって危険動作が停止する。
- 起動ボタン S2 を押して各危険動作を開始する前に光バリアを試験する。このために、PLC 出力 O1.2 はソフトウェア指令に応答して光バリアトランスミッタを遮断する。受光器の反応（K2 は再びドロップアウトする）は、PLC 入力 I1.1 および I1.2 で監視される。その動作にフォールト（故障）がなければ、K2 は O1.2 により閉じ、S2 の解放により危険動作が開始できる。

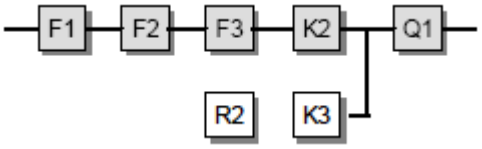



K1 は O1.0 により遮断され、主接触器 Q1 は O1.1 によって作動する。

- 試験により光バリアまたは K2 でフォールト（故障）が検出されると、出力 O1.1 および O1.2 は出力せず、作動信号はそれ以上主接触器 Q1 に送られない。
- PLC の全故障（出力 O1.0 低電圧、出力 O1.1 および O1.2 高電圧）の場合は、光ビームの遮断によって PLC とは無関係に K2 が遮断する。この独立性を確保するために、分離用ダイオード R2 によって光バリア出力を PLC から切り離す。好ましくない状況においては、起動ボタンを作動させ、K2 によって光バリアを再稼働させることが可能で、それにより主接触器 Q1 が作動する。この場合、試験機器（のみ）が故障しているのかもしれない。このような状況下で、試験機器の故障は機能的な異常処理の確率により検出される。
- 試験中、K1 および O1.1 による Q1 の作動は阻止される。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- IEC 61496-2 の適正な光学特性（開口角、外光不感性など）を持った特殊光バリアを採用する。
- いくつかの光バリアをカスケード接続し、2 つの PLC 入力および 1 個のリレーまたは接触器リレーのみで監視できる。
- 接触器リレーK1 および K2 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。接触器 Q1 は、IEC60947-4-1　付属書 F によるミラー接点を有する。
- 6.3.10 項の指示により、標準構成部品 F1 から Fn および K3 を採用する。
- PL b の要求事項（多様性により低下させた）および 6.3 項の指示により、ソフトウェア（SRASW）をプログラミングする。
- 起動ボタン S2 は、危険領域外で、かつ危険領域/危険個所が見える場所に配置しなければならない。
- 光ビームの数、配置および高さは、EN 999 および IEC 62046 に準拠しなければならない。




・　危険領域の安全防護対策の配置で感知領域の背後に立ち入ることが出来る場合には、再起動インターロックなどのさらなる対策が必要である。起動ボタン S2 をこの目的に使用できる。そのために、PLC K3 は、ボタンが押されている時間と最長および最短値を比較する。条件を満たしたときのみ、起動指令は有効になる。

**備考**

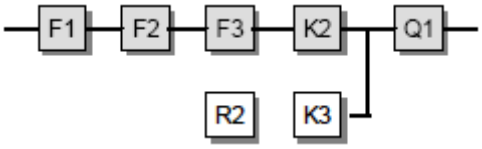
・　この例は、安全機能へのまれな要求がある場合に適用するためのものである。これは、カテゴリー2 に対する規定アーキテクチャへの要求事項、すなわち「安全機能へのデマンドよりもはるかに頻繁な試験」（付属書 G 参照）を満たすことを可能にする。
・　停止の始動後も、光バリアは次の起動まで停止状態を保持する。これにより例えば、それを回路に「登録」せずに、危険領域に入る事が可能となる。該当する回路の適用により動作を修正できる。

**故障確率計算**

・　例として、F1 から F3 までの 3 個の光バリアを故障確率計算に検討する。第 2 危険区域の安全防護対策は、別途計算されるさらなる安全機能を構成する。
・　故障確率計算のために、全体システムを、「光バリア」と「主接触器」（Q1）の 2 つのサブシステムに分ける。

「光バリア」サブシステム用：

・　F1、F2、F3 および K2 は、カテゴリー2 回路構造の機能用経路を構成する。PLC K3 分離用ダイオード R2 を含む）は試験機器を構成する。S2 および K1 は、光バリアの試験を起動させる機能を持っており、故障確率計算には関係しない。
・　$MTTF_d$：F1 から F3 のそれぞれに、100 年[E]の $MTTF_d$ を想定する。K2 の $B_{10d}$ 値は、20,000,000 サイクル[S]である。稼働日 240 日、稼働時間 16 時間、サイクル時間が 180 秒の場合、$\boldsymbol{n}_{op}$ は 1 年に 76,800 サイクルである。上記の試験ではこの値は 2 倍になり、$\boldsymbol{n}_{op}$ は 1 年に 153,600 サイクルで、K2 の $MTTF_d$ は 1,302 年となる。これらの値により、機能用チャンネルの $MTTF_d$ は 32 年（「高」）となる。K3 に 50 年[E]の $MTTF_d$ を想定する。相対的に、分離用ダイオード R2 の 228,311 年[S]の $MTTF_d$ 値は無関係になる。



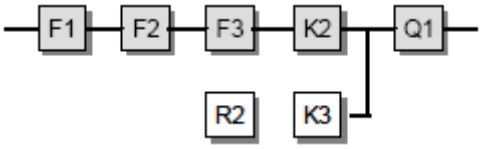

- $DC_{avg}$：F1 から F3 の 60%の DC は、記載の通り機能試験による。K2 の 99%の DC は、機械的に連結した接点要素を用いた K3 での直接監視から算出される。$DC_{avg}$ の平均化式により 61.0%（「低」）の結果が返る。
- 共通原因故障に対する適正な対策（85 点）：分離（15）、多様性（20）、過電圧保護など（15）および環境条件（25 + 10）
- 「光バリア」サブシステムにおける制御要素の組み合わせは、チャンネルごとの高い $MTTF_d$（32.5 年）と低い $DC_{avg}$（61.0%）のカテゴリー2 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.85 \times 10^{-6}$ となる。

「主接触器」サブシステムには以下のように仮定する。

- 1 年あたり 76,800 サイクルの $n_{op}$ で、$B_{10d}$ は 2,000,000 サイクル[S]。これは 260.4 年の $MTTF_d$ につながり、規格による上限の 100 年に達する。構造はカテゴリー1 に相当するため、$DC_{avg}$ と共通原因故障は関係しない。これにより、危険側故障の平均確率は 1 時間あたり $1.14 \times 10^{-6}$ となる。
- 2 つのサブシステムの危険側故障の平均確率を合計すると、1 時間あたり $3.0 \times 10^{-6}$ となる。これは PL c に相当する。
- 安全機能に対して、カテゴリー2 の規定アーキテクチャに対して仮定された頻度よりも頻繁（比率は 100：1 未満、すなわち 5 時間に 1 度よりも頻繁）にデマンドが行われると予想される場合には、付属書 G により 10%のペナルティーが付いた 25：1 の比率に下げてこれを考慮できる。3 個の光バリアを使用するここで考慮したケースでは、「光バリア」サブシステムには、まだ 1 時間あたり $2.04 \times 10^{-6}$ の故障確率がある。しかしながら、1 時間あたり $3.18 \times 10^{-6}$ の危険側故障の総合平均確率では PL b にしか達しない。PL c に達するには、例えば光バリアの数を減らすか、より高い $MTTF_d$ の構成部品を採用しなければならない。

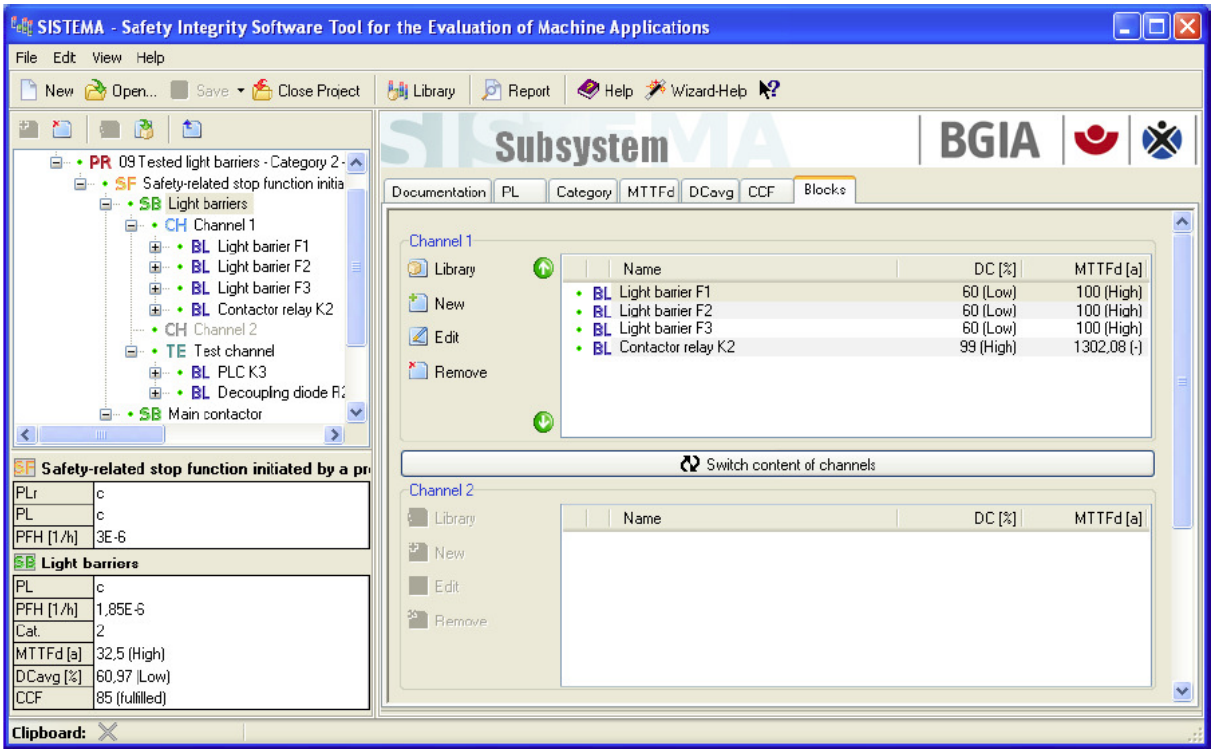
**より詳細な参考文献**


- *Grigulewitsch, W.; Reinert, D.*: Lichtschranken mit Testung. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 228. 22th suppl. V/94. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin, 1985 – loose-leaf ed.
  www.bgia-handbuchdigital.de/330228
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)



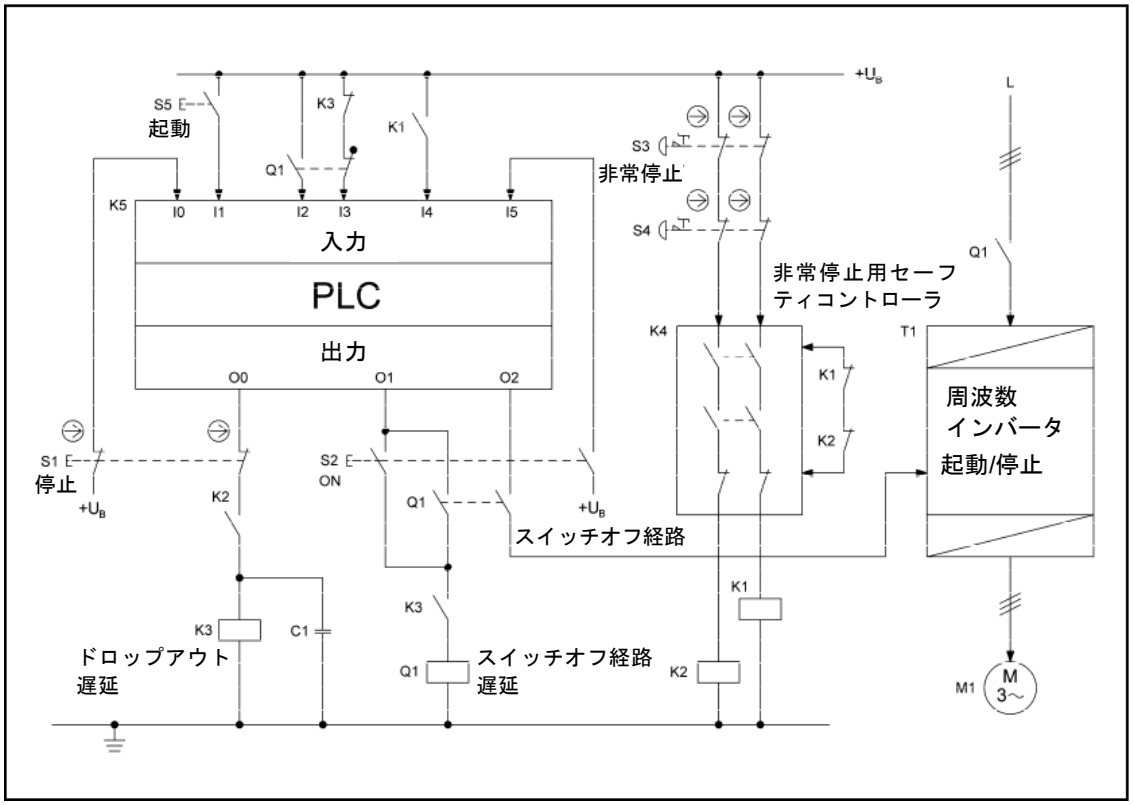

- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (draft standard IEC 44/501/CD:2005)
- EN 999: Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body (10.98)

図 8.18：SISTEMA による PL の決定



### 8.2.10　非常停止付き PLC 駆動ドライブの安全停止　－　カテゴリー3　－　PL c（例 10）

図 8.19：停止または非常停止指令による PLC 駆動の周波数インバータドライブの停止

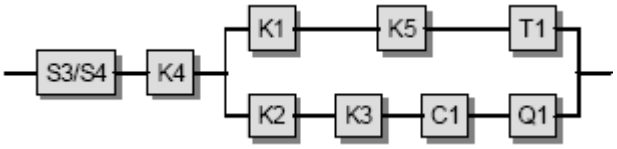



**安全機能**

- 安全関連停止機能/非常停止機能：停止または非常停止指令によりドライブが停止する。（SS1－安全停止 1）

**機能の説明**

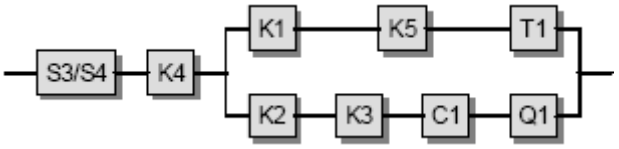
- 停止ボタン S1 または非常停止装置 S3 か S4 のうち 1 つの、どちらか片方でも作動すると、危険動作が冗長的に遮断される。非常時には S3/S4 の作動により非常停止用セーフティコントローラ K4 が出力せず、接触器リレーK1 および K2 が遮断されることで駆動が停止する。PLC K5 の入力 I4 の常時開接点 K1 が開くと、PLC 出力 O2 によって周波数インバータ（FI）T1 への起動信号をキャンセルする。K1-K5-T1 経路に冗長して、接触器リレーK3（ドロップアウト遅延付き）の上流にある常時開接点 K2 が開くと、ブレーキタイマーが開始する。ブレーキタイマーのタイムアウトと同時に、主接触器 Q1 の作動信号が遮断される。タイマーの設定は、好ましくない運転状態において、主接触器 Q1 がドロップアウトする前に機械の動作が停止するように選択する。




- 停止ボタン S1 の 2 つの常時閉接点が開くことで、停止デマンド後に駆動の機能停止が起こる。非常停止と同様に、まず PLC K5 が、この場合は入力 I0 を通して状態の走査を行い、PLC 出力 O2 のリセットにより FI が遮断される。このプロセスに冗長して、接触器リレーK3－コンデンサ C1 によるドロップアウト遅延付き－が遮断され、設定されたブレーキ時間のタイムアウト後に、主接触器 Q1 への作動信号が遮断される。
- PLC K5、周波数インバータ T1、主接触器 Q1、接触器リレーK1/K2 またはドロップアウト遅延付き接触器リレーK3 の故障の場合は､2 つの相互に独立した遮断経路が常に存在するため、駆動の停止が確保される。接触器リレーK1 および K2 のドロップアウトの失敗は、遅くても作動した非常停止装置のリセット後に検出される。これは、非常停止用セーフティコントローラ K4 内の機械的に連結した常時閉接点の監視により達成される。補助接触器 K3 のドロップアウトの失敗は、遅くても、機械的に連結した常時閉接点の PLC 入力 I3 へのフィードバックを通して機械動作が再起動する前に検出される。主接触器 Q1 のドロップアウトの失敗は、PLC 入力 I3 に読み込まれるミラー接点により検出される。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 接触器リレーK1、K2 および K3 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。
- 押しボタン S1、S3 および S4 の接点は、IEC60947-5-1　付属書 K に従い機械的に連結されている。
- 接触器 Q1 は、IEC60947-4-1　付属書 F によるミラー接点を有する。
- 6.3.10 項の指示により、標準構成部品 K5 および T1 を採用する。
- PL b の要求事項（多様性により低下させた）および 6.3 項の指示により、ソフトウェア（SRASW）をプログラミングする。
- フォールト（故障）の場合に、第 2 遮断経路のみでの停止の開始が遅れることにより、許容できないほど高い残存リスクを引き起こしてはならない。
- 非常停止用セーフティコントローラ K4 の安全関連制御部品は、カテゴリー3 および PL d の全ての要求事項を満たす。



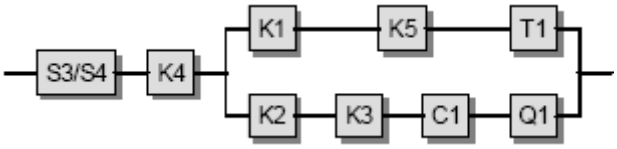

**故障確率計算**

非常停止機能の故障確率のみを計算する。安全関連停止機能の分析には、S3/S4 および K4 を S1 に差し替え、K1 および K2 を除外しなければならない。

- 表 D.2 に記載の、開閉装置のミッション時間内の 6,050 回の開閉サイクルの最大値を超えないため、非常停止装置 S3/S4 にはフォールト（故障）排除を想定する。非常停止用セーフティコントローラ K4 は、試験済み安全構成部品である。その故障確率は 1 時間あたり 3.0 x $10^{-7}$[M]であり、計算の最後に追加される。これは開閉装置のミッション時間内の、6,050 回の開閉サイクルの最大値に適用される。

下記の 2 チャンネル構造の故障確率には以下を適用する。

- $MTTF_d$：以下の $MTTF_d$ を想定する：K5 に対して 25 年、および T1 に対して 50 年[E]。コンデンサ C1 は 45,662 年[D]の $MTTF_d$ で計算に含める。400,000 サイクル[S]の $B_{10d}$ 値、および 240 稼働日での毎日の通電の開閉頻度で、K1 および K2 の $MTTF_d$ は 16,667 年になる。400,000 サイクル[S]の $B_{10d}$ 値で、稼働日 240 日、稼働時間 16 時間、サイクル時間が 3 分の場合、$n_{op}$ は 1 年に 76,800 サイクルとなり、K3 および Q1 のそれぞれの $MTTF_d$ は 52 年となる。これらの値により、チャンネルの対称化 $MTTF_d$ は 21 年（「中」）となる。
- $DC_{avg}$：減速ランプの作動故障の場合のプロセスによるフォールト（故障）検出で K5 の DC は 30%となる。T1 については、プロセスによるフォールト（故障）検出の結果として同様に DC は 60%となる。K1 および K2 は、K4 での一体的なフォールト（故障）検出により 99%の DC となり、K3 は K5 によるフォールト（故障）検出により 99%の DC となる。C1 については、FI を遮断した状態でのタイミング要素の試験により、DC は 60%となる。Q1 については、K5 での直接監視により、DC は 99%となる。$DC_{avg}$ の平均化式により 63%（「低」）の結果となる。
- 共通原因故障に対する適正な対策（75 点）：分離（15）、多様性（20）、FMEA（5）および環境条件（25 + 10）
- 制御要素の 2 チャンネルの組み合わせは、チャンネルごとの中間の $MTTF_d$（21 年）と低い $DC_{avg}$（63%）のカテゴリー3 を満たす。これにより、危険側故障の平均確率は 1 時間あたり 1.04 x $10^{-6}$ となる。これは PL c に相当する。全故障確率は、K4 の危険側故障確率を加えて決定し、それは 1 時間あたり 1.34 x $10^{-6}$ に等しい。よってこれも同様に PL c に相当する。



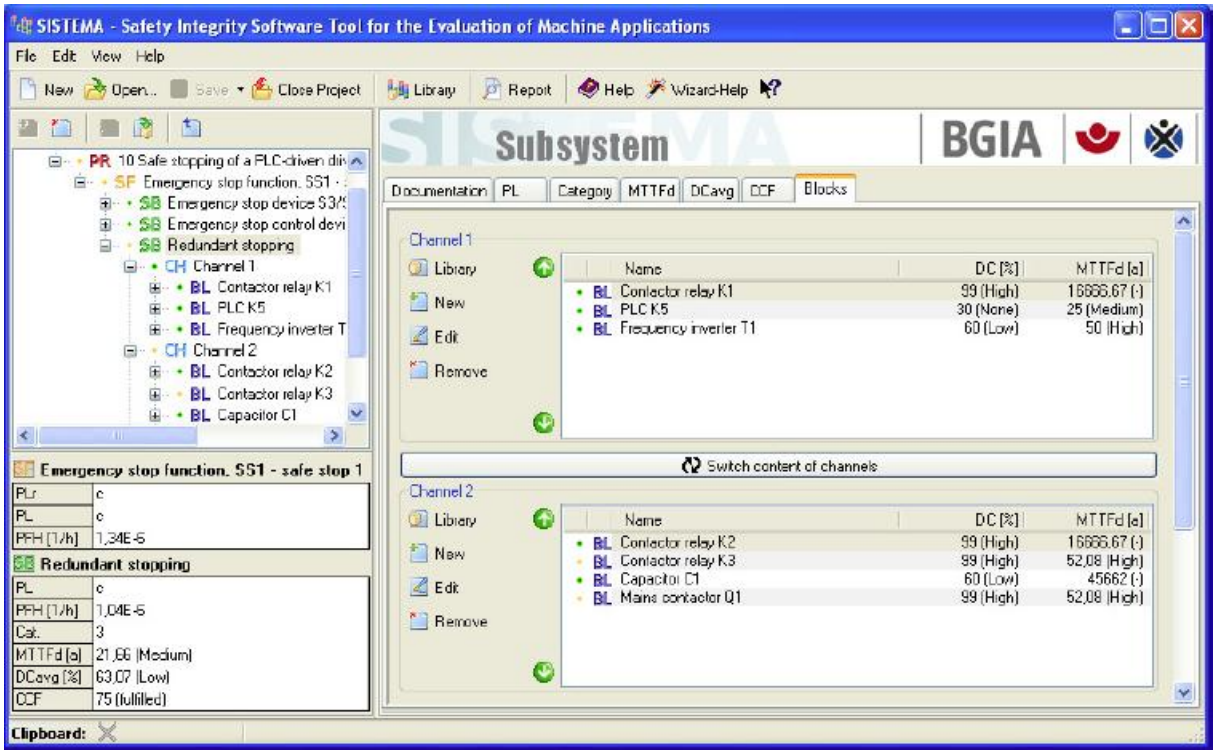

・　摩耗要素 K3 および Q1 は、約 5 年（$T_{10d}$）ごとに交換することが望ましい。

**より詳細な参考文献**

・　*Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003.
www.dguv.de/bgia, Webcode d6428

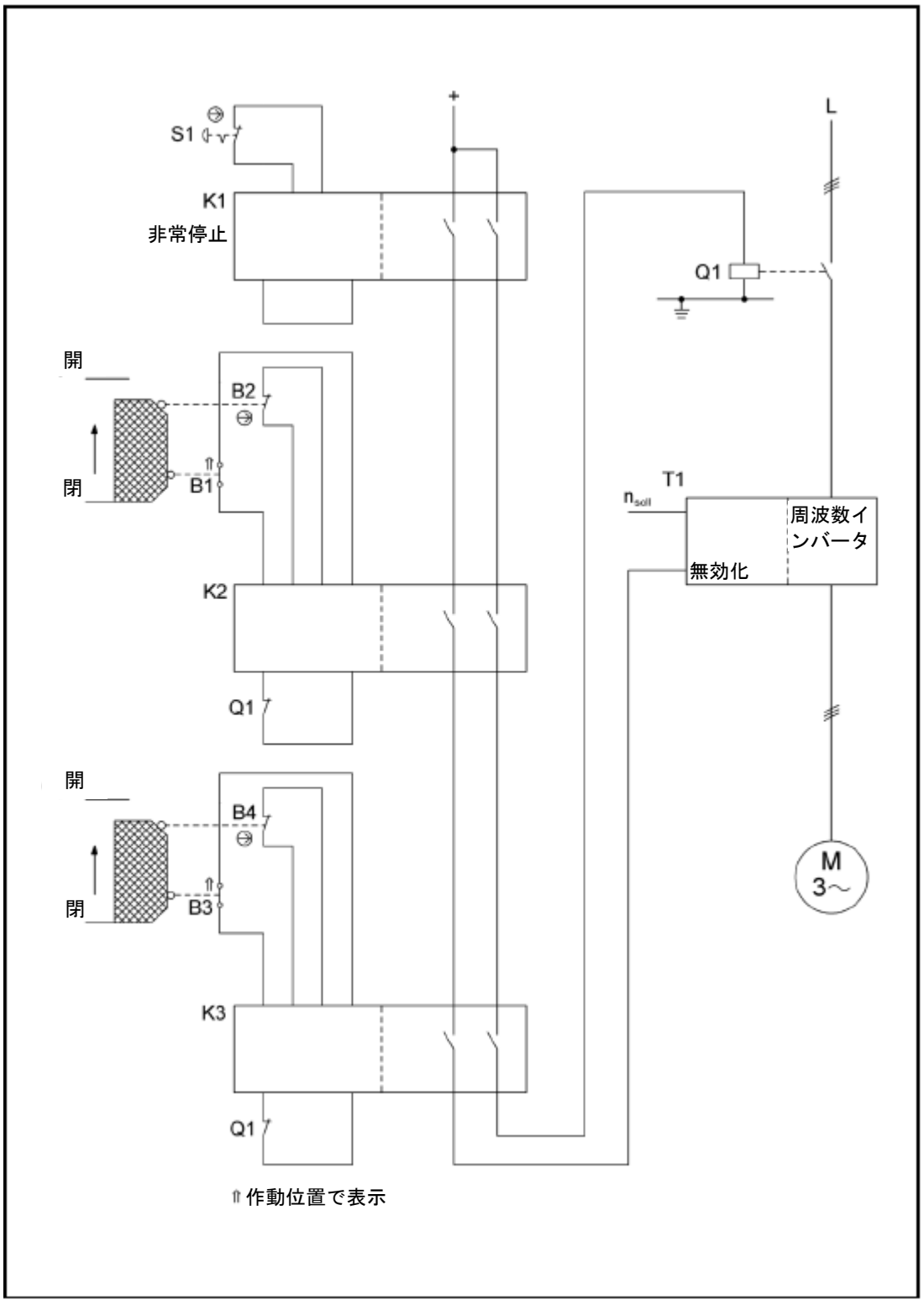
・　IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

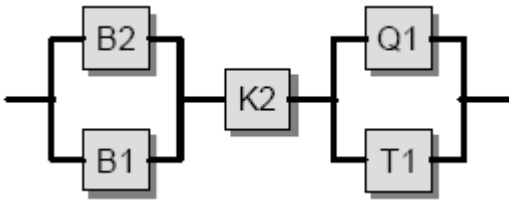
図 8.20：SISTEMA による PL の決定



### 8.2.17　安全モジュールによる保護装置のカスケード接続　－　カテゴリー3　－　PL d（例 17）

図 8.31：安全モジュールによる保護装置のカスケード接続（非常停止機能、STO）






**安全機能**

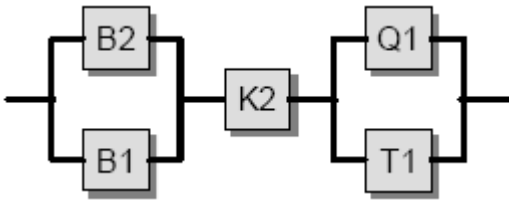
- 非常停止機能、非常停止装置の作動による STO－安全トルクオフ
- 保護装置によって起動する安全関連停止機能：可動式ガードが開くことで安全機能 STO－安全トルクオフが起動する。

**機能の説明**

- 非常停止装置 S1 が作動すると、接触器 Q1 の制御電圧の遮断および周波数インバータ T1 のコントローラインヒビットの選択により、安全モジュール K1 を通して冗長的に危険な動作や状態が遮断される。危険区域はまた 2 つの可動式ガード（例えば積載と荷降し用に 1 つづつ）によって防護されている。安全ガードの開動作は、常時閉接点/常時開接点の組み合わせである 2 つの位置スイッチ B1/B2 で検知され、中央安全モジュール K2 で評価される。後者は K1 と同じ方法で危険な動作や状態を遮断または防止できる。第 2 安全ガードは、2 つの位置スイッチ B3/B4 および安全モジュール K3 により同様に監視され、また Q1 および T1 に作用する。
- 安全機能は構成部品の故障の場合に保持される。
- 構成部品の主な故障は検出され、操作禁止につながる。安全ガード上の 2 つの位置スイッチは、関連安全モジュールで妥当性を監視される。安全モジュールはまた内部診断方策を採用する。接触器 Q1 でのフォールト（故障）は、機械的に連結した接点と、K2 および K3 でのリードバックにより検出される。非常停止機能のデマンドがそれほど頻繁ではないため、K1 での追加のリードバックは必要ない。T1 でのフォールト（故障）の 1 部はプロセスにより検出される。少数のフォールト（故障）は、コントローラでは検出されない。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 位置スイッチの作動のために保護装置の安定した配置を確保する。
- 非常停止装置 S1 は EN ISO 13850 に対応する; B2 および B4 は IEC 60947-5-1　付属書 K による直接開接点付き位置スイッチである。
- 位置スイッチ B1 および B4 への電源配線は、別々に配線または保護されている。



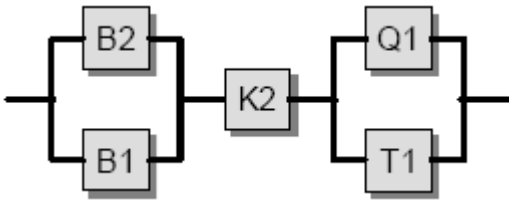

- 接触器 Q1 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。
- 安全モジュール K1、K2 および K3 は、カテゴリー4 および PL d の全ての要求事項を満たす。
- 周波数インバータ T1 は一体となった安全機能を持たない。

**備考**

- 非常停止機能は、EN ISO 12100-2:2004 による補完保護対策である。

**故障確率計算**

- 回路配置は 3 つの安全機能に分けられ、各機能は 3 つのサブシステムに割り当てられる。1 度に 1 つの保護装置しか開かないため、安全関連ブロック図には 1 つの保護装置の安全関連停止機能を例示する。同様の安全機能および同一の故障確率計算を 2 つ目の保護装置に適用する。非常停止機能については、非常停止装置 S1 および安全モジュール K1 が、初めの 2 つのサブシステムの代わりをする。標準安全モジュール K1、K2 および K3 の故障確率は計算の最後に追加される（1 時間あたり 2.31 x $10^{-9}$[M]、PL e に適する）。残りのサブシステムについては、故障確率を下記の通り計算する。
- S1 は EN ISO 13850 の標準非常停止装置である。本レポートの表 D.2 に記載の操作回数を超えなければ、フォールト（故障）排除が直接開接点および機械的要素に適用される。1 年に 3 回の作動を $n_{op}$ に仮定する。Q1 および周波数インバータの全体電気回路に関する両方の安全機能のさらなる計算の目的では、この値は無視される。
- $MTTF_d$：直接開動作付き位置スイッチ B2 の電気接点に対し、フォールト（故障）を排除することが可能である。位置スイッチ B1 の電気的常時開接点については、$B_{10d}$ 値は 1,000,000 開閉操作[M]となる。1,000,000 サイクルの $B_{10d}$ 値[M]は、B2 および B1 の機械的部品について提示されている。稼働日 365 日、稼働時間 16 時間、サイクル時間が 10 分の場合、これらの構成部品の $n_{op}$ は 1 年に 35,040 サイクルで、B2 の $MTTF_d$ は 285 年となり、B1 の $MTTF_d$ は 142 年となる。接触器 Q1 では、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,000,000 回の開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。

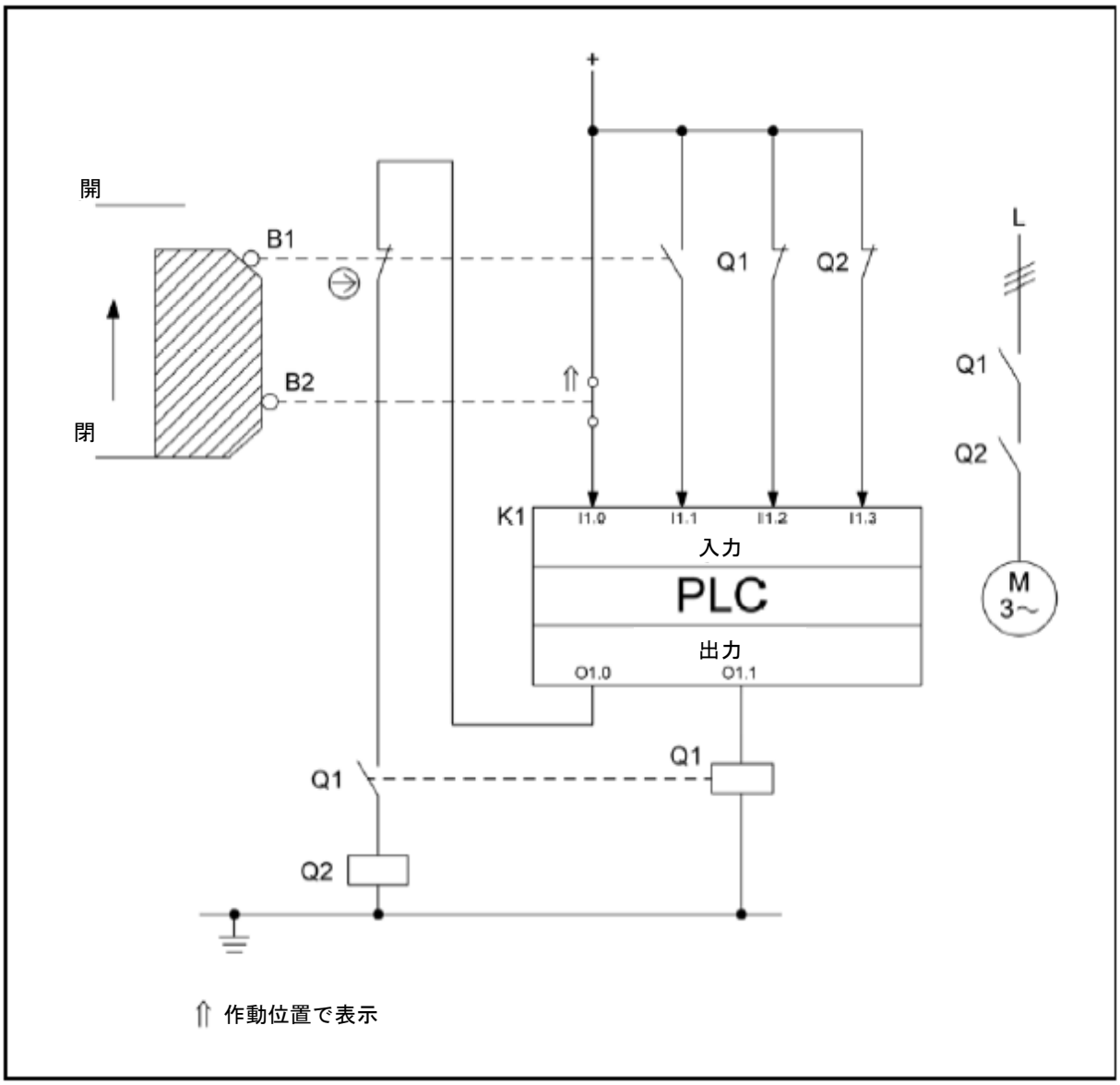



Q1 は両方の安全関連停止機能に関係するため、上記 $n_{op}$ の想定値を 2 倍して、$MTTF_d$ は 285 年となる。周波数インバータ T1 の $MTTF_d$ は 20 年[M]となる。全体で、サブシステム Q1/T1 内のチャンネルあたりの対称化 $MTTF_d$ は 68 年（「高」）となる。

- $DC_{avg}$ : B1 および B2 の 99%の DC は、K2 での常時閉接点/常時開接点の組み合わせの妥当性監視に基づく。これはサブシステムの $DC_{avg}$ に相当する。接触器 Q1 の 99%の DC は、安全モジュールでの接点位置のリードバックから算出される。プロセスによるフォールト（故障）検出により、周波数インバータ T1 の DC は 60%となる。そのため、平均化によりサブシステム Q1/T1 の $DC_{avg}$ は 62%（「低」）という結果になる。
- サブシステム B1/B2 および Q1/T2 における共通原因故障に対する適正な対策（それぞれ 70 および 85 点）: 分離（15）、過電圧保護など（15）および環境条件（25 + 10）、B2/B1 の十分に実証済みの構成部品（5）、Q1/T1 の多様性（20）
- サブシステム B1/B2 は、高い $MTTF_d$（100 年）と高い $DC_{avg}$（99%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $2.47 \times 10^{-8}$ となる。サブシステム Q1/T1 は、高い $MTTF_d$（68 年）と低い $DC_{avg}$（62%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.73 \times 10^{-7}$ となる。
- 安全関連停止機能については、危険側故障の平均確率は 1 時間あたり $2.00 \times 10^{-7}$ となる。これは PL d に相当する。
- 非常停止機能の危険側故障の平均確率は、1 時間あたり $1.75 \times 10^{-7}$ となる。これは PL d に相当する。

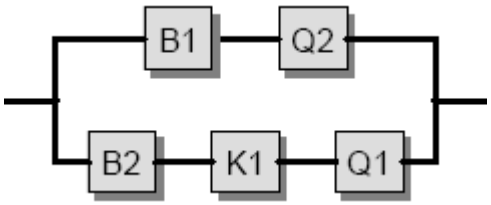
### 8.2.18　可動式ガードの位置監視　－　カテゴリー3　－　PL d（例 18）

図 8.32：技術的実装に多様性を採用した可動式ガードの冗長的な位置監視（電気機械およびプログラマブル電子）




**安全機能**

- 保護装置によって起動する安全関連停止機能：可動式ガード（保護格子）が開くことで安全機能 STO（安全トルクオフ）が起動する。

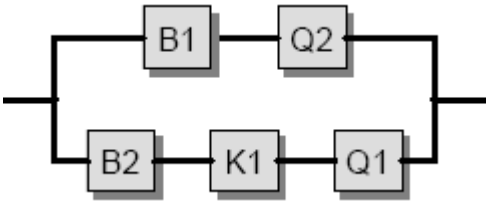



**機能の説明**

- 可動式ガード（例えば安全ガード）の開動作は、N.C.接点/N.O.接点の組み合わせである 2 つの位置スイッチ B1 および B2 が検知する。直接開接点付き位置スイッチ B1 は、ドロップアウトにより危険な動作や状態を遮断または防止する接触器 Q2 を作動させる。N.O.接点付き位置スイッチ B2 は、2 つ目の接触器 Q1 の作動により同じ遮断反応を引き起こすことができる、標準 PLC K1 により読み込まれる。
- 構成部品の故障の場合に安全機能が維持される。
- B1 の開閉位置も N.O.接点によって PLC K1 に読み込まれ、B2 の開閉位置との妥当性を比較される。接触器 Q1 および Q2 の開閉位置は、機械的に連結したリードバック接点により K1 で同様に監視される。B1、B2、Q1 および Q2 での構成部品の故障は K1 により検出され、Q1 および Q2 のドロップアウトにより操作禁止となる。PLC K1 でのフォールト（故障）は、機能（プロセスによるフォールト（故障）検出）によってのみ検出される。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 位置スイッチの作動のために保護装置の安定した配置を確保する。
- B1 は IEC60947-5-1　付属書 K による直接開接点付き位置スイッチである。
- 位置スイッチへの電源配線は、別々に配線または保護されている。
- 起動および作動メカニズムでのフォールト（故障）は、作動の原則が異なる（N.C.接点および N.O.接点）2 つの位置スイッチによって検出される。
- Q1 および Q2 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。
- PLC K1 は 6.3 項に記載の必須要求事項を満たす。




**故障確率計算**

- $MTTF_d$：直接開接点付き位置スイッチ B1 の電気接点に対し、フォールト（故障）を排除することが可能である。位置スイッチ B2 の電気的 N.O.接点については、$B_{10d}$ 値は 1,000,000 開閉操作[M]となる。1,000,000 サイクルの $B_{10d}$ 値[M]は、B1 および B2 の機械的部品について提示されている。稼働日 365 日、1 日あたりの稼働時間 16 時間、サイクル時間が 1 時間の場合、これらの構成部品の $n_{op}$ は 1 年に 5,840 サイクルで、$MTTF_d$ は、B1 について 1,712 年となり、B2 については 856 年となる。接触器 Q1 および Q2 では、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,300,000 開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。上記 $n_{op}$ の想定値から、Q1 および Q2 の $MTTF_d$ は 4,452 年となる。PLC の 15 年[M]の $MTTF_d$ 値は置換され、2 倍することで 30 年の $MTTF_d$ 値になる。B1 と Q2 の組み合わせで、第 1 チャンネルの $MTTF_d$ は 1,236 年となり、B2、K1 および Q2 の組み合わせで、第 2 チャンネルの $MTTF_d$ は 28 年となる。全体で、両チャンネルに渡り対称化 $MTTF_d$ 値は、チャンネルあたり 70 年（「高」）となる。
- $DC_{avg}$：B1 および B2 の 99%の DC は、PLC K1 での 2 つの開閉状態の妥当性監視に基づく。接触器 Q1 および Q2 の 99%の DC は、機械的に連結した接点要素を通して、また K1 でのリードバックから算出される。プロセスによるフォールト（故障）検出の可能性により、K1 の DC は 60%と想定される。そのため、平均化により $DC_{avg}$ は 62%（「低」）という結果になる。
- 共通原因故障に対する適正な対策（65 点）: 分離（15）、過電圧保護など（15）および環境条件（25 + 10）
- 制御要素の組み合わせは、高い $MTTF_d$（70 年）と低い $DC_{avg}$（62%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.66 \times 10^{-7}$ となる。これは PL d に相当する。

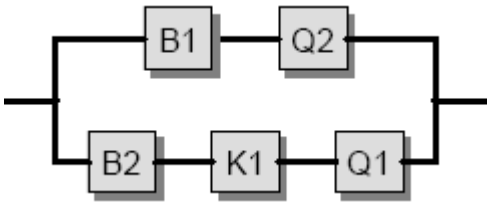
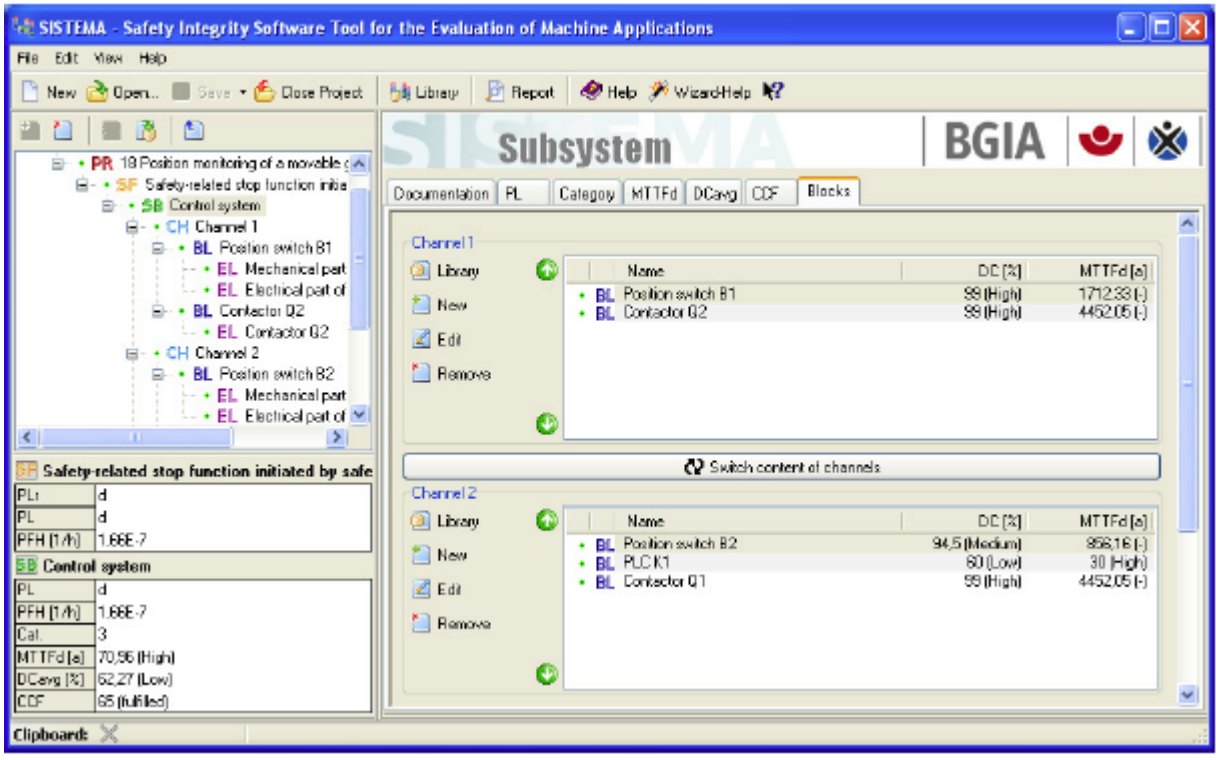
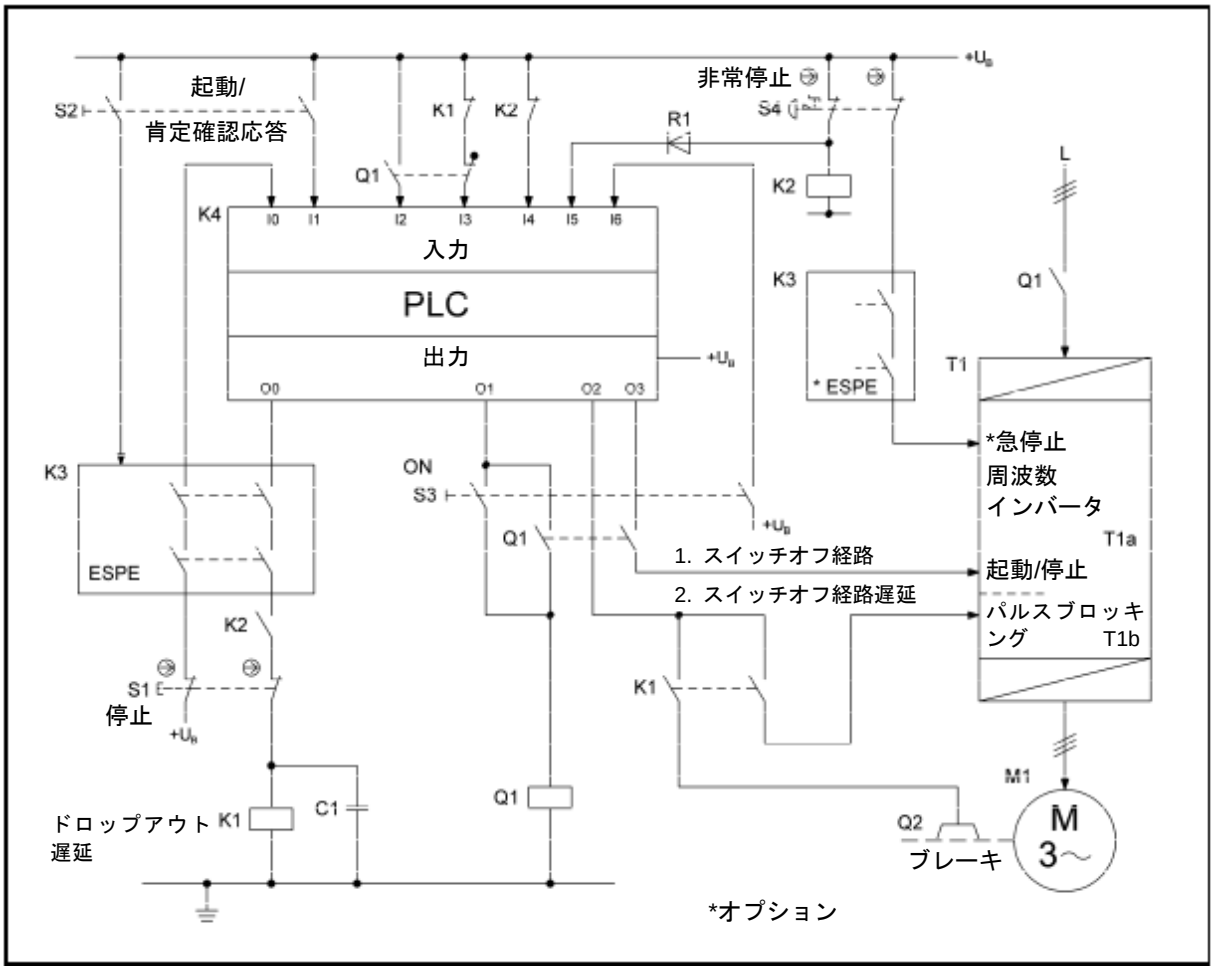



図 8.33：SISTEMA による PL の決定



### 8.2.20　PLC 駆動ドライブの安全停止　－　カテゴリー3　－　PL d（例 20）

図 8.36：停止または非常停止指令による、または保護装置（この場合 ESPE）のトリップによる PLC 駆動の周波数インバータドライブの安全停止

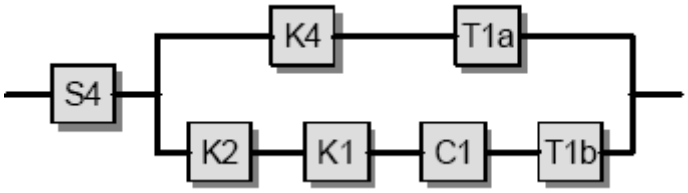



**安全機能**

- 保護装置によって起動する安全関連停止機能：停止または非常停止指令により、または保護装置のトリップによりドライブが停止する。（SS1－安全停止 1）

**機能の説明**

- 停止ボタン S1 か保護装置 K3（回路図に、電気的検知保護機器（ESPE）として表示）のどちらか片方でも作動すると、危険動作は冗長的に停止される。非常時には非常停止装置 S4 の作動により駆動が停止する。3 ケース全てにおいて、周波数インバータ（FI）T1 で「起動/停止」入力（T1a）が不活性化することにより、PLC K4 の出力 O3 を通して 1 次設定されたブレーキ時間が実行される。

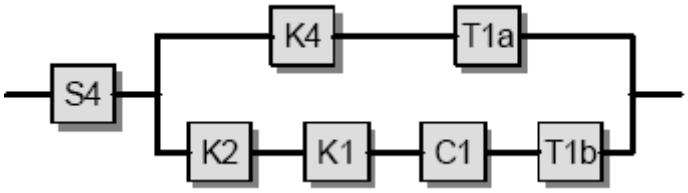



この配置に冗長して、2 次設定されたブレーキ時間は、接触器リレーK1（ドロップアウト遅延用にコンデンサ C1 を使用）の遮断、およびブレーキ Q2 の適用によりもたらされる、T1 での「パルスブロッキング」入力（T1b）が不活性化して実行される。そのため、第 1 消勢遮断経路は PLC K4 により直接実行され、反対に第 2 消勢遮断経路は、リレー技術および遅延ドロップアウトを採用する。PLC プログラムの O2 および K1 のタイマー設定は、好ましくない運転状態においても機械動作が停止するように選択する。

- 特に急減速付きの「急停止」入力が FI に付いていれば、回路図に示すように、必要に応じて非常停止装置および ESPE をそれに接続できる。このオプションは以下では考慮されない。
- PLC K4、周波数インバータ入力 T1a/T1b、ドロップアウト遅延付き接触器リレーK1 または接触器リレーK2 の故障の場合は、2 つの相互に独立した遮断経路が常に存在するため、駆動の停止が確保される。補助接触器 K1 または K2 のドロップアウトの失敗は、遅くても、機械的に連結した常時閉接点の PLC 入力 I3 および I4 へのフィードバックにより機械動作が再起動する前に検出される。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 安全パルスブロッキング付き周波数インバータの使用により、接触器 Q1 は電源電圧の遮断のために必ずしも絶対的に必須ではなくなる。周波数インバータはランプ上昇及びブレーキングに適していなければならない。
- 接触器リレーK1 および K2 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。
- 押しボタン S1 および S4 の接点は、IEC60947-5-1　付属書 K に従い機械的に連結されている。
- 6.3.10 項の指示により、標準構成部品 K4 および T1 を採用する。
- PL c の要求事項（多様性により低下させた）および 6.3 項の指示により、ソフトウェア（SRASW）をプログラミングする。
- ブレーキ Q2 が機能的理由のみで備えられていれば、すなわち安全機能の実行に無関係であれば、この例のように故障確率の計算において無視される。この手段には、パルスブロッキングのみで遮断される T1a の故障（以下参照）の場合に、駆動のコーストダウンが許容できないほど高い残存リスクを付随しないことが要求される。




FI の使用と連動した安全機能の実行へのブレーキの使用を、回転ドア制御の例に記載する。（例 23）

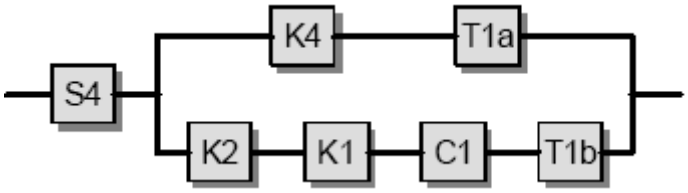
- ESPE K3 は、例えば光カーテンの形で、EN 61496-1 および IEC 61496-2 のタイプ 4、および PL e の要求事項を満たす。

**故障確率計算**

- 安全関連ブロック図にも示されている非常停止装置 S4 または ESPE により始まる安全停止の故障確率を計算する。FI の「急停止」機能や Q1 を通して FI へ送られる電源の遮断用設備は安全機能の故障確率計算には考慮されない。
- 周波数インバータ T1 は、ブロック T1a および T1b に分けられる。ブロック T1a は起動および停止の機能及び制御システム内での実行を含む。ブロック T1b は、少数の構成部品により実現するパルスブロッキングを含む。

非常停止装置 S4 により始まる安全停止：

- 表 D.2 に記載の作動回数を超えないため、非常停止装置にフォールト（故障）排除を仮定する。
- $MTTF_d$：以下の $MTTF_d$ を想定する：K4 に対して 50 年、T1a に対して 100 年、および T1b に対して 1,000 年[E]。400,000 サイクル[S]の $B_{10d}$ 値で、稼働日 240 日、稼働時間 8 時間、サイクル時間が 6 分の場合、$n_{op}$ は 1 年に 19,200 サイクルとなり、K1 の $MTTF_d$ は 208 年となる。400,000 サイクル[S]の $B_{10d}$ 値、および 240 稼働日での毎日の作動で、K2 の $MTTF_d$ は 16,667 年になる。コンデンサ C1 は 45,662 年[D]の $MTTF_d$ で計算に含める。これらの値により、チャンネルごとの対称化 $MTTF_d$ は 72 年（「高」）となる。
- $DC_{avg}$：プロセスによるフォールト（故障）検出で、K4 の DC は 30%、T1a の DC は 90%、T1b の DC は 60%となる。K1 の 99%の DC および C1 の 60%の DC は、FI を遮断した状態でのタイミング要素の試験により算出される。K2 の DC は、S4 の開閉状態での K4 での妥当性試験により 99%となる。$DC_{avg}$ の平均化式により 56.9%（「低」の公差内）となる。
- 共通原因故障に対する適正な対策（85 点）：分離（15）、多様性（20）、過電圧保護など（15）および環境条件（25 + 10）




- 制御要素の組み合わせは、チャンネルごとの高い $MTTF_d$（72 年）と低い $DC_{avg}$（56.9%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $1.76 \times 10^{-7}$ となる。これは PL d に相当する。

ESPE K3 により始まる安全停止：

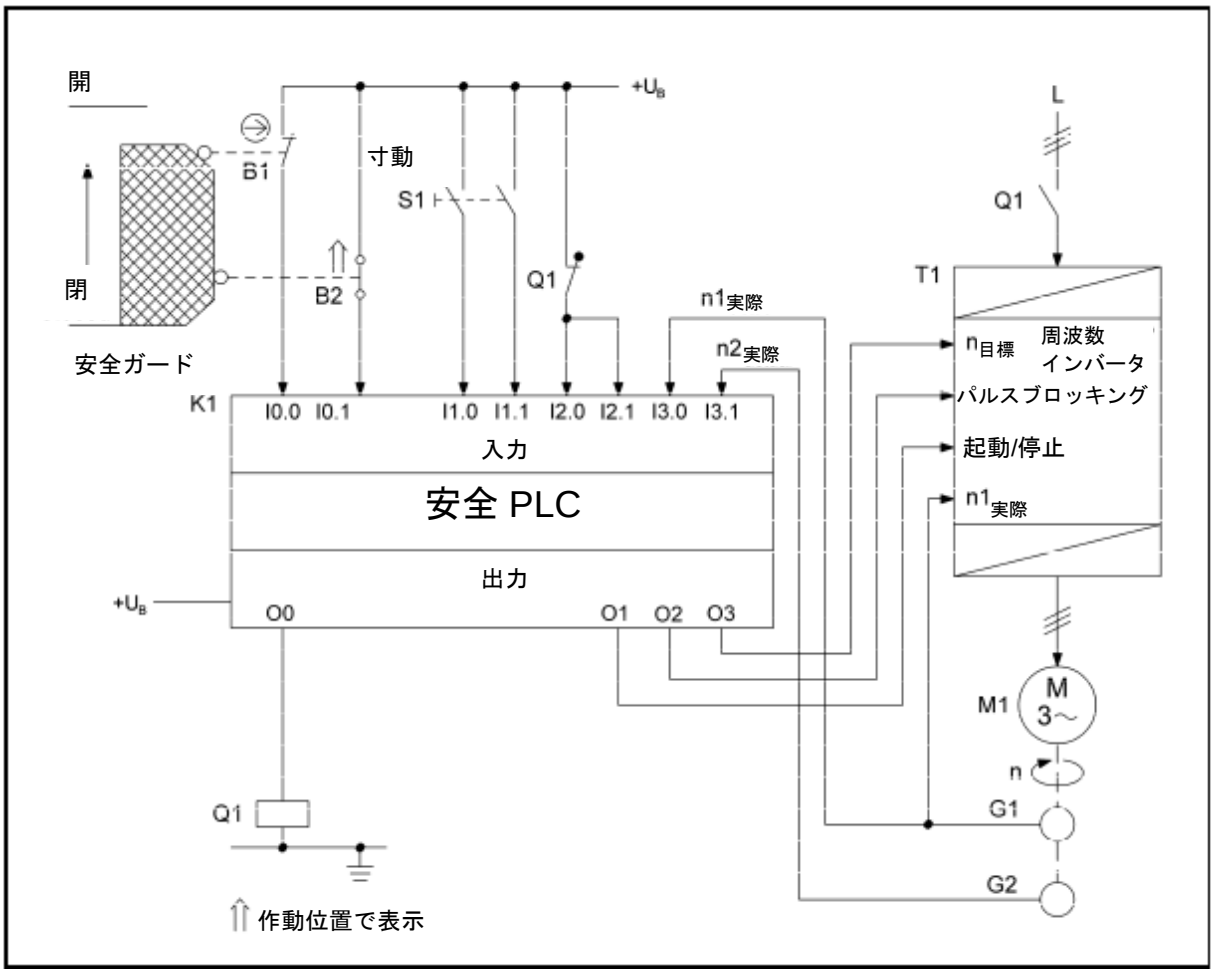
- ESPE K3 は標準の安全構成部品である。その故障確率は 1 時間あたり $3.0 \times 10^{-8}$[M]であり、計算の最後に追加される。
- 「PLC/電気機械」2 チャンネル構造の故障確率は、上記と同様の $MTTF_d$ および DC 値を使用して計算される。しかしながら、構成部品 K2 はこの安全機能の実行に関係しない。結果として、1 チャンネルの $MTTF_d$ は 72 年（「高」）となり、$DC_{avg}$ は 56.8%（「低」の公差内）となる。カテゴリー3 ではこれにより危険側故障の平均確率は 1 時間あたり $1.77 \times 10^{-7}$ となる。全故障確率は加算して決定し、1 時間あたり $2.07 \times 10^{-7}$ の結果となる。これも PL d に相当する。

**より詳細な参考文献**


- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003. www.dguv.de/bgia, Webcode d6428
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

### 8.2.21　寸動モード用安全制限速度　－　カテゴリー3　－　PL d（例 21）

図 8.37：安全ガード開時の安全制限速度、安全 PLC 内の目標/実際値比較および規定速度制限値付き寸動モード

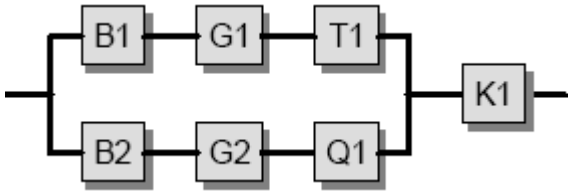



**安全機能**

・　安全制限速度（SLS）：安全ガードが開いている時に、寸動モードでの許容速度の超過を防止する。

**機能の説明**

・　安全ガードが開いている時に、危険動作を安全に防止または遮断する。安全ガードの開動作は、常時閉接点/常時開接点の組み合わせである 2 つの位置スイッチ B1 および B2 により検知される。押しボタン S1 が作動すると、安全 PLC K1 によって周波数インバータ T1 に安全制限速度が設定される。PLC の 2 つのプロセスチャンネルは、それぞれ相互に独立してアプリケーションソフトウェアから制限値設定を受け取る。

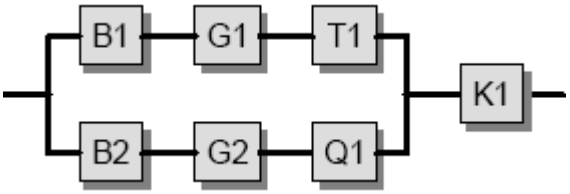



K1 の入力 I3.0 および I3.1 での寸動速度の実際の回転速度値は、2 つの別のタコジェネレータ G1 および G2 で監視する。PLC の各チャンネルは、目標/実際速度比較を独立して行う。T1 によって速度が制限値までうまく低下しなければ、起動/停止信号のブロッキングおよびインバータのパルスブロッキングにより、K1 で停止を開始できる。T1 への電源は、主接触器 Q1 によって遮断できる。

- 安全関連データは安全 PLC K1 の内部インターフェースを通して交換される。それらのデータは、2 つのプロセスチャンネル間の状態比較により、例えばフォールト（故障）検出用に採用される。1 つのプロセスチャンネルが故障すると、残りの機能しているプロセスチャンネルがインバータ T1 の速度を低下させ、主接触器 Q1 を遮断させる。例えば予期しない起動、連続した運転または加速につながる可能性のあるインバータの故障は、両プロセスチャンネルのタコジェネレータ G1 および G2 による個別の速度監視によって検出される。主接触器 Q1 のドロップアウトの失敗は、両プロセスチャンネル（K1 の入力 I2.0 および I2.1）にある常時閉接点により検出され、起動/停止信号のブロックと、両プロセスチャンネルによるインバータでのパルスブロッキングにつながる。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 位置スイッチの作動のために保護装置の安定した配置を確保する。
- 位置スイッチ B1 は、IEC60947-5-1　付属書 K による直接開動作を有する。位置スイッチ B2 もまた IEC60947-5-1 に準拠する。
- 接触器 Q1 は、IEC60947-4-1　付属書 F によるミラー接点を有する。
- 位置スイッチへの電源配線は、別々に配線または機械的損傷から保護されている。
- 安全機能「安全制限速度」については、エンコーダ軸破損（G1/G2）のフォールト（故障）状態には、フォールト（故障）の排除を想定する。フォールト（故障）排除の可能性についての詳細は、例えば IEC 61800-5-2　表 D.16 で参照できる。
- 6.3.10 項の指示により、標準構成部品 G1 および G2（回転信号エンコーダに関連する場合）および T1 を採用する。



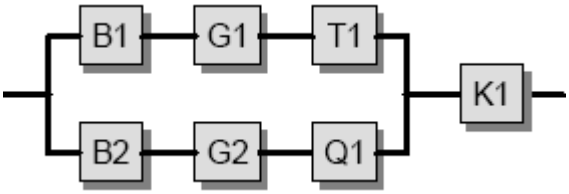

- 安全構成部品 K1 はカテゴリー3 および PL d の全ての要求事項を満たす。PL d の要求事項および 6.3 項の指示により、ソフトウェア（SRASW）をプログラミングする。
- 安全 PLC の各出力が PLC の両プロセスチャンネル（除く O3）により作動すると想定する。

**備考**

- EN 1010-1 によれば、オペレータが危険箇所へ日常的に介入しない機械では、各インタロック付きガードに IEC 60947-5-1　付属書 K の直接開動作付き位置スイッチ 1 つを使用すれば十分である。この文脈でのフォールト（故障）排除は、EN 60204-1 に従って取り付けられるスイッチを条件とする。
- 寸動モードの完全実施のためには、安全機能「寸動モードでの予期しない起動の禁止」も考慮しなければならない。

**故障確率計算**

- SRP/CS を、センサ/アクチュエータと PLC の 2 つのサブシステムに分ける。PLC サブシステムには、PL d に適する試験済み安全 PLC を採用する。この PLC の 1 時間あたり $1.5 \times 10^{-7}$ の故障確率[E]は、センサ/アクチュエータサブシステムの計算の最後に追加される。ブロック図の作成には、図 6.14 および関連文章中の該当するコメントも参照のこと。センサ/アクチュエータサブシステムの故障確率は、下記の通り計算する。
- $MTTF_d$ : 稼働日 240 日、稼働時間 8 時間、サイクル時間が 1 時間の場合、$n_{op}$ は 1 年に 1,920 サイクルである。直接開動作であることから、位置スイッチ B1 には、20,000,000 サイクル[S]の $B_{10d}$ 値を想定し、付随する $MTTF_d$ 値は 104,116 年となる。規定された制御電流（低負荷で、接触器の機械的寿命が決定的要因である。）により、位置スイッチ B2 には、1,000,000 サイクル[E]の $B_{10d}$ 値を想定し（表 D.2 も参照）、それにより $MTTF_d$ 値は 5,208 年となる。400,000 サイクルの $B_{10d}$ 値のある接触器 Q1 は、運転上毎日 1 回だけ開閉し、それは 1 年あたり 240 サイクルの $n_{op}$ および 16,667 年の $MTTF_d$ に相当する。以下の値を想定する：T1 の $MTTF_d$ は 100 年および G1/G2 の $MTTF_d$ は 50 年[E]。これらの値により、チャンネルごとの対称化 $MTTF_d$ は 41 年（「高」）となる。
- $DC_{avg}$ : 使用される構成部品のそれぞれに、99%の DC を想定する。位置スイッチおよびタコジェネレータについては、この値は K1 の入力信号の照合検査に基づく。インバータ T1 については、フォールト（故障）検出はプロセスにより行い、主接触器 Q1 は PLC に直接監視される。




これらの値により、$DC_{avg}$ は 99%（「高」）となる。

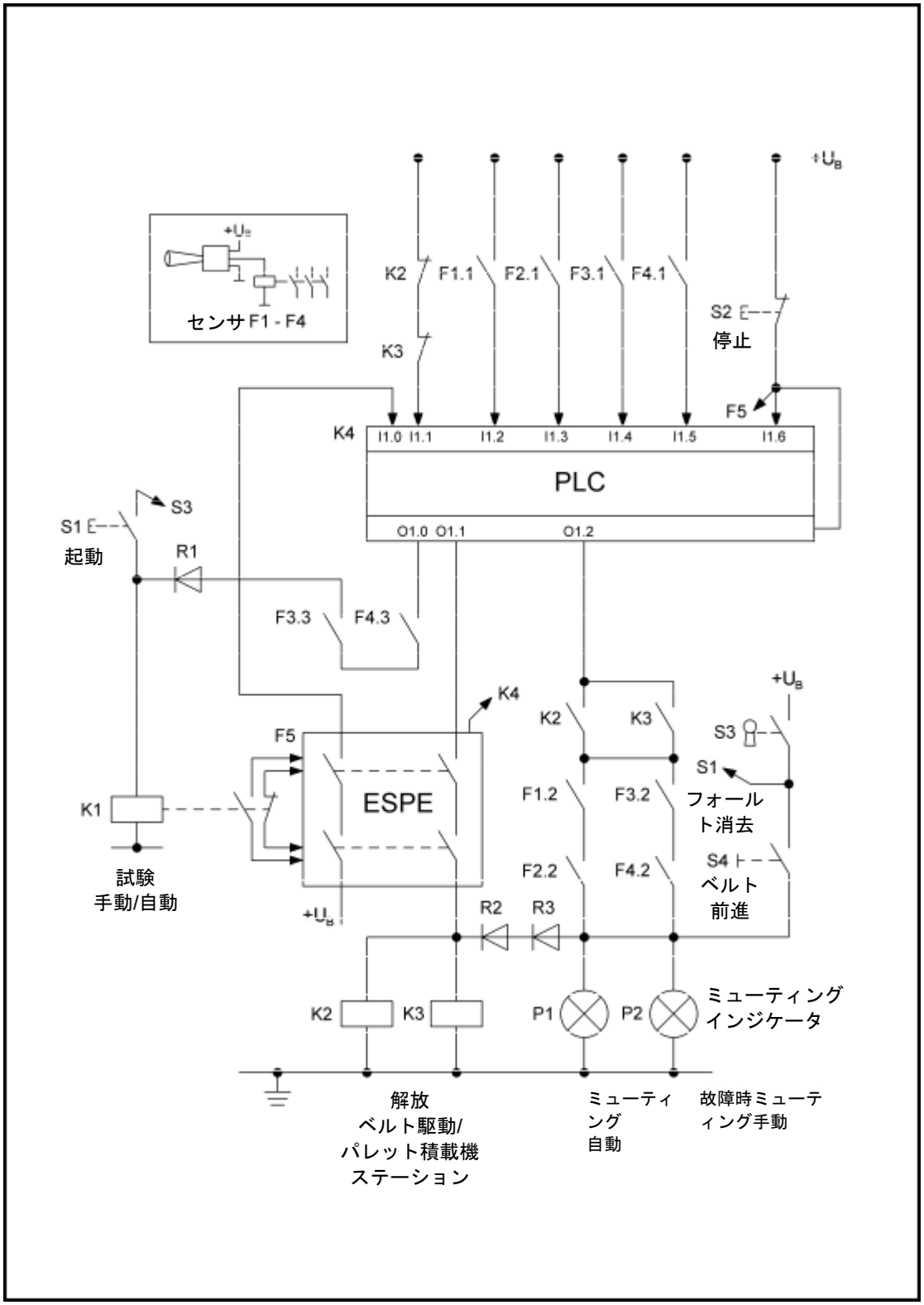
- 共通原因故障に対する適正な対策（70 点）：分離（15）、FMEA（5）、過電圧保護など（15）および環境条件（25 + 10）
- センサ/アクチュエータサブシステムは、チャンネルごとの高い $MTTF_d$（41 年）と高い $DC_{avg}$（99%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり 6.56 x $10^{-8}$ となる。これは PL e に相当する。このため $PL_r$ d を超え、構成部品の少ないハードウェアの要求される 2 チャンネル設計、規格による $B_{10d}$ 値の使用、「高い」DC および「中程度の」開閉頻度が事実上常にそのケースとなる。
- 全故障確率は、K1 の危険側故障確率（1 時間あたり 1.5 x $10^{-7}$）を加えて決定し、それは 1 時間あたり 2.16 x $10^{-7}$ となる。これは PL d に相当する。

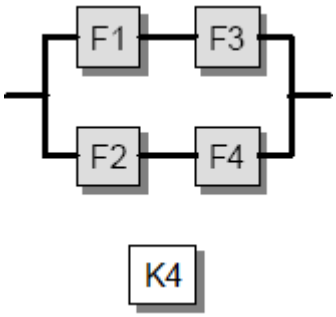
**より詳細な参考文献**


- *Grigulewitsch, W.; Reinert, D.*: Schaltungsbeispiele mit programmierbaren Steuerungen zur Umsetzung der Steuerungskategorie 3. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 227.
  27th suppl. I/95. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – looseleaf ed.
  www.bgia-handbuchdigital.de/330227
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)
- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (12.04)

### 8.2.22　保護装置のミューティング　－　カテゴリー3　－　PL d（例 22）

図 8.38：PLC 制御のパレット積載装置からの排出点における保護装置のミューティング






**安全機能**

- ミューティング機能：プロセスの機能としての保護装置の一時的なミューティング。パレット積載装置へのアクセスの安全防護や起動/再起動インターロックのようなさらなる安全機能は、以下の詳細では扱わない。

**機能の説明**

- パレット積載装置からの排出個所へのアクセスは、EN 61496 のタイプ 4 の 3 重ビーム光バリア（ESPE）F5 によって安全防護している。光バリアは、2 つの相反入力によって実行される、起動インターロックおよび再起動インターロックの追加機能を具体化する。光バリアの起動インターロックの無効化は、ベルト駆動用の起動コマンド、すなわちパレット積載ステーションの通電と接続し、起動ボタン S1 の作動および解放に応答した接触器リレーK1 のピックアップとそれに続くドロップアウトによって始まる。有効な起動コマンドの条件は、接触器リレーK2 および K3 がドロップアウトし（入力 I1.1 を通して走査される）、かつ起動インターロックがキャンセルされた（入力 I1.0 を通して走査される）状態である。出力 O1.1 は結果として設定される。
- 4 つの赤外線光センサ F1 から F4（配置については、図 8.38 も参照）を、ミューティングプロセスの制御のために組み込む。2 つのプログラムされた時間設定を考慮して、入力 I1.2 から I1.5 では、PLC がセンサの接点 F1.1 から F4.1 を通して 4 つの赤外線光センサの作動シーケンスを監視する。ミューティング機能は、光バリア F5 の出力回路とは独立して、PLC の出力回路（出力 O1.2）にのみ実装される。直列に接続されたミューティング接点 F1.2 および F2.2/F3.2 および F4.2 は、ダイオード R2 および R3 それぞれを通して、接触器リレーK2 および K3 によって実行される「イネーブル」機能のついた OR ロジックにより接続される。
- ミューティング機能がアクティブでなければ、R2 および R3 はミューティング機能を正しく表示させ、活性化したイネーブル出力をミューティング表示 P1/P2 から分離させる。R2 または R3 でのフォールト（故障）は、望ましからぬミューティング（すなわちミューティング機能の危険側故障）にはつながらない。
- 停電やそれに続く電圧の復旧の場合、または光バリア F5 が遮断されミューティング機能がアクティブでない場合は、接触器リレーK2 および K3 は遮断される。ミューティング回路が再度閉まる時には、これらの条件下でのラッチインの不在により、それらが再度ピックアップするのを防ぐ。再起動インターロックを無効にすること、すなわち起動ボタン S1 の意図的な作動および解放によってのみ、装置を再起動できる。

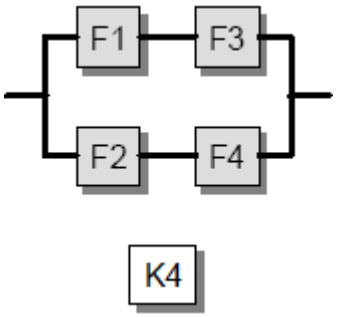
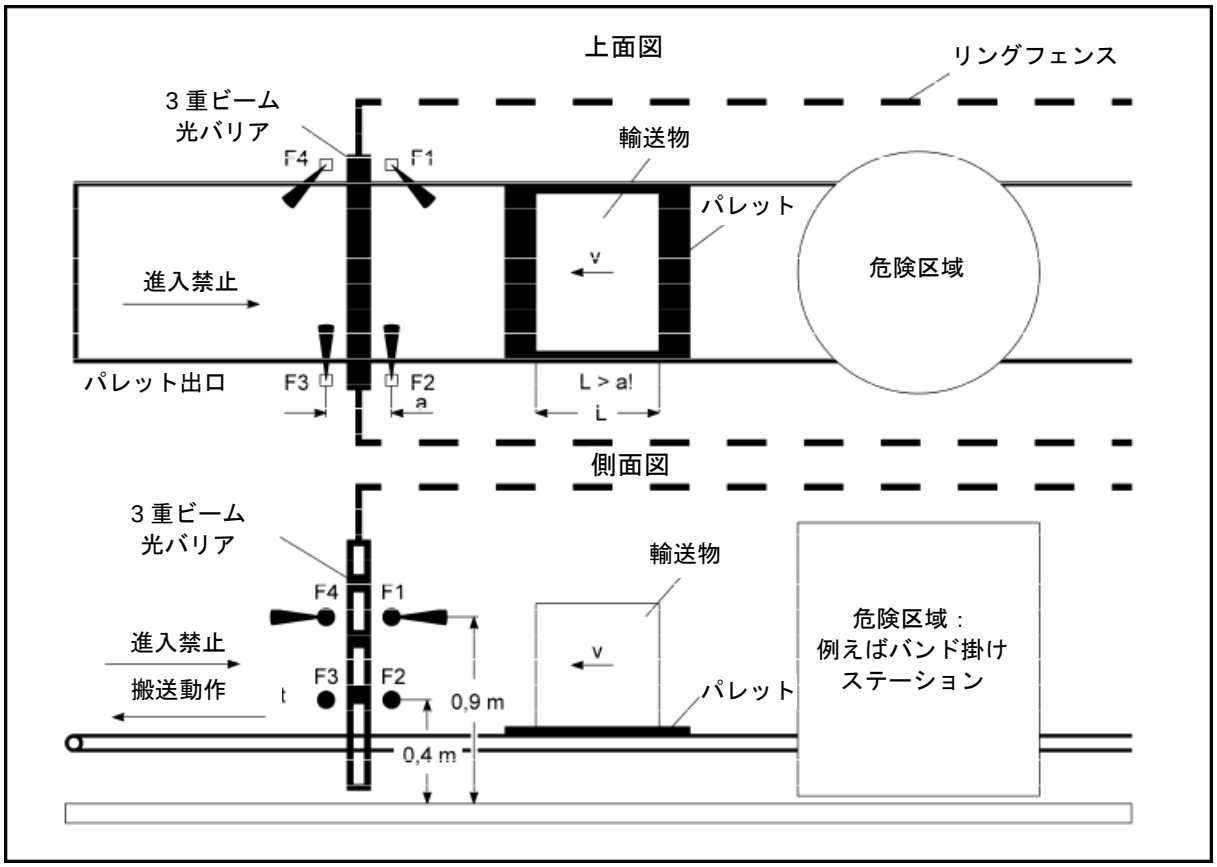
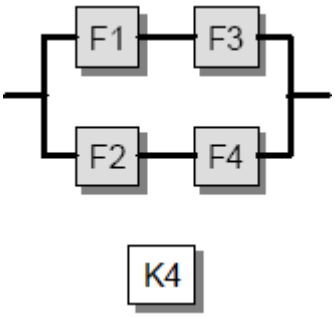



図 8.39: 自動制御付きパレット積載ステーション　－　光バリアおよびミューティングセンサ F1 から F4 の配置によるパレット排出箇所の安全防護原則




・　意図された、例えば装置のフォールト（故障）の後の起動/再起動では、キースイッチ S3 が作動しなければならない。フォールト（故障）状態の場合は、オペレータはパレットをデッドマンボタン S4 によって光バリアやミューティングセンサの検出領域から取り出すことができる。

排出口を通してパレットを円滑に進行させるためには、PLC プログラムでの 2 つの時間設定が搬送動作の速度にマッチしなければならない：

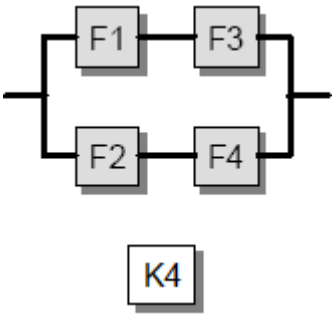



- 時間設定 T1 は、センサ F1 の活性化の後にセンサ F2 が起動し、輸送物によってミューティング機能が始まらなければならない最大期間を決定する。
- 時間設定 T2 は、センサ F2 の再消去から始まる。T2 は、光バリアの検出区域が再度空になった時に K1 が通電し、センサ F3 が輸送物によって不活性化し、ミューティング機能がそれによって終了する前に再度遮断されるように選択しなければならない。

・ 接触器 K2 および K3 のドロップアウトの失敗は、遅くても、機械的に連結した常時閉接点の PLC 入力 I1.1 へのフィードバックによりベルト駆動/パレット積載装置が再起動する前に検出される。K1 の故障は、次のパレット排出時に検出される。
・ 停電やそれに続く復旧または標準 PLC の故障の場合の意図しないベルト駆動/パレット積載装置の起動は、起動および再起動インターロックの機能により、防止される。パレットが光バリアを超えた直後、すなわちセンサ F3 および F4 がまだアクティブである時にのみ、PLC は再起動インターロックを無効にすることができる。
・ 個々のミューティングセンサの故障は、PLC プログラムによって（活性化および不活性化の適切な完了の監視によって）直接検出されるか、またはパレット搬送中の操作禁止によって明らかになる。
・ フォールト（故障）を消去するため（手動ミューティング）にだけ使用されるデッドマンボタン S4 の故障は、ユーザによって直接検出される。

**設計特性**

・ 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
・ 接触器リレーK1 から K3 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。
・ 光バリア F5 およびデッドマンボタン S4 への電源配線は、個々の配線間での短絡（供給電源へも含む）を排除できるように設置する。
・ 制御構成部品 S1 から S4 は、危険領域外で、かつそれが見える場所に配置する。




- ミューティング状態は、危険領域へのアクセス箇所でオペレータにはっきりと見える 2 つの表示灯で表示される。
- 6.3.10 項の指示により、適用できる場合は標準構成部品 F1 から F4 を採用する。

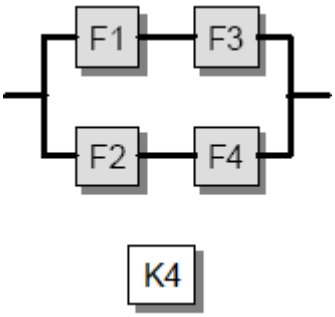
**備考**

- パレット積載および荷降しプロセス、搬送ステーション、バンド掛け機または上包み機へのアクセス箇所の安全防護対策付きの自動輸送物排出の実行例。輸送物搬入のためのアクセス箇所にも同様の原則が使用できる。
- EN 415-4 によると、下記を含む要求事項を満たしていれば、搬入または排出口を通る人のアクセスが検知されないことは、十分確実に防止されると想定し得る。
  - 必要な（アクセス箇所が開いた状態または空のパレットがそこにある状態での）取り付け高さを考慮した 2 本または 3 本の光ビームバリアの使用、または
  - 側面と 0.2m 未満の隙間がある積載されたパレットによってミュートされる光バリアの保護機能付き、および光ビームの遮断の直前にパレット積載物によって活性化するミューティング（大きなタイミング間隔や寸法的なギャップのない）付き

**故障確率計算**

ミューティングに採用されている接点が自動フォールト（故障）検出の対象ではないため、以下の計算では、ミューティングセンサ F1 から F4 の出力リレーに 0%の DC を想定する。これにより、単純な方法で実行できる定期的な手動点検が規定されている。

- $MTTF_d$：ミューティングセンサ F1 から F4 のそれぞれのセンサ部分に、100 年[E]の $MTTF_d$ を想定する。出力リレーF1 から F4 に 2,000,000 サイクル[S]の $B_{10d}$ 値を適用する。稼働日 300 日、稼働時間 16 時間、サイクル時間が 200 秒の場合、$n_{op}$ は 1 年に 86,400 サイクルとなり、これらの要素の $MTTF_d$ は 231 年となる。チャンネルの $MTTF_d$ は 35 年（「高」）となる。
- $DC_{avg}$：PLC の監視により、ミューティングセンサ F1 から F4 のセンサ部分の DC は 90%に達する。出力リレーの DC は、安全側に誤作動し 0%と推定される。その結果 $DC_{avg}$ 値は 63%（「低」）となる。
- 共通原因故障に対する適正な対策（65 点）：分離（15）、過電圧保護など（15）および環境条件（25 + 10）



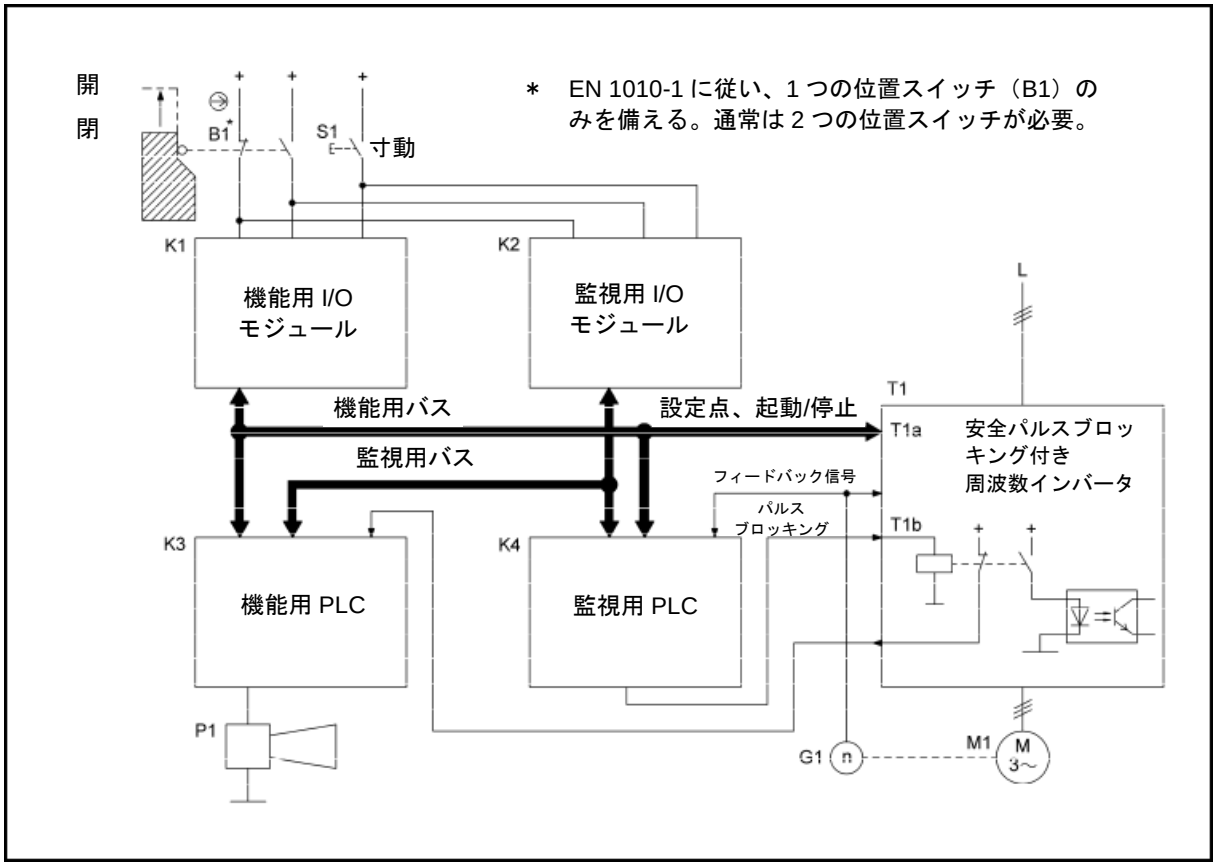

- 制御要素の組み合わせは、チャンネルごとの高い $MTTF_d$（35 年）と低い $DC_{avg}$（63%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $5.16 \times 10^{-7}$ となる。これは PL d に相当する。

**より詳細な参考文献**


- *Grigulewitsch, W.*: Speicherprogrammierbare Steuerung (SPS) zum zeitlich begrenzten, prozessabhängigen Aufheben einer Sicherheitsfunktion – Schaltungsbeispiel. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 231. 36th suppl. XII/99. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed. www.bgia-handbuchdigital.de/330231
- *Kreutzkampf, F.; Hertel, W.*: Zeitbegrenztes Aufheben von Sicherheitsfunktionen. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 214. 19th suppl. X/92. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin 1985 – loose-leaf ed. www.bgia-handbuchdigital.de/330214
- EN 415-4: Safety of packaging machines – Part 4: Palletisers and depalletisers (03.97) and amendment AC (12.02)
- EN 61496-1: Safety of machinery – Electro-sensitive protective equipment – Part 1: General requirements and tests (05.04)
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (draft standard IEC 44/501/CD:2005)
- EN 999: Safety of machinery – The positioning of protective equipment in respect of approach speeds of parts of the human body (10.98)

### 8.2.24　印刷機での安全制限速度付き寸動モード　－　カテゴリー3　－　PL d（例 24）

図 8.42：2 チャンネルマイクロプロセッサ制御付き印刷機の、安全制限速度付き寸動モード

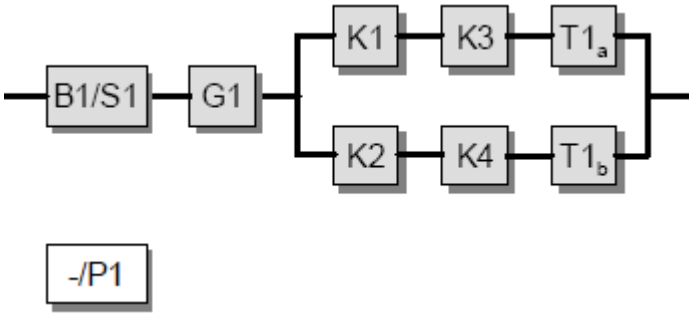



**安全機能**

- 保護装置によって起動する安全関連停止機能：安全ガードの開動作によりドライブが停止する。（SS1－安全停止 1）
- 安全制限速度（SLS）：安全ガードが開いている時に、制限速度でのみ機械動作が可能。
- 寸動モード：安全ガードが開いている時に、寸動ボタンを押している間だけ動作が可能。

**機能の説明**

- リモート I/O モジュール K1 は、人員安全機能 B1 付き位置スイッチおよび寸動ボタン S1 の状態を登録し、かつこの情報を機能用バス上に供給する。情報は機能用 PLC K3 によって評価され、機能用バスを通して周波数インバータ T1 が作動する（機能的作動 T1a）。

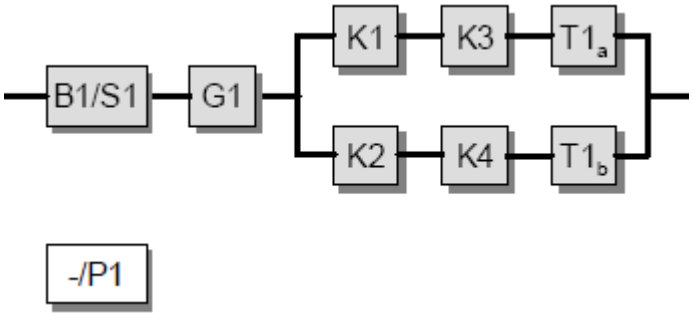



監視専用バスで通信する I/O モジュール K2 および監視用 PLC K4 は、K1 および K3 に冗長的に作用する。K4 は、T1 の安全パルスブロッキングにアドレスすることによって制御されていない停止（コーストダウン）を引き起こすことができる（安全シャットダウン　T1b）。

- B1 が開いた状態では、安全制限速度付き S1 を使用する寸動モードのみを許可する。
- EN 1010-1 によれば、単一の位置スイッチ B1 で十分である。S1 での大部分のフォールト（故障）は、P1 を含む音響起動警告および強制された動作により検出され制御される。すなわち S1 を初めて押すと音響警告（P1）が出力され、S1 を離して再度押した場合にのみ、遅延を伴って駆動が再起動する。
- K1 および K2 でのフォールト（故障）は、K4 での状態比較により検出される。K4 はまた、入力および出力情報を監視することで K3 を監視する。さらに、K3 でのフォールト（故障）は、プロセス中のフォールト（故障）によって部分的に明確になる。セルフテスト（例えば内部ウォッチドッグによるプログラムシーケンス監視）が K4 で行われる。さらに、K3 はパルスブロッキングの定期的なアドレス指定のために K4 を使用し、かつ T1 のパルスブロッキングリレーの機械的に連結した常時閉接点を通して、K4 からのフィードバックを監視する。
- sin/cos エンコーダ G1 とともに、周波数インバータ T1 は、フォールト（故障）（印刷エラー、紙の破れ）を生産プロセスにより検出する高度に同期的な閉ループ制御システムを形成する。監視や安全制限速度に対し、G1 はまた K4 にリードバックされ、sin/cos 情報（$\sin^2 + \cos^2 = 1$）の妥当性および T1 の設定点への準拠性を監視される。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- B1 の常時閉接点は、IEC60947-5-1　付属書 K を満たす。位置ずれおよび合理的に予測可能な誤用を防止するための対策を実施する（EN 1088　付属書 A1 参照）。位置スイッチの作動のために、保護装置の安定した配置を確保する。
- 起動時の警告や強制された動作にもかかわらず、寸動中に S1 がハングアップするかもしれない。そのため、追加要求事項として、非常停止装置をオペレータの手の届く範囲内に設置しなければならない。



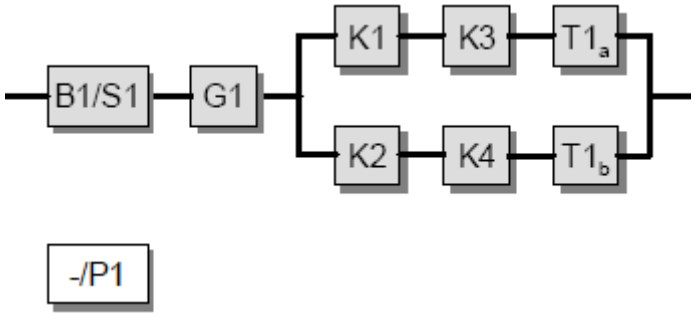

- EN ISO 13849-2 の表 D.4 に従った配線短絡に対するフォールト（故障）の排除のための条件を、S1 への接続線で守られなければならない。B1 への接続線でのフォールト（故障）は、K1 および K2 の常時閉および常時開接点の不一致監視により検出される。
- プログラマブル構成部品 K1 から K4 は、6.3 項の必須要求事項を満たす。
- G1 は冗長的な位置情報（例えば sin/cos エンコーダ）を提供し、かつ閉ループ制御回路に集積化される（整流の取得）。
- T1 は、成功したアドレス指定が機械的に連結した常時閉接点によりリードバックされる安全パルスブロッキング（T1b）を有する。
- 6.3.10 項の指示により、標準構成部品 G1 および T1 を採用する。
- 6.2.17 項の指示により、バスシステム（機能用バス、監視用バス）を採用する。

**備考**

- 例えば輪転印刷機の捕捉個所の安全防護対策の適用。オペレータが危険領域へ周期的に介入しない、すなわち 1 時間に 1 度未満の頻度での介入の場合は、EN 1010-1 ではガード位置の監視には位置スイッチ 1 つのみが必要とされる。カテゴリー3 のフォールト（故障）許容基準では、同様の機械制御システムには、通常 2 つの位置スイッチ（例えば常時閉接点を 1 つと常時開接点を 1 つ）の使用が必要となる。
- 安全制限速度が既に保証されていれば、寸動モードにはある一定の条件下で危険源を回避する可能性を想定し得る。

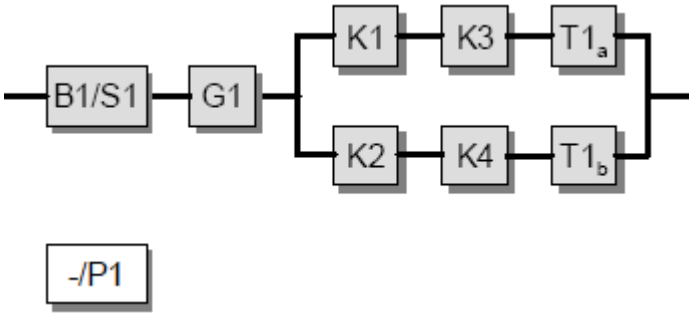
**故障確率計算**

- センサレベル B1、S1 および G1 は冗長的なロジックおよびアクチュエータレベルの外側にあり、そのため区別して考慮する。
- B1 の直接開電気接点に対し、フォールト（故障）を排除することが可能である。B1 の機械的部品には 20,000,000 サイクル[S]の $B_{10d}$ 値を想定する。1 週間に 10 回の運転で、$n_{op}$ は 1 年に 520 サイクル、$MTTF_d$ は 384,615 年となる。これは、1 時間あたり 2.97 x $10^{-10}$ の危険側故障の平均確率に数学的に相当する。




EN 1010-1 の特定局面を考慮するために、この値を、通常 1 チャンネルの $MTTF_d$ が 100 年で達する上限の代わりに、PL d の 1 時間あたり $1.00 \times 10^{-7}$ の最大マーカー値に下げる。

- S1 は 100,000 サイクル[M]の $B_{10d}$ 値を持つ。1 週間に 10 回の運転で、$n_{op}$ は 1 年に 520 サイクル、$MTTF_d$ は 1,923 年となる。強制された動作および起動警告により、少なくても 60%の DC を想定する（しかしながら繰り返しの寸動に続くハングアップは検出されない）。カテゴリー2 構造への取り込みにより、S1 は 1 時間あたり $5.28 \times 10^{-7}$ の危険側故障の平均確率に達する。
- sin/cos 信号の評価および閉ループ制御回路でのその使用（整流化）により、G1 はカテゴリー3 に従って集積化される。チャンネルごとの 30 年[E]の $MTTF_d$ およびプロセスでの妥当性テストおよびフォールト（故障）検出による 90%の DC で、危険側故障の平均確率は 1 時間あたり $2.65 \times 10^{-7}$ となる。
- $MTTF_d$ : K1 および K2 に 100 年[E]、K4 に 50 年[E]、かつ K3 に 30 年[E]を許容する。さらに、T1a に 30 年[E]、T1b に 1,000 年[E]を代入する。全体で、チャンネルごとの対称化 $MTTF_d$ 値は 24 年（「中」）となる。
- $DC_{avg}$ : K1 および K2 の 99%の DC は、K4 に供給される状態情報の直接比較により生じる。K3 の 99%の DC は、K4 での全ての安全関連情報の並列処理、および中間結果と K3 によって形成される出力信号との K4 での直接比較に基づく。K4 で行われるセルフテストと、K3 によるパルスブロッキングのリードバックによる部分監視によって、K4 の DC は 60%という結果になる。T1a の 99%の DC は、軸位置の設定点と実際値間の K4 での比較に基づく。T1b については、パルスブロッキングのアドレス指定のリードバックによる内部オプトカプラのフォールト（故障）の排除の想定によって、DC は 60%という結果になる。そのため、平均化により $DC_{avg}$ は 91%（「中」）となる。
- 共通原因故障に対する適正な対策（70 点）: 分離（15）、FMEA（5）、過電圧保護など（15）および環境条件（25 + 10）
- K1 から K4 および T1 の組み合わせは、チャンネルごとの中間の $MTTF_d$（24 年）と中間の $DC_{avg}$（91%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $3.33 \times 10^{-7}$ となる。安全関連停止機能および安全制限速度に対しては B1 および G1 の値をこの値に加算しなければならない。




そのため、1 時間あたり（1.00 + 2.65 + 3.33） x $10^{-7}$ = 1 時間あたり 6.98 x $10^{-7}$ により、PL d という結果になる。S1 および G1 の値を寸動モードに加算しなければならない。そのため、1 時間あたり（5.28 + 2.65 + 3.33） x $10^{-7}$ = 1 時間あたり 1.13 x $10^{-6}$ という値になる。これは PL c に相当する。

**より詳細な参考文献**


- EN 1010-1: Safety of machinery – Safety requirements for the design and construction of printing and paper converting machines – Part 1: Common requirements (12.04)
- Safety in Construction and Design of Printing and Paper Converting Machines. Electrical Equipment and Control Systems. Ed.: Berufsgenossenschaft Druck und Papierverarbeitung, Wiesbaden, 2004. www.bgdp.de/pages/service/download/medien/220-2e.pdf
- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin, 2003. www.dguv.de/bgia, Webcode d6428

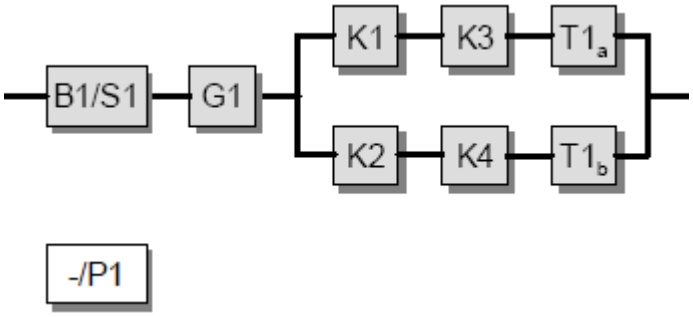
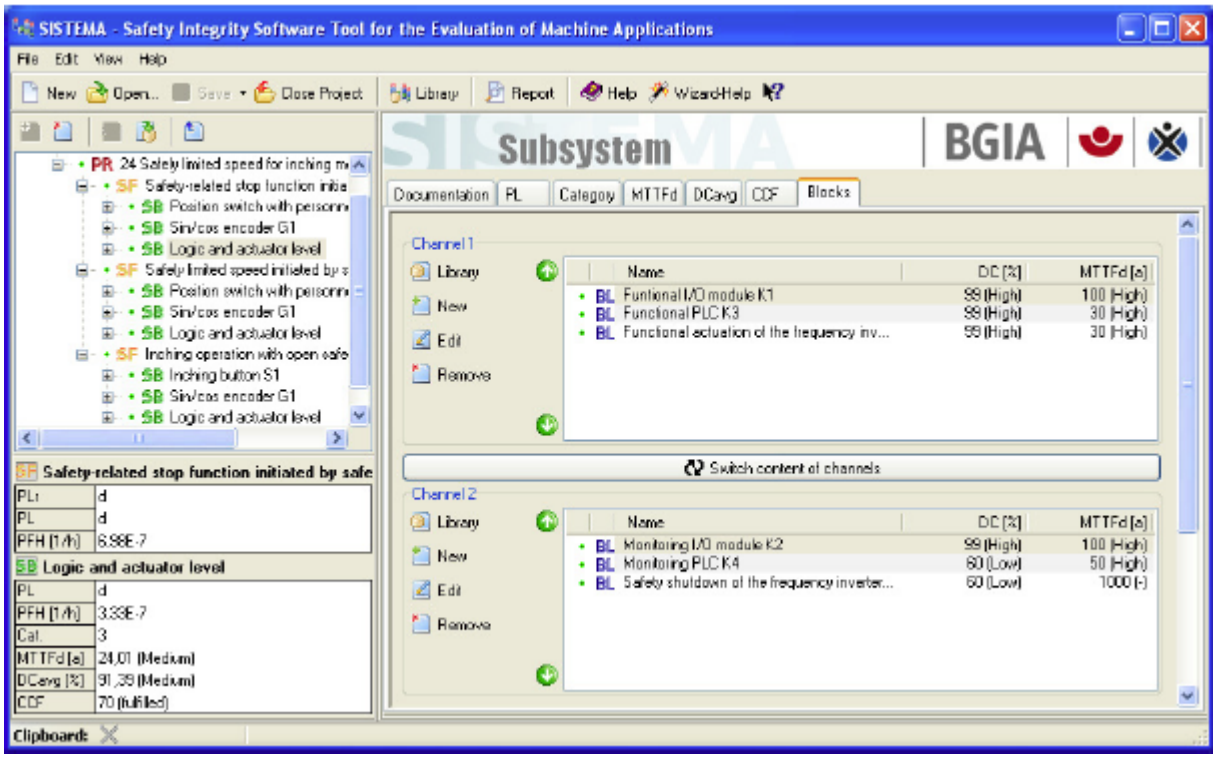
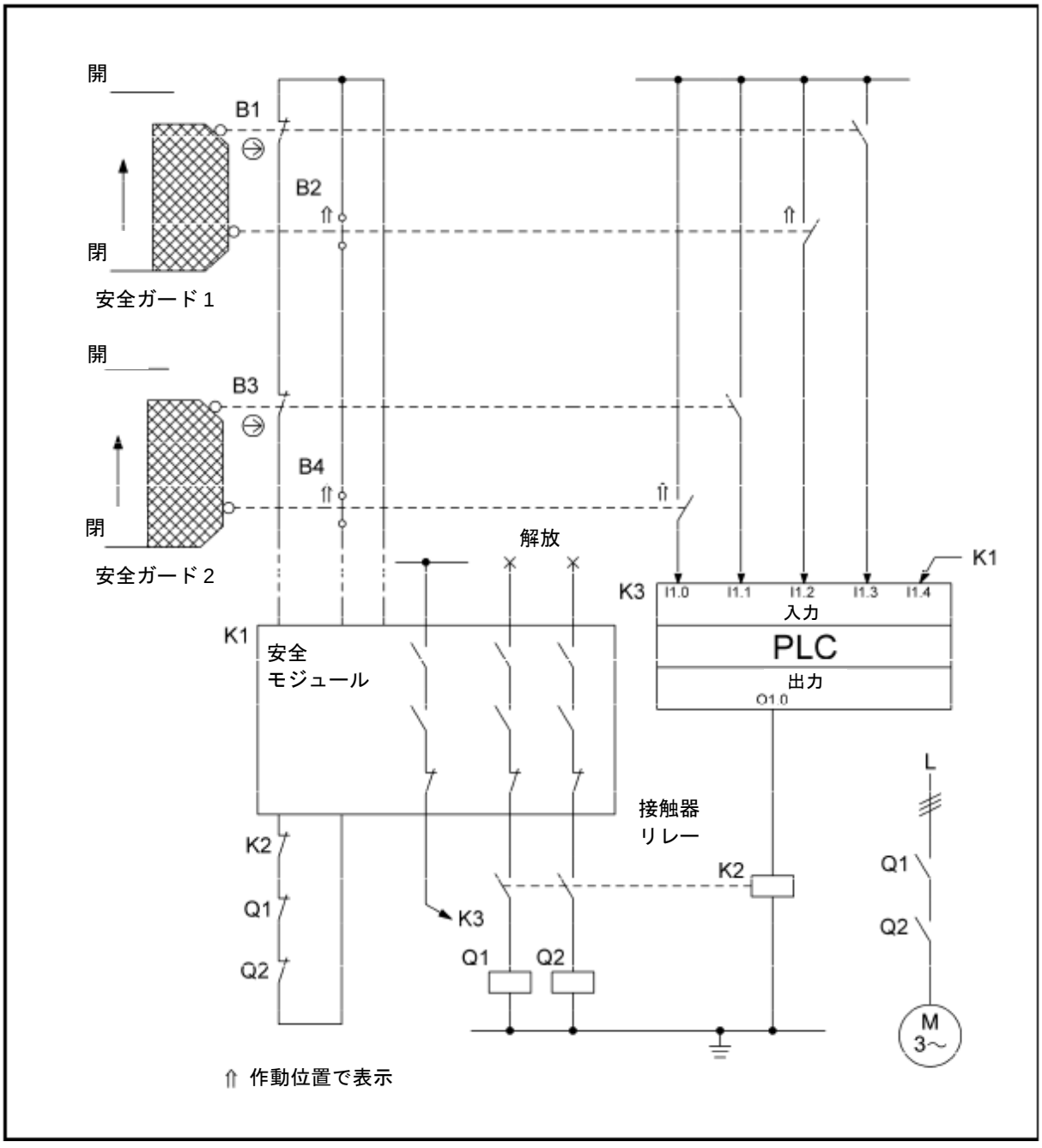



図 8.43：SISTEMA による PL の決定



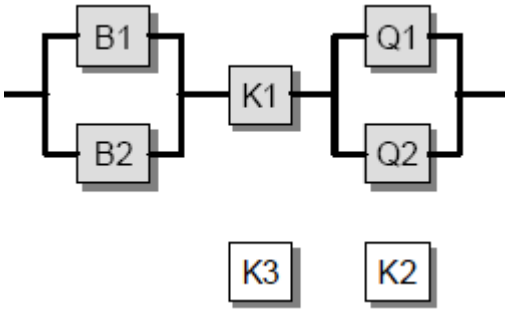
### 8.2.28　可動式ガードの位置監視　－　カテゴリー4　－　PL e（例 28）

図 8.49：危険動作防止のための可動式ガードの位置監視




**安全機能**

- 保護装置によって起動する安全関連停止機能：可動式ガード（安全ガード）が開くことで安全機能 STO（安全トルクオフ）が起動する。

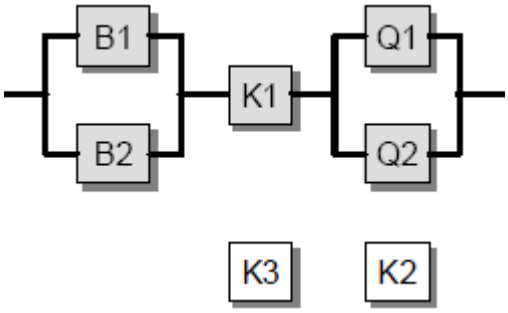



**機能の説明**

- 危険区域は、2 つの可動式ガード（安全ガード）によって安全防護している。2 つの安全ガードの開動作は、常時閉接点/常時開接点の組み合わせからなる 2 つの位置スイッチ B1/B2 および B3/B4 が検知し、中央安全モジュール K1 が評価する。K1 は、ドロップアウトにより危険な動作や状態を遮断または防止する 2 つの接触器 Q1 および Q2 を作動させる。
- フォールト（故障）検出のために、全ての位置スイッチの状態を第 2 接点が機能制御を主目的とする標準 PLC K3 に読み込む。フォールト（故障）の場合、K3 は、K1 と独立して接触器リレーK2 により接触器 Q1 および Q2 を遮断させることができる。K2、Q1 および Q2 のフォールト（故障）は、安全モジュール K1 で検出される。少数のフォールト（故障）は検出されない（例えば B2 および B4 の接点の開動作失敗）。
- 構成部品の故障の場合に安全機能が維持される。大多数の構成部品の故障は検出され、操作禁止につながる。検出されないフォールト（故障）が重なっても安全機能のロスにはならない。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 位置スイッチの作動のために保護装置の安定した配置を確保する。
- B1 および B3 は IEC 60947-5-1　付属書 K による直接開接点付き位置スイッチである。
- 位置スイッチへの電源配線は、別々に配線または保護されている。
- 起動および作動メカニズムでのフォールト（故障）は、作動の原則（常時閉および常時開接点の組み合わせ）に違いのある 2 つの位置スイッチによって検出される。
- いくつかの保護装置がカスケード接続されることがある。
- 安全モジュール K1 は、カテゴリー4 および PL e の全ての要求事項を満たす。
- 接触器 K2、Q1 および Q2 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。




・　PLC K1 は 6.3 項に記載の必須要求事項を満たす。

**故障確率計算**

・　回路配置は、安全関連ブロック図に示すとおり 3 つのサブシステムに分けられる。安全モジュール K1 の故障確率は計算の最後に追加される（1 時間あたり 2.31 x $10^{-9}$[M]、PL e に適する）。残りのサブシステムについては、故障確率を下記の通り計算する。各安全ガードは専用の安全機能の一部を形成するため、計算はここでは保護装置 1 を代理として示す。

・　$MTTF_d$：直接開接点付き位置スイッチ B1 の電気接点に対し、フォールト（故障）を排除することが可能である。位置スイッチ B2 の電気的常時開接点については、$B_{10d}$ 値は 1,000,000 開閉操作[M]である。1,000,000 サイクルの $B_{10d}$ 値[M]が、B1 および B2 の機械的部品について提示されている。稼働日 365 日、稼働時間 16 時間、サイクル時間が 1 時間の場合、これらの構成部品の $\boldsymbol{n}_{op}$ は 1 年に 5,840 サイクルで、B1 の $MTTF_d$ は 1,712 年となり、B2 の $MTTF_d$ は 856 年となる。接触器 Q1 および Q2 では、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,000,000 回の開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。上記 $\boldsymbol{n}_{op}$ の想定値から、Q1 および Q2 のチャンネルごとの $MTTF_d$ は 3,424 年となる。全体で、2 つのサブシステムの対称化 $MTTF_d$ 値は、チャンネルあたり 100 年（「高」）となる。

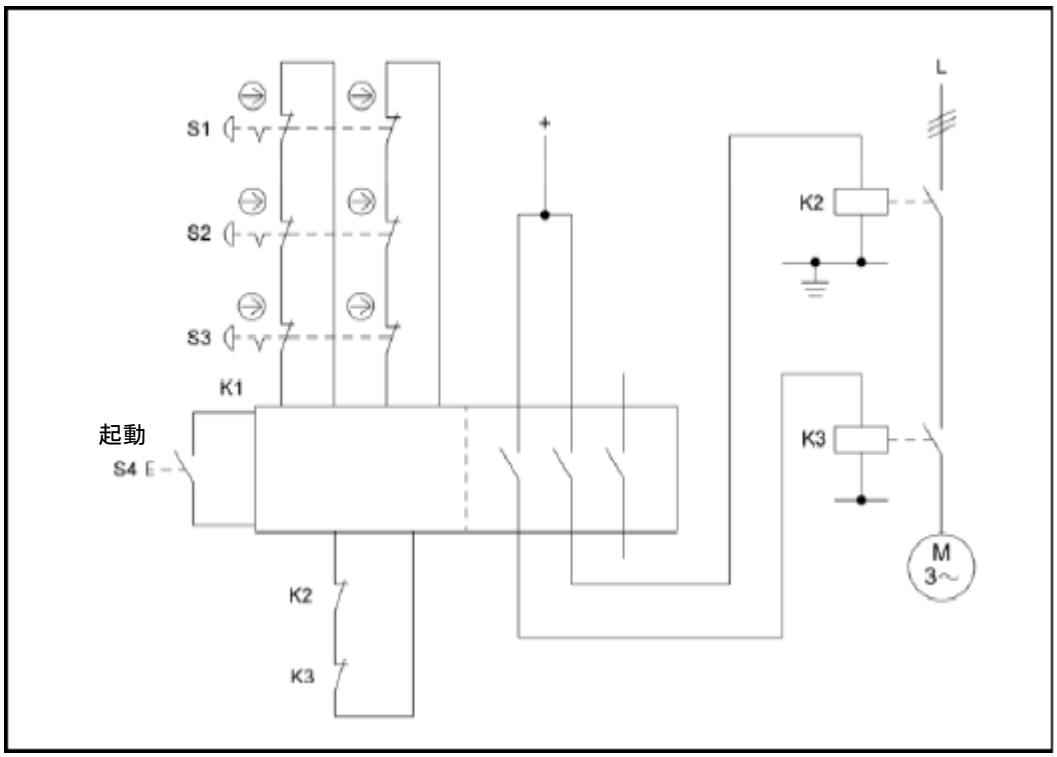
・　$DC_{avg}$：B1 および B2 の 99%の DC は、PLC K3 での常時閉/常時開接点の組み合わせの妥当性監視に基づく。接触器 Q1 および Q2 の 99%の DC は、K1 の各通電時の監視から算出される。堤示された DC 値は、関連するサブシステムの $DC_{avg}$ に相当する。

・　サブシステム B1/B2 および Q1/Q2 における共通原因故障に対する適正な対策（70 点）: 分離（15）、十分に実証済みの構成部品（5）、過電圧保護など（15）および環境条件（25 + 10）

・　サブシステム B1/B2 および Q1/Q2 は、どちらも高い $MTTF_d$（100 年）と高い $DC_{avg}$（99%）のカテゴリー4 に相当する。これにより、ケースごとの危険側故障の平均確率は 1 時間あたり 2.47 x $10^{-8}$ となる。サブシステム K1 の加算により、危険側故障の平均確率は 1 時間あたり 5.16 x $10^{-8}$ となる。これは PL e に相当する。

### 8.2.29　安全モジュールによる非常停止装置のカスケード接続　－　カテゴリー3　－　PL e（例 29）

図 8.50：安全モジュールによる非常停止装置のカスケード接続（非常停止機能、STO）

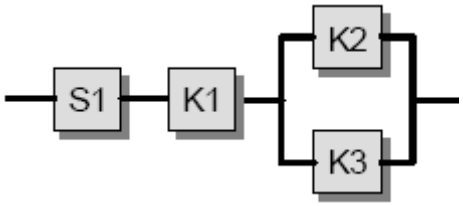



**安全機能**

- 非常停止機能、非常停止装置の作動による STO

**機能の説明**

- 非常停止装置の作動により、危険な動作や状態が遮断または防止される。5.3.2 項の例 3 に示すように、各非常停止装置は、それ自体の安全機能を始動させる。以下では S1 が全ての装置の典型であると考える。S1 は、2 つの冗長な接触器リレーK2 および K3 を作動させる安全モジュール K1 によって評価される。
- 非常停止装置からの信号は、フォールト（故障）検出用安全モジュール K1 に冗長的に読み込まれる。K1 はまた内部試験方策を有する。接触器リレーK2 および K3 も、機械的に連結したリードバック接点によって K1 で監視される。K2 および K3 は、1 ヶ月に約 2 度の各起動コマンド時にスイッチ S4 で操作される。連続した 2 度の作動の間に 2 つ以上のフォールト（故障）が重なると、安全機能のロスにつながる可能性がある。
- 2 つ以上の非常停止装置が同時に押されることは想定しない。




**設計特性**

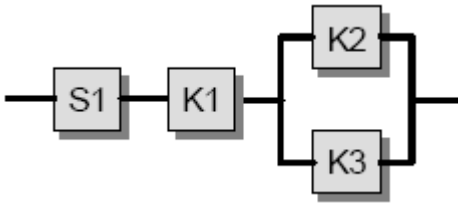
- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 非常停止装置 S1、S2 および S3 は IEC 60947-5-1　付属書 K による直接開接点付き開閉装置である。
- 開閉装置への電源配線は、別々に配線または保護されている。
- 安全モジュール K1 は、カテゴリー4 および PL e の全ての要求事項を満たす。
- K2 および K3 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。

**備考**

- 非常停止機能は、EN ISO 12100-2:2004 による補完保護対策である。

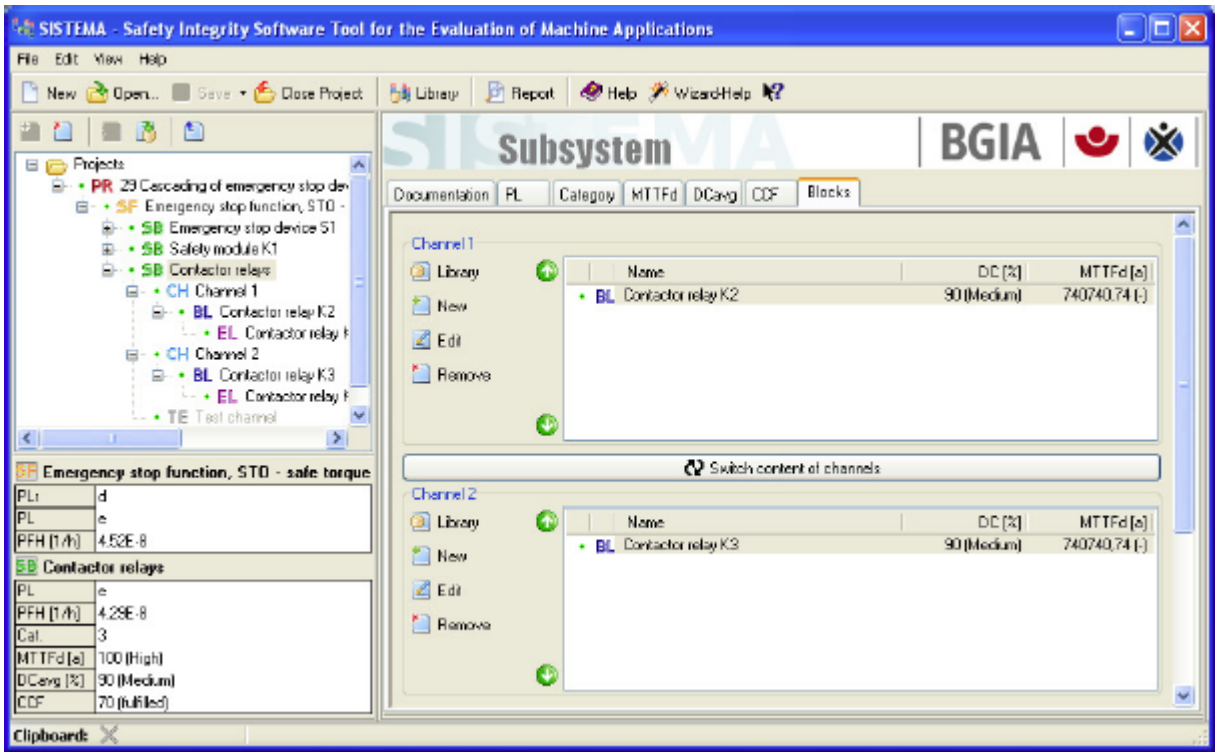
**故障確率計算**

- S1、S2 および S3 は EN ISO 13850 の標準非常停止装置である。本レポートの表 D.2 に記載の操作回数を超えなければ、フォールト（故障）の排除が直接開接点および機械的要素に適用される。
- 最終安全モジュール K1 の故障確率は計算の最後に追加される（1 時間あたり 2.31 x $10^{-9}$[M]、PL e に適する）。サブシステム K2/K3 については、故障確率を下記の通り計算する。
- $MTTF_d$：接触器リレーK2 および K3 については、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,000,000 回の開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。1 年に非常停止機能への 3 回のデマンドおよび 24 回の起動コマンドがあると、$n_{op}$ は 1 年に 27 サイクルで、$MTTF_d$ は 740,740 年となる。これはまたチャンネルの対称化 $MTTF_d$ であり、上限の 100 年（「高」）に達する。
- $DC_{avg}$ : K2 および K3 の 99%の DC は、安全モジュール K1 による試験に基づく。これはまた $DC_{avg}$（「中」）である。
- 共通原因故障に対する適正な対策（70 点）: 分離（15）、十分に実証済みの構成部品（5）、過電圧保護など（15）および環境条件（25 + 10）



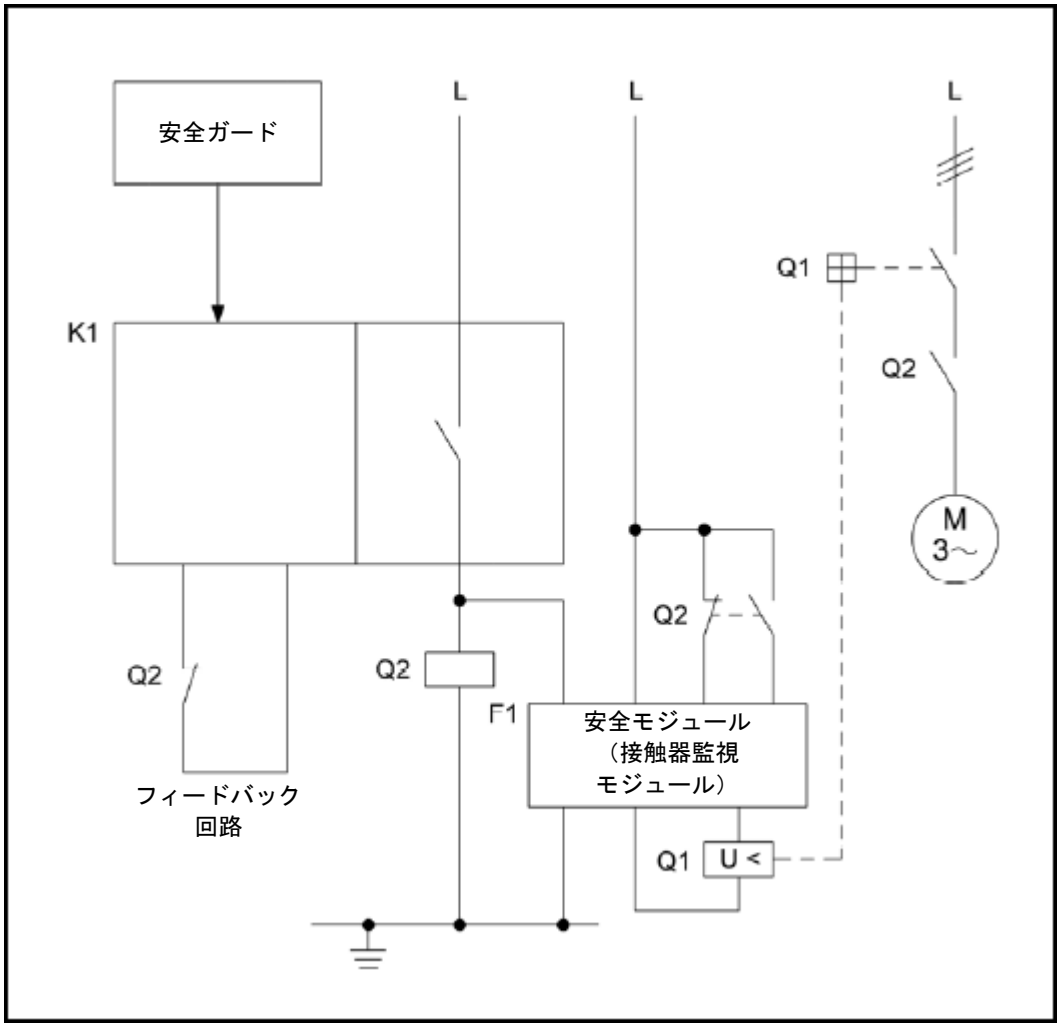

- サブシステム K2/K3 は、高い $MTTF_d$（100 年）と中間の $DC_{avg}$（90%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $4.29 \times 10^{-8}$ となる。サブシステム K1 の加算により、危険側故障の平均確率は 1 時間あたり $4.52 \times 10^{-8}$ となる。これは PL e に相当し、そのため、d の $PL_r$ を超える。

図 8.51：SISTEMA による PL の決定



### 8.2.30　接触器監視モジュール　－　カテゴリー3　－　PL e（例 30）

図 8.52：安全モジュールおよび接触器監視モジュールによる STO（安全トルクオフ）の起動

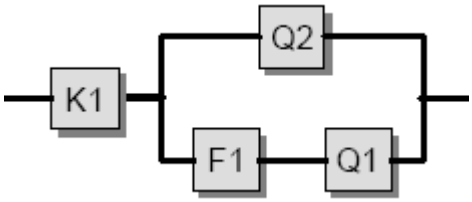



**安全機能**

- 保護装置によって起動する安全関連停止機能：可動式ガードが開くことで安全機能 STO（安全トルクオフ）が起動する。

**機能の説明**

- 危険区域は、開動作が安全モジュール K1 によって検知される保護装置によって安全防護している。安全モジュールは、接触器 Q2 と、接触器監視モジュール F1 および無電圧ブレーカ Q1 の組み合わせを作動させる。Q2 のドロップアウトが、危険な動作を遮断し危険な状態を防止する。接触器監視モジュール F1 は、接触器 Q2 の主接点溶着を監視する機能を有する。Q2 がドロップアウトに失敗すると、F1 が上流のサーキットブレーカまたは Q1 の無電圧ブレーカを通してモータ・スタータ Q1 をトリップさせる。




その後、サーキットブレーカまたはモータ・スタータがモータのスイッチを切る。

- 安全機能は構成部品の故障の場合に保持される。
- 2 度の連続した作動の間にフォールト（故障）が重なると、安全機能のロスにつながる可能性がある。

**設計特性**

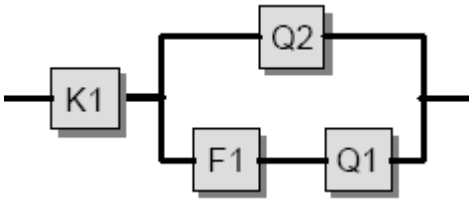
- サーキットブレーカ Q1 は、手動で実行される試験機能により定期的に点検する。試験の間隔は Q1 の $MTTF_d$ の 100 分の 1 を超えないことが望ましい; 試験は例えば機械のメンテナンス中に行うことができる。接触器 Q2 は、接触器監視モジュールにより連続的に試験されている。カテゴリー2 では可能な、試験間の安全機能のロスは起こり得ない。そのため、単独フォールト（故障）の許容は確保され、カテゴリー3 の要求事項を満たす。
- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 簡略化の理由から、保護装置の詳細はプレゼンテーションから省略している。
- 保護装置は、カテゴリー3 または 4 および PL e の全ての要求事項を満たす安全モジュール K1 に作用する。
- 接触器 Q2 は、IEC 60947-4-1　付属書 F によるミラー接点を有し、接触器のフォールト（故障）検出用安全モジュール K1 のフィードバックに集積化される。
- Q2（ミラー接点付き）および接触器監視モジュール F1 の内部リレーに対するフォールト（故障）の考え方は、機械的に連結した接点と同じである。

**備考**

- Q1 のドロップアウトに関しては、接触器監視モジュール F1 によって生じる応答時間を考慮に入れなければならない。

**故障確率計算**

- 安全機能により、2 つのサブシステムに分けることができる。保護装置および安全モジュール K1 から成るサブシステムについては、この例では考慮しない。
- $MTTF_d$：接触器監視モジュール F1 については、1 年に 350,400 サイクルの最大 $n_{op}$ [M]で $MTTF_d$ は 125 年である。誘導負荷（AC 3）下において、Q1 の $B_{10d}$ 値は 10,000 開閉サイクルで、Q2 の $B_{10d}$ 値は 1,300,000 開閉サイクルである。

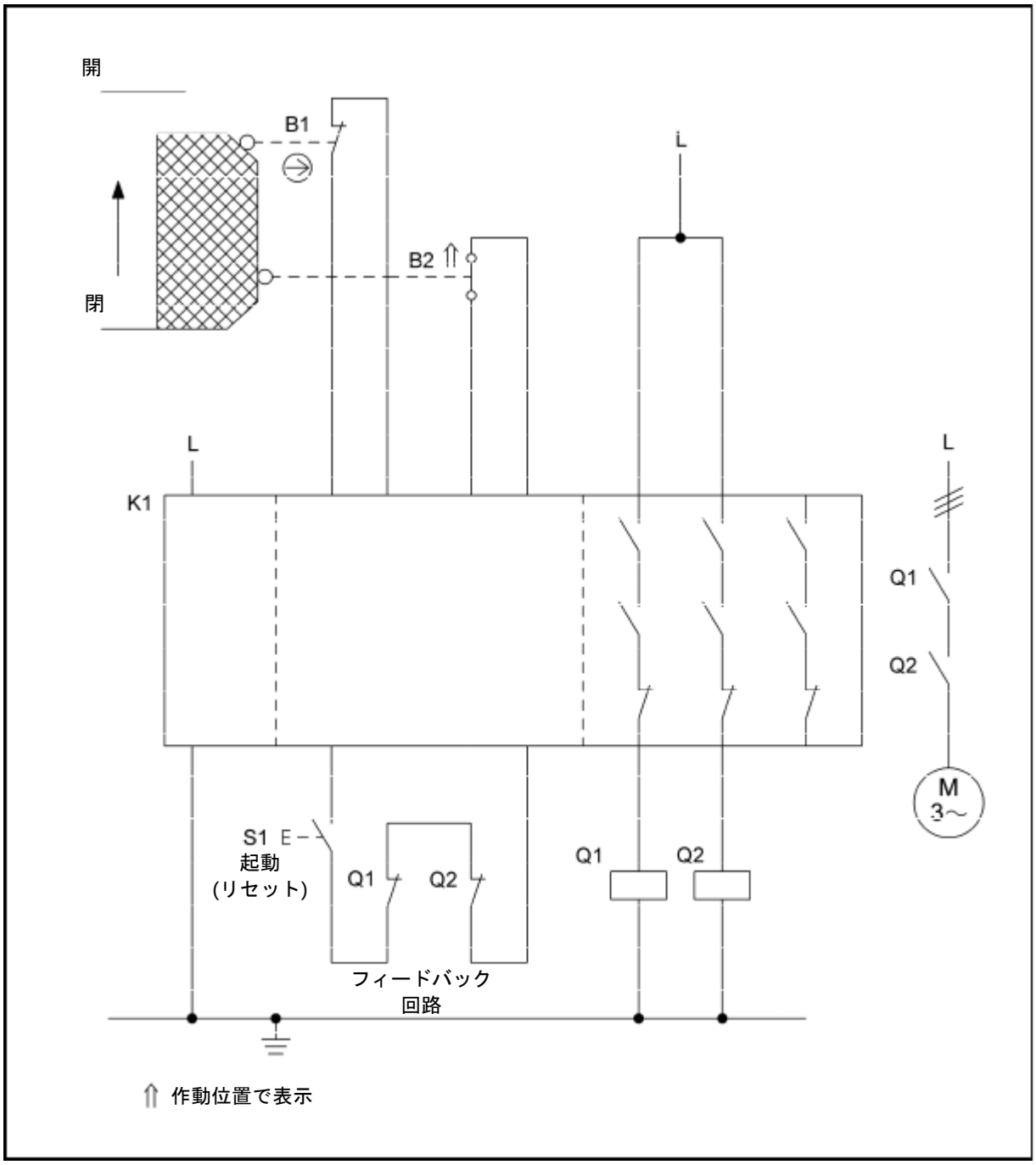



稼働日 365 日中に毎日 1 度作動すると仮定すると、Q1 の $n_{op}$ は 1 年に 365 サイクルで、$MTTF_d$ は 274 年となる。稼働日 365 日、稼働時間 16 時間、サイクル時間が 1 分の場合、Q2 の $n_{op}$ は 1 年に 350,400 サイクルで、$MTTF_d$ は 37 年となる。これにより、F1 および Q1 から成るチャンネルについては、$MTTF_d$ は 85 年となる。全体で、対称化 $MTTF_d$ 値は、チャンネルあたり 64 年（「高」）となる。

- $DC_{avg}$：Q2 の 99%の DC は、接触器監視モジュール F1 による試験に基づく。F1 の 99%の DC は、接触器監視モジュール内のフォールト（故障）検出方策により得られる。サーキットブレーカは、実装されるべき手動試験機能により試験される；これにより DC は 90%になる。F1 に 99%の DC を代入する。そのため、平均化により $DC_{avg}$ は 98%（「中」）となる。
- 共通原因故障に対する適正な対策（65 点）：分離（15）、過電圧保護など（15）および環境条件（25 + 10）
- Q1、Q2 および F1 から成るサブシステムは、高い $MTTF_d$（64 年）と中間の $DC_{avg}$（98%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $4.45 \times 10^{-8}$ となる。これは PL e に相当する。保護装置および安全モジュール K1 から成るサブシステムの加算により、PL はある一定の状況下で低くなる可能性がある。
- 上記のとおり、安全側への誤作動を考慮すると、摩耗要素 Q2 の $T_{10d}$ 値は、規定通り交換される場合は 3.7 年となる。

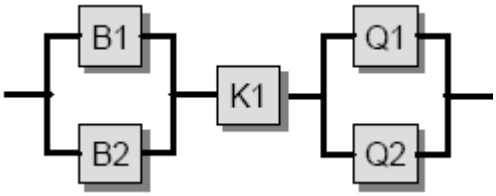
### 8.2.34　可動式ガードの位置監視　－　カテゴリー4　－　PL e（例 34）

図 8.58：安全モジュールによる可動式ガードの位置監視




**安全機能**

- 保護装置によって起動する安全関連停止機能：可動式ガード（安全ガード）が開くことで安全機能 STO（安全トルクオフ）が起動する。




**機能の説明**

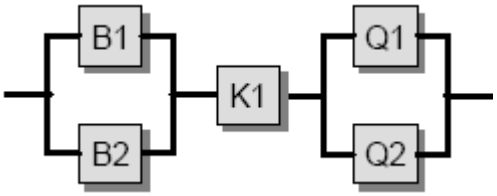
- 危険区域は、可動式ガード（安全ガード）によって安全防護している。安全ガードの開動作は、常時閉接点/常時開接点の組み合わせを採用した 2 つの位置スイッチ B1/B2 が検知し、中央安全モジュール K1 が評価する。K1 は、ドロップアウトにより危険な動作や状態を遮断または防止する 2 つの接触器 Q1 および Q2 を作動させる。
- 位置スイッチは、フォールト（故障）検出のために K1 で妥当性を監視される。Q1 および Q2 でのフォールト（故障）は、K1 での起動試験によって検出される。起動コマンドは、Q1 および Q2 が前もってドロップアウトしている場合にのみ成功する。保護装置の開閉による起動試験は必要ない。
- 安全機能は、構成部品の故障の場合に損傷を受けないまま保持される。フォールト（故障）は運転中もしくは保護装置の作動（開閉）時に Q1 及び Q2 のドロップアウトと運転禁止によって検出される。
- 連続した 2 度の作動の間に 2 つ以上のフォールト（故障）が重なると、安全機能のロスにつながる可能性がある。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 位置スイッチの作動のために保護装置の安定した配置を確保する。
- スイッチ B1 は IEC 60947-5-1　付属書 K による直接開接点付き位置スイッチである。
- 位置スイッチ B1 および B2 への電源配線は、別々に配線または保護されている。
- 安全モジュール K1 は、カテゴリー4 および PL e の全ての要求事項を満たす。
- 接触器 Q1 および Q2 は、IEC 60947-5-1　付属書 L による機械的に連結した接点要素を有する。

**備考**

- スイッチのフォールト（故障）が検出できないため、異なる保護装置用の複数の機械的位置スイッチが直列に接続されていない（すなわちカスケード接続でない）場合にのみ、カテゴリー4 が守られる。

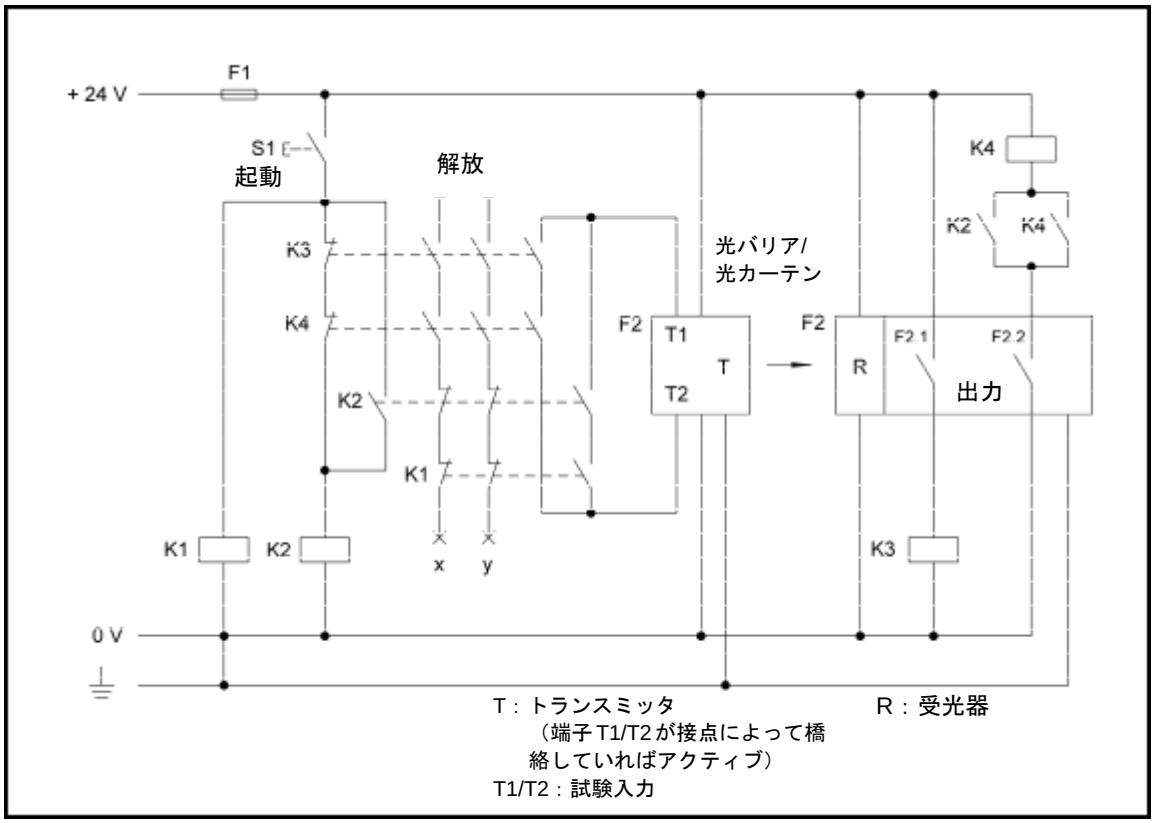



**故障確率計算**

- 回路配置は、安全関連ブロック図に示すとおり 3 つのサブシステムに分けられる。標準安全モジュール K1 の故障確率は計算の最後に追加される（1 時間あたり 2.31 x $10^{-9}$[M]、PL e に適する）。残りのサブシステムについては、故障確率を下記の通り計算する。
- $MTTF_d$：直接開動作付き位置スイッチ B1 の電気接点に対し、フォールト（故障）を排除することが可能である。位置スイッチ B2 の電気的常時開接点については、$B_{10d}$ 値は 1,000,000 開閉操作[M]である。1,000,000 サイクルの $B_{10d}$ 値[M]が、B1 および B2 の機械的部品について提示されている。稼働日 365 日、稼働時間 16 時間、サイクル時間が 1 時間の場合、これらの構成部品の $n_{op}$ は 1 年に 5,840 サイクルで、B1 の $MTTF_d$ は 1,712 年となり、B2 の $MTTF_d$ は 856 年となる。接触器 Q1 および Q2 では、誘導負荷（AC 3）下において、$B_{10}$ 値は 1,000,000 回の開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、$B_{10d}$ 値は $B_{10}$ 値の 2 倍になる。上記 $n_{op}$ の想定値から、Q1 および Q2 のチャンネルごとの $MTTF_d$ は 3,424 年となる。全体で、2 つのサブシステムの対称化 $MTTF_d$ 値は、チャンネルあたり 100 年（「高」）となる。
- $DC_{avg}$ : B1 および B2 の 99%の DC は、K1 での常時閉/常時開接点の組み合わせの妥当性監視に基づく。接触器 Q1 および Q2 の 99%の DC は、起動中の K1 による定期的な監視から算出される。堤示された DC 値は、各サブシステムの $DC_{avg}$ に相当する。
- サブシステム B1/B2 および Q1/Q2 における共通原因故障に対する適正な対策（70 点）: 分離（15）、十分に実証済みの構成部品（5）、過電圧保護など（15）および環境条件（25 + 10）
- サブシステム B1/B2 および Q1/Q2 は、どちらも高い $MTTF_d$（100 年）と高い $DC_{avg}$（99%）のカテゴリー4 に相当する。これにより、危険側故障の平均確率は 1 時間あたり 2.47 x $10^{-8}$ となる。サブシステム K1 の加算により、危険側故障の平均確率は 1 時間あたり 5.16 x $10^{-8}$ となる。これは PL e に相当する。

### 8.2.36　光バリアからの信号処理　－　カテゴリー4　－　PL e（例 36）

図 8.60：光バリアまたは光カーテンの例に関する機械制御システムへの安全関連信号の電気機械入力

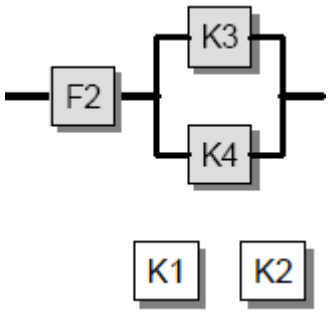



**安全機能**

- 保護装置によって起動する安全関連停止機能：危険領域への進入または危険区域でのオペレータの介入に応じた危険動作の停止の維持、および起動および再起動インターロック。

**機能の説明**

- 危険領域への進入または危険区域でのオペレータの介入は、光バリア F2 によって検知する。光バリア（常時開接点 F2.1 および F2.2）からの安全関連出力信号は、コイルが電源にオフセット配置で接続されている接触器リレーK3 および K4 を遮断する。その後 K3 および K4 はイネーブル信号 x および y をブロックする。
- 光バリアトランスミッタの活性化のためには、起動ボタン S1 の作動により、接触器リレー K1 および K2 のピックアップによって、まず試験入力 T1 および T2 を接続する。接触器リレーK3/K4 がドロップアウトしている時にのみ、K2 のピックアップとラッチインが可能である。光経路が完全になれば、K3 および K4 がピックアップする。K2 の常時開接点によってのみ、K4 はピックアップおよびラッチインする。

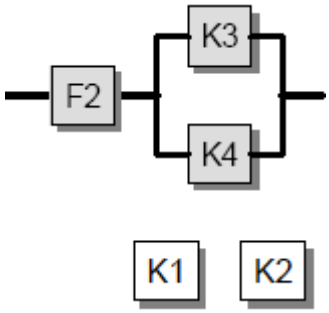



K3 および K4 がピックアップし、かつ起動ボタンが押されたままの状態で、光バリアトランスミッタは活性化しラッチする；そのため、起動ボタンを放すことができ、K1 および K2 が一旦ドロップアウトすると、イネーブル経路 x および y もまた閉じる。光ビームの遮断後、または停電およびそれに続く電圧の復旧の場合は、起動ボタンを再度押した後に K3 および K4 が再度ピックアップするまで、起動/再起動インターロックの機能がイネーブル信号の有効になるのを防ぐ。

- K3 および K4 のそれぞれ 1 つの常時開接点は、どちらも 2 つのイネーブル経路および光バリアトランスミッタの活性化のための入力回路（試験入力 T1/T2）に集積化される。試験入力の接続によって、例えば規定された短時間の光ビームの消去による、装置内での内部起動試験を形成する。受光器側では、この試験は短時間に論理的に有効と評価される。起動試験に合格すれば、光バリア出力は有効になる。反対に、停止またはフォールト（故障）の場合、または光ビームが遮断された場合には、それらはブロックされる。
- 組み合わさると安全機能のロスにつながる可能性のある回路内の他の構成部品（接触器リレー、光バリアの出力接点、起動ボタン）でのフォールト（故障）は、光ビームの遮断後の起動/再起動試験中に検出され、再度のイネーブルを防ぐ。

**設計特性**

- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 接触器リレーK1 から K4 は、IEC 60947-5-1　付属書 L による機械的に連結した接点要素を有する。接触器リレーK3 および K4 のリレー操作電圧は、ケーブルでの短絡（直列接続により、接触器のコイル間で電圧が分割される）の場合に、たとえ他の故障と組み合わさったとしても K3 および K4 の同時ピックアップが危険を及ぼさないよう、電源の電圧の半分よりも大きくなくてはならない。
- 光バリア F2 からの出力信号は、受光器の電気室から機械制御システムの電気室まで、電源配線と共にケーブル内を経由する。閉回路電流原則および接地制御回路内のオフセットコイル（K3、K4）の原則の適用により、全ての回路開放、接地故障、および回路間の短絡は、光バリアが活性化状態になると（とりわけ、ヒューズ F1 のトリップによって）直ちに検出される。




単一出力を橋絡させる短絡は、遅くても起動ボタンを後で作動させた際の光バリアの次の遮断で検出される。そのため、単一ケーブル内での出力信号の共通のルーティングが許容される。

- 光バリアは、EN 61496-1 および IEC 61496-2 のタイプ 4、および PL e の要求事項を満たす。

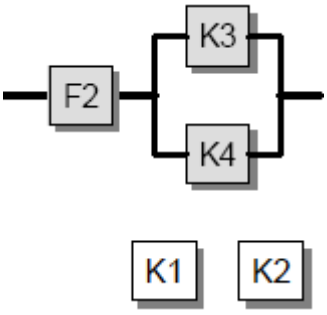
**備考**

- 光バリアがごくまれに開閉する用途に回路を採用する場合は、フォールト（故障）（2 つの別々の検出されないフォールト（故障））が重なった結果として安全機能が失われる可能性を考慮しなければならない。そのようなロスは、定期的な試験によって対応し得る。
- 光バリアの最大開閉頻度に関するメーカの情報を守らなければならない。

**故障確率計算**

安全関連ブロック図にも示されている安全関連停止機能の故障確率を計算する。制御システムによってイネーブル経路 x および y の接点がさらに処理される場合は、関連する追加の制御構成部品、例えば接触器を、故障確率計算に考慮しなければならない。

- 光バリア F2 は、標準安全構成部品である。その故障確率は 1 時間あたり $3.0 \times 10^{-8}$[M]であり、計算の最後に追加される。
- $MTTF_d$：未知の負荷により、K3 および K4 の $B_{10d}$ 値は 400,000 サイクル[S]である。稼働日 220 日、稼働時間 8 時間、サイクル時間が 120 秒の場合、$n_{op}$ は 1 年に 52,800 回の開閉操作となり、$MTTF_d$ は 75 年となる。これはまたチャンネルごとの $MTTF_d$（「高」）である。
- $DC_{avg}$：K3 から K4 の 99%の DC は、K2 の作動回路への機械的に連結した常時閉接点の使用から算出される。これはまた $DC_{avg}$（「高」）に相当する。
- 共通原因故障に対する適正な対策（75 点）：分離（15）、十分に実証済みの構成部品（5）、FMEA（5）、過電圧保護など（15）および環境条件（25 + 10）
- サブシステム K3/K4 は、チャンネルごとの高い $MTTF_d$（75 年）と高い $DC_{avg}$（99%）のカテゴリー4 に相当する。これにより、危険側故障の平均確率は 1 時間あたり $3.37 \times 10^{-8}$ となる。




全故障確率は、F2 の危険側故障の確率（1 時間あたり 3.0 x $10^{-8}$）を加算して決定し、それは 1 時間あたり 6.37 x $10^{-8}$ に等しい。これは PL e に相当する。下流動力構成部品の故障確率を、安全機能を完成させるために加算しなければならない可能性がある。

- 摩耗要素 K3 および K4 は、約 7 年（$T_{10d}$）ごとに交換することが望ましい。

**より詳細な参考文献**

- EN 60204-1: Safety of machinery – Electrical equipment of machines –
  Part 1: General requirements (IEC 60204-1:2005, modified) (06.06).
  Section 9.4.3: “Protection against maloperation due to earth faults, voltage interruptions and loss of circuit continuity”

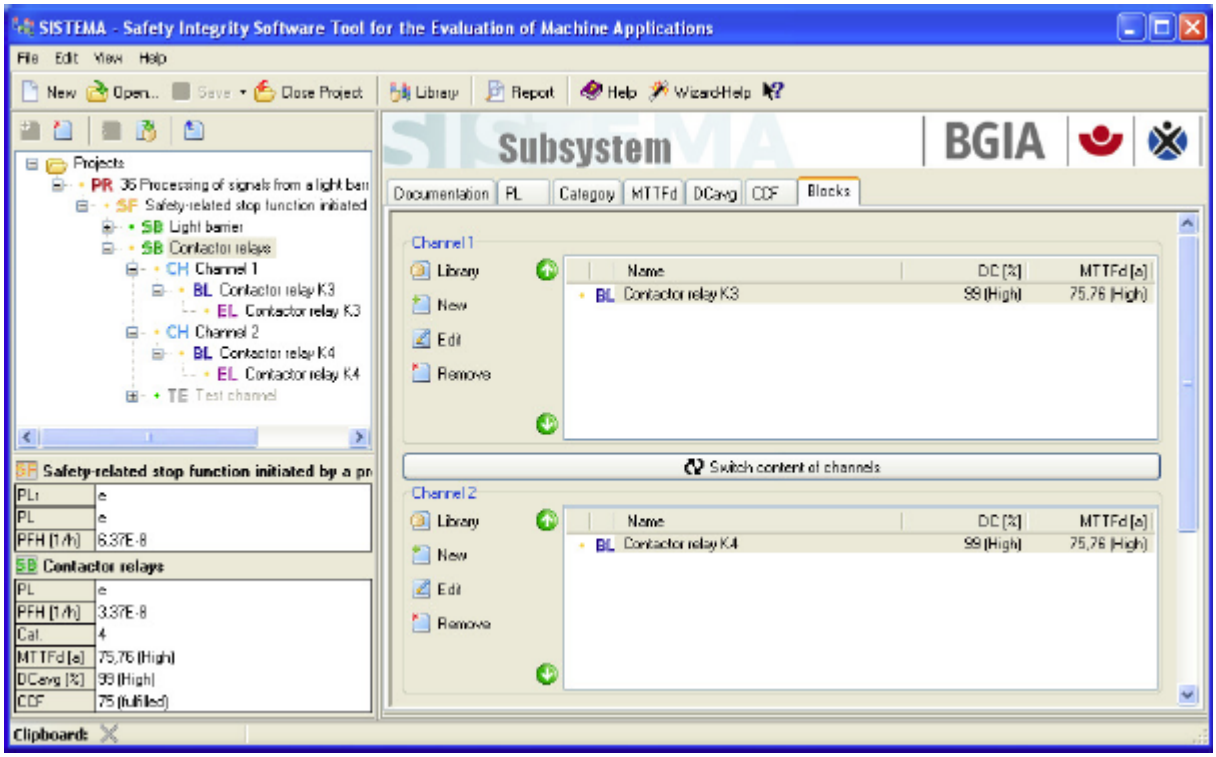



図 8.61：SISTEMA による PL の決定