日機連２１標準化－２

平成２１年度
印刷産業機械の機能安全に関する
調査研究報告書

平成２２年３月

社団法人　日本機械工業連合会
社団法人　日本印刷産業機械工業会

この事業は、競輪の補助金を受けて実施したものです。

http://ringring-keirin.jp

序

我が国では、標準化の重要性は以前から十分認識されており、特に機械工業においてはきわめて精巧な規格が制定されてきています。また経済の国際化に伴い、世界的規模で規格の国際共通化が進められております。

しかし、我が国の規格の中には独自で制定したものもあり、国際化の視点での見直しを行う必要性が高まっています。弊会ではこれに対応するため、従来から機械工業に係わる国内規格の国際規格との整合化事業等に取り組んで参りました。

近年、国際標準化にも新しい動きが起こり、製品を中心とした規格に加え、安全、品質、環境など安心のための基本要素をはじめとするマネジメントに係わる規格などが制定されてきております。弊会においてもこの動きに対応し、機械安全、環境保全など機械工業におけるマネジメントにかかわる規格や、機械工業の横断的な規格についての取り組みを強化しているところです。

具体的には、国内規格と国際規格との整合を目指した諸活動、機械安全規格整備とリスクアセスメントの普及活動、機械安全への取り組みが競争力強化につながる方策の検討、各専門分野の機関・団体の協力による機種別・課題別標準化の推進などです。これらの事業成果は、関連業界共通のガイドライン、日本発の国際規格への提案や国際規格と整合した日本工業規格(JIS)、団体規格の早期制定などとなって実を結ぶものであります。

こうした背景に鑑み、弊会では機械工業の標準化推進のテーマの一つとして社団法人日本印刷産業機械工業会に「印刷産業機械の機能安全に関する調査研究」を調査委託いたしました。本報告書は、この研究成果であり、関係各位のご参考に寄与すれば幸甚です。

平成２２年３月

社団法人　日本機械工業連合会

会　長　　伊　藤　源　嗣

はしがき

近年、ISO 国際安全規格においては、ISO 12100 等に規定された機械類の安全性に関する一般原則をはじめ機械安全や電気安全などの規格が改正、整備されてきており、機械の製造者は、これらに準拠した機械の設計、製造が求められております。

印刷産業機械の安全規格である ISO 12643-1～5 においても、新たにグループ安全規格（B 規格）として規定された機械の安全制御部に関する ISO 13849-1:2006 の要求事項を適用するための審議が進められております。

これらの新しい規格に適合することは、印刷産業機械の主要製造国である我が国の印刷産業機械製造者にとって大きな課題であり、安全性を確保するための具体的な取り組みを推進し国際競争力を一層強化することが必要となっております。

本調査研究は、印刷産業機械の製造者として ISO 13849-1:2006 が要求する安全制御回路システムにおける PL（パフォーマンスレベル）評価の取り組みを推進するための指針について検討を行ったものであり、これらの成果を報告書に取りまとめました。

本報告書が皆様のご参考に資すれば誠に幸いであります。

本調査研究の実施にあたりましては、長岡技術科学大学の福田隆文准教授をはじめ NPO 安全工学研究所及び印刷産業機械業界の方々には多くのご協力をいただきました。また、PL 評価の実証調査においてはドイツ BG（ドイツ職業保険組合）のご指導を賜り、これらの成果は本調査研究の要とすることができました。

ここに厚くお礼を申し上げる次第であります。

平成２２年３月

社団法人 日本印刷産業機械工業会

会長　小森善治

委 員 会 名 簿

（敬称略、順不同）

１．委 員 名 簿

委 員 長	福 田 隆 文	長岡技術科学大学 システム安全系 准教授
委　　員	鈴木美智男	(株)ＩＳＯＷＡ 電子技術グループ リーダー
委　　員	菅 原 大 助	イトーテック(株) 設計開発部 電気課 課長
委　　員	郷 間 英 樹	(株)尾埼製作所 技術課 係長
委　　員	海老原宏満	(株)小森コーポレーション　開発部開発４課
委　　員	田 中 広 志	(株)桜井グラフィックシステムズ 電気設計課 係長
委　　員	青 島 寿 彦	(株)篠原鐵工所 設計課 課長
委　　員	桐 栄 敬 二	大日本スクリーン製造(株) 技術開発カンパニー 部長
委　　員	田 村 俊 一	(株)東京機械製作所 電機制御部 主任
委　　員	渡 辺 達 男	太陽精機(株) 開発本部 制御開発Ⅲ （ホリゾン・インターナショナル(株)）
委　　員	奥 原 秀 雄	三菱重工業(株) 印刷機械技術部 特許技術管理グループ グループ長
委　　員	木 村 隆 志	リョービ(株) グラフィックシステム本部 技術部印刷機設計課 課長
委　　員	田 尾 玄 治	元(株)小森コーポレーション 社長室
オブザーバー	伊 藤　桂	経済産業省 製造産業局 産業機械課 調整専門職
事 務 局	樋 口 恭 司	(社)日本印刷産業機械工業会 専務理事
事 務 局	長 沼　勉	(社)日本印刷産業機械工業会 事務局長
事 務 局	松 尾 正 明	(社)日本印刷産業機械工業会 業務部長
事 務 局	杉 田 行 人	(社)日本印刷産業機械工業会 調査課長

（敬称略、順不同）

２．グループ名簿

グループ A（オフセット枚葉印刷機）

主　査	青 島 寿 彦	(株)篠原鐵工所
委　員	田 中 広 志	(株)桜井グラフィックシステムズ
委　員	桐 栄 敬 二	大日本スクリーン製造(株)
委　員	奥 原 秀 雄	三菱重工業(株)
委　員	木 村 隆 志	リョービ(株)

グループ B（WEB オフセット輪転印刷機）

主　査	海老原宏満	(株)小森コーポレーション
委　員	田 村 俊 一	(株)東京機械製作所

グループ C（断裁機）

主　査	鈴木美智男	(株)ＩＳＯＷＡ
委　員	菅 原 大 助	イトーテック(株)
委　員	郷 間 英 樹	(株)尾垰製作所
委　員	渡 辺 達 男	太陽精機(株)（ホリゾン・インターナショナル(株)）

３．委 員 会 の 経 過

当該事業の委員会及び分科会の活動経過は、以下のとおりである。

(1) 第1回 印刷産業機械の機能安全に関する調査研究委員会（平成21年7月30日）
① 事業概要及び事業実施計画・スケジュールの確認
② 講演会の開催（PLの評価方法について）
③ 各グループのPLモデル回路の作成について検討

(2) 第2回 印刷産業機械の機能安全に関する調査研究委員会（平成21年9月18日）
① PLモデル回路の説明資料の記載内容について検討
② BGIA Report（回路図解説書）の翻訳について検討
③ SISTEMA（システマ）の解説書作成について検討
④ ISO 13849-1:2006のソフトウェア安全要求事項について検討
⑤ 委託業務の内容について検討（PL評価の検証等）

(3) 第3回 印刷産業機械の機能安全に関する調査研究委員会（平成21年10月21日）
① 講演会の開催（機械・設備の安全関連系エンジニアリングにおける機能安全認証の手引きについて）
② PLモデル回路の説明資料の確認
③ ISO 13849-1:2006の要求事項の解釈について検討
④ BGIA Report（回路図解説書）の翻訳について検討
⑤ SISTEMA（システマ）の解説書作成について検討
⑥ 報告書の構成と執筆分担について検討

(4) PL評価の現地調査（平成21年11月6日）
安全制御回路のPL実機調査（Ａ社）

(5) 第4回 印刷産業機械の機能安全に関する調査研究委員会（平成21年11月26日）
① PLモデル回路の説明資料の最終確認
② 安全制御回路のPL評価実機調査の概要報告
③ ISO 13849-1:2006のソフトウェアに関する要求事項について検討
④ ISO 13849-1及びPL評価についての講演会開催について検討
⑤ 報告書の骨子について検討

(6) 第5回 印刷産業機械の機能安全に関する調査研究委員会（平成22年1月7日）
① 講演会の開催（ISO 13849-1:2006及び爆発予防の概要、PL評価）

② PL 評価の検証結果について討論

(7) 第 6 回 印刷産業機械の機能安全に関する調査研究委員会（平成 22 年 1 月 28 日）

① 各グループの PL 評価に関する検証結果のまとめについて検討

② 報告書原案について検討

③ 事業のまとめの方向について検討

(8) 第 7 回 印刷産業機械の機能安全に関する調査研究委員会（平成 22 年 3 月 1 日）

① 各章の報告書原案について検討

② 調査研究のまとめについて検討

(9) 第 1 回 編集分科会（平成 22 年 3 月 12 日）

① 報告書原案の最終確認

② 報告書の総括及び編集

＜備考＞

本調査研究は事前調査として平成 21 年 1 月に準備委員会を立ち上げ、6 月までの間に計 5 回の準備委員会を開催し、事業の基本的な内容について調査研究を行った。

― 目 次 ―

序
はしがき
委員会名簿
目次

第 1 章　調査研究の目的及び概要 1
1.1　調査研究の背景と目的 1
1.2　調査研究の概要 1
第 2 章　ISO 13849-1:2006 の要求内容について 4
2.1 ISO 13849-1 の概要 4
2.1.1 ISO 13849 の位置付けと関連規格との関係 4
2.1.2 ISO 13849 の 2006 年改正の概要 5
2.1.3 パフォーマンスレベル（PL） 5
2.1.4 PL の計算の基礎 8
2.1.5 ソフトウェアの要求事項 11
2.1.6 SIL と PL の整合(参考) 12
2.2 ISO 12643 への適合及び印刷産業機械の PL 要求値 14
2.3 実機による検証（ISO 13849-1:2006 の要求値と実機による PL 評価の妥当性検証） 16
2.3.1 目的と調査の概要 16
2.3.2 調査項目 17
2.4 まとめ 22
第 3 章　関連業界における ISO 13849-1:2006 の取り組み状況について 24
3.1　欧州、日本の電気メーカーの取り組み（MTTFd、B10d） 24
3.1.1　欧州電気部品業界の PL 対応状況について 24
3.1.2　日本の電気部品業界の PL 対応状況について 25
3.2　BG の ISO 13849-1:2006 の PL 計算の手引き 26
3.3　入手可能な PL 計算ソフトの紹介 27
3.3.1　SISTEMA 27
3.3.2　PAScal 27
3.3.3　PL Evaluator lite 27
3.3.4　Safety Evaluation tool 27
第 4 章　印刷産業機械における PL 評価の検証について 28
4.1　PL 評価の検証 28
4.1.1　目的 28
4.1.2　手順及び日程 28

4.2　印刷産業機械の安全性評価の試行 30
4.2.1　オフセット枚葉印刷機の安全性評価（A グループ） 30
4.2.2　WEB オフセット輪転印刷機の安全性評価（B グループ） 63
4.2.3　断裁機のバックゲージ部の安全性評価（C グループ） 75
4.3　BG による検証結果について 112
4.4　総括 113
第 5 章　調査研究のまとめ 117
― 資料編 ― 119

第 1 章　調査研究の目的及び概要

1.1 調査研究の背景と目的

印刷産業機械の製造者は、機械の安全性を確保するため ISO 等の安全規格の要求事項に適合することが求められている。2006 年には、全ての機械類に適用される ISO グループ安全規格（B 規格）の ISO 13849-1（制御システムの安全関連部）が改正された。

2006 年の ISO 13849-1 の改正は、安全装置等の信頼性評価に関して、機械類に使用する部品等の信頼性に対する従来のカテゴリ評価に加え、安全制御システムの信頼性を長期使用時の寿命という考えまで拡大し、それらを確率論的に求めたパフォーマンスレベル（以下 PL）評価を行うことを要求している。

本改正を受けて、ISO/TC130/WG5（人間工学/印刷産業機械の安全性）国際会議においては、印刷産業機械の安全規格である ISO 12643-1～5（C 規格）に、ISO 13849-1:2006 の要求事項を盛り込むための審議が進められており、順次規格化する予定である。

これにより、印刷産業機械の安全制御システムの評価は、従来のカテゴリ評価から、ISO 13849-1 規格の PL 評価または IEC 62061 規格の SIL が要求されることとなった。

本調査研究は、ISO 13849-1: 2006 の規格を取り上げ、印刷産業機械業界として PL 要求値に対する評価方法を確立し、各社における評価レベルの統一化を図るとともに、印刷産業機械の製造者が ISO 13849-1: 2006 の要求事項に適切に対応するための指針を示し、今後のガイドライン策定のための基本的な内容を整理することを目的とした。

本指針は、中小企業性の高い当業界の国際競争力の強化に寄与し重要な示唆を与えるものとして期待されているものである。

本調査研究において ISO 13849-1:2006 の規格を取り上げたのは、IEC 62061 規格にも SIL の評価方法が規定されているが、趨勢としては従来よりカテゴリ評価に対応してきた印刷産業機械業界においては ISO 13849-1:2006 の PL 評価が適していると判断したためである。

1.2 調査研究の概要

本調査研究は、ISO 13849-1:2006 の規格の要求事項に適合するため、規格の内容を吟味し、PL 評価の取り組み課題を抽出するとともに、試行的に安全制御システムのモデル回路を作成し PL 評価を行ったうえ、認証機関に検証を依頼する等により、これらの対応指針を検討し報告書に取りまとめたものである。

印刷産業機械の安全規格である ISO 12643-1～5 は、ISO 13849-1:2006 の規格に基づき、制御システムの安全関連部の PL 要求値が規定されており、現在、ISO/TC130/WG5 で最終審議を行っているところである。

当委員会では、ISO 12643-1～5 に規定した PL 要求値を満たすための PL 評価の取り組みに関し、以下の内容を中心に調査研究を行った。

(1) PL の評価方法に関する調査

ここでは、ISO 13849-1:2006 が要求する安全制御システムの PL 評価に関連する基本的事項について、以下の調査を行った。

① ISO 13849-1:2006 の安全制御システムの要求性能レベルに関する調査及び印刷産業機械の安全規格（ISO 12643-1～5）が求める PL 要求値に関する調査。

② 印刷産業機械の実機による PL 要求値の検証。

③ PL の各種計算システムの評価。

(2) 安全制御回路モデルによる PL 評価実証調査

印刷産業機械業界として適切な PL 評価の取り組みを推進するため、当委員会において、印刷産業機械の回路図を想定した安全制御システムのモデル回路を作成し、PL 評価を試みた。それらの検証は認証機関に依頼した。

モデル回路は、機種別に設置した、オフセット枚葉印刷機（Ａグループ）、WEB オフセット輪転機（Ｂグループ）、断裁機（Ｃグループ）の３グループごとに作成のうえ、ISO 13849-1:2006 の手順に従い PL 評価を行った。

これらの実施手順及び実証は以下のとおり行った。

① 機種別の安全制御システムのモデル回路を作成。

② モデル回路の PL 要求値を求める。
（ISO 12643 規格に基づき PL 要求値を求めることにしたが、ISO 12643 規格に規定がない場合、リスク分析により PL 要求値を求めた）

③ 安全制御回路モデルの PL 評価の試行。
- モデル回路のブロック展開
- PL 評価の計算（手計算または PL 評価自動計算システムを使用）
- レポート作成

④ PL 評価の実証
各グループがレポートにまとめた PL 評価資料の検証については、印刷産業機械の認証に実績のあるドイツの認証機関 BG（ドイツ職業保険組合/以下 BG）に調査を依頼し、具体的な回答を得た。

(3) 指針・ガイドライン策定

上記(1)～(2)の調査研究成果に基づき、印刷産業機械の製造者が ISO 13849-1:2006 の要求事項に適合した PL 評価の取り組みを推進するための指針を示し、今後のガイドライン策定を念頭においた取りまとめを行った。

本報告書の構成について以下に記述する。

第 2 章では、ISO 13849-1 の基本的な概要を理解するため、PL の考え方や計算手順及び印刷産業機械の PL 要求値等について取りまとめた。

第 3 章では、欧州や日本の電気メーカーにおける ISO 13849-1:2006 の対応に関して、各社の MTTFd または B10d の部品リストの公表状況及び各社が公表している PL 計算ソフトの開発状況等について調査した結果を取りまとめた。

第 4 章では、PL 評価の取り組みに関して、その手順等について検証を行った結果を取りまとめた。これらは、委員会の各グループにおいて安全制御システムのモデル回路を作成したうえで PL 評価を行い、ドイツ BG の認証官（Dipl.-Ing Klaus-Dieter Becker）に検証を依頼したものである。ここでは、主に、各グループが試行した PL 評価についての資料と Dr.Becker の検証結果、その解説及び Dr.Becker と各グループとの討論並びに成果について取りまとめた。

第 5 章では、印刷産業機械の製造者が ISO 13849-1:2006 の取り組みを推進するための課題を整理し、本調査研究の成果と今後の取り組み指針を取りまとめた。

また、巻末の資料編には、当委員会が参考にした以下の三点の資料を紹介した。

- BGIA Report 2/2008 の翻訳（仮訳）
  (BGIA が発行している ISO 13849-1 に関係する回路等の解説書であり、ISO 13849-1:2006 の理解を深めるため関連箇所のみを抜粋し当委員会において仮訳したもの。ここでは第 8 章の回路の解説部分を紹介した。)
- SISTEMA の簡易解説書
  (BG が公開している SISTEMA は PL 計算評価ソフトの一つであり、当委員会において回路例を基に操作方法についてまとめたもの。)
- ISO 13849-1:2006 の疑問と解釈についての Q&A（当委員会の質問に対する Dr.Becker の回答)

第 2 章　ISO 13849-1:2006 の要求内容について

2.1 ISO 13849-1 の概要

本節で取り上げるのは、ISO 13849-1:2006“Safety of machinery --- Safety-related part of control systems --- Part 1: General principles for design[1)]”である。この規格は、機械の安全制御部のなかで安全に関連する部分の設計指針で、初版は 1999 年に発行され、我が国メーカーも対応してきている。今回の改正では、昨今の電子化され、またソフトを使用した安全関連制御部が増えたことを反映して、ソフトウェア開発における V モデル、信頼性指標である PL(Performance Level、全制御部の作動の確実性を示す指標)の導入等がなされた。

2.1.1 ISO 13849 の位置付けと関連規格との関係

ISO 13849 は機械安全規格の体系のなかでは B 規格(グループ安全規格)である(図 2.1)。

機械の制御の安全関連部の作動信頼性を規定しているという点では IEC 61508 の傘下規格である IEC 62061[2)]と重複している部分(表 2.1)があり、2.1.6 で記述するが、両者の整合化が課題となっている。また、ISO 13849 でも、PL=e に対応するソフトウェアの設計に関しては IEC 61508[3)] を参照している。

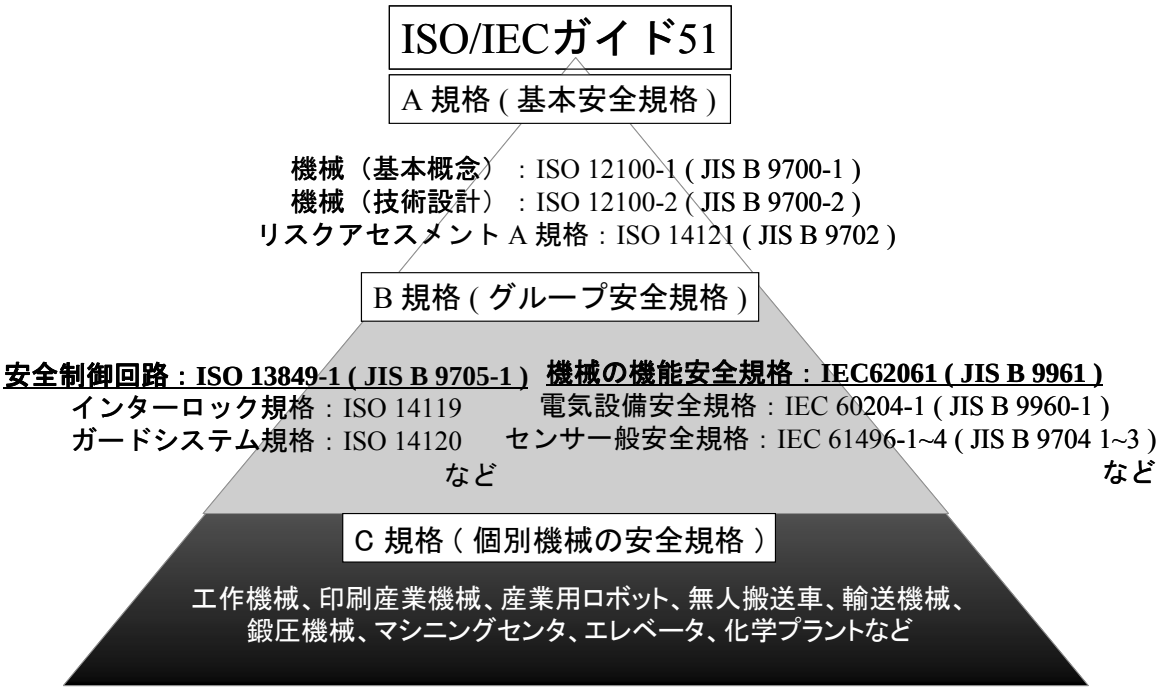


図 2.1　機械類の安全規格の体系

表 2.1 両規格の適用範囲の推奨案(一部簡略)

安全関連性能を実現する技術方式		ISO 13849-1:2006	IEC 62061:2005
A	非電気的、例えば液圧式	適用できる	適用できない
B	電気･機械的部品 (例えば、リレー)、又は非複雑電子部品	PL e までの指定のアーキテクチャに適用	SIL3までのすべてのアーキテクチャに適用
C	高複雑度電子システム､例えばプログラム式	PL d までの指定のアーキテクチャに適用	同上
D	AとBの複合	PL e までの指定のアーキテクチャに適用	非電気的な制御システムには、サブシステムとしてISO 13849-1:2006に適合する部品を用いる
E	CとBの複合	PL d までの指定のアーキテクチャに適用	SIL3までのすべてのアーキテクチャに適用
F	CとA、又はCとA及びBの複合	高複雑度電子システムには、ISO 13849-1:2006に指定されるPL d までのアーキテクチャ又はこの規格によるすべてのアーキテクチャを用いることができる	非電気的な制御システムには、サブシステムとしてISO 13849-1:2006に適合する部品を用いる

(注)この表は、ISO 13849-1:2006、IEC 62061 で、それぞれの表 1 として記載されている。

2.1.2 ISO 13849 の 2006 年改正の概要

主な改定点は次の事項である。

1. リスクの数量的な低減という視点が強く打ち出された。これは、ISO 13849-1:2006 の図 2 に示されている。従来でも、リスクグラフでカテゴリを決定する際に、本質的安全方策でどこまで行うかを考慮していたので、実質同じであるが、リスクを連続量としてとらえる図を用いて説明している。
2. 1.を受け、カテゴリの考え方に信頼性の指標である PL が導入された。また、従来のカテゴリ(だけ)による方法では、カテゴリ 1、2、3、4 で構造の違いは規定されていたが、それが必ずしもリスク低減と一致していたか明確でなかったことが、PL 導入のいきさつの一つと思われる[*1]。
3. いままでソフトウェアを用いる制御回路の扱いの規定がなく､また電子回路を用いた安全制御回路の扱いが明確でなかったので、これらの事項を規定された。

2.1.3 パフォーマンスレベル(PL)

ISO 13849 は制御システムの安全関連部の設計・評価に関する規格であり、上述のように、評価に PL が規定された。PL は、安全関連部の一時間当たりの危険側故障の平均確率を基に考える。ただし、安全側の故障は考えず、危険側故障のみを評価する。定義は表 2.2 のとおりである。手順は次のようになる。

(1) 始めに、危険源同定の結果を受け、リスク低減方策を実施する。

[*1] ISO/TC199 委員でこの改正のまとめ役であった Dr. Becker(BG)の講演などによる。

(2) その結果、制御による本質的安全設計方策あるいは安全防護及び付加防護を行うことになった時に、この規格に従った検討を行うことになる。

(3) リスクグラフ(ISO 13849-1:2006附属書Aの図A.1参照)あるいは他の妥当な方法により、安全制御部の有すべきパフォーマンスレベル(PLr)を決定する。または、個別C規格で規定されているので、それに従う。印刷産業機械では、ISO 12643 に規定されている(2.2参照)。

(4) PLr に適合する設計を行う。

表 2.2 パフォーマンスレベル(PL)

PL	一時間当たりの危険側故障発生の平均確率 Average probability of dangerous failure per hour [1/h]
a	$\geq 10^{-5}$ to $<10^{-4}$
b	$\geq 3\times10^{-6}$ to $<10^{-5}$
c	$\geq 10^{-6}$ to $<3\times10^{-6}$
d	$\geq 10^{-7}$ to $<10^{-6}$
e	$\geq 10^{-8}$ to $<10^{-7}$

しかし、実際的には、設計した回路の作動信頼性を厳密に計算するのではなく、CD、 MTTFd、共通原因故障（CCF）の評価を行い、最後に図 2.2 から PL が決まる。この計算プロセスは、カテゴリ毎の指定アーキテクチャを想定したうえで、図 2.3 に示すフローによる。CD、MTTFd の計算、CCF の評価などは、規格の附属書（表 2.3）に示されている。

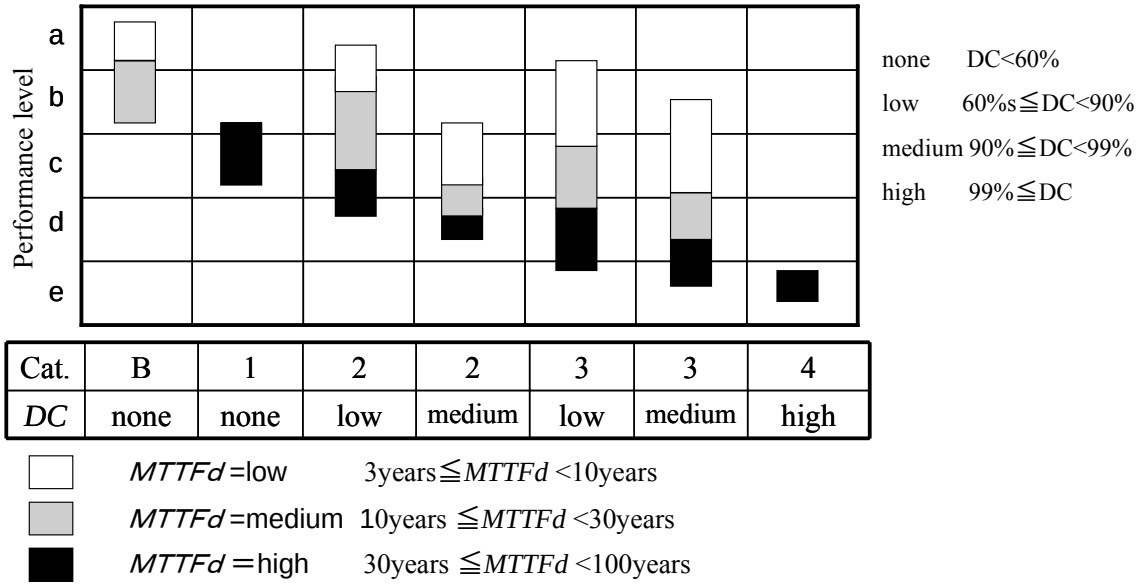


図 2.2 PL の判定法

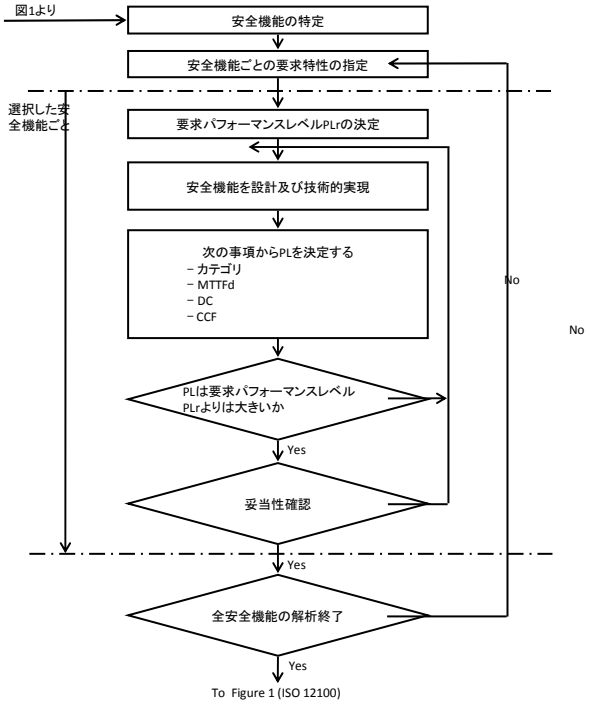


図2.3 PLの決定

表 2.3 ISO 12643 附属書

附属書	表題
A	要求パフォーマンスレベル PLr の決定
B	ブロックメソッド及び安全関連ブロックダイアグラム
C	単一コンポーネントの MTTFd 値計算又は見積もり
D	単一チャンネルの MTTFd 値計算又は見積もり
E	機能及びモジュールの診断範囲(DC)の見積もり
F	共通原因故障(CCF)の見積もり
G	系統的故障
H	制御システムの安全関連部の組み合わせの例
I	例
J	ソフトウェア
K	(ISO 13849-1:2006 の)図 5 の値

2.1.4 PL の計算の基礎

信頼性工学の基礎は、この規格の理解のために必要であり、その概要は理解しておくべきである。信頼性工学では、次の式を基礎としている。

信頼度関数：　$R(t) = 1 - F(t)$　(1)

確率密度関数：　$f(t) = -\dfrac{\mathrm{d}R(t)}{\mathrm{d}t} = \dfrac{\mathrm{d}F(t)}{\mathrm{d}t}$　(2)

故障率関数：　$\lambda(t) = \dfrac{f(t)}{R(t)}$　(3)

また、規格でよく引用される $MTTF$（平均故障間隔時間[*2]）は次式で求められる。

$$MTTF = \int_0^\infty t f(t) dt \qquad (4)$$

なお、この規格では危険側故障を取り扱うので、平均危険側故障間隔時間 $MTTF_d$ を問題とし、安全側故障については議論していない。

この規格では、コンポーネントは指数分布に従うと考えており、信頼度関数などが次式で示される。

$$R(t) = e^{-\lambda t} \qquad (5)$$

$$F(t) = 1 - e^{-\lambda t} \qquad (6)$$

$$f(t) = \lambda e^{-\lambda t} \qquad (7)$$

$\lambda(t) = \lambda$　（故障率関数が一定）　(8)

$$MTTF = \int_0^\infty t\lambda e^{-\lambda t} dt = \frac{1}{\lambda} \qquad (9)$$

直列系／並列系の故障率，平均故障間隔時間

ここでは、規格に出ている式を理解するために必要な式を列記する。なお、上でも述べたが、規格は危険側故障のみを問題としている。従って、規格では $MTTF_d$ と記述している。本章の議論は、信頼性工学の一般論であるので、添え字の d は付していない。

【直列の場合】

$$R(t) = e^{-\lambda_1 t} e^{-\lambda_2 t} = e^{-(\lambda_1+\lambda_2)t} \qquad (10)$$

$$f(t) = (\lambda_1+\lambda_2) e^{-(\lambda_1+\lambda_2)t} \qquad (11)$$

$$\lambda(t) = \frac{(\lambda_1+\lambda_2) e^{-(\lambda_1+\lambda_2)t}}{e^{-(\lambda_1+\lambda_2)t}} = \lambda_1 + \lambda_2 \qquad (12)$$

$$MTTF = \frac{1}{\dfrac{1}{MTTF_1} + \dfrac{1}{MTTF_2}} \qquad (13)$$

[*2] JIS Z 8115:2000 ディペンダビリティー用語では、故障までの平均時間と云う。なお、$MTBF$（Mean Time Between Failure）を平均故障間隔という。

故障率は各故障率の和になる。また、$\lambda = \frac{1}{MTTF}$ の関係を(12)式に代入すると、

$$\frac{1}{MTTF} = \frac{1}{MTTF_1} + \frac{1}{MTTF_2} \qquad (14)$$

となる。このことから、附属書Dに示されているパーツ・カウント・メソッドは、各コンポーネントが直接系になっていると見なしていることと理解できる。

【並列系の場合】

$$R(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t} \qquad (15)$$

$$f(t) = \lambda_1 e^{-\lambda_1 t} + \lambda_2 e^{-\lambda_2 t} - (\lambda_1+\lambda_2) e^{-(\lambda_1+\lambda_2)t} \qquad (16)$$

$$\lambda(t) = \frac{\lambda_1 e^{-\lambda_1 t} + \lambda_2 e^{-\lambda_2 t} - (\lambda_1+\lambda_2) e^{-(\lambda_1+\lambda_2)t}}{e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t}} \qquad (16)＜注　時間に対して一定ではない＞$$

$$MTTF = MTTF_1 + MTTF_2 - \frac{1}{\frac{1}{MTTF_1} + \frac{1}{MTTF_2}} \qquad (17)$$

(17)式と附属書Dの異なるチャンネルに対するMTTFdと各チャンネルのMTTFdの調和に示される(D.2)式を比較すると、並列(冗長)系としたときにMTTFが“大きくなりすぎないように”係数2/3を乗じていることが分かる[*3]。

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

この規格では、B10 ライフ、つまり 10%のアイテムが故障に至る時間を指標に使っている。年間の運転回数n_{op}との関係式

$$\mathrm{MTTF_d} = \frac{B_{10d}}{0.1 \times n_{OP}} \qquad (18),\ (C.1)$$

が示されている。この式もアイテムの故障が指数分布に従うという仮定から、次のように導き出せる。

B10 ライフをT_{10}とすると、$R(T_{10}) = 0.9$（$F(T_{10}) = 0.1$）であるから、

$$R(t) = e^{-\lambda T_{10}} = 0.9 \qquad (19)$$

となる。これから、

$$-\lambda T_{10} = \ln 0.9 = -0.10536$$

となり、

[*3] 資料編の 3. ISO 13849-1 に関する疑問点と BG の回答の 24 参照。

$$T_{10} = 0.10536/\lambda \approx 0.1/\lambda \qquad (20)$$

である。$\mathrm{MTTF} = 1/\lambda$を代入すると$T_{10} = 0.10536/\lambda = 0.10536\mathrm{MTTF}$となる。

したがって、$\mathrm{MTTF} = T_{10}/0.10536$である。したがって、一年当たりのサイクルを$n_{OP}$、B10ライフまでのサイクル数を$B_{10}$とおけば、

$$\mathrm{MTTF} = \frac{B_{10}}{0.10536 \times n_{OP}} \qquad (21)$$

となる。

規格では、0.10536を0.1と丸めて、

$$\mathrm{MTTF} = \frac{B_{10}}{0.1 \times n_{OP}} \qquad (22)$$

としている。

詳しくは他にも検討事項があるが、本節に記した直列系、並列系の故障率及びMTTFの計算根拠を理解しておくことで、規格の式や意味が大まかに類推できる。

2.1.5 ソフトウェアの要求事項

ソフトウェアの扱いは従来の ISO 13849-1 になかったことであるので、関連箇条を抽出し、表 2.4 に示す。細かい要求事項は各関連規格類を参照しなければならない。さらに、ソフトウェアの開発は、図 2.4 に示す V モデルに基づくことが規定されたので、（2.3 に示すように、実質的には今までも行ってきているが）安全要求仕様の明確化、各ステップでの検証作業の計画、実施と結果のドキュメンテーションを残すことが求められる。これらのことについては、附属書 J の表 J.1 に示されている。

表 2.4 ソフトウェアに関する要求事項及び関連規格類

ISO13849-1ソフトウェア一要求事項		その他関連規格・事項		
箇条	概略内容	規格番号/名称	箇条	概略内容
4.6.1	概要:			
	Vモデル図開発フロー			
4.6.2	安全関連ソフトウエア（SRESW）			
	a～dまでのPLを持つ部品の為のSRESW要求方策			
	bまたは、dのPLを持つ部品の為のSRESW要求方策	IEC61508		プロジェクト管理
		ISO9001		品質管理システム
	PL=eを持つ部品の為のSRESW要求方策	IEC61508-3:1998	7	ソフトウエア安全ライフサイクル要求事項
		IEC61508-7:2000		電気電子プログラマブル電子安全関連系の機能安全 技術及び手法の概観
4.6.3	安全関連応用ソフトウエア（SRASW）			
	LVLで書かれ、要求事項に適応するSRASWは、a～eまで達成可能			
	FVLで書かれる場合、SRESWの要求事項を適応でa～eまで達成可能			
	＊PLc～eまでのPLを持つ部品の為のSRESWは下記の追加方策必要			
	a)ソフトウエア仕様のレビュー	ISO13849-1	付録J1	ソフトウエアの機能ブロック・レベルのデザイン例
			付録J2	ソフトウエアの安全寿命期間のVモデルの適応
			付録J3	ソフトウエア仕様の検証
			付録J4	プログラミングルールの例
	b)ツール、ライブラリ、言語の選択	IEC61131-3		PLC5種の言語（LD、SFC、FBD、ST、IL）定義
	c)ソフトウエアドキュメント			
	d)RASWと非ARASWの組み合わされている場合の要求事項			
	e)実効とコーディング要求事項			
	f)試験			
	g)文書化（変更履歴管理）			
	h)検証			
	I)設定管理（開発時の環境設定のバックアップ）			
	j)変更（変更の権限と履歴管理要求）			
4.6.4	ソフトウエア・ベースのパラメーター化 データーは、完全性及び識別 変更履歴、無資格者から保護を行なう			
4.7	達成されたPLがPLrを満たしていることの検証	ISO13849-1		4.3項の要求に一致しなければならない
4.8	設計の人間工学的側面	ISO12100-2		機械類の安全性―設計のための基本概念、一般原則 第1部：基本用語、方法論
	マンマシンは、いかなる誤使用にも危険に曝されないこと	EN614-1		機械の安全性－人間工学に基づく設計原則 第１部：用語及び一般原則
		ISO9355-1		表示器及び制御作動器の設計における人間工学的必要条件－第1部：表示器及び制御作動器と人間との相互作用
		ISO9355-3		表示器及び制御作動器の設計における人間工学的必要条件
		EN1005-3		機械の安全性－人間の身体的機能
		IEC60204-1:2000	10	機械類の安全性－機械の電気装置 第1部：一般要求事項
		IEC60447		マンマシンインタフェース（MMI）―操作の基準
		IEC61310		機械の安全性－指示，マーキング及び作動

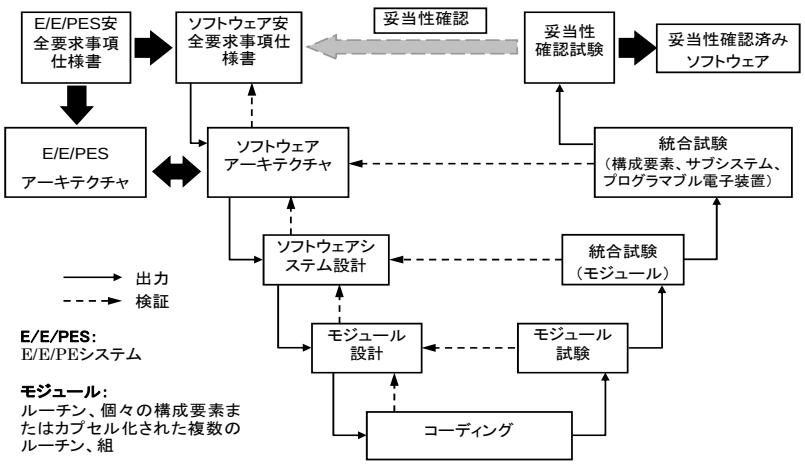


図 2.4 ソフトウェア開発のための V モデル

2.1.6 SIL と PL の整合(参考)

ISO 13849 の PL は一時間当たりの危険側故障の平均確率で定義されている。一方、IEC 62061 における安全度水準 SIL は PFHD で規定されている。どちらも同等な指標であり、両者の関係は次の表 2.5 で示される。

表 2.5 SIL と PL の関係

ISO 13849			IEC 62061	
カテゴリ	PL	PDF [*4]	SIL	PFH_D
1	a	$\geq 10^{-5}$ to $<10^{-4}$	PL=a に該当する SIL は規定されていない	
2	b	$\geq 3\times10^{-6}$ to $<10^{-5}$	1	$10^{-6} \leq PFH_D < 10^{-5}$
	c	$\geq 10^{-6}$ to $<3\times10^{-6}$		
3	d	$\geq 10^{-7}$ to $<10^{-6}$	2	$10^{-7} \leq PFH_D < 10^{-6}$
4	e	$\geq 10^{-8}$ to $<10^{-7}$	3	$10^{-8} \leq PFH_D < 10^{-7}$

ISO 13849、IEC 62061 の両規格は適用範囲の重なり、現場ではどちらを使用するか判断するか迷うことが予想された。その対応として、ISO 13849 を担当する ISO/TC199 と IEC 62061 を担当する IEC/TC44 の合同チームがつくられ、共通の附属書を作成して、使い分けのガイドを作成する作業が始まった。その最初のアウトプットとして、両規格を比較及び可動ガードによる動力遮断制御回路に関する計算結果の比較・考察した文書が、TR(Technical Report、技術報告書)のドラフト [4] として出された。このなかで可動ガードの位置を二つのポジションスイッチ

[*4] 一時間当たりの危険側故障発生の平均確率。英語は Average probability of dangerous failure per hour [1/h]。実質的には IEC 62061 の PFH_D と同じである。

で検知し[*5]、安全モジュールで処理しコンタクタを制御することで、ガード開のときにモータへの動力を遮断する制御回路(図 2.5)について、両規格による比較が行われた。ISO 13849:2006の手順にしたがって評価した結果は平均危険側故障確率 2.70×10^{-8} で PL=e、一方 IEC 62061 の手順にしたがって評価した結果は 4.28×10^{-8} で SIL 3 となった。どちらも一時間当たりの危険側故障の発生確率であるから同じ結果になるべきものであるが、この TR 案は計算結果の数値の違いは予想していた程度であり、許容される程度であるとしている。又、共通原因故障の扱いの差異が「小さく許容できる差の原因となる」としている。今回の例では、PL=e、SIL 3 と同等のレベルとなったが、PL=d、SIL 3 のように異なるレベルとなることも十分考えられる。このような状況は混乱を招くので、両手法の一層の整合化が望まれる。

当面は共通の附属書の作成を目指しているが、将来は両規格を統合して ISO/IEC 共通規格とすることが計画されている。

また、使用する故障率のデータによっても結果の差が出る。信頼性のデータが整備されることが、ISO 13849、IEC 62061 規格の適切な使用に欠かせない。この点は、産業界の共通の課題として整備をして頂きたい。

なお、この問題については、佐藤ら[5)]のグループが関心を持ち、解析している。

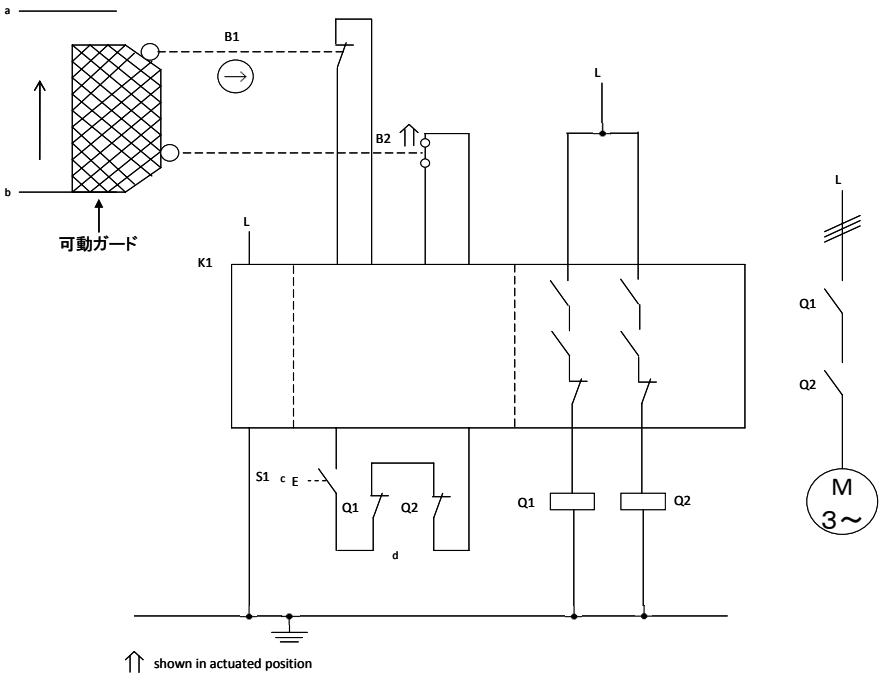


図 2.5 比較検討回路(IEC/TR 62061-1/Ed.1:2009[6)]の Fig.1)

[*5] 可動ガードの位置は、各々のポジションスイッチの状態(押し込まれている・押し込まれていない)の組合せから判別できる。

2.2 ISO 12643 への適合及び印刷産業機械の PL 要求値

機械の設計に当たっては、リスクアセスメント結果に基づき、さらに附属書 A に示されるリスクグラフによって、要求パフォーマンスレベル PLr を決定し、その要求に合致した制御の安全関連部を構築することになる。現実的には、印刷産業機械の安全に関する C 規格 ISO 12643 シリーズに規定されていること PLr を少なくとも達成することが求められる。そこで、規定の要求パフォーマンスレベルを ISO 12643 から抽出したのが、表 2.6 である。

表 2.6 要求パフォーマンスレベル一覧

ISO/DIS 12643-1: [Revision of first edition (ISO 12643-1:2007)]

箇条	項目	要求パフォーマンスレベル
6.5.4.2	**Safety-position switches for interlocking guards**（インタロック付きガードのための要員安全スイッチ） Control systems of safety-position switches	PLr d
	Safety-position switches for interlocking guards（インタロック付きガードのための要員安全スイッチ） control systems for safety-position switches （For access to hazard points,）	PLr e
6.6	**Hold-to-run controls**（ホールド・トゥ・ラン制御器） Guard circuitry for the hold-to-run condition	PLr d
	Hold-to-run controls（ホールド・トゥ・ラン制御器） Control circuitry (including selector switch relays and PLC circuits) that allows interlocked areas to be operated independently	PLr b
6.10.4.2	**Pile changing devices for sheet-feeding and delivery systems**（給紙装置及び排紙装置のパイル交換装置）	PLr d
7.8.3	**Ozone hazards caused by UV radiation**（UV 放射がもたらすオゾンの危険源）	PLr c
10.2.3.1.3	**Emergency stop devices**（非常停止装置）	PLr d
10.7	**Pressure-sensitive mats, pressure-sensitive bumpers, trip devices** （圧力検知マット，圧力検知バンパ及びトリップ装置） Trip devices	PLr d
	Pressure-sensitive mats, pressure-sensitive bumpers, trip devices （圧力検知マット，圧力検知バンパ及びトリップ装置） Trip devices and pressure-sensitive mats, and their related signal processing,	PLr d
11.2.1.2	**Maintaining system and data integrity** （システム及びデータの完全性の保持） The equipment manufacturer or service provider	PLr d
	Maintaining system and data integrity （システム及びデータの完全性の保持） the measures	PLr d
12.1.2	**Performance levels**（パフォーマンスレベル） In the hydraulic/pneumatic control system, the safety-related parts	PLr c
	Performance levels（パフォーマンスレベル） If there is a risk of head or torso injuries then the required performance level	PLr d

	Performance levels（パフォーマンスレベル） If a malfunction of the safety related control system can cause permanent injuries, or if there is a risk of head or torso injuries,	PLr d
	Performance levels（パフォーマンスレベル） If the hazards caused by a malfunction of the safety related control system are small (no permanent injuries)	PLr c
12.3	Cut-off of main energy source（主電源の遮断）	PLr c
12.4	Residual-pile monitoring systems（残留パイル監視システム）	PLr b
12.5	Unobserved unguarded hazard zones（見えない防護していない危険区域）	PLr b
12.7.2	Hydraulic/pneumatic control system（液圧及び空気圧の制御システム）	PLr d
12.7.3	Electric/electronic control system（電気的及び電子的制御システム）	PLr e

ISO/DIS 12643-2: [Revision of first edition (ISO 12643-2:2007)]

箇条	項目	要求パフォーマンスレベル
6.3.1	Guarding in-running nips on sheet-fed presses（枚葉印刷機の引込みニップの防護）	PLr d
6.7.2.3.2.2	Bypass function for removing sample sheets （サンプル紙抜取りのためのバイパス機能）	PLr b
6.7.2.3.2.4	Bypass function for inserting empty pallets and moving in equipment （空パレットの挿入及び機器の進入のためのバイパス機能）	PLr d
6.7.2.3.2.6	Automatic bypass function for pile removal （パイル搬出のための自動バイパス機能）	PLr b
6.7.4	Guarding plate clamping devices （刷版くわ（咥）え装置の防護）	PLr d
6.7.6.2	Exception for folder delivery guarding （折機排紙部の防護の例外） -The bypassing means （バイパスの手段を，規定に適合させる。）	PLr d
8.2.2.2.2	Vapours and mists（蒸気及び霧）	PLr d
8.2.2.4	Exhaust systems of drying devices （乾燥装置の排気システム）	PLr d
10	Control systems for screen printing presses （スクリーン印刷機の制御システム）	PLr e
11.2	Electric/electronic control system of prepress machinery （プリプレス機械の制御システム） The parts of the electric/electronic control system of machines and equipment for the preparation of printing plates	PLr b
	Electric/electronic control system of prepress machinery （プリプレス機械の制御システム） The control systems of interlocking device for safety devices that prevent access to laser radiation class 3R, 3B or 4, as classified in IEC 60825-1,	PLr d

ISO/DIS 12643-3: [Revision of first edition (ISO 12643-3:2008)]

箇条	項目	要求パフォーマンスレベル
5.2.2	Exception for machine motion at production speed	PLr d
5.3.4	Separating elements on hopper feeders	PLr b

5.4.5.3	Glue pans	PLr c
5.10	Trimmers	PLr c

ISO/DIS 12643-4

箇条	項目	要求パフォーマンスレベル
6.1.3	Zone control with stop/safe devices	PLr d
6.4.3	Wrap roller and wrap arms	PLr c
6.5.8	Hazard points between movable gluing unit and fixed machine part	PLr c
6.9.2	Hazard points	PLr c
6.12.1	Crushing points	PLr c
6.13.4	Movement of slitting and scoring units under hold-to-run control	PLr c
	Movement of slitting and scoring units under hold-to-run control	PLr c
7.1.4	Automatic format setting	PLr c
9.3.3.3	Semi-automatic printing forme changes b) the use of hold-to-run control	PLr d
	Semi-automatic printing forme changes c) the use of a foot pedal	PLr d
10.1.2	Automatic diecutting devices	PLr c

ISO/DIS 12643-5

箇条	項目	要求パフォーマンスレベル
5.1.1	Additional safeguarding requirements Trip devices (including knee bars)	PLr e
	Additional safeguarding requirements Sensors used in laser scanners	PLr d
	Additional safeguarding requirements The safety system that controls trip devices and their related signal processing, which safeguard routine and regular access to a hazard point on a manually-fed device,	PLr e
5.4	Main drive braking and clutch/brake mechanism	PLr e

ISO/TC130/SWG5 アムステルダム会議(2008 年 9 月 22 日(月)～24 日(水))においてカテゴリから PL への置き換え時に、表 2.7 の左の二列の関係で機械的に置き換えられるか、我が国がドイツと共にチェックを担当した。我が国では、リスクグラフによる解析を行った。その結果は、上の表 2.6 であり、機械的な置き換え結果とリスクグラフから求めた結果と一致した。したがって、従来のカテゴリを満たした設計であれば、特に問題なく PL に移行できると思われる。実際、次の 2.3 に示す実機による確認で、無理なく要求パフォーマンスレベルに合致した設計になっていることが確認できた。

2.3 実機による検証(ISO 13849-1:2006 の要求値と実機による PL 評価の妥当性検証)

2.3.1 目的と調査の概要

ISO 12643-1“一般要求事項”、ISO 12634 -2“印刷機械及びシステム”に規定される安全防護装置のパフォーマンスレベルに実機において対応されているか調査する。また、カテゴリからパフォーマンスレベルへの移行する際の問題点を抽出する。

実施日時　2009 年 11 月 6 日(金)13:00～16:00
実施場所　A 社事業所（国内）
対象機械　中型オフセット枚葉機（仕向け先：国内）
調査担当　委員長　　福田　隆文
　　委　員　　田尾　玄治
　　事務局　　杉田　行人
予備調査項目　ISO12643-1、 -2 でパフォーマンスレベルを規定している箇条は、表 2.7 “調査箇所”のとおりである。これは、表 2.6 “要求パフォーマンスレベル一覧”からの抜粋である。

2.3.2 調査項目

以上のなかから、次の 4 箇所について調査した。

表 2.7 調査箇所と規格の要求パフォーマンスレベル PLr

安全制御の機能	要求パフォーマンスレベル	該当規格番号，箇条
非常停止	d	ISO/DIS 12643-1:10.2.3.1.3
インキガード	d	ISO/DIS 12643-1:6.5.4.2
安全バー(トリップニップバー)	d	ISO/DIS 12643-1:10.7
デリバリ部光線式安全回路	——	——

ハードウェアの各箇所の調査は、
1. 想定パフォーマンスレベルの確認
2. アーキテクチャが想定パフォーマンスレベルに適合しているかの確認(安全関連制御部のみ抽出した回路図(図 2.6)及び全体回路図)
3. 2.を示したブロック図の確認(図 2.7)
4. パフォーマンスレベル計算書及びサマリー(図 2.8 図、2.9)の確認
5. 実機による配線の確認の順で行った[*6]。また、セーフティーPLC のソフトウェアについては、
6. 仕様決定、コーディング、検証の過程についてヒアリングを行った。

今回の調査対象の安全制御機能は全てカテゴリ 3、パフォーマンスレベル d であった。したがって、2.、 3.については、カテゴリ 3 の指定アーキテクチャ(ISO13849-1:2006 の Fig.11)との照合を行った。要点は、
・基本構成が基本安全原則に則している
・入力装置、論理部、出力装置がそれぞれ二重化になっていること
・論理部内に相互監視があること
・出力部の監視があること
である。カテゴリ 3 の指定アーキテクチャを図 2.10 に示す。

[*6] 動力線と信号線の分離、配線色など IEC60204 に規定される事項は今回の調査対象ではない。

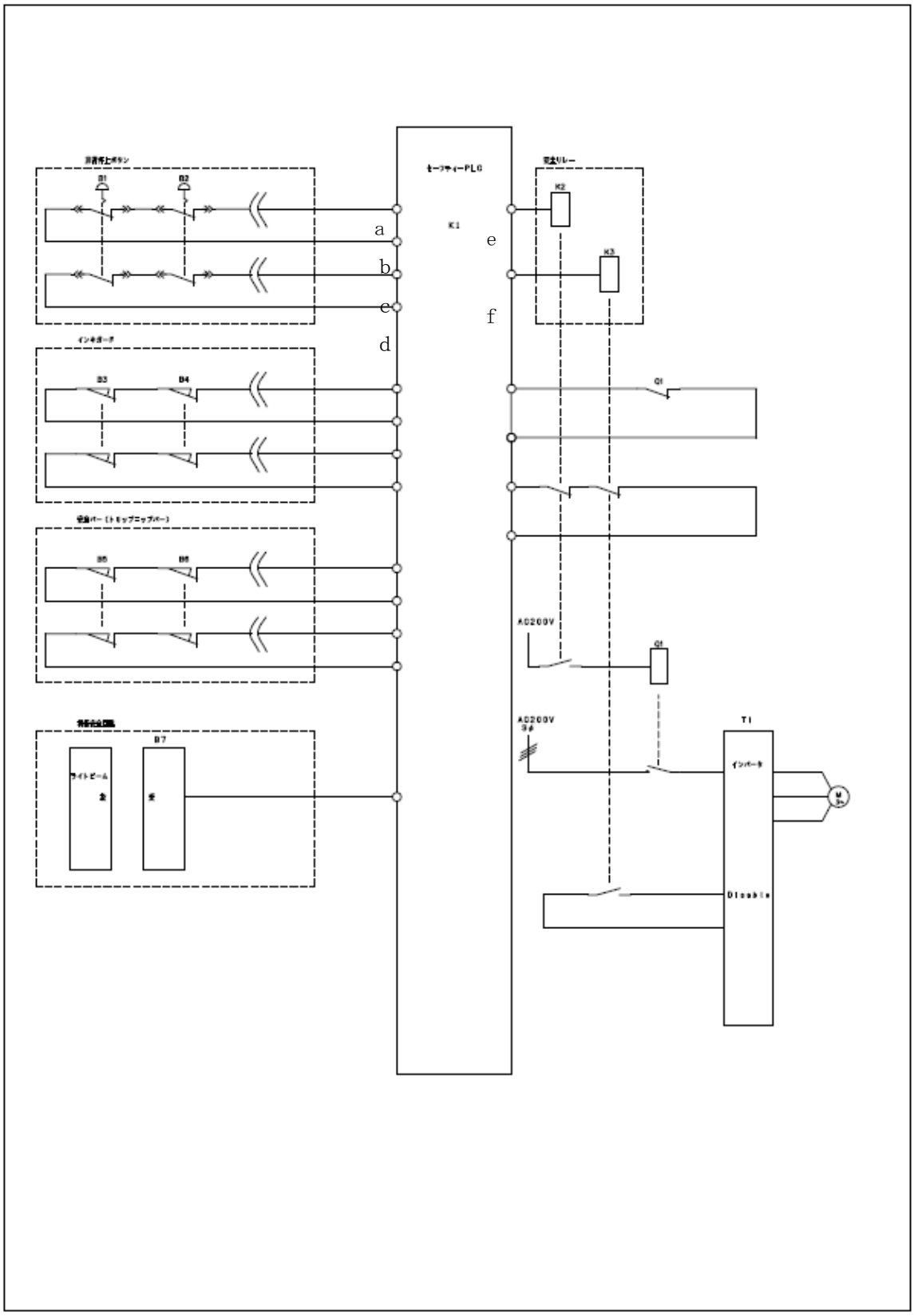
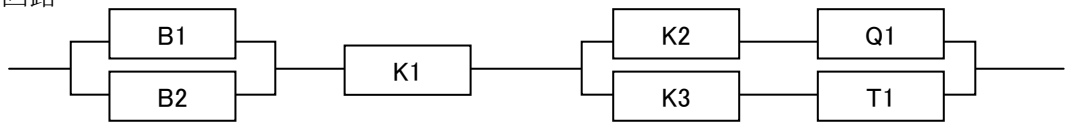
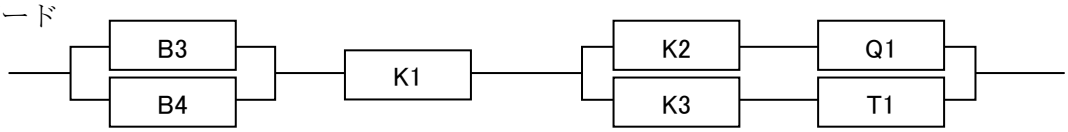


図 2.6 調査対象枚葉印刷機の制御の安全関連部回路

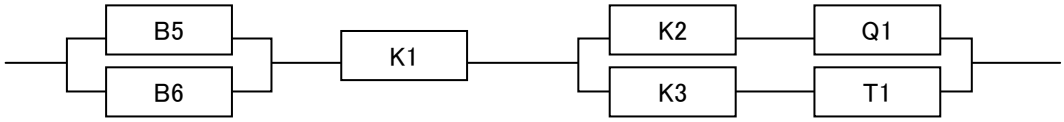
非常停止回路



インキガード



安全バー（トリップニップバー）



排紙安全回路（デリバリライトビーム）

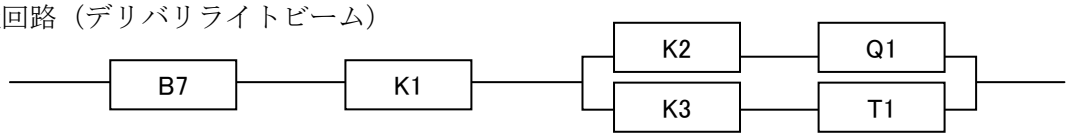


図 2.7　調査対象枚葉印刷機の制御の安全関連部のブロック図

非常停止回路

ブロック1 B1、B2	1サイクル時間	tcycle	3600（1time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	100000
		nop	2500
		MTTFd	400
		DC	99
ブロック1 K1		MTTFd	100
		DC	99
ブロック1 K2	1サイクル時間	tcycle	3600（1time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック1 Q1	1サイクル時間	tcycle	3600（1time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	1000000
		nop	2500
		MTTFd	4000
		DC	90
ブロック2 K3	1サイクル時間	tcycle	3600（1time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック2 T1		MTTFd	20
		DC	90
ブロック1		MTTFd	74.76636
ブロック2		MTTFd	15.84158
全体		MTTFd	51.28539 high
		DCavg	0.919334 medium
		Category	3
		PL	d

インキガード

ブロック1 B3, B4	1サイクル時間	tcycle	360（10time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	20000000
		nop	25000
		MTTFd	8000
		DC	99
ブロック1 K1		MTTFd	100
		DC	99
ブロック1 K2	1サイクル時間	tcycle	3600（10time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック1 Q1	1サイクル時間	tcycle	3600（10time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	1000000
		nop	2500
		MTTFd	4000
		DC	90
ブロック2 K3	1サイクル時間	tcycle	3600（10time/1hour）
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック2 T1		MTTFd	20
		DC	90
ブロック1		MTTFd	90.90909
ブロック2		MTTFd	16.46091
全体		MTTFd	62.28847 high
		DCavg	0.91661 medium
		Category	3
		PL	d

図 2.8　非常停止(左)及びインキガード(右)の PL 計算書

安全バー(トリップニップバー)

ブロック1 B5, B6	1サイクル時間	tcycle	360 (10time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	20000000
		nop	25000
		MTTFd	8000
		DC	99
ブロック1 K1		MTTFd	100
		DC	99
ブロック1 K2	1サイクル時間	tcycle	360 (10time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック1 Q1	1サイクル時間	tcycle	360 (10time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	1000000
		nop	2500
		MTTFd	4000
		DC	90
ブロック2 K3	1サイクル時間	tcycle	360 (10time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック2 T1		MTTFd	20
		DC	90

ブロック1	MTTFd	90.90909
ブロック2	MTTFd	16.46091
全体	MTTFd	62.28847 high
	DCavg	0.91661 medium
	Category	3
	PL	d

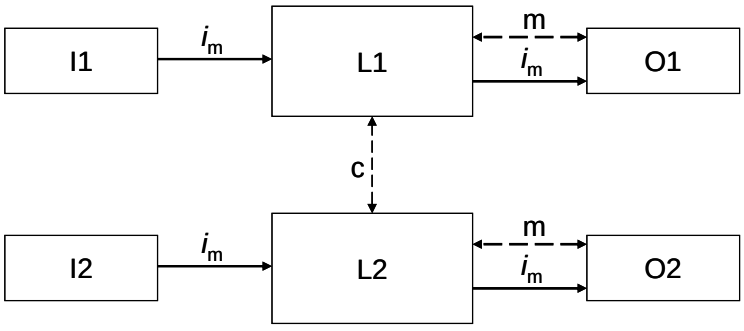
MTTFd

接紙安全(デリバリーライトビーム)

ブロック1 B7		MTTFd	100
		DC	99
ブロック1 K1		MTTFd	100
		DC	99
ブロック1 K2	1サイクル時間	tcycle	3600 (1time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック1 Q1	1サイクル時間	tcycle	3600 (1time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	1000000
		nop	2500
		MTTFd	4000
		DC	90
ブロック2 K3	1サイクル時間	tcycle	3600 (1time/1hour)
	1日の稼動時間	hop	10
	1年の稼動時間	dop	250
		B10d	400000
		nop	2500
		MTTFd	1600
		DC	99
ブロック2 T1		MTTFd	20
		DC	90

ブロック1	MTTFd	47.90419
ブロック2	MTTFd	14.15929
全体	MTTFd	40.64707 high
	DCavg	0.926747 medium
	Category	3
	PL	d

図 2.9 トリップニップバー(左)及びデリバリーライトカーテン(右)の PL 計算書



破線は、合理的に実行可能な障害検出を示す。

記号の説明

I_m	内部接続手段
c	相互監視
I1, I2	入力装置。例えばセンサ
L1, L2	論理
m	監視
O1, O2	出力装置。例えば、メインコンタクタ

図 2.10 カテゴリ 3 の指定アーキテクチャ

【非常停止】

要求パフォーマンスレベルはリスクグラフより PLr=d としており、また ISO/DIS 12643-1:10.2.3.1.3 で規定のＰＬｒと合致しており、妥当である。

1. 回路構成は、センサ部は強制乖離型の B 接点を二重化して使用している。また、安全 PLC は安全認証取得製品であり、筐体は単一であるが内部で二重化されており相互監視も行われている。出力は二個のリレーをそれぞれ駆動している。リレーはコイルの励磁により A 接点を閉じることでそれ以降を制御している。また、A 接点の状態は B 接点によりバックチャックされている。

   一つのリレーは A 接点でコンタクタ Q1 を制御し、コンタクタ A 接点によりインバーターへの電力供給を制御している。コンタクタの A 接点の状態も B 接点でバックチェックされ安全 PLC により監視されている。もう一方のリレーの A 接点はインバーターを直接制御する回路に挿入され、やはり閉じることでインバーターの運転が開始される構成となっている。従って、安全 PLC からの信号断によりインバーターは運転停止する構成である。また、以上の構成は、エネルギ消散によりインバーターをオフする構成であり、停電、断線、地絡、接触等への防護がなされている。
2. 以上の機能上の構成は、ブロック図に示されている。
3. パフォーマンスレベル判定のための PFH_D の計算はサマリーの他、その基となった計算書により確認した。
4. 以上のことが実機でも具現されていることを確認するため、制御盤から非常停止スイッチ B1、B2 への配線(図 2.6 の a、b、c、d 部)及びリレーK2、K3 への配線(同 e、f 部)を回路図の線番と照合することで確認した。

【インキガード、安全バー(トリップニップバー)】

入力部は B 接点で構成されており、インキガード開あるいはトリップニップバーが引かれたときに「開」となるように構成されており、適切であることを、回路図で確認し、また実機でもその様になっていることを確認した。安全 PLC 以降の処理は非常停止と共通である。

【デリバリ部光線式安全回路】

入力部である光カーテンはコンポーネントメーカーにおいて認証取得品が選定されていた。

【安全 PLC 出力部(各機能に共通)】

上記事項共通の安全 PLC のソフトウェアについて設計担当者へのヒアリングを行った。その結果、旧版 ISO 13849-1:1999（現行 JIS B 9705 はこの版の翻訳 JIS であり、2006 年版 ISO の翻訳 JIS は未だ制定、発行されていない）では要求箇条がないが、ソフトウェア開発時には、安全要求仕様と妥当性検証法を定め、その後コーディングを行い、妥当性検証を行っていた。また、安全 PLC は、ソフトを含めた認証品であり、機能ブロック（ソフトウェア）自体も認証品であり、内部に手を加えることはできない構造となっていた。

【実機調査のまとめ】

調査の結果、次の点が明らかになった。

1. ハードウェアの面では、現在有効な規格ではカテゴリで規定されており、設計、製造もそれに従っているが、設計上の検討はすでに開始され、相当程度に進んでいた。従って、規格の趣旨を理解し、相応の準備をすれば設計実務上の対応は可能と思われる。
2. ソフトウェアの妥当性の検証は体系的に精緻に行われており問題点はないと思われるが、規格の定めるVモデル(ISO13849-1:2006のFig.6)との整合性は今後検討が要るように思われる。これは、一社の問題ではなく、工業会としてモデルを構築する必要があろう。
3. 一方、回路が定まっても信頼性データによっては達成できるパフォーマンスレベルが異なることがある。スイッチなどの信頼性データは供給者から提供されるべきものであり、各社、あるいは工業会から要求し、早めに入手することは必須である。

2.4 まとめ

ISO 13849 の改正は一見大幅なもので戸惑うところもある。しかし、構造そのものはカテゴリをそのまま引継ぎ、その上で信頼性の要素を上乗せしているもので、計算の煩雑さはあるが、準備すれば対応可能と思われる。同時に、次のような課題があると考えられる。

1. 規格に沿った設計事例の蓄積、これは本工業会が可能な範囲で事例を持ち寄り、また検討回路例を作成して実施することが望まれる。そのスタートとして今年度に、本調査研究で行ったが、その継続が有効であろう[*7]。
2. 認証取得対応の準備、基本的にはカテゴリを中心とした従来の認証と変わらないと思われるが、信頼性データそれ自身の評価、ソフトウェアの扱いなど新たな点があり、各メーカーは認証取得を想定した仕様書、説明書の作成法を考えておくことが有効であろう。また、PL=eでソフトウェアが入ると、IEC 61508 を用いた説明と記述も要求されているので、その準備も欠かせない。
3. 共通原因故障がスコアーで処理されていること妥当性など､規格に従ったPLの評価が制御回路の安全関連部の適切な評価であるかどうかの実機適用の視点での検証　これは、大学、研究所が主体的に行う必要があろう。
4. 信頼性データの蓄積、これはコンポーネントメーカーにお願いすることになろう。

これらのことを通じて、我々の規格に対する知見を高め、よりよい安全設計を行うと共に、遠くない将来に行われる IEC 62061 との統合化の議論に積極的に参画する準備もしておきたい。

また、この規格の機械指令適用が 2009 年末に予定されていたが、それが二年間延期された。理由ははっきりしないが、EU 内でも準備が十分でなかったと思われる。このことは、我が国も相応の準備が必要であることを示している。

[*7] この課題は全ての分野のメーカーに共通することであり、(社)日本機械工業連合会が中心となって、我が国の研究の集成を行い、BGIA レポート[7)]の日本版をまとめることも有効であると考える。具体的な実施形態、内容は今後検討するものである。

≪参考文献≫

1) ISO 13849-1:2006 “Safety of machinery - Safety-related parts of control systems -- part 1: General principles for design”

2) IEC 62061:2005 “Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems” (JIS B 9961:2006 “機械類の安全性―安全関連の電気・電子・プログラマブル電子制御システムの機能安全―”)

3) IEC 61508 Series:1998-2000 “Functional safety of electrical / electronic / programmable electronic safety-related systems” (JIS C 0508:1999-2000 “電気・電子・プログラマブル電子の安全関連系の機能安全”)

4)＆6) IEC/TR 62061-1/Ed.1:2009 “Guidance on the application of ISO 13849-1 & IEC 62061 in the design of safety-related control systems for machinery”

5) 櫛引豪, 陶山貢市, 佐藤吉信：機械類の安全制御に関する国際規格の整合性について, 信頼性 Vol. 32, No. 1, pp.69-79 (2010)

7) BGIA: Functional safety of machine controls -- Application of EN ISO 13849 (BGIA Report 2/2008e), ISMB:978-3-88383-730-X (2008)

第 3 章　関連業界における ISO 13849-1:2006 の取り組み状況について

3.1 欧州、日本の電気メーカーの取り組み（MTTFd、B10d）

3.1.1 欧州電気部品業界の PL 対応状況について

ISO 13849-1 は従来の制御関連部の安全に関する EN 954-1 に、従来の確定論に基づく概念に、信頼性概念として MTTFd、DC、 CCF を評価対象として加えたものである。1980 年代半ばのニューアプローチ指令に基づくリスクベースド・アプローチ(RBA)及び EN 954-1 のリスクグラフ及びカテゴリ概念は既に永年定着しているが、EN 954-1 を EN 整合規格として 2009 年末に廃止し、その後継規格として ISO 13849-1 のみが EN 整合規格として適用されると言うことに、ドイツ機械産業連合会 VDMA が反対した。反対は会員企業の 2/3 に達すると言われ、その主な理由は、会員企業の大半を占める中小企業にとっては、PL の概念が困難なため、従来のカテゴリに置換するには無理があるとのことであった。2009 年 12 月に、EN 954-1 は年末で廃止するとの当初の決議は延期されたが、その有効期限は 2 年間延長されることになった。

この事例が示すとおり、欧州でさえ ISO 13849-1 の実施につき困難は伴っている。

一方で、欧州電気部品業界、とりわけ安全機器製造者は、ISO 13849-1 への規格対応が数年前に既に実施されていることから、PL 対応の安全機器を既に大半の製造者は用意している。因みに、SISTEMA については、現時点でおよそ 50 社の安全機器製造者がライブラリーを提供している。

(1) 電気部品メーカーが公表している MTTFd または B10d の部品リスト等

MTTFd 及び B10d のデータについて、主なものは ISO 13849-1 の C5 にある記述のとおり、主として SN 29500 が拠り所とされている。その他、MIL-HDBK-217E があり、典型値については本規格に掲載されている。

電気部品メーカーのうち安全関連製品を提供しているメーカーデータについては、約 50 社が SISTEMA Library を作成し、データが公表されている。

(2) 電気部品メーカーの自社製 PL ソフトの開発状況等（メーカー名・ソフトの概要）

PL ソフトについては、BGIA Report 2/2008 を作成・発行した BGIA の SISTEMA が、専門性の観点から、そして前述のとおり Library 提供を含めて主流である。

SISTEMA 以外には、ドイツ PILZ 社の PASCal 及びドイツ SIEMENS 社の SET が PL ソフトとして提供されている。

当委員会が調査した各社の PL 計算ソフトの概要を 3.2 に示す。

3.1.2 日本の電気部品業界の PL 対応状況について

ISO 13849-1:2006 での PL 評価をするために MTTFd、DC、 CCF 等の、部品データが必要であるが、当初、欧州の電気部品メーカーからは提供されるのに対し、日本の電気部品メーカーの対応が遅れていた。しかし最近では日本の主要電気部品メーカーも、MTTFd、DC、 CCF 等のデータを提供できるようになってきた。もちろん ISO 13849-1:2006 Annex C、E、F にある MTTFd、DC、CCF 等のデータを代表値として使用すること可能であるが、電気部品メーカーから提供されたデータを使用することができればその方がベターである。

以下の表 3.1、表 3.2、表 3.3 に部品メーカー3 社の MTTFd、DC、CCF 等のデータを紹介する。

A 社：制御機器、電子部品を中心とする大手メーカー。自動改札機、ATM（現金自動支払機）など世の中にない製品を創り出すベンチャー精神がある。近年は液晶テレビのバックライトが知られる。ISO 13849-1:2006 の PL 評価の説明会を開催し取り組み、早くからこの問題に取り組んでいる。

表 3.1 A 社の機器信頼性データ

機器	機器名称	型式	PL	MTTFd（年）	DC		B10	B10d （サイクル）	備考
S1 (S1-1、S1-2)	非常停止用押しボタンスイッチ	A165E、A22E			99%			100,000回	
S2 (S2-1、S2-2)	イネーブルスイッチ	A4E、A4EG			99%			100,000回	
B4 (B4-1, B4-2)	ロック付安全ドアスイッチ	D4NL 、D4GL 、D4JL 、D4BL			99%			2,000,000回	
K1 (k1-1, k1-2)	安全リレーユニット	G9SX-AD、NE1A	e	100	99%				
K2 (K2-1, K2-2)	安全リレーユニット	G9SX-AD、NE1A	e	100	99%				

B 社：制御機器製品、制御装置及びファクトリーオートメーションシステム製品等の製造メーカー。スイッチ、リレー、タイマー、センサ等の機械制御のための機器、これらの組み合わせの制御装置、ファクトリーオートメーションシステム製品、防災関連機器等の製造・販売を行っている。

表 3.2 B 社の機器信頼性データ

機器	機器名称	型式	PL	MTTFd（年）	DC		B10	B10d （サイクル）
S1 (S1-1、S1-2)	非常停止用押ボタンスイッチ セーフブレークアクション搭載 セーフティポテンシャル構造 パドロック対応タイプ（φ30）	XAシリーズ（φ16） XWシリーズ（φ22） XNシリーズ（φ30）						（K1,K2と組み合わせた場合） 100,000 （直接負荷を遮断する場合） 6,050 ISO13849-1:2006 Annex Cより
	非常停止用押ボタンスイッチ	H6シリーズ（φ16） HWシリーズ（φ22） HNシリーズ（φ30）						
S2 (S2-1、S2-2)	イネーブルスイッチ	HEシリーズ						100,000 ISO13849-1:2006 Annex Cより
	グリップスイッチ	HE*Gシリーズ						
B4 (B4-1, B4-2)	ロック付安全スイッチ ロック付金属ヘッドタイプ安全スイッチ 表面ロック解除付有 ロック付安全スイッチ	HS1*シリーズ HS5Eシリーズ HS6Eシリーズ						2,000,000 ISO13849-1:2006 Annex Cより
	ロック無し金属ヘッド対応安全スイッチ ヘッド外れ検知機能搭載 ロック無し金属ヘッド対応安全スイッチ ロック無し安全スイッチ	HS5Dシリーズ HS5Bシリーズ HS6Bシリーズ						
K1 (k1-1, k1-2)	安全リレーモジュール（Cat.3）	HR1S-ACシリーズ	d	100	99%			
	安全リレーモジュール（Cat.4）	HR1S-AFシリーズ HR1S-AKシリーズ	e	100	99%			
	セーフティコントローラ プログラムレス、ツールレス	FS1Aシリーズ	e	100	99%			
K2 (K2-1, K2-2)	安全リレーモジュール（Cat.3）	HR1S-ACシリーズ	d	100	99%			
	安全リレーモジュール（Cat.4）	HR1S-AFシリーズ HR1S-AKシリーズ	e	100	99%			
	セーフティコントローラ プログラムレス、ツールレス	FS1Aシリーズ	e	100	99%			

C 社：大手電気メーカーの中核事業会社の一つで電力・産業システムを製造・設置するグループにおける電機システム[1]及び電子デバイス[2]の 2 部門で中核を成している企業である。ドイツの大手制御機器メーカーとの提携等も行っている。

表 3.3 C 社の機器信頼性データ

機器番号	機器名称	弊社形式 *1	ブランド名	PL	MTTFd (年)	DC *3	B10 (万回)	B10d (万回) *6	備考
S1 (S1-1,S1-2)	非常停止用押しボタンスイッチ	AR22V2R-02R	富士電機機器制御	—*2	—*3	99.0% *4	100,000	100,000	定格負荷(AC15,220V,3A)での自己宣言データ
		AM22V0E-02R	富士電機機器制御	—*2	—*3	99.0% *4	100,000	100,000	定格負荷(AC15,220V,3A)での自己宣言データ
		XB4BS8444	Schneider	—*2	—*3	99.0% *4	300,000	300,000	定格負荷(AC15,230V,2A)での自己宣言データ
		XB5AS84444	Schneider	—*2	—*3	99.0% *4	300,000	300,000	定格負荷(AC15,230V,2A)での自己宣言データ
B4	ロック付安全ドアスイッチ	XCSTE731*	Schneider	—*2	—*3	99.0% *4	1,000,000	1,000,000	定格負荷(AC15,220V,1.5A)での自己宣言データ
		XCSE731*	Schneider	—*2	—*3	99.0% *4	1,000,000	1,000,000	定格負荷(AC15,220V,1.5A)での自己宣言データ
K0	コンタクタ	SC-N5A、100V	富士電機機器制御	—*2	—*3	99.0% *5	1,000,000	1,000,000	定格負荷(AC3,220V,93A)での自己宣言データ
		LC1D95*K7 + LAD8N11	Schneider	—*2	—*3	99.0% *5	1,000,000	1,000,000	定格負荷(AC3,220V,95A)での自己宣言データ
K1 (K1-1,K1-2)	安全リレーユニット	XPSAV11113*	Schneider	e	50/ch	99.53%	100,000	100,000	自己宣言データ B10dは負荷：AC15,230V,1.5A時 *7
		XPSATE5110*	Schneider	e d	171.2/ch 65.9/ch	99.9% 98.1%	800,000 800,000	800,000 800,000	上段：瞬時接点 下段：ディレイ接点
K2 (K2-1,K2-2)	安全リレーユニット	K1と同じ		K1と同じです					
K3	コンタクタ	SJ-0G DC24V 1b	富士電機機器制御	—*2	—*3	99.0% *5	1,000,000	1,000,000	定格負荷(AC3,220V,12A)での自己宣言データ
		LP4K0601BW3	Schneider	—*2	—*3	99.0% *5	1,000,000	1,000,000	定格負荷(AC3,220V,6A)での自己宣言データ
K4	安全リレーユニット	K1と同じ		K1と同じです					
K7	コンタクタ	K3と同じ		K3と同じです					
K8	コンタクタ	K3と同じ		K3と同じです					

表 3.1、表 3.2、表 3.3 の出典：PL の評価方法についての講演会資料（(社) 日本工作機械工業会より）

3.2 BG の ISO 13849-1:2006 の PL 計算の手引き

BGIA Report 2/2008 は、機械の安全関連制御システムの構築に関する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手引きである。

具体的には、制御システムの安全機能に関する要求 PLr の選択、そして実際に達成される PL の決定が詳しく説明され、それぞれの PL 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あ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、PL「a」から「e」が、カテゴリ「B」から「4」とともに、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。また、これらの回路例には、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も示してある。さらに、各ケースについてより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。

本レポートは、ISO 13849-1:2006 の要求事項が実際の技術手法で実行できるものであることを示したものであり、本規格が国内及び国際レベルで統一して適用され、実施されるための重要な手引きとなる。

本調査研究では、これらの理解を深めるため、本レポートの第 1 章～第 7 章の全部及び第 8 章のうち印刷産業機械と関連のある回路の解説箇所を抽出し翻訳（仮訳）を行い参考にした。

本報告書では、本レポート第 8 章の翻訳（仮訳）を巻末の資料編に掲載した。

なお、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、原本である独文または英文を参照されたい。

BGIA Report 2/2008

http://www.dguv.de/ifa/de/pub/rep/pdf/rep07/biar0208/2_2008.pdf　(独文)

http://www.dguv.de/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf　(英文)

3.3 入手可能な PL 計算ソフトの紹介

PL(パフォーマンス・レベル)の評価計算ソフトには、いくつかのものがある。ここでは、4 つのソフトの概要について紹介する。

各ソフトともに、ISO 13849-1 の附属書にある表 C.1 の部品データ(MTTFd,B10d)、表 E.1 の診断範囲データ(DC)、表 F.1 の共通原因故障データ(CCF)が登録されている。

3.3.1 SISTEMA【システマ】(ドイツ BGIA、英語版、無料)

アドレス：http://www.dguv.de/bgia/en/pra/softwa/sistema/index.jsp

SISTEMA は、ドイツの BGIA(ドイツ職業保険組合・労働安全研究所)が作成したもので、使用する安全部品のデータ(カテゴリ、MTTFd、DCavg、CCF 等)を入力して ISO 13849-1 の PL を評価するソフトである。

3.3.2 PAScal【パスカル】(ピルツジャパン㈱、日本語版、有料)

アドレス：http://www.pilz.com/index.jsp

PAScal は、ISO 13849-1 の PL と IEC 62061 の SIL の両方の評価が可能なソフトである。また、ピルツ製品の安全部品のデータが登録されている。

安全機能ブロックの入力、論理、出力ごとに使用する安全部品をライブラリーから選択して入力する。必要に応じて、MTTFd、DCavg、CCF の数値を入力する。

3.3.3 PL Evaluator lite (OMRON㈱、日本語版、無料)

アドレス：http://www.fa.omron.co.jp/product/specia/4/safety_support/contract.html

PL Evaluator lite は、使用する安全部品のデータを入力して ISO 13849-1 の PL を評価するソフトである。OMRON 製品の安全部品のデータが登録されている。

安全機能ブロックの入力、論理、出力ごとに使用する安全部品をライブラリーから選択し、MTTFd、DCavg、CCF の数値を入力する。

3.3.4 Safety Evaluation tool (SIMENS、英語版、無料)

アドレス：http://auromation.siemens.com

Safety Evaluation tool は、ISO 13849-1 の PL と IEC 62061 の SIL の両方の評価が可能なソフトである。このソフトは、インターネット上で使用するようになっており、パソコンにインストールしないでも使用できる。

第 4 章　印刷産業機械における PL 評価の検証について

4.1　PL 評価の検証

4.1.1　目的

設計者が印刷産業用機械の制御回路の安全関連部の PL 評価を行うためには、適切な例題が大きな助けとなる。また、評価は多くの場合、専門の第三者(認証機関)により行われるので、評価者への出す資料の種類、書き方も重要なノウハウである。これらの資料と経験を蓄積することを目的に、代表的な三機種について、回路の設計、認証に必要な書類の作成等を行い、BG に提出して、評価を受けた。

4.1.2　手順及び日程

以下のように、回路、書類を作成し、BG に送付し、評価結果を文書で得た。また、担当者を当委員会に招いて、ISO 13849 全般の講演及び評価結果についての討論を行った。

【選定対象機器及び担当グループ】

- ・オフセット枚葉印刷機におけるホールドトゥラン機能・デリバリ侵入防止機能・非常停止押しボタン（A グループ）
- ・WEB オフセット輪転印刷機の安全カバー停止回路（B グループ）
- ・断裁機のバックゲージ部（C グループ）

実施手順は次のとおりである。

1. 委員会において、PL 評価を行う機種を決め、対応するグループを編成した。(平成 21 年 6 月 18 日)
2. グループ別に、安全機能を定め、それに対応する制御回路の安全制御部の回路設計を行った。(平成 21 年 6 月 18 日～10 月 21 日)
   回路設計にあたっては、特定の実機の回路ではなく、共通的に使用できうる回路を、委員の知見を基に、共同作業で作成した。したがって、典型的・標準的な回路構成となっている。4.2 に示されるグループ毎のレポートに記述があるが、一部回路は、今後使われる可能性のある先進的なものとしている。
3. 委員会において、各グループが作成の回路図、資料(安全機能説明書、計算書、購入品カタログなど)を説明し、最終確認とした。(平成 21 年 10 月 21 日)
4. 最終確認をした資料（4.2 の(1)）を BG へ送付した。(平成 21 年 10 月 28 日)
5. BG より評価回答書（4.2 の(2)）が、NPO 安全工学研究所経由で届けられた。(平成 21 年 12 月 21 日)
6. 評価書を検討し、討論会での質疑事項の準備を行った。
7. BG における評価者を招いて講習会を開催した。(平成 22 年 1 月 7 日、図 4.1 参照)

8. 評価書、討論結果（4.2 の(3)）を踏まえ、認証取得を想定してレポートを修正した（4.2 の(4)）。

2009年1月7日(木)
於:機械振興会館　地下3階「B3－1号室」

	時　間		プログラム
午前の部	10:00～		福田委員長挨拶 講師紹介
	10:00～ 12:00	120分	1. **ISO 13849-1の説明** 講師　Klaus Dieter Becker氏
	12:00～ 12:30	30分	**2. 防爆予防の説明** 講師　Mr.Albrecht Gloeckle氏(BGDP予防部門　部門長)
	12:30～ 12:40	10分	ー休憩ー
	12:40～ 13:40	60分	**3. ISO 13849-1の演習** **4. SISTEMAの概要説明**
	13:40～ 14:30	50分	ー昼食・休憩ー
午後の部	14:30～ 15:30	60分	**5. ISO 13849-1の質問に対する解説**
	15:30～ 17:00	90分	**6. PL評価の妥当性検証の解説・意見交換**
	17:00		福田委員長閉会挨拶

図 4.1　講習会プログラム

4.2 に上記 3 機種の安全制御回路の評価結果を示す。記載事項は、次のとおりである。

(1) BG への提出レポート（和文、英文）：各機械の危険源から、制御によるリスク低減が妥当なものをいくつかを抽出して、安全制御回路を設計した。回路図及び安全機能の説明、計算書などを作成し、必要に応じてカタログ等を添付し、認証取得と同様な準備を行い、レポートとして BG に提出した。

(2) BG からの指摘（和文、独文の順）：BG から送付された「評価書」をそのまま記載した。

(3) BG との討論内容

(4) 修正レポート：評価書、討論結果（4.2 の(3)）を踏まえ、認証取得を想定してレポートを修正した結果である。

(5) 考察

である。

なお、回路は今回の研究調査のためのものである。また(4)の修正レポートについては、BG 評価書の検討及び討論の結果を受けて作成しているが、BG に提示してはいない。したがって、修正レポートをもってして認証を取得できることを保証するものではない。この点は、調査研究の目的と制約からくるものである。

4.2 印刷産業機械の安全性評価の試行

4.2.1 オフセット枚葉印刷機の安全性評価（Aグループ）

(1)BG への提出レポート

【概要】

オフセット枚葉印刷機における代表的な安全機能は次の３点である。

1. 保守メンテナンス作業時にガードを開けてのホールドトゥラン機能　PLb
2. 排紙部の人体侵入を制限するデリバリー侵入防止機能　PLd
3. 危険時に機械を停止させる非常停止押しボタン　PLd

本回路は以上３点の安全性を評価するものである。

【安全機能】

- ホールドトゥラン機能－回転移動量制限
- 保護装置起動による安全停止機能－安全なトルクオフ
- 非常停止機能－非常停止装置の起動による安全なトルクオフ

【機能説明】

- カバー安全リレーK2 がカバー開を検出した状態で、センサーB4 の入力による機械の速度を K10 により検出し速度制限内であれば機械は回転する。
  ただし、速度オーバーになった場合は速度オーバーリレーK9 が作動し非常停止安全リレーモジュール K3 が主動力源であるマグネットコンタクターMC1 をオフする。
- 排紙ライトカーテン B1 が人体侵入を検出した場合、安全 PLC の K1 が安全リレーK4、K5 が非常停止安全リレーモジュール K3 を作動し主動力源であるマグネットコンタクターMC1 をオフすると共に PLC 電源を遮断しインバーターT1 の駆動信号を遮断する。
- 非常停止押しボタンスイッチ B2 が作動した場合､非常停止安全リレーモジュール K3 が主動力源であるマグネットコンタクターMC1 をオフすると共に安全リレーK8 によりインバーターT1 を無効化する。

【設計の特徴】

- 非常停止押しボタンスイッチ B2 は IEC 60204-1 に準拠した強制開離接点を持つ
- 非常停止安全リレーK3 は EN 954 カテゴリ 4 に適応するものである
- 安全カバーリミットスイッチは IEC 60204-1 に準拠した強制開離接点を持つ
- カバー安全リレーモジュール K2 は EN 954 カテゴリ 4 に適応するものである
- 安全リレーは EN 50205 に適合した強制ガイド接点である（K4、5、6、7、8、9）
- ライトカーテンは EN 954 カテゴリ 4 に適応するものである
- 安全 PLC は EN 954 カテゴリ 4 に適応するものである

Safety evaluation of sheet-fed offset printing press
Group A

【Outline】

There are 3 typical safety functions for a sheet-fed offset printing press.

1. Hold-to-run function, when a guard is opened during a maintenance work. PLb
2. Protective function against a full body access into a delivery area. PLd
3. Emergency stop push-button, which is to stop the printing press in case of emergency. PLd

This circuit diagram is to evaluate the safety of these 3 functions.

【Safety functions】

- Hold-to-run function - limitation of rotation distance
- Safe stop function by activating a protective device - safe torque off
- Emergency stop function - safe torque off by activating an emergency stop device

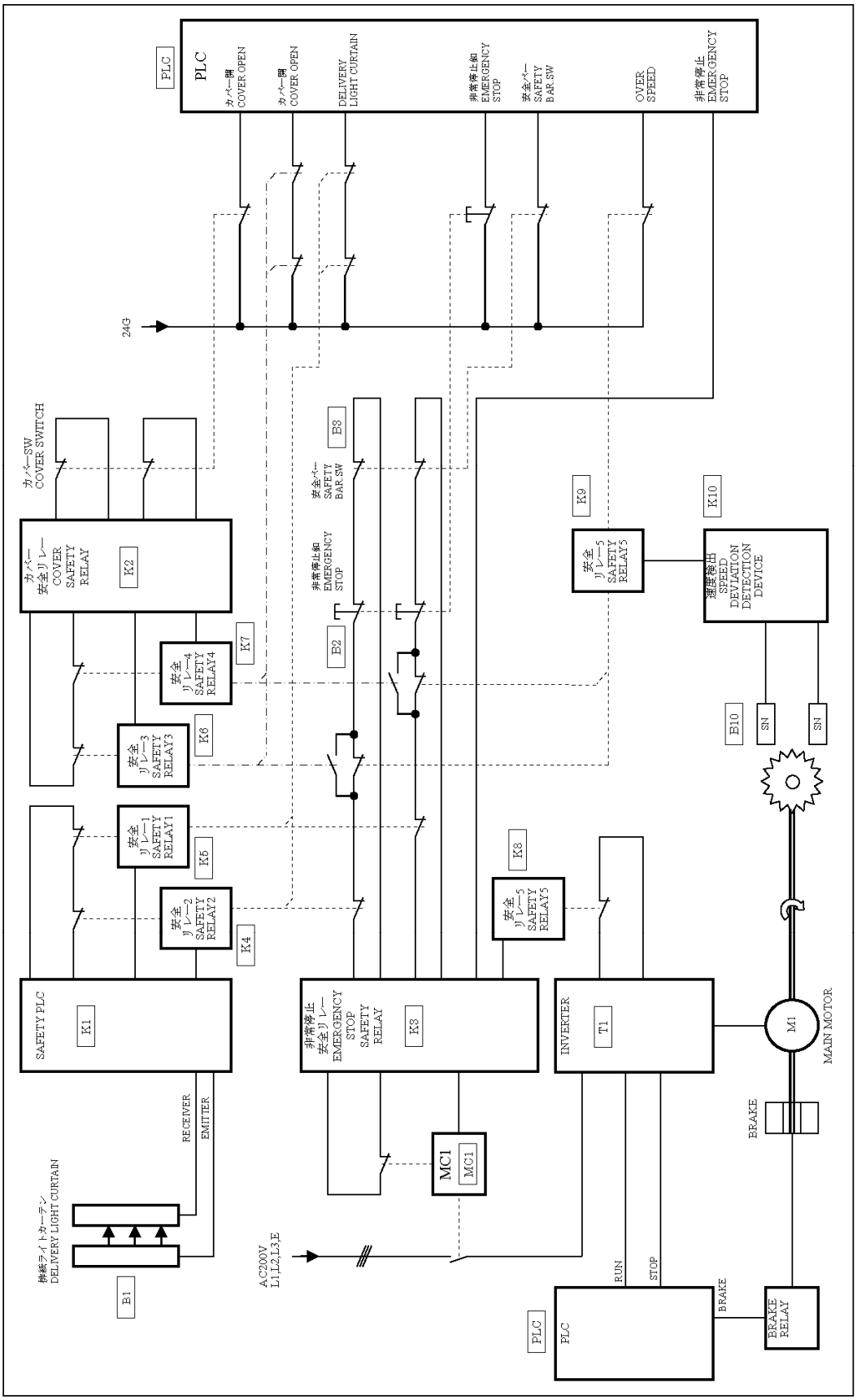
【Function description】

- When Cover safety relay K2 detects an open cover and the machine speed detected by the input of Sensor B4 and K10 is within the speed limit, the machine runs.
  However, if it goes over the speed limit, Overspeed relay K9 is activated and Emergency stop safety relay module K3 turns off Magnet Contactor MC1 of the main power source.
- When Delivery light curtain B1 detects a body access, Safety PLC K1 turns on Safety relays K4, K5 turns on Emergency stop safety relay module K3, and it turns off Magnet Contactor MC1 of the main power source, and at the same time, shuts off the PLC power and it shuts off the drive signal of Inverter T1.
- When Emergency stop push-button switch B2 is activated, Emergency stop safety relay module K3 turns off Magnet Contactor MC1 of the main power source, and at the same time, Safety relay K8 deactivates Inverter T1.

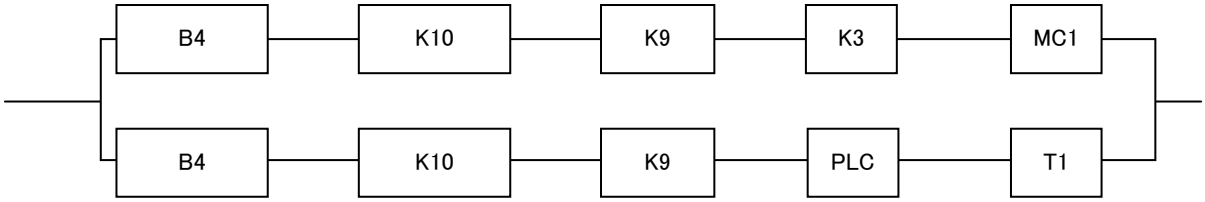
【Design features】

- Emergency stop push-button switch B2 has a positive break of a switch contact to IEC 60204-1.
- Emergency stop safety relay K3 complies with Category 4 of EN 954.
- A safety cover limit switch has a positive break of a switch contact to IEC 60204-1.
- A cover safety relay module K2 complies with Category 4 of EN 954.
- A safety relay is a positive guide contact to EN 50205 (K4, 5, 6, 7, 8, 9).
- A light curtain complies with Category 4 of EN 954.
- A safety PLC complies with Category 4 of EN 954.

オフセット枚葉印刷機の安全性評価（回路図）



ホールドトゥラン回路ブロック図
HOLD TO RUN



機器の信頼性データ
MTTFd and DC about parts.

	機器名 PARTS NAME	型式 PARTS NUMBER	メーカー MAKER	MTTFd (年 YEAR)	B10d	DC(%)
B4	近接センサー (SENSOR)	E2E-X2D1-N	オムロン	8.888888889	20,000,000	90
K3	安全リレー (SAFETY RELAY)	G9SA-301-P	オムロン	100	-	99
K9	安全リレー (SAFETY RELAY)	G7SA-3A1B	オムロン	1,600	400,000	99
K10	速度検出 (SPEED DEVIATION DETECTION DEVICE)	-	自社基板	20	-	90
T1	インバーター (INVERTER)	VF-A7	東芝産機	20	-	90
MC1	マグネットコンタクター (MAGNETIC CONTACTOR)	SC-N8	富士電機	4,000	1,000,000	90
PLC	PLC	CS1H	オムロン (OMRON)	20	-	90

※1 マグネットコンタクターは、電気的耐久性を B10d として代用する(メーカー推奨)
※2 データ入手できない製品は、MTTFd=20 年、DC=90 と仮定する。
※3 近接センサーは、付属書 C-1 表の B10d を使用する。

機器の MTTFd の計算

近接センサー

B4 の MTTFd の計算	B10d=	20,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3600/tcycle	一日の稼動時間 hop=	1	※カバー開時のみ作動とする
nop=250×1×3,600/0＝22,500,000	一年の稼動時間 dop=	250	
MTTFd=20,000,000/(0.1×22,500,000)=8.8888889 年	1 サイクル時間 Tcycle=	0.04	※1 秒間に 25 回作動するとする

安全リレー

K9 の MTTFd の計算	B10d=	400,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3600＝2,500	一年の稼動時間 dop=	250	
MTTFd=400,000/(0.1×2,500)＝1,600 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

マグネットコンタクター

MC1 の MTTFd の計算	B10d=	1,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3600/tcycle	一日の稼動時間 hop=	10	
nop＝250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=1,000,000/(0.1×2,500)＝4,000 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

ホールドトゥラン回路のMTTFdの計算

チャンネル1のMTTFdの計算

$$MTTFd(ch1)=\frac{1}{\left(\frac{1}{MTTFd(B4)}+\frac{1}{MTTFd(K10)}+\frac{1}{MTTFd(K9)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(MC1)}\right)}$$

$$=\frac{1}{\left(\frac{1}{8.888888889}+\frac{1}{20}+\frac{1}{1,600}+\frac{1}{100}+\frac{1}{4,000}\right)}$$

$$=\frac{1}{0.1125+0.05+0.000625+0.01+0.00025}$$

$$= 5.767844 \quad 年$$

チャンネル2のMTTFdの計算

$$MTTFd(ch2)=\frac{1}{\left(\frac{1}{MTTFd(B4)}+\frac{1}{MTTFd(K10)}+\frac{1}{MTTFd(K9)}+\frac{1}{MTTFd(PLC)}+\frac{1}{MTTFd(T1)}\right)}$$

$$=\frac{1}{\left(\frac{1}{8.888888889}+\frac{1}{20}+\frac{1}{1,600}+\frac{1}{20}+\frac{1}{20}\right)}$$

$$=\frac{1}{0.1125+0.05+0.000625+0.05+0.05}$$

$$= 3.800475 \quad 年$$

全体のMTTFdの計算

$$MTTFd(ch1-ch2)=\frac{2}{3}\times\left(MTTFd(ch1)+MTTFd(ch2)-\frac{1}{\frac{1}{MTTFd(ch1)}+\frac{1}{MTTFd(ch2)}}\right)$$

$$=\frac{2}{3}\times\left(5.7678443+3.800475-\frac{1}{\frac{1}{5.767844268}+\frac{1}{3.800475059}}\right)$$

$$= 0.666667 \times \left(9.5683193-2.290951\right)$$

$$= 4.851579 \quad 年$$

全体のMTTFdの分類条件 3年≦MTTFd＜10年により
システム全体のMTTFdは"LOW"に分類されます。

DCavgの計算

$$DCavg=\frac{\frac{DC(B4)}{MTTFd(B4)}+\frac{DC(K10)}{MTTFd(K10)}+\frac{DC(K9)}{MTTFd(K9)}+\frac{DC(K3)}{MTTFd(K3)}+\frac{DC(PLC)}{MTTFd(PLC)}+\frac{DC(MC1)}{MTTFd(MC1)}+\frac{DC(T1)}{MTTFd(T1)}}{\frac{1}{MTTFd(B4)}+\frac{1}{MTTFd(K10)}+\frac{1}{MTTFd(K9)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(PLC)}+\frac{1}{MTTFd(MC1)}+\frac{1}{MTTFd(T1)}}$$

$$=\frac{\frac{0.9}{8.888888889}+\frac{0.99}{20}+\frac{0.99}{1,600}+\frac{0.99}{100}+\frac{0.9}{20}+\frac{0.9}{4,000}+\frac{0.9}{20}}{\frac{1}{8.888888889}+\frac{1}{20}+\frac{1}{1,600}+\frac{1}{100}+\frac{1}{20}+\frac{1}{4,000}+\frac{1}{20}}$$

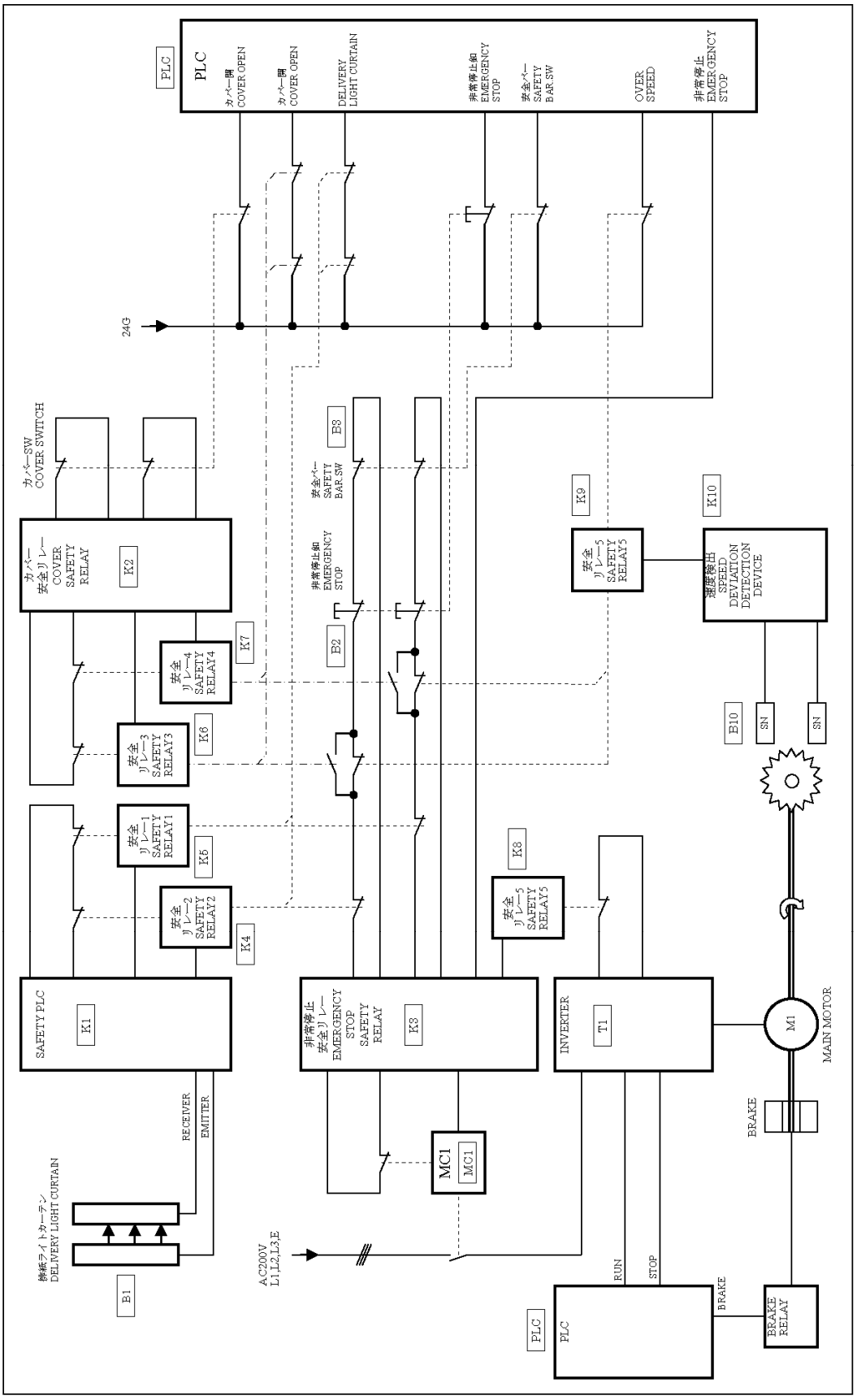
$$=\frac{0.10125+0.0495+0.000619+0.0099+0.045+0.000225+0}{0.1125+0.05+0.000625+0.01+0.05+0.00025+0.1}$$

$$=\frac{0.251494}{0.273375}$$

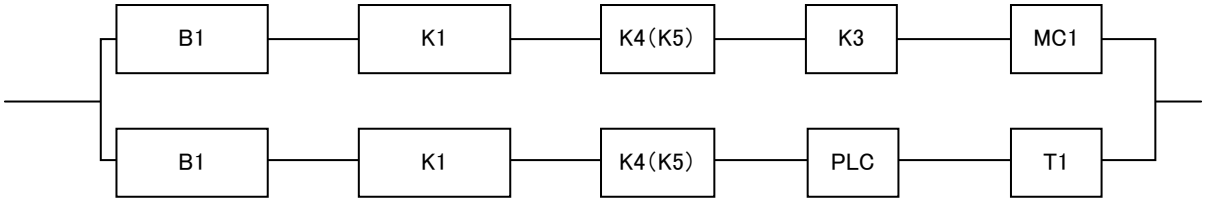
DCavg= **0.919959**

DCavgの分類条件　90%≦DC＜99%により
DCavgは"MEDIUM"に分類されます。

オフセット枚葉印刷機の安全性評価（回路図）



排紙安全部ブロック図
DELIVERY LIGHT CURTAIN



機器の信頼性データ
MTTFd and DC about parts.

	機器名 PARTS NAME	型式 PARTS NUMBER	メーカー MAKER	MTTFd (年 YEAR)	B10d	DC(%)
B1	ライトカーテン (LIGHT CURTAIN)	F3SJ-AM3P300	オムロン (OMRON)	100	-	99
K1	安全 PLC (SAFETY PLC)	NE1A-SCPU02	オムロン (OMRON)	100	-	99
K3	安全リレー (SAFETY RELAY)	G9SA-301-P	オムロン (OMRON)	100	-	99
K4	安全リレー (SAFETY RELAY)	G7SA-3A1B	オムロン (OMRON)	1,600	400,000	99
K5	安全リレー (SAFETY RELAY)	G7SA-3A1B	オムロン (OMRON)	1,600	400,000	99
T1	インバーター (INVERTER)	VF-A7	東芝産機 (TOSHIBA)	20	-	90
MC1	マグネットコンタクター (MAGNETIC CONTACTOR)	SC-N8	富士電機 (FUJI)	4,000	1,000,000	90
PLC	PLC	CS1H	オムロン (OMRON)	20	-	90

※1 マグネットコンタクターは、電気的耐久性を B10d として代用する(メーカー推奨)
※2 データ入手できない製品は、MTTFd=20 年、DC=90 と仮定する。

機器の MTTFd の計算

安全リレー			
K4(K5)の MTTFd の計算	B10d=	400,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=400,000/(0.1×2,500)=1,600 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

マグネットコンタクター			
MC1 の MTTFd の計算	B10d=	1,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3600/tcycle	一日の稼動時間 hop=	10	
nop＝250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=1,000,000/(0.1×2,500)＝4,000 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

排紙安全回路のMTTFdの計算

チャンネル1のMTTFdの計算

$$MTTFd(ch1) = \frac{1}{\left(\frac{1}{MTTFd(B1)} + \frac{1}{MTTFd(K1)} + \frac{1}{MTTFd(K4orK5)} + \frac{1}{MTTFd(K3)} + \frac{1}{MTTFd(MC1)}\right)}$$

$$= \frac{1}{\left(\frac{1}{100} + \frac{1}{100} + \frac{1}{1{,}600} + \frac{1}{100} + \frac{1}{4{,}000}\right)}$$

$$= \frac{1}{0.01 + 0.01 + 0.000625 + 0.01 + 0.00025}$$

$$= \mathbf{32.38866} \quad 年$$

チャンネル2のMTTFdの計算

$$MTTFd(ch2) = \frac{1}{\left(\frac{1}{MTTFd(B1)} + \frac{1}{MTTFd(K1)} + \frac{1}{MTTFd(K4orK5)} + \frac{1}{MTTFd(PLC)} + \frac{1}{MTTFd(T1)}\right)}$$

$$= \frac{1}{\left(\frac{1}{100} + \frac{1}{100} + \frac{1}{1{,}600} + \frac{1}{20} + \frac{1}{20}\right)}$$

$$= \frac{1}{0.01 + 0.01 + 0.000625 + 0.05 + 0.05}$$

$$= \mathbf{8.29016} \quad 年$$

全体のMTTFdの計算

$$MTTFd(ch1-ch2) = \frac{2}{3} \times \left(MTTFd(ch1) + MTTFd(ch2) - \frac{1}{\frac{1}{MTTFd(ch1)} + \frac{1}{MTTFd(ch2)}} \right)$$

$$= \frac{2}{3} \times \left(32.38866 + 8.290155 - \frac{1}{\frac{1}{32.38866397} + \frac{1}{8.29015544}} \right)$$

$$= 0.67 \times \left(40.67882 - 6.60066 \right)$$

$$= \mathbf{22.71877} \quad 年$$

全体のMTTFdの分類条件 10年≦MTTFd＜30年により
システム全体のMTTFdは"MEDIUM"に分類されます。

DCavgの計算

$$DCavg=\frac{\frac{DC(B1)}{TTFd(B}+\frac{DC(K1)}{MTTFd(K1)}+\frac{DC(K4)}{MTTFd(K4)}+\frac{DC(K3)}{MTTFd(K3)}+\frac{DC(PLC)}{MTTFd(PLC)}+\frac{DC(MC1)}{MTTFd(MC1)}+\frac{DC(T1)}{MTTFd(T1)}}{\frac{1}{MTTFd(B}+\frac{1}{MTTFd(K1)}+\frac{1}{MTTFd(K4)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(PLC)}+\frac{1}{MTTFd(MC1)}+\frac{1}{MTTFd(T1)}}$$

$$=\frac{\frac{0.99}{0}+\frac{0.99}{0}+\frac{0.99}{0}+\frac{0.99}{0}+\frac{0.9}{0}+\frac{0.9}{0}+\frac{0.9}{0}}{\frac{1}{0}+\frac{1}{0}+\frac{1}{0}+\frac{1}{0}+\frac{1}{0}+\frac{1}{0}+\frac{1}{0}}$$

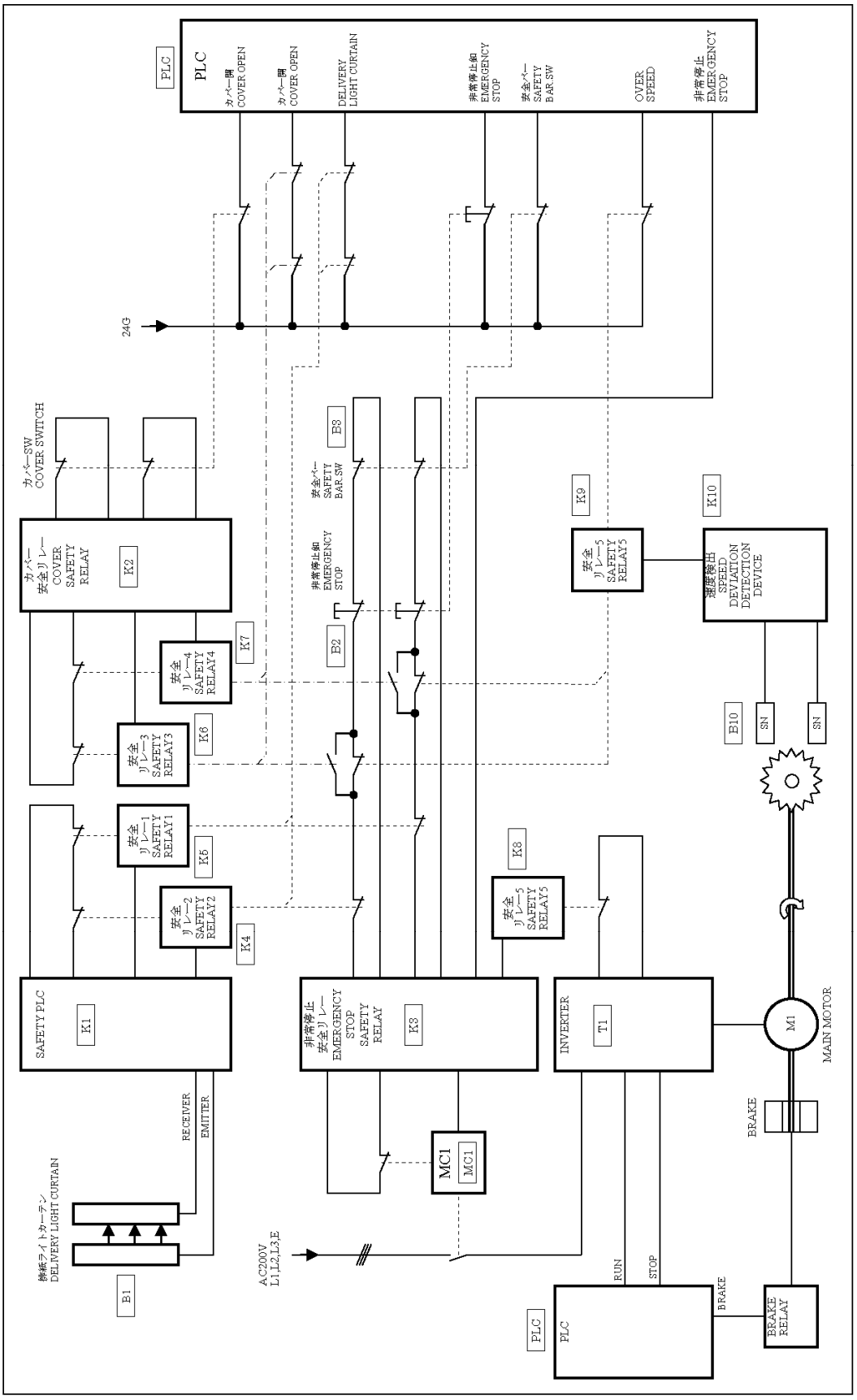
$$=\frac{0.01+0.0099+0.000619+0.0099+0.045+0.000225+0.045}{0.01+0.01+0.000625+0.01+0.05+0.00025+0.05}$$

$$=\frac{0.12}{0.13}$$

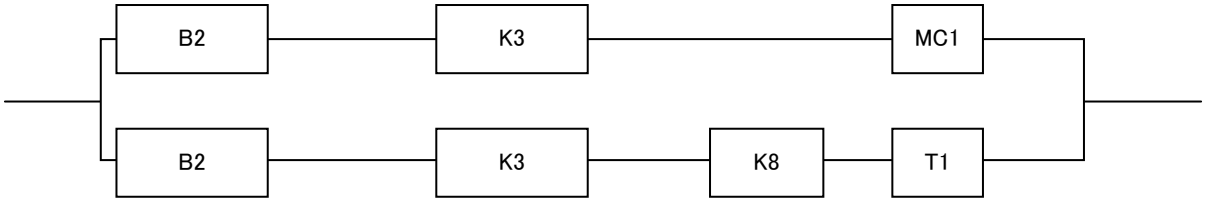
DCavg= **0.92**

DCavgの分類条件　90%≦DC＜99%により
DCavgは"MEDIUM"に分類されます。

オフセット枚葉印刷機の安全性評価（回路図）



非常停止部ブロック図
EMERGENCY STOP



機器の信頼性データ
MTTFd and DC about parts.

	機器名 PARTS NAME	型式 PARTS NUMBER	メーカー MAKER	MTTFd (年 YEAR)	B10d	DC(%)
B2	非常停止釦 (EMERGENCY STOP P.B.)	XA1E-BV303R	IDEC	400	100,000	99
K3	安全リレー (SAFETY RELAY)	G9SA-301-P	オムロン (OMRON)	100	-	99
K8	安全リレー (SAFETY RELAY)	G7SA-3A1B	オムロン (OMRON)	1,600	400,000	99
T1	インバーター (INVERTER)	VF-A7	東芝産機 (TOSHIBA)	20	-	90
MC1	マグネットコンタクター (MAGNETIC CONTACTOR)	SC-N8	富士電機 (FUJI)	4,000	1,000,000	90

※1 マグネットコンタクターは、電気的耐久性を B10d として代用する(メーカー推奨)
※2 データ入手できない製品は、MTTFd=20 年、DC=90 と仮定する。

機器の MTTFd の計算

非常停止釦			
B2 の MTTFd の計算	B10d=	100,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=100,000/(0.1×2,500)=400 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

安全リレー			
K8 の MTTFd の計算	B10d=	400,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=400,000/(0.1×2,500)＝1,600 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

マグネットコンタクター			
MC1 の MTTFd の計算	B10d=	1,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop＝250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=1,000,000/(0.1×2,500)＝4,000 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

非常停止回路のMTTFdの計算

チャンネル1のMTTFdの計算

$$MTTFd(ch1)=\frac{1}{\left(\frac{1}{MTTFd(B2)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(MC1)}\right)}$$

$$=\frac{1}{\left(\frac{1}{400}+\frac{1}{100}+\frac{1}{4,000}\right)}$$

$$=\frac{1}{0.0025+0.01+0.00025}$$

$$= 78.43137 \quad 年$$

チャンネル2のMTTFdの計算

$$MTTFd(ch2)=\frac{1}{\left(\frac{1}{MTTFd(B2)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(K8)}+\frac{1}{MTTFd(T1)}\right)}$$

$$=\frac{1}{\left(\frac{1}{400}+\frac{1}{100}+\frac{1}{1,600}+\frac{1}{20}\right)}$$

$$=\frac{1}{0.0025+0.01+0.000625+0.05}$$

$$= 15.84158 \quad 年$$

全体のMTTFdの計算

$$MTTFd(ch1-ch2)=\frac{2}{3}\times\left(MTTFd(ch1)+MTTFd(ch2)-\frac{1}{\frac{1}{MTTFd(ch1)}+\frac{1}{MTTFd(ch2)}}\right)$$

$$=\frac{2}{3}\times\left(78.43137+15.84158-\frac{1}{\frac{1}{78.43137255}+\frac{1}{15.84158416}}\right)$$

$$= 0.666667 \times \left(94.27296-13.17957\right)$$

$$= 54.06226 \quad 年$$

全体のMTTFdの分類条件　30年≦MTTFd＜100年により
システム全体のMTTFdは"HIGH"に分類されます。

DCavgの計算

$$DCavg=\frac{\frac{DC(B2)}{MTTFd(B2)}+\frac{DC(K3)}{MTTFd(K3)}+\frac{DC(K8)}{MTTFd(K8)}+\frac{DC(MC1)}{MTTFd(MC1)}+\frac{DC(T1)}{MTTFd(T1)}}{\frac{1}{MTTFd(B2)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(K8)}+\frac{1}{MTTFd(MC1)}+\frac{1}{MTTFd(T1)}}$$

$$=\frac{\frac{0.99}{400}+\frac{0.99}{100}+\frac{0.99}{1,600}+\frac{0.9}{4,000}+\frac{0.9}{20}}{\frac{1}{400}+\frac{1}{100}+\frac{1}{1,600}+\frac{1}{4,000}+\frac{1}{20}}$$

$$=\frac{0.002475+0.0099+0.000619+0.000225+0.045}{0.0025+0.01+0.000625+0.00025+0.05}$$

$$=\frac{0.058219}{0.063375}$$

DCavg= **0.918639**

DCavgの分類条件　90%≦DC＜99%により
DCavgは"MEDIUM"に分類されます。

(2)BG からの指摘

安全機能： タッピング動作での安全に減速された速度(Hold to run)

- 安全に減速された速度に関するリスクアセスメントの結果和 PLr=d となる。
  要求されたパーフォーマンスレベルを達成するためには、冗長な制御構造を適用することに意味がある。

- 安全機能に関する仕様はさらに厳密に記述する必要がある。すなわち、この例では調整(regulate)された駆動システムなのか、制御(control)された駆動システムなのかの区別が判別できない。私の推測では、これは調整駆動システムであり、その場合は、安全な速度の実現には調整の量が関係するため、調整プロセスを配慮する必要がある。
- その意味は、安全な速度の実現には、駆動システムの要求値をブロックダイアグラムのロジックで示すことが必要とされる。その際、その要求値がインターロック付き保護装置の開状態に作用するかを明確にすることが要求される。二つ目の回路は、例で示されたように B4、 K10、 K9、 K3 及び MC1 で構成することが可能である。

Sicherheitsfunktion “Sicher reduzierte Geschwindigkeit im Tippbetrieb (Hold to run)”

- Das Ergebnis der Risikoanalyse bzgl. der sicher reduzierten Geschwindigkeit ergibt einen PLr=d. Um den erforderlichen Performancelevel erfüllen zu können, ist es sinnvoll, auf eine redundanten Steuerungsarchitektur zurückzugreifen.

- Die Spezifikation der Sicherheitsfunktion sollte genauer beschrieben werden. Das bedeutet, dass aus dem Beispiel nicht ersichtlich ist, ob es um ein geregeltes Antriebssystem handelt oder um ein gesteuertes Antriebssystem. Sollte es sich um ein geregeltes Antriebssystem handeln, was ich vermute, ist es sinnvoll, den Regelprozess mit aufgenommen, da zur Realisierung der sicheren Geschwindigkeit die Regelgröße mitberücksichtigt werden sollte.
  Dies bedeutet, dass zur Realisierung der sicheren Geschwindigkeit der erste Weg mittelbar über die Sollwertvorgabe im Antrieb als logisches Blockschaltbild dargestellt werden sollte. Wobei zu klären ist, wie der Sollwert bei geöffneter verriegelter Schutzeinrichtung generiert wird. Der zweite Kanal kann dann, wie im Beispiel dargestellt, über B4, K10, K9, K3 und MC1 gebildet werden.
  Ich werde während meines Vortrages auf Lösungsmöglichkeiten eingehen.

(3)BGとの討論内容

・ホールドトゥラン回路

減速された速度のリスクアセスメントをPLrbとした理由について質問を受けた。

ISO 12643-1 6.6 Hold-to-run controls の記載から、防護回路については PLrd、制御についてはPLrbと解釈したことを説明したが、BGからは「安全速度はPLrd」との指摘だった。

現状回路では速度検出用センサーは汎用品であり、さらにギアを検出し回転制御をするため、１サイクル時間（Tcycle）が非常に小さくなり、その結果MTTFｄが１桁となってしまいPLrdは構築できないことになる。

BGとの討論ではセンサーが非接触式であること、センサーを２つ使用することから冗長制御となる旨のアドバイスがあり、具体案の提示は無かったがPLd可能の示唆があった。しかしT cycleが小さいことに変わりはないため、対応案では１日のホールドトゥラン制御運転時間を現実的な範囲で短くしT cycleを伸ばし、対応する。

また、同センサーのB10d、DCの算出についても説明を求められた。

ISO 13849-1　付属書C（表C.1コンポーネントのMTTFｄ又はB10ｄを扱う国際規格）及び付属書E（表E.1診断範囲の見積り）からの選出であることを説明したが、DCについては単に付属書からの選択であってはならない旨の指摘を受けた。

ブロック図においてもセンサーB4、速度検出装置K10が冗長となっていることの誤りを指摘された。

駆動システムについて多くの説明を求められ、回答をした。

・ 排紙安全回路

モーター駆動システムについての説明を求められ、回答をした。

インバーターT1のDC算出について説明を求められた。

ホールドツゥラン回路センサーと同様に算出方法に誤りがあることを指摘された。

・ 非常停止回路

システム全体について説明を求められ、回答した。

・ その他

メーカーからのB10d、MTTFd等の書類に書式があるのかを質問した。

規定書類はないが、何らかのデータシートは欲しいとのこと。

(4)修正レポート

オフセット枚葉印刷機

【概要】

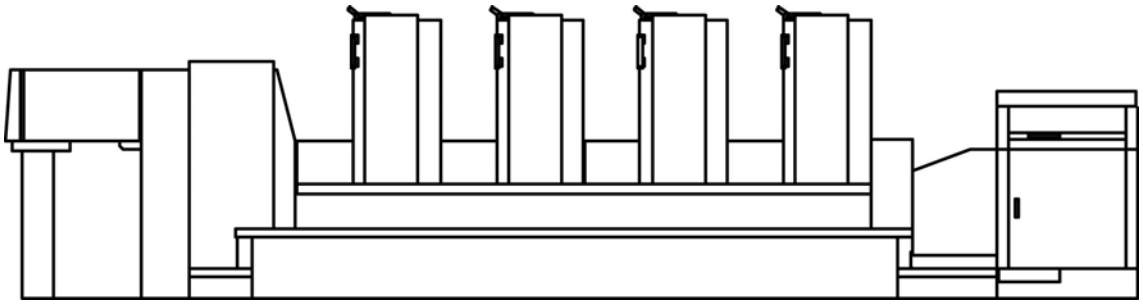


図 4.2 オフセット枚葉印刷機

オフセット枚葉印刷機は、直接紙等にインキを転写するのではなく、ブランケットと呼ばれるゴムに転写してから紙等にインキを転写するものである。

図 4.2 の機械は４色印刷機を示す。

今回は､枚葉印刷機の危険度の高い安全ガードが開いている状態でのホールドトゥラン回路、印刷物の排出部の人体侵入を防ぐ排紙部安全回路、非常停止押しボタン回路を評価する。

ホールドトゥラン　ーカテゴリ 3ー　PLd

【安全機能】

- 保護装置によって起動する安全停止機能：安全ガードの開動作によるドライブ停止
- 安全速度制限：安全ガードが開いている時に制限速度内での動作が可能
- 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

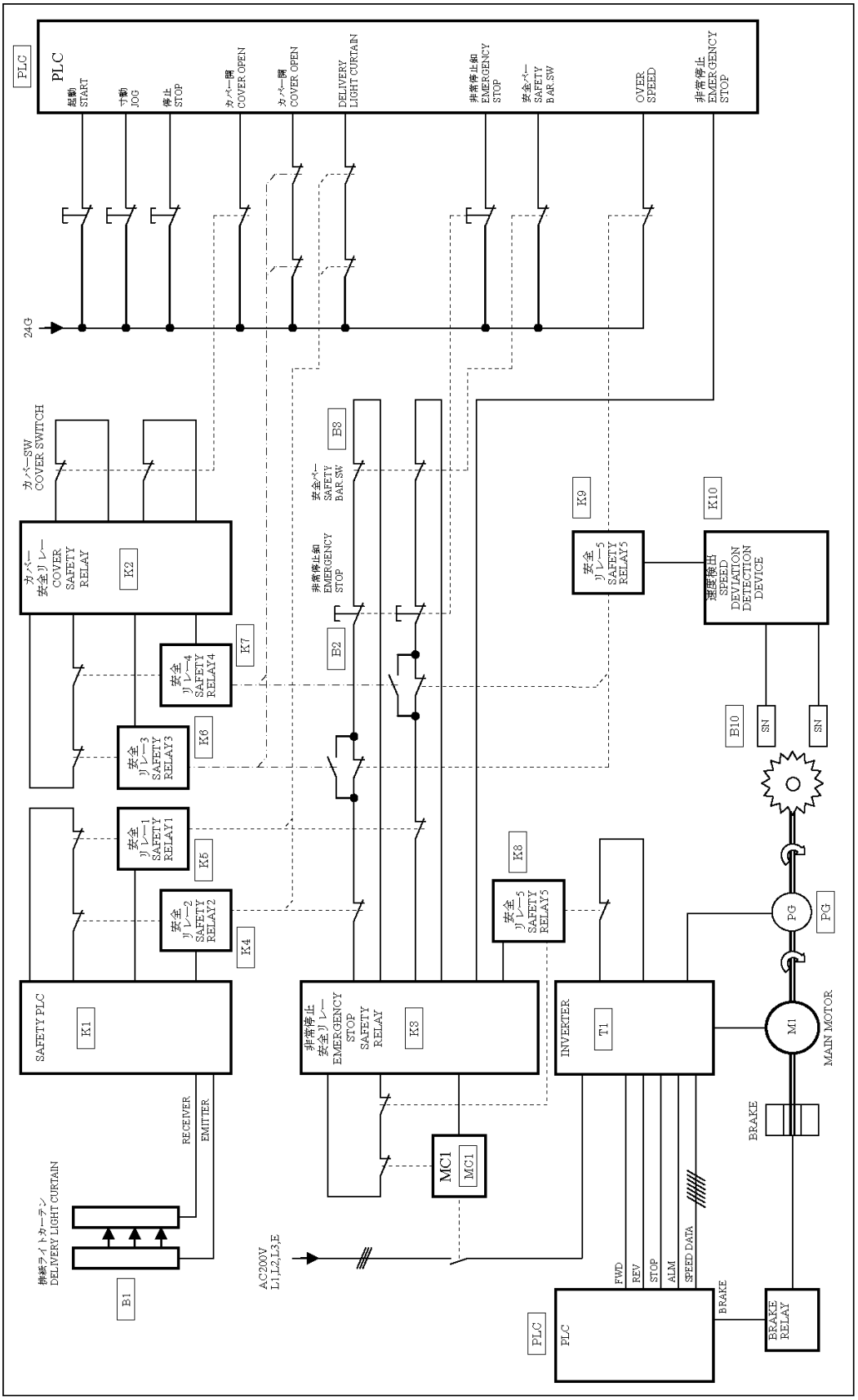
【機能説明】

- 機械動作中に安全ガードが開いた場合は安全リレーK2 によりガード開状態を検出し非常停止リレーK3 によりインバーター電源 MC１を遮断し、同時に安全リレーK8 によりインバーターT1 のフリーラン信号を起動し機械停止する。
- 安全ガードが開いている状態では寸動ボタンを押している間のみ機械動作を許可する。
- 寸動モードでは速度検出センサーB4 及び速度制限装置Ｋ10 により機械速度を検出し、制限を越える速度の場合はスピードオーバーリレーK9 が作動し非常停止リレーK3 によりインバーター電源 MC１を遮断する。
- 寸動モード時は機械操作モーターの速度検出パルスジェネレーターPG により速度監視を行いインバーターT1 と同期的な閉ループを形成する。
- インバーターT1 により制限を越えた速度が検出された場合はその情報が PLC に伝達され、PLC から T1 のストップ信号が出力される。

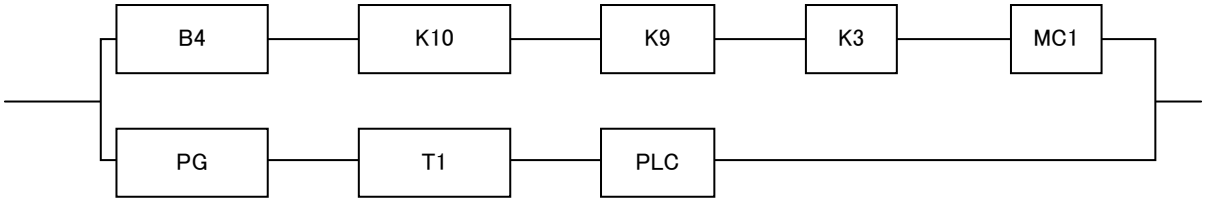
【設計特性】

- 基本及び充分に実証済みの安全原則を守り、カテゴリ B の要求事項を満たす。
- 速度制限については ISO 12643-1 6.6 Hold-to-run controls に従う。
- 安全ガードリミットスイッチは IEC 60204-1 に準拠した強制開離接点を持つ。
- 安全ガード安全リレーモジュール K2 は EN 954 カテゴリ 4 に適応するものである。
- 非常停止安全リレーモジュール K3 は EN 954 カテゴリ 4 に適応するものである。
- 安全リレーは EN 50205 に適合した強制ガイド接点である（K6、7、8、9）
- 速度検出装置 K10 により２つのセンサーB4 を診断し、いずれかのセンサーが故障した場合は速度オーバーと同じ制御となり寸動モードは許可されない。
- マグネットスイッチ MC1 は十分に実証済みの構成部品である。
- インバーターT1 は十分に実証済みの構成部品である。

オフセット枚葉印刷機の安全性評価（回路図）



ホールドトゥラン回路ブロック図
HOLD TO RUN



機器の信頼性データ
MTTFd and DC about parts.

	PARTS NAME	Type	Manufacturer	B10d	MTTFd	DC(%)
B4	SENSOR	E2E-X2D1-N	OMRON	20000000	88.8888	90
K3	SAFETY RELAY	G9SA-301-P	OMRON	100	-	99
K9	SAFETY RELAY	G7SA-3A1B	OMRON	400000	1600	99
K10	SPEED DEVIATION DETECTION DEVICE	-	自社基板	—	20	90
T1	INVERTER	VF-A7	TOSHIBA	20	-	90
MC1	MAGNETIC CONTACTOR	SC-N8	FUJI	1000000	4000	90
PLC	PLC	CS1H	OMRON	20	-	90
PG	PULSE GENERATOR	TS2622N71E11	TAMAGAWA	—	20	90

※1 マグネットコンタクターは、電気的耐久性を B10d として代用する(メーカー推奨)
※2 データ入手できない製品は、MTTFd=20 年、DC=90 と仮定する。
※3 近接センサーは、付属書 C-1 表の B10d を使用する。

機器の MTTFd の計算

近接センサー

B4 の MTTFd の計算	B10d=	20,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	0.5	※カバー開時のみ作動とする
nop=250×0.5×3,600/0.20＝2,250,000	一年の稼動時間 dop=	250	
MTTFd=20,000,000/(0.1×2,250,000)=88.8888889 年	1 サイクル時間 Tcycle=	0.2	※1 秒間に 5 回作動するとする

安全リレー

K9 の MTTFd の計算	B10d=	400,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=400,000/(0.1×2,500)＝1,600 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

マグネットコンタクター

MC1 の MTTFd の計算	B10d=	1,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop = 250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=1,000,000/(0.1×2,500)＝4,000 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

ホールドトゥラン回路の MTTFd の計算

チャンネル 1 の MTTFd の計算

MTTFd(ch1)=

$$\frac{1}{\left(\frac{1}{MTTFd(B4)}+\frac{1}{MTTFd(K10)}+\frac{1}{MTTFd(K9)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(MC1)}\right)}$$

$$=\frac{1}{\left(\frac{1}{88.8888889}+\frac{1}{20}+\frac{1}{1600}+\frac{1}{100}+\frac{1}{4000}\right)}$$

$$=\frac{1}{0.01125+0.05+0.000625+0.01+0.00025}$$

=13.86482 年

チャンネル 2 の MTTFd の計算

$$\text{MTTFd(ch2)}=\frac{1}{\left(\frac{1}{MTTFd(PG)}+\frac{1}{MTTFd(T1)}+\frac{1}{MTTFd(PLC)}\right)}$$

$$=\frac{1}{\left(\frac{1}{20}+\frac{1}{20}+\frac{1}{20}\right)}$$

$$=\frac{1}{0.05+0.05+0.05}$$

=6.666667 年

全体の MTTFd の計算

$$\text{MTTFd(ch1-ch2)}=\frac{2}{3}\times\left(MTTFd(ch1)+MTTFd(ch2)-\frac{1}{\frac{1}{MTTFd(ch1)}+\frac{1}{MTTFd(ch2)}}\right)$$

$$=\frac{2}{3}\times\left(13.864818+6.666667-\frac{1}{\frac{1}{13.86481802}+\frac{1}{6.666666667}}\right)$$

=0.666667 × (20.5314847 - 4.50197)

=10.68634 年

全体の MTTFd の分類条件 10 年≦MTTFd＜30 年により

システム全体の MTTFd は“MEDIUM”に分類されます。

DCavg の計算

DCavg=

$$\frac{\frac{DC(B4)}{MTTFd(B4)}+\frac{DC(K10)}{MTTFd(K10)}+\frac{DC(K9)}{MTTFd(K9)}+\frac{DC(K3)}{MTTFd(K3)}+\frac{DC(PLC)}{MTTFd(PLC)}+\frac{DC(MC1)}{MTTFd(MC1)}+\frac{DC(T1)}{MTTFd(T1)}+\frac{DC(PG)}{MTTFd(PG)}}{\frac{1}{MTTFd(B4)}+\frac{1}{MTTFd(K10)}+\frac{1}{MTTFd(K9)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(PLC)}+\frac{1}{MTTFd(MC1)}+\frac{1}{MTTFd(T1)}+\frac{1}{MTTFd(PG)}}$$

$$=\frac{\frac{0.9}{88.88888889}+\frac{0.99}{20}+\frac{0.99}{1600}+\frac{0.99}{100}+\frac{0.9}{20}+\frac{0.9}{4000}+\frac{0.9}{20}+\frac{0.9}{20}}{\frac{1}{88.8888889}+\frac{1}{20}+\frac{1}{1600}+\frac{1}{100}+\frac{1}{20}+\frac{1}{4000}+\frac{1}{20}+\frac{1}{20}}$$

$$=\frac{0.010125+0.0495+0.000619+0.0099+0.045+0.000225+0.045+0.045}{0.01125+0.05+0.000625+0.01+0.05+0.00025+0.05+0.05}$$

$$=\frac{0.20536875}{0.222125}$$

DCavg=0.92456387

DCavg の分類条件　90%≦DC＜99%により

DCavg は“MEDIUM”に分類されます。

排紙部ライトカーテン安全　－カテゴリ 3－　PLd

【安全機能】

・ ライトカーテンによって起動する STO－安全トルクオフ

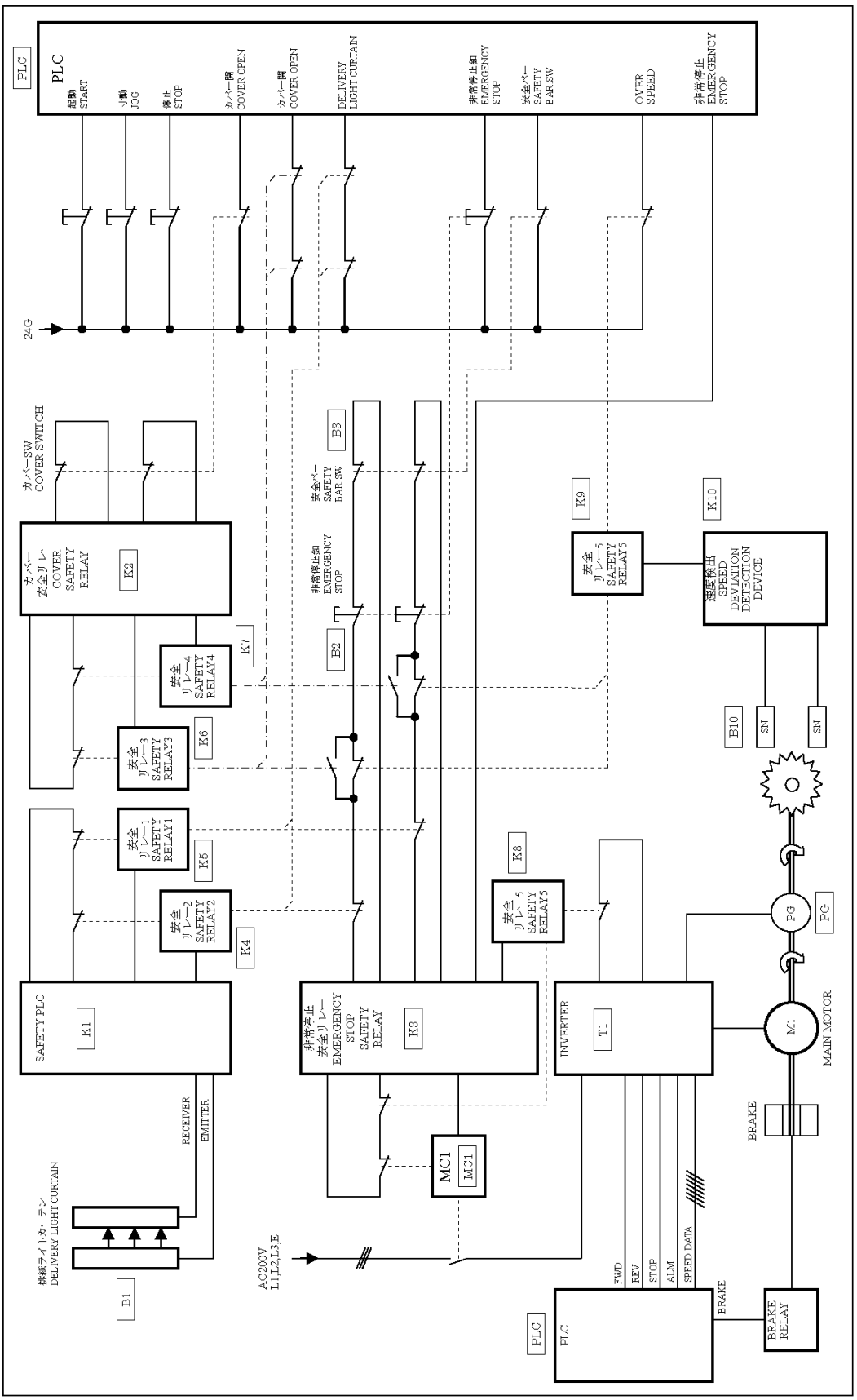
【機能説明】

・ 排紙部ライトカーテン B1 が作動した場合、セーフティ PLC K1 により検出される。
・ B1 作動を検出したセーフティ PLC K1 は安全リレーK4、K5 し非常停止リレーK3 によりインバーター電源 MC1 を遮断し、同時にインバーターT1 のフリーラン信号を K8 により起動し機械停止する。

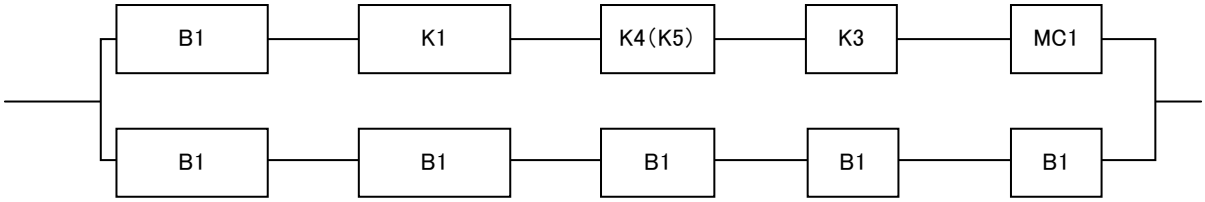
【設計特性】

・ 基本及び充分に実証済みの安全原則を守り、カテゴリＢの要求事項を満たす。
・ 排紙安全に関しては ISO 12643-2 6.7 Additional safeguarding methods for machine devices and components に従う。
・ ライトカーテンは EN954 カテゴリ４に適応するものである
・ 非常停止安全リレーモジュール K3 は EN 954 カテゴリ４に適応するものである。
・ 安全リレーは EN 50205 に適合した強制ガイド接点である（K6,7,8,9）
・ マグネットスイッチ MC1 は十分に実証済みの構成部品である。
・ インバーターT1 は十分に実証済みの構成部品である。

オフセット枚葉印刷機の安全性評価（回路図）



排紙安全部ブロック図
DELIVERY LIGHT CURTAIN



機器の信頼性データ
MTTFd and DC about parts.

ID	Part Name	Type	Manufacturer	B10d	MTTFd	DC(%)
B1	LIGHT CURTAIN	F3SJ-AM3P300	OMRON	100	-	99
K1	SAFETY PLC	NE1A-SCPU02	OMRON	100	-	99
K3	SEFETY RELAY	G9SA-301-P	OMRON	100	-	99
K4	SEFETY RELAY	G7SA-3A1B	OMRON	400000	1600	99
K5	SEFETY RELAY	G7SA-3A1B	OMRON	400000	1600	99
T1	INVERTER	VF-A7	TOSHIBA	20	-	90
MC1	MAGNETIC CONTACTOR	SC-N8	FUJI	1000000	4000	90
PLC	PLC	CS1H	OMRON	20	-	99

※1 マグネットコンタクターは、電気的耐久性を B10d として代用する(メーカー推奨)
※2 データ入手できない製品は、MTTFd=20 年、DC=90 と仮定する。

機器の MTTFd の計算

安全リレー			
K4(K5)の MTTFd の計算	B10d=	400,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=400,000/(0.1×2,500)=1,600 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

マグネットコンタクター			
MC1 の MTTFd の計算	B10d=	1,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop＝250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=1,000,000/(0.1×2,500)＝4,000 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

排紙安全回路の MTTFd の計算

チャンネル 1 の MTTFd の計算

MTTFd(CH1)=

$$\frac{1}{(\frac{1}{MTTFd(B1)}+\frac{1}{MTTFd(K1)}+\frac{1}{MTTFd(K4orK5)}+\frac{1}{MFFTd(K3)}+\frac{1}{MTTFd(MC1)})}$$

$$=\frac{1}{(\frac{1}{100}+\frac{1}{100}+\frac{1}{1600}+\frac{1}{100}+\frac{1}{4000})}$$

$$=\frac{1}{(0.01+0.01+0.000625+0.01+0.00025}$$

=32.38866 年

チャンネル 2 の MTTFd の計算

MTTFd(CH2)=

$$\frac{1}{(\frac{1}{MTTFd(B1)}+\frac{1}{MTTFd(K1)}+\frac{1}{MTTFd(K4orK5)}+\frac{1}{MFFTd(PLC)}+\frac{1}{MTTFd(T1)})}$$

$$=\frac{1}{(\frac{1}{100}+\frac{1}{100}+\frac{1}{1600}+\frac{1}{20}+\frac{1}{20})}$$

$$=\frac{1}{(0.01+0.01+0.000625+0.05+0.05}$$

=8.290155 年

全体の MTTFd の計算

$$\text{MTTFd(ch1-ch2)}=\frac{2}{3}\times\left(MTTFd(ch1)+MTTFd(ch2)-\frac{1}{\frac{1}{MTTFd(ch1)}+\frac{1}{MTTFd(ch2)}}\right)$$

$$=\frac{2}{3}\times\left(32.38866+8.290155-\frac{1}{\frac{1}{32.38866397}+\frac{1}{8.29015544}}\right)$$

=0.666667 × (40.67882 - 6.60066)

=22.71877 年

全体の MTTFd の分類条件 10≦MTTFd＜30 年により

システム全体の MTTFd は“MEDIUM”に分類されます。

DCavg の計算

DCavg=

$$\frac{\frac{DC(B1)}{MTTFd(B1)}+\frac{DC(K1)}{MTTFd(K1)}+\frac{DC(K4)}{MTTFd(K4)}+\frac{DC(K3)}{MTTFd(K3)}+\frac{DC(PLC)}{MTTFd(PLC)}+\frac{DC(MC1)}{MTTFd(MC1)}+\frac{DC(T1)}{MTTFd(T1)}}{\frac{1}{MTTFd(B1)}+\frac{1}{MTTFd(K1)}+\frac{1}{MTTFd(K4)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(PLC)}+\frac{1}{MTTFd(MC1)}+\frac{1}{MTTFd(T1)}}$$

$$=\frac{\frac{0.99}{100}+\frac{0.99}{100}+\frac{0.99}{1600}+\frac{0.99}{100}+\frac{0.9}{20}+\frac{0.9}{4000}+\frac{0.9}{20}}{\frac{1}{100}+\frac{1}{100}+\frac{1}{1600}+\frac{1}{100}+\frac{1}{20}+\frac{1}{4000}+\frac{1}{20}}$$

$$=\frac{0.0099+0.0099+0.000619+0.0099+0.045+0.000225+0.045}{0.01+0.01+0.000625+0.01+0.05+0.00025+0.05}$$

=0.92106

DCavg の分類条件 90%≦DC＜99%

DCavg は“MEDIUM”に分類されます。

非常停止回路　ーカテゴリ3ー　PLd

【安全機能】

・ 非常停止装置の作動による STOー安全トルクオフ

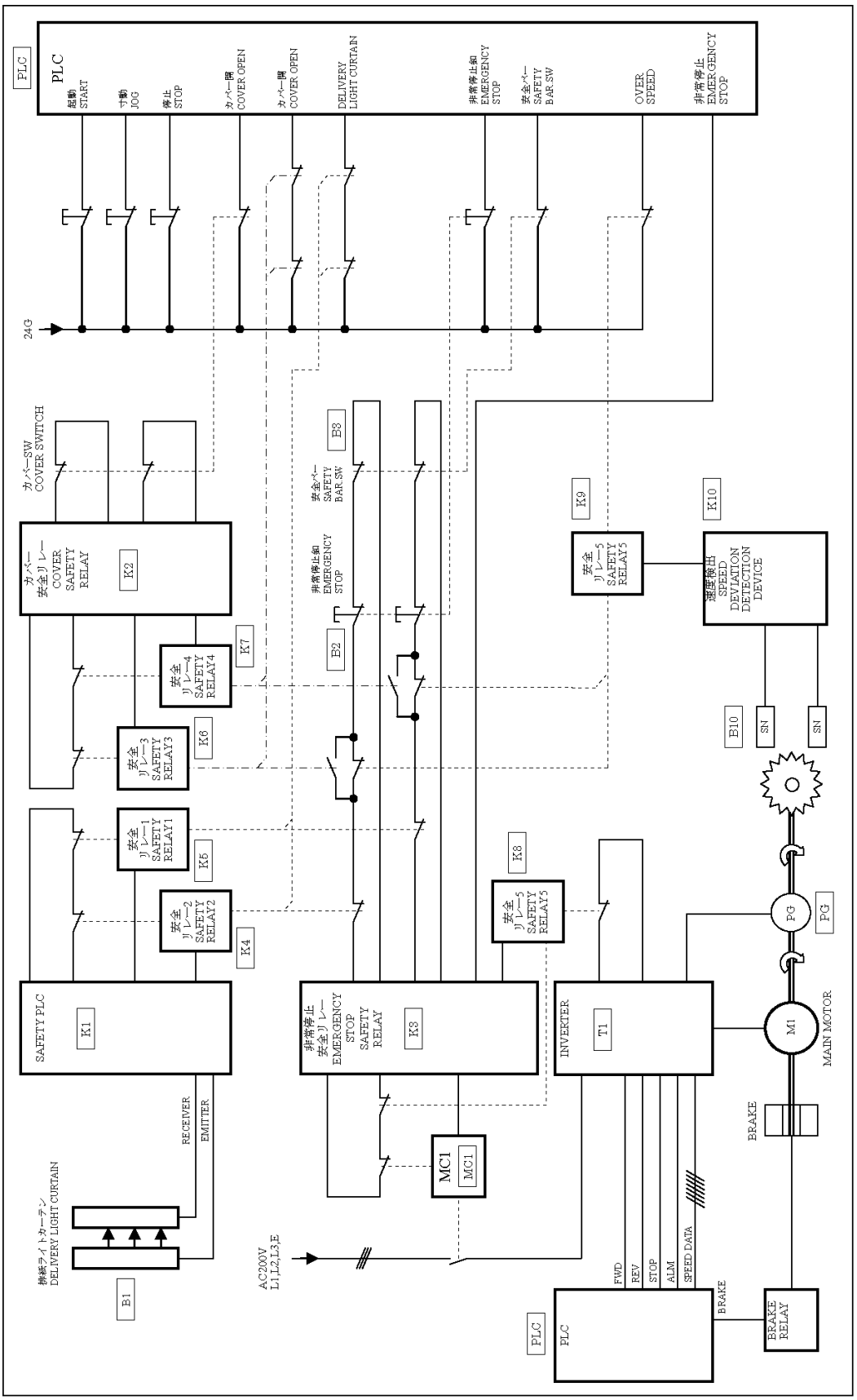
【機能説明】

・ 非常停止押しボタン B2 が作動した場合、非常停止安全リレーK3 により検出される。
・ B1 作動を検出したセーフティ PLC　K1 は安全リレーK4、K5 し非常停止リレーK3 によりインバーター電源 MC1 を遮断し、同時にインバーターT1 のフリーラン信号を K8 により起動し機械停止する。

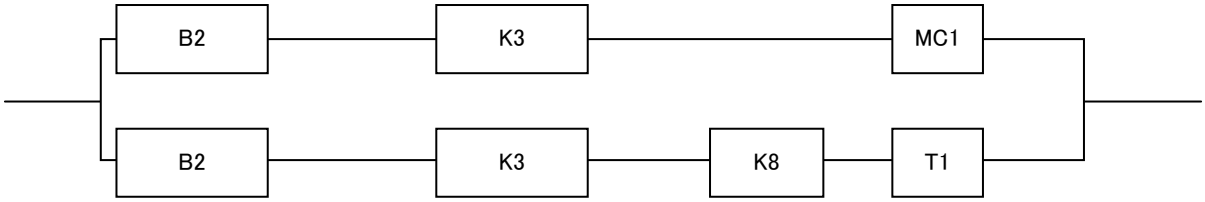
【設計特性】

・ 基本及び充分に実証済みの安全原則を守り、カテゴリＢの要求事項を満たす。
・ 非常停止押し機能は ISO 12643-1 10.2.3.1 Emergency stop の要求事項を満たす。
・ 安全バーは ISO 12643-1 6.4 Guarding in-running nips の要求事項を満たす。
・ 非常停止押しボタンスイッチ B2 は IEC 60204-1 に準拠した強制開離接点を持つ
・ 安全バーリミットスイッチは IEC 60204-1 に準拠した強制開離接点を持つ
・ 非常停止安全リレーK3 は EN 954 カテゴリ４に適応するものである
・ 安全リレーは EN 50205 に適合した強制ガイド接点である（K4、5、8、9）
・ マグネットスイッチ MC1 は十分に実証済みの構成部品である。
・ インバーターT1 は十分に実証済みの構成部品である。

オフセット枚葉印刷機の安全性評価（回路図）



非常停止部ブロック図
EMERGENCY STOP



機器の信頼性データ
MTTFd and DC about parts.

ID	Part Name	Type	Manufacturer	B10d	MTTFd	DC(%)
B2	EMERGENCY STOP P.B	XA1E-BV303R	IDEC	100000	400	99
K3	SEFETY RELAY	G9SA-301-P	OMRON	100	-	99
K8	SEFETY RELAY	G7SA-3A1B	OMRON	400000	1600	99
T1	INVERTER	VF-A7	TOSHIBA	20	-	90
MC1	MAGNETIC CONTACTOR	SC-N8	FUJI	1000000	4000	90

※1 マグネットコンタクターは、電気的耐久性を B10d として代用する(メーカー推奨)
※2 データ入手できない製品は、MTTFd=20 年、DC=90 と仮定する。

機器の MTTFd の計算

非常停止釦			
B2 の MTTFd の計算	B10d=	100,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=100,000/(0.1×2,500)=400 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

安全リレー			
K8 の MTTFd の計算	B10d=	400,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop=250×10×3,600/3600＝2,500	一年の稼動時間 dop=	250	
MTTFd=400,000/(0.1×2,500)＝1,600 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

マグネットコンタクター			
MC1 の MTTFd の計算	B10d=	1,000,000	
MTTFd=B10d/(0.1×nop)　nop=dop×hop×3,600/tcycle	一日の稼動時間 hop=	10	
nop＝250×10×3,600/3,600＝2,500	一年の稼動時間 dop=	250	
MTTFd=1,000,000/(0.1×2,500)＝4,000 年	1 サイクル時間 Tcycle=	3,600	※1 時間に 1 回作動するとする

非常停止回路の MTTFd の計算

チャンネル 1 の MTTFd の計算

$$\text{MTTFd(ch1)} = \frac{1}{\left(\frac{1}{MTTFd(B2)} + \frac{1}{MTTFd(K3)} + \frac{1}{MTTFd(MC1)}\right)}$$

$$= \frac{1}{\left(\frac{1}{400} + \frac{1}{100} + \frac{1}{4000}\right)}$$

$$= \frac{1}{(0.0025 + 0.01 + 0.00025)}$$

=78.43137 年

チャンネル 2 の MTTFd の計算

$$\text{MTTFd(ch2)} = \frac{1}{\left(\frac{1}{MTTFd(B2)} + \frac{1}{MTTF(K3)} + \frac{1}{MTTFd(K8)} + \frac{1}{MTTF(T1)}\right)}$$

$$= \frac{1}{\left(\frac{1}{400} + \frac{1}{100} + \frac{1}{1600} + \frac{1}{20}\right)}$$

$$= \frac{1}{(0.0025 + 0.01 + 0.000625 + 0.05)}$$

=15.84158 年

全体の MTTFd の計算

$$\text{MTTFd(ch1+ch2)} = \frac{2}{3} \times \left(MTTFd(ch1) + MTTFd(ch2) - \frac{1}{\frac{1}{MTTFd(ch1)} + \frac{1}{MTTFd(ch2)}} \right)$$

$$= \frac{2}{3} \times \left(78.43137 + 15.84158 - \frac{1}{\frac{1}{78.43137255} + \frac{1}{15.84158416}} \right)$$

=0.666667 × (94.27296 - 13.17957)

=54.06226 年

全体の MTTFd の分類条件　30 年≦MTTFd＜100 年により

システム全体の MTTFd は“HIGH”に分類されます。

DCavg の計算

$$DCavg=\frac{\frac{DC(B2)}{MTTFd(B2)}+\frac{DC(K3)}{MTTFd(K3)}+\frac{DC(K8)}{MTTFd(K8)}+\frac{DC(MC1)}{MTTFd(MC1)}+\frac{DC(T1)}{MTTFd(T1)}}{\frac{1}{MTTFd(B2)}+\frac{1}{MTTFd(K3)}+\frac{1}{MTTFd(K8)}+\frac{1}{MTTFd(MC1)}+\frac{1}{MTTFd(T1)}}$$

$$=\frac{\frac{0.99}{400}+\frac{0.99}{100}+\frac{0.99}{1600}+\frac{0.9}{4000}+\frac{0.9}{20}}{\frac{1}{400}+\frac{1}{100}+\frac{1}{1600}+\frac{1}{4000}+\frac{1}{20}}$$

$$=\frac{0.002475+0.0099+0.000619+0.000225+0.045}{0.0025+0.01+0.000625+0.00025+0.05}$$

$$=\frac{0.058219}{0.063375}$$

DCavg=0.918639

DCavg の分類条件　90%≦DC＜99%により
DCavg は“MEDIUM”に分類されます。

(5)考察

まず感じたことは機能説明不足である。

電気図面が複雑であったことも理解し難かった原因と思われる。

図面は製品図面とは別の正確且つ簡易的な図面で機能ポイントが抑えられたものを準備する必要があり、機能説明はBGIAレポートと同等かそれ以上のものが必要である。

次にB10d､DCの算出方法であるが基本的に装置メーカーからのレポートがあれば対応が容易であることを実感した。これは製品がメーカーで対応していることを意味し、同時にコストアップが懸念される。

メーカーからの書類については、規定書式は無いとのことからカタログ記載の内容程度で良いのかメーカーからのデータシートを必要とするのかは明確ではない。逆にメーカーレポートが無い製品については認証不可能では無いがB10d、MTTFd、DCの数値を証明できる準備と説明が必要となる。

インバーターのDC算出にあるようにISO 61800-5準拠の冗長性があり、パルスブロック機能を持ったインバーターが推奨されるが現状では国内では対応機種が少ない。

また、改めて規格ISO 12643の解釈の重要性を感じた。

ホールドトゥラン制御での防護回路はPLrdであることを認識していたが、制御回路はPLrbとのことから速度制御についてもbと解釈していたが間違いであることを指摘された。

以上のことを踏まえ、今回の検証結果によるポイントは、

① 理解し易い図面であること

② 充分な機能説明があること

③ 費用対効果を考慮したPL対応製品の使用

である。

上記３点を踏まえ準備することが認証への近道と考える。

4.2.2 WEB オフセット輪転印刷機の安全性評価(B グループ)

(1)BG への提出レポート

安全カバー停止回路　Cat３　PLd

安全カバー位置につての冗長回路をハードワイヤーと PLC とで構成する内容である。

安全カバーを開くとメインモーター停止する。

機械が低速(この場合 100rpm 以下)の場合は、停止回路はバイパスされるので安全カバーを開いても停止しない。

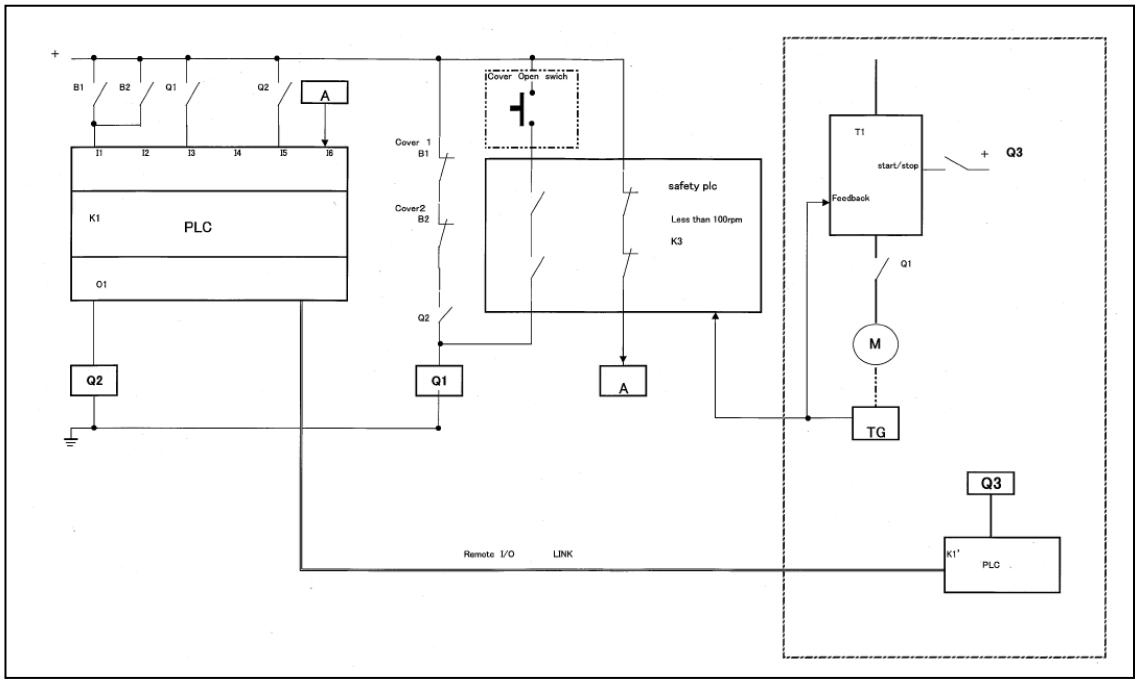
Position monitoring of a moveable guard (STO) - Category 3 - PL d

Figure:

Redundant position monitoring of a moveable guard employing diversity in its technical implementation (electromechanical and programmable electric).

When a safe cover opens, a main drive stops. The motor does not stop even if the open a cover if a machine turn is low (less than 100rpm).

WEB オフセット輪転印刷機の安全性評価(回路図)



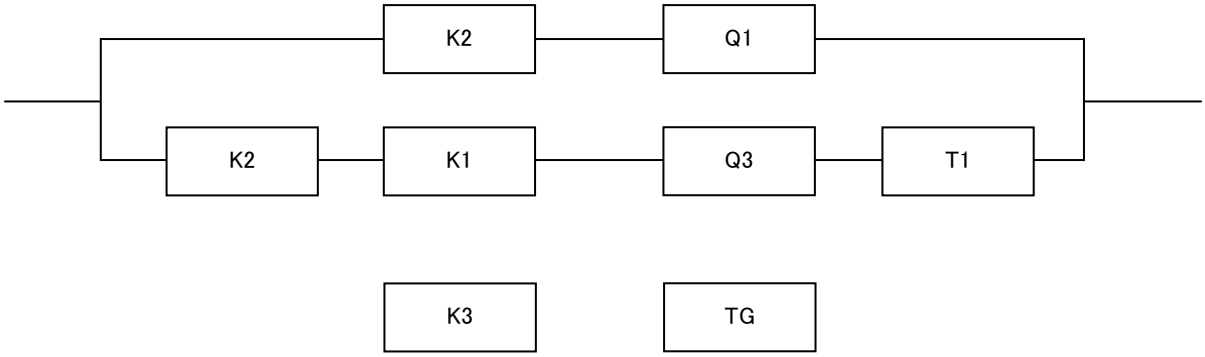
保護装置の安全停止機能：

安全カバーの動作は、リミットスイッチにて行なわれます。

安全カバーが開くと停止が機能します（安全なトルク）。

Safety function:

Safety-related stop function, initiated by a protective device:
Actuation of the limit switch when the moveable guard (safety guard) is opened initiates the safety function STO (safe torque off).



Block-diagram Position monitoring of a moveable guard (STO)

【機能】

安全カバーが開くとリミットスイッチ B1、B2 が作動し、リレーQ1 が OFF し回転中のモーターM は、停止する。

モーター回転は、安全 PLC により 100rpm 以下かの速度検知を行うため、カバーが開いてもモーターは、回転可能となる。

【設計】

モーター動作の Q1 リレーは、安全カバーB1、B2 のリミットスイッチによりオフするが、PLC もモニターしているので PLC からも停止可能。

T1 インバーターの停止は、Q3 によって行う。

この冗長により停止カテゴリ０、１が可能。

これは、カテゴリ３　PL レベルは d を満足する。

Functional description:

When safety cover (B1 or B2) is opened while the motor is running (the machine is operated), relay Q1 becomes OFF and the machine drive motor M stops.
Since the safety PLC detects the speed of motor M falling below 100 rpm, the motor can run even if the cover is opened. Safety cover open switch also serves as open/close drive switch for cleaning purpose.

Design features:
Motor drive relay Q1 becomes OFF by B1 or B2 limiting operation, but since PLC monitors the contact, it can stop with PLC.
Inverter T1 is activated and stopped with Q3.
Redundancy is provided for the inverter with stop category 0 and 1.
This SRP/CS satisfies category 3, performance level d.

【計算】

故障の除外は、2個の安全カバーのリミットスイッチB1、B2によりQ1、Q3を直接開閉する。

Q1、Q3のB10dは、誘導負荷2,000,000を使用。

50%の故障が危険側と考えるとB10dは2倍となる。

Q1、Q3のMTTFdは、3,333年よって100年のMTTFdとなる。

PLC　K2は、安全認証品より100年、PLC　K1　は、20年、インバーターT1はMTTFd　10年を使用する。

1チャンネルのK2、Q1の組み合わせは、MTTFd97.09年。

2チャンネルの組み合わせ、K2、K1、Q3及びT1はMTTFd6.24年。

平均化より、両方に適応されるMTTFdは64.98年でMTTFd　hight　を得る。

DC_{avg}:

PLC　K2のDCは99%、PLC　K1は60%。安全リレーQ1、Q3は強制ガイド接点付きで

DC　99%。インバーターT1は60%を得て、結果DC　64.71%　Lowを得る。

CCF　75ポイント

制御要素の組合せは、MTTFd　hight（64.98年）とDcavg　low（64.71%）でカテゴリ３と一致する。これは、毎時1.84E-7の危険平均確率になる。

これは、PL dと一致する。

Calculation of the probability of failure:
$MTTF_d$: fault exclusion is possible for the electrical contact of the cover switch B1 and B2 with direct opening contact. For the contactors Q1 and Q3, the B_{10} value under inductive load (AC3) corresponds to an electrical life of 2,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_d$ of 3,333 years for Q1 and Q3. An MTTF value of 100 years [M] is substituted for the PLC (K2), an MTTF value of 20 years [M] is substituted for the PLC (K1), and an MTTF value of 10 years [M] is substituted for the Frequency inverter (T1).
The combination of K2 and Q1 results in an $MTTF_d$ of 97.09 years for the first channel; K2, K1, Q3 and T1 contribute to an $MTTF_d$ of 6.24 years in the second channel. Altogether, the $MTTF_d$ value symmetrized over both channels is 64.98 years per channel (high).
DC_{avg}: The *DC* of 99% for the PLC (K2), and the *DC* of 60% for the PLC (K1). The *DC* of 99% for the safety relay Q1 and Q3 is derived from readback via mechanically linked contact elements. The *DC* of 60% for the frequency inverter T1. Averaging thus results in a DC_{avg} of 64.71% (low).
Adequate measures against common cause failure (75 points)

The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ (64.98 years) and low DC_{avg} (64.71%). This results in an average probability of dangerous failure of 1.84E-7 per hour. This corresponds to PL d.

(2)BG からの指摘

これは回転印刷機の特殊な機能を記述していると推測する。

安全機能の使用に明記されなければならない。生産技術の観点から折り畳み機が生産の開始時に、人の介入が必要とされる場合（例えば不良品の撤去）、インターロック付き保護装置を8m/min(シリンダーの付随的速度)の速度範囲まで、機械の運転を中断することなく開くことができる。その場合、同時にすぐ近くに保護装置につながるスイッチが動作されることが条件となる。

保護装置を開ける際に、スイッチを動作すると危険な動きは最短で停止状態に導かれなければならない。これは保護装置が複数あり、その上位にここの保護装置を監視する駆動スイッチがある場合でも適用できる。

安全な減速は最低 PLr=d に合致しなければならない。安全に減速された速度とは、タコジェネレータの単一故障が、タッピング動作での許容されない速度に達しないことを意味する。この例では、タコジェネレータの信号が調整量及び監視回路用として使用されている(K2 へのフィードバック)。タコジェネレータ信号の単一故障においてタッピング動作の安全な速度は保障されていない。

さらに指摘点として、通常の PLC K1 が単独で、安全な速度の実現を担っていることで、これは要求地及び直接 K2 により読み取られることで監視の役割も果たしている。

この回路図からは、どの安全機能が定量化されるのか明確でない（推測では、安全な速度に関するものと思われる)。

残念ながら安全リレーK2 に関する情報が欠如している。

故障検知の方策があれば、PLC K1 には DC=60%しか適用できない。インバーターの T1 についても同様である。この例では診断方策が記述されていない。

- Ich vermute hier wird eine besondere Funktion einer Rotationsdruckmaschine beschrieben. Dies sollte aus der Spezifikation der Sicherheitsfunktion deutlich hervorgehen. Ist aus produktionstechnischen Gründen am **Falzwerk in der Anlaufsphase** der Produktion ein Zugriff erforderlich (z.B. Entnahme von Fehlprodukten), so ist es zulässig, dass die verriegelte Schutzeinrichtung bis zu einer Geschwindigkeit von 8m/min (Tangentialgeschwindigkeit der Zylinder) ohne Unterbrechung des Maschinenlaufs geöffnet werden kann, solange gleichzeitig ein in unmittelbarer Nähe der Schutzeinrichtung angeordneter Taster betätigt wird. Nach Loslassen des Tasters bei geöffneter Schutzeinrichtung muss die gefahrbringende Bewegung auf kürzestem Weg zum Stillstand kommen. Dies ist auch für mehrere Schutzeinrichtungen zulässig, solange für jede Schutzeinrichtung der zugeordnete Taster betätigt wird. Die sicherreduzierte muss mindestens dem PLr=d entsprechen. Sicher reduzierte Geschwindigkeit bedeutet, dass ein Fehler des Tachogenerators nicht zu einer

unzulässigen Geschwindigkeit im Tippbetrieb führen darf. In dem Beispiel wird das Tachosignal sowohl als Regelgröße als auch für den Überwachungskanal genutzt (Feedback zu K2). Bei einem Fehler des Tachosignals wäre die sichere Geschwindigkeit im Tippbetreib nicht sichergestellt.
Ferner muss darauf hingewiesen werden, dass die Standard SPS K1 alleinig für die Realisierung der sicheren Geschwindigkeit verantwortlich ist, da sie sowohl den Sollwert bildet als auch die mittelbar durch das Zurücklesen von K2 für die Überwachung zuständig ist.
Aus dem Blockschaltbild geht nicht eindeutig hervor, welche Sicherheitsfunktion quantifiziert wurde. (Ich nehme an, es handelt sich um die sichere Geschwindigkeit).

- Leider liegt keine Information bzgl. dem Sicherheitsrelais K2 vor.
- Für die SPS K1 kann nur ein DC=60% vergeben werden, wenn Maßnahmen zur Fehlererkennung ergriffen wurden. Das gleiche gilt für den Umrichter T1. In dem Beispiel sind die Diagnosemaßnahmen nicht beschrieben.

(3) BG との討論内容

- BG：これは、何について評価するかが明確ではなかった。
- 委員：回路目的を説明
  WEB 機は大型なので、PLC リンクシステムを使用する場合が多い。
  この場合、1 つの PLC とみなして良いか？
  また、機械速度が低い時、カバーを開けても停止させないバイパス回路は、
  モーターPG を使用して PLr を達成できるか？である。
- BG：内容は、分かるがまず説明が不足である。
  安全回路の仕様があるはず。これを十分に記述して欲しい
  PLC のリンクは、どういうものかが不明である。十分データが保証されているか？など説明の記述が欲しい。
  速度検出は、PG で行なっているが、単一故障を検出できない。
  MTTF d の計算についても、根拠となるデータがない。
- 委員：PLC リンク詳細説明については、了解。
  PG の故障検出だが、2 出力あるので可能である。診断率は上げることができる。
- BG：PG の故障検知が可能なら、その動作を記述して欲しい。
  文面には、何も記述がないので、もっと詳しく記述して欲しい。
  停止のバイパスは、その後どうなるのか？ また、スイッチはなにか？
- 委員：カバー開閉のインターロックである。カバーが開いている時のみバイパス可能としている。
  ＊この後、速度制限と寸動速度制限の話や、カバーを開くスイッチと起動ボタンの関係など操作面でどういう動きになるのか？というシステム的なことになった。結局、バイパス回路単独の検証では無理と理解した。周辺を合わせた安全性を説明するべきと理解した。

(4) 修正レポート

安全カバー停止回路

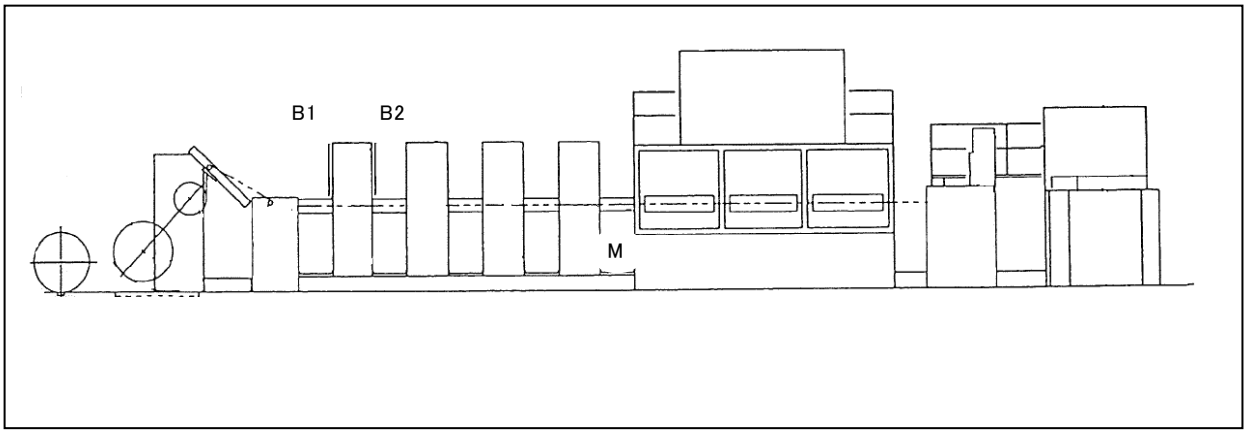


図 4.3 Web オフセット輪転印刷機

【概要】

印刷ユニットのカバーは、機械が運転中（安全速度以上）で開けると主原動モーターを停止させて、機械停止を行う。

また、ローラーの洗浄や保守のため、安全速度以下では、安全カバーが開いても主原動モーターは、動作可能である機能が要求される。

本回路例は、停止回路とそのバイパス回路の PL を診断しようとするものである。

停止回路の安全要求は、カテゴリ３　PLrd

ミューティングは､印刷ユニットには､停止ボタンがあることからカテゴリ 2　PLb とした。

（機械速度制限は、別途 EN 1010-1 で要求あるため除外）

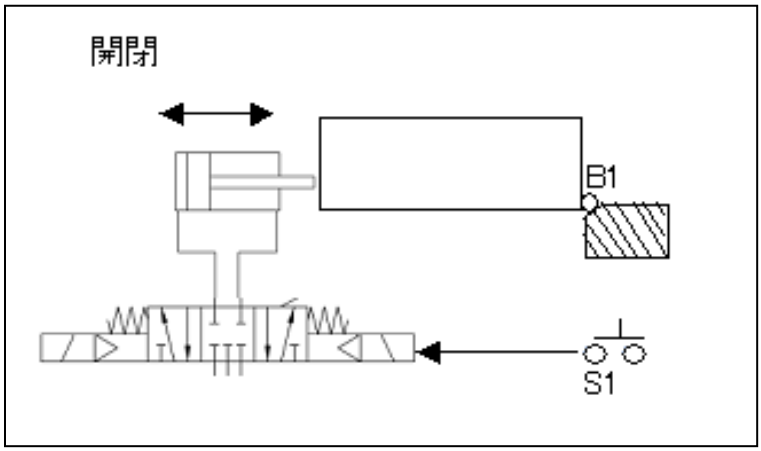
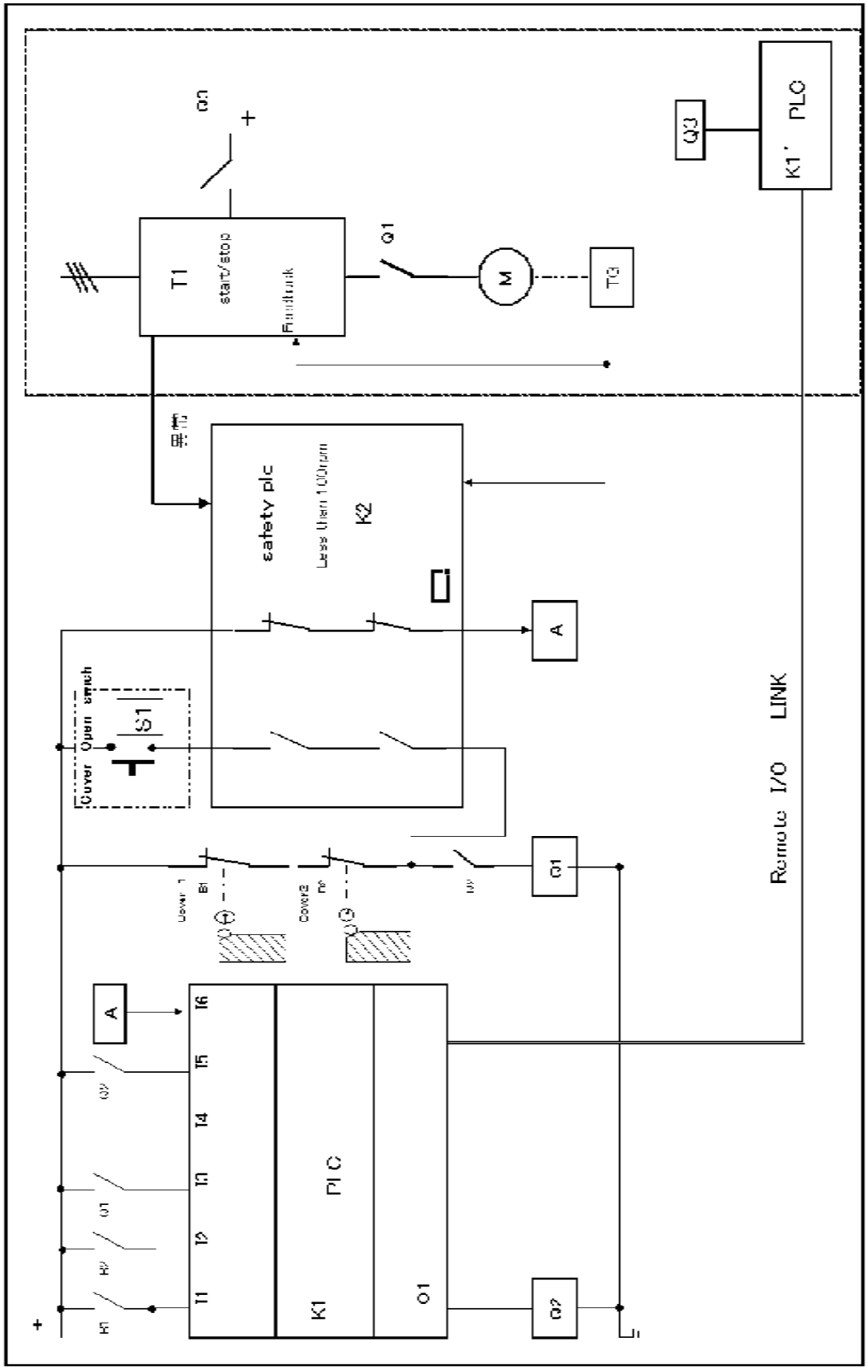
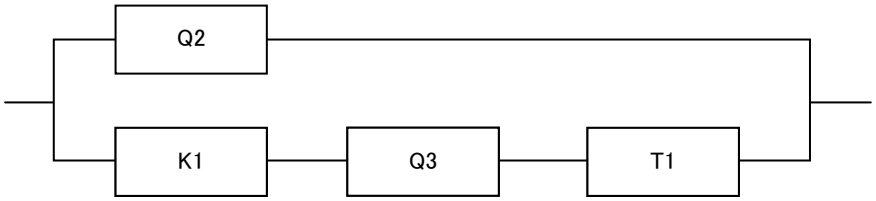


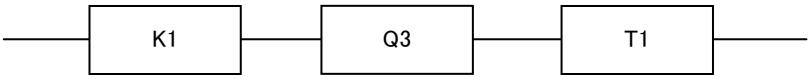
図 4.4 安全カバー動作構成

WEB オフセット輪転印刷機の安全性評価（回路図）





安全カバー停止ブロック



停止ミューティングブロック

【安全機能】

・ 保護装置によって起動する安全関連停止機能：

安全ガードが開くことで安全機能 STO－安全トルクオフする。

・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。

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。

【安全機能の説明】

印刷ユニットは、安全カバー（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からなる位置スイッチ B1/B2 が検知し、PLC　K1 が評価する。

PLC　K1 は、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 及び Q2 を作動させる。異常検出のために、全ての位置スイッチの状態を第 2 接点が制御を主目的とする標準 PLC K１に入力される。

異常の場合、PLC　K1 と独立して接触器 Q1 及び Q2 を OFF させることができる。

Q1 及び Q2 の異常は、PLC　K1 で検出される。

PLC と PLC を接続するリモートバスは、信号の伝達エラーを予防または、検知可能なシステムをとっている。伝達エラーは、データの損失、異常データの挿入、伝達順序の誤り、伝送データの崩れがある。これらは、ID の付加、CRC チェック、サムチェックなどの技術で防止されている。さらに、伝達遅れに関しては、応答時間監視、応答メッセージ確認を行い防止している。これらの、監視により異常が検知された場合は、各 PLC の出力は、安全側論理に切り替わる安全対策を採っている。

B1/B2 は、強制乖離機構のリミットスイッチであるため、閉状態で故障はない。

構成部品の故障の場合に安全機能が維持される。

【ミューティング】

モーターPG により機械速度を監視する。モーター用インバーターは、PG の 2 つのパルスを監視している。また、PLC　K2 においても PG から送られる 2 つのパルスを監視している。PG から出される 2 つのパルスは、９０度位相差を持って出力されておりその位相差の論理を判別することで故障検知機能を達成させることができる。

これにより、PG の故障は、検知される。モーター速度が安全速度以下になると、安全速度検出器 K2 が検出し、内部安全リレーを ON にする。

安全速度以下でも、安全カバーリミットが働くとモーターは、停止する。

安全カバーを動作させるスイッチ S1 によって安全カバーを開けることによって、安全速度以下でのモーター停止をミューティングできる。

速度とスイッチの 2 重安全である。

【設計の特徴】

強制乖離機構のリミットスイッチの使用

（IEC 60947-5-1　付属書 L による機械的に連結した接点）

安全速度検出ユニットの採用

（ISO 13849-1　PLd 認証取得品）

リミットスイッチの作動のために保護装置の安定した配置。

リミットスイッチへの配線は、別々に配線または保護されている。

【故障確率計算】

機器データ及び計算は、計算書参照。

機能ブロック図より、MTTFd の算出を行う。

チャンネル I

故障の除外は、2 個の安全カバーのリミットスイッチ B1、B2 により Q1 を直接開閉する。

Q1 の B10d は、誘導負荷 2,000,000 となる。

Q1 の MTTFd は、3,333 年よって、チャンネル 1 は 100 年の MTTFd となる。

チャンネル 2

汎用 PLCK1 は、メーカーからのデータがないので、付属書より 10 年を採用する。

リレーQ3 は、電磁接触器で、B10d 2,000,000 より MTTFd 3,333 年となる。

汎用 PLCK1 は、メーカーからのデータがないので、付属書より 10 年を選択。

インバーターT1 は、メーカーからのデータがないので、付属書より 10 年を選択よって、

チャンネル 2 の MTTFd は、5 年となる。

平均化

安全機能ブロック図の平均化は、規格書からの計算で行う。

上記からの計算結果より、66 年となり、MTTFd hight を得る。

【ミューティング】

PGは、付属書より10年を選択し、K2は安全モジュールより100年となる。

カバー開閉スイッチは、付属書と稼動より計算すると、83年となり総合的には、8年となり、MTTFd　Low　を得る。

DC_{avg}:

PLC　K2のDCは、安全PLCでメーカーデータより99%。

PLC　K1は、規格書より60%を使用。

安全リレーQ1、Q2、Q3は強制ガイド接点付きで規格書より　DC　99%。

インバーターT1は、規格書より60%を使用。

結果DC　60%　Lowを得る。

【部品データ】

Tcycle：操作の時間間隔　3600秒/回　3600秒

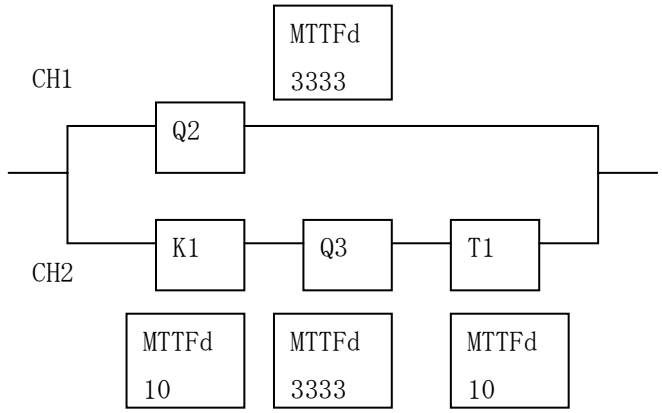
Hop　：一日の稼動時間　20時間/日　20時間

Dop　：年間の稼動時間　300日/年　300日

No	記号	名称	メーカー	型式	B10d	MTTFd	DC	他
1	B1	リミットスイッチ	オムロン	D4N	20,000,000	33333	99	ISO 13849-1：2006 Annex C
2	B2	リミットスイッチ	オムロン	D4N	20,000,000	33333	99	ISO 13849-1：2006 Annex C
3	Q1	コンタクタ	富士電機	SC7	2,000,000	3333	99	ISO 13849-1：2006 Annex C
4	Q2	安全リレー	オムロン	G7S	2,000,000	3333	99	ISO 13849-1：2006 Annex C
5	Q3	安全リレー	オムロン	G7S	2,000,000	3333	99	ISO 13849-1：2006 Annex C
6	S1	押しボタン	富士電機	AH22	100,000	83	60	ISO 13849-1：2006 Annex C
7	K1	PLC	オムロン	CJ1		10	60	ISO 13849-1：2006 Annex C
8	K2	安全PLC	オムロン	G9SX		100	99	メーカーデータ
9	TG	エンコーダー	多摩川	OIH		10	60	ISO 13849-1：2006 Annex C
10	T1	インバーター	富士電機	VG7S		10	60	ISO 13849-1：2006 Annex C

MTTFd

カバー



CH1

$$3333 = \frac{1}{1/Q2} = \frac{1}{1/3333}$$

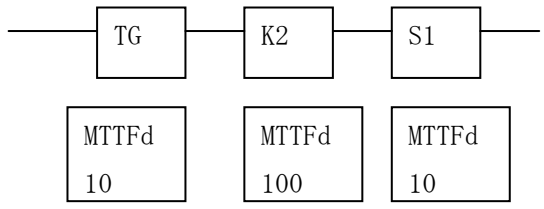
CH2

$$6.65 = \frac{1}{1/k1+1/Q3+1/T1} = \frac{1}{1/20+1/3333+1/10}$$

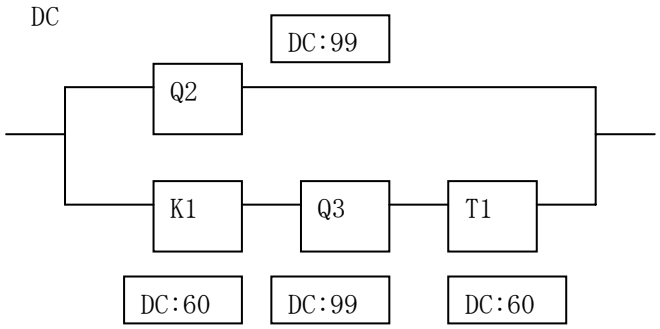
$$66.7 = 2/3\ (\ CH1+CH2-\ \frac{1}{1/CH1+1/ch2}\ )$$

$$= 2/3\ (\ 100+6.65-\ \frac{1}{1/100+1/6.65}\ )$$

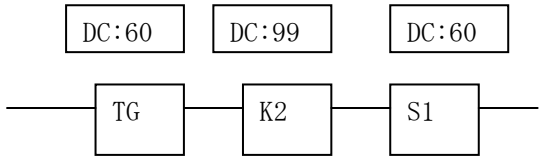
ミューティング



$$8 = \frac{1}{1/TG+1/k2+1/S1} = \frac{1}{1/10+1/100+1/10}$$



$$60\% = \frac{0.99/3333 + 0.6/10 + 0.99/3333 + 0.6/10}{1/3333 + 1/10 + 1/3333 + 1/10}$$



$$62\% = \frac{0.6/10 + 0.99/100 + 0.6/10}{1/10 + 1/100 + 1/10}$$

【結果】

＊CCF 評価は、今回のレポートでは除く。

安全回路部は

MTTFd　:　Hight Dcavg：Low となり PLr d の要求を満たす。

ミューティング

MTTFd　：Low　Dcavg：Low となり PLrb の要求を満たす。

(5) 考察

修正した回路と説明文は、まだ不足感がある。

記述とバックデータの説明不足は感じている。

BG より指摘された点は、十分理解したが安全設計思想を根拠を持って記述するのは難しい。また、分かりやすく説明すべきなので、構造などの絵を使うなど工夫はしたかったが、時間や絵の権利の問題もあって割愛した。

少なくとも、安全設計仕様書は作成しておかなければならない。

サンプルで今回作成したが、ねらいがぼけてしまった感じがある。

レポート作成の書式がないと書きづらい。

今回 BG のサンプル書 BGIA Report 2/2008e を参考にできたのが助かった。

4.2.3 断裁機のバックゲージ部の安全性評価（C グループ）

(1) BG への提出レポート

C グループでは、PLd と PLe の２つの回路案について評価を行った。

それぞれ和文と英文があり、①～④の章分けで記載した。

① PLd 回路案の和文

② PLe 回路案の和文

③ PLd 回路案の英文

④ PLe 回路案の英文

現状の断裁機の PLr は PLd で良いと思われるが、会社の方針、設計者の考え方、また、将来的に、機械の高速化、大型化に伴って PLe に対応しなければならない可能性があり、PLd の回路例の他、PLe で設計する場合の一例も挙げてみた。

① 断裁機のバックゲージ部の PL 評価について Cat.3 PLd

1)概要

バックゲージとは、製本時に紙を断裁する際、所定の寸法で切断するための紙揃えの当てである。裁断したい寸法の場所にバックゲージを移動させ、切りたい紙などをバックゲージに当てて紙などを揃えて、ナイフスイッチを押して、それを切るというのが裁断工程である。本評価では、裁断機のうちバックゲージ部の PL 評価を行う。

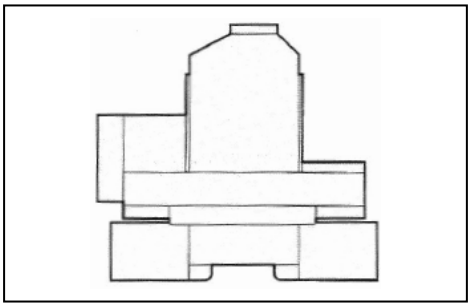
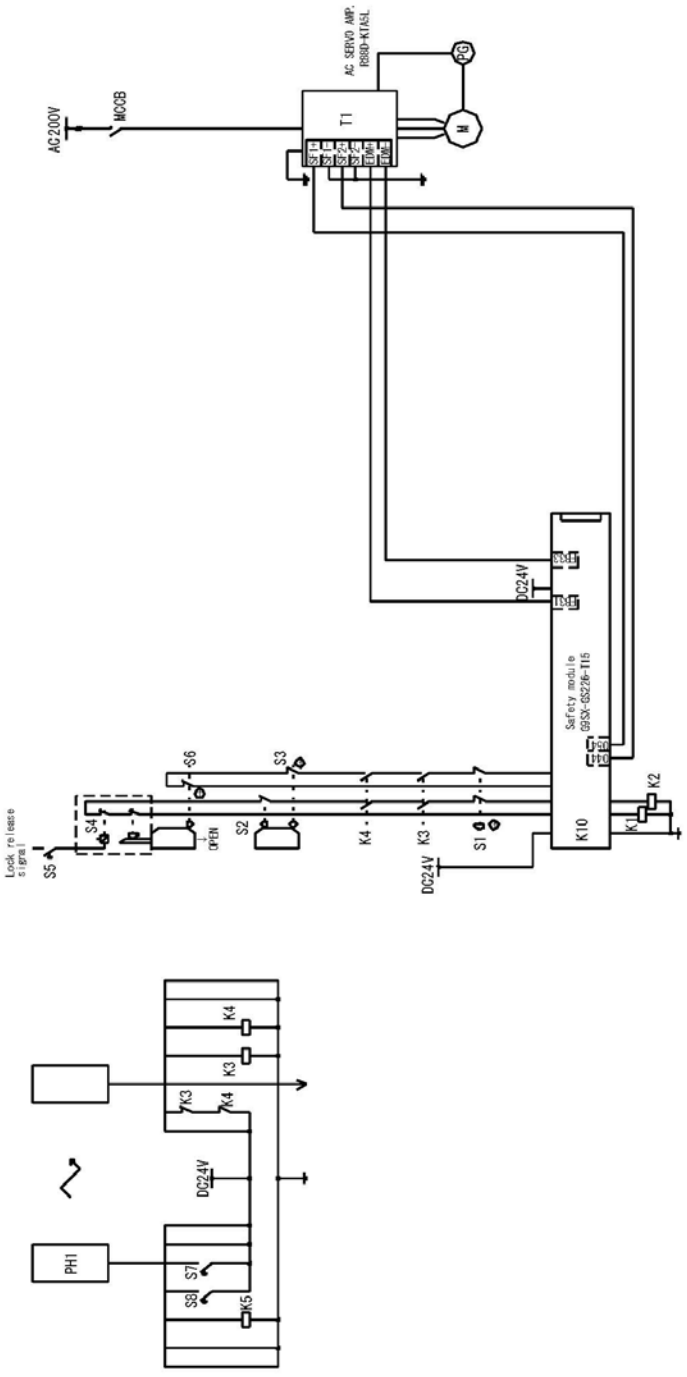


図 4.5 断裁機

断裁機（回路図／PLd）


AC200V
MCCB
T1
AC SERVO AMP.
R88D-KTA5L
PG
M
DC24V
Safety module
G9SX-GS226-T15
K10
K1
K2
S1
S2
S3
S4
S5
S6
K4
K3
OPEN
Lock release signal
PH1
S7
S8
K5

2)安全機能

保護装置によって起動する安全関連停止機能

A) ライトカーテン

ライトカーテンが人体を検出すると、STO 機能によりバックゲージのモーターを停止させる。

B) 非常停止スイッチ

非常停止スイッチが押されると、STO 機能によりバックゲージのモーターを停止させる。

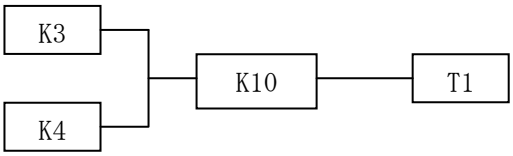
C) 可動式ガード

可動式ガード（安全ガード）が開くと、STO 機能によりバックゲージのモーターを停止させる。

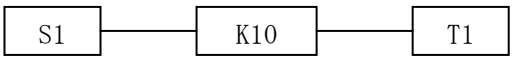
D) ロック式安全ガード

可動式ガード（安全ガード）が開く、または、安全ガードが解錠されると、STO 機能によりバックゲージのモーターを停止させる。

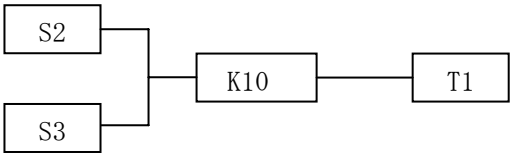
A) ライトカーテン



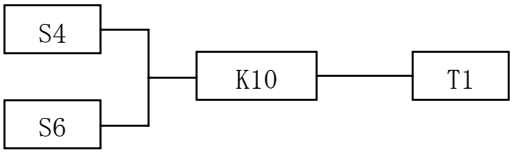
B) 非常停止スイッチ



C) 可動式ガード



D) ロック式安全ガード



3)機能の説明

A) ライトカーテン

ライトカーテンの PH1 が物体を検出する、または、自己診断機能によりライトカーテン自体の不具合を検出すると、異常接点 K3/K4 が開き、AC サーボドライブ T1 は、安全モジュール K10 からの STO 出力 044/054 により安全トルクオフされる。

B) 非常停止スイッチ

非常停止スイッチが操作され接点が開いたことを安全モジュール K10 が検出すると、AC サーボドライブ T1 は、044 と 054 により安全トルクオフされる。

C) 可動式ガード

可動式ガード（例：安全ガード）が開いたことを 2 位置スイッチ S2／S3 が検出すると、AC サーボドライブ T1 は、安全モジュールからの STO 出力 044／054 により安全トルクオフされる。

D) ロック式安全ガード

ロック式安全ガードの解錠検出接点 S4 が開くか、または、リミットスイッチ S6 により安全ガードが開いたことを検出すると、AC サーボドライブ T1 は、安全モジュールからの STO 出力 044／054 により安全トルクオフされる。

4)設計特性

・基本及び十分に実証済みの安全原則を守り、カテゴリ B の要求事項を満たす。
・位置スイッチ S2/S3 への配線は、別々に配線または保護されている。
・位置スイッチ S4/S6 への配線は、別々に配線または保護されている。
・位置スイッチ作動のために保護装置の安定した配置を確保する。
・非常停止スイッチ S1 は、EN ISO 13850 に対応する。
ポジションスイッチ S3/S6 は、IEC 60947-5-1　付属書 K による強制開離機構を有する。
・安全モジュール K10 は、EN954-1(カテゴリ 4)と IEC/EN61508(SIL3)を満たす。
・AC サーボアンプ T1 は PLd に適合する。
・AC サーボアンプ T1 の不具合は安全モジュール K10 により検出され、044／054 の出力を切る。安全ユニット K10 の故障は K10 自身の機能により検出される（プロセスによる故障検出）。

5)推定故障率の計算

各部品の MTTFd と DC

No.	ID	Name	Manufac -turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	G9SX-GS226	--	100	99
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	99

1. K3/K4

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd1 ＝ B10d / 0.1×Nop ＝ 20,000,000 / 0.1×980 ＝ 204082 years

DC1 = 99%

2. K10 MTTFd2 ＝ 100 years DC2 = 99%

Manufacturer spec.

3. T1 MTTFd3 ＝ 85 years DC3 = 87%

Manufacturer spec.

4. S1

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd4 ＝ B10d / 0.1×Nop ＝ 100,000 / 0.1×980 ＝ 1024 years

DC4 = 99%

5. S2/S6

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) ＝ 1960

MTTFd5 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×1960 ＝ 102041 years

DC5 = 99%

6)PL 計算結果

PL 判定結果

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	46	0.925	3	65＜	d
B	44	0.928	3	65＜	d
C/D	46	0.925	3	65＜	d

MTTFd

A)

$$\frac{1}{1/\mathrm{MTTFd1} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{1}{1/204082 + 1/100 + 1/85} \fallingdotseq 46 \text{ year}$$

B)

$$\frac{1}{1/\mathrm{MTTFd4} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{1}{1/1024 + 1/100 + 1/85} \fallingdotseq 44 \text{ year}$$

C/D)

$$\frac{1}{1/\mathrm{MTTFd5} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{1}{1/102041 + 1/100 + 1/85} \fallingdotseq 46 \text{ year}$$

DCavg

A)

$$\frac{\mathrm{DC1/MTTFd1+DC2/MTTFd2+DC3/MTTFd3}}{1/\mathrm{MTTFd1} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{0.99/204082+0.99/100+0.87/85}{1/204082 + 1/100 + 1/85} \fallingdotseq 0.925$$

B)

$$\frac{\mathrm{DC4/MTTFd4+DC2/MTTFd2+DC3/MTTFd3}}{1/\mathrm{MTTFd4} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{0.99/1024+0.99/100+0.87/85}{1/1024 + 1/100 + 1/85} \fallingdotseq 0.928$$

C/D)

$$\frac{\mathrm{DC5/MTTFd5+DC2/MTTFd2+DC3/MTTFd3}}{1/\mathrm{MTTFd5} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{0.99/102041+0.99/100+0.87/85}{1/102041 + 1/100 + 1/85} \fallingdotseq 0.925$$

1-5 Applicable Standards

EC Directives

EC directive	Product	Applicable standards
Low voltage command	AC Servo Drive	EN 61800-5-1
	AC Servomotor	EN60034-1/-5
EMC directives	AC Servo Drive AC Servomotor	EN 55011 class A group 1
		IEC61800-3
		EN61000-6-2

Note. To conform to EMC directives, the Servo Motor and Servo Drive must be installed under the conditions described in "4-3 Wiring Conforming to EMC Directives" (P.4-21).

UL and cUL Standards

Standard	Product	Applicable standards	File number
UL standards	AC Servo Drive	UL508C	E179149
	AC Servomotor	UL1004-1 [100 V, 200 V] 3,000 r/min 50 to 750 W	E331224
		UL1004	E179189
CSA standards	AC Servo Drive	CSA22.2 No. 14	E179149
	AC Servomotor	CSA22.2 No. 100 [100 V, 200 V] 3,000 r/min 50 to 750 W	E331224
		CSA22.2 No. 100	E179189

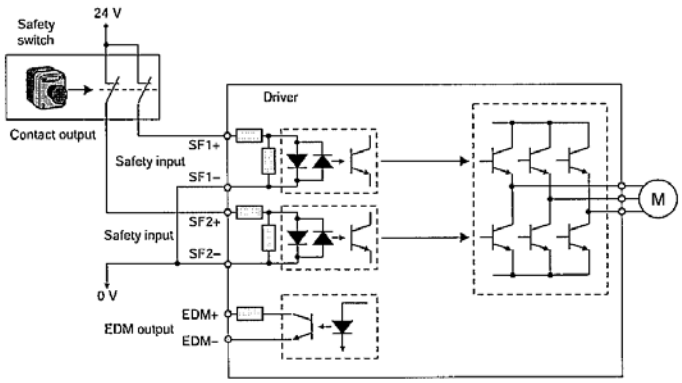
Functional Safety

Standard	Product	Applicable standards
Functional safety	AC Servo Drive	EN954-1 (Category 3) ISO13849-1 (Performance level D) EN61508 (SIL2) EN62061 (SIL2) EV61800-5-2 (STO) IEC61326-3-1 (SIL2)

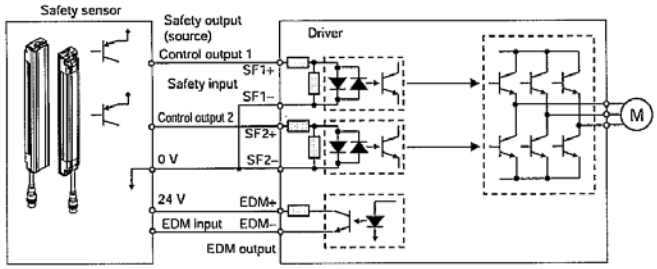
AC サーボアンプ T1 の仕様 1

7-3 Connection Examples

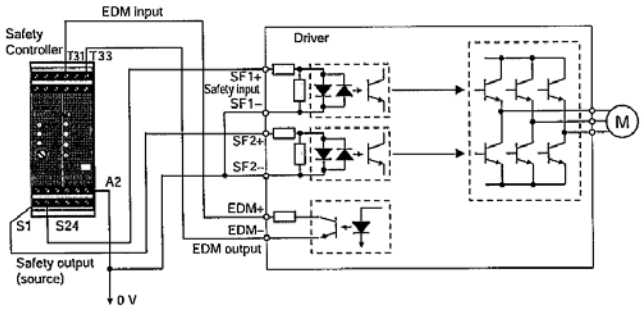
Connection Example 1: Connection with a Safety Switch



Connection Example 2: Connection with a Safety Sensor



Connection Example 3: Connection with a Safety Controller



AC サーボアンプ T1 の仕様 2

② 断裁機のバックゲージ部の PL 評価について　Cat.3 PLe

1)概要

バックゲージとは、製本時に紙を断裁する際、所定の寸法で切断するための紙揃えの当てである。裁断したい寸法の場所にバックゲージを移動させ、切りたい紙などをバックゲージに当てて紙などを揃えて、ナイフスイッチを押して、それを切るというのが裁断工程である。本評価では、裁断機のうちバックゲージ部の PL 評価を行う。

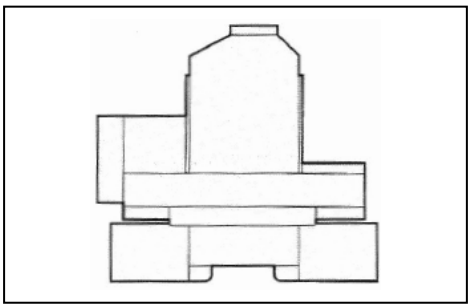
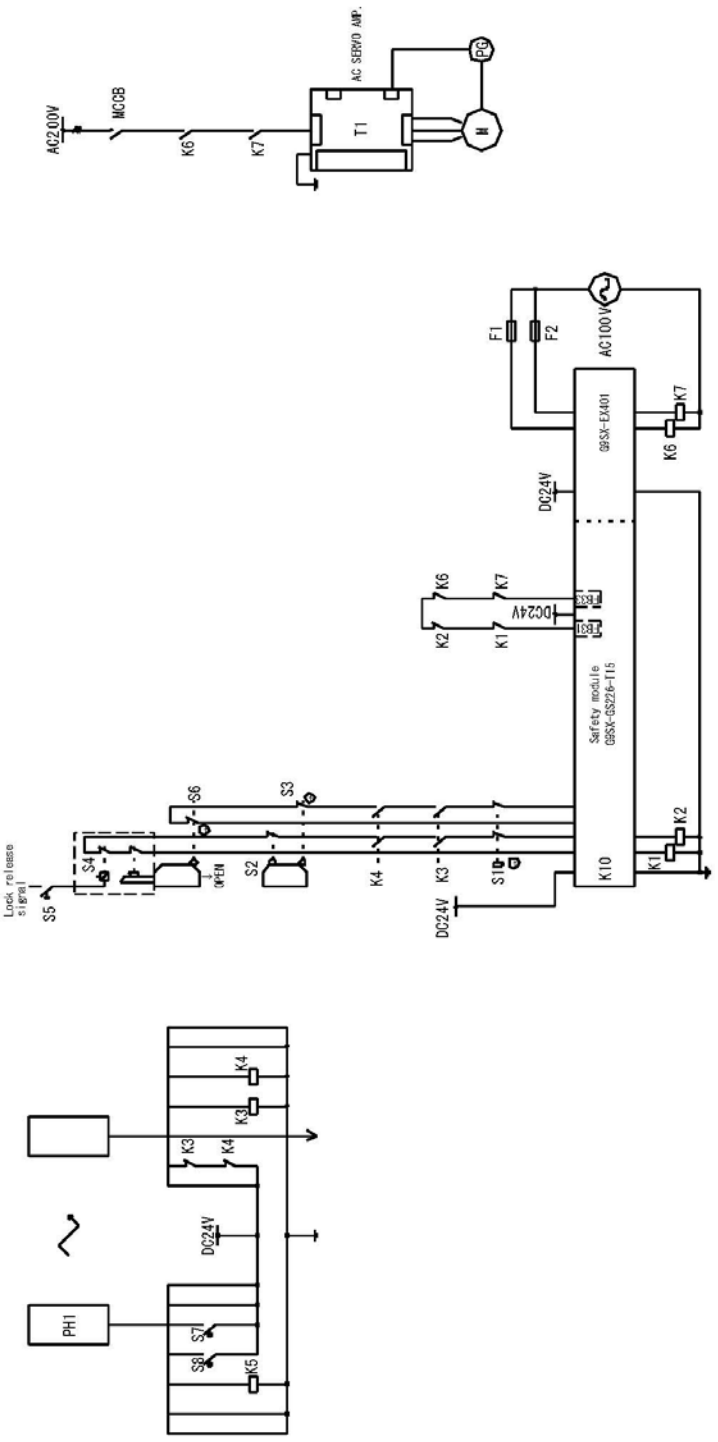


図 4.6　断裁機

断裁機（回路図／PLe）


AC200V
MCCB
K6
K7
AC SERVO AMP.
T1
PG
M
F1
F2
AC100V
GRSX-EX401
K7
K6
DC24V
K6
K7
K2
K1
DC24V
Safety module
GRSX-GS226-115
S6
S3
S4
S2
K4
K3
S1
K10
K1
K2
Lock release signal
S5
DC24V
K4
K3
K3
K4
DC24V
PH1
S7
S8
K5

2)安全機能

保護装置によって起動する安全関連停止機能

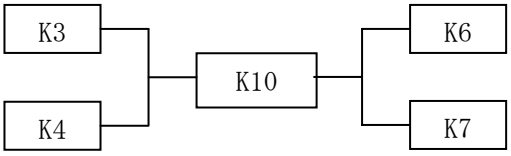
A) ライトカーテン
ライトカーテンが人体を検出すると、AC サーボアンプ T1 は、接触機 K6/K7 により電源 OFF される。

B) 非常停止スイッチ
非常停止スイッチが押されると、AC サーボアンプ T1 は、接触機 K6/K7 により電源 OFF される。

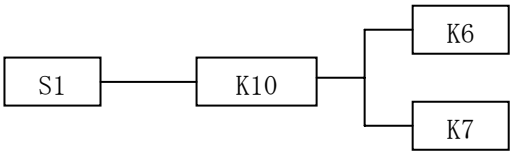
C) 可動式ガード
可動式ガード（安全ガード）が開くと、AC サーボアンプ T1 は、接触機 K6/K7 により電源 OFF される。

D) ロック式安全ガード
可動式ガード（安全ガード）が開く、または、安全ガードが解錠されると、AC サーボアンプ T1 は、接触機 K6/K7 により電源 OFF される。

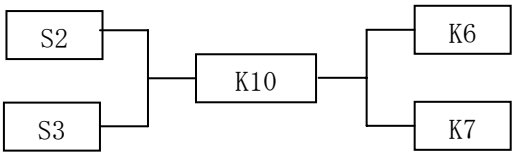
A) ライトカーテン



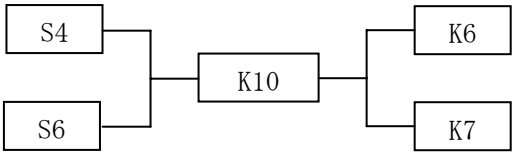
B) 非常停止スイッチ



C) 可動式ガード



D) ロック式安全ガード



3)機能の説明

A) ライトカーテン

ライトカーテンの PH1 が物体を検出する、または、自己診断機能によりライトカーテン自体の不具合を検出すると、異常接点 K3/K4 が開き、安全モジュール K10 が接点の開状態を検出し、K6/K7 を作動させ、AC サーボドライブ K10 の電源が切りとなる。

B) 非常停止スイッチ

非常停止スイッチが操作され接点が開いたことを安全モジュール K10 が検出すると、AC サーボドライブ T1 は、K6/K7 により電源が切りとなる。

C) 可動式ガード

可動式ガード（例：安全ガード）が開いたことを２位置スイッチ S2/S3 が検出すると、AC サーボドライブ T1 は、開状態を検出した安全モジュール K10 からの出力により K6/K7 が開き、電源が切りとなる。

D) ロック式安全ガード

ロック式安全ガードの解錠検出接点 S4 が開くか、または、リミットスイッチ S6 により安全ガードが開いたことを検出すると、AC サーボドライブ T1 は、安全モジュールからの出力 K6/K7 により電源切りとなる。

4)設計特性

・基本及び十分に実証済みの安全原則を守り、カテゴリ B の要求事項を満たす。
・位置スイッチ S2/S3 への配線は、別々に配線または保護されている。
・位置スイッチ S4/S6 への配線は、別々に配線または保護されている。
・位置スイッチ作動のために保護装置の安定した配置を確保する。
・非常停止スイッチ S1 は、EN ISO 13850 に対応する。
ポジションスイッチ S3/S6 は、IEC 60947-5-1　付属書 K による強制開離機構を有する。
・安全モジュール K10 は、EN 954-1(カテゴリ 4)と IEC/EN 61508(SIL3)を満たす。
・AC サーボアンプ T1 は PLd に適合する。
・K6/K7 の故障は K10 により検出され、K6/K7 への動作指令を切る。
安全ユニット K10 の故障は K10 自身の機能により検出される（プロセスによる故障検出)。

5)推定故障率の計算

各部品の MTTFd と DC

No.	ID	Name	Manufac -turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	G9SX-GS226	--	100	99
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	99
6	K6/K7	Contactor	Schneider Electric	LC1D12	2,000,000	20408	99

1. K3/K4

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd1 ＝ B10d / 0.1×Nop ＝ 20,000,000 / 0.1×980 ＝ 204082 years

DC1 = 99%

2. K10 MTTFd2 ＝ 100 years DC2 = 99%

Manufacturer spec.

3. T1 MTTFd3 ＝ 85 years DC3 = 87%

Manufacturer spec.

4. S1

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd4 ＝ B10d / 0.1×Nop ＝ 100,000 / 0.1×980 ＝ 1024 years

DC4 = 99%

5. S2/S6

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) ＝ 1960

MTTFd5 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×1960 ＝ 102041 years

DC5 = 99%

6. K6/K7

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd6 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×980 ＝ 20408 years

DC6 = 99%

6)PL 計算結果

PL 判定結果

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	99	0.99	3	65＜	e
B	91	0.99	3	65＜	e
C/D	99	0.99	3	65＜	e

MTTFd

A)

$$\frac{1}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/204082 + 1/100 + 1/20408} \fallingdotseq 99 \text{ year}$$

B)

$$\frac{1}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/1024 + 1/100 + 1/20408} \fallingdotseq 91 \text{ year}$$

C/D)

$$\frac{1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/102041 + 1/100 + 1/20408} \fallingdotseq 99 \text{ year}$$

DCavg

A)

$$\frac{DC1/MTTFd1+DC2/MTTFd2+DC6/MTTFd6}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd6} = \frac{0.99/204082+0.99/100+0.99/20408}{1/204082 + 1/100 + 1/20408} \fallingdotseq 0.99$$

B)

$$\frac{DC4/MTTFd4+DC2/MTTFd2+DC6/MTTFd6}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd6} = \frac{0.99/1024+0.99/100+0.99/20408}{1/1024 + 1/100 + 1/20408} \fallingdotseq 0.99$$

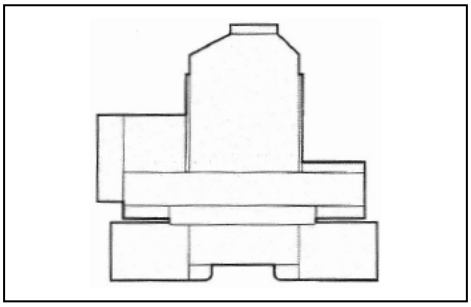
C/D)

$$\frac{DC5/MTTFd5+DC2/MTTFd2+DC1/MTTFd1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd1} = \frac{0.99/102041+0.99/100+0.99/204082}{1/102041+1/100 + 1/204082} \fallingdotseq 0.99$$

③ Safety assessment of Back Gauge of Sheet Cutting Machine Cat.3 PLd

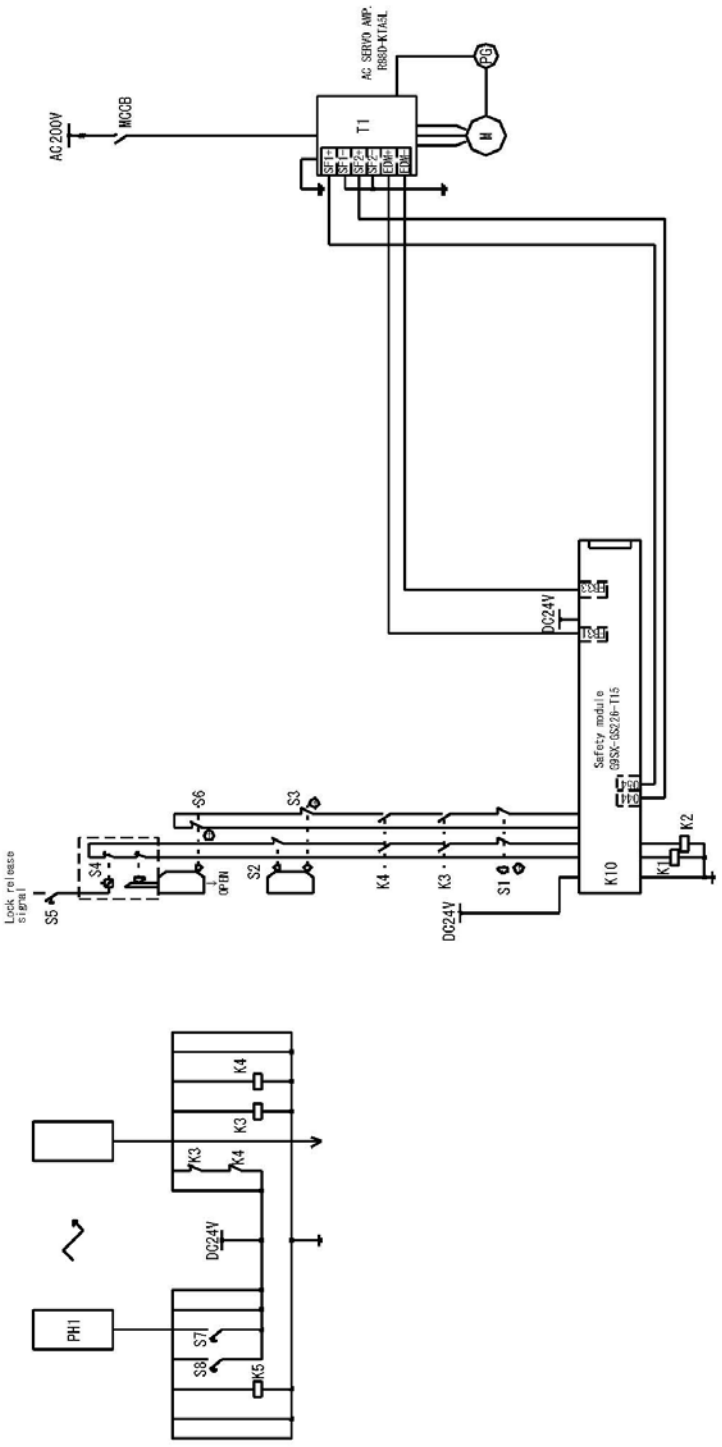
1) Outline

Back Gauge is a guide to line up the sheet when cutting it into a given size for bookbinding. Moving the back gauge according to the cutting size, lining up the sheet using back gauge, and pressing the knife switch to cut the sheet is a sheet cutting process. Safety assessment of back gauge of sheet cutting machine is evaluated by this document.



Sheet Cutting Machine

Circuit Diagram（PLd）



2) Safety function

Safety-related stop function, initiated by a protective device:

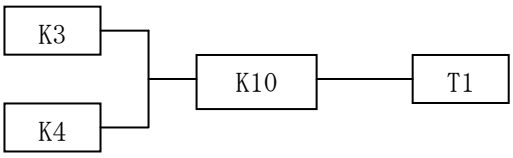
A) Light curtain
When the light curtain detects a person, the safety function STO (safe torque off) is initiated to stop the motor of back gauge.

B) Emergency stop switch
When the Emergency stop switch is pushed, the safety function STO (safe torque off) is initiated to stop the motor of back gauge.

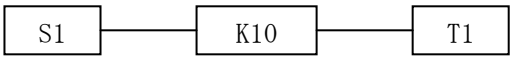
C) Moveable guard
When the moveable guard (safety guard) is opened, the safety function STO (safe torque off) is initiated by actuation of the limit switch to stop the motor of back gauge.

D) Lock type safety guard
When the moveable guard (safety guard) is opened or safety guard is unlocked, the safety function STO(safe torque off) is initiated to stop the motor of back gauge.

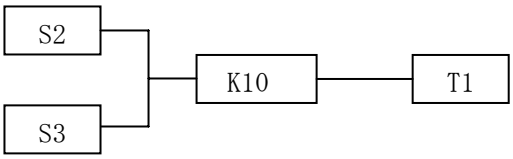
A) Light Curtain



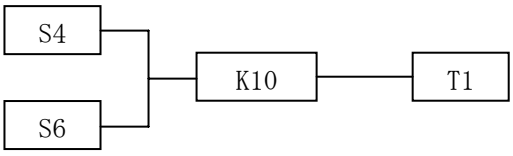
B) Emergency stop switch



C) Moveable guard



D) Lock type safety guard



3)Functional description:

A) Light curtain
When light curtain PH1 detects an object or detects any failure by self-diagnosis function, abnormal contact K3 and K4 is opened and the AC servo amp T1 is safety torque off by contactor 044 and 054 which is initiated by safety module K10.

B) Emergency stop switch
Power of AC servo amp T1 is safety torque off by contactor 044 and 054 when emergency stop switch S1 operates and opening of the contact is detected by safety module K10.

C) Moveable guard
Opening of the moveable guard (e.g. safety guard) is detected by two position switches S2 and S3 in a break contact. Power of AC servo amp T1 is safety torque off by contactor 044 and 054 which is initiated by safety module K10.

D) Lock type safety guard
When the lock type safety guard is unlocked and then contact S4 is opened or when release of safety guard is detected by limit switch S6, power of AC servo amp T1 is safety torque off by contactor 044 and 054 which is initiated by safety module K10.

4)Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The supply conductors to the position switches S2 and S3 are laid separately or with protection.
- The supply conductors to the position switches S4 and S6 are laid separately or with protection.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- The emergency stop device S1 corresponds to EN ISO 13850:S3 and S6 are position switches with detect opening contact to IEC 60947-5-1, Annex K.
- The safety modules K10 satisfy all the requirements for EN954-1(Category 4) and IEC/EN61508 (SIL3).
- AC servo amp T1 is corresponds to PLd.
- Component failures in AC servo amp T1 are detected by the Safety unit K10 and lead to operation inhabitation owing to the dropping out of 044 and 054. Faults in the Safety unit K10 are detected only by the function (fault detection by the process).

5) Calculation of the probability of failure

MTTFd and DC about parts

No.	ID	Name	Manufac -turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	G9SX-GS226	--	100	99
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	99

1. K3/K4

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) = 980

MTTFd1 = B10d / 0.1×Nop = 20,000,000 / 0.1×980 = 204082 years

DC1 = 99%

2. K10 MTTFd2 = 100 years DC2 = 99%

Manufacturer spec.

3. T1 MTTFd3 = 85 years DC3 = 87%

Manufacturer spec.

4. S1

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) = 980

MTTFd4 = B10d / 0.1×Nop = 100,000 / 0.1×980 = 1024 years

DC4 = 99%

5. S2/S6

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) = 1960

MTTFd5 = B10d / 0.1×Nop = 2,000,000 / 0.1×1960 = 102041 years

DC5 = 99%

6)PL diagnosis results

PL diagnosis results

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	46	0.925	3	65<	d
B	44	0.928	3	65<	d
C/D	46	0.925	3	65<	d

MTTFd

A)

$$\frac{1}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd3} = \frac{1}{1/204082 + 1/100 + 1/85} \fallingdotseq 46 \text{ year}$$

B)

$$\frac{1}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd3} = \frac{1}{1/1024 + 1/100 + 1/85} \fallingdotseq 44 \text{ year}$$

C/D)

$$\frac{1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd3} = \frac{1}{1/102041 + 1/100 + 1/85} \fallingdotseq 46 \text{ year}$$

DCavg

A)

$$\frac{DC1/MTTFd1+DC2/MTTFd2+DC3/MTTFd3}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd3} = \frac{0.99/204082+0.99/100+0.87/85}{1/204082 + 1/100 + 1/85} \fallingdotseq 0.925$$

B)

$$\frac{DC4/MTTFd4+DC2/MTTFd2+DC3/MTTFd3}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd3} = \frac{0.99/1024+0.99/100+0.87/85}{1/1024 + 1/100 + 1/85} \fallingdotseq 0.928$$

C/D)

$$\frac{DC5/MTTFd5+DC2/MTTFd2+DC3/MTTFd3}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd3} = \frac{0.99/102041+0.99/100+0.87/85}{1/102041 + 1/100 + 1/85} \fallingdotseq 0.925$$

1-5 Applicable Standards

EC Directives

EC directive	Product	Applicable standards
Low voltage command	AC Servo Drive	EN 61800-5-1
	AC Servomotor	EN60034-1/-5
EMC directives	AC Servo Drive AC Servomotor	EN 55011 class A group 1
		IEC61800-3
		EN61000-6-2

Note. To conform to EMC directives, the Servo Motor and Servo Drive must be installed under the conditions described in "4-3 Wiring Conforming to EMC Directives" (P.4-21).

UL and cUL Standards

Standard	Product	Applicable standards	File number
UL standards	AC Servo Drive	UL508C	E179149
	AC Servomotor	UL1004-1 [100 V, 200 V] 3,000 r/min 50 to 750 W	E331224
		UL1004	E179189
CSA standards	AC Servo Drive	CSA22.2 No. 14	E179149
	AC Servomotor	CSA22.2 No. 100 [100 V, 200 V] 3,000 r/min 50 to 750 W	E331224
		CSA22.2 No. 100	E179189

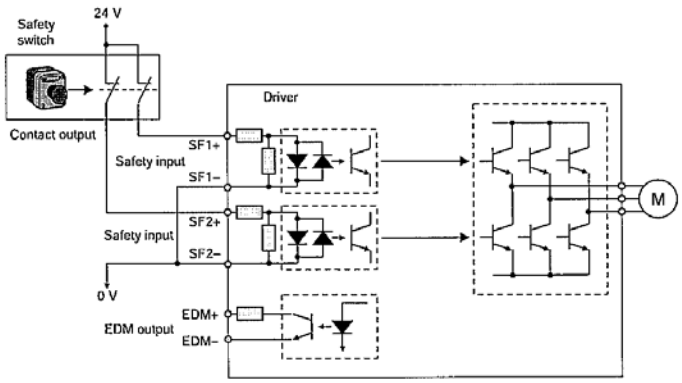
Functional Safety

Standard	Product	Applicable standards
Functional safety	AC Servo Drive	EN954-1 (Category 3) ISO13849-1 (Performance level D) EN61508 (SIL2) EN62061 (SIL2) EV61800-5-2 (STO) IEC61326-3-1 (SIL2)

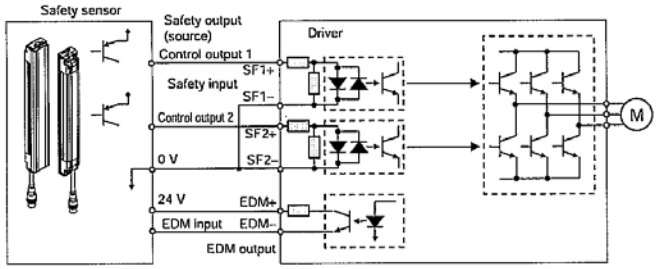
AC servo amplifier T1 specification 1

7-3 Connection Examples

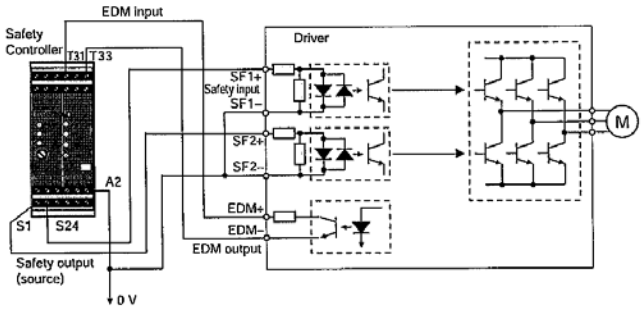
Connection Example 1: Connection with a Safety Switch



Connection Example 2: Connection with a Safety Sensor



Connection Example 3: Connection with a Safety Controller

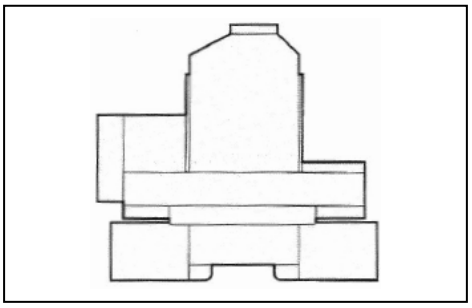


AC servo amplifier T1 specification 2

④ Safety assessment of Back Gauge of Sheet Cutting Machine Cat.3 PLe

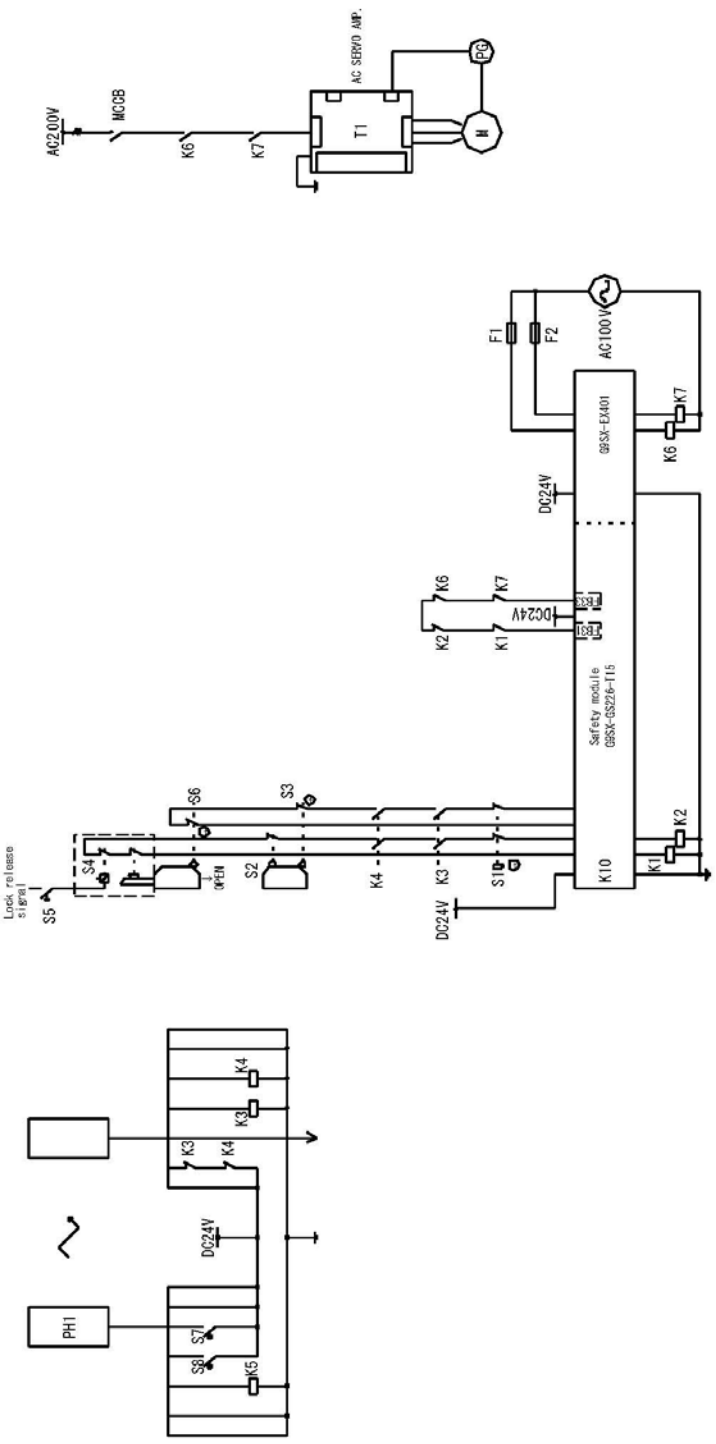
1) Outline

Back Gauge is a guide to line up the sheet when cutting it into a given size for bookbinding. Moving the back gauge according to the cutting size, lining up the sheet using back gauge, and pressing the knife switch to cut the sheet is a sheet cutting process. Safety assessment of back gauge of sheet cutting machine is evaluated by this document.



Sheet Cutting Machine

Circuit Diagram（PLe）



2) Safety function

Safety-related stop function, initiated by a protective device:

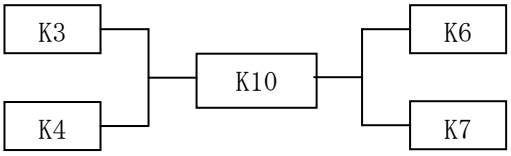
A) Light curtain
When the light curtain detects a person, AC servo amp T1 is turned off by contactor K6 and K7.

B) Emergency stop switch
When the Emergency stop switch is pushed, AC servo amp T1 is turned off by contactor K6 and K7.

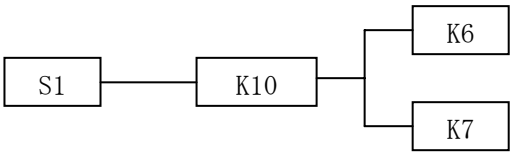
C) Moveable guard
When the moveable guard (safety guard) is opened, the limit switch is initiated, and AC servo amp T1 is the turned off by contactor K6 and K7

D) Lock type safety guard
When the moveable guard (safety guard) is opened, or safety guard is unlocked, the limit switch is initiated, and AC servo amp T1 is turned off by contactor K6 and K7.

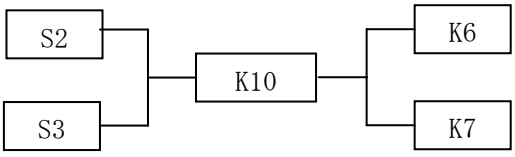
A) Light Curtain



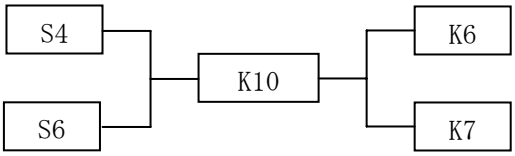
B) Emergency stop switch



C) Moveable guard



D) Lock type safety guard



3)Functional description

A) Light curtain
When light curtain PH1 detects an object or detects any failure by self-diagnosis function, abnormal contact K3 and K4 is opened and power of AC servo amp T1 is turned off by contactor K6 and K7 which is initiated by safety module K10 detecting opening of contact.

B) Emergency stop switch
Power of AC servo amp T1 is turned off by contactor K6 and K7 when emergency stop switch S1 operates and opening of the contact is detected by safety module K10.

C) Moveable guard
Opening of the moveable guard (e.g. safety guard) is detected by two position switches S2 and S3 in a break contact. Power of AC servo amp T1 is turned off by contactor K6 and K7 when opening of the contact is detected by safety module K10.

D) Lock type safety guard
When the lock type safety guard is unlocked and then contact S4 is opened or when release of safety guard is detected by limit switch S6, power of AC servo amp T1 is turned off by contactor K6 and K7 which is initiated by safety module K10 detecting opening of contact.

4)Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met.
- The supply conductors to the position switches S2 and S3 are laid separately or with protection.
- The supply conductors to the position switches S4 and S6 are laid separately or with protection.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- The emergency stop device S1 corresponds to EN ISO 13850:S3 and S6 are position switches with detect opening contact to IEC 60947-5-1, Annex K.
- The safety modules K10 satisfy all the requirements for EN954-1(Category 4) and IEC/EN61508 (SIL3).
- Component failures in K6 and K7 are detected by K10 and lead to operation inhabitation owing to the dropping out of K6 and K7. Faults in the Safety unit K1 are detected only by the function (fault detection by the process).

5) Calculation of the probability of failure

MTTFd and DC about parts

No.	ID	Name	Manufac -turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	G9SX-GS226	--	100	99
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	99
6	K6/K7	Contactor	Schneider Electric	LC1D12	2,000,000	20408	99

1. K3/K4

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) = 980

MTTFd1 = B10d / 0.1×Nop = 20,000,000 / 0.1×980 = 204082 years

DC1 = 99%

2. K10 MTTFd2 = 100 years DC2 = 99%

Manufacturer spec.

3. T1 MTTFd3 = 85 years DC3 = 87%

Manufacturer spec.

4. S1

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) = 980

MTTFd4 = B10d / 0.1×Nop = 100,000 / 0.1×980 = 1024 years

DC4 = 99%

5. S2/S6

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) = 1960

MTTFd5 = B10d / 0.1×Nop = 2,000,000 / 0.1×1960 = 102041 years

DC5 = 99%

6. K6/K7

Nop = 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) = 980

MTTFd6 = B10d / 0.1×Nop = 2,000,000 / 0.1×980 = 20408 years

DC6 = 99%

6)PL diagnosis results

PL diagnosis results

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	99	0.99	3	65<	e
B	91	0.99	3	65<	e
C/D	99	0.99	3	65<	e

MTTFd

A)

$$\frac{1}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/204082 + 1/100 + 1/20408} \fallingdotseq 99 \text{ year}$$

B)

$$\frac{1}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/1024 + 1/100 + 1/20408} \fallingdotseq 91 \text{ year}$$

C/D)

$$\frac{1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/102041 + 1/100 + 1/20408} \fallingdotseq 99 \text{ year}$$

DCavg

A)

$$\frac{DC1/MTTFd1+DC2/MTTFd2+DC6/MTTFd6}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd6} = \frac{0.99/204082+0.99/100+0.99/20408}{1/204082 + 1/100 + 1/20408} \fallingdotseq 0.99$$

B)

$$\frac{DC4/MTTFd4+DC2/MTTFd2+DC6/MTTFd6}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd6} = \frac{0.99/1024+0.99/100+0.99/20408}{1/1024 + 1/100 + 1/20408} \fallingdotseq 0.99$$

C/D)

$$\frac{DC5/MTTFd5+DC2/MTTFd2+DC1/MTTFd1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd1} = \frac{0.99/102041+0.99/100+0.99/204082}{1/102041+1/100 + 1/204082} \fallingdotseq 0.99$$

(2) BG からの指摘

- „moveable guard“ の安全スイッチ S2 と S3 及び„Lock type safety guard“の安全スイッチ S4 及び S6 はそれぞれカスケードとして安全モジュール K10 へ導かれる。この場合 DC は最高で 90%となる。
- Da die Sicherheitsschalter S4 und S6 der „Lock type safety guard“ mit den Sicherheitsschalter S2 und S3 der „moveable guard“ jeweils als Kaskade auf das Sicherheitsmodul K10 geführt sind, kann als Diagnosedeckungsgrad höchstes 90% vergeben werden.

一般事項:制御カテゴリ 4 に関する MTTF への置換は PFH の値をもってのみ有効である。
すなわち制御カテゴリ 4 の制御を単に MTTFd=100a に置き換えることはできない。
この置換は付録の表をもってのみ可能である。

Allgemein: Es muss darauf hingewiesen werden, dass eine Umrechnung auf MTTFd bzgl. Kategorie 4 Steuerungen nur über den PFH-Wert zulässig ist. D.h. man kann nicht einfach einer Kategorie 4 Steuerung den MTTFd=100a zuordnen. Die Umrechnung kann anhand der als Anlage beigefügten Tabelle erfolgen.

例えば T1 の様なコンポーネントで該当値が存在しない場合、単純に DC90%を適用することはできない。何故ならば、DC 値は診断機能により決定されるからである。それは例えば、インバーターT1 のセンサー値が PLC に入力され、インバーターの駆動系の PL による故障時に安全なパルスブロックにより静止状態に導かれることにより達成される。この場合、規格により DC90%が適用されうる。

Für Komponenten, z.B. T1, bei denen keine Kennwerte vorhanden sind kann nicht einfach ein DC Wert von 90% angenommen werden. Denn der Kennwerte DC wird durch die Diagnosemaßnahmen bestimmt. Das kann z.B. dadurch erfolgen, dass der Sensorwert des Inverters T1 in die PLC zurückgelesen wird und bei einem Fehlverhalten des Inverters durch die PLC der Antrieb durch die sichere Impulssperre stillgesetzt wird. In diesem Fall kann entsprechend der Norm ein Diagnosewert von 90% angenommen werden.

(3) BG との討論内容

- 全体をとおして特に問題はなかった。
- PLd のサンプル回路例は、PLe に近い d と考えられる。
- 重要な部分の説明が十分でない。
- 安全リレーモジュールを一般的なリレーモジュールに変更しても、同じ PLd とすることはできない。
- 安全スイッチのカスケード接続における DC は、最大でも 90%になる。単独接続した場合は、99%として計算することは可能である。
- MTTF への置換は PFH の値でもってのみ有効で、単に MTTFd=100 とは置き換えられない。

(4) 修正レポート

※修正内容は、ｲ)とﾛ)の２項目。
　文章中の**太字**が修正部分。

ｲ) 4.2.3.①.4) 設計特性項の AC サーボアンプの記述を修正する。
　AC サーボアンプ T1 は、**IEC61800-5-2 に適合し**、PLd にも適合する。
　AC サーボアンプ T1 の DC は、メーカー公表値で 87%である。

ﾛ) S2 の DC を 90%から 99%へ修正する。

5) 推定故障率の計算

各部品の MTTFd と DC

No.	ID	Name	Manufac -turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	G9SX-GS226	--	100	99
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	**90**

1. K3/K4
　Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980
　MTTFd1 ＝ B10d / 0.1×Nop ＝ 20,000,000 / 0.1×980 ＝ 204082 years
　DC1 = 99%

2. K10 MTTFd2 ＝ 100 years　　DC2 = 99%
　Manufacturer spec.

3. T1 MTTFd3 ＝ 85 years　　DC3 = 87%
　Manufacturer spec.

4. S1
　Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980
　MTTFd4 ＝ B10d / 0.1×Nop ＝ 100,000 / 0.1×980 ＝ 1024 years
　DC4 = 99%

5. S2/S6
　Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) ＝ 1960
　MTTFd5 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×1960 ＝ 102041 years
　DC5 = 90%

6) PL 計算結果

PL 判定結果

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	46	0.925	3	65＜	d
B	44	0.928	3	65＜	d
C / D	46	0.925	3	65＜	d

MTTFd

A)

$$\frac{1}{1/\mathrm{MTTFd1} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{1}{1/204082 + 1/100 + 1/85} \fallingdotseq \mathbf{46\ year}$$

B)

$$\frac{1}{1/\mathrm{MTTFd4} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{1}{1/1024 + 1/100 + 1/85} \fallingdotseq \mathbf{44\ year}$$

C/D)

$$\frac{1}{1/\mathrm{MTTFd5} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{1}{1/102041 + 1/100 + 1/85} \fallingdotseq \mathbf{46\ year}$$

DCavg

A)

$$\frac{\mathrm{DC1}/\mathrm{MTTFd1}+\mathrm{DC2}/\mathrm{MTTFd2}+\mathrm{DC3}/\mathrm{MTTFd3}}{1/\mathrm{MTTFd1} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{0.99/204082+0.99/100+0.87/85}{1/204082 + 1/100 + 1/85}$$

$$\fallingdotseq 0.925$$

B)

$$\frac{\mathrm{DC4}/\mathrm{MTTFd4}+\mathrm{DC2}/\mathrm{MTTFd2}+\mathrm{DC3}/\mathrm{MTTFd3}}{1/\mathrm{MTTFd4} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{0.99/1024+0.99/100+0.87/85}{1/1024 + 1/100 + 1/85}$$

$$\fallingdotseq 0.928$$

C/D)

$$\frac{\mathrm{DC5}/\mathrm{MTTFd5}+\mathrm{DC2}/\mathrm{MTTFd2}+\mathrm{DC3}/\mathrm{MTTFd3}}{1/\mathrm{MTTFd5} + 1/\mathrm{MTTFd2} + 1/\mathrm{MTTFd3}} = \frac{\mathbf{0.9}/102041+0.99/100+0.87/85}{1/102041 + 1/100 + 1/85}$$

$$\fallingdotseq 0.925$$

5) 推定故障率の計算

各部品の MTTFd と DC

No.	ID	Name	Manufac -turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	G9SX-GS226	--	100	99
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	**90**
6	K6/K7	Contactor	Schneider Electric	LC1D12	2,000,000	20408	99

1. K3/K4

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd1 ＝ B10d / 0.1×Nop ＝ 20,000,000 / 0.1×980 ＝ 204082 years

DC1 = 99%

2. K10 MTTFd2 ＝ 100 years DC2 = 99%

Manufacturer spec.

3. T1 MTTFd3 ＝ 85 years DC3 = 87%

Manufacturer spec.

4. S1

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd4 ＝ B10d / 0.1×Nop ＝ 100,000 / 0.1×980 ＝ 1024 years

DC4 = 99%

5. S2/S6

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) ＝ 1960

MTTFd5 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×1960 ＝ 102041 years

DC5 = 90%

6. K6/K7

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd6 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×980 ＝ 20408 years

DC6 = 99%

6) PL diagnosis results

PL 判定結果

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	99	0.99	3	65＜	e
B	91	0.99	3	65＜	e
C / D	99	0.99	3	65＜	e

MTTFd

A)

$$\frac{1}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/204082 + 1/100 + 1/20408} \fallingdotseq 99 \text{ year}$$

B)

$$\frac{1}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/1024 + 1/100 + 1/20408} \fallingdotseq 91 \text{ year}$$

C/D)

$$\frac{1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd6} = \frac{1}{1/102041 + 1/100 + 1/20408} \fallingdotseq 99 \text{ year}$$

DCavg

A)

$$\frac{DC1/MTTFd1+DC2/MTTFd2+DC6/MTTFd6}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd6} = \frac{0.99/204082+0.99/100+0.99/20408}{1/204082 + 1/100 + 1/20408} \fallingdotseq 0.99$$

B)

$$\frac{DC4/MTTFd4+DC2/MTTFd2+DC6/MTTFd6}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd6} = \frac{0.99/1024+0.99/100+0.99/20408}{1/1024 + 1/100 + 1/20408} \fallingdotseq 0.99$$

C/D)

$$\frac{DC5/MTTFd5+DC2/MTTFd2+DC1/MTTFd1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd1} = \frac{0.9/102041+0.99/100+0.99/204082}{1/102041+1/100 + 1/204082} \fallingdotseq 0.99$$

(5) 考察

・認定資料としてカタログを添付しても、あまり確認されていなかった。資料としては第 3 社機関による認証書を手に入れる必要があると思われる。

・各部品のパラメータをメーカーに請求する際は、PFH をもらうようにする。

・インバーター、サーボアンプなどのパワードライブシステム部品が IEC 61800-5-2 適合品で、制御信号の二重化、故障保証されておれば、入力電源遮断のためのリレー2 段は必要なくなることが PLd のサンプル回路例でわかった。

(6) 図面の修正

1) 修正に至った経緯

今回Cグループではオムロン製安全リレーユニットG9SXとサーボアンプドライバG5シリーズを使用した回路例で PL 計算を行ったが、後日オムロン社より連絡を受け、修正するに至った。安全リレーユニットG9SXの入力電圧が24Vdc一定であれば、サーボドライバG5シリーズの安全保障信号(EDM機能)が2回路まで接続・動作可能であるが、G9SXの入力電圧がMin.保証値である20.4Vdcまで低下すると安全保障信号が機能せず、システム全体が異常を検知して停止してしまうというものである。オムロン社では新商品としてセーフティコントローラG9SPシリーズを発表されており、そのコントローラであればMin.保証値20.4Vdcまで低下しても安全保障信号が4回路まで接続・動作可能で、このコントローラによる回路例に修正して欲しいとの要望を受けた。PL 計算に関与するパラメータ類はG9SX・G9SPともにほぼ同等で結果には影響しないとのことである。G9SXでは入力が2点までだったが、セーフティコントローラは入力が最低 10 点ありスイッチ等の信号を個別に入力・再計算することも可能であるが、すでに委員会は終了し、あくまで修正という今回の作業内容から、採用部品の変更に伴う図面変更とPLの再計算の作業とした。

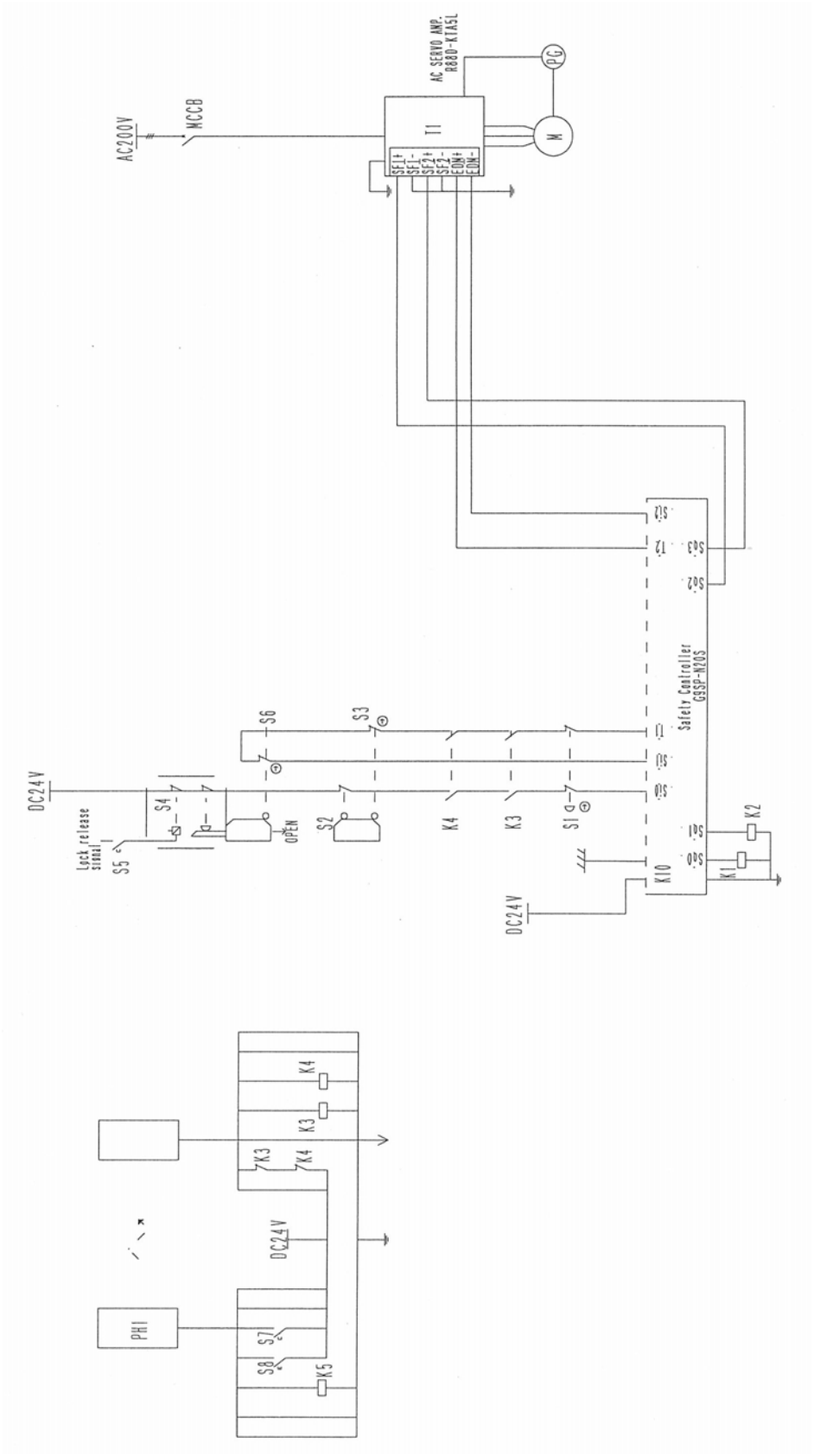
2) 修正図面

G9SPを使用した修正図面を次ページに示す。

G5シリーズの安全保障信号（EDM機能）に関わる点の修正のため、該当する信号を使用しているPLdの例のみ修正した。

参考までに、G9SPに変更した場合でも、PLはG9SXと同じPLdとなった。

断裁機 修正回路図(PLd)



3) 推定故障率の計算

各部品の MTTFd と DC

No.	ID	Name	Manufac-turer	Type	B10d	MTTFd [Year]	DC [%]
1	K3/K4	Safety Relay	Omron Corp.	G7S-3A3B	20,000,000	204082	99
2	K10	Safety Module	Omron Corp.	**G9SP-N20S**	--	100	**90**
3	T1	Servo Amp.	Omron Corp.	R88D-KT	--	85	87
4	S1	Emergency Stop Switch	Omron Corp.	A22E-M-02	100,000	1024	99
5	S2/S6	Safety Limit Switch	Omron Corp.	D4N-□A20	2,000,000	102041	99

1. K3/K4

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd1 ＝ B10d / 0.1×Nop ＝ 20,000,000 / 0.1×980 ＝ 204082 years

DC1 = 99%

2. K10 MTTFd2 ＝ 100 years DC2 = **90%**

Manufacturer spec.

3. T1 MTTFd3 ＝ 85 years DC3 = 87%

Manufacturer spec.

4. S1

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 4 times) ＝ 980

MTTFd4 ＝ B10d / 0.1×Nop ＝ 100,000 / 0.1×980 ＝ 1024 years

DC4 = 99%

5. S2/S6

Nop ＝ 245 days×8 hours×3600 / (3600 sec.×8 hours / 8times) ＝ 1960

MTTFd5 ＝ B10d / 0.1×Nop ＝ 2,000,000 / 0.1×1960 ＝ 102041 years

DC5 = 99%

4) PL 計算結果

PL 判定結果

No.	MTTFd [year]	DCavg	Safety Category	CCF	PL
A	46	**0.884**	3	65＜	d
B	44	**0.888**	3	65＜	d
C/D	46	**0.884**	3	65＜	d

MTTFd

A)

$$\frac{1}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd3} = \frac{1}{1/204082 + 1/100 + 1/85} \fallingdotseq 46 \text{ year}$$

B)

$$\frac{1}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd3} = \frac{1}{1/1024 + 1/100 + 1/85} \fallingdotseq 44 \text{ year}$$

C/D)

$$\frac{1}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd3} = \frac{1}{1/102041 + 1/100 + 1/85} \fallingdotseq 46 \text{ year}$$

DCavg

A)

$$\frac{DC1/MTTFd1+DC2/MTTFd2+DC3/MTTFd3}{1/MTTFd1 + 1/MTTFd2 + 1/MTTFd3} = \frac{0.99/204082+\mathbf{0.90}/100+0.87/85}{1/204082 + 1/100 + 1/85} \fallingdotseq \mathbf{0.884}$$

B)

$$\frac{DC4/MTTFd4+DC2/MTTFd2+DC3/MTTFd3}{1/MTTFd4 + 1/MTTFd2 + 1/MTTFd3} = \frac{0.99/1024+\mathbf{0.90}/100+0.87/85}{1/1024 + 1/100 + 1/85} \fallingdotseq \mathbf{0.888}$$

C/D)

$$\frac{DC5/MTTFd5+DC2/MTTFd2+DC3/MTTFd3}{1/MTTFd5 + 1/MTTFd2 + 1/MTTFd3} = \frac{0.99/102041+\mathbf{0.90}/100+0.87/85}{1/102041 + 1/100 + 1/85} \fallingdotseq \mathbf{0.884}$$

4.3　BG による検証結果について

枚葉機（A グループ）では、チャレンジ的な回路も組み込んだため、審査側に意図を伝えるのが難しかった。これは、印刷機では定型的な回路であっても審査官はメーカー担当者よりも広範な機械を扱っているので、安全機能とその実現については、詳細の説明が必要であることがわかった。今回のように、チャレンジ的な回路を実機で使う場合にはなおさらであると思われる。一方、そうであっても、説明することで理解を得ることもできたわけで、その意味では、今回のような検証等を通じて、テクニカルコミュニケーションの方法を取得することは、大きな効果があると思われる。また、工業会で標準的な書式を作ることも有効であると考えられる。

輪転機（B グループ）では、安全機能の説明の伝達で苦労した。BG はある程度解釈（類推）して査定したようであった。しかし、十分に設計意図が伝われないなかでの認証は、不的確との判定になりかねない。そのような極端なことはないにしても、望ましいことではなく、また文書化しておいても、万が一の際に設計の妥当性の証明として活用できないこともありうる。日本人は文書化が苦手といわれるが、もともと持っている設計技術に見合った説明能力と文書化能力で、国際競争力が増すと考えられ、PL の認証の問題に限らず、向上が必要なスキルであることが再認識させられた。

断裁機（C グループ）については、オーソドックスな回路であり、特に大きな指摘事項はなかったが、カタログのコピーを添付しても必ずしも提出者の意図が伝わるとは限らないことを体験した。今回のように IEC 61800-5-2 など認証を取得したものを使う際には、認証書のコピーを取り寄せ添付することが、その後の審査をスムーズに進める上で大切なようである。これは、審査時に問われてから対応してもかまわないという意味で本質ではないが、円滑に審査を進めることは、審査側、受審側にとって好ましいことで準備すべきことであろう。また、準備のなかで、設計者にとっても、設計の妥当性の確認にもなる。

以上のようであるが、共通的事項を再度まとめると次の各項目となる。

1. PL 設計妥当性検証試験では、回路構成、計算結果に対する否定的なコメントはなかった。むしろ、設計の意図を正確に伝えることがキーポイントであった。その意味で、当初の文書と妥当性確認結果受領、討論後の文書を見比べ、設計者の文書化の要点を理解してほしい。
2. 制御システムのなかの安全関連部は、設計した安全機能とそれを担保する回路は略さずに記すこと必要であった。これは、回路図そのままという意味ではなく、安全機能の作動の仕組みがわかるものである。また、その作動説明の文書も必要であった。今回、当初の文書では、添付資料などについて、なぜ添付したのか理解されずに評価されていた点があった。規格適合品を使用した場合には、そのコンポーネントの認証書をメーカーから取り寄せ、添付することが必要あると感じられた。
3. MTTFd についても、カタログのコピーを付けるのではなく、試験成績書等の形で取り寄せ、

添付することが望ましいと考えられる。討論会でも、BG 側から「ファックスでもよいので、メーカーの書面を付けること」を推奨していた。認証側としては、対象機器で使われているコンポーネントのデータと明示的にわかるものを求めているものと思われる。

4. DC については、複数のグループで根拠を示すことが要求された。特に、「カテゴリ４の構成であるからという理由では 99%とはならない」ことを強調していた。

4.4 総括

今回の PL 評価・妥当性確認を通じて、表 4.1 に示す疑問点が上がった。これらについて、検証回路等と一緒に BG に送ったところ、同表右の回答を得た。また、講習会における質疑の内容も下部に記載してある。

回答は我々の予想したものであった。このことから、メーカーである我々と認証機関であり、またこの改正の中心となった機関でもある BG との間で、ISO 13849-1:2006 で導入された PL の解釈に大きさ相違がなかったことが確かめられたわけで、そのこと自体、一つの成果であった。

表 4.1 ISO 13849 の疑問点と BG からの回答

（その１）

No.	質問	回答
1	コンポーネントメーカーから MTTFd や B10d が提示されない場合、そのコンポーネントの電気的寿命から算出してよいか？（附属書の値があまりに大きいため）	メーカーから MTTFd または、B10d が得られないなら、 a. ISO 138949-1:2006 付属書　C または D の値を使用する。 b. 10 年を選択する。
2	電気的寿命は、Ｂ10 と考え、危険側故障が 50%と考えて、Ｂ10ｄは、電気的寿命の２倍としてよいか？	電気寿命の B10 データの 2 倍と見積もる。（付属書 C 参照）
3	MTTFd や B10 の数値がメーカーから提供されない場合は、ISO 13849-1:2006 の附属書 C に記載ある「表 C.1-コンポーネントの MTTFd または B10 を扱う国際規格」の標準数値を使用してよいか。 また、使用する場合の注意点は何か。	メーカーから MTTFd または、B10d が得られないなら、 a. ISO 138949-1:2006 付属書　C または D の値を使用する。 b. 10 年を選択する。
4	安全関連部に自社基板を使用している場合の MTTFd を求める場合は、ISO 13849-1:2006 の附属書 D の D.1 のパーツ・カウント・メソッドの「表 D.1-回路基板の部品リストの例」に記載あるように使用部品ごとの 1/MTTFd を求め、合計すればよいか。	パーツカウント方法にてにより数値化する。
5	推奨データベースはあるのか。B10d などをデータベースから取ったとき、データベース選択の妥当性も認証時に問われるか （どのような信頼性データベースなら使用してもよいか）。	私は SN 29500 からデータベースを推薦する。
6	MTTFd, DC などの PL を計算するのに必要なデータが開示されていない場合、サブシステムの SIL を PL に置き換えるやり方が記載されているが、必要なデータを入手する努力をせずに置き換えてしまう懸念がないのか。	カテゴリ IV システムの PFH 値を持っているという場合、DC ＝ 99%と MTTFd （ PFH 値に依存 ）を決定することができる。

7	コンポーネントメーカーから提供されるB10dなどのデータはそのまま計算基礎として使用してよいのでしょうか。もし、メーカーのこれらデータを計算に使うための条件があるとしたら教えてください。	確証の結果として、製造業者からリリースされたデータの信頼性をチェックしなければならない。
8	PLCで、Remote I/O LINK等を使用した場合、PLCは同一の１つのコンポーネントとして、考えればよいのか？　それとも、それぞれ、コンポーネントとして計算しなければならないのか？	バスシステムには、1パーセントルールで考える（エラーレートを時間当たり1パーセント以内にする）。
9	出力部品で、安全リレーを２個並列で出力し、その接点を２個シリアル接続で使用した場合、計算は、安全リレー１個として、計算するのか。２個をコンポーネントとして扱うと、MTTFdは、1／2になっていく。本来、故障への信頼性は、２倍になると思うが、MTTFdは下がっていくという点が釈然としません。	冗長システムのためにMTTF　dの計算をしなければならない（シングルシステム）。
10	並列冗長系のMTBFを評価する時2/3をかける、あるいは低い方のMTBFを使うこと が規定されている、という件で、並列冗長系が、２系統の場合、式が定義されていると思うが、３系統の場合などは、どうしたらよいか？まず、２系統を計算して、さらに、計算したものと残りの１系統で２系統の計算式で、計算するという方法でよいのか？それとも、選択して、高いもの２つで計算すればよいのか？３系統で冗長させているのに、MTTFdは下がっていくという点が釈然としません。	私の提案は、最も高いMTTFd値でチャンネルを選んで、対称化公式で計算をすることである。
11	機械回転を検出する近接スイッチのサイクルは、どう判断するのか？60rpmで回転すると１秒間１回になり、Nopが大きくなり、結果、MTTFdが小さくなる。	近接スイッチは、低信頼性部品である。B10dを考慮し計算しなければならない。
12	CEマーキングの自己宣言書にPL計算の結果として、SISTEMAの出力結果を正式文書としても問題ないか。別に手計算による書類が必要なのか。	SISTEMAから出力された結果を使うことはできる。
13	ソフトウェアの安全要求事項に関する項目についての判定ができるCCFのような点数付けされたチェックリストのようなものがないのか。例えば、IEC 61508などに。	チェックリストはない。
14	規定アーキテクチャーを満たすことは必須か。それともそれとは無関係にISO 13849-1:2006の表１を満たしていることを立証できれば規定アーキテクチャーでなくともPLは認められるのか。必須であるとすれば、どの規定に規定されているのか。	ISO 13849-1:2006の表１は、今は使用しても問題ない。 簡略化された手順によって計算をするならば、ISO 13849-1:2006の６で言及される構造を考慮しなければならない。
15	並列冗長系のMTBFを評価する時2/3をかける、あるいは低い方のMTBFを使うことが規定されている。このことは冗長化の意味を否定しているように思われるが、どのように考えるか。	弾力的な数値。信頼性には大きく影響しない。

16	SISTEMA のレポートをみると、ミッションタイムを記入してある。これは機械（製品）保証期間（？）、試用期間（？）？ Mission Time（a） : 20 チャンネル（CH1）の MTTFd（a）：19.88 という計算になることがある。 機械（製品）保証期間 20 年に対し、19.88 年では未適合ということになるのか？ それとも、CH1＋CH2 のトータルの MTTFd が、20 年を超えていれば、よいのか？ そこまで、気にしなくてよいのか？	信頼性は低い部品で 20 年未満なら保守などによりその期間を満足させる。

（その２）

No.	質問	回答
17	EN 954-1 の問題点 「カテゴリ 1 での故障除去はリスク低減の決定に不十分な階層に導かれない。」の意味は？	リスク低減を定量的に規定する時に、カテゴリ 1 の故障除去という概念では評価が適切に行えない。ISO 13849-1 では、カテゴリ 1 は最大で PL=“c”まで対応可能。
18	DC の決定（スライド 33）で、SW1 の DC が 99%で SW2 の DC が 90%である理由は？	SW1 は､強制開離機構を有するため 99%となる。
19	ガス検知器への要求事項→PL=“d”の中でセンサは 1ch でよいのか？	SIL2 なら 1ch で良い。SIL3 なら 2ch が必要。しかしキャリブレーションを頻繁に実施すれば 1ch でも可。
20	安全ドライブシステムインバーターのパルスブロックによる停止は、電源遮断による停止と同等の安全機能とみなせるのか？	同等である。残留エネルギーの問題もパルスブロック方式では回避できるという利点あり。
21	安全ドライブシステムインバーターのパルスブロックによる停止回路のカテゴリ、PL は？	カテゴリは 3。PL については自己診断機能、MTTFd（通常の PLC で 50～70 年）などを考慮して“d”。
22	安全ドライブシステムインバーターのシャフトレス制御の場合にも適用できるのか？	適用可能、むしろ軸数の多いシャフトレス制御の場合に有効である。
23	PG が 1 個でも PL=“d”が達成できる理由は？2ch は必要ないのか？（モーター速度監視にて）	自己診断を常時実施することにより 1ch でも問題なし。
24	並列システムの MTTFd の計算式の 2/3 の意味は？	これは、たとえば MTTFd=100 年のシステムを 2ch 並列にすると通常の信頼性工学の式では、150 年になってしまう。並列の場合にもシングルの場合と同等にしたいという意図があり､2/3 を付けたもの。

備考：表 4.1 の（その 1）の 1～16 は、当委員会から事前に BG へ質問した内容とその回答である。（その 2）の 17～24 は、講習会における質疑を要約して記載したものである。
（事前の質問に対する回答は英文であったが、ここでは和訳を表にまとめた。巻末には質問と回答の英文を添付したので参照されたい。）

今回は問題とはなっていないが、自社製のボードを使うときMTTFdをパーツカウント法で推算すると、かなり厳しい（MTTFdが小さい）結果となるのか、あるいは緩い（MTTFdが大きい）結果となるのか、また直列系のブロックの評価法も今回は経験していない。

このように、まだ検討していない課題もある。また、実装上の問題は、そもそも対象としていない。しかし、今回の実証研究は一企業では行えないことである。この研究を通じて、事前にPLによる認証を模擬的に行い、より詳細で要点を得た説明が必要なことなど、多くの成果が得られたことは成果である。なお、研究母体が(社)日本印刷産業機械工業会であるので、二種類の印刷機械と製本紙工機械（断裁機）の制御回路の安全関連部を基に議論しているが、制御の安全関連部の構成は多くの機械類で共通である。したがって、この成果は、種々の工業会、企業で活用できるものである。

第５章　調査研究のまとめ

印刷産業機械の製造者は、機械の安全性を確保するため、ISO の機械安全規格に適合することが求められている。2006 年 11 月には、ISO グループ安全規格（B 規格）の ISO 13849-1 の改正版が発行された。改正の結果、機械類に使用する部品の信頼性に対する従来のカテゴリ評価に加え、安全制御システムの信頼性を確率論的に求めた評価、すなわち「パフォーマンスレベル（PL)」に対応することが要求がされた。この改正を受けて、ISO/TC130/WG5 において審議が進められている印刷産業機械の安全規格（ISO 12643-1～5）では、評価基準が“カテゴリ”から“PL”に移行した。今後、印刷産業機械の製造者は、ISO 12643-1～5 の規格が要求する電気部品及び安全制御システムの要求 PL 値（PL r ）に適合することが要求される。そこで、設計した制御回路の安全関連部の PL による評価が適切に行えることが必要である。しかし、今まで馴染みにない概念であり、業界各社が個別に対応するのではなく、評価方法を明確にして、全ての会社が適切に対応できるようにすることが課題である。特に、EU 圏内向けの製品は、単に ISO 適合というだけでなく、法的要請である機械指令の整合規格 EN ISO 13849 に適合させなければならないという側面がある[*8]。

これら課題の解決のために、本調査研究では、印刷産業機械業界が PL を理解するのに必要な諸項目の整理、調査・研究を行った。得られた主な成果（ISO 13849 改定の要約も含む）は、次のとおりである。

1. 信頼性指標が導入され、さらにソフトウェアについての規定が加わった。これは、最近の電子化された回路の採用、PLC の採用などに対応している。
2. ソフトウェアの要求事項を抽出したが、求められる文書化の詳細は今回の調査だけでは明らかにし切っていない。これは、印刷産業機械に限ったことではない。IEC 61508 規格における認証評価などの例を参考にしつつ、検討を継続する必要がある。
3. ISO 12643 の規定は PLr となったが、従来の規格で規定していたカテゴリから特に問題なく、ほぼそのまま移行できそうである。
4. PLr を満たす制御の安全関連部設計の「教科書」は必要で、現状ないが将来は我が国独自のものが用意されることが望ましい。
5. このような現状下では、BG レポート翻訳は貴重な「教科書」であり、これは印刷産業機械工業会だけでなく、広く各業界において使える。いち早く翻訳した（レポートの第８章は現時点では部分訳である）ことは、我が国工業へ大きく貢献できる。有効活用頂きたい。
6. 設計実務では計算ツールが必要である。その観点から入手可能なものを比べた。
7. 特に、SISTEMA は有用なツールの一つであるので、使い方を具体例を用いて平易に解説した。資料編を参照されたい。この資料により、SISTEMA が使いやすくなったと思われる。
8. BG・ベッカー氏による PL の検証では、回路構成、計算結果に対する否定的なコメントはなか

[*8] 2009 年末から適用される予定であったが、二年間延期された。

った。むしろ、設計の意図を正確に伝えることがキーポイントであった。その意味で、当初の文書と妥当性確認結果受領、討論後の文書を見比べることで、参考となるものと考える。

9. 同じく、説明に関しては、制御システムのなかの安全関連部は、略さずに記すこと必要であった。これは、回路図をそのまま記載するという意味ではない。制御回路の安全関連部の作動説明は、詳しく説明する必要があった。今回、当初の文書では、BG としての経験からある程度の推定をして評価していたように思われる点があった。安全機能、その具現法をきちんと表現しきるスキルは、電気設計と同じように重要である。
10. DC については、根拠を示すことが要求された。
11. なお、ベッカー氏の一般講演のなかで言及されていたが、IEC 62061 との整合化は今後の課題である。実際、ISO、IEC 両団体でも、リエゾンを作って議論中である。この動向は、次の ISO 13849 の改正につながるので、注視が必要でるとともに、我が国からも積極的な提案がなされてしかるべきである。

以上のように、印刷産業機械での使用を想定して、PLr に適合した回路の計算事例を例示することにより、PL 評価の一連の手順を示した。また、その際に援用できるコンピュータによる自動計算システム SISTEMA の日本語の解説書を作成した。このことにより、業界各社において設計した安全制御回路の PL の検証が、容易かつ日本語で操作法を確認しながら実施可能となった。

これらは調査・研究の結果は、印刷産業機械の安全化への対応に関するレベルアップに貢献するとともに、中小企業が多くを占める本業界分野全体に大きな成果であると考える。

PL は信頼性評価が新に加わったことは、大きな変更であるし、コンポーネントメーカーの協力を得てデータを準備する、PL の推算をするなど、いままでの回路設計以外に行うことが増えた。しかし、今回の PL 評価実証研究及び実機での対応状況の調査から、基本的なことは従来の安全制御回路でも対応できることが示唆された。

準備は必要であるが、既存の技術を基本に、データの用意及び信頼性の基礎的な知識で対応できるものと考えられる。その準備としては、本報告書の各章がガイドラインとなり得ると考えている。

謝辞

本調査研究を進めるなかで、電気業界、工作機械業界等の多くの方々には、ご講演など頂いたことに対し感謝致します。また、今回の調査研究の一部を委託した NPO 安全工学研究所の期待以上の協力と業務報告に感謝致します。併せて、本事業においては、今までの調査研究以上に委員各位と事務局の努力――それは自社のためではなく、工業界全体の安全向上と合理的な設計、認証取得のための努力――があり、その成果が妥当性検証、付録その他の資料として結実しました。委員及び事務局各位に感謝の意を表します。

― 資料編 ―

1. BGIA Report 回路図解説書（翻訳・仮訳の紹介）..... 120
2. BG-SISTEMA の概要..... 185
2.1 SISTEMA とは..... 185
2.2 SISTEMA のダウンロードとインストール..... 185
2.2.1 ダウンロード方法..... 185
2.2.2 インストール方法..... 185
2.3 SISTEMA 基本操作説明..... 186
2.3.1 Main window（メイン画面）..... 186
2.3.2 ナビゲーションパネルのオブジェクトタイプ（Object type）の記号説明..... 187
2.3.3 操作画面の用語説明..... 188
2.3.4 その他の操作説明..... 189
2.3.5 メッセージパネル（Massage pane）の説明..... 193
2.4 SISTEMA の回路例による操作説明..... 195
2.4.1 回路例 5：可動式ガードの位置監視-カテゴリ 1(PL=c)..... 195
2.4.2 回路例 9：試験済み光バリア-カテゴリ 2- PL=c..... 207
2.4.3 回路例 17：安全モジュールによる保護装置のカスケード-カテゴリ 3（PL=d)..... 220
3. ISO 13849-1:2006 の疑問点と BG からの回答..... 232

1.BGIA Report 回路図解説書（翻訳・仮訳の紹介）

BGIA Report2/2008 和訳（仮訳）箇所

No.	回路番号	カテゴリ-PL	備考
1	8.2.4	Cat.1 - PLc	電気回路
2	8.2.5	Cat.1 - PLc	電気回路
3	8.2.6	Cat.1 - PLc	電気回路
4	8.2.8	Cat.1 - PLc	電気回路
5	8.2.9	Cat.2 - PLc	電気回路
6	8.2.10	Cat.3 - PLc	電気回路
7	8.2.17	Cat.3 - PLd	電気回路
8	8.2.18	Cat.3 - PLd	電気回路
9	8.2.20	Cat.3 - PLd	電気回路
10	8.2.21	Cat.3 - PLd	電気回路
11	8.2.22	Cat.3 - PLd	電気回路
12	8.2.24	Cat.3 - PLd	電気回路
13	8.2.28	Cat.4 - PLe	電気回路
14	8.2.29	Cat.3 - PLe	電気回路
15	8.2.30	Cat.3 - PLe	電気回路
16	8.2.34	Cat.4 - PLe	電気回路
17	8.2.36	Cat.4 - PLe	電気回路

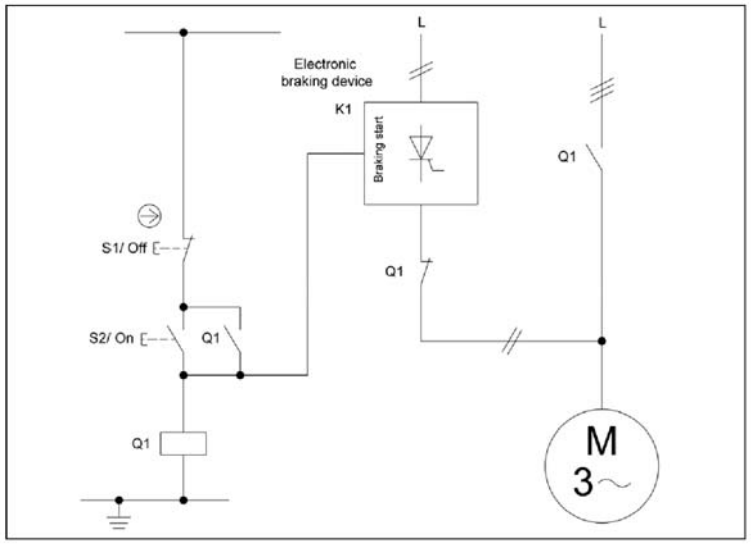
＊当委員会では、BGIA Report2/2008 の第 8 章の回路の解説のうち電気回路を中心に英語版の和訳（仮訳）を行った。なお、和訳の内容及び用語等に関して確認を要する場合には、原本である独文又は英文を参照されたい。

http://www.dguv.de/ifa/de/pub/rep/pdf/rep07/biar0208/2_2008.pdf （独文）

http://www.dguv.de/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf（英文）

8.2.4 Stopping of woodworking machines – Category 1 – PL c (Example 4)

Figure 8.9:
Combination of electromechanical control equipment and a simple electronic braking device for the stopping of woodworking machines



Safety function

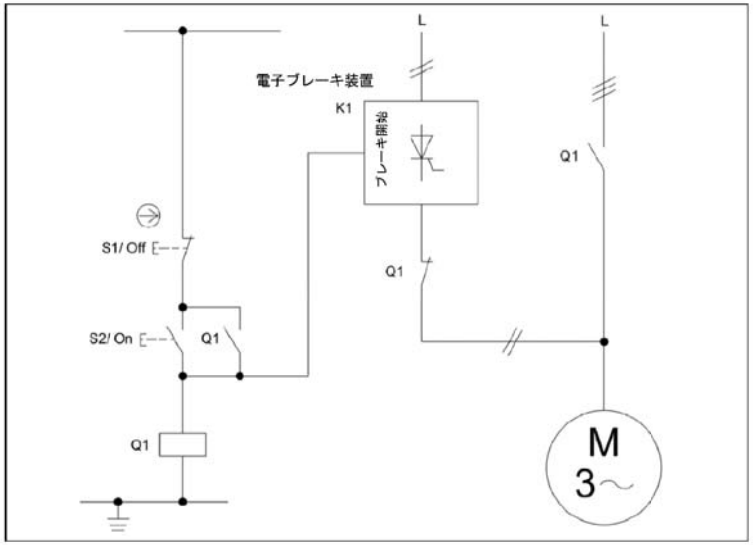
- Actuation of the Off button leads to SS1 (safe stop 1), a controlled stopping of the motor within a maximum permissible time.

Functional description

- Stopping of the motor is initiated by actuation of the Off button S1. The motor contactor Q1 drops out and the braking function is initiated. The motor is braked by a direct current generated in braking unit K1 by a thyristor employing phase-angle control and generating a braking torque in the motor winding.
- The run-down time must not exceed a maximum value (e.g. 10 seconds). The level of braking current required for this purpose can be set by means of a potentiometer on the braking unit.

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。

- Upon expiration of the maximum braking time, the control signal to the thyristor ceases and the current path for the braking current is interrupted. The stopping process corresponds to a Category 1 stop in accordance with EN 60204-1.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The de-energization principle (closed-circuit current) is employed as the basic safety principle. For protection against unexpected start-up following restoration of the power supply, the control system features latching-in at Q1.
- S1 is a pushbutton with positive mode of actuation to IEC 60947-5-1, Annex K (direct opening action). S1 is therefore regarded as a well-tried component.
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.
- The braking unit K1 is designed exclusively from simple electronic components such as transistors, capacitors, diodes, resistors and thyristors, which are regarded as well-tried components. Fault-free performance of the safety-related braking function is characterized by the selection of the components. Internal measures for fault detection are not implemented. No complex electronic components (e.g. microprocessors) are employed that are not considered to be in accordance with EN ISO 13849-1, Section 6.2.4 as being equivalent to well-tried components.

Application

- On woodworking machines or similar machines on which unbraked stopping would result in an impermissibly long run-down of the hazardous tool movements. The control system must be designed such that at least PL b is attained (GS-HO-01 test principles for woodworking machines).

Calculation of the probability of failure

- S1 is a pushbutton with positive mode of actuation to IEC 60947-5-1, Annex K (direct opening action). If a pushbutton of this type is employed as a control device, fault exclusion is possible for failure of the electrical contact to open, including the mechanical components within the push-button.
- $MTTF_d$: a B_{10d} value of 2,000,000 switching operations [S] is assumed at nominal load for the contactor Q1. At 300 working days, 8 working hours and a cycle time of 2 minutes, n_{op} is 72,000 cycles per year and the $MTTF_d$ is

- 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。

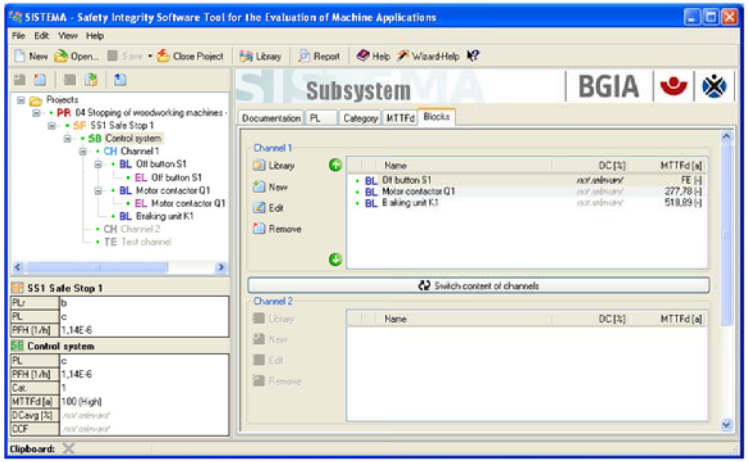
277 years. The $MTTF_d$ for the braking unit K1 was determined by means of the parts count method. The parts information from the parts list and the values from the SN 29500 database [36] produce an $MTTF_d$ of 518 years [D]. The combination of Q1 and K1 results in an $MTTF_d$ of 180 years for the channel, which is capped to 100 years ("high").

- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c. The PL_r of b is therefore surpassed.

More detailed reference

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

Figure 8.10:
Determining of the PL by means of SISTEMA



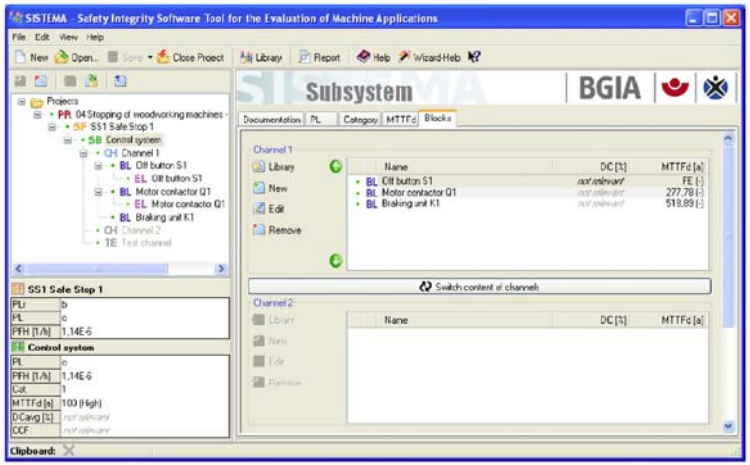
ブレーキユニット K1 の $MTTF_d$ は部品カウント法により決定される。パーツリストからのパーツ情報と SN 29500 データベース[36]からの値で、$MTTF_d$ は 518 年[D]となる。Q1 と K1 の組み合わせで、そのチャンネルの $MTTF_d$ は 180 年となり、上限の 100 年（「高」）に達する。

- 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 1.14×10^{-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 Position monitoring of moveable guards – Category 1 – PL c (Example 5)

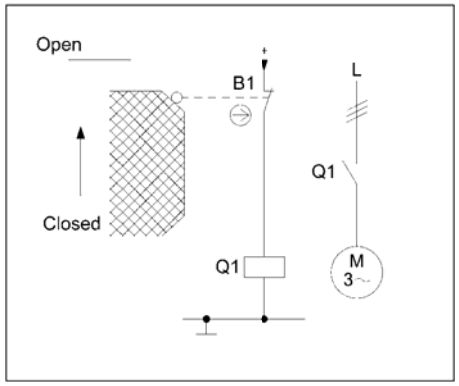


Figure 8.11:
Position monitoring of moveable guards for the prevention of hazardous movements (STO – safe torque off)

Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO – safe torque off.

Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by a position switch B1 with direct opening action which actuates a contactor Q1. The dropping out of Q1 interrupts or prevents hazardous movements or states.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.
- Removal of the protective device is not detected.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle is employed as a basic safety principle. Earthing of the control circuit is regarded as a well-tried safety principle.

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

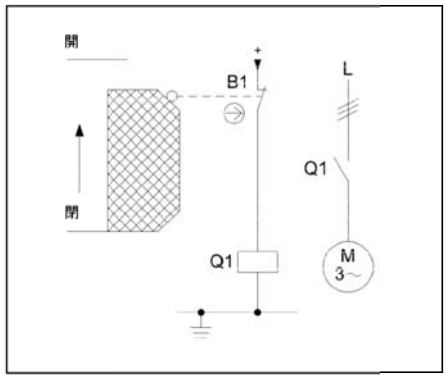


図 8.11：
危険動作防止のための可動式ガードの位置監視
（STO－安全トルクオフ）

安全機能

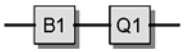
- 保護装置によって起動する安全関連停止機能：可動式ガードが開くことで安全機能 STO－安全トルクオフが起動する。

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。



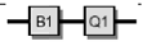
- Switch B1 is a position switch with direct opening action in accordance with IEC 60947-5-1, Annex K and is therefore regarded as a well-tried component. The break contact interrupts the circuit directly mechanically when the protective device is not in the safe position.
- Contactor Q1 is a well-tried component provided that the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.
- A position switch is employed for position monitoring. A stable arrangement of the protective device is assured for actuation of the position switch. The actuating elements of the position switch are protected against displacement. Only rigid mechanical parts (no spring elements between actuator and contact) are employed.
- The actuating stroke for the position switch complies with the manufacturer's specification.

Calculation of the probability of failure

- $MTTF_d$: fault exclusion for the direct opening electrical contact is possible for B1. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1. At 365 working days, 16 working hours per day and a cycle time of 10 minutes, n_{op} is 35,045 cycles per year and the $MTTF_d$ is 285 years for these components. For contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,300,000 switching cycles [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_d$ of 742 years for Q1. The combination of B1 and Q1 results in an $MTTF_d$ of 206 years for the channel. This value is capped to 100 years ("high").
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c. The PL_r of b is therefore surpassed.

More detailed reference

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



- 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、N.C. 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 1.14×10^{-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)

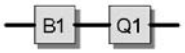
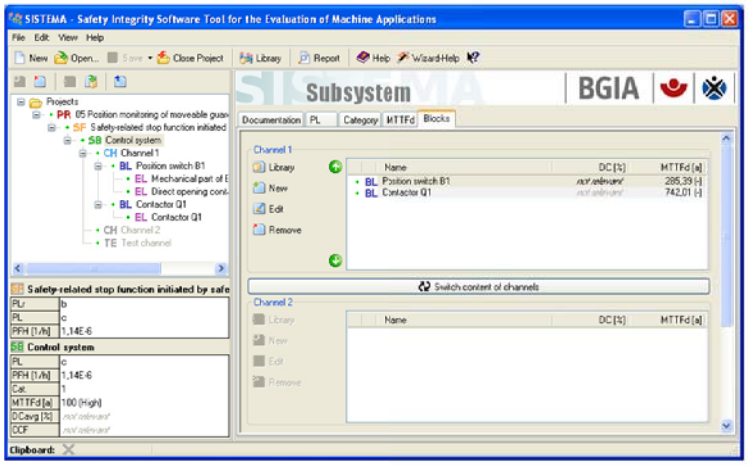


Figure 8.12:
Determining of the PL by means of SISTEMA



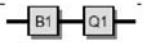
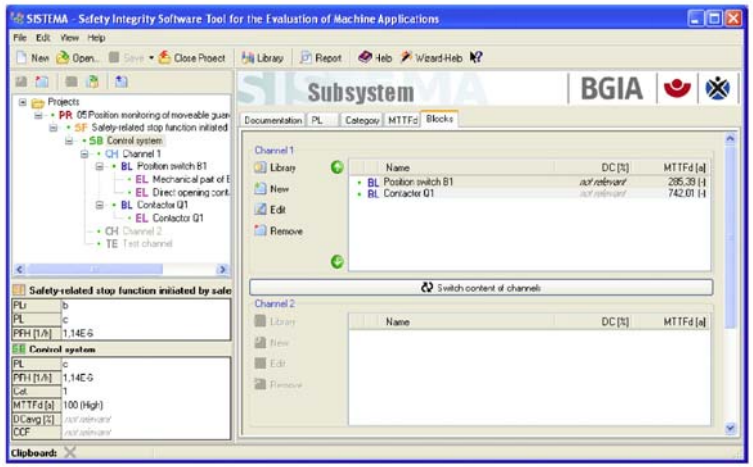


図 8.12： SISTEMA による PL の決定



8.2.6 Start/stop facility with emergency stop device – Category 1 – PL c (Example 6)

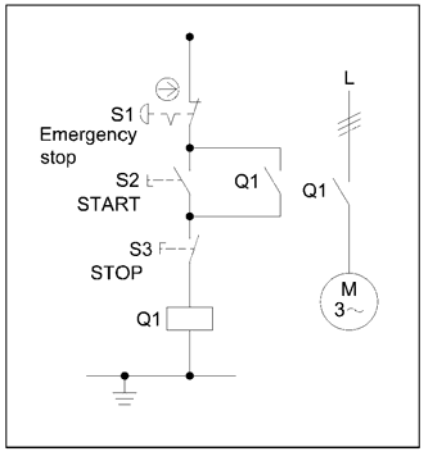


Figure 8.13:
Combined start/stop facility with emergency stop device

Safety function

- Emergency stop function, STO – safe torque off by actuation of the emergency stop device

Functional description

- Hazardous movements or states are de-energized by interruption of the control voltage of contactor Q1 when the emergency stop device S1 is actuated.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- No measures for fault detection are implemented.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The closed-circuit current principle is employed as a basic safety principle. The control circuit is also earthed, as a well-tried safety principle.

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）

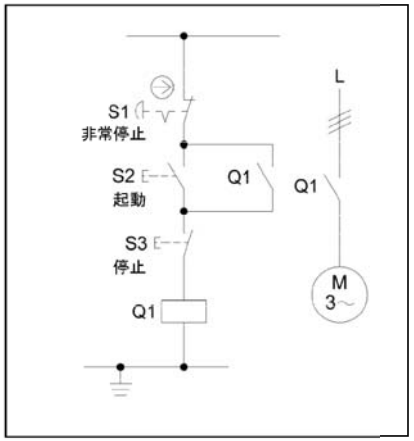


図 8.13：
非常停止装置付き起動/停止複合設備

安全機能

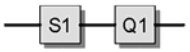
- 非常停止機能、非常停止装置の作動による STO－安全トルクオフ

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。



- The emergency stop device S1 is a switch with direct mode of actuation in accordance with IEC 60947-5-1, Annex K, and is therefore a well-tried component in accordance with Table D.4 of EN ISO 13849-2.
- The signal is processed by a contactor (stop category 0 to EN 60204-1).
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.

Remark

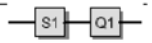
- The function for stopping in an emergency is a protective measure which complements the safety functions for the safeguarding of hazardous zones.

Calculation of the probability of failure

- $MTTF_d$: S1 is a standard emergency stop device to EN ISO 13850. Fault exclusion applies for the direct opening contact and the mechanical elements, provided the number of operations indicated in Table D.2 of this report is not exceeded. For contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,300,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. If the start/stop facility is assumed to be actuated twice a day on 365 working days and the emergency stop device to be actuated three times a year, then at an n_{op} of 733 cycles per year, Q1 has an $MTTF_d$ of 35,470 years. This is also the $MTTF_d$ for the channel, which is capped to 100 years ("high").
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. This corresponds to PL c.

More detailed references

- 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)



- 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

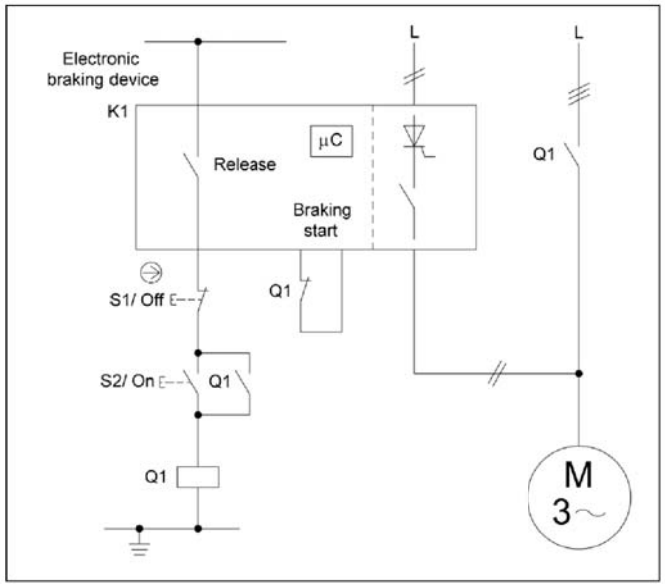
- $MTTF_d$：S1 は EN ISO13850 の標準非常停止装置である。本レポートの表 D.2 に記載の操作回数を超えなければ、フォールト（故障）の排除が直接開接点および機械的要素に適用される。接触器 Q1 では、誘導負荷（AC 3）下において、B_{10} 値は 1,300,000 回の開閉操作[M]の電気的寿命に相当する。故障の 50%を危険側だと仮定すると、B_{10d} 値は B_{10} 値の 2 倍になる。起動/停止設備が稼働日 365 日で 1 日に 2 回作動し、非常停止装置が 1 年に 3 回作動すると仮定すると、1 年あたり 733 サイクルの n_{op} で、Q1 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 1.14×10^{-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 Stopping of woodworking machines – Category 1 – PL c (Example 8)

Figure 8.15:
Combination of electromechanical control equipment and a programmable electronic braking device for the stopping of woodworking machines



Safety function

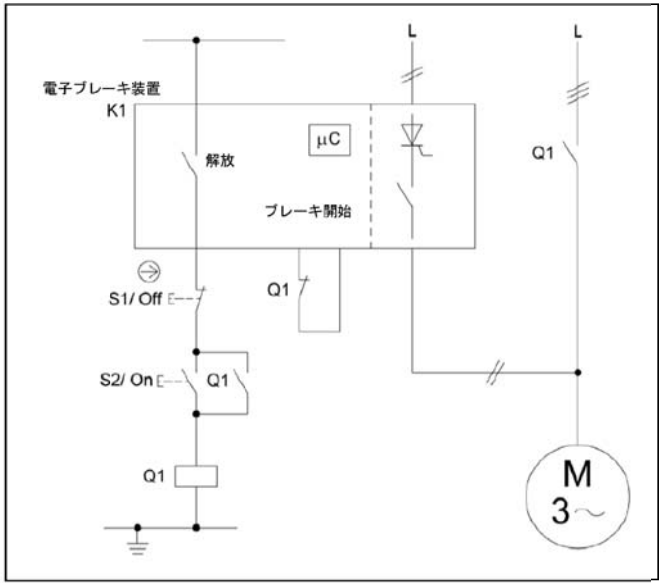
- Actuation of the Off button leads to SS1 (safe stop 1), a controlled stopping of the motor within a maximum permissible time.

Functional description

- Stopping of the motor is initiated by actuation of the Off button S1. The motor contactor Q1 drops out and the braking function is initiated. The motor is braked by a direct current generated in braking unit K1 by thyristors employing phase-angle control, and which is connected to the motor winding by internal relays.
- The run-down time must not exceed a maximum value (e.g. 10 seconds). The desired run-down time and any other required parameters (e.g. braking current, threshold for zero-speed detection) can be set on the braking device.

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。

- Once the motor is stationary or upon expiration of the maximum braking time, the braking device switches off the braking current and disconnects the motor again from the supply. The stopping process corresponds to a Category 1 stop in accordance with EN 60204-1.
- The safety function cannot be maintained with all component failures, and is dependent upon the reliability of the components.
- Fault-free performance of the braking function is monitored regularly by the braking device K1. Should a fault be detected, e.g. exceeding of the maximum permissible braking time, a release contact in the device prevents the motor from restarting. Measures for fault detection are not implemented in S1 or Q1.

Design features

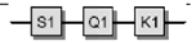
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented. The de-energization principle (closed-circuit current) is employed as the basic safety principle. For protection against unexpected start-up following restoration of the power supply, the control system features latching-in at Q1.
- S1 is a pushbutton with direct mode of actuation to IEC 60947-5-1, Annex K (direct opening action). S1 is therefore regarded as a well-tried component.
- Contactor Q1 is a well-tried component provided the additional conditions in accordance with Table D.4 of EN ISO 13849-2 are observed.
- The braking device K1, which is controlled by a microcontroller, meets all requirements for Category 2 and PL c. The safety-related functions are tested at regular intervals. The program sequence timing of the microcontroller is monitored by a separate watchdog.

Application

- On woodworking machines or similar machines on which unbraked stopping would result in an impermissibly long run-down of the hazardous tool movements. The control system must be designed such that at least Performance Level b is attained (GS-HO-01 “Test principles for woodworking machines”).

Calculation of the probability of failure

- Since a standard module is employed for the electronic braking device K1, its probability of failure (5.28 × 10^{-7} per hour [M]) is added following calculation by SISTEMA. For the remaining part of the control system, the probability of failure is calculated below.
- S1 is a pushbutton with direct mode of actuation to IEC 60947-5-1, Annex K (direct opening action). If a pushbutton of this type is employed as a control device, fault exclusion is possible for failure of the electrical contact to open, including for the mechanical components within the push-button.



- 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-HC-01）

故障確率計算

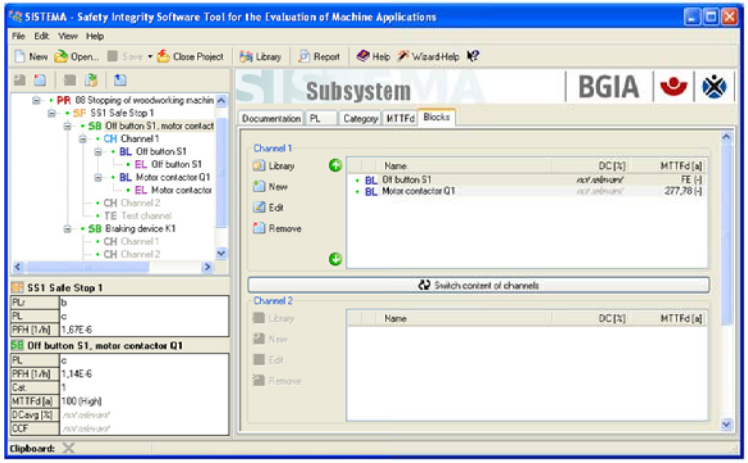
- 電子ブレーキ装置 K1 には標準モジュールが採用されているため、故障の確率（5.28 x 10^{-7}/hr [M]）が SISTEMA による下記の計算に追加される。制御システムの残りの部分については、故障確率を下記の通り計算する。
- S1 は、IEC 60947-5-1　付属書 K（直接開動作）の直接作動モード付き押しボタンである。この種の押しボタンが制御装置として採用されていれば、押しボタン内の機械的構成部品を含む電気接点が開かない故障によるフォールト（故障）を排除することが可能である。

- $MTTF_d$: a B_{10d} value of 2,000,000 switching operations [S] at nominal load is assumed for the contactor Q1. At 300 working days, 8 working hours and a cycle time of 2 minutes, n_{op} is 72,000 cycles per year and the $MTTF_d$ is 277 years. This is also the $MTTF_d$ for the channel, which is capped to 100 years ("high").
- DC_{avg} and measures against common cause failures are not relevant in Category 1.
- The electromechanical control system, consisting of S1 and Q1, corresponds to Category 1 with a high $MTTF_d$ (100 years). This results in an average probability of dangerous failure of 1.14×10^{-6} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 1.67×10^{-6} per hour. This corresponds to PL c. The PL_r of b is therefore surpassed.

More detailed reference

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

Figure 8.16:
Determining of the PL by means of SISTEMA

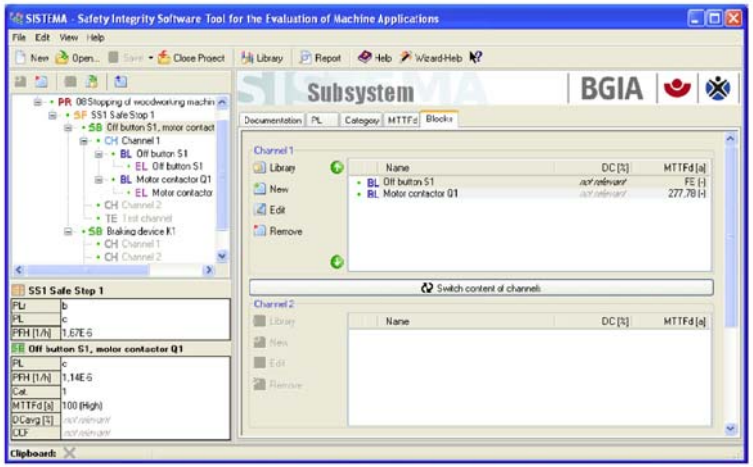


- $MTTF_d$：定格負荷での 2,000,000 回の開閉操作の B_{10d} 値[S]を接触器 Q1 に対して想定する。稼働日 300 日、稼働時間 8 時間、サイクル時間が 2 分の場合、n_{op} は 1 年に 72,000 サイクルで、$MTTF_d$ は 277 年となる。これはまたチャンネルの $MTTF_d$ であり、上限の 100 年（「高」）に達する。
- カテゴリー1 では、DC_{avg} と共通原因故障に対する対策は関係しない。
- S1 および Q1 からなる電気機械制御システムは、高い $MTTF_d$（100 年）のカテゴリー1 に相当する。これにより、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

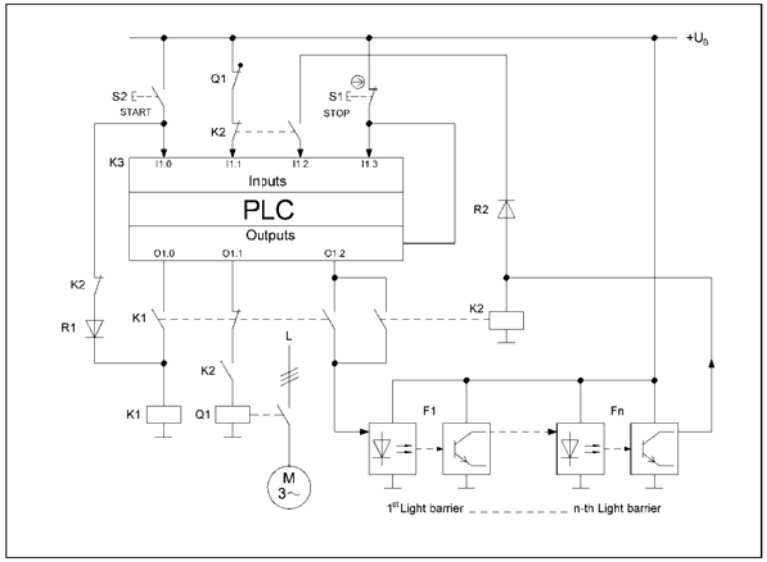
- Grundsätze für die Prüfung und Zertifizierung von Holzbearbeitungsmaschinen GS-HO-01 (12/2007). www.dguv.de, Webcode d14898

図 8.16：SISTEMA による PL の決定



8.2.9 Tested light barriers – Category 2 – PL c with downstream Category 1 output signal switching device (Example 9)

Figure 8.17:
Testing of light barriers with a standard PLC



Safety function

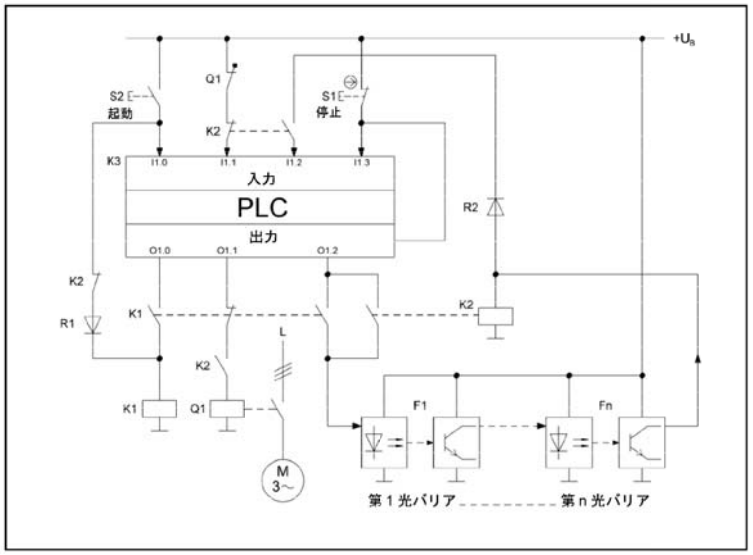
- Safety-related stop function, initiated by a protective device: when the light beam is interrupted, a hazardous movement is halted (STO – safe torque off).

Functional description

- Interruption of the light beam of the *n* cascaded light barriers F1 to Fn triggers a de-energization command both by relays, by de-energization of the contactor relay K2, and via the PLC output (O1.1) of the test channel. The hazardous movement is then halted by means of the contactor Q1.
- The light barriers are tested before each start of the hazardous movement following pressing of the start button S2. For this purpose, PLC output O1.2 de-energizes the light barrier transmitter in response to a software command. The reaction of the receiver (K2 drops out again) is monitored on PLC inputs I1.1 and I1.2. Provided the behaviour is free of faults, K2 seals in via O1.2, and

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

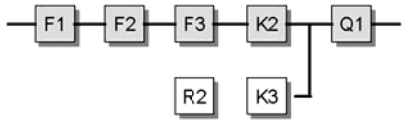


安全機能

- 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。

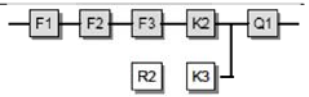


the hazardous movement can be initiated by the releasing of S2. K1 is de-energized via O1.0, and the main contactor Q1 actuated via O1.1.

- Should a fault in a light barrier or in K2 be detected by the test, the outputs O1.1 and O1.2 are deactivated, and an actuating signal is no longer applied to the main contactor Q1.
- In the event of global failure of the PLC (output O1.0 at low potential, outputs O1.1 and O1.2 at high potential), interruption of a light beam results in de-energization of K2, independently of the PLC. In order to ensure this independence, the light barrier outputs are decoupled from the PLC by the decoupling diode R2. Under unfavourable circumstances, the light barriers can be re-activated by K2 by actuation of the start button, and the main contactor Q1 thus actuated. In this case the test equipment (only) would have failed. Failure of the test equipment is detected owing to the probability of a functionally defective process under these circumstances.
- During the test, actuation of Q1 by K1 and O1.1 is blocked.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Special light barriers with adequate optical characteristics (aperture angle, extraneous light immunity, etc.) to IEC 61496-2 are employed.
- Several light barriers can be cascaded and monitored by only two PLC inputs and a relay or contactor relay.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L. The contactor Q1 possesses a mirror contact in accordance with IEC 60947-4-1, Annex F.
- The standard components F1 to Fn and K3 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.
- The start button S2 must be located outside the hazardous area and at a point from which the hazardous area/danger point is visible.
- The number, arrangement and height of the light beams must comply with EN 999 and IEC 62046.

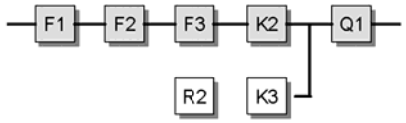


K1 は O1.0 により遮断され、主接触器 Q1 は O1.1 によって作動する。

- 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。



- Should an arrangement for the safeguarding of hazardous areas permit stepping behind the sensing field, further measures are required, such as a restart interlock. The start button S2 can be used for this purpose. To this end, the PLC K3 compares the duration for which the button is pressed with maximum and minimum values. Only if the conditions are met is a start command assumed to be valid.

Remarks

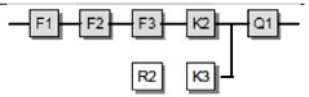
- The example is intended for use in applications with an infrequent demand upon the safety function. This enables the requirement of the designated architecture for Category 2 to be satisfied, i.e. “testing much more frequent than the demand upon the safety function” (cf. Annex G).
- Following triggering of a stop, the light barriers remain deactivated until the next start. This enables a hazardous area, for example, to be entered without this being “registered” by the circuit. The behaviour can be modified by corresponding adaptation of the circuit.

Calculation of the probability of failure

- For the sake of example, three light barriers F1 to F3 are considered for calculation of the probability of failure. Safeguarding of a second hazardous zone constitutes a further safety function for which calculation is performed separately.
- For calculation of the probability of failure, the overall system is divided into two subsystems, “light barriers” and “main contactor” (Q1).

For the “light barriers” subsystem:

- F1, F2, F3 and K2 constitute the functional path of the Category 2 circuit structure; the PLC K3 (including decoupling diode R2) constitutes the test equipment. S2 and K1 have the function of activating testing of the light barrier, and are not involved in the calculation of the probability of failure.
- $MTTF_d$: an $MTTF_d$ of 100 years [E] is assumed for each of F1 to F3. The B_{10d} value for K2 is 20,000,000 cycles [S]. At 240 working days, 16 working hours and a cycle time of 180 seconds, n_{op} is 76,800 cycles per year. Testing as described above doubles this value, to an n_{op} of 153,600 cycles per year with an $MTTF_d$ of 1,302 years for K2. These values yield an $MTTF_d$ of 32 years (“high”) for the functional channel. An $MTTF_d$ of 50 years [E] is assumed for K3. In comparison, the $MTTF_d$ value of 228,311 years [S] for the decoupling diode R2 is irrelevant.



- 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

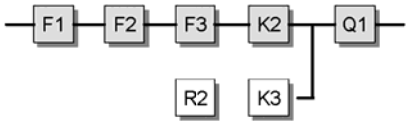
- この例は、安全機能へのまれな要求がある場合に適用するためのものである。これは、カテゴリー2 に対する規定アーキテクチャへの要求事項、すなわち「安全機能へのデマンドよりもはるかに頻繁な試験」（付属書 G 参照）を満たすことを可能にする。
- 停止の始動後も、光バリアは次の起動まで停止状態を保持する。これにより例えば、それを回路に「登録」せずに、危険領域に入る事が可能となる。該当する回路の適用により動作を修正できる。

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、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、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。



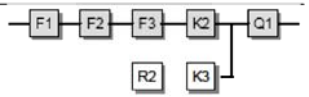
- DC_{avg}: the DC of 60% for F1 to F3 is attributable to the function test as described. The *DC* of 99% for K2 is derived from direct monitoring in K3 with the aid of mechanically linked contact elements. The averaging formula for DC_{avg} returns a result of 61.0% ("low").
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements in the "light barriers" subsystem corresponds to Category 2 with a high $MTTF_d$ per channel (32.5 years) and low DC_{avg} (61.0%). This results in an average probability of dangerous failure of 1.85×10^{-6} per hour.

The following assumptions are made for the "main contactor" subsystem:

- B_{10d} = 2,000,000 cycles [S] with a n_{op} of 76,800 cycles per year. This leads to an $MTTF_d$ of 260.4 years, which in accordance with the standard is capped to 100 years. The structure corresponds to Category 1; DC_{avg} and common cause failures are not therefore relevant. The resulting average probability of dangerous failure is 1.14×10^{-6} per hour.
- Addition of the average probability of dangerous failure of the two subsystems results in a value of 3.0×10^{-6} per hour. This corresponds to PL c.
- If it is anticipated that a demand will be made upon the safety function more frequently than assumed for the Category 2 designated architecture (the ratio is lower than 100 : 1, i.e. more frequently than once every 5 hours), this can be considered in accordance with Annex G down to a ratio of 25 : 1 with a penalty of 10%. In the case considered here with three light barriers, the "light barriers" subsystem still attains a probability of failure of 2.04×10^{-6} per hour. The overall average probability of dangerous failure of 3.18×10^{-6} per hour only attains PL b, however. For PL c to be attained, the number of light barriers would for example have to be reduced, or components with a higher $MTTF_d$ employed.

More detailed references

- *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)



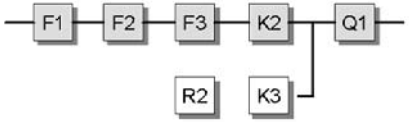
- DC_{avg} : F1 から F3 の 60%の DC は、記載の通り機能試験による。K2 の 99%の DC は、機械的に連結した接点要素を用いた K3 での直接監視から算出される。DC_{avg} の平均化式により 61.0%（「低」）の結果が返る。
- 共通原因故障に対する適正な対策（85 点）: 分離（15）、多様性（20）、過電圧保護など（15）および環境条件（25 + 10）
- 「光バリア」サブシステムにおける制御要素の組み合わせは、チャンネルごとの高い $MTTF_d$（32.5 年）と低い DC_{avg}（61.0%）のカテゴリー2 に相当する。これにより、危険側故障の平均確率は 1 時間あたり 1.85×10^{-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 1.14×10^{-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 3.0×10^{-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 2.04×10^{-6} の故障確率がある。しかしながら、1 時間あたり 3.18×10^{-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。

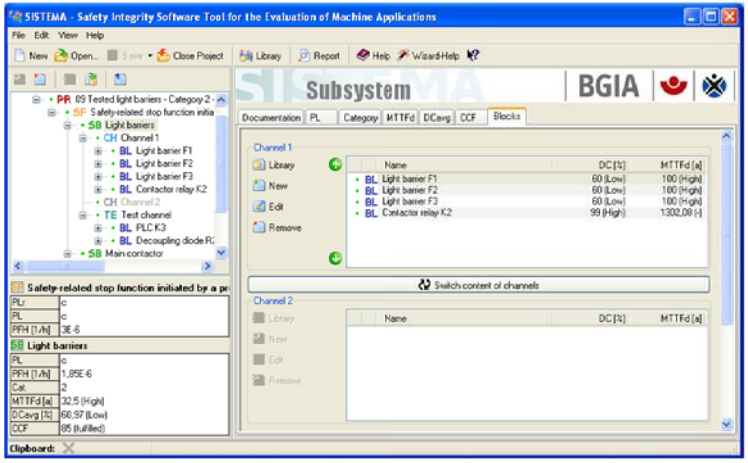
より詳細な参考文献

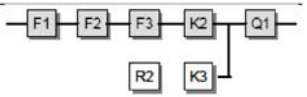
- *Grigulewitsch, W.; Reinert, D.*: Lichtschranken mit Testung. In: BGIA-Handbuch Sicherheit und Gesundheitsschutz am Arbeitsplatz. Kennzahl 330 228. 22th suppl. V/94. Ed.: BGIA – Institut für Arbeitsschutz der Deutschen Gesetzlichen Unfallversicherung, Sankt Augustin. Erich Schmidt, Berlin, 1985 – loose-leaf 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)

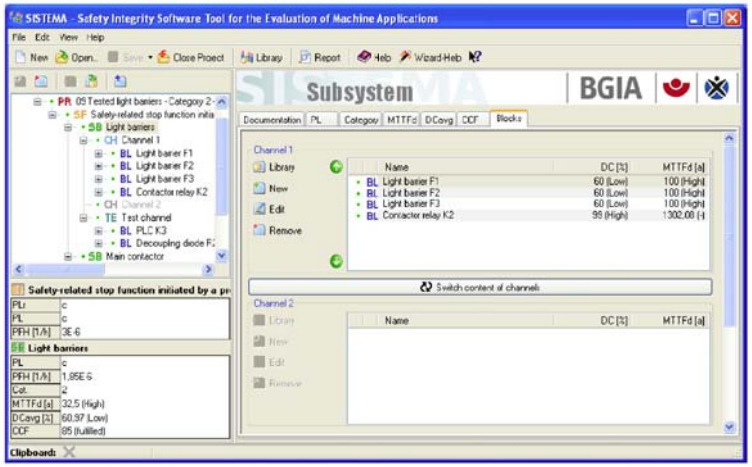
Figure 8.18:
Determining of the PL by means of SISTEMA





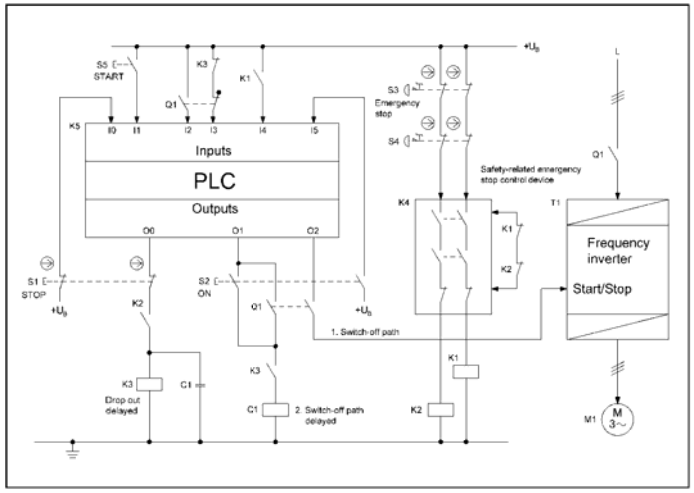
- IEC 61496-2: Safety of machinery – Electro-sensitive protective equipment – Part 2: Particular requirements for equipment using active opto-electronic protective devices (AOPDs) (04.06)
- IEC 62046: Safety of machinery – Application of protective equipment to detect the presence of persons (draft standard 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 Safe stopping of a PLC-driven drive with emergency stop – Category 3 – PL c (Example 10)

Figure 8.19:
Stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command



Safety function

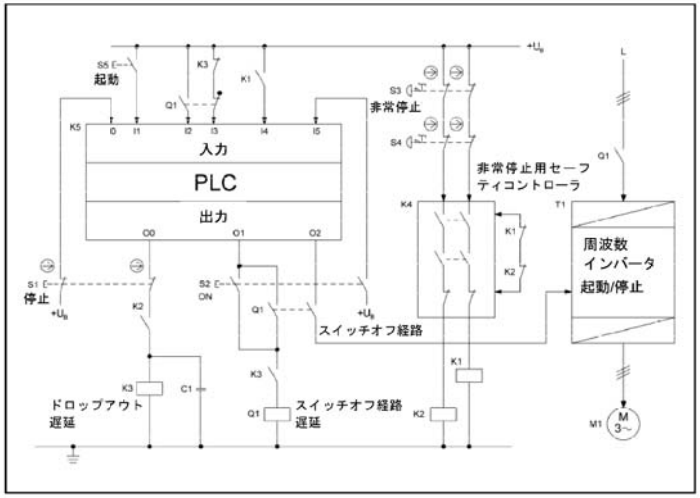
- Safety-related stop function/emergency stop function: following a stop or emergency stop command, the drive is halted (SS1 – safe stop 1).

Functional description

- The hazardous movement is interrupted redundantly if either the stop button S1 or one of the emergency stop devices S3 or S4 is actuated. The drive is halted in an emergency following actuation of S3/S4, resulting in deactivation of the safety-related emergency stop control device K4 and de-energization of the contactor relays K1 and K2. Opening of the make contact K1 on input I4 of the PLC K5 causes the starting signal on the frequency inverter (FI) T1 to be cancelled via the PLC output O2. Redundantly to the K1-K5-T1 chain, opening of the make contact K2 upstream of the contactor relay K3 (with drop-out delay) initiates a braking timer. Upon timeout of the braking timer the actuating signal for the mains contactor Q1 is interrupted. The timer setting is selected such that under unfavourable operating conditions, the machine movement is halted before the mains contactor Q1 has dropped out.

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

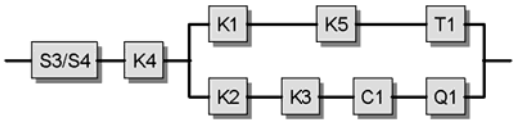


安全機能

- 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

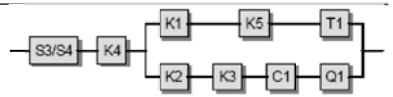
- 停止ボタン S1 または非常停止装置 S3 か S4 のうち 1 つの、どちらか片方でも作動すると、危険動作が冗長的に遮断される。非常時には S3/S4 の作動により非常停止用セーフティコントローラ K4 が出力せず、接触器リレーK1 および K2 が遮断されることで駆動が停止する。PLC K5 の入力 I4 の N.O.接点 K1 が開くと、PLC 出力 O2 によって周波数インバータ（FI）T1 への起動信号をキャンセルする。K1-K5-T1 経路に冗長して、接触器リレーK3（ドロップアウト遅延付き）の上流にある N.O.接点 K2 が開くと、ブレーキタイマーが開始する。ブレーキタイマ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。



- Functional stopping of the drive following a stop command is caused by the opening of the two break contacts of the stop button S1. As with stopping in an emergency, the status is first queried by PLC K5, in this case via input I0, and the FI is shut down by resetting of the PLC output O2. Redundantly to this process, the contactor relay K3 is de-energized – with drop-out delay provided by the capacitor C1 – and following timeout of the set braking time, the activation signal to mains contactor Q1 is interrupted.
- In the event of failure of the PLC K5, the frequency inverter T1, the mains contactor Q1, the contactor relays K1/K2 or the contactor relay with drop-out delay K3, stopping of the drive is assured since two mutually independent de-energization paths are always present. Failure of the contactor relays K1 and K2 to drop out is detected, at the latest, following resetting of the actuated emergency stop device. This is achieved by monitoring of the mechanically linked break contacts within the safety-related emergency stop control device K4. Failure of the auxiliary contactor K3 to drop out is detected, at the latest, before renewed start-up of the machine movement through feedback of the mechanically linked break contact to the PLC input I3. Failure of the mains contactor Q1 to drop out is detected by the mirror contact read in on PLC input I3.

Design features

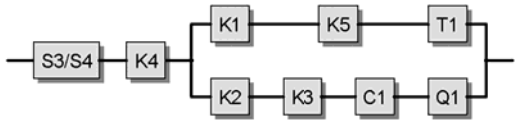
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The contactor relays K1, K2 and K3 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the pushbuttons S1, S3 and S4 are mechanically linked in accordance with IEC 60947-5-1, Annex K.
- The contactor Q1 possesses a mirror contact according to IEC 60947-4-1, Annex F.
- The standard components K5 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL b (downgraded owing to diversity) and the instructions in Section 6.3.
- The delayed initiation of the stopping by the second de-energization path alone in the event of a fault must not involve an unacceptably high residual risk.
- The safety-related control part of the safety-related emergency stop control device K4 satisfies all requirements for Category 3 and PL d.



- 停止ボタン S1 の 2 つの N.C.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 N.C.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 N.C.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。



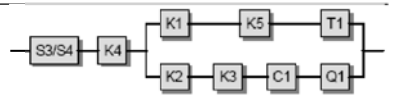
Calculation of the probability of failure

Only the probability of failure of the emergency stop function is calculated. For analysis of the safety-related stop function, S3/S4 and K4 must be replaced by S1, and K1 and K2 omitted.

- Fault exclusion is assumed for the emergency stop devices S3/S4, since the maximum number of 6,050 switching cycles within the mission time of the switching device as stated in Table D.2 is not exceeded. The safety-related emergency stop control device K4 is a tested safety component. Its probability of failure is 3.0×10^{-7} per hour [M], and is added at the end of the calculation. The value applies for a maximum number of 6,050 switching cycles within the mission time of the switching device.

The following applies for the probability of failure of the two-channel structure below:

- $MTTF_d$: the following $MTTF_d$ values are estimated: 25 years for K5 and 50 years for T1 [E]. The capacitor C1 is included in the calculation with an $MTTF_d$ of 45,662 years [D]. At a B_{10d} value of 400,000 cycles [S] and a switching frequency of daily energization on 240 working days, the result is an $MTTF_d$ of 16,667 years for K1 and K2. At a B_{10d} value of 400,000 cycles [S] and at 240 working days, 16 working hours and a cycle time of 3 minutes, the result for n_{op} is 76,800 cycles per year and for the $MTTF_d$ 52 years in each case for K3 and Q1. These values produce a symmetrized $MTTF_d$ of the channel of 21 years ("medium").
- DC_{avg}: fault detection by the process in the event of failure in the actuation of the deceleration ramp leads to a DC of 30% for K5. For T1, the DC is 60%, likewise as a result of fault detection by the process. K1 and K2 yield a DC of 99% owing to the integral fault detection in K4, and K3 a DC of 99% owing to fault detection by K5. For C1, the DC is 60% owing to testing of the timing element with the FI de-energized. For Q1, the DC is thus 99% owing to direct monitoring in K5. The averaging formula for DC_{avg} produces a result of 63% ("low").
- Adequate measures against common cause failure (75 points): separation (15), diversity (20), FMEA (5) and environmental conditions (25 + 10)
- The two-channel combination of the control elements satisfies Category 3 with a medium $MTTF_d$ per channel (21 years) and low DC_{avg} (63%). This results in an average probability of dangerous failure of 1.04×10^{-6} per hour. This corresponds to PL c. The overall probability of failure is determined by addition of the probability of dangerous failure of K4, and is equal to 1.34×10^{-6} per hour. This then likewise corresponds to PL c.



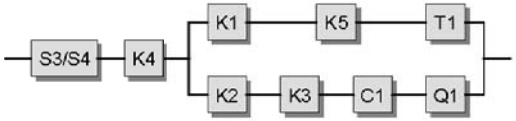
故障確率計算

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 3.0×10^{-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 1.04×10^{-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 1.34×10^{-6} に等しい。よってこれも同様に PL c に相当する。

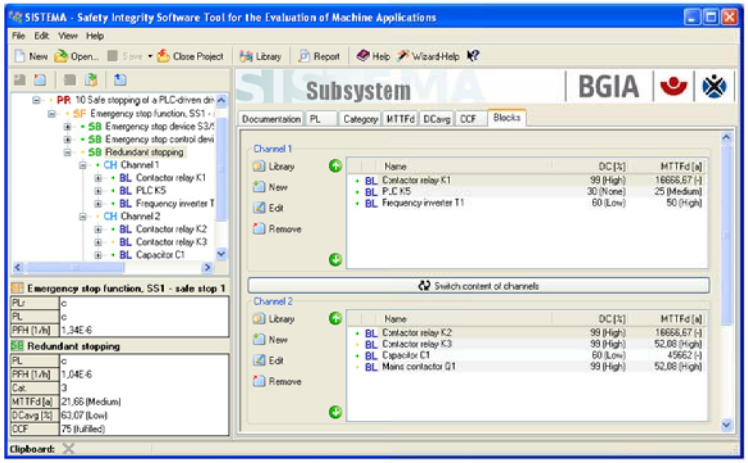


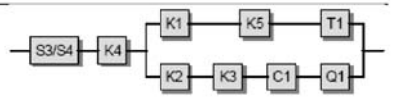
- The wearing elements K3 and Q1 should be replaced at intervals of approximately five years (T_{10d}).

More detailed references

- *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)

Figure 8.20:
Determining of the PL by means of SISTEMA



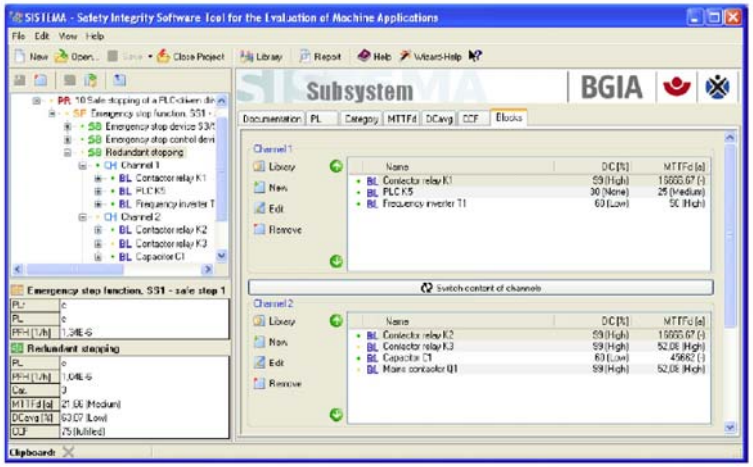


- 摩耗要素 K3 および Q1 は、約 5 年（T_{10d}）ごとに交換することが望ましい。

より詳細な参考文献

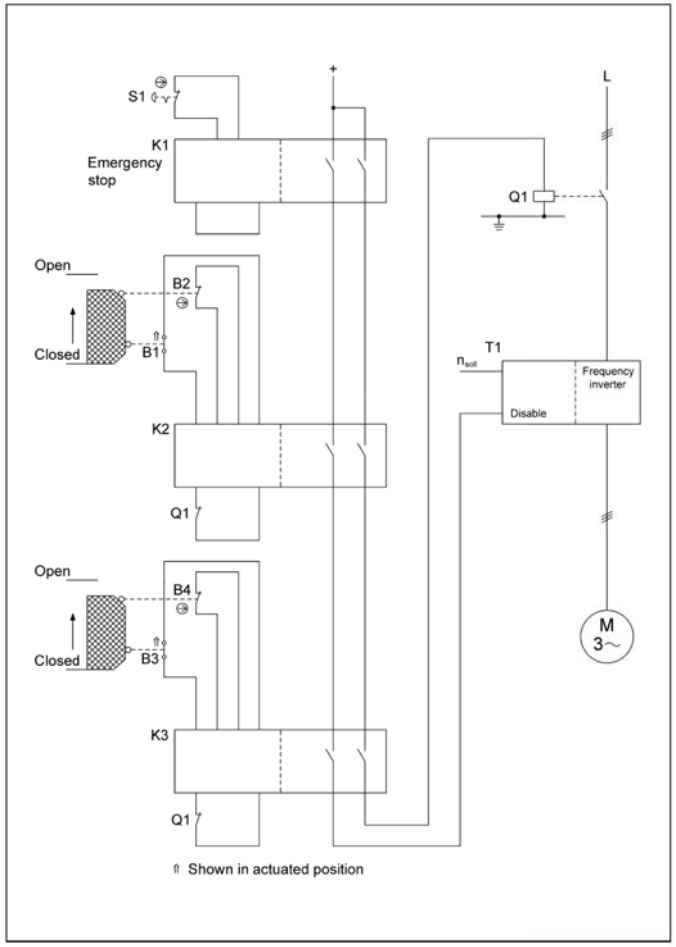
- *Apfeld, R.; Zilligen, H.*: Sichere Antriebssteuerungen mit Frequenzumrichtern. BIA-Report 5/2003. Ed.: Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), Sankt Augustin 2003.
  www.dguv.de/bgia, Webcode d6428
- IEC 61800-5-2: Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional (07.07)

図 8.20：SISTEMA による PL の決定



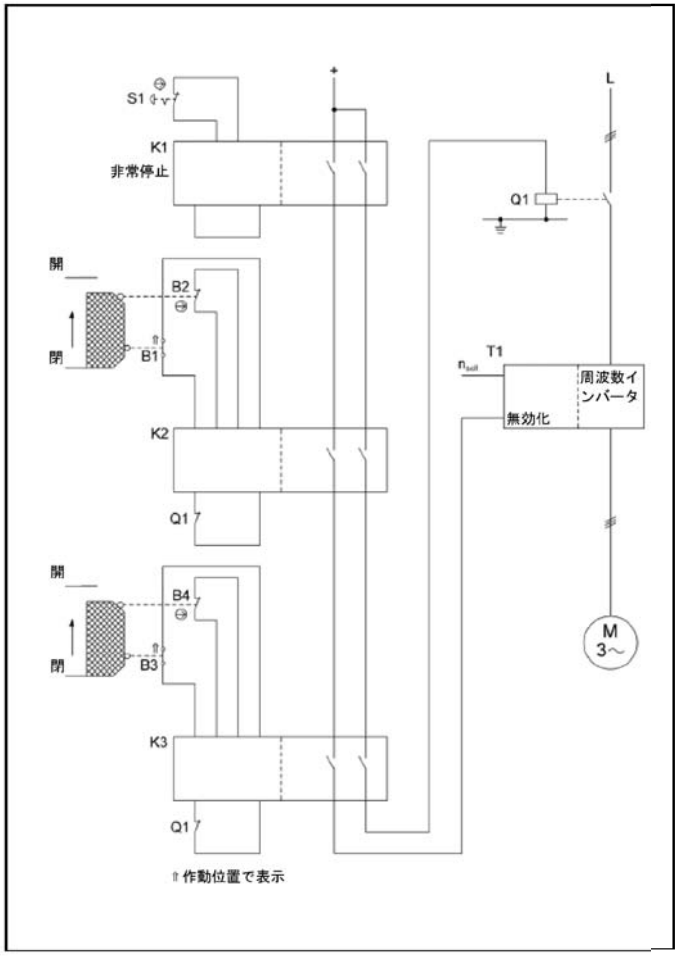
8.2.17 Cascading of protective devices by means of safety modules – Category 3 – PL d (Example 17)

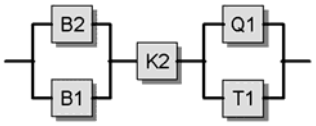
Figure 8.31:
Cascading of protective devices by means of safety modules
(emergency stop function, STO)



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）





Safety functions

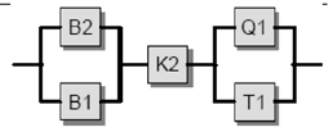
- Emergency stop function, STO – safe torque off by actuation of the emergency stop device
- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO – safe torque off.

Functional description

- Actuation of the emergency stop device S1 causes hazardous movements or states to be de-energized redundantly via the safety module K1, by interruption of the control voltage of the contactor Q1 and selection of the controller inhibit of the frequency inverter T1. A hazardous zone is also guarded by two moveable guards (e.g. one each for loading and unloading). Opening of the safety guard is detected by two position switches B1/B2 in a break contact/make contact combination, and evaluation by a central safety module K2. The latter can interrupt or prevent hazardous movements or states in the same way as K1. The second safety guard is monitored in the same way by the two position switches B3/B4 and a safety module K3, also acting upon Q1 and T1.
- The safety function is retained in the event of a component failure.
- The majority of component failures are detected and lead to operating inhibition. The two position switches on a safety guard are monitored for plausibility in the associated safety module. The safety module also employs internal diagnostics measures. Faults in the contactor Q1 are detected by means of mechanically linked contacts and their readback in K2 and K3. Additional readback in K1 is not necessary, since a demand for the emergency stop function is much less frequent. A part of the faults in T1 are detected by the process. A small number of faults are not detected by the controller.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- The emergency stop device S1 corresponds to EN ISO 13850; B2 and B4 are position switches with direct opening contact to IEC 60947-5-1, Annex K.
- The supply conductors to the position switches B1 and B4 are laid separately or with protection.



安全機能

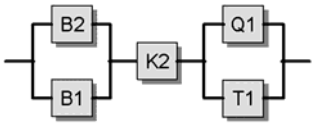
- 非常停止機能、非常停止装置の作動による STO－安全トルクオフ
- 保護装置によって起動する安全関連停止機能：可動式ガードが開くことで安全機能 STO－安全トルクオフが起動する。

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、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/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。



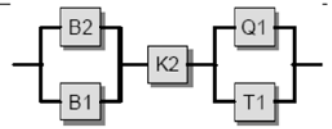
- The contactor Q1 possesses mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The safety modules K1, K2 and K3 satisfy all the requirements for Category 4 and PL d.
- The frequency inverter T1 has no integral safety function.

Remark

- The emergency stop function is a complementary protective measure to EN ISO 12100-2:2004.

Calculation of the probability of failure

- The circuit arrangement can be divided into three safety functions, each of which is assigned to three subsystems. The safety-related block diagram shows the safety-related stop function with reference to an example for one protective device, since only one protective device is open at any one time. The same safety function and an identical calculation of the probability of failure apply to the second protective device. For the emergency stop function, the emergency stop device S1 and the safety module K1 take the place of the first two subsystems. The probability of failure of the standard safety modules K1, K2 and K3 is added at the end of the calculation (2.31×10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows.
- S1 is a standard emergency stop device to EN ISO 13850. Fault exclusion applies for the direct opening contact and the mechanical elements, provided the number of operations indicated in Table D.2 of this report is not exceeded. Three actuations per year is assumed for n_{op}. This value is ignored for the purpose of further calculation for both safety functions with regard to the overall circuitry of Q1 and the frequency inverter.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B2 with direct opening action. For the electrical make contact of the position switch B1, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B2 and B1. At 365 working days, 16 working hours and a cycle time of 10 minutes, n_{op} is 35,040 cycles per year for these components, and the $MTTF_d$ is 285 years for B2 and 142 years for B1. For the contactor Q1, the B_{10} value corresponds under inductive load (AC 3) to an electrical life of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. Since Q1 is involved in both safety-related stop functions,



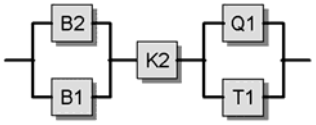
- 接触器 Q1 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。
- 安全モジュール K1、K2 および K3 は、カテゴリー4 および PL d の全ての要求事項を満たす。
- 周波数インバータ T1 は一体となった安全機能を持たない。

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。

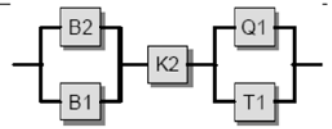
故障確率計算

- 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 2.31×10^{-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 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、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。



double the value assumed above for n_{op} results in an $MTTF_d$ of 285 years. The $MTTF_d$ for the frequency inverter T1 is 20 years [M]. Altogether, the symmetrized $MTTF_d$ value per channel in the subsystem Q1/T1 is 68 years ("high").

- DC_{avg}: the DC of 99% for B1 and B2 is based upon plausibility monitoring of the break contact/make contact combination in K2. This corresponds to the DC_{avg} for the subsystem. The DC of 99% for the contactor Q1 is derived from readback of the contact position in the safety modules. Fault detection by the process yields a DC of 60% for the frequency inverter T1. Averaging thus results in a DC_{avg} of 62% ("low") for the subsystem Q1/T1.
- Adequate measures against common cause failure in subsystems B1/B2 and Q1/T2 (70 and 85 points respectively): separation (15), protection against overvoltage etc. (15) and environmental conditions (25 + 10), well-tried components in B2/B1 (5), diversity in Q1/T1 (20)
- The subsystem B1/B2 corresponds to Category 3 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 2.47×10^{-8} per hour. The subsystem Q1/T1 corresponds to Category 3 with a high $MTTF_d$ (68 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of 1.73×10^{-7} per hour.
- For the safety-related stop function, the resulting average probability of dangerous failure is 2.00×10^{-7} per hour. This corresponds to PL d.
- The resulting average probability of dangerous failure for the emergency stop function is 1.75×10^{-7} per hour. This corresponds to PL d.

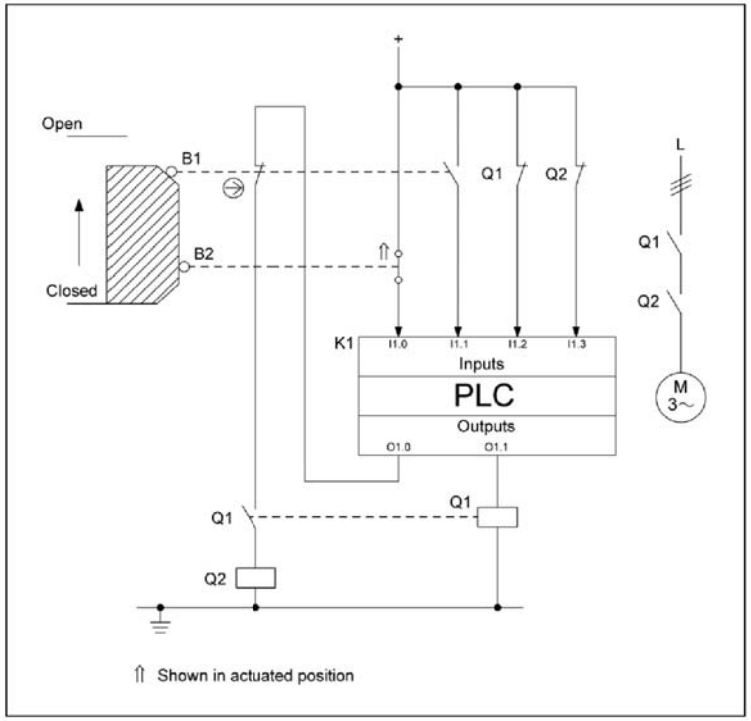


Q1 は両方の安全関連停止機能に関係するため、上記 n_{op} の想定値を 2 倍して、$MTTF_d$ は 285 年となる。周波数インバータ T1 の $MTTF_d$ は 20 年[M]となる。全体で、サブシステム Q1/T1 内のチャンネルあたりの対称化 $MTTF_d$ は 68 年（「高」）となる。

- DC_{avg}：B1 および B2 の 99%の DC は、K2 での N.C.接点/ N.O.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 2.47×10^{-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 1.73×10^{-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 2.00×10^{-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 1.75×10^{-7} となる。これは PL d に相当する。

8.2.18 Position monitoring of a moveable guard – Category 3 – PL d (Example 18)

Figure 8.32:
Redundant position monitoring of a moveable guard employing diversity in its technical implementation (electromechanical and programmable electronic)

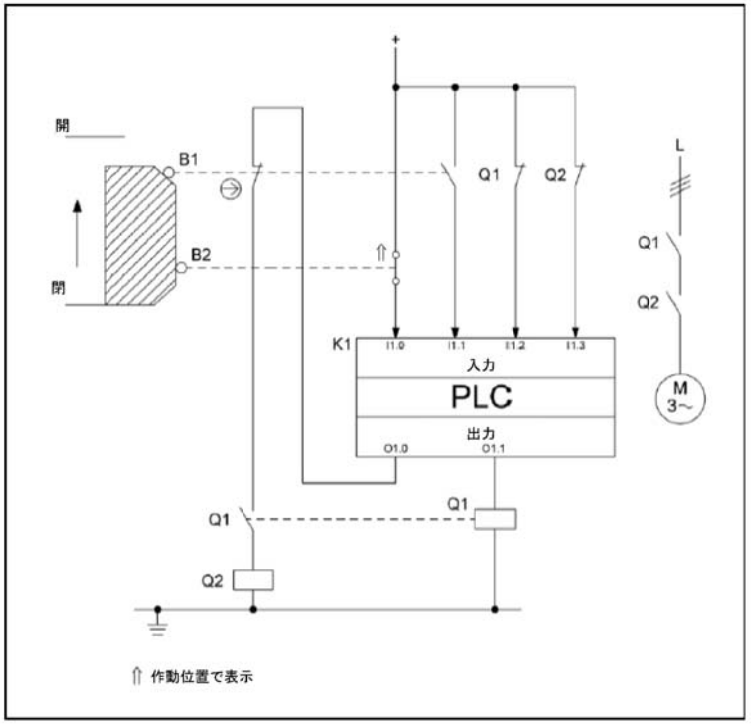


Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard (protective grating) initiates the safety function STO (safe torque off).

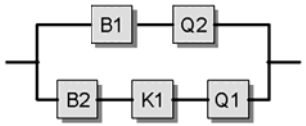
8.2.18 可動式ガードの位置監視 ― カテゴリー3 ― PL d（例 18）

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。

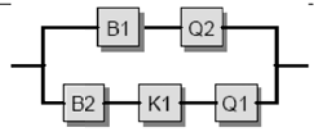


Functional description

- Opening of the moveable guard (e.g. safety guard) is detected by two position switches B1 and B2 in a break contact/make contact combination. The position switch B1 with direct opening contact actuates a contactor Q2 which interrupts/ prevents hazardous movements or states when it drops out. The position switch B2 with make contact is read in by a standard PLC K1, which can bring about the same de-energization response by actuation of a second contactor Q1.
- The safety function is retained in the event of a component failure.
- The switching position of B1 is also read into the PLC K1 by means of a make contact, and is compared for plausibility with the switching position of B2. The switching positions of the contactors Q1 and Q2 are likewise monitored in K1 by mechanically linked readback contacts. Component failures in B1, B2, Q1 and Q2 are detected by K1 and lead to operating inhibition owing to the dropping-out of Q1 and Q2. Faults in the PLC K1 are detected only by the function (fault detection by the process).

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective device is assured for actuation of the position switch.
- B1 is a position switch with direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the start-up and actuation mechanism are detected by the use of two position switches differing in the principle of their actuation (break and make contacts).
- Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.
- The PLC K1 satisfies the normative requirements described in Section 6.3.

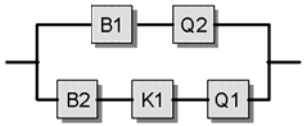


機能の説明

- 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。開離作動式位置スイッチ 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。

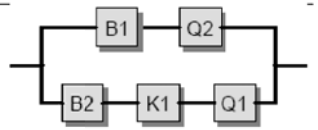
設計特性

- 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 による開離作動式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。



Calculation of the probability of failure

- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening contact. For the electrical make contact of the position switch B2, the B_{10d} is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the $MTTF_d$ is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, the B_{10} value under inductive load (AC3) corresponds to an electrical life of 1,300,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The above assumed value for n_{op} results in an $MTTF_d$ of 4,452 years for Q1 and Q2. An MTTF value of 15 years [M] is substituted for the PLC, resulting through doubling in an $MTTF_d$ value of 30 years. The combination of B1 and Q2 results in an $MTTF_d$ of 1,236 years for the first channel; B2, K1 and Q2 contribute to an $MTTF_d$ of 28 years in the second channel. Altogether, the $MTTF_d$ value symmetrized over both channels is 70 years per channel ("high").
- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the two switching states in the PLC K1. The *DC* of 99% for the contactors Q1 and Q2 is derived from readback via mechanically linked contact elements, also in K1. Owing to the possibility of fault detection by the process, a *DC* of 60% is assumed for K1. Averaging thus results in a DC_{avg} of 62% ("low").
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ (70 years) and low DC_{avg} (62%). This results in an average probability of dangerous failure of 1.66×10^{-7} per hour. This corresponds to PL d.



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 1.66×10^{-7} となる。これは PL d に相当する。

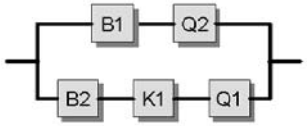
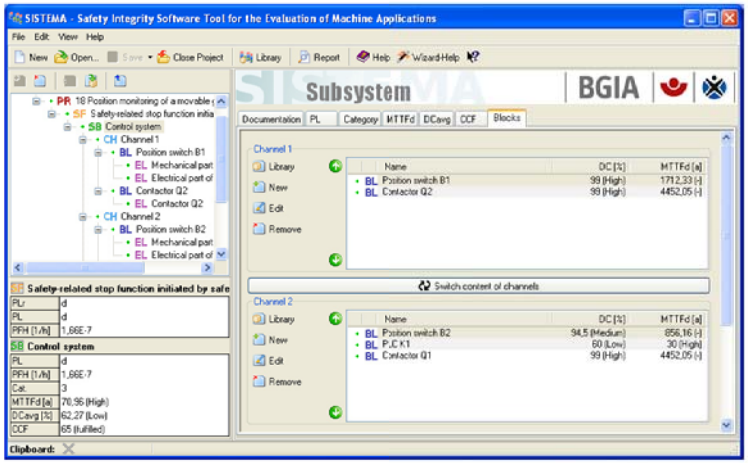


Figure 8.33:
Determining of the PL by means of SISTEMA



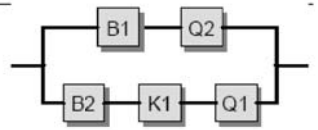
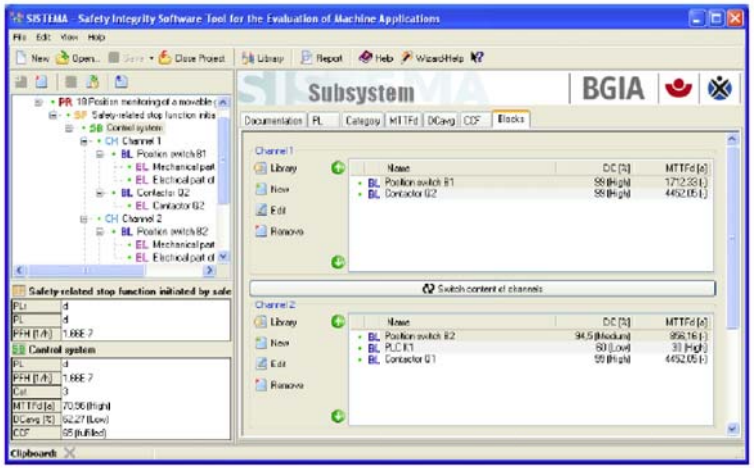
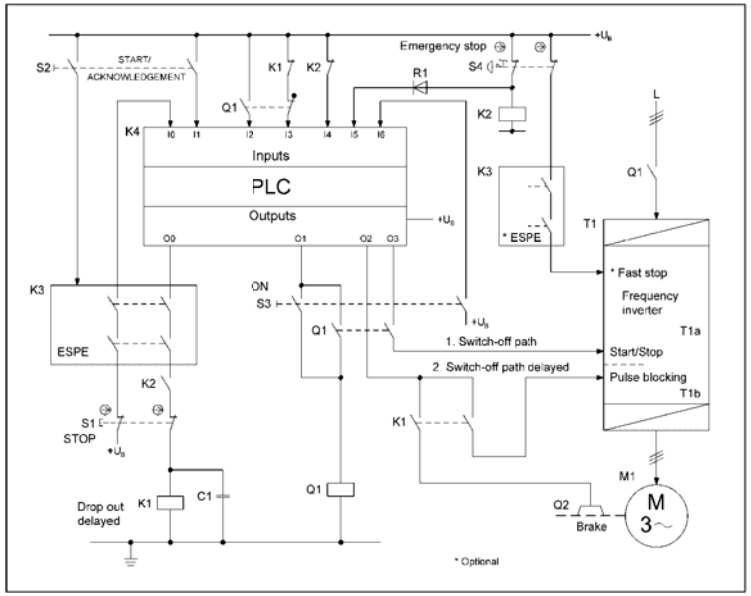


図 8.33：SISTEMA による PL の決定



8.2.20 Safe stopping of a PLC-driven drive – Category 3 – PL d (Example 20)

Figure 8.36:
Safe stopping of a PLC-driven frequency inverter drive following a stop or emergency stop command or following tripping of a protective device (in this case, an ESPE)



Safety function

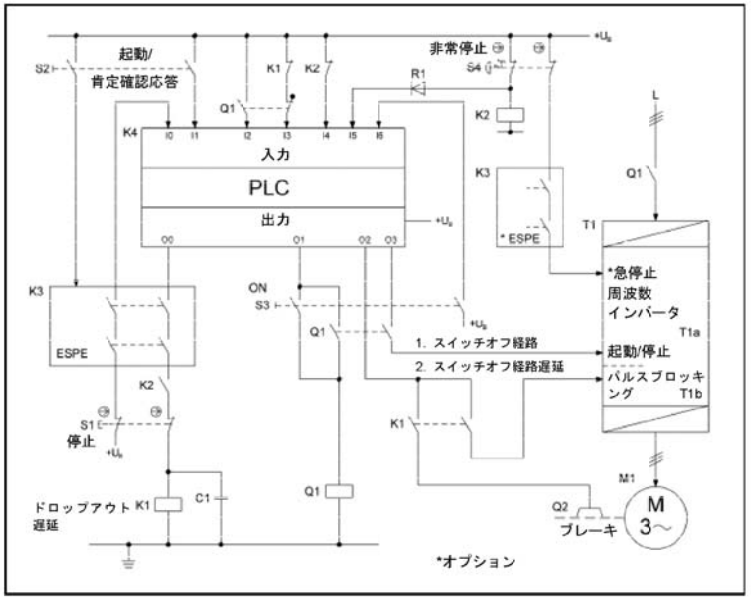
- Safety-related stop function, initiated by a protective device: following a stop or emergency stop command or tripping of a protective device, the drive is halted (SS1 – safe stop 1).

Functional description

- The hazardous movement is interrupted redundantly if either the stop button S1 or the protective device K3 (shown in the circuit diagram as electro-sensitive protective equipment (ESPE)) is actuated. The drive is halted in an emergency following actuation of the emergency stop device S4. In all three cases, the first set braking time is implemented via the output O3 of the PLC K4 by deactivation of the “Start/Stop” input (T1a) on the frequency inverter (FI) T1. Redundantly to this arrangement, the second set braking time takes the form of deactivation of

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

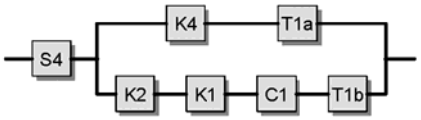


安全機能

- 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）がオフすることにより、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。

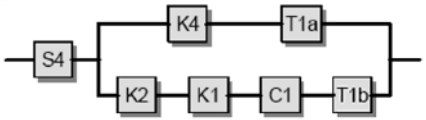


the “pulse blocking” input (T1b) on T1, which is achieved by de-energization of the contactor relay K1 (with the use of the capacitor C1 for drop-out delay), and application of the brake Q2. The first de-energization path is thus implemented directly by the PLC K4; conversely, the second de-energization path employs relay technology and delayed drop-out. The timer settings for O2 in the PLC program and for K1 are selected such that the machine movement is halted even under unfavourable operating conditions.

- Should a “fast stop” input with a particularly rapid speed reduction be available on the FI, the emergency stop device and ESPE may be connected to it if desired, as shown on the circuit diagram. This option is not considered further below.
- In the event of failure of the PLC K4, the frequency inverter inputs T1a/T1b, the contactor relay K1 with drop-out delay or the contactor relay K2, stopping of the drive is assured, since two mutually independent de-energization paths are always present. Failure of the auxiliary contactors K1 or K2 to drop out is detected, at the latest before renewed start-up of the machine movement, by the feedback of the mechanically linked break contacts to the PLC inputs I3 and I4.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Owing to the use of a frequency inverter with safe pulse blocking, the contactor Q1 is no longer absolutely essential for de-energization of the supply voltage. The frequency inverter must be suitable for ramping up and braking.
- The contactor relays K1 and K2 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The contacts of the pushbuttons S1 and S4 are mechanically linked in accordance with IEC 60947-5-1, Annex K.
- The standard components K4 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The software (SRASW) is programmed in accordance with the requirements for PL c (downgraded owing to diversity) and the instructions in Section 6.3.
- If the brake Q2 is provided for functional reasons only, i.e. it is not involved in execution of the safety function, it is disregarded in the calculation of the probability of failure, as in this example. This procedure requires that coasting down of the drive in the event of a failure of T1a (see below), in which case

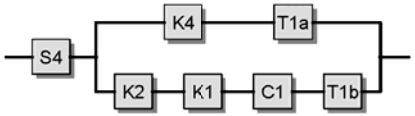


この配置に冗長して、2 次設定されたブレーキ時間は、接触器リレーK1（ドロップアウト遅延用にコンデンサ C1 を使用）の遮断、およびブレーキ Q2 の適用によりもたらされる、T1 での「パルスブロッキング」入力（T1b）がオフして実行される。そのため、第 1 遮断経路は PLC K4 により直接実行され、反対に第 2 遮断経路は、リレー技術および遅延ドロップアウトを採用する。PLC プログラムの O2 および K1 のタイマー設定は、好ましくない運転状態においても機械動作が停止するように選択する。

- 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 N.C.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。



de-energization is effected by means of pulse blocking alone, is not associated with an unacceptably high residual risk. The involvement of a brake in execution of the safety function in conjunction with the use of an FI is described in the example of a revolving door control (Example 23).

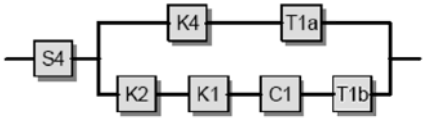
- The ESPE K3, for example in the form of a light curtain, satisfies the requirements for Type 4 to EN 61496-1 and IEC 61496-2, and for PL e.

Calculation of the probability of failure

- The probability of failure of safe stopping triggered by the emergency stop device S4 or by the ESPE, which is also shown on the safety-related block diagram, is calculated. The “fast stop” function of the FI and the facility for de-energization of the power supply to the FI via Q1 are not considered in the calculation of the probability of failure of the safety function.
- The frequency inverter T1 is broken down into the blocks T1a and T1b. The block T1a contains the functions Start and Stop and their implementation in the control system. The block T1b contains the pulse blocking, which is achieved by a low number of components.

Safe stop triggered by the emergency stop device S4:

- A fault exclusion is assumed for the emergency stop device, since the number of actuations stated in Table D.2 is not exceeded.
- $MTTF_d$: the following $MTTF_d$ values are estimated: 50 years for K4, 100 years for T1a and 1,000 years for T1b [E]. At a B_{10d} value of 400,000 cycles [S] and at 240 working days, 8 working hours and a cycle time of 6 minutes, the n_{op} is 19,200 cycles per year and the $MTTF_d$ 208 years for K1. At a B_{10d} value of 400,000 cycles [S] and daily actuation on 240 working days, the $MTTF_d$ for K2 is 16,667 years. The capacitor C1 is included in the calculation with an $MTTF_d$ of 45,662 years [D]. These values produce a symmetrized $MTTF_d$ for each channel of 72 years (“high”).
- DC_{avg}: fault detection by the process results in a *DC* of 30% for K4, a *DC* of 90% for T1a and a *DC* of 60% for T1b. A *DC* of 99% for K1 and a *DC* of 60% for C1 are derived by testing of the timing element with the FI de-energized. The *DC* for K2 is 99% owing to plausibility testing in K4 with the switching status of S4. The averaging formula for DC_{avg} yields 56.9 % (within the tolerance for “low”).
- Adequate measures against common cause failure (85 points): separation (15), diversity (20), overvoltage protection etc. (15) and environmental conditions (25 + 10)



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）

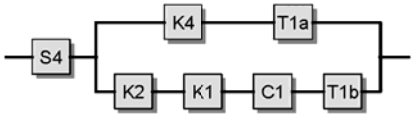
- ESPE K3 は、例えば光カーテンの形で、EN 61496-1 および IEC 61496-2 のタイプ 4、および PL e の要求事項を満たす。

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）



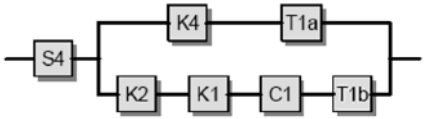
- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ per channel (72 years) and a low DC_{avg} (56.9%). This results in an average probability of dangerous failure of 1.76×10^{-7} per hour. This corresponds to PL d.

Safe stop triggered by the ESPE K3:

- The ESPE K3 is a standard safety component. Its probability of failure is 3.0×10^{-8} per hour [M], and is added at the end of the calculation.
- The probability of failure of the "PLC/electromechanical" two-channel structure is calculated using the same $MTTF_d$ and DC values as those described above. The component K2 however is not involved in execution of this safety function. The results are: an $MTTF_d$ for one channel of 72 years ("high") and a DC_{avg} of 56.8% (within the tolerance for "low"). For Category 3, this results in an average probability of dangerous failure of 1.77×10^{-7} per hour. The overall probability of failure is determined by addition, producing a result of 2.07×10^{-7} per hour. This also corresponds to PL d.

More detailed references

- *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)



- 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 1.76×10^{-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：

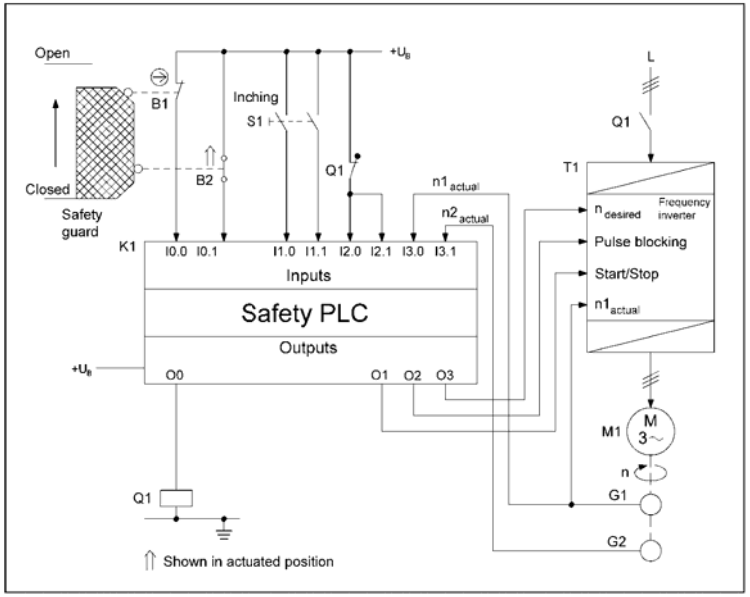
- ESPE K3 は標準の安全構成部品である。その故障確率は 1 時間あたり 3.0×10^{-8}[M]であり、計算の最後に追加される。
- 「PLC/電気機械」2 チャンネル構造の故障確率は、上記と同様の $MTTF_d$ および DC 値を使用して計算される。しかしながら、構成部品 K2 はこの安全機能の実行に関係しない。結果として、1 チャンネルの $MTTF_d$ は 72 年（「高」）となり、DC_{avg} は 56.8%（「低」の公差内）となる。カテゴリー3 ではこれにより危険側故障の平均確率は 1 時間あたり 1.77×10^{-7} となる。全故障確率は加算して決定し、1 時間あたり 2.07×10^{-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 Safely limited speed for inching mode – Category 3 – PL d (Example 21)

Figure 8.37:
Inching mode with safely limited speed when the safety guard is open, with desired/actual value comparison and defined speed limit value within a safety PLC



Safety function

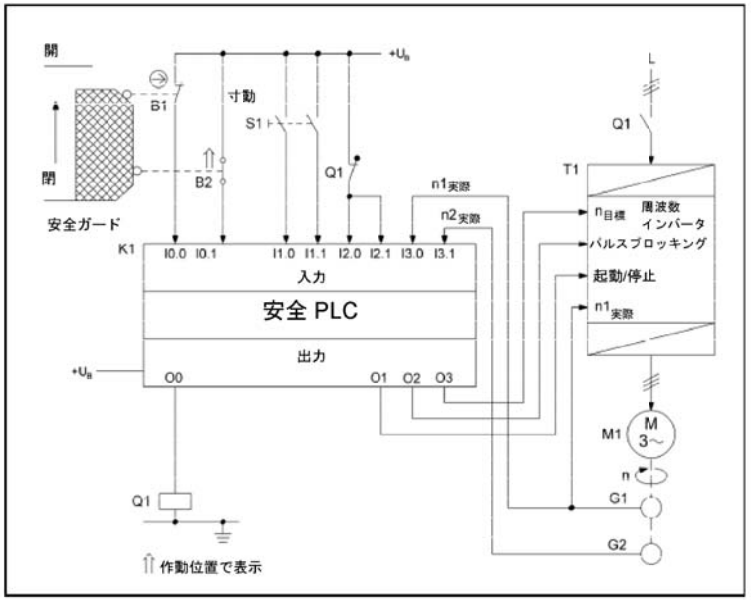
- Safely limited speed (SLS): when the safety guard is open, exceeding of a permissible speed in inching mode is prevented.

Functional description

- A hazardous movement is safely prevented or interrupted when the safety guard is open. Opening of the safety guard is detected by two position switches B1 and B2 in a break contact/make contact combination. When the pushbutton S1 is actuated a safely limited speed is set on the frequency inverter T1 by means of the safety PLC K1. The two processing channels within the PLC each receive limit value settings independently of each other from their appli-

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

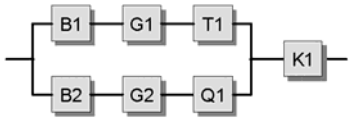


安全機能

- 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、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 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。

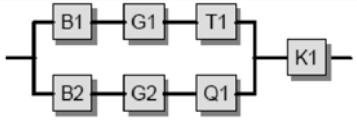


cation software. The actual rotational speed value of the inching speed on the inputs I3.0 and I3.1 of K1 is monitored by two separate tachogenerators G1 and G2. Each channel of the PLC performs the desired/actual speed comparison independently. Should the speed not be reduced successfully to the limited value by means of T1, K1 can initiate a halt by blocking of the start/stop signal and pulse blocking on the inverter. The power supply to T1 can also be interrupted by a mains contactor Q1.

- Safety-related data is exchanged through an internal interface in the safety PLC K1. Such data is employed for example for fault detection by a state comparison between the two processing channels. Should one processing channel fail, the remaining functioning processing channel reduces the speed of the inverter T1 and de-energizes the mains contactor Q1. A failure of the inverter which could for example lead to unexpected start-up, continued running or an increase in the speed is detected by separate monitoring of the speed by the tachogenerators G1 and G2 in both processing channels. Failure of the mains contactor Q1 to drop out is detected by the break contacts present in both processing channels (inputs I2.0 and I2.1 of K1), and leads both to blocking of the start/stop signal and to pulse blocking on the inverter by both processing channels.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective device is assured for actuation of the position switch.
- The position switch B1 features direct opening action in accordance with IEC 60947-5-1, Annex K. The position switch B2 also complies with IEC 60947-5-1.
- The contactor Q1 possesses a mirror contact according to IEC 60947-4-1, Annex F.
- The supply conductors to the position switches are laid either separately or with protection against mechanical damage.
- For the safety function “safely limited speed”, a fault exclusion is assumed for the fault condition of encoder shaft breakage (G1/G2). Details of the possibility of a fault exclusion can be found for example in IEC 61800-5-2, Table D.16.
- The standard components G1 and G2 (where relevant for the rotary signal encoders) and T1 are employed in accordance with the instructions in Section 6.3.10.

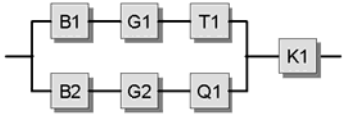


K1 の入力 I3.0 および I3.1 での寸動速度の実際の回転速度値は、2 つの別のタコジェネレータ G1 および G2 で監視する。PLC の各チャンネルは、目標/実際速度比較を独立して行う。T1 によって速度が制限値までうまく低下しなければ、起動/停止信号のブロッキングおよびインバータのパルスブロッキングにより、K1 で停止を開始できる。T1 への電源は、主接触器 Q1 によって遮断できる。

- 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 N.C.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。



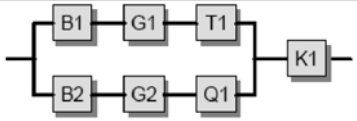
- The safety component K1 satisfies all requirements for Category 3 and PL d. The software (SRASW) is programmed in accordance with the requirements for PL d and the instructions in Section 6.3.
- It is assumed that each output of the safety PLC is actuated by both processing channels of the PLC (exception: O3).

Remarks

- According to EN 1010-1, the use of one position switch with direct opening action to IEC 60947-5-1, Annex K for each interlocked guard is sufficient on machines without routine operator intervention at danger points. Fault exclusion in this context is conditional upon the switch being installed in accordance with EN 60204-1.
- For full implementation of inching mode, the safety function “no unexpected start-up in inching mode” must also be considered.

Calculation of the probability of failure

- The SRP/CS is divided into the two subsystems sensor/actuator and PLC. For the PLC subsystem, a tested safety PLC suitable for PL d is employed. This PLC's probability of failure of 1.5×10^{-7} per hour [E] is added at the end of the calculation for the sensor/actuator subsystem. For production of the block diagram, refer also to Figure 6.14 and the corresponding comments in the associated text. The probability of failure for the sensor/actuator subsystem is calculated below.
- $MTTF_d$: at 240 working days, 8 working hours and a cycle time of one hour, n_{op} is 1,920 cycles per year. A B_{10d} value of 20,000,000 cycles [S] is assumed for the position switch B1 owing to its direct opening action; the associated $MTTF_d$ value is 104,116 years. Owing to the defined control current (low load; the mechanical lifetime of the contacts is the determining factor), for the position switch B2 a B_{10d} value of 1,000,000 cycles [E] is assumed (see also Table D.2), and therefore an $MTTF_d$ of 5,208 years. The contactor Q1 with a B_{10d} value of 400,000 cycles switches operationally only once daily, corresponding to a n_{op} of 240 cycles per year and an $MTTF_d$ of 16,667 years. The following values are estimated: an $MTTF_d$ of 100 years for T1 and an $MTTF_d$ of 50 years for G1/G2 [E]. These values produce a symmetrized $MTTF_d$ for each channel of 41 years (“high”).
- DC_{avg}: for each of the components used, a DC of 99% is assumed. For the position switches and the tachogenerators, this value is based upon cross-checking of input signals in K1. For the inverter T1, fault detection is provided by the



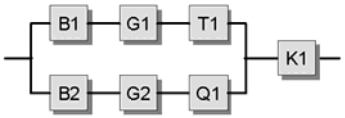
- 安全構成部品 K1 はカテゴリー3 および PL d の全ての要求事項を満たす。PL d の要求事項および 6.3 項の指示により、ソフトウェア（SRASW）をプログラミングする。
- 安全 PLC の各出力が PLC の両プロセスチャンネル（除く O3）により作動すると想定する。

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 1.5×10^{-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。

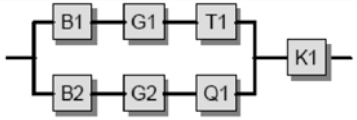


process; the mains contactor Q1 is monitored directly by the PLC. These values produce a DC_{avg} of 99% ("high").

- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The sensor/actuator subsystem corresponds to Category 3 with a high $MTTF_d$ per channel (41 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 6.56×10^{-8} per hour. This corresponds to PL e. PL_r d is thus surpassed, which with the required two-channel design of the hardware with few components, the use of B_{10d} values in accordance with the standard, a *DC* of "high" and a "moderate" switching frequency will virtually always be the case.
- The overall probability of failure is determined by addition of the probability of dangerous failure of K1 (1.5×10^{-7} per hour) and is 2.16×10^{-7} per hour. This corresponds to PL d.

More detailed references

- *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)



これらの値により、DC_{avg} は 99%（「高」）となる。

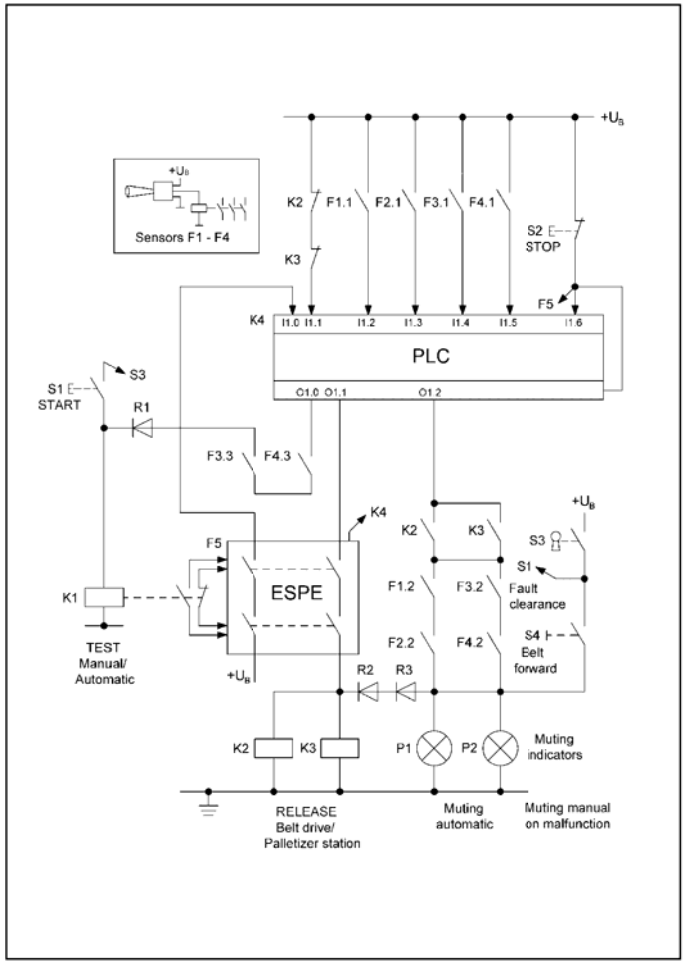
- 共通原因故障に対する適正な対策（70 点）：分離（15）、FMEA（5）、過電圧保護など（15）および環境条件（25 + 10）
- センサ/アクチュエータサブシステムは、チャンネルごとの高い $MTTF_d$（41 年）と高い DC_{avg}（99%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり 6.56×10^{-8} となる。これは PL e に相当する。このため PL_r d を超え、構成部品の少ないハードウェアの要求される 2 チャンネル設計、規格による B_{10d} 値の使用、「高い」DC および「中程度の」開閉頻度が事実上常にそのケースと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

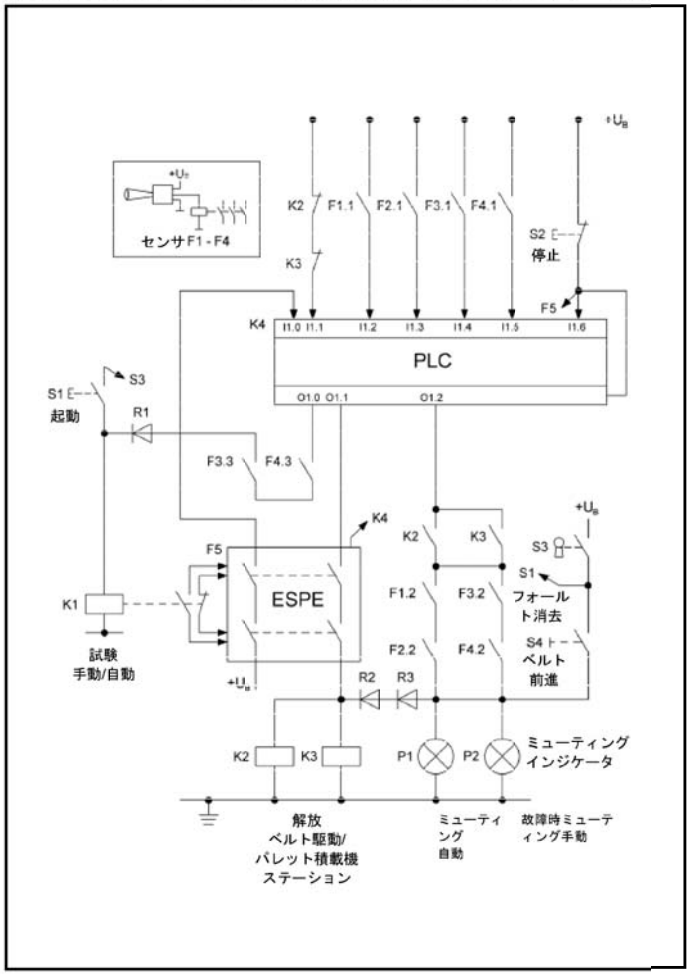
8.2.22 Muting of a protective device – Category 3 – PL d (Example 22)

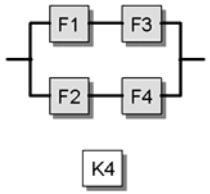
Figure 8.38:
Muting of a protective device at the discharge point from a palletizing installation controlled by a PLC



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



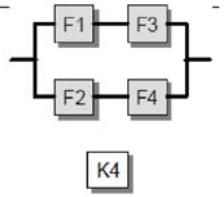


Safety function

- Muting function: temporary muting of a protective device as a function of the process. Further safety functions, such as safeguarding of access to the palletizing installation or the start/restart interlock, are not dealt with in detail below.

Functional description

- Access to the discharge point from the palletizing installation is safeguarded by a triple-beam light barrier (ESPE) F5 of Type 4 to EN 61496. The light barrier embodies the additional functions of start interlock and restart interlock which are implemented by means of two antivalent inputs. Disabling of the start interlock of the light barrier is coupled to the start command for the belt drive, i.e. energization of the palletizing station, and is initiated by picking-up and subsequent dropping-out of contactor relay K1 in response to actuation and release of the start button S1. A condition for a valid start command is that contactor relays K2 and K3 have dropped out (queried via input I1.1) and that the start interlock has been cancelled (queried via input I1.0). Output O1.1 is set as a result.
- Four infrared light sensors F1 to F4 (for arrangement, refer also to Figure 8.38) are incorporated for control of the muting process. On inputs I1.2 to I1.5, the PLC monitors the actuation sequence of the four infrared light sensors via the sensors' contacts F1.1 to F4.1, in consideration of two programmed time settings. The muting function is implemented only in the output circuit of the PLC (output O1.2) independently of the output circuit of the light barrier F5. The muting contacts F1.2 and F2.2/F3.2 and F4.2, connected in series, are connected, via the diodes R2 and R3 respectively, by OR logic with the “enabling” function implemented by the contactor relays K2 and K3.
- R2 and R3 cause the muting function to be displayed correctly, and isolate the activated enabling output from the muting displays P1/P2 should the muting function not be active. Faults in R2 or R3 cannot lead to undesired muting (i.e. dangerous failure of the muting function).
- In the event of breakdown and subsequent restoration of the voltage, or with light barrier F5 interrupted and the muting function not active, the contactor relays K2 and K3 are de-energized. The absence under these conditions of latching-in prevents them from picking up again should the muting circuits be closed again. The installation can be restarted only by disabling of the restart interlock, i.e. by deliberate actuation and release of the start button S1.



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。

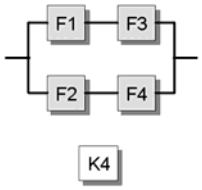
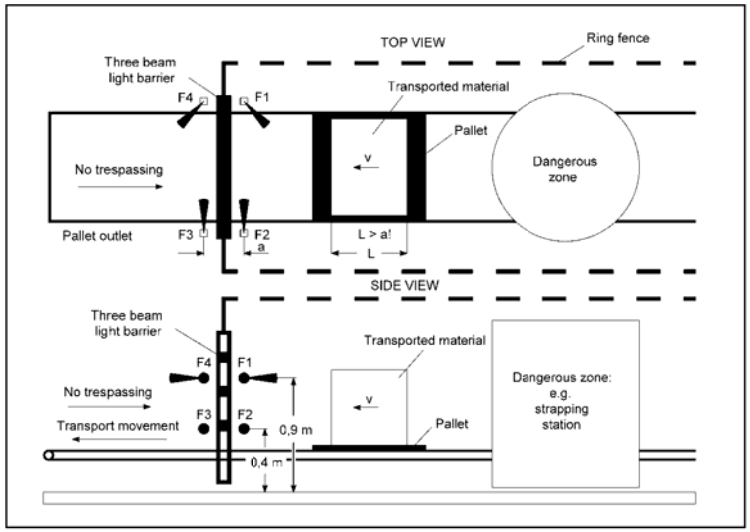


Figure 8.39:
Palletizing station with automatic control – principle of safeguarding of the pallet discharge point by means of a light barrier and arrangement of the muting sensors F1 to F4



- For intended starting/restarting, for example following a fault on the installation, the key switch S3 must be actuated. In the event of a fault condition, the operator can eject a pallet from the detection area of the light barrier and the muting sensors by means of the dead-man's button S4.

  For smooth progress of the pallets through the discharge opening, two time settings in the PLC program must be matched to the velocity of the transport movement:

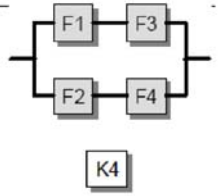
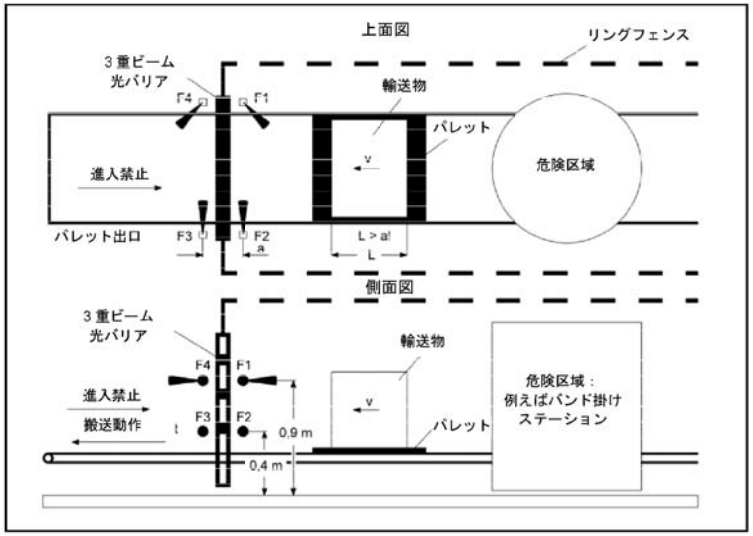
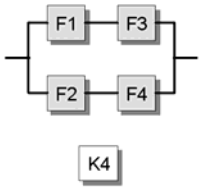


図 8.39: 自動制御付きパレット積載ステーション － 光バリアおよびミューティングセンサ F1 から F4 の配置によるパレット排出箇所の安全防護原則



- 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：



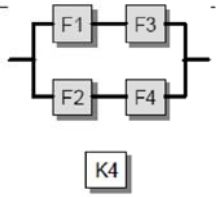
– The time setting T1 determines the maximum period within which – following activation of the sensor F1 – the sensor F2 must be activated and the muting function thus initiated by the transported product.

– Time setting T2 begins with renewed clearing of sensor F2. T2 must be selected such that when the detection zone of the light barriers becomes clear again, K1 is energized and de-energized again before sensor F3 is deactivated by the transported product and the muting function thereby terminated.

- Failure of the contactors K2 and K3 to drop out is detected at the latest before the belt drive/the palletizing installation start up again, owing to the feedback of the mechanically linked break contacts to the PLC input I1.1. Failure of K1 is detected at the next discharge of a pallet.
- Unintended start-up of the belt drive/palletizing installation in the event of the loss and subsequent restoration of power or a failure of the standard PLC is prevented by the function of the start-up and restart interlocks. The PLC can disable the restart interlock only immediately after the pallet has passed the light barrier, i.e. whilst sensors F3 and F4 are still activated.
- The failure of individual muting sensors is either detected directly by the PLC program (owing to monitoring for proper completion of activation and deactivation), or becomes evident by operating inhibition during transport of the pallet.
- Failure of the dead-man's button S4, which is used only for the clearing of faults (manual muting), is detected directly by the user.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- Contactor relays K1 to K3 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L.
- The supply conductors to light barrier F5 and to the dead man's button S4 are laid such that short-circuits between individual conductors (including to the supply voltage) can be excluded.
- The control components S1 to S4 are located at a point outside the hazardous area and with a view of it.

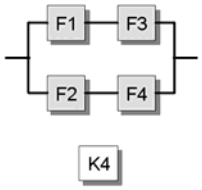


- 時間設定 T1 は、センサ F1 の活性化の後にセンサ F2 が起動し、輸送物によってミューティング機能が始まらなければならない最大期間を決定する。
- 時間設定 T2 は、センサ F2 の再消去から始まる。T2 は、光バリアの検出区域が再度空になった時に K1 が通電し、センサ F3 が輸送物によってオフし、ミューティング機能がそれによって終了する前に再度遮断されるように選択しなければならない。

- 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 N.C.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（オン・オフ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。



- The muting state is displayed by two lights clearly visible to the operator at the access point to the hazardous area.
- The standard components F1 to F4 are employed, where applicable, in accordance with the instructions in Section 6.3.10.

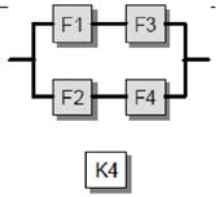
Remarks

- Example implementation of automated material discharge with safeguarding of access points to palletization and depalletization processes, transfer stations, strapping or wrapping machines. The same principle can be used for access points for material infeed.
- In accordance with EN 415-4, it can be assumed that the undetected access of persons through feed or discharge openings is prevented sufficiently reliably when requirements including the following are met:
  – use of a two or three-beam light barrier in consideration of the necessary fitting height (with the access point open or an empty pallet present in it), or
  – with the protective function of the light barrier muted by the loaded pallet with clearances to the side of less than 0.2 m and with muting being activated by the pallet load only immediately prior to interruption of the light beams (without greater timing intervals and geometrical gaps).

Calculation of the probability of failure

In the calculation below, a *DC* of 0% is assumed for the output relays of the muting sensors F1 to F4, since the contacts employed for muting are not subject to automatic fault detection. For this reason, periodic manual inspection which can be achieved by simple means is specified.

- $MTTF_d$: an $MTTF_d$ of 100 years [E] is assumed for the sensor part of each of the muting sensors F1 to F4. A B_{10d} value of 2,000,000 cycles [S] applies for the output relays F1 to F4. At 300 working days, 16 working hours and a cycle time of 200 seconds, n_{op} is 86,400 cycles per year and the $MTTF_d$ is 231 years for these elements. The $MTTF_d$ of the channel is 35 years (“high”).
- DC_{avg}: a *DC* of 90% for the sensor part of the muting sensors F1 to F4 is attained by the PLC monitoring. The *DC* for the output relays is estimated erring on the safe side at 0%. The resulting DC_{avg} value is 63% (“low”).
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)



- 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。

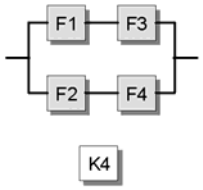
備考

- 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。

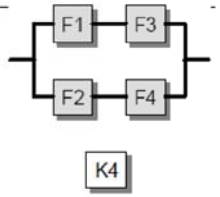
- $MTTF_d$：ミューティングセンサ F1 から F4 のそれぞれのセンサ部分に、100 年[E]の $MTTF_d$ を想定する。出力リレーF1 から F4 に 2,000,000 サイクル[S]の B_{10d} 値を適用する。稼働日 300 日、稼働時間 16 時間、サイクル時間が 200 秒の場合、n_{op} は 1 年に 86,400 サイクルとなり、これらの要素の $MTTF_d$ は 231 年となる。チャンネルの $MTTF_d$ は 35 年（「高」）となる。
- DC_{avg}：PLC の監視により、ミューティングセンサ F1 から F4 のセンサ部分の DC は 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）



- The combination of the control elements corresponds to Category 3 with a high $MTTF_d$ per channel (35 years) and low DC_{avg} (63%). This results in an average probability of dangerous failure of 5.16×10^{-7} per hour. This corresponds to PL d.

More detailed references

- *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)



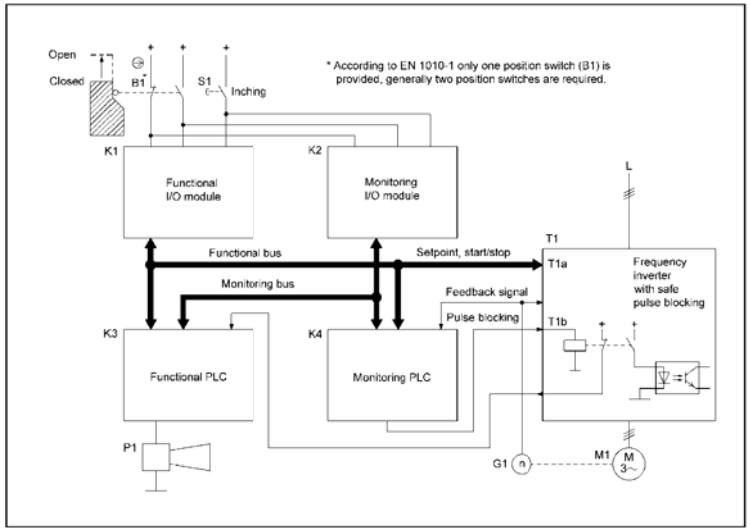
- 制御要素の組み合わせは、チャンネルごとの高い $MTTF_d$（35 年）と低い DC_{avg}（63%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり 5.16×10^{-7} となる。これは PL d に相当する。

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 Inching mode with safely limited speed on a printing machine – Category 3 – PL d (Example 24)

Figure 8.42:
Inching mode with safely limited speed on a printing machine with two-channel microprocessor control



Safety functions

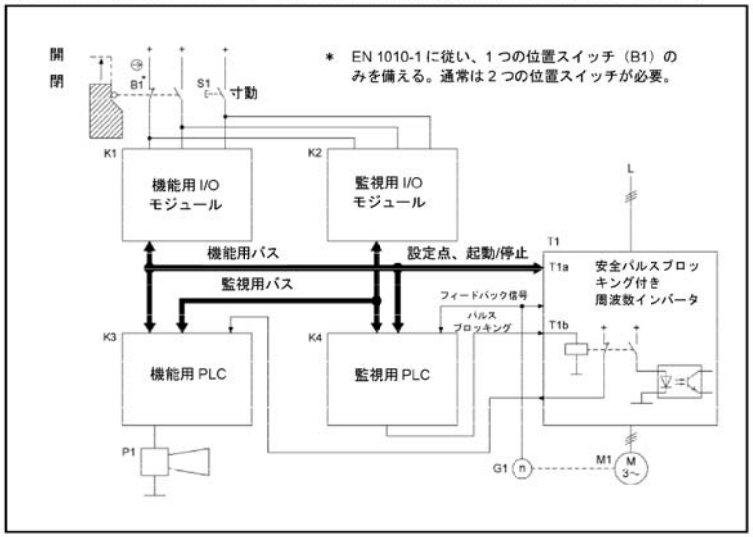
- Safety-related stop function, initiated by a protective device: the drive is to stop when the safety guard is opened (SS1 – safe stop 1).
- Safely limited speed (SLS): when the safety guard is open, machine movements may occur only at limited speed.
- Inching mode: when the safety guard is open, movements are possible only whilst an inching button is pressed.

Functional description

- The remote I/O module K1 registers the states of the position switch with personnel safety function B1 and of the inching button S1, and makes this information available on the functional bus. The information is evaluated by the functional PLC K3 and results in the frequency inverter T1 being actuated (functional actuation T1a) via the functional bus. The I/O module K2 and the monitoring PLC K4, which communicate over a dedicated monitoring bus,

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

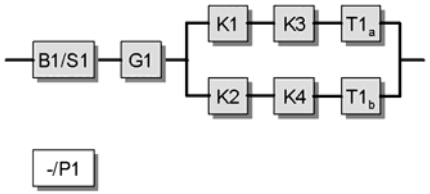


安全機能

- 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）。

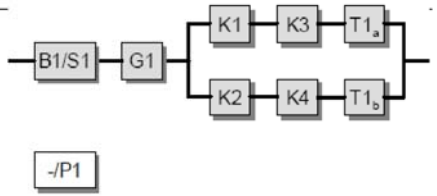


operate redundantly to K1 and K3. K4 can bring about an uncontrolled stopping (coasting down) by addressing the safe pulse blocking of T1 (safety shutdown T1b).

- With B1 open, only inching mode using S1 with safely limited speed is permitted.
- In accordance with EN 1010-1, a single position switch B1 is sufficient. The majority of faults in S1 are detected and controlled by an acoustic start-up warning involving P1 and forced dynamics: when S1 is pressed for the first time, an acoustic warning (P1) is output; only when S1 is released and pressed again does the drive start up again, with delay.
- Faults in K1 and K2 are detected by a status comparison in K4. K4 also monitors K3 by monitoring the input and output information. In addition, the faults in K3 are partly revealed by faults in the process. Self-tests (e.g. program sequence monitoring by an internal watchdog) are performed in K4; in addition, K3 uses K4 for regular addressing of the pulse blocking and monitors feedback from the latter via the mechanically linked break contact of the pulse blocking relay of T1.
- Together with the sin/cos encoder G1, the frequency inverter T1 forms a closed-loop control system in which faults (printing errors, paper tearing) are detected by the production process, which is highly synchronous. For monitoring or the safely limited speed, G1 is also read back into K4 and monitored for plausibility of the sin/cos information ($\sin^2 + \cos^2 = 1$) and for compliance with the setpoint for T1.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The break contact of B1 satisfies IEC 60947-5-1, Annex K. Measures are implemented for prevention of displacement and reasonably foreseeable misuse (see EN 1088 with Annex A1). A stable arrangement of the protective device is assured for actuation of the position switch.
- Despite the warning at start-up and forced dynamics, S1 may hang during inching operation. An additional requirement is therefore that an emergency stop device be installed within the operator's reach.

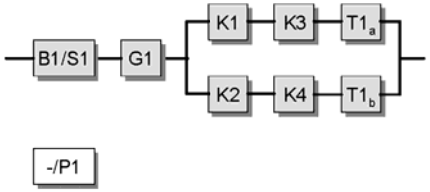


監視専用バスで通信する I/O モジュール K2 および監視用 PLC K4 は、K1 および K3 に冗長的に作用する。K4 は、T1 の安全パルスブロッキングにアドレスすることによって制御されていない停止（コーストダウン）を引き起こすことができる（安全シャットダウン　T1b）。

- 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 N.C.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 N.C.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。



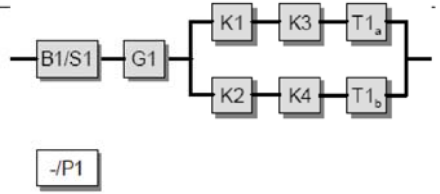
- The conditions for fault exclusion for conductor short-circuits to EN ISO 13849-2, Table D.4 must be observed for the connecting lines to S1. Faults in the connecting lines to B1 are detected by non-equivalence monitoring of the break and make contact in K1 and K2.
- The programmable components K1 to K4 satisfy the normative requirements in accordance with Section 6.3.
- G1 supplies redundant position information (e.g. sin/cos encoder) and is integrated into the closed-loop control circuit (acquisition of the commutation).
- T1 possesses safe pulse blocking (T1b), successful addressing of which is read back by a mechanically linked break contact.
- The standard components G1 and T1 are employed in accordance with the instructions in Section 6.3.10.
- The bus systems (functional bus, monitoring bus) are employed in accordance with the instructions in Section 6.2.17.

Remarks

- Application for example for the safeguarding of entrapment points on rotary printing machines. For non-cyclical operator intervention in the hazardous area, i.e. less frequently than one intervention per hour, EN 1010-1 requires only one position switch for monitoring of the guard position. The fault-tolerance criterion for Category 3 generally requires the use of two position switches (e.g. one break contact, one make contact) for similar machine control systems.
- For inching mode subject to the condition that safely limited speed is already guaranteed, the possibility of avoiding the hazard can be assumed under certain conditions.

Calculation of the probability of failure

- The sensor level B1, S1 and G1 lies outside the redundant logic and actuator level and is therefore considered separately.
- Fault exclusion for the direct opening electrical contact is possible for B1. A B_{10d} value of 20,000,000 cycles [S] is assumed for the mechanical part of B1. At 10 operations per week, n_{op} is 520 cycles per year and the $MTTF_d$ is 384,615 years. This corresponds mathematically to an average probability of dangerous failure of 2.97×10^{-10} per hour. In order for consideration to be given



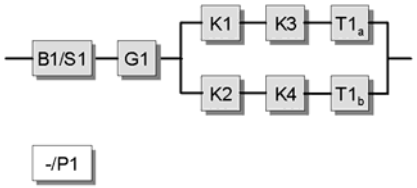
- EN ISO 13849-2 の表 D.4 に従った配線短絡に対するフォールト（故障）の排除のための条件を、S1 への接続線で守られなければならない。B1 への接続線でのフォールト（故障）は、K1 および K2 の N.C.および N.O.接点の不一致監視により検出される。
- プログラマブル構成部品 K1 から K4 は、6.3 項の必須要求事項を満たす。
- G1 は冗長的な位置情報（例えば sin/cos エンコーダ）を提供し、かつ閉ループ制御回路に集積化される（整流の取得）。
- T1 は、成功したアドレス指定が機械的に連結した N.C.接点によりリードバックされる安全パルスブロッキング（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 N.C.接点を 1 つと N.O.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。

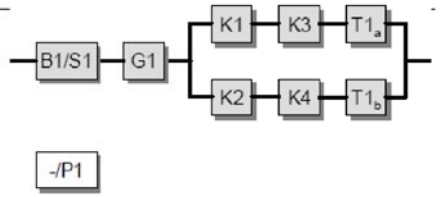
故障確率計算

- 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 2.97×10^{-10} の危険側故障の平均確率に数学的に相当する。



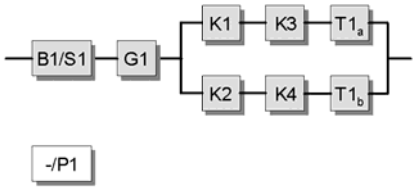
to the particular aspects of EN 1010-1, this value is downgraded to the upper marker value of 1.00 × 10^{-7} per hour for PL d, instead of the $MTTF_d$ for one channel being capped to 100 years as usual.

- S1 has a B_{10d} value of 100,000 cycles [M]. At 10 operations per week, n_{op} is 520 cycles per year and the $MTTF_d$ is 1,923 years. Owing to forced dynamics and the start-up warning, a *DC* of at least 60% is assumed (hanging following repeated inching is not detected, however). By incorporation into a Category 2 structure, S1 thus attains an average probability of dangerous failure of 5.28 × 10^{-7} per hour.
- Owing to evaluation of the sin/cos signals and its use in the closed-loop control circuit (for commutation), G1 is integrated in accordance with Category 3. At an $MTTF_d$ per channel of 30 years [E] and a *DC* of 90% owing to plausibility testing and fault detection in the process, the average probability of dangerous failure is 2.65 × 10^{-7} per hour.
- $MTTF_d$: 100 years [E] is allowed for K1 and K2, 50 years [E] for K4, and 30 years [E] for K3. In addition, 30 years [E] is substituted for T1a and 1,000 years [E] for T1b. Overall, this produces a symmetrized $MTTF_d$ value per channel of 24 years ("medium").
- DC_{avg}: the *DC* of 99% for K1 and K2 is produced by direct comparison of the supplied status information in K4. The *DC* of 99% for K3 is based upon parallel processing of all safety-related information in K4 and upon the direct comparison in K4 with the intermediate results and output signals formed by K3. The self-tests implemented in K4 together with partial monitoring by the reading back of pulse blocking by K3 result in a *DC* of 60% for K4. The *DC* of 99% for T1a is based upon comparison in K4 between the setpoint and actual value of the shaft position. For T1b, assumption of a fault exclusion for the internal optocoupler owing to readback of addressing of pulse blocking results in a *DC* of 60%. Averaging then produces a DC_{avg} of 91% ("medium").
- Adequate measures against common cause failure (70 points): separation (15), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The combination of K1 to K4 and T1 corresponds to Category 3 with a medium $MTTF_d$ per channel (24 years) and a medium DC_{avg} (91%). This results in an average probability of dangerous failure of 3.33 × 10^{-7} per hour. The values for B1 and of G1 must be added to this figure for the safety-related stop function



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 x 10^{-7} の最大マーカー値に下げる。

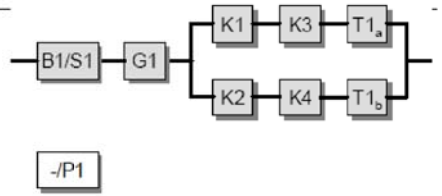
- S1 は 100,000 サイクル[M]の B_{10d} 値を持つ。1 週間に 10 回の運転で、n_{op} は 1 年に 520 サイクル、$MTTF_d$ は 1,923 年となる。強制された動作および起動警告により、少なくても 60% の DC を想定する（しかしながら繰り返しの寸動に続くハングアップは検出されない）。カテゴリー2 構造への取り込みにより、S1 は 1 時間あたり 5.28 x 10^{-7} の危険側故障の平均確率に達する。
- sin/cos 信号の評価および閉ループ制御回路でのその使用（整流化）により、G1 はカテゴリー3 に従って集積化される。チャンネルごとの 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 x 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~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 x 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。



and the safely limited speed. (1.00 + 2.65 + 3.33) × 10^{-7} per hour = 6.98 × 10^{-7} per hour thus results in a PL of d. The values for S1 and G1 must be added for inching mode: a value of (5.28 + 2.65 + 3.33) × 10^{-7} per hour = 1.13 × 10^{-6} per hour is thus produced. This corresponds to PL c.

More detailed references

- 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



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

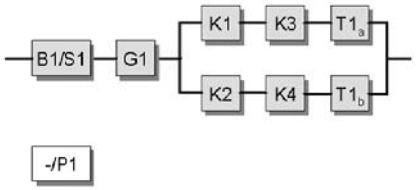
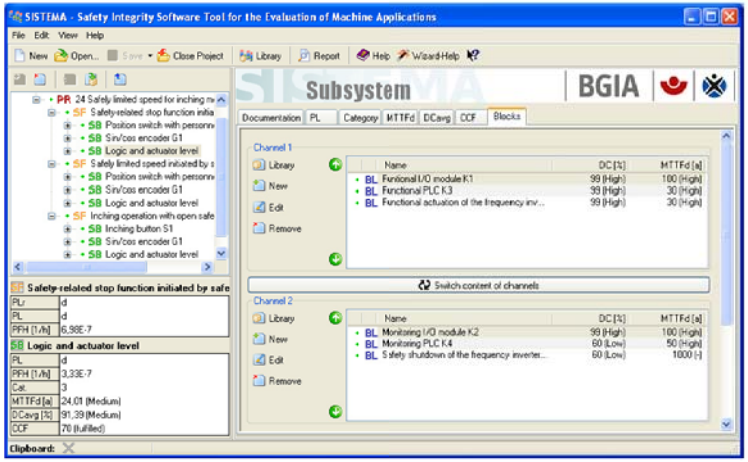


Figure 8.43:
Determining of the PL by means of SISTEMA



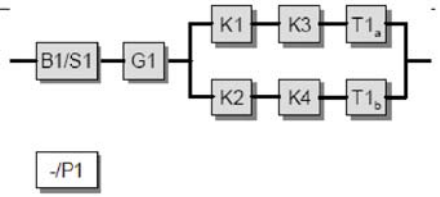
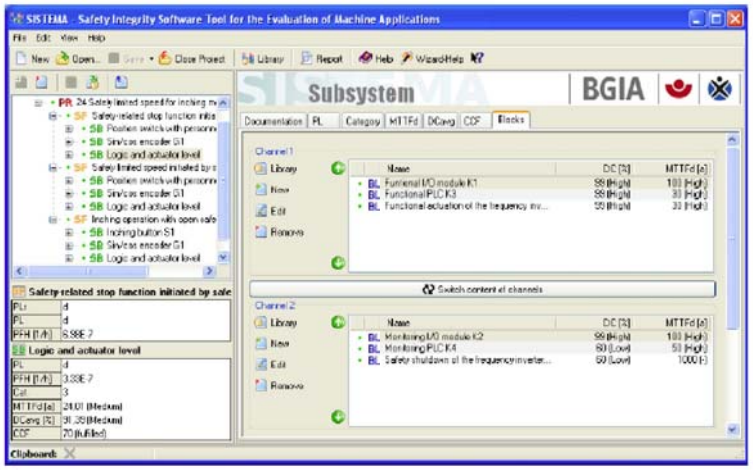
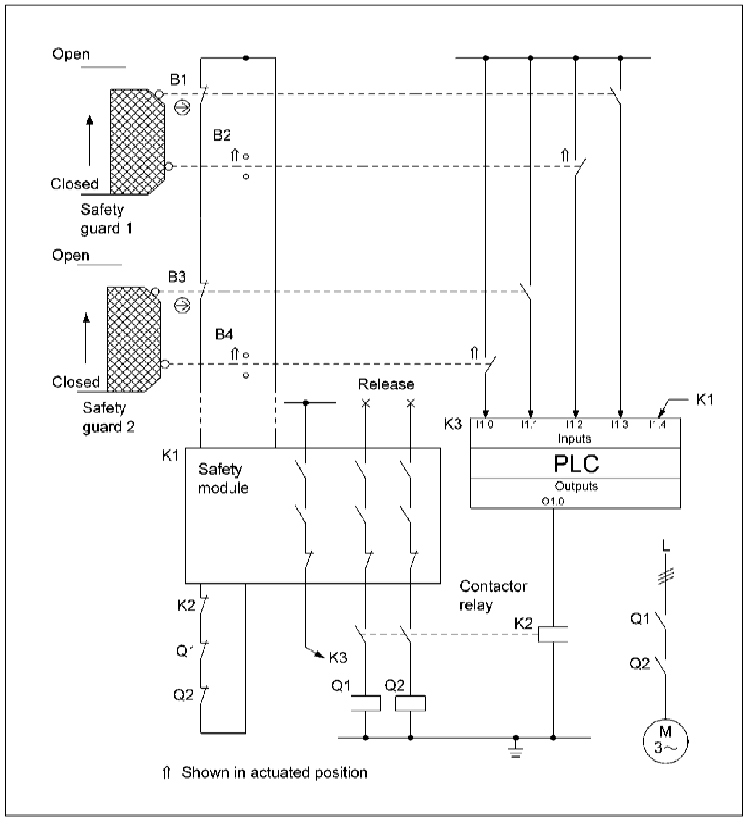


図 8.43：SISTEMA による PL の決定



8.2.28 Position monitoring of moveable guards – Category 4 – PL e (Example 28)

Figure 8.49:
Position monitoring of moveable guards for the prevention of hazardous movements

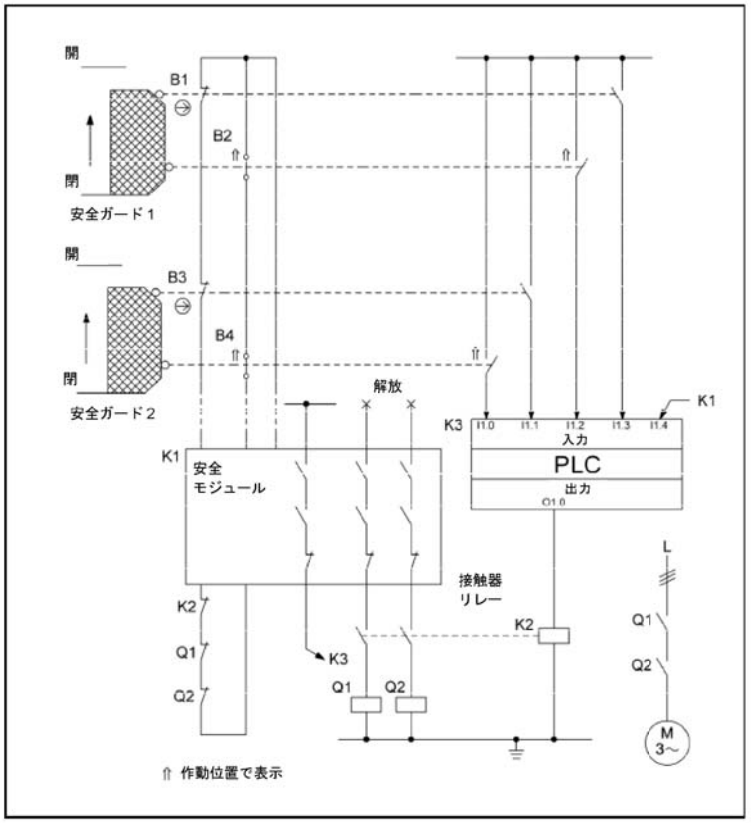


Safety function

- Safety-related stop function, initiated by a protective device: opening of a moveable guard (safety guard) initiates the safety function STO (safe torque off).

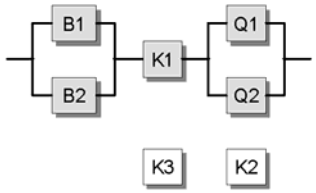
8.2.28 可動式ガードの位置監視 － カテゴリー4 － PL e（例 28）

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。

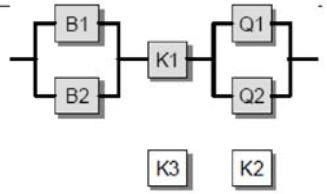


Functional description

- A hazardous zone is safeguarded by two moveable guards (safety guards). Opening of the two safety guards is detected by two position switches B1/B2 and B3/B4 comprising break contact/make contact combinations and evaluated by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- For fault detection purposes, all position switch states are read by a second contact into a standard PLC K3, the chief purpose of which is functional control. In the event of a fault, K3 can de-energize the contactors Q1 and Q2 independently of K1 by means of a contactor relay K2. Faults in K2, Q1 and Q2 are detected by the safety module K1. A small number of faults are not detected (e.g. failure of the contacts in B2 and B4 to break).
- The safety function is retained in the event of a component failure. The majority of component failures are detected and lead to operating inhibition. An accumulation of undetected faults does not result in loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- B1 and B3 are position switches with direct opening contacts according to IEC 60947-5-1, Annex K.
- The supply conductors to the position switches are laid separately or with protection.
- Faults in the start-up and actuation mechanism are detected by the use of two position switches differing in the principle of their actuation (break and make contact combination).
- Several protective devices may be cascaded.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors K2, Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

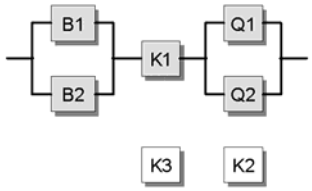


機能の説明

- 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、N.C.接点/ N.O.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

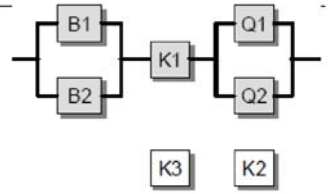
- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 位置スイッチの作動のために保護装置の安定した配置を確保する。
- B1 および B3 は IEC 60947-5-1　付属書 K による直接開接点付き位置スイッチである。
- 位置スイッチへの電源配線は、別々に配線または保護されている。
- 起動および作動メカニズムでのフォールト（故障）は、作動の原則（N.C.および N.O.接点の組み合わせ）に違いのある 2 つの位置スイッチによって検出される。
- いくつかの保護装置がカスケード接続され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



- The PLC K1 satisfies the normative requirements described in Section 6.3.

Calculation of the probability of failure

- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the safety module K1 is added at the end of the calculation (2.31×10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows. Since each safety guard forms part of a dedicated safety function, calculation is shown here by substitution for protective device 1.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening contact. For the electrical make contact of the position switch B2, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the $MTTF_d$ is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The value assumed above for n_{op} results in an $MTTF_d$ of 3,424 years per channel for Q1 and Q2. Altogether, the symmetrized $MTTF_d$ value per channel in the two subsystems is 100 years ("high").
- DC_{avg}: the DC of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact combinations in the PLC K3. The DC of 99% for the contactors Q1 and Q2 is derived from monitoring at each energization of K1. The DC values stated correspond to the DC_{avg} of the subsystem concerned.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The subsystems B1/B2 and Q1/Q2 both correspond to Category 4 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure in each case of 2.47×10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 5.16×10^{-8} per hour. This corresponds to PL e.



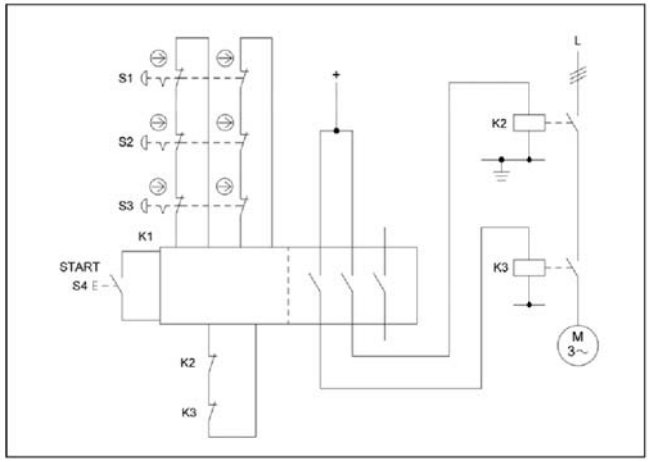
- PLC K1 は 6.3 項に記載の必須要求事項を満たす。

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 2.31×10^{-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 N.O.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、PLC K3 での N.C./ N.O.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。提示された 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 2.47×10^{-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 5.16×10^{-8} となる。これは PL e に相当する。

8.2.29 Cascading of emergency stop devices by means of a safety module – Category 3 – PL e (Example 29)

Figure 8.50:
Cascading of emergency stop devices by means of a safety module (emergency stop function, STO)



Safety function

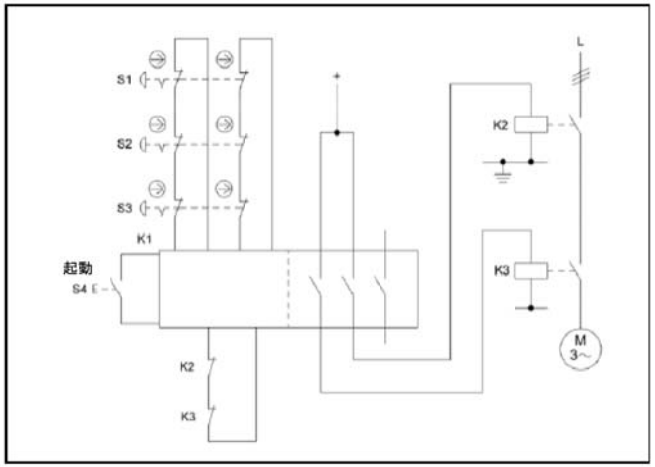
- Emergency stop function, STO by actuation of an emergency stop device

Functional description

- Hazardous movements or states are interrupted or prevented by actuation of an emergency stop device. As shown by Example 3 in Section 5.3.2, each emergency stop device triggers a safety function of its own. S1 is considered below as being representative of all the devices. S1 is evaluated in a safety module K1, which actuates two redundant contactor relays K2 and K3.
- The signals from the emergency stop devices are read redundantly into the safety module K1 for fault detection. K1 also features internal test measures. The contactor relays K2 and K3 are also monitored in K1, by means of mechanically linked readback contacts. K2 and K3 are operated by switch S4 at each start-up command, approximately twice each month. An accumulation of more than two faults in the period between two successive actuations may lead to loss of the safety function.
- It is not assumed that more than one emergency stop device is pressed simultaneously.

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）

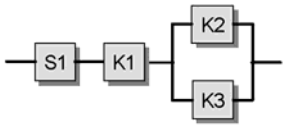


安全機能

- 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。



Design features

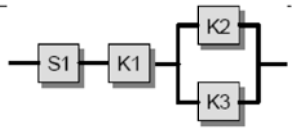
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The emergency stop devices S1, S2 and S3 are switching devices with direct opening contacts in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to the switching devices are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- K2 and K3 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

Remark

- The emergency stop function is a complementary protective measure to EN ISO 12100-2:2004.

Calculation of the probability of failure:

- S1, S2 and S3 are standard emergency stop devices to EN ISO 13850. Fault exclusions apply for the direct opening contacts and for the mechanical elements, provided the number of operations stated in Table D.2 of this report is not exceeded.
- The probability of failure of the final safety module K1 is added at the end of the calculation (2.31×10^{-9} per hour [M], suitable for PL e). For the subsystem K2/K3, the probability of failure is calculated as follows.
- $MTTF_d$: for the contactor relays K2 and K3, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. With three demands upon the emergency stop function and 24 start commands per year, n_{op} is 27 cycles per year and the $MTTF_d$ is 740,740 years. This is also the symmetrical $MTTF_d$ for the channel, which is capped to 100 years ("high").
- DC_{avg}: the *DC* of 90% for K2 and K3 is based upon testing by the safety module K1. This is also the DC_{avg} ("medium").
- Adequate measures against common cause failure (70 points): separation (15), well-tried components (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)



設計特性

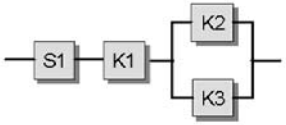
- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 非常停止装置 S1、S2 および S3 は IEC 60947-5-1　付属書 K による直接開接点付き開閉装置である。
- 開閉装置への電源配線は、別々に配線または保護されている。
- 安全モジュール K1 は、カテゴリー4 および PL e の全ての要求事項を満たす。
- K2 および K3 は、IEC60947-5-1　付属書 L による機械的に連結した接点要素を有する。

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。

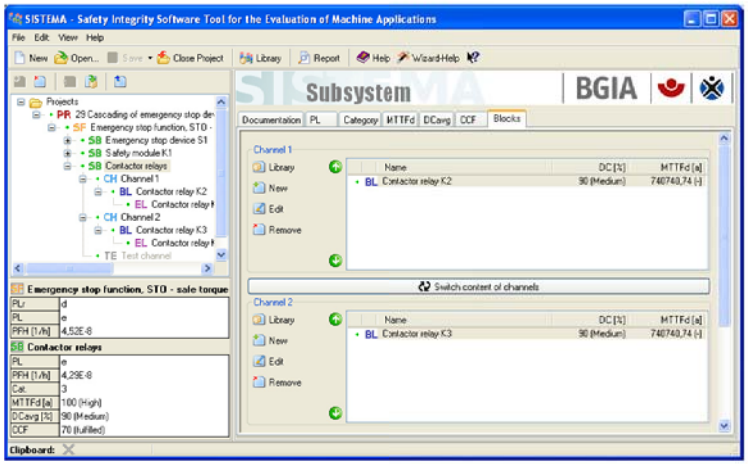
故障確率計算

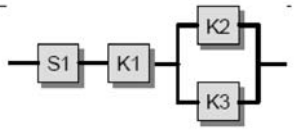
- S1、S2 および S3 は EN ISO 13850 の標準非常停止装置である。本レポートの表 D.2 に記載の操作回数を超えなければ、フォールト（故障）の排除が直接開接点および機械的要素に適用される。
- 最終安全モジュール K1 の故障確率は計算の最後に追加される（1 時間あたり 2.31×10^{-9}[M]、PL e に適する）。サブシステム K2/K3 については、故障確率を下記の通り計算する。
- $MTTF_d$：接触器リレーK2 および K3 については、誘導負荷（AC 3）下において、B_{10} 値は 1,000,000 回の開閉操作[M]の電気的寿命に相当する。故障の 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）



- The subsystem K2/K3 corresponds to Category 3 with a high $MTTF_d$ (100 years) and medium DC_{avg} (90%). This results in an average probability of dangerous failure of 4.29×10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 4.52×10^{-8} per hour. This corresponds to PL e. The PL_r of d is thus surpassed.

Figure 8.51:
Determining of the PL by means of SISTEMA



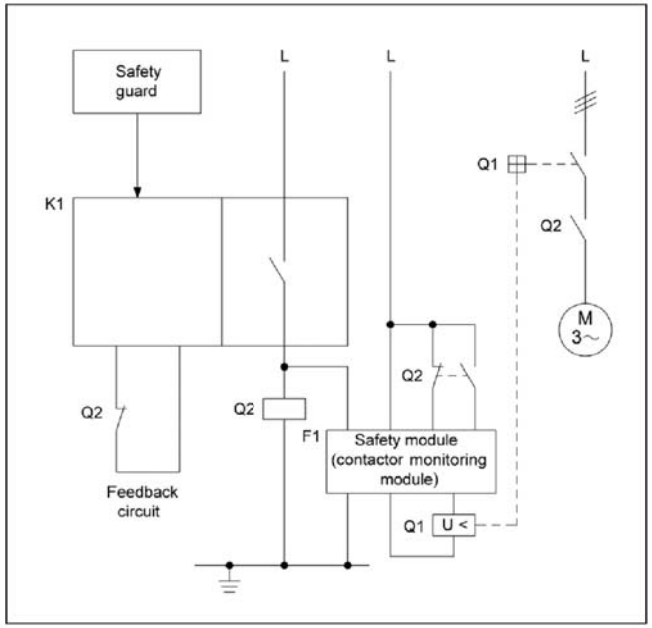


- サブシステム K2/K3 は、高い $MTTF_d$（100 年）と中間の DC_{avg}（90%）のカテゴリー3 に相当する。これにより、危険側故障の平均確率は 1 時間あたり 4.29×10^{-8} となる。サブシステム K1 の加算により、危険側故障の平均確率は 1 時間あたり 4.52×10^{-8} となる。これは PL e に相当し、そのため、d の PL_r を超える。

図 8.51：SISTEMA による PL の決定

8.2.30 Contactor monitoring module – Category 3 – PL e (Example 30)

Figure 8.52:
Initiation of STO (safe torque off) by means of a safety module and contactor monitoring module



Safety function

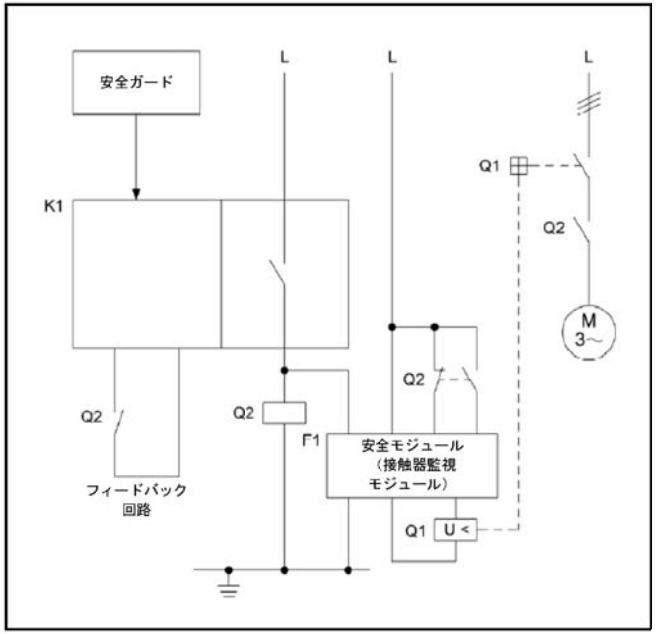
- Safety-related stop function, initiated by a protective device: opening of the moveable guard initiates the safety function STO (safe torque off).

Functional description

- A hazardous zone is safeguarded by means of a protective device the opening of which is detected by a safety module K1. The latter actuates a contactor Q2 and a combination of a contactor monitoring module F1 and an undervoltage release Q1. The dropping-out of Q2 interrupts hazardous movements and prevents hazardous states. The contactor monitoring module F1 has the function of monitoring the main contacts of contactor Q2 for contact welding. Should Q2 fail to drop out, F1 trips the upstream circuit-breaker or motor starter Q1 via the

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

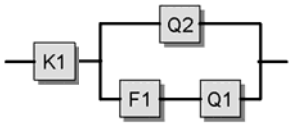


安全機能

- 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。



latter's undervoltage release. The circuit-breaker or motor starter then switches off the motor.

- The safety function is retained in the event of a component failure.
- An accumulation of faults between two successive actuations may lead to loss of the safety function.

Design features

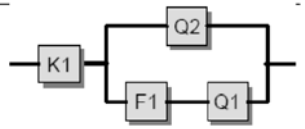
- Circuit-breaker Q1 is checked regularly by means of a test function which is to be implemented manually. The interval between the tests should not exceed one-hundredth of the $MTTF_d$ of Q1; the test could be performed for example during maintenance of the machine. The contactor Q2 is tested continually by the contactor monitoring module. Loss of the safety function between the tests, as is possible with Category 2, cannot occur. The single-fault tolerance is thus assured and the requirements of Category 3 are met.
- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- For reasons of simplification, details of the protective device have been omitted from the presentation.
- The protective device acts upon a safety module K1 which satisfies all requirements for Category 3 or 4 and PL e.
- Contactor Q2 features mirror contacts to IEC 60947-4-1, Annex F, and is integrated into the feedback of safety module K1 for contactor fault detection.
- Fault consideration for Q2 (with mirror contacts) and for the internal relay of the contactor monitoring module F1 is as for mechanically linked contacts.

Remark

- Consideration must be given to the response time caused by contactor monitoring module F1 with regard to the dropping-out of Q1.

Calculation of the probability of failure

- The safety function permits division into two subsystems. The subsystem consisting of the protective device and safety module K1 is not considered in this example.
- $MTTF_d$: for the contactor monitoring module F1, the $MTTF_d$ is 125 years at a maximum n_{op} of 350,400 cycles per year [M]. Under inductive load (AC 3), the B_{10d} value for Q1 is 10,000 switching cycles, and the B_{10d} value for Q2



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

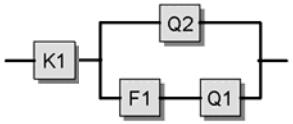
- サーキットブレーカ Q1 は、手動で実行される試験機能により定期的に点検する。試験の間隔は Q1 の $MTTF_d$ の 100 分の 1 を超えないことが望ましい；試験は例えば機械のメンテナンス中に行うことができる。接触器 Q2 は、接触器監視モジュールにより連続的に試験されている。カテゴリー2 では可能な、試験間の安全機能のロスは起こり得ない。そのため、単独フォールト（故障）の許容は確保され、カテゴリー3 の要求事項を満たす。
- 基本および十分に実証済みの安全原則を守り、カテゴリーB の要求事項を満たす。8 章の最初のパラグラフに記載の保護回路（例えば接点保護）を実装する。
- 簡略化の理由から、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。

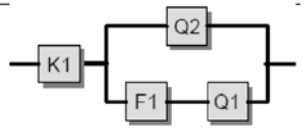
故障確率計算

- 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。



1,300,000 switching cycles. Assuming a once daily actuation on 365 working days, n_{op} is 365 cycles per year for Q1, and the $MTTF_d$ is 274 years. At 365 working days, 16 working hours per day and a cycle time of 1 minute, n_{op} is 350,400 cycles per year for Q2, and the $MTTF_d$ is 37 years. For the channel consisting of F1 and Q1, this results in an $MTTF_d$ of 85 years. Overall, the resulting symmetrized $MTTF_d$ value per channel is 64 years ("high").

- DC_{avg}: the DC of 99% for Q2 is based upon testing by means of the contactor monitoring module F1. A DC of 99% for F1 is achieved by fault-detection measures within the contactor monitoring module. The circuit-breaker is tested by means of the manual test function which is to be implemented; this produces a DC of 90%. A DC of 99% is substituted for F1. Averaging thus yields a DC_{avg} of 98% ("medium").
- Adequate measures against common cause failure (65 points): separation (15), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The subsystem comprising Q1, Q2 and F1 corresponds to Category 3 with a high $MTTF_d$ (64 years) and medium DC_{avg} (98%). This results in an average probability of dangerous failure of 4.45×10^{-8} per hour. This corresponds to PL e. Following addition of the subsystem comprising protective device and safety module K1, the PL may under certain circumstances be lower.
- In consideration of estimation erring on the safe side as described above, a T_{10d} value of 3.7 years is produced for the wearing element Q2 when replaced as specified.

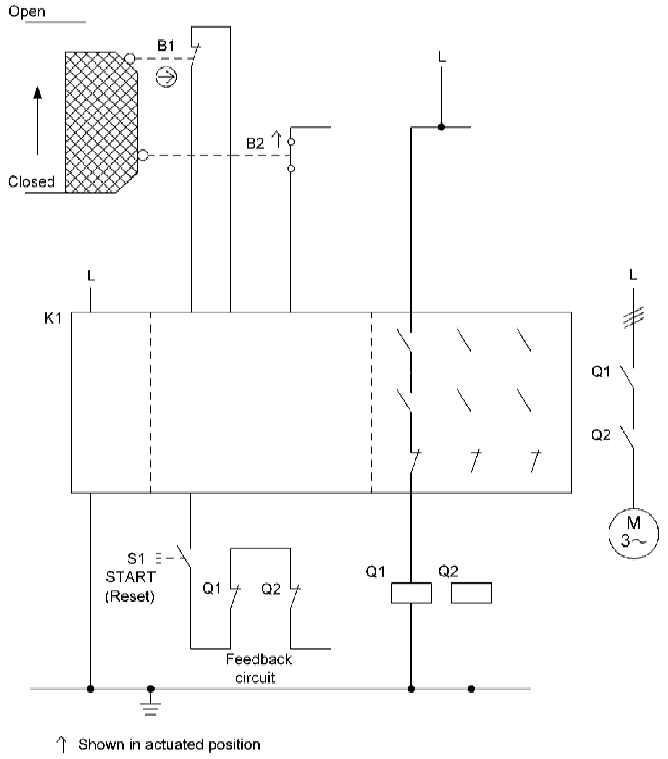


稼働日 365 日中に毎日 1 度作動すると仮定すると、Q1 の n_{op} は 1 年に 365 サイクルで、$MTTF_d$ は 274 年となる。稼働日 365 日、稼働時間 16 時間、サイクル時間が 1 分の場合、Q2 の n_{op} は 1 年に 350,400 サイクルで、$MTTF_d$ は 37 年となる。これにより、F1 および Q1 から成るチャンネルについては、$MTTF_d$ は 85 年となる。全体で、対称化 $MTTF_d$ 値は、チャンネルあたり 64 年（「高」）となる。

- 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 4.45×10^{-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 Position monitoring of moveable guards – Category 4 – PL e (Example 34)

Figure 8.58:
Position monitoring of moveable guards by means of a safety module

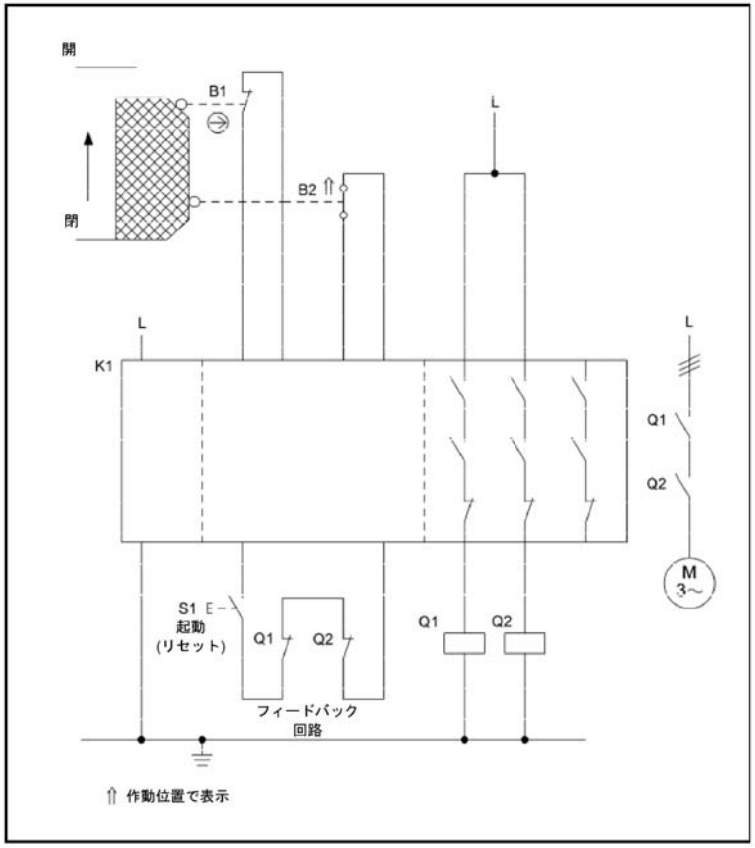


Safety function

- Safety-related stop function, initiated by a protective device: opening of the moveable guard (safety guard) initiates the safety function STO (safe torque off).

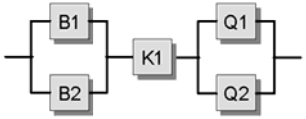
8.2.34 可動式ガードの位置監視 － カテゴリー4 － PL e（例 34）

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。



Functional description

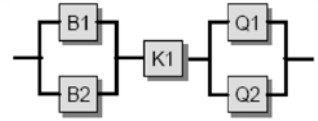
- A hazardous zone is safeguarded by a moveable guard (safety guard). Opening of the safety guard is detected by two position switches B1/B2, employing a break contact/make contact combination, and evaluation by a central safety module K1. K1 actuates two contactors, Q1 and Q2, dropping out of which interrupts or prevents hazardous movements or states.
- The position switches are monitored for plausibility in K1 for the purpose of fault detection. Faults in Q1 and Q2 are detected by a start-up test in K1. A start command is successful only if Q1 and Q2 had previously dropped out. Start-up testing by opening and closing of the protective device is not required.
- The safety function remains intact in the event of a component failure. Faults are detected during operation or at actuation (opening and closing) of the protective device by the dropping out of Q1 and Q2 and operating inhibition.
- An accumulation of more than two faults in the period between two successive actuations may lead to loss of the safety function.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- A stable arrangement of the protective devices is assured for actuation of the position switches.
- Switch B1 is a position switch with direct opening contact in accordance with IEC 60947-5-1, Annex K.
- The supply conductors to position switches B1 and B2 are laid separately or with protection.
- The safety module K1 satisfies all requirements for Category 4 and PL e.
- The contactors Q1 and Q2 possess mechanically linked contact elements to IEC 60947-5-1, Annex L.

Remark

- Category 4 is observed only if multiple mechanical position switches for different protective devices are not connected in a series arrangement (i.e. no cascading), since faults in the switches cannot otherwise be detected.



機能の説明

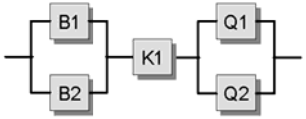
- 危険区域は、可動式ガード（安全ガード）によって安全防護している。安全ガードの開動作は、N.C./ N.O.接点の組み合わせを採用した 2 つの位置スイッチ B1/B2 が検知し、中央安全モジュール K1 が評価する。K1 は、ドロップアウトにより危険な動作や状態を遮断または防止する 2 つの接触器 Q1 および Q2 を作動させる。
- 位置スイッチは、フォールト（故障）検出のために K1 で妥当性を監視される。Q1 および Q2 でのフォールト（故障）は、K1 での起動試験によって検出される。起動コマンドは、Q1 および Q2 が前もってドロップアウトしている場合にのみ成功する。保護装置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。

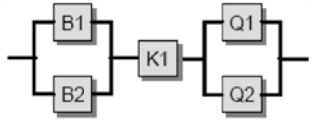
備考

- 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。



Calculation of the probability of failure

- The circuit arrangement can be divided into three subsystems as shown in the safety-related block diagram. The probability of failure of the standard safety module K1 is added at the end of the calculation (2.31 × 10^{-9} per hour [M], suitable for PL e). For the remaining subsystems, the probability of failure is calculated as follows.
- $MTTF_d$: fault exclusion is possible for the electrical contact of the position switch B1 with direct opening action. For the electrical make contact of the position switch B2, the B_{10d} value is 1,000,000 switching operations [M]. A B_{10d} value of 1,000,000 cycles [M] is stated for the mechanical part of B1 and B2. At 365 working days, 16 working hours per day and a cycle time of 1 hour, n_{op} is 5,840 cycles per year for these components, and the $MTTF_d$ is 1,712 years for B1 and 856 years for B2. For the contactors Q1 and Q2, the B_{10} value corresponds under inductive load (AC 3) to an electrical lifetime of 1,000,000 switching operations [M]. If 50% of failures are assumed to be dangerous, the B_{10d} value is produced by doubling of the B_{10} value. The value assumed above for n_{op} results in an $MTTF_d$ of 3,424 years per channel for Q1 and Q2. Altogether, the symmetrized $MTTF_d$ value per channel in the two subsystems is 100 years ("high").
- DC_{avg}: the *DC* of 99% for B1 and B2 is based upon plausibility monitoring of the break/make contact combination in K1. The *DC* of 99% for contactors Q1 and Q2 is derived from regular monitoring by K1 during start-up. The DC values stated correspond to the DC_{avg} for each subsystem.
- Adequate measures against common cause failure in the subsystems B1/B2 and Q1/Q2 (70 points): separation (15), well-tried components (5), protection against overvoltage etc. (15) and environmental conditions (25 + 10)
- The subsystems B1/B2 and Q1/Q2 each correspond to Category 4 with a high $MTTF_d$ (100 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 2.47 × 10^{-8} per hour. Following addition of the subsystem K1, the average probability of dangerous failure is 5.16 × 10^{-8} per hour. This corresponds to PL e.

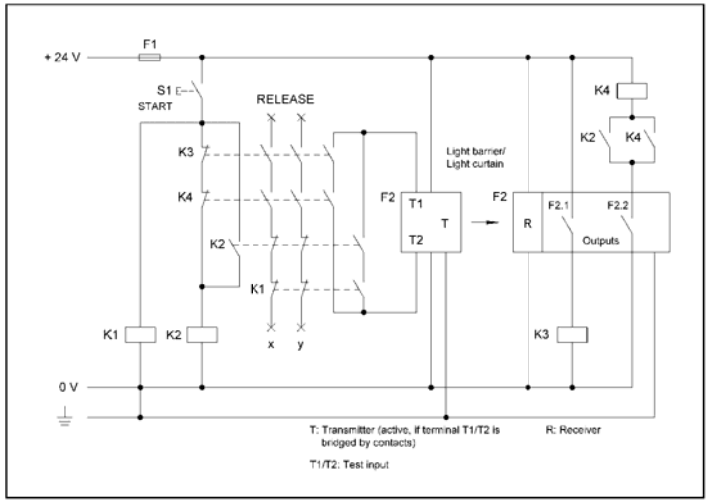


故障確率計算

- 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 N.O.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 N.C./ N.O.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。提示された 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 Processing of signals from a light barrier – Category 4 – PL e (Example 36)

Figure 8.60:
Electromechanical input of safety-related signals into the machine control system with reference to the example of a light barrier or light curtain



Safety function

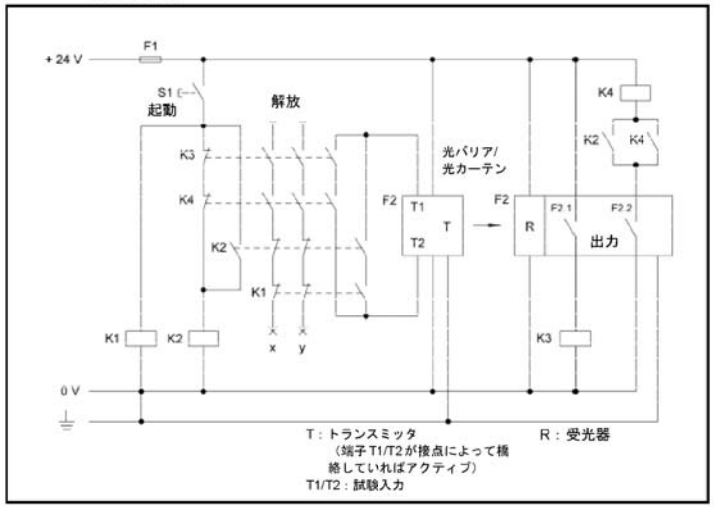
- Safety-related stop function initiated by a protective device: sustained stopping of a hazardous movement in response to entry into a hazardous area or operator intervention at a hazardous zone, and start and restart interlock

Functional description

- Entry into a hazardous area or operator intervention at a hazardous zone is detected by the light barrier F2. The safety-related output signals from the light barrier (make contacts F2.1 and F2.2) de-energize the contactor relays K3 and K4, the coils of which are connected to the power supply in an offset arrangement. K3 and K4 then block the enabling signals x and y.
- For activation of the light barrier transmitter, actuation of the start button S1 first causes the test inputs T1 and T2 to be connected together by picking up of the contactor relays K1 and K2. K2 can pick up and latch in only once the contactor relays K3/K4 have dropped out. With the light path completed, K3 and K4 then pick up. K4 picks up and latches in only by means of the make contact of K2. With K3 and K4 picked up and the start button still depressed, the light barrier

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

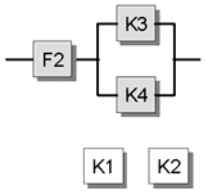


安全機能

- 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（N.O.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 N.O.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。

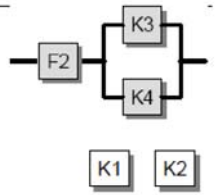


transmitter is activated and latched; the start button can therefore be released, and once K1 and K2 have dropped out, the enabling paths x and y are also closed. Following interruption of the light beam or in the event of breakdown and subsequent restoration of the voltage, the function of the start/restarting interlock prevents a valid enabling signal until K3 and K4 have picked up again following renewed pressing of the start button.

- One make contact each on K3 and K4 is integrated both into the two enabling paths and into the input circuit for activation of the light barrier transmitter (test inputs T1/T2). Connection of the test inputs generates an internal start-up test within the device, for example by blanking of the light beam for a short defined period. On the receiver side, this test is logically evaluated as valid only within a narrow time window. Provided the start-up test is passed, the light barrier outputs are enabled. Conversely, in the event of an outage or fault, or interruption of the light beam, they are blocked.
- Faults in other components in the circuit (contactor relays, output contacts of the light barrier, start button) which in combination could result in the loss of a safety function are detected during the start-up/restarting test following an interruption of the light beam, and prevent renewed enabling.

Design features

- Basic and well-tried safety principles are observed and the requirements of Category B are met. Protective circuits (e.g. contact protection) as described in the initial paragraphs of Chapter 8 are implemented.
- The contactor relays K1 to K4 possess mechanically linked contact elements in accordance with IEC 60947-5-1, Annex L. The relay operating voltage of the contactor relays K3 and K4 must be greater than half the value of the power supply, so that simultaneous pick-up of K3 and K4 in the event of a short-circuit in the cable (connection in series results in the voltage being divided between the contactor coils) does not present a hazard, even in combination with other faults.
- The output signals from the light barrier F2 are routed in a cable, together with the supply conductors, from the electrical compartment of the receiver to the electrical compartment of the machine control system. Owing to application of the closed-circuit current principle and the principle of offset coils (K3, K4) in the earthed control circuit, all open circuits, earth faults and circuit-to-circuit shorts are detected immediately when the light barrier is in the activated state (among other things, by tripping of the fuse F1). A short-circuit which causes a single

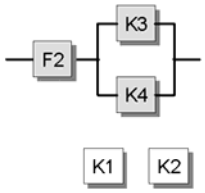


K3 および K4 がピックアップし、かつ起動ボタンが押されたままの状態で、光バリアトランスミッタは活性化しラッチする；そのため、起動ボタンを放すことができ、K1 および K2 が一旦ドロップアウトすると、イネーブル経路 x および y もまた閉じる。光ビームの遮断後、または停電およびそれに続く電圧の復旧の場合は、起動ボタンを再度押した後に K3 および K4 が再度ピックアップするまで、起動/再起動インターロックの機能がイネーブル信号の有効になるのを防ぐ。

- K3 および K4 のそれぞれ 1 つの N.O.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。



output to be bridged is detected at the latest at the next interruption of the light barrier when the start button is subsequently actuated. Common routing of the output signals within a single cable is therefore permissible.

- The light barrier satisfies the requirements for Type 4 in accordance with EN 61496-1 and IEC 61496-2, and PL e.

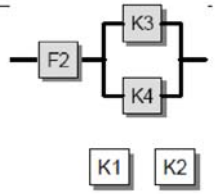
Remarks

- If the circuit is employed in applications in which the light barrier switches very infrequently, the possibility must be considered of the safety function being lost as a result of an accumulation of faults (two discrete undetected faults). Such loss may be countered by periodic testing.
- The manufacturer's information concerning the maximum switching frequency of the light barrier must be observed.

Calculation of the probability of failure

The probability of failure of the safety-related stop function, which is also shown on the safety-related block diagram, is calculated. If the contacts of the enabling paths x and y are processed further by the control system, the additional control components concerned, e.g. contactors, must be considered in the calculation of the probability of failure.

- The light barrier F2 is a standard safety component. The probability of failure of 3.0×10^{-8} per hour [E] is added at the end of the calculation.
- $MTTF_d$: owing to the unknown loads, the B_{10d} value for K3 and K4 is 400,000 cycles [S]. At 220 working days, 8 working hours per day and a cycle time of 120 seconds, n_{op} is 52,800 switching operations per year, and the $MTTF_d$ is thus 75 years. This is also the $MTTF_d$ value of each channel ("high").
- DC_{avg}: the *DC* of 99% for K3 to K4 is derived from incorporation of the mechanically linked break contacts into the actuation circuit of K2. This also corresponds to the DC_{avg} ("high").
- Adequate measures against common cause failure (75 points): separation (15), well-tried components (5), FMEA (5), overvoltage protection etc. (15) and environmental conditions (25 + 10)
- The K3/K4 subsystem corresponds to Category 4 with a high $MTTF_d$ per channel (75 years) and high DC_{avg} (99%). This results in an average probability of dangerous failure of 3.37×10^{-8} per hour. The overall probability of failure is



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。

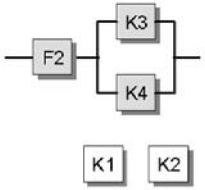
備考

- 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 3.0×10^{-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 N.C.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 3.37×10^{-8} となる。



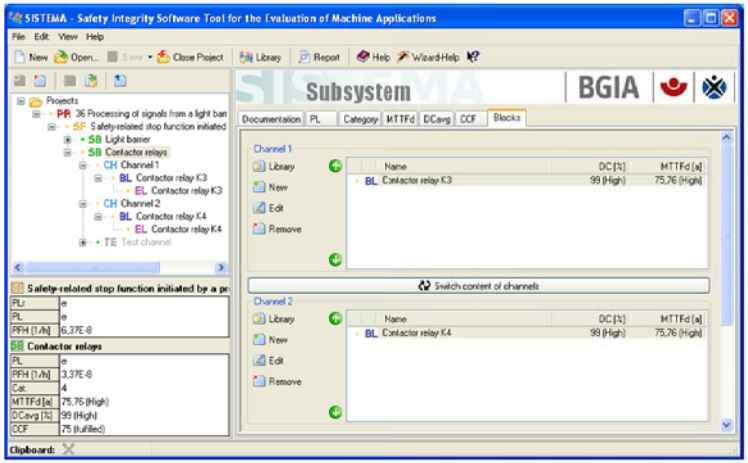
determined by addition of the probability of dangerous failure of F2 (3.0×10^{-8} per hour) and is equal to 6.37×10^{-8} per hour. This corresponds to PL e. The probability of failure of downstream power components may have to be added for completion of the safety function.

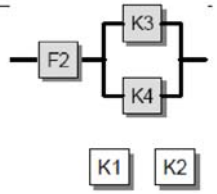
- The wearing elements K3 and K4 should be replaced at intervals of approximately seven years (T_{10d}).

More detailed reference

- 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"

Figure 8.61:
Determining of the PL by means of SISTEMA





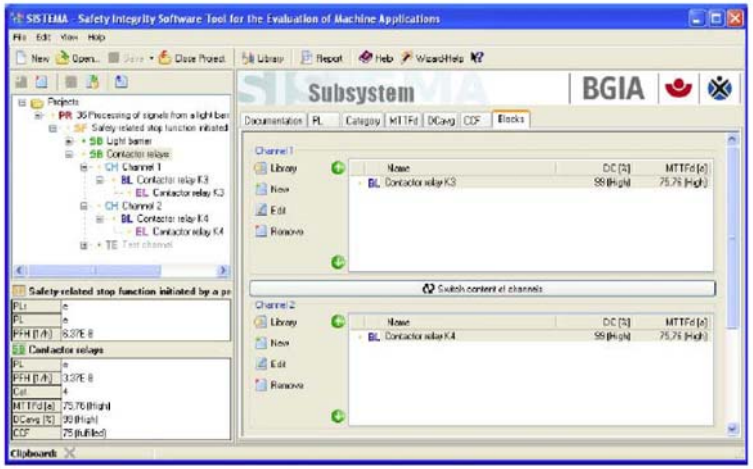
全故障確率は、F2 の危険側故障の確率（1 時間あたり 3.0×10^{-8}）を加算して決定し、それは 1 時間あたり 6.37×10^{-8} に等しい。これは PL e に相当する。下流動力構成部品の故障確率を、安全機能を完成させるために加算しなければならない可能性がある。

- 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



2. BG-SISTEMA の概要

2.1 SISTEMA とは

SISTEMA は、ドイツの BGIA が作成したパフォーマンス・レベル(PL)評価ソフトである。このソフトは、ISO 13849-1 の 2006 年版に基づいて構築した安全関連部の安全機能について PL の評価を数値的に行うためのものである。評価としては、安全機能の要求 PL を求め、この要求 PL を満足できているかを、構築しているカテゴリの選択、使用している各部品の MTTFd、DCavg、CCF から PL 値を算出して行う。

2.2 SISTEMA のダウンロードとインストール

2010 年 2 月現在の SISTEMA のバージョンは 1.1.1 です。

アドレス：http://www.dguv.de/bgia/en/pra/softwa/sistema/index.jsp

ダウンロードファイル名とデータ容量：　SISTEMA.ZIP　サイズ:10.1MB

2.2.1 ダウンロード方法

上記アドレスにアクセスすると下記の画面となる。

上記の画面から、DownloadVersion:1.1.1 を押すと次ページの画面になる。

e-mail address に自分のメールアドレスを入力して、Submit(送信)を押す。

自分のメールボックスに BGIA より SISTEMA をダウンロードするためのリンクデータが送信される。

メールに記載のリンクは次のようになっており(Click this link to download the software)、リンクを押すと下記のホームページが開く。

BGIA より SISTEMA のアップデート情報を送ってもらうかの選択をし、SISTEMA Download のボタンを押すと“SISTEMA.ZIP”のダウンロードが開始される。

2.2.2 インストール方法

ダウンロードした SISTEMA ファイルは、ZIP 形式となっていますので、解凍する必要がある。別途 ZIP を解凍するソフトが必要である。

SISTEMA.ZIP ファイルを解凍すると、SISTEMA フォルダが前記ファイルと同じ場所に下記のファイルが作成される。

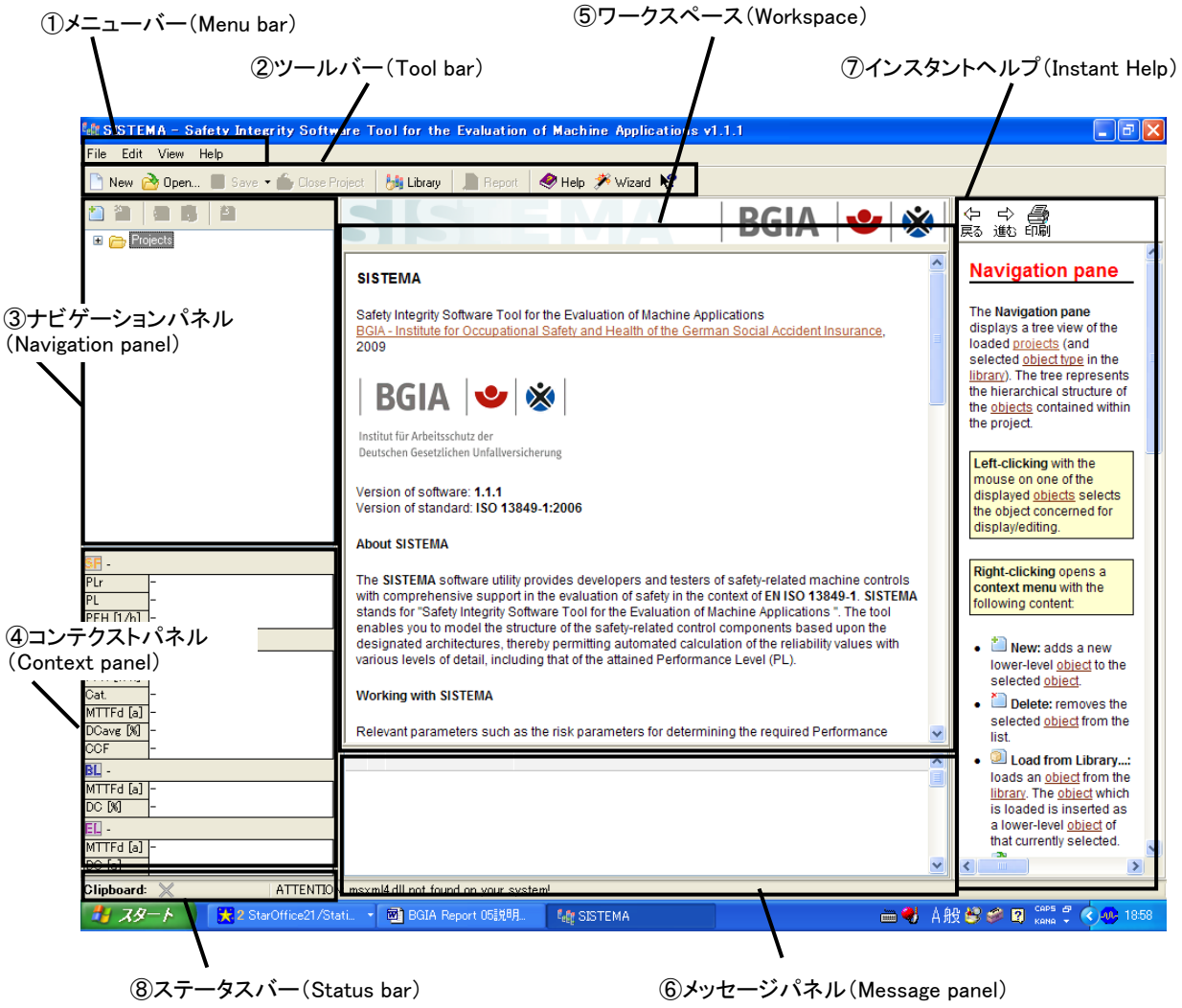
SISTEMA_1_1_1.exe、　サイズ：10.1MB

このファイルをインストールすると、SISTEMA が使用できる。

2.3 SISTEMA 基本操作説明

2.3.1 Main window（メイン画面）

SISTEMA のメイン画面は以下の領域に分割されています。



① メニューバー（Menu bar）：すべての操作へアクセスできます。
② ツールバー（Tool bar）：頻繁に使用される操作へ高速アクセスできます。
③ ナビゲーションパネル（Navigation pane）：
ロードされた projects に関するツリー構造で、下位レベル objects の全てを表示します。
④ コンテクストパネル（Context pane）：
現在、選択されている、最上位レベルの objects の主なパラメタ値を表示します。
⑤ ワークスペース（Workspace）：選択された object の詳細情報を表示します。
⑥ メッセージパネル（Message pane）：
選択された object に関連する警告やエラーメッセージのような情報を表示します。
⑦ インスタントヘルプ（Instant Help）：文脈特有のヘルプ情報を表示します。
⑧ ステータスバー（Status bar）：SISTEMA に関連する様々な状態情報を表示します。

2.3.2 ナビゲーションパネルのオブジェクトタイプ（Object type）の記号説明

SISTEMA は 7 つの異なったタイプのオブジェクトがあります。

・PR：**プロジェクト**（Project）
セーフティファンクションオブジェクトタイプの上にそれは階層構造に位置します。
プロジェクトはいくつかのセーフティファンクション（安全機能）を含むかもしれません。
プロジェクト自体はオブジェクトタイプの階層構造の最上位レベルを構成します。

・SF：**セーフティファンクション**（Safety function）
プロジェクトの下位で、サブシステムの上位の階層構造に位置します。
その故障が直接リスク増加につながるかもしれない分析中の機械のどんな機能もセーフティ・ファンクションとして記述されます。
セーフティファンクションは１つ以上のサブシステムで実行されます。

・SB：**サブシステム**（Subsystem）
セーフティファンクションの下位で、チェンネル／テストチャンネルの上位の階層構造に位置します。サブシステムは、安全関連の信号を処理して、発生させる制御システムの一部です。いくつかのサブシステムがセーフティファンクションの実現のためのシリーズアレンジメントで接続されるのは、可能です。 一般に、サブシステムは指定された構造を満たします。この場合、基本的構造はチャンネルの数と、そしてテスト装置(カテゴリ 2 だけにおける）の項目によって決定します。

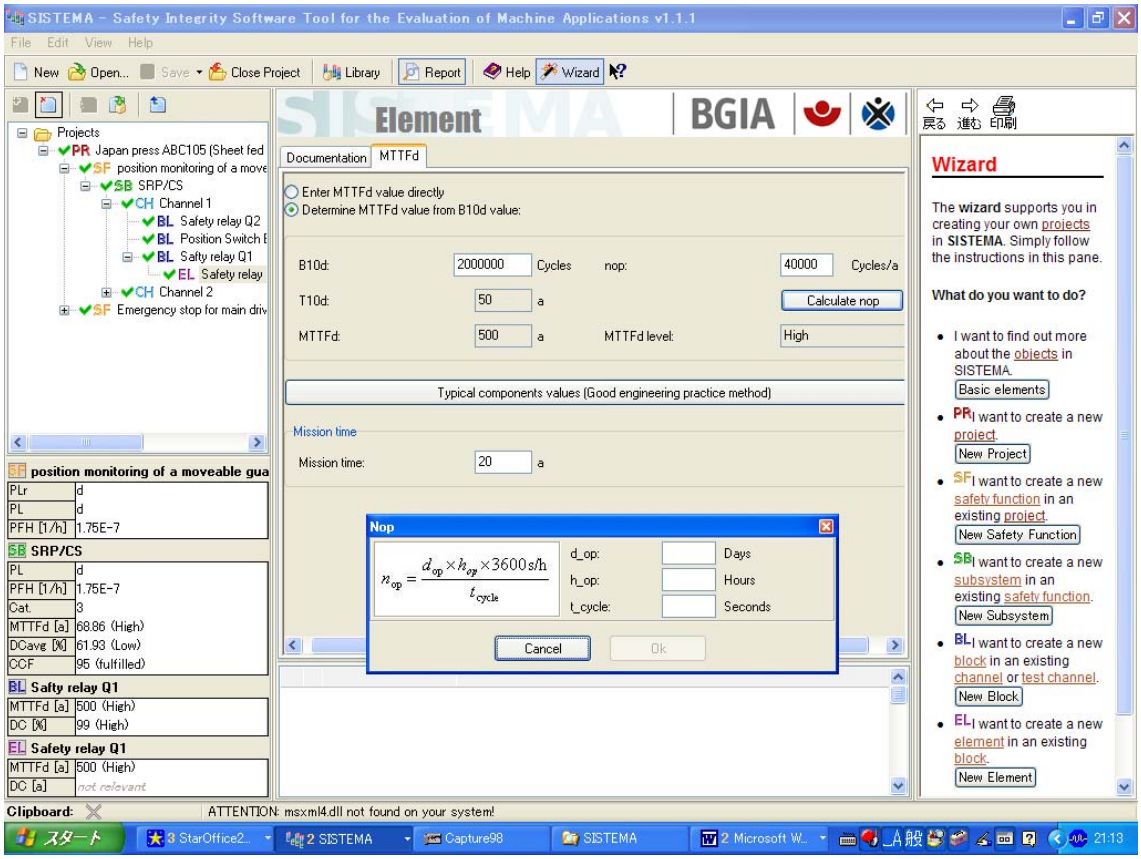
・CH：**チェンネル**（Channel）
サブシステムは１か２個のチャンネルで構成されます。チェンネルオブジャクトはブロックで構成され、マルチチャンネル構造のモデル化を可能にします。 チャンネルの数は、より上位レベルのサブシステムと関連する指定された構造のカテゴリの選択で決定されます。

・TE：**テストチャンネル**（Test Channel）
カテゴリ２の構造の中では、テストチャンネルやテスト要件の項目がファンクションチャンネルの機能が適切に実行されるかどうかに関する繰り返されたテストの機能を持っています。
チャンネル１のように、テストチャンネルはサブシステムの一部を形成します。
サブシステムは、１つ未満のテストチャンネルを持っているかもしれません。

・BL：**ブロック**（Block）
ブロックオブジャクトは論理的なブロック図の中の機能ブロックを構成します。
それは論理的な機能的なユニット(例えば、センサ、論理、メイン接触器)の中でチャンネルを分割します。チャンネルはいつも少なくとも１つのブロックを含まれるべきです。
ブロックがその構成エレメントのリストによって、さらに大きいモデル化できます。

・EL：**エレメント**（Element）
エレメントはオブジェクトタイプの中で最も下位を構成します。
エレメントは機能ブロックが構成している電子の、または、電気機械の、または、水力の、または、機械的であるか空気のコンポーネントです。

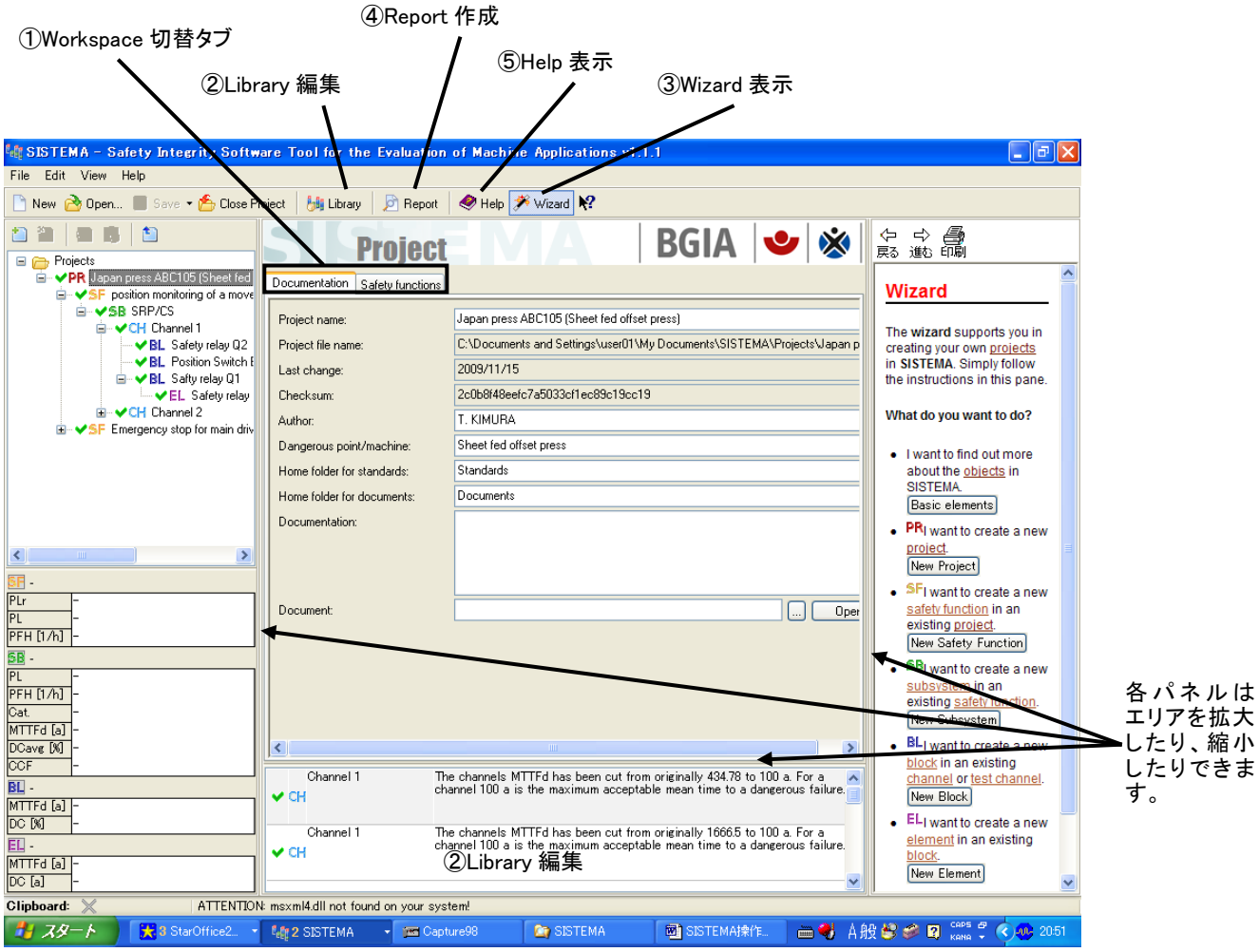
2.3.3 操作画面の用語説明



用語の説明

- PL：Performance Level：到達パフォーマンスレベル
- PLr：the required Performance Level：要求パフォーマンスレベル
- PFH：the average probability of a dangerous failure per hour
  ：時間当たり危険側故障の平均確率
- MTTFd：the Mean Time to a Dangerous Failure
  ：平均危険側故障間隔（平均）時間
- DCavg：the average Diagnostic Coverage：平均診断範囲
- CCF：Common Cause Failure：共通原因故障
- B10d：the Mean Number of Cycles until 10% of the Components Fail Dangerously
  ：コンポーネントの 10%が危険側に故障するまでの平均サイクル数
- T10d：the Mean Time until 10% of the Components Fail Dangerously
  ：コンポーネントの 10%が危険側に故障までの平均時間
- nop：the Mean Number of Annual Operations：通常操作での平均回数
- hop：the Mean Operation Hour per Day：１日の稼動時間（単位：hour/day）
- dop：the Mean Operation Days per Year：年間稼働日（単位：day/year）
- Tcycle：the Mean Time between the Beginning of Two Successive Cycles of the Component
  ：１操作サイクルの平均時間間隔（単位：second/cycle）

2.3.4 その他の操作説明



① Workspace 切替タブ

ワークスペースでの入力項目により、切替タブがあり、入力画面を切り替えることができます。

② Library 編集

ライブラリの編集ができます。

③ Wizard 表示

ウィザードの表示を行いことができます。

④ Report 作成

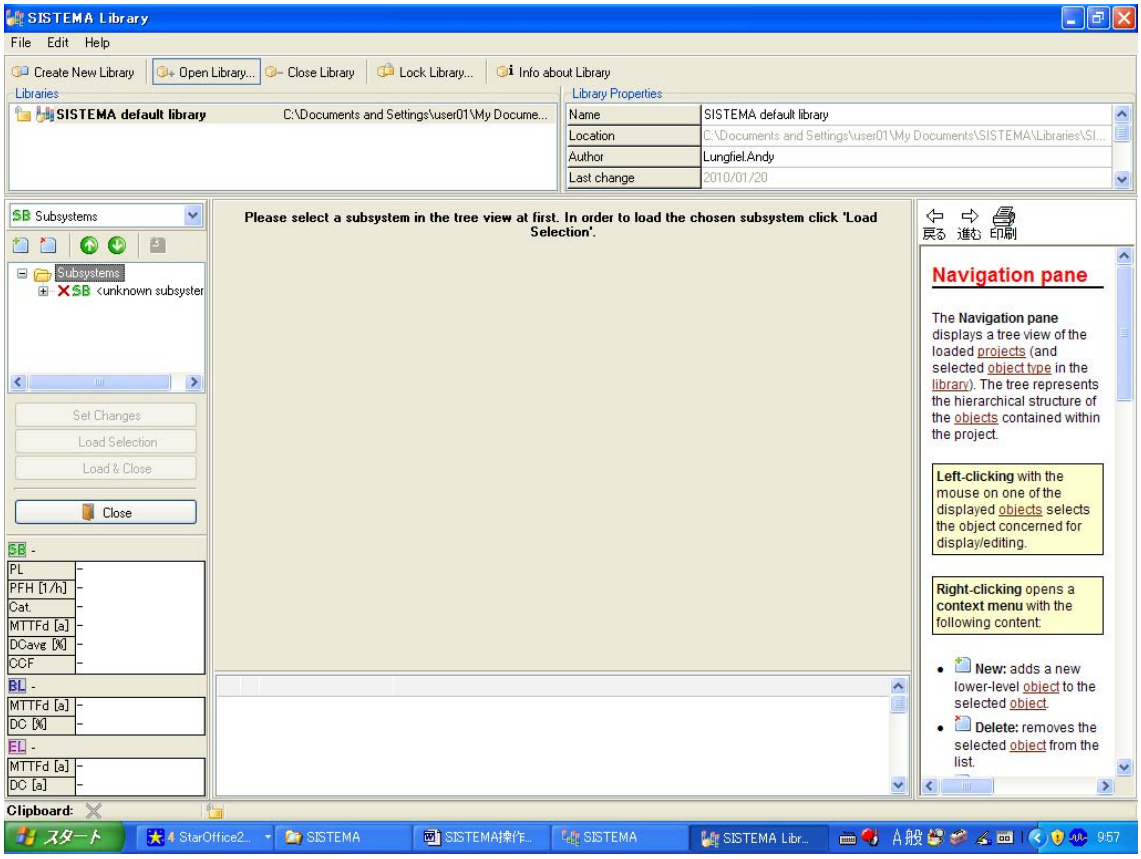
作成したプロジェクトに対する内容を、レポート形式でプリント出力できます。

⑤ Help 表示

SISTEMA の操作の中で、用語の説明や操作方法について、説明文を見ることができます。

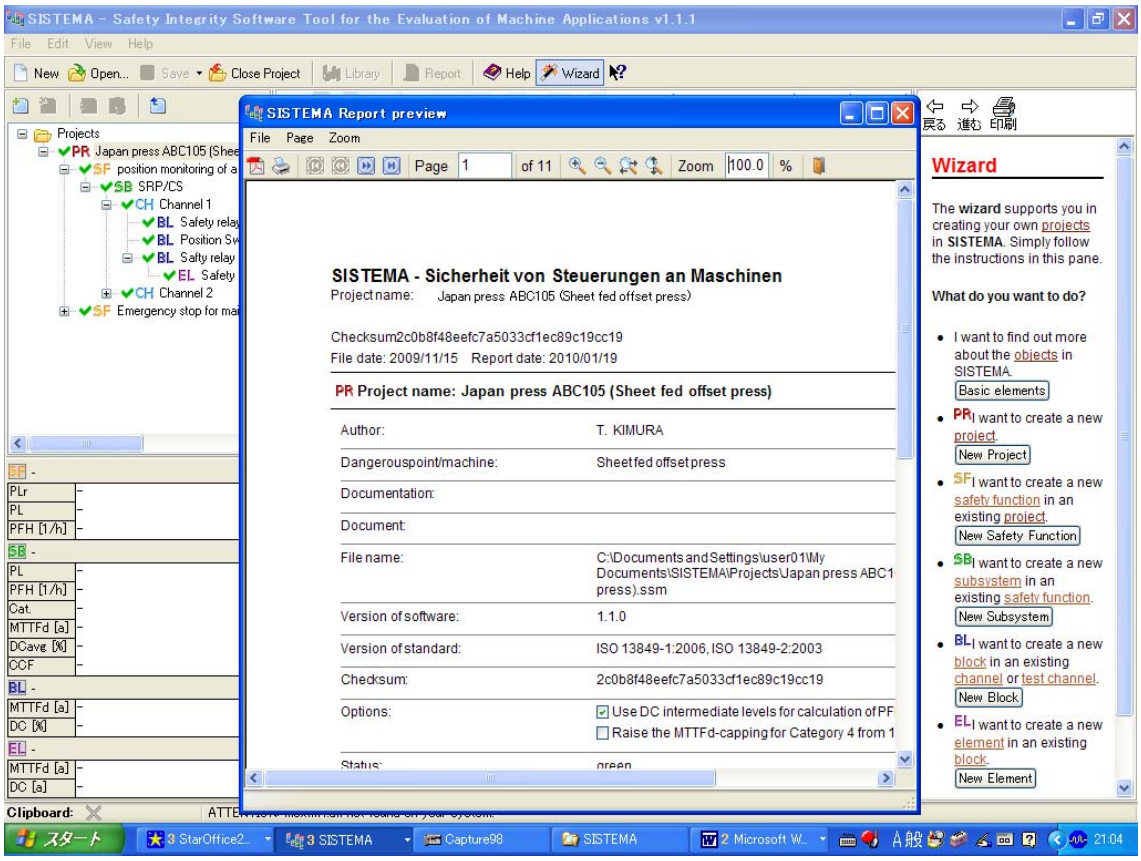
(1)Library 編集の説明

ツールバーの Lobrary 表示のボタンをクリックすると、ライブラリが編集できます。



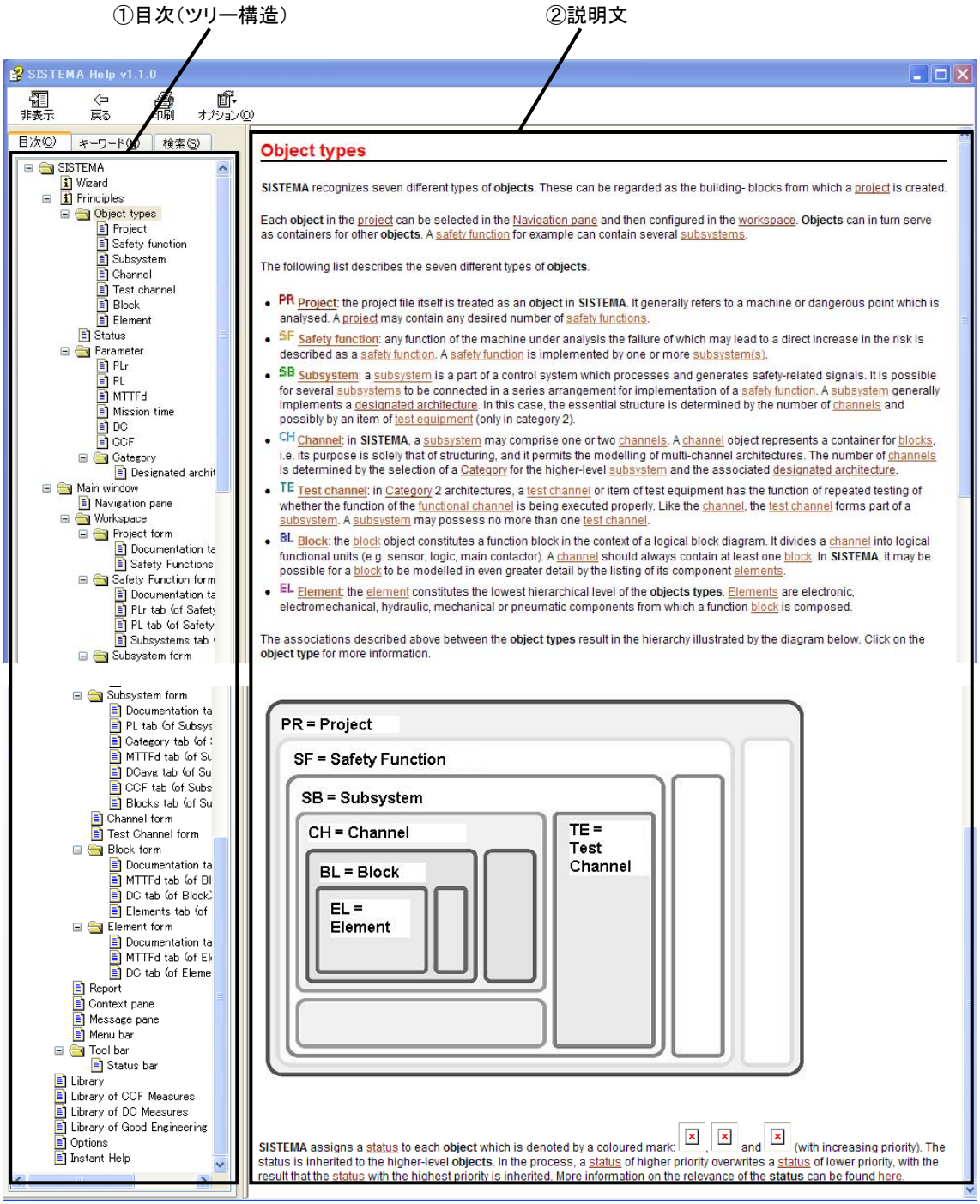
(2)Report 作成の説明

ツールバーの Report 表示のボタンをクリックすると、レポートが作成できます。
このレポートは、プリント出力することができます。



(3)Help 表示の説明

ツールバーの Help 表示のボタンをクリックすると、各機能、用語、記号などの説明を見ることができます。



① 目次（ツリー構造）

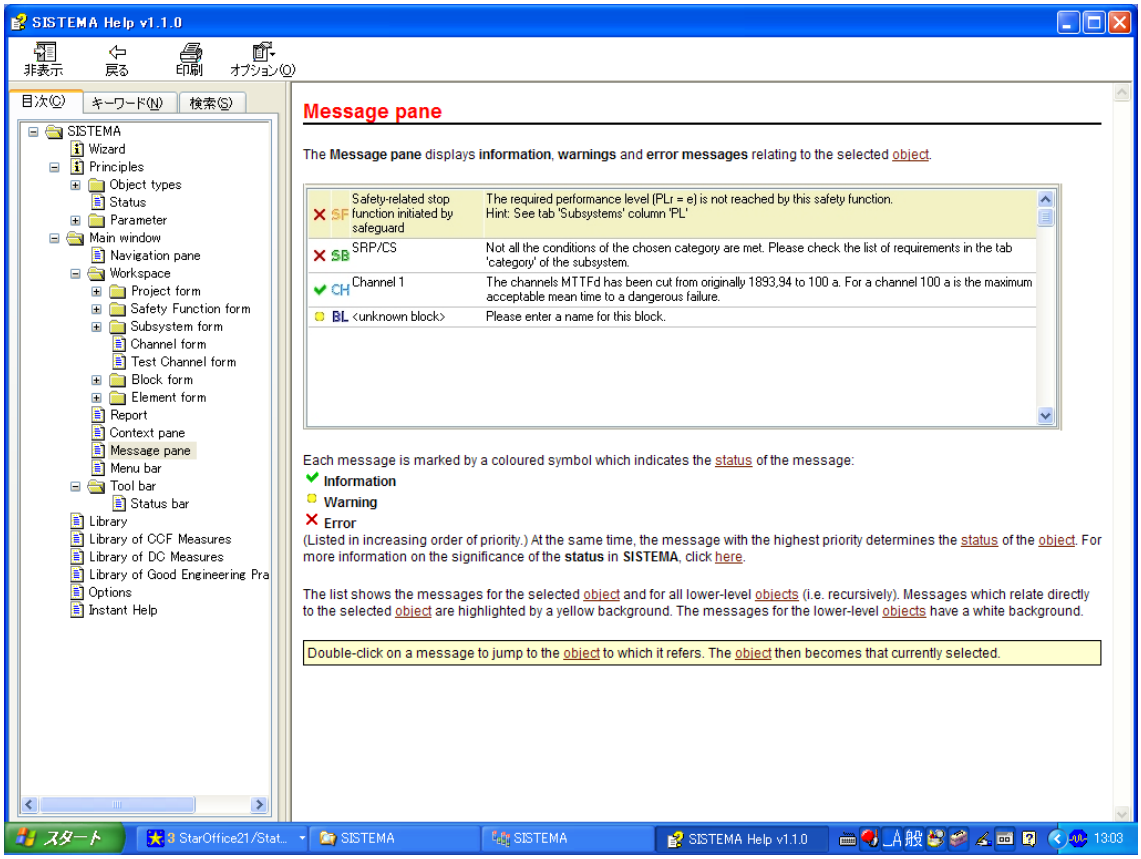
目次がツリー構造で表示されます。項目をクリックすると、その説明が表示されます。

② 説明文

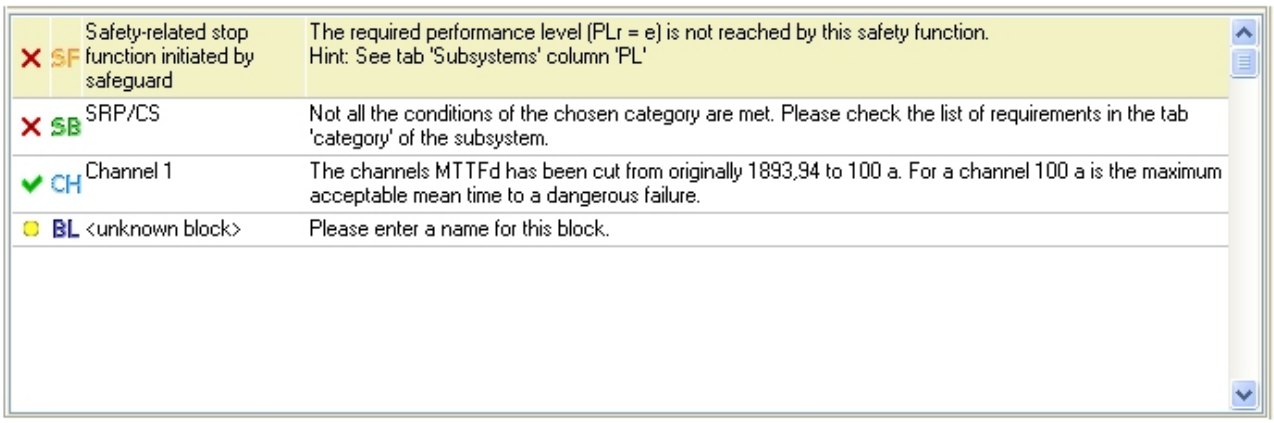
各機能、用語、記号などの詳細な内容説明が分かりやすく表示されます。

また、説明文内の各機能、用語、記号などアンダラインのある単語をクリックすると、さらに、その単語の説明文を表示します。

2.3.5 メッセージパネル（Massage pane）の説明



(1)警告、エラーメッセージ表示の説明



SISTEMA は 3 つのステータス（Status（状態））で、判断し表示します。

Information	・緑色は、オブジェクトが警告、誤り、矛盾、または満たされていない状態もないことを意味しています。但し、メッセージパネル内のあらゆる情報を確認してください。
Warning	・黄色は、オブジェクトに対し、少なくとも 1 つの警告が発行されたことを意味します。メッセージパネル内の説明文を確認してください。
Error	・赤色は、オブジェクトに対し、少なくとも 1 つの誤り、矛盾、または満たされていない状態を含んでいることを意味します。メッセージパネル内の説明文を確認してください。

構成が完成した時、プロジェクトの状態が赤色でないこと確認してください。 プロジェクトの状態が黄色や赤色であるなら、どのような警告かメッセージか、その内容を確認してください。

(2)警告、エラーメッセージ表示（Help 表示内のサンプル）の翻訳

SISTEMA はメッセージパネル内に警告、エラーメッセージ内容を表示します。
例として、Help 表示内のサンプルを翻訳します。

① SF(Safety-related stop function initiated by safeguard)
SF（安全ガードによる安全関連停止機能）
The required performance level(PLr=e) is not reached by this safety function.
Hint : See tab ‘Subsystem’ column ‘PL’
要求されたパフォーマンスレベル(PLr=e)は、このセーフティフンクションで達成されていない。
ヒント：“サブシステム”タブ内の‘PL’欄を見なさい。

② SB(SRP/CS)
Not all the conditions of the chosen category are met.
Please check the list of requirements in the tab ‘category’ of the subsystem.
選択されたカテゴリの全ての状態が合致していません。
サブシステムの‘カテゴリ’タブ内の要求事項のリストを確認しなさい。

③ CH(Channel1)

CH(チェンネル１)

The channels MTTFd has been cut from originally 1893,94 to 100 a.

For a channel 100 a is the maximum acceptable mean time to a dangerous failure.

チャンネルの MTTFd は、オリジナルの 1893,94 年から 100 年にカットされなければならない。

チャンネルの 100 年は、危険側故障の最大容認平均時間です。

④ BL (unknown block)

BL (未確認のブロック)

Please enter a name for this block.

このブロックのための名前を入力しなさい。

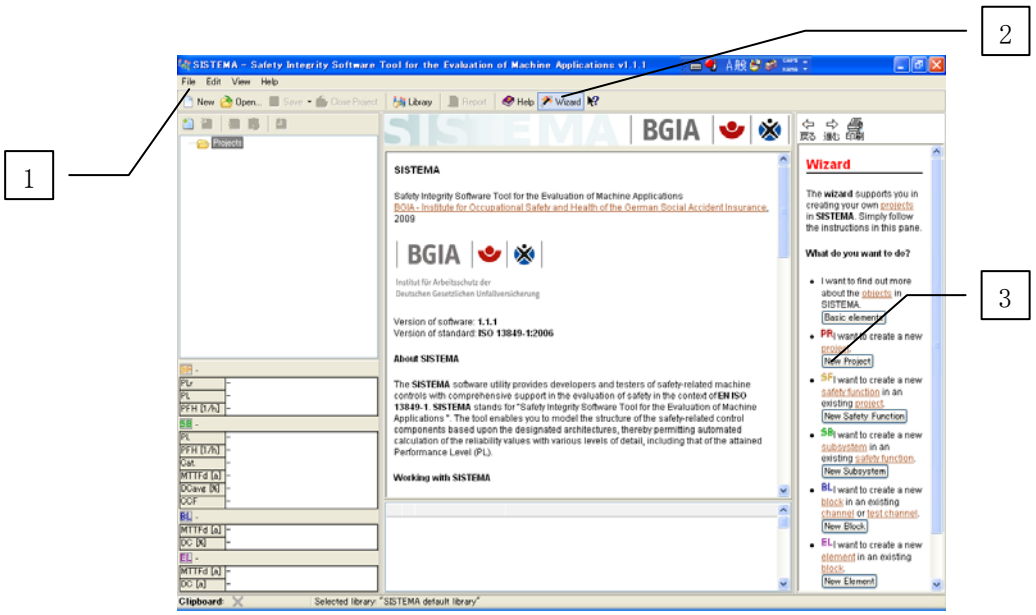
2.4 SISTEMA の回路例による操作説明

本章では、BGIA Report 02-2008e に記載してある回路例の 5、9、17 の 3 つの回路によるパフォーマンス・レベル(PL)を SISTEMA で計算するための入力方法の概要を説明する。

2.4.1 回路例 5:可動式ガードの位置監視-カテゴリ 1(PL=c)

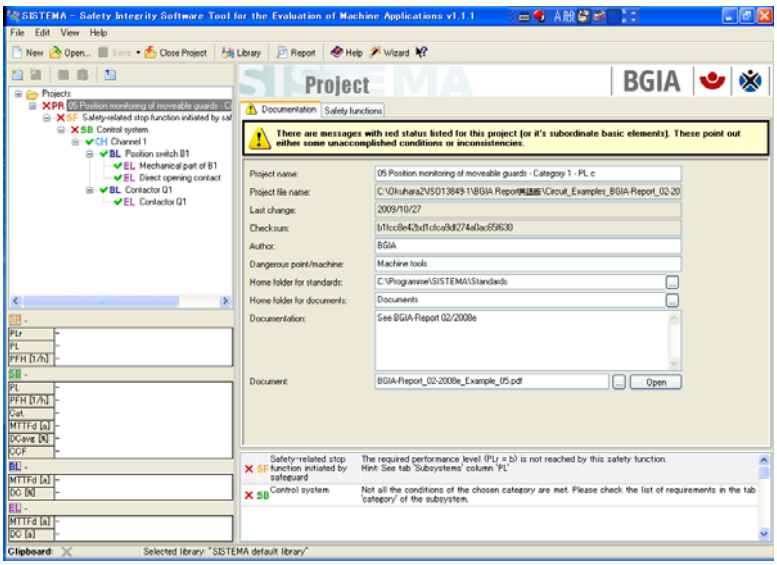
(1)プロジェクト(Project)

1)プロジェクトの作成



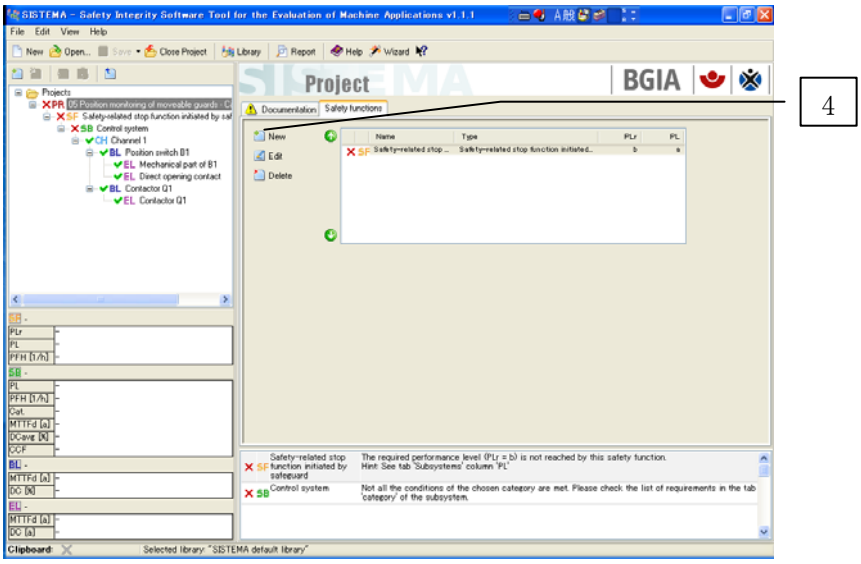
初めて SISTEMA を起動しますと、上記の画面が表示される。この画面から、各種データの作成を行う。まずは、プロジェクト(Project)を作成する。プロジェクトは、メニューバーの 1 ファイル(File)の新規(New)から作成する。又は、ツールバーの 2 ウィザード(Wizard)を開いて、 3 ニュー・プロジェクト(New Project)から作成する。

2)プロジェクトのドキュメントデータの入力



プロジェクトを作成すると上記の画面が表示される。この画面の Project name, Author, Dangerous point/machine, Documentation の項目に必要事項を入力する。なお、各フォルダ(folder)の設定は、デフォルトのままとするが必要があれば変更する。

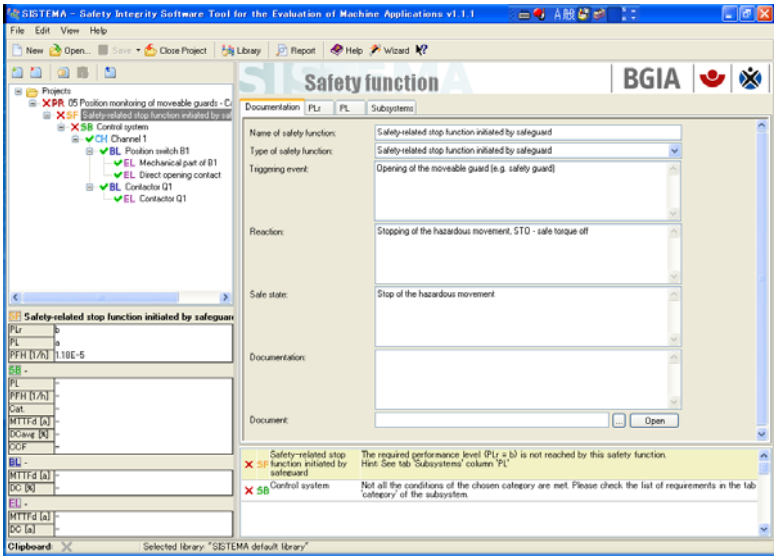
3)セーフティ･ファンクションの作成



プロジェクトにセーフティ･ファンクション(Safety function)の項目を作成する場合、上記画面を開いて、4 新規(New)をクリックする。もし、セーフティ･ファンクションが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

(2)セーフティ･ファンクション(Safety function)

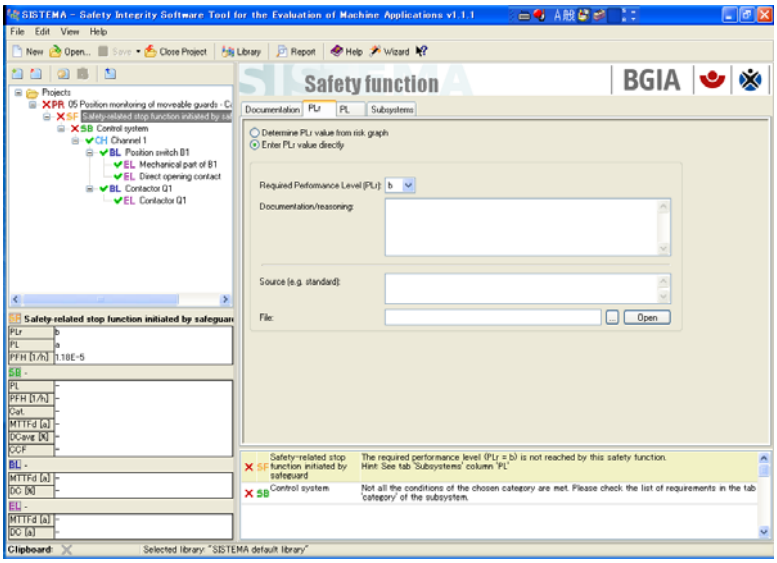
1)セーフティ･ファンクションのドキュメントデータの入力



セーフティ･ファンクションを作成すると上記の画面が表示される。この画面の Name of safety function, Triggering event, Reaction, Safe state, Documentation の項目に必要事項を入力する。Type of safety function は、必要なタイプを選択する。

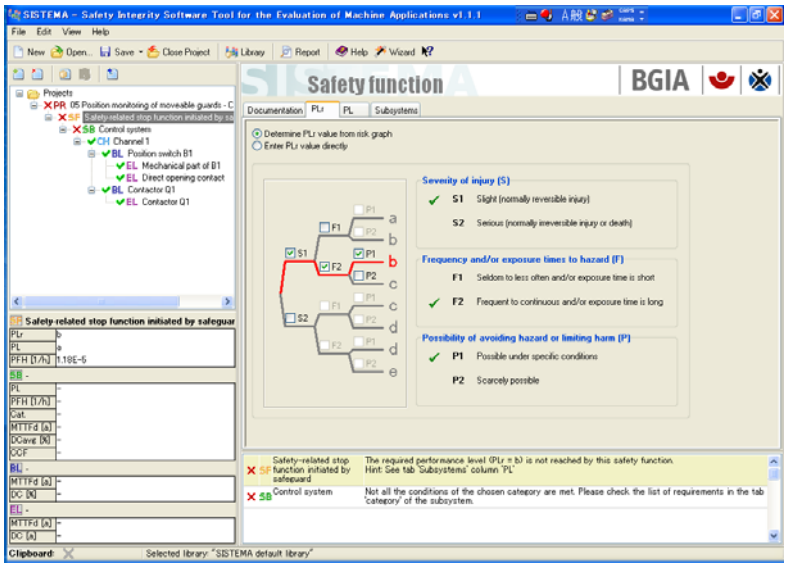
2)要求パフォーマンス･レベルの入力

①直接入力



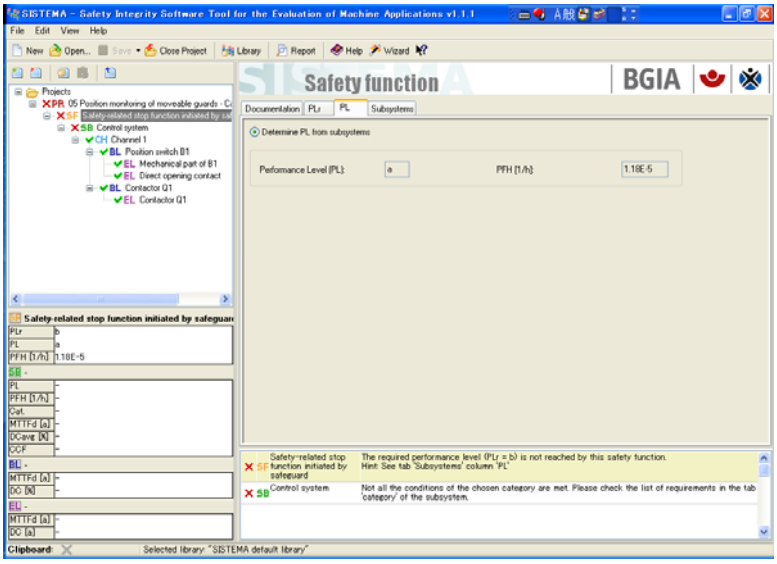
このセーフティ･ファンクションの要求パフォーマンス･レベル(PLr)を入力する方法は、2 つある。ひとつは、上記画面のように直接 PLr を入力する方法である。このとき、要求パフォーマンス・レベルを選定した理由や情報源について記載する。(Documentation/reasoning, Source へ記入)

②リスクグラフによる選択入力



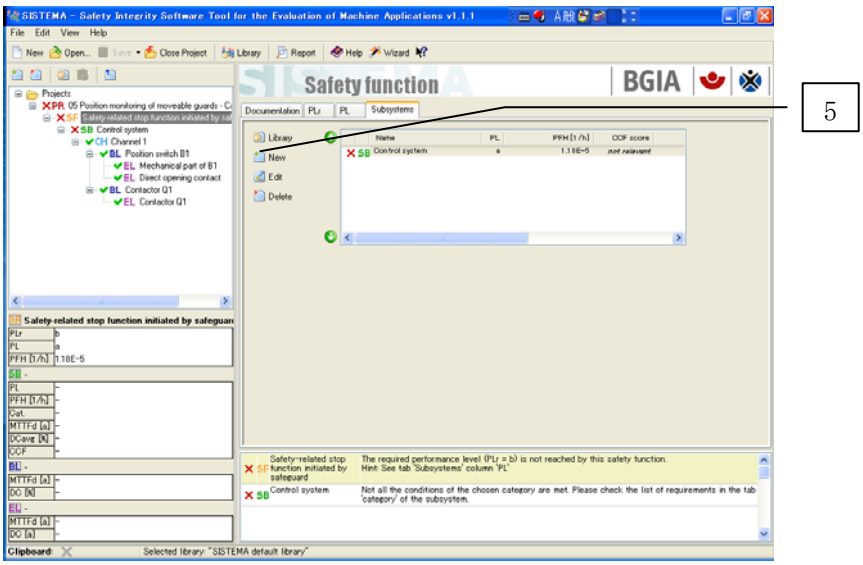
もうひとつは、要求パフォーマンス・レベルを上記画面のリスクグラフ(risk graph)から求める方法である。要求パフォーマンス・レベルは、どちらかの方法で入力する。

3)パフォーマンス・レベルの判定結果



この画面は、下位にあるサブシステム(subsystem)から計算されたパフォーマンス・レベルと PFH(1/h)が表示される。

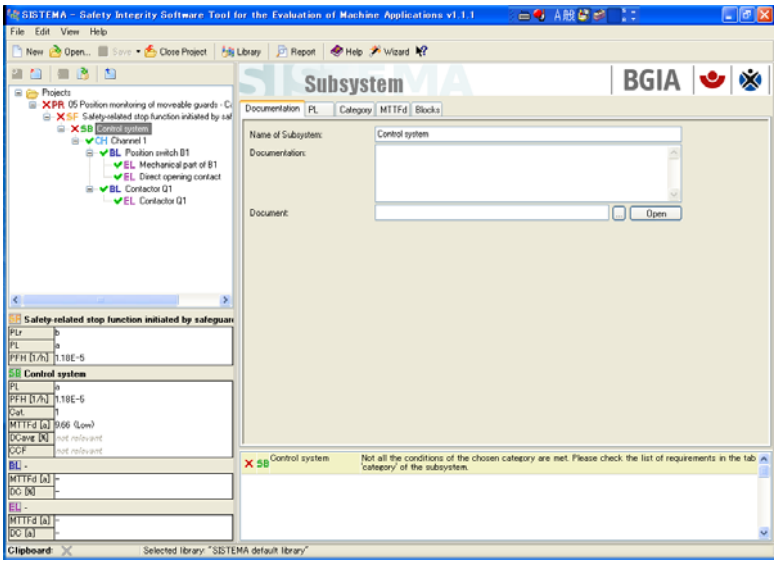
4)サブシステムの作成



セーフティ・ファンクションにサブシステム(Subsystem)の項目を作成する場合、上記画面を開いて、5 新規(New)をクリックする。もし、サブシステムが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

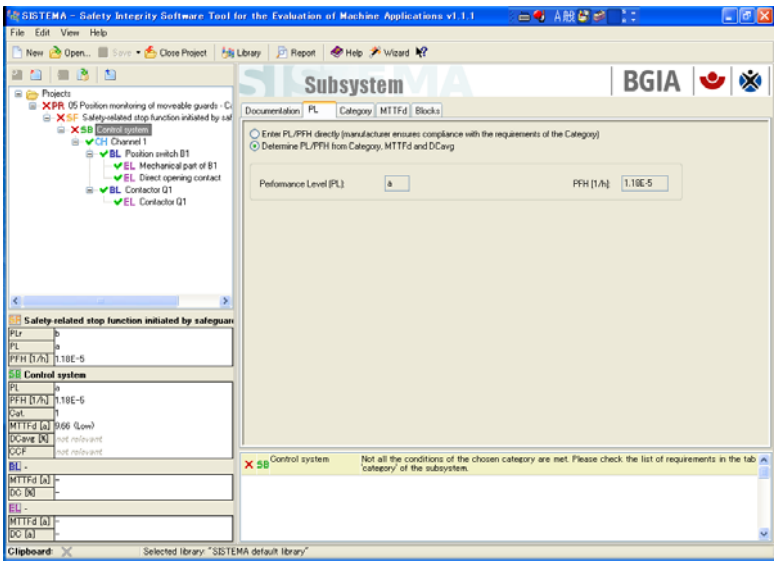
(3)サブシステム(Subsystem)

1)サブシステムのドキュメントデータの入力



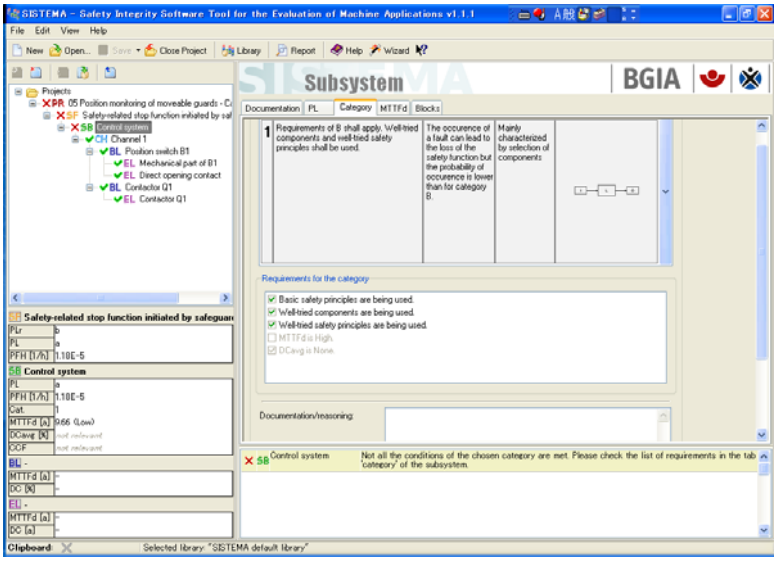
サブシステムを作成すると上記の画面が表示される。この画面の Name of Subsystem, Documentation の項目に必要事項を入力する。

2)パフォーマンス･レベル(PL)の入力、又は表示



サブシステムのパフォーマンス･レベルは、上記画面を開いて選択する。入力は、直接入力する方法とサブシステムのカテゴリ、MTTFd と DCavg より求める方法の 2 つがある。通常は、後者の方法を選択する。

3)カテゴリの選択

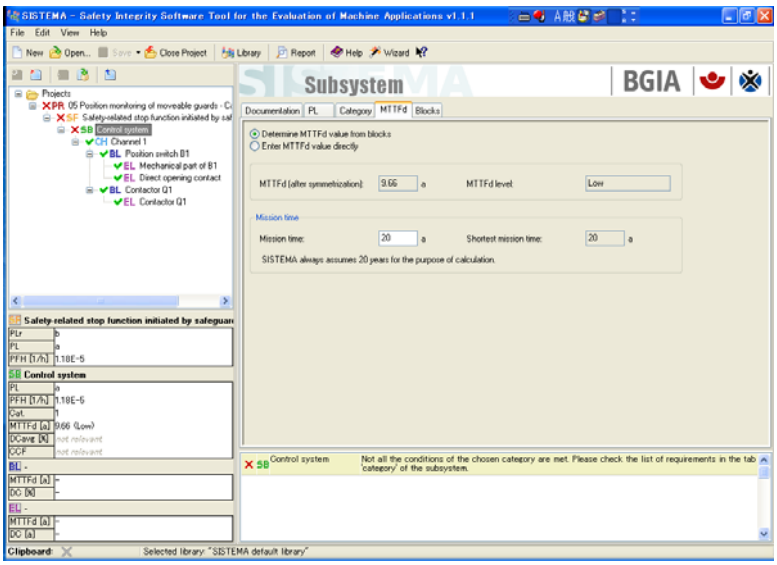


サブシステムのカテゴリ(B、1、2、3、4)を選択する場合は、上記画面を開いて選択する。要求パフォーマンス･レベルにあったカテゴリを選択し、各カテゴリ要求(Requirements for the category)を満足しているかチェックをする。必要な場合、Documentation/reasoning に記入する。カテゴリを選択すると、カテゴリに応じたチャンネルが作成される。

また、カテゴリ B や 1 では、システム内には診断範囲はなく(DCavg=0%)、そのような構造(単一チャンネルシステム)においては、共通原因故障(CCF)の考慮が不要となる。

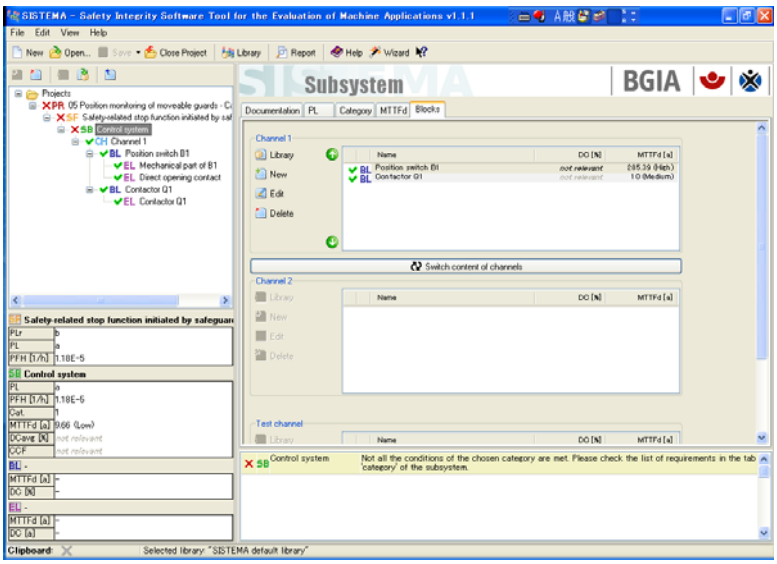
そのため SISTEMA では、カテゴリ B や 1 を選択すると DCavg と CCF の入力項目が表示されなくなる。

4)危険側故障までの平均時間(MTTFd)の入力、又は表示



サブシステムの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とブロック(block)の MTTFd より求める方法の 2 つがある。通常は、後者の方法を選択する。

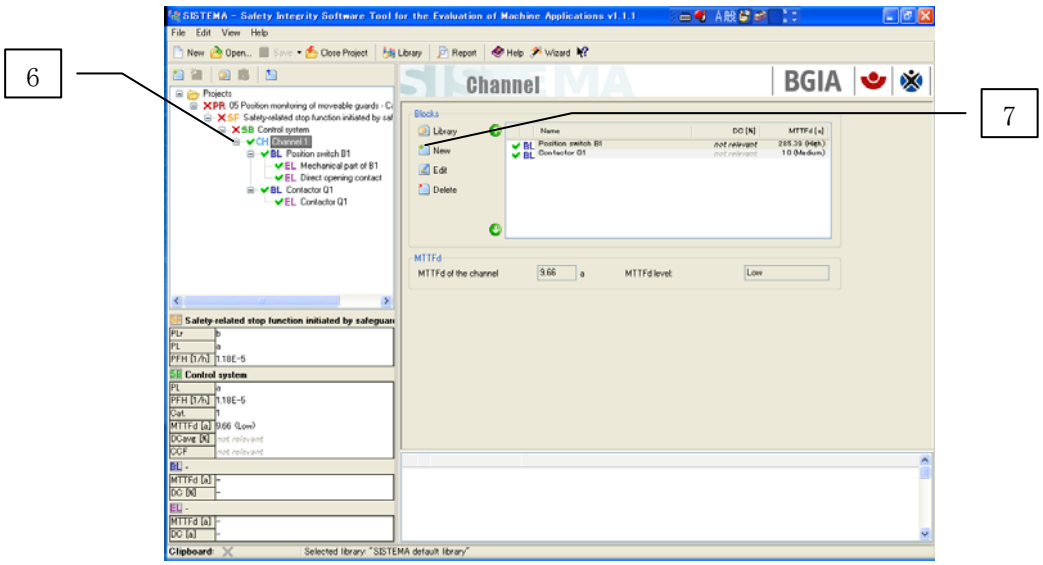
5)サブシステムからのブロックの作成



サブシステムにブロック(Block)の項目を作成する場合、上記画面を開いて、新規(New)をクリックする。もし、ブロックが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

6)チャンネルからのブロックの作成

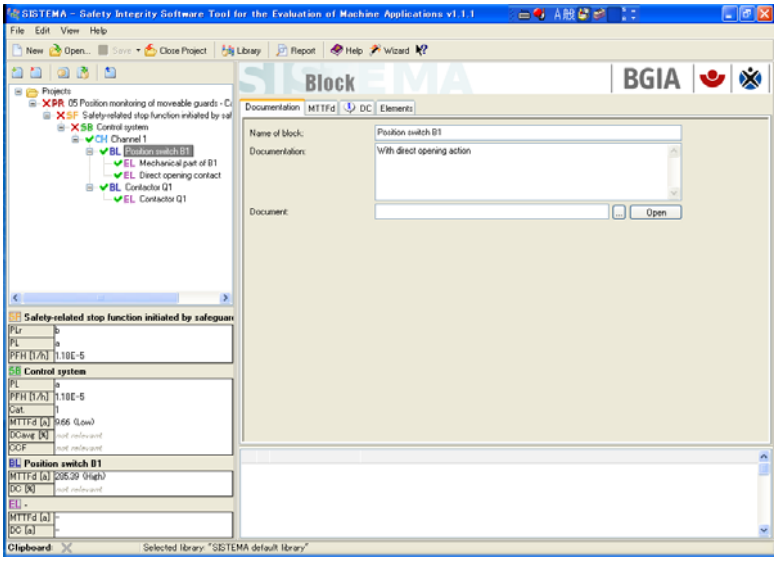
チャンネル(Channel)は、サブシステムで選択したカテゴリにより、チャンネル 1(CH1)、チャンネル 2(CH2)、テストチャンネル(TE)が作成される。



又は、左側のディレクトリの 6 チャンネル(Channel)から上記画面を開いて、7 新規(New)をクリックし、ブロック(Block)の項目を作成する。もし、ブロックが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

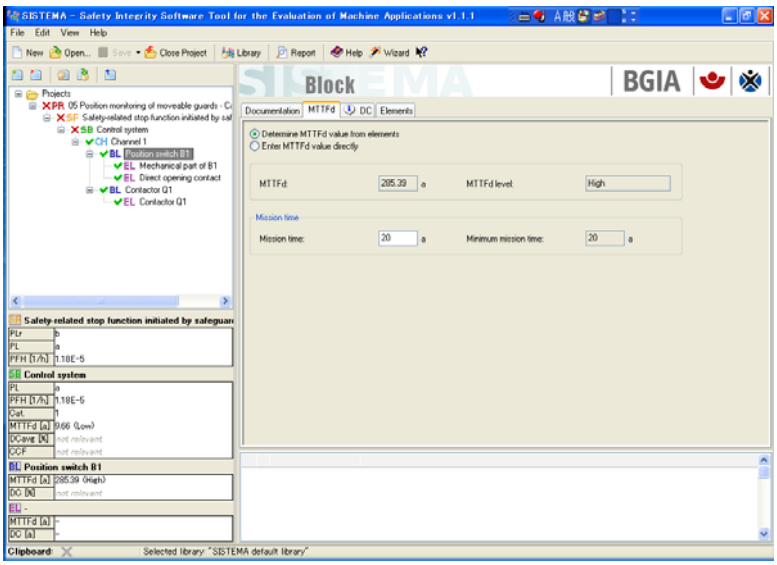
(4)ブロック(Block)

1)ブロックのドキュメントデータの入力



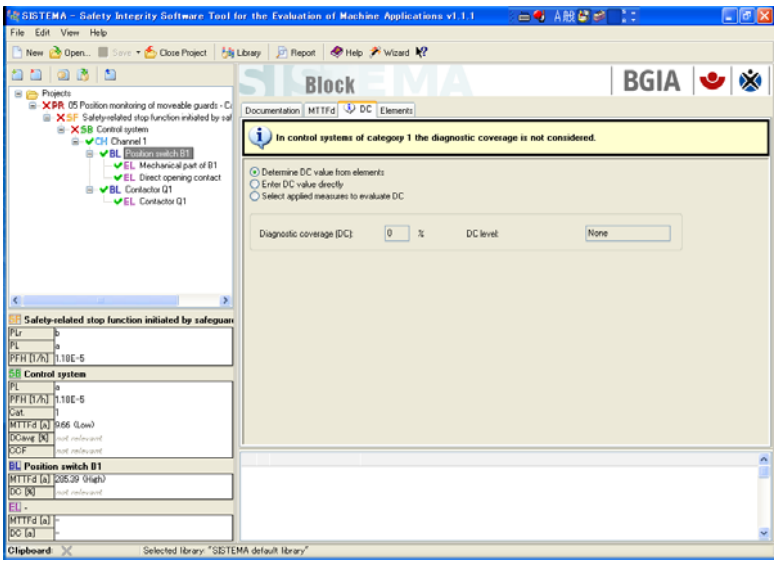
ブロックを作成すると上記の画面が表示される。この画面の Name of block, Documentation の項目に必要事項を入力する。

2)危険側故障までの平均時間(MTTFd)の入力、又は表示



ブロックの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とエレメント(element)の MTTFd より求める方法の 2 つがある。通常は、後者の方法を選択する。

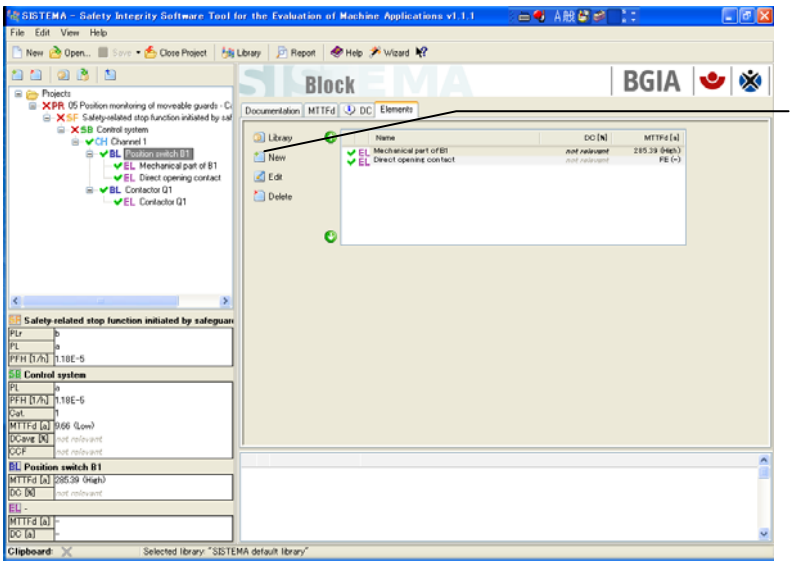
3)診断範囲(DC)の入力



ブロックの DC の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法、エレメント(element)の DC より求める方法、ISO 13849-1 の付属書 E の表 E1 から選択する方法の 3 つがある。表 E1 からの選択方法は、上記画面で“Select applied measures to evaluate DC”を選択する。これを選択すると画面が変更される。表示された画面の下側に“Library”の表示がありますので、そこを押すと表 E1 がポップアップされる。表示された表 E1 の項目を選択し、“Load Selection”を押すと DC の値が入力される。

なお、本回路例では、カテゴリが 1 のため DC の入力は不要である。

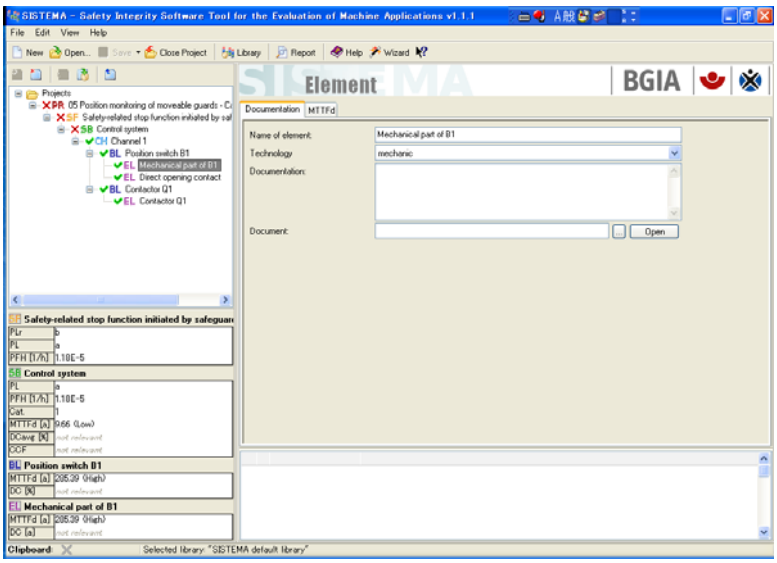
4)ブロックからのエレメントの作成



ブロックにエレメント(Element)の項目を作成する場合、上記画面を開いて、8 新規(New)をクリックする。もし、エレメントが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

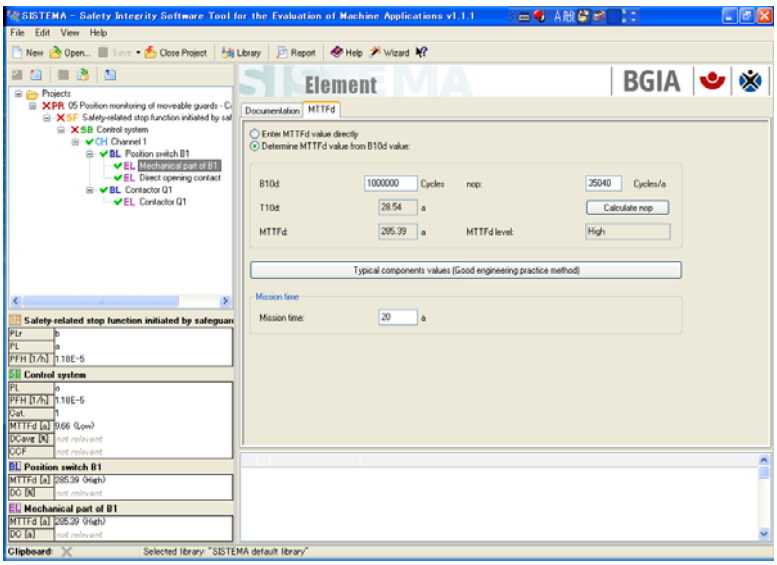
(5)エレメント(Element)

1)エレメントのドキュメントデータの入力



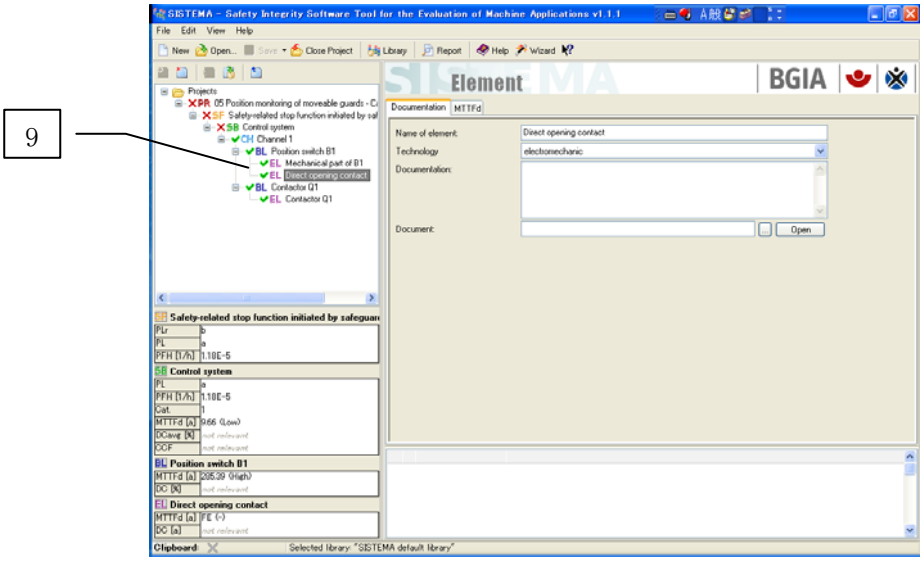
エレメントを作成すると上記の画面が表示される。この画面の Name of element, Documentation の項目に必要事項を入力する。

2)危険側故障までの平均時間(MTTFd)の入力



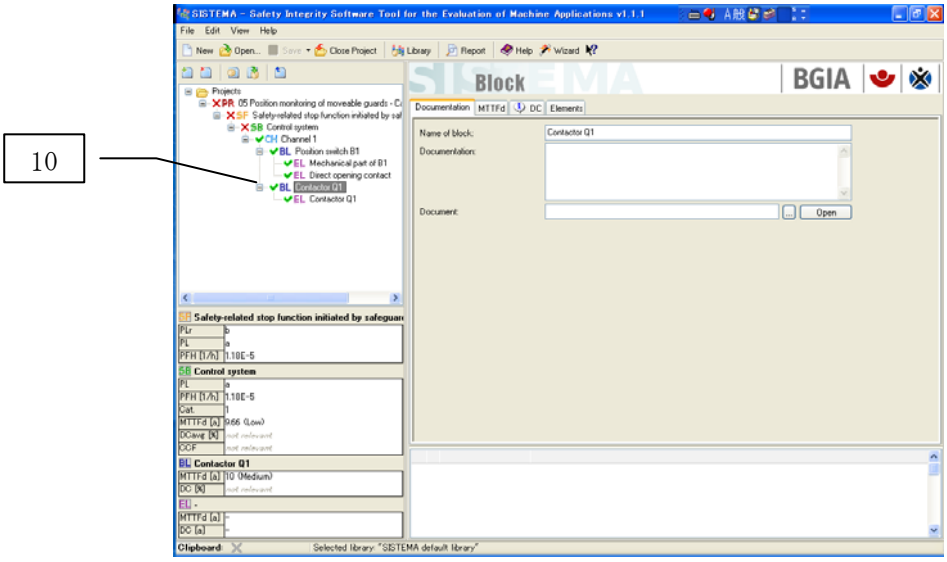
エレメントの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法と B10d と nop の値から MTTFd より求める方法の 2 つがある。 B10d と nop の値から MTTFd を計算する場合、B10d と nop の値を直接入力する仕方と ISO 13849-1 の附属書 C の表 C1 から MTTFd や B10d を選択する仕方がある。表 C1 から選択する仕方は、上記画面の“Typical components values (Good engineering practice method)”を押す。押すと表 C1 が表示されるので、該当する項目を選択し、OK を押す。OK を押したら、選択した MTTFd や B10d が入力される。

3)追加されたエレメントの選択



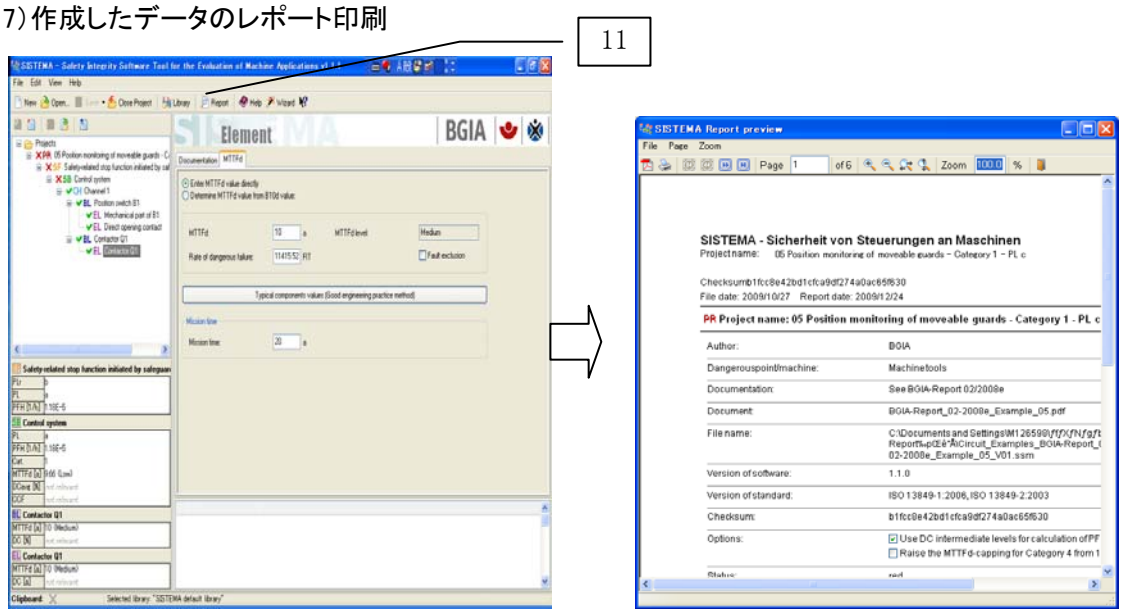
ブロックで追加されたエレメントの選択は､左側のディレクトリの 9 該当項目をクリックすることにより、上記画面が表示される。表示されたら、前で記載した内容と同様に必要なデータを入力する。

(6)追加されたブロックの選択



サブシステムで追加されたブロックの選択は、左側のディレクトリの10該当項目をクリックすることにより、上記画面が表示される。表示されたら、前で記載した内容と同様に必要なデータを入力する。このブロックの下位にあるエレメントも前で記載した内容と同様に必要なデータを入力する。

(7)作成したデータのレポート印刷



このようにして、各項目の必要なデータを入力することにより、パフォーマンス・レベル(PL)や PFH(1/h)が計算され、要求パフォーマンス・レベルと同等になっているか自動的に計算される。計算された結果の印刷は、ツールバーの11レポート(Report)から行う。レポートを押すとプレビュー画面が開くので、左上のファイル(File)から印刷(Print)を選択して印刷する。また、ファイル(File)から“Save As”を選択すると PDF ファイルの保存ができる。しかし、“Save AS”で保存した PDF ファイルが開かない場合がある。その場合は、ファイル(File)で印刷を選択して、印刷する場合のプリンタ設定で PDF 作成や TIF 作成を行う。

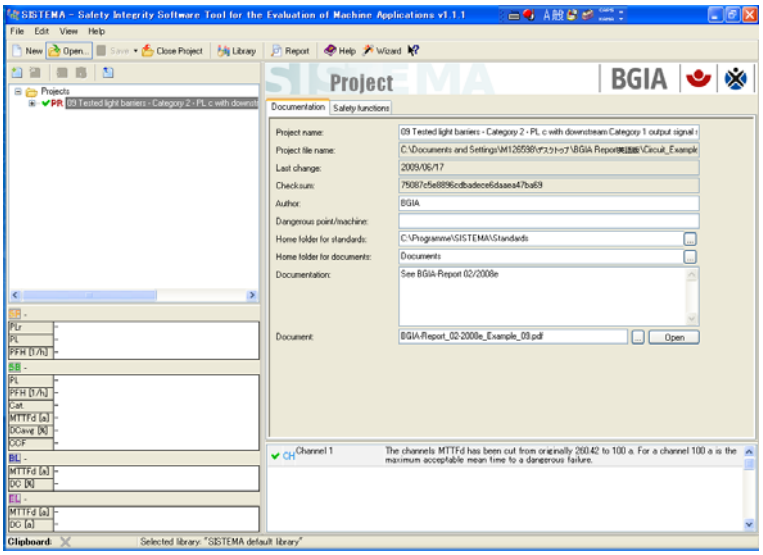
2.4.2 回路例 9：試験済み光バリア−カテゴリ 2− PL=c

(1)プロジェクト(Project)

1)プロジェクトの作成

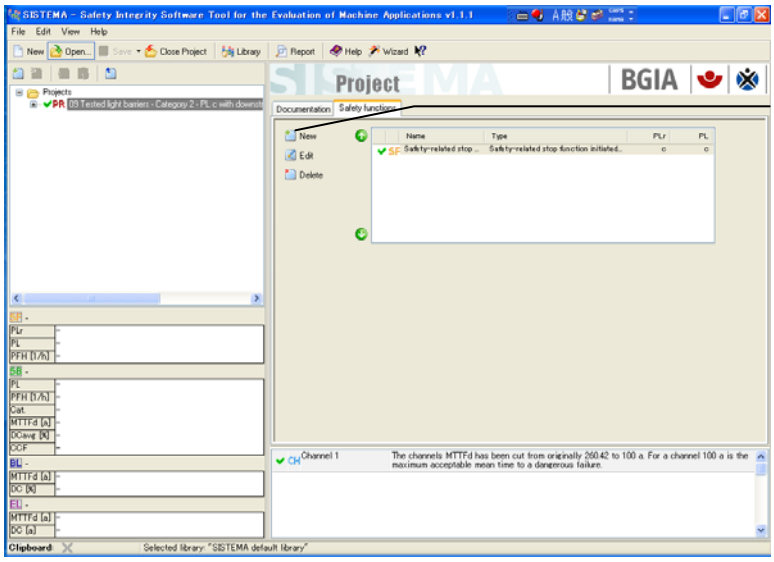
初めて SISTEMA を起動すると、上記の画面が表示される。この画面から、各種データの作成を行う。まずは、プロジェクト(Project)を作成する。プロジェクトは、メニューバーの 1 ファイル(File)の新規(New)から作成する。又は、ツールバーの 2 ウィザード(Wizard)を開いて、 3 ニュー・プロジェクト(New Project)から作成する。

2)プロジェクトのドキュメントデータの入力



プロジェクトを作成すると上記の画面が表示される。この画面の Project name, Author, Dangerous point/machine, Documentation の項目に必要事項を入力する。なお、各フォルダ(folder)の設定は、デフォルトのままとするが必要があれば変更する。

3)セーフティ･ファンクションの作成

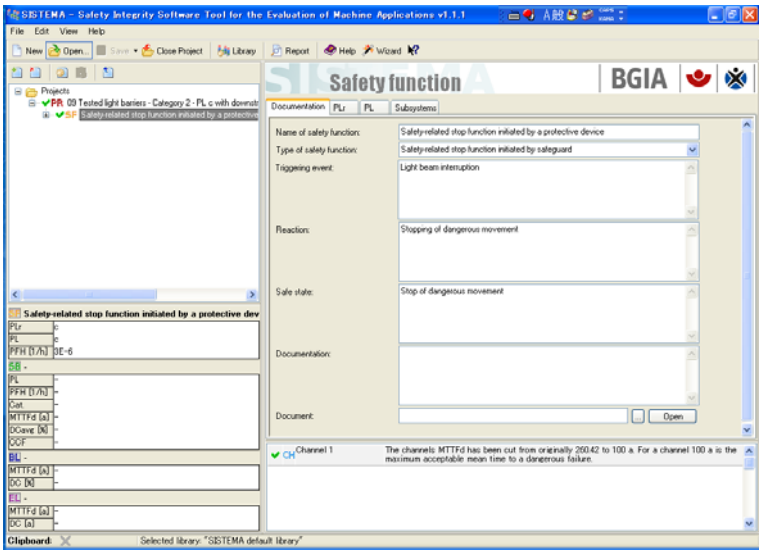


4

プロジェクトにセーフティ･ファンクション(Safety function)の項目を作成する場合、上記画面を開いて、4 新規(New)をクリックする。もし、セーフティ･ファンクションが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

(2)セーフティ･ファンクション(Safety function)

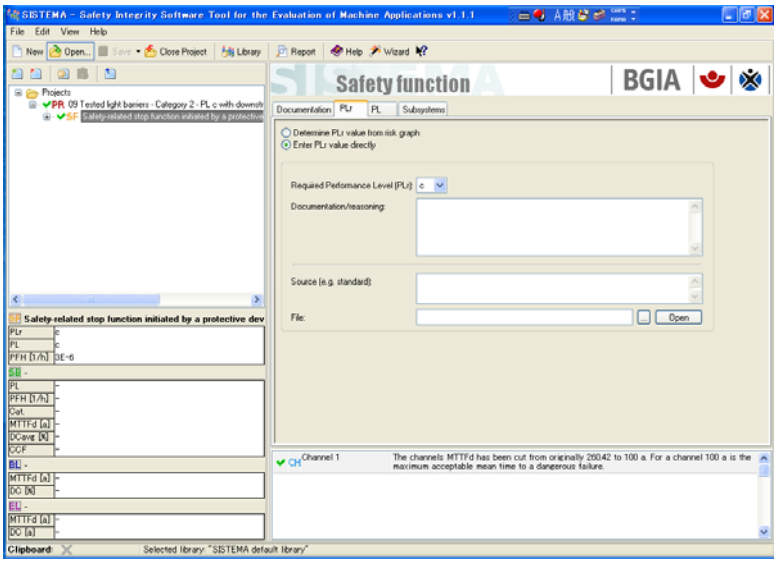
1)セーフティ･ファンクションのドキュメントデータの入力



セーフティ･ファンクションを作成すると上記の画面が表示される。この画面の Name of safety function, Triggering event, Reaction, Safe state, Documentation の項目に必要事項を入力する。Type of safety function は、必要なタイプを選択する。

2)要求パフォーマンス･レベルの入力

①直接入力

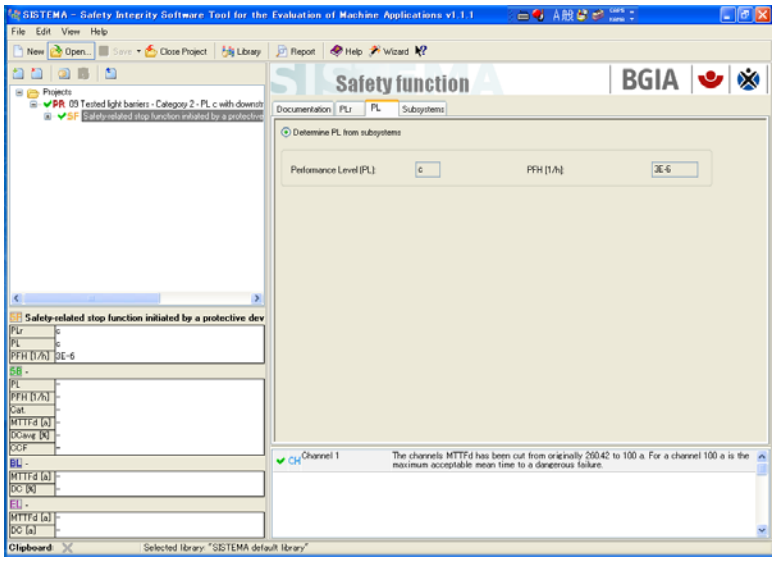


このセーフティ･ファンクションの要求パフォーマンス･レベル(PLr)を入力する方法は、2 つある。ひとつは、上記画面のように直接 PLr を入力する方法である。このとき、要求パフォーマンス・レベルを選定した理由や情報源について記載する。(Documentation/reasoning, Source へ記入)

②リスクグラフによる選択入力

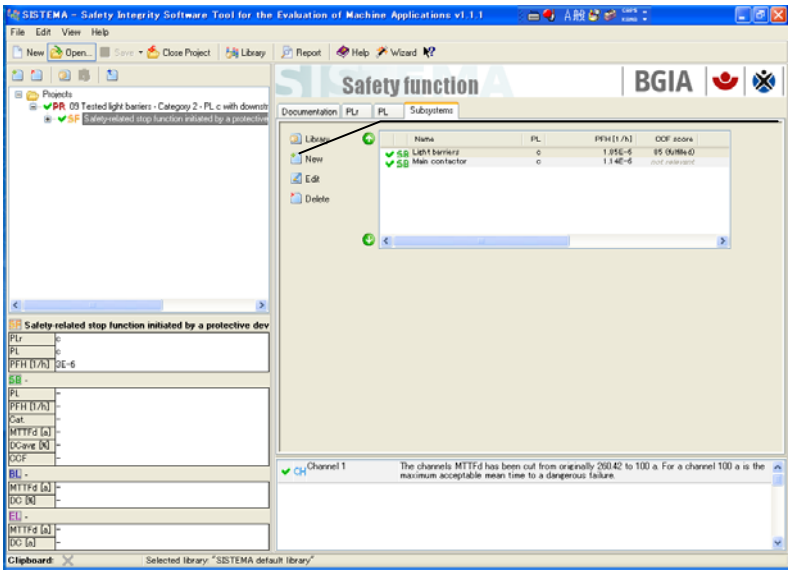
もうひとつは、要求パフォーマンス･レベルをリスクグラフ(risk graph)から求める方法である。要求パフォーマンス・レベルはどちらかの方法で入力する。

3)パフォーマンス･レベルの判定結果



この画面は、下位にあるサブシステム(subsystem)から計算されたパフォーマンス･レベルと PFH(1/h)が表示される。

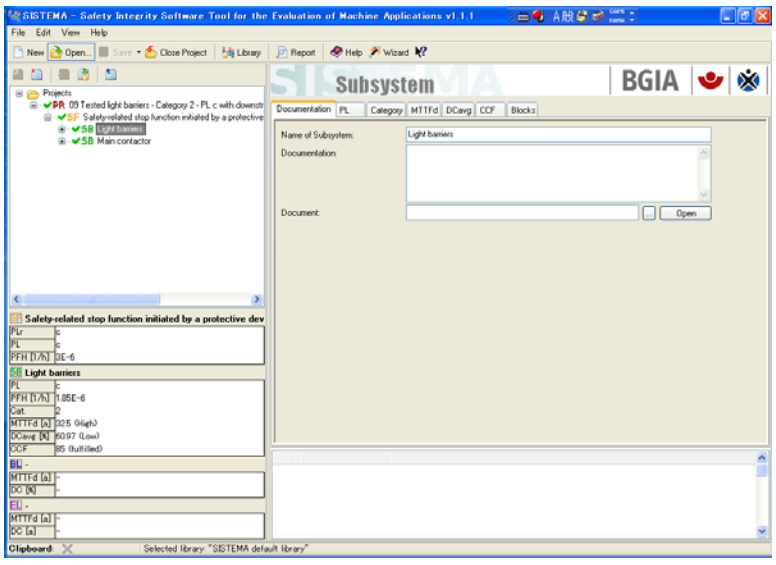
4)サブシステムの作成



セーフティ・ファンクションにサブシステム(Subsystem)の項目を作成する場合、上記画面を開いて、5 新規(New)をクリックする。もし、サブシステムが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

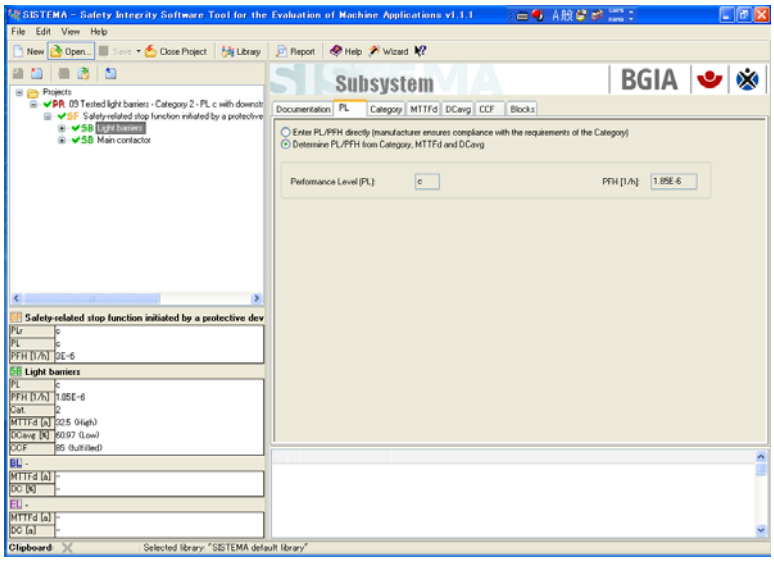
(3)サブシステム(Subsystem)

1)サブシステムのドキュメントデータの入力



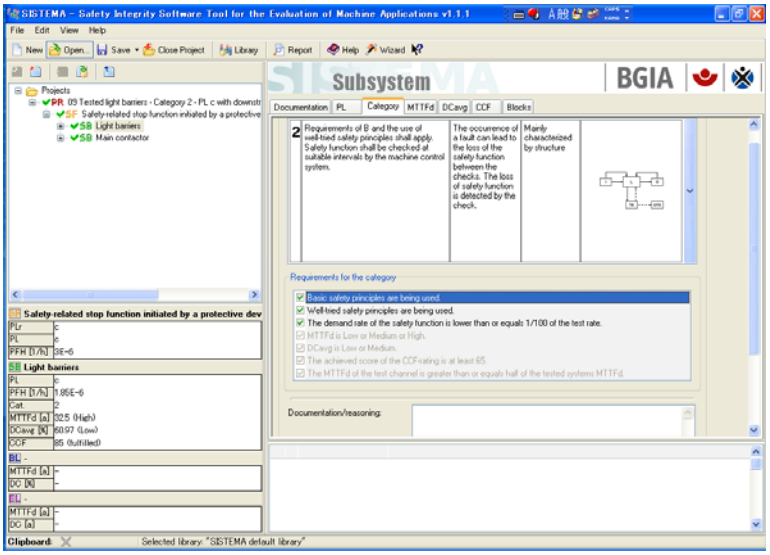
サブシステムを作成すると上記の画面が表示される。この画面の Name of Subsystem, Documentation の項目に必要事項を入力する。

2)パフォーマンス･レベルの入力、又は表示



サブシステムのパフォーマンス･レベルは、上記画面を開いて選択する。入力は、直接入力する方法とサブシステムのカテゴリ、MTTFd と DCavg より求める方法の 2 つがある。通常は、後者の方法を選択する。

3)カテゴリ(Category)の選択



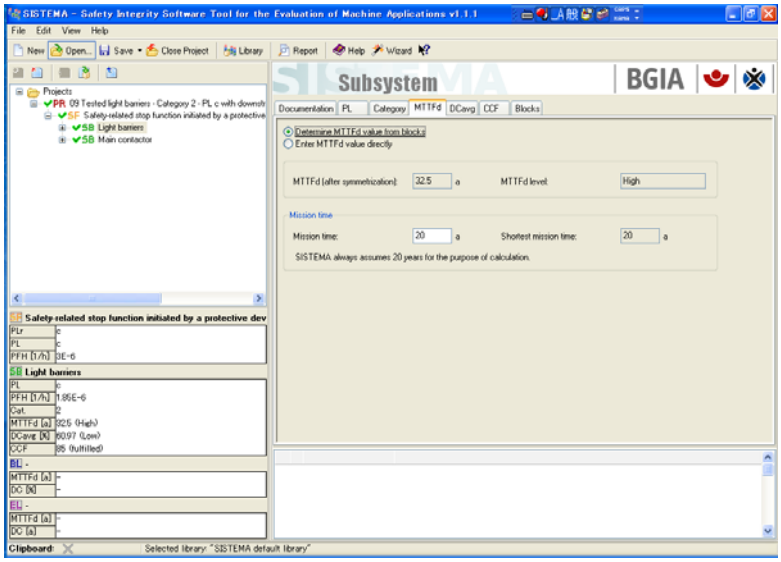
サブシステムのカテゴリ(B、1、2、3、4)を選択する場合は、上記画面を開いて選択する。要求パフォーマンス･レベルにあったカテゴリを選択し、各カテゴリ要求(Requirements for the category)を満足しているかチェックをする。必要な場合、Documentation/reasoning に記入する。カテゴリを選択すると、カテゴリに応じたチャンネルが作成される。

また、カテゴリ B や 1 では、システム内には診断範囲はなく(DCavg=0%)、そのような構造(単一チャンネルシステム)においては、共通原因故障(CCF)の考慮が不要となる。

そのため SISTEMA では、カテゴリ B や 1 を選択すると DCavg と CCF の入力項目が表示されなくなる。

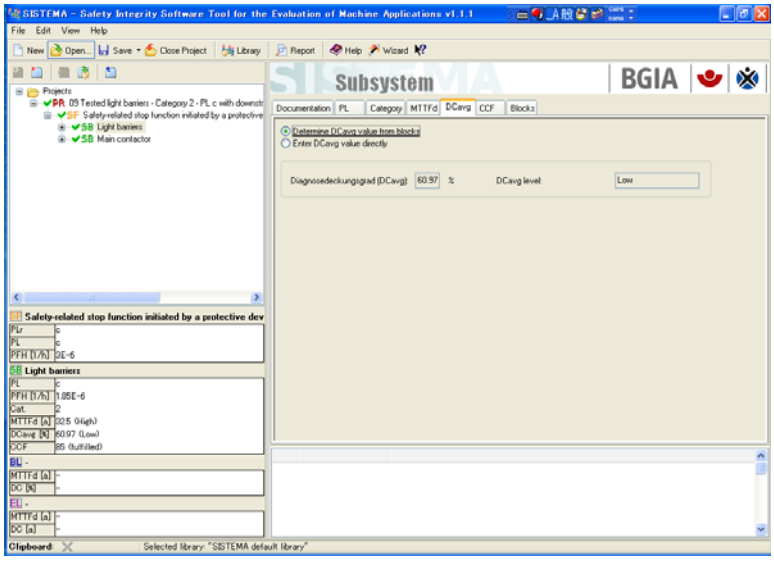
本回路例では、カテゴリ 2 を選択しているのでチャンネル 1 とテストチャンネルが作成される。

4)危険側故障までの平均時間(MTTFd)の入力、又は表示



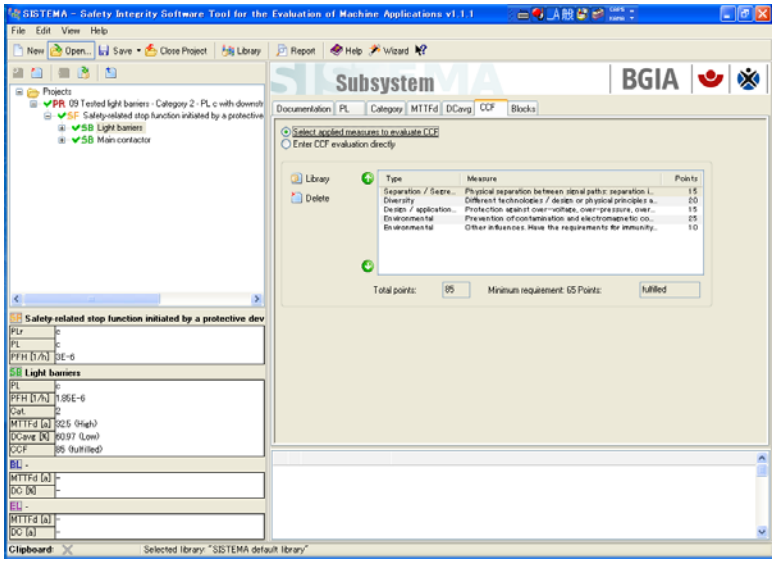
サブシステムの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とブロック(block)の MTTFd より求める方法の 2 つがある。通常は、後者の方法を選択する。

5)平均診断範囲(DCavg)の入力、又は表示



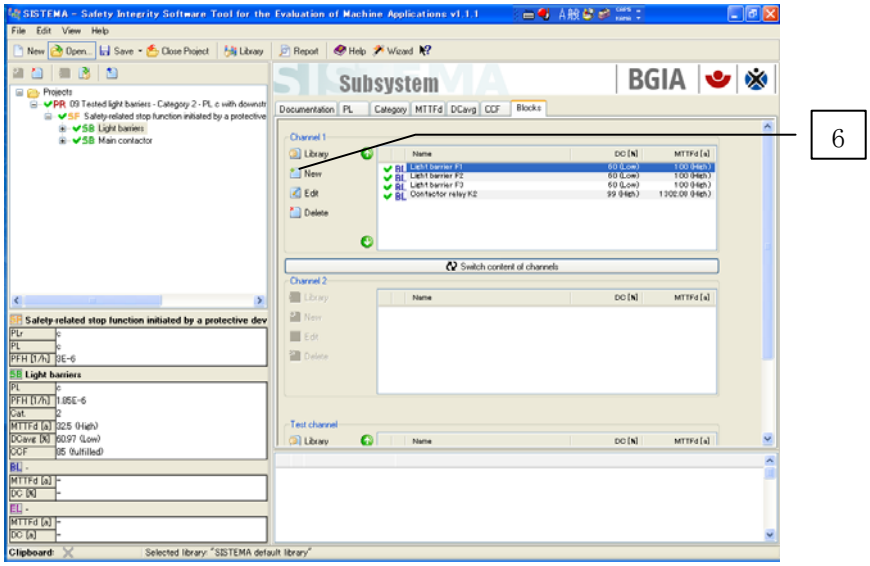
サブシステムの DCavg の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とブロック(block)の DCavg より求める方法の 2 つがある。通常は、後者の方法を選択する。

6)共通原因故障(CCF)の入力



サブシステムの CCF の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法と Library(ISO 13849-1:2006 附属書 F の表 F.1)から項目を選択していく方法の 2 つがある。

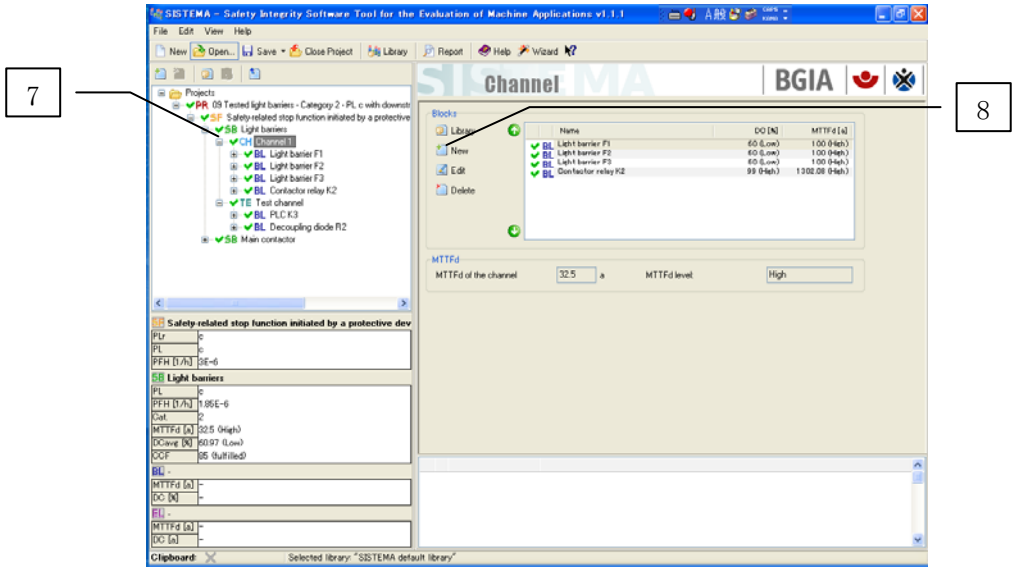
7)サブシステムからのブロックの作成



サブシステムにブロック(Block)の項目を作成する場合、上記画面を開いて、6 新規(New)をクリックする。もし、ブロックが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

8)チャンネルからのブロックの作成

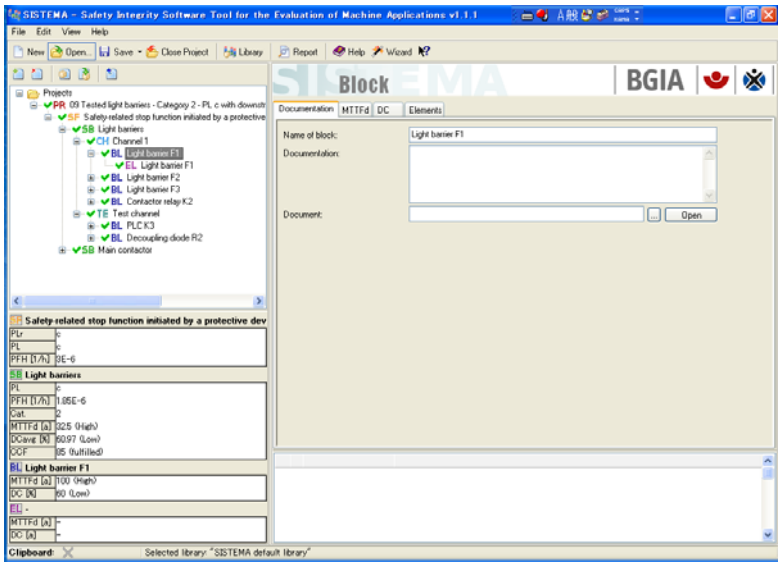
チャンネルは、サブシステムで選択したカテゴリにより、チャンネル 1, チャンネル 2, テストチャンネルが作成される。



又は、左側のディレクトリの 7 チャンネル(Channel)から上記画面を開いて、8 新規(New)をクリックし、ブロック(Block)の項目を作成する。もし、ブロックが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

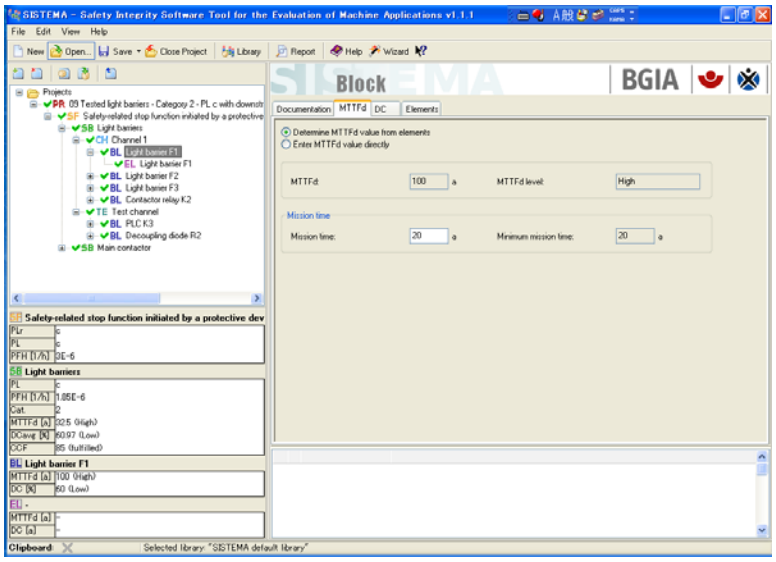
(4)ブロック(Block)

1)ブロックのドキュメントデータの入力



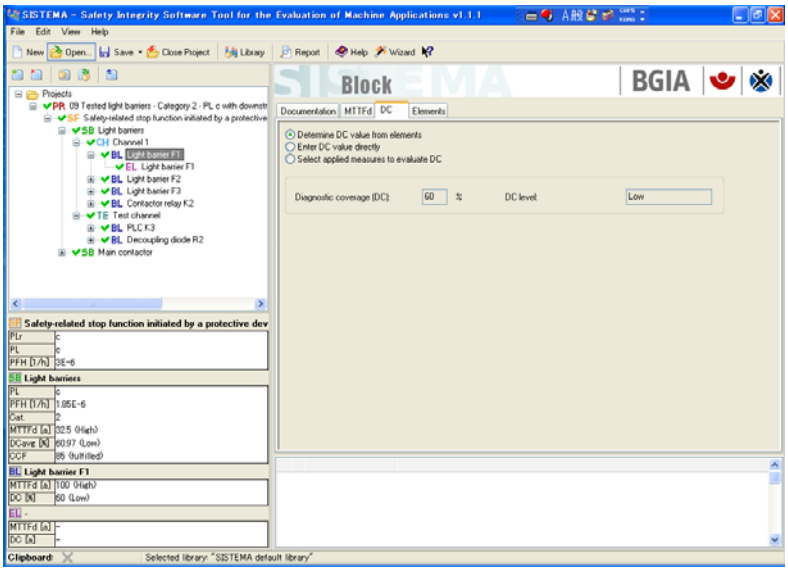
ブロックを作成すると上記の画面が表示される。この画面の Name of block, Documentation の項目に必要事項を入力する。

2)危険側故障までの平均時間(MTTFd)の入力、又は表示



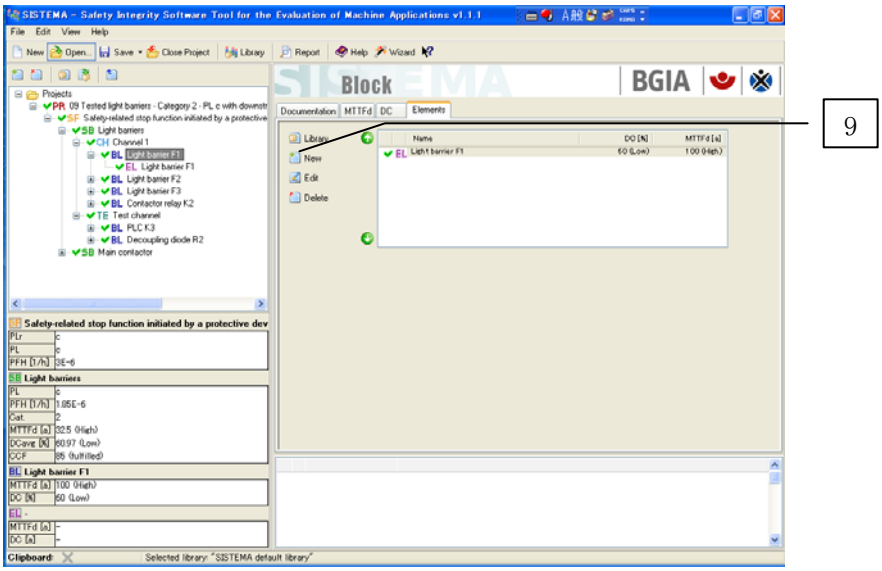
ブロックの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とエレメント(element)の MTTFd より求める方法の 2 つがある。通常は、後者の方法を選択する。

3)診断範囲(DC)の入力、又は表示



ブロックの DC の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法、エレメント(element)の DC より求める方法、ISO 13849-1 の付属書 E の表 E1 から選択する方法の 3 つがある。表 E1 からの選択方法は、上記画面で“Select applied measures to evaluate DC”を選択する。これを選択すると画面が変更される。表示された画面の下側に“Library”の表示があるので、そこを押すと表 E1 がポップアップされる。表示された表 E1 の項目を選択し、“Load Selection”を押すと DC の値が入力される。

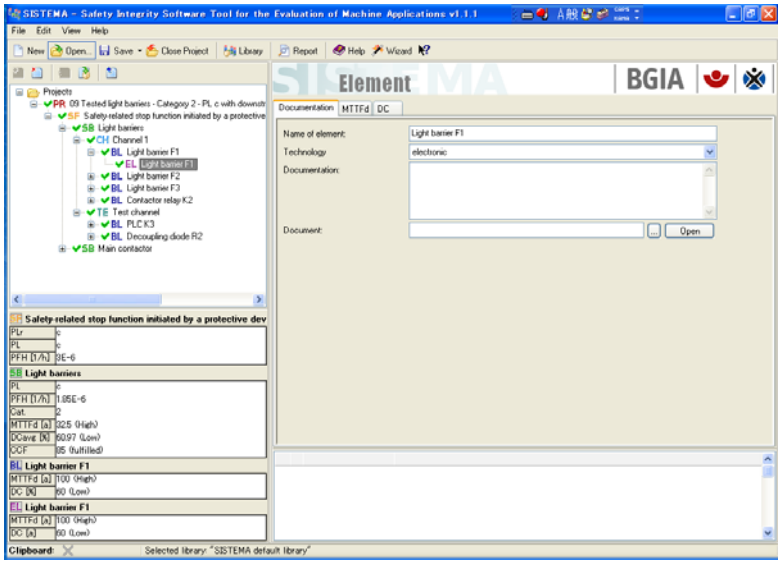
4)ブロックからのエレメントの作成



ブロックにエレメント(Element)の項目を作成する場合、上記画面を開いて、9 新規(New)をクリックする。もし、エレメントが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

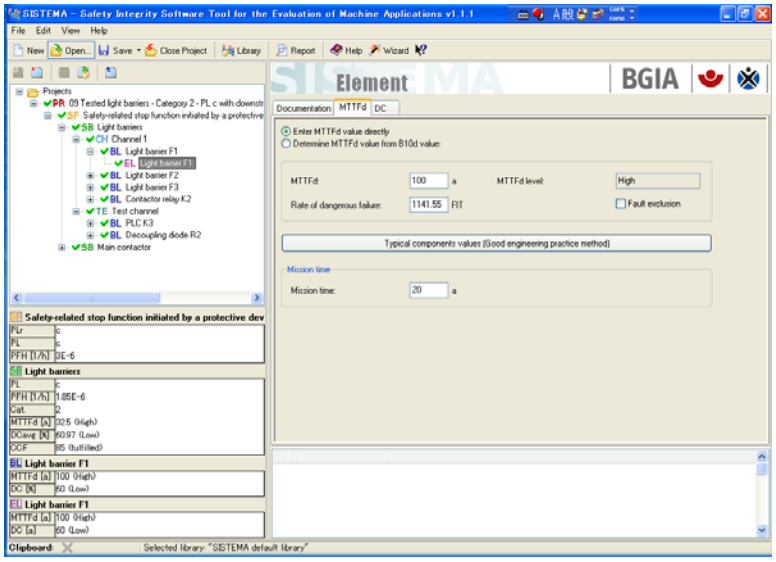
(5)エレメント(Element)

1)エレメントのドキュメントデータの入力



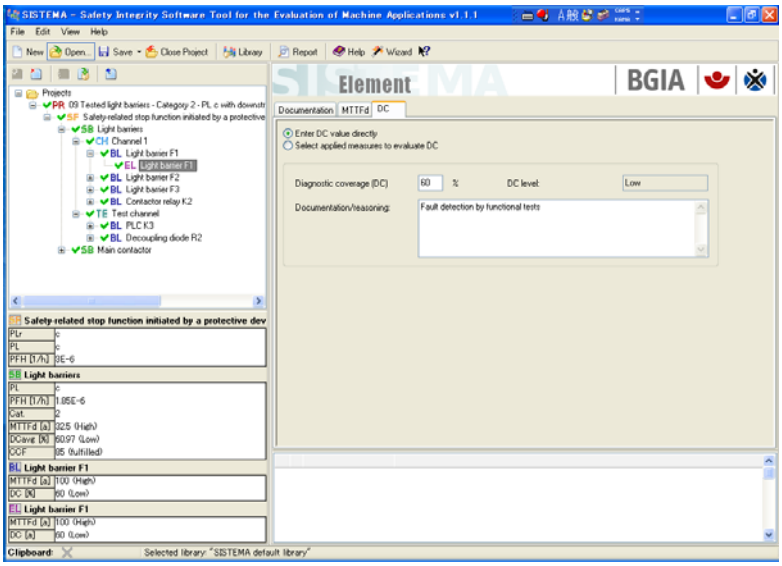
エレメントを作成すると上記の画面が表示される。この画面の Name of element, Documentation の項目に必要事項を入力する。

2)危険側故障までの平均時間(MTTFd)の入力



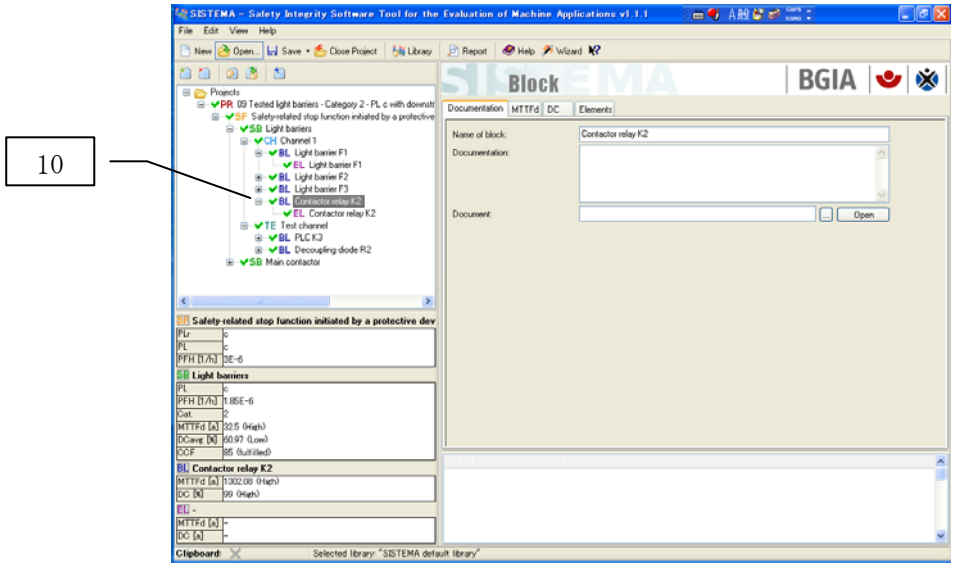
エレメントの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法と B10d と nop の値から MTTFd より求める方法の 2 つがある。 B10d と nop の値から MTTFd を計算する場合、B10d と nop の値を直接入力する仕方と ISO 13849-1 の附属書 C の表 C1 から MTTFd や B10d を選択する仕方がある。表 C1 から選択する仕方は、上記画面の“Typical components values (Good engineering practice method)”を押す。押すと表 C1 が表示されますので、該当する項目を選択し、OK を押す。OK を押したら、選択した MTTFd や B10d が入力される。

3)診断範囲(DC)の入力



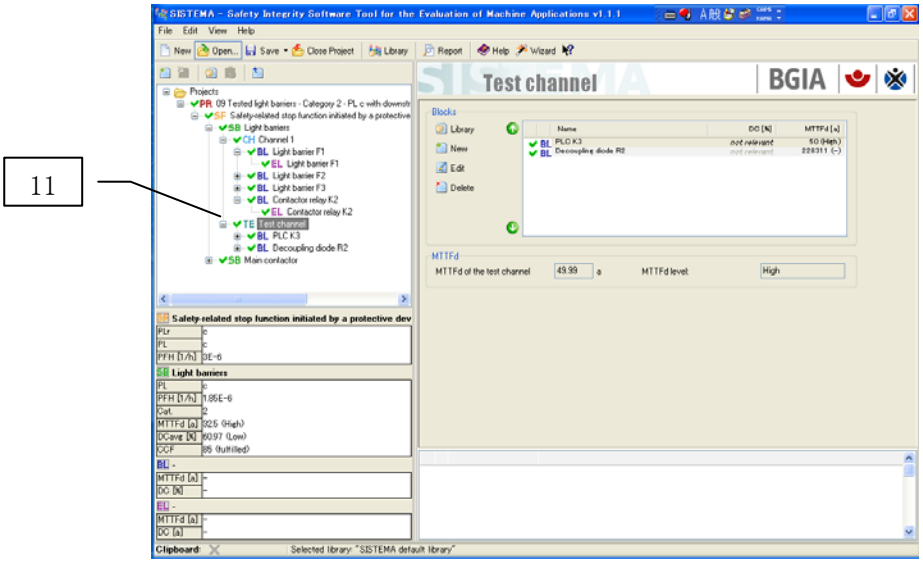
ブロックの DC の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法、ISO 13849-1 の付属書 E の表 E1 から選択する方法の 2 つがある。表 E1 からの選択方法は、上記画面で“Select applied measures to evaluate DC”を選択する。これを選択すると画面が変更される。表示された画面の下側に“Library”の表示があるので、そこを押すと表 E1 がポップアップされる。表示された表 E1 の項目を選択し、“Load Selection”を押すと DC の値が入力される。

(6)追加されたブロックの選択



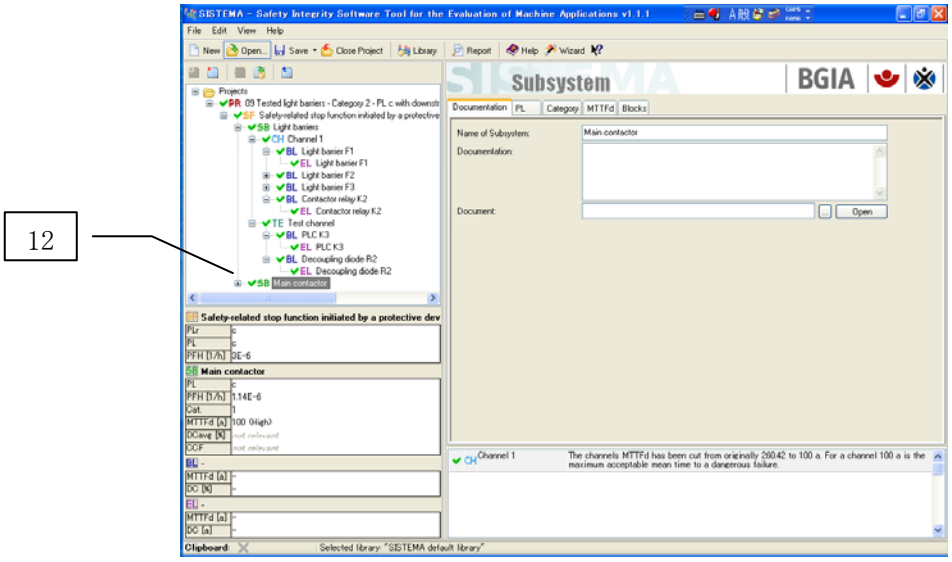
サブシステムで追加されたブロックの選択は、左側のディレクトリの10該当項目をクリックすることにより、上記画面が表示される。表示されたら、前で記載した内容と同様に必要なデータを入力する。このブロックの下位にあるエレメントも前で記載した内容と同様に必要なデータを入力する。

(7)テストチャンネルからのブロックの作成



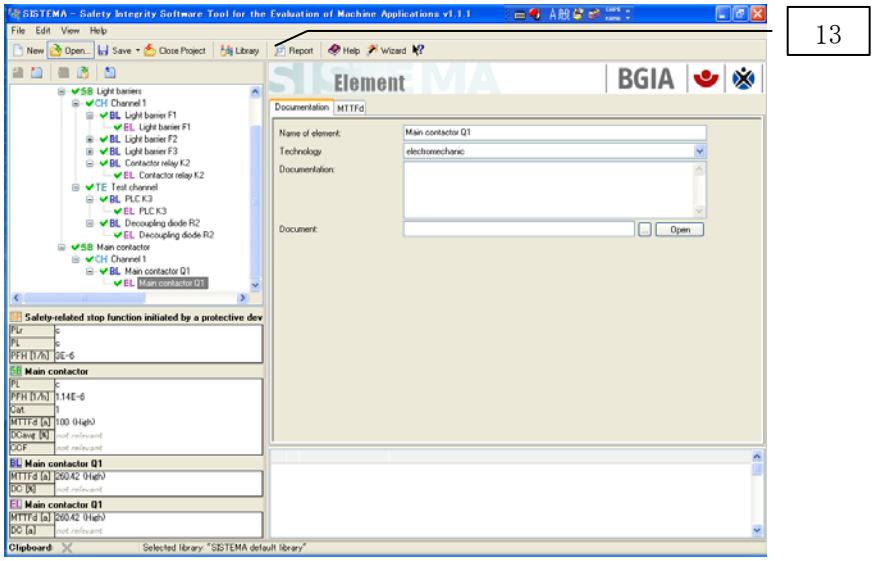
テストチャンネルにブロック(Block)を作成する場合は、左側のディレクトリの11TE(テストチャンネル)から上記画面を開いて、新規(New)をクリックし、ブロック(Block)の項目を作成する。作成したブロックやエレメントのデータは、前で記載した内容と同様にて入力する。

(8)追加されたサブシステムの選択



セーフティファンクションで作成されたサブシステムの選択は、左側のディレクトリの12該当項目をクリックすることにより、上記画面が表示される。表示されたら、前で記載した内容と同様に必要なデータを入力する。このサブシステムの下位で作成したブロック、エレメントも前で記載した内容と同様に必要なデータを入力する。

(9)作成したデータのレポート印刷



このようにして、各項目の必要なデータを入力することにより、パフォーマンス・レベル(PL)や PFH(1/h)が計算され、要求パフォーマンス・レベルと同等になっているか自動的に計算される。計算された結果の印刷は、ツールバーの13レポート(Report)から行う。レポートを押すとプレビュー画面が開くので、左上のファイル(File)から印刷(Print)を選択して印刷する。また、ファイル(File)から“Save As”を選択しますと PDF ファイルの保存ができる。しかし、“Save AS”で保存した PDF ファイルが開かない場合がある。その場合は、ファイル(File)で印刷を選択して、印刷する場合のプリンタ設定で PDF 作成や TIF 作成を行う。

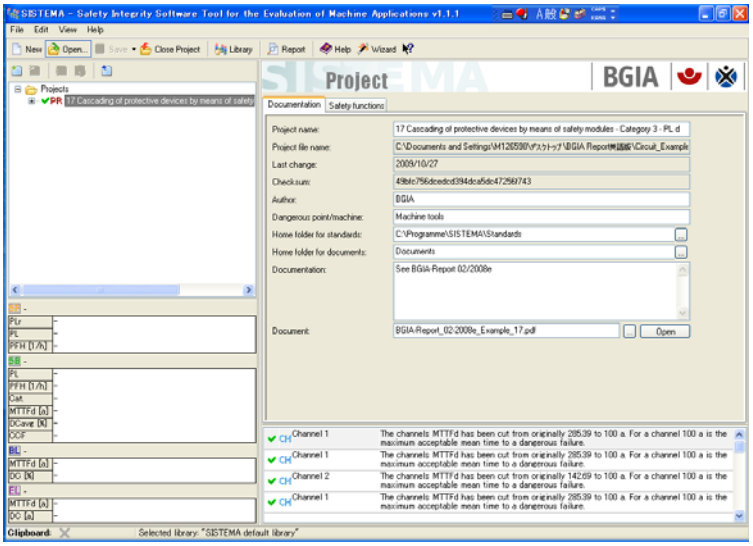
2.4.3 回路例 17:安全モジュールによる保護装置のカスケード-カテゴリ 3 (PL=d)

(1)プロジェクト(Project)

1)プロジェクトの作成

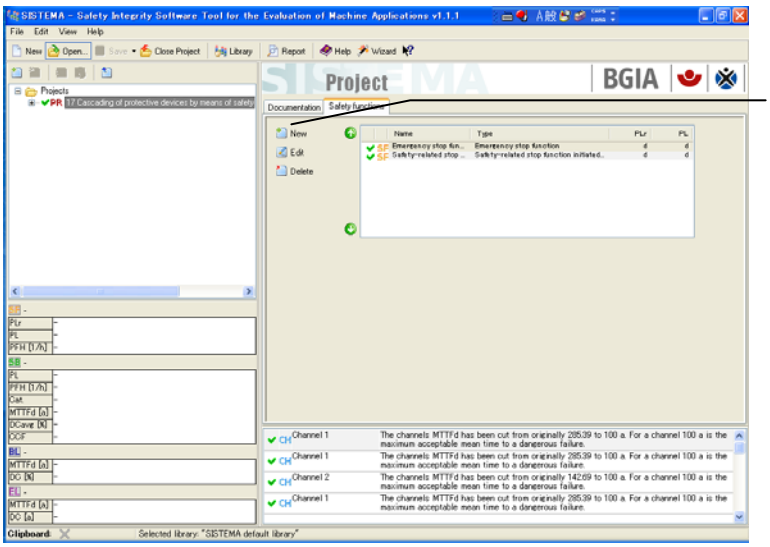
初めて SISTEMA を起動しますと、上記の画面が表示される。この画面から、各種データの作成を行う。まずは、プロジェクト(Project)を作成する。プロジェクトは、メニューバーの 1 ファイル(File)の新規(New)から作成する。又は、ツールバーの 2 ウィザード(Wizard)を開いて、 3 ニュー・プロジェクト(New Project)から作成する。

2)プロジェクトのドキュメントデータの入力



プロジェクトを作成すると上記の画面が表示される。この画面の Project name, Author, Dangerous point/machine, Documentation の項目に必要事項を入力する。なお、各フォルダ(folder)の設定は、デフォルトのままとするが必要があれば変更する。

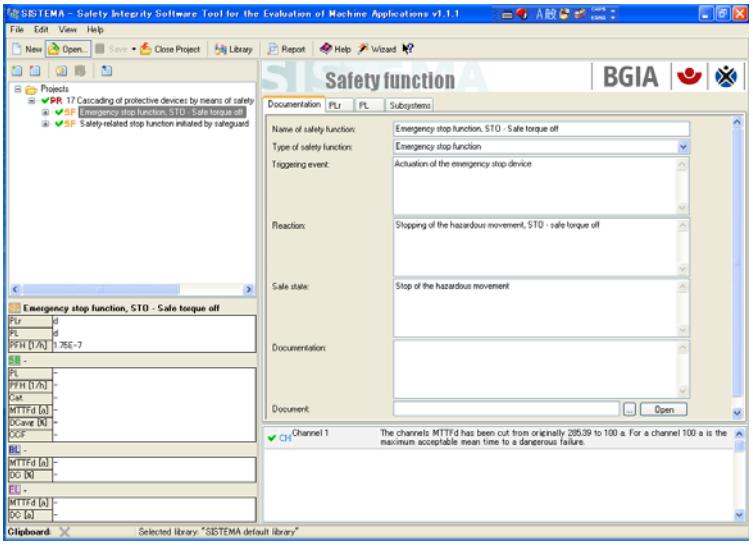
3)セーフティ･ファンクションの作成



プロジェクトにセーフティ･ファンクション(Safety function)の項目を作成する場合、上記画面を開いて、4 新規(New)をクリックする。もし、セーフティ･ファンクションが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

(2)セーフティ･ファンクション(Safety function)

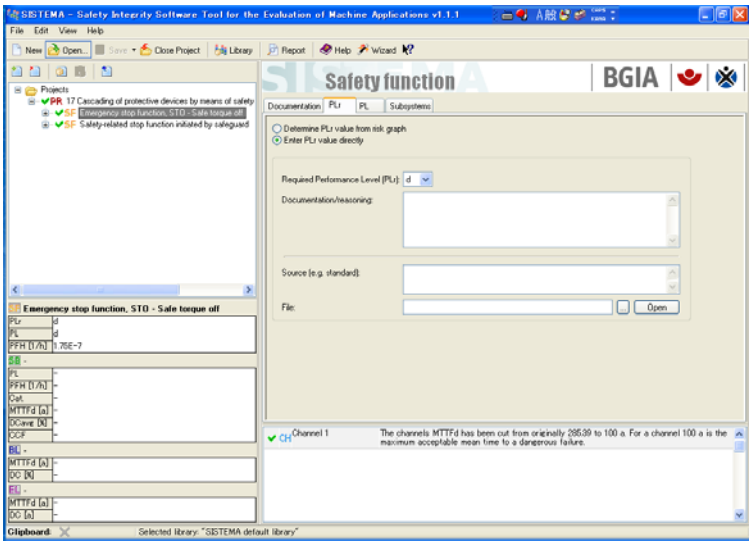
1)セーフティ･ファンクションのドキュメントデータ入力



セーフティ･ファンクションを作成すると上記の画面が表示される。この画面の Name of safety function, Triggering event, Reaction, Safe state, Documentation の項目に必要事項を入力する。Type of safety function は、必要なタイプを選択する。

2)要求パフォーマンス･レベルの入力

①直接入力

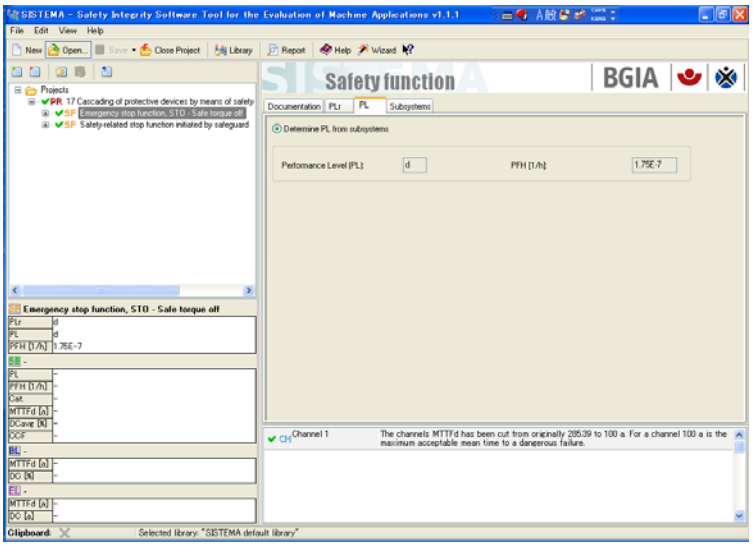


このセーフティ･ファンクションの要求パフォーマンス･レベル(PLr)を入力する方法は、2 つある。ひとつは、上記画面のように直接 PLr を入力する方法である。このとき、要求パフォーマンス・レベルを選定した理由や情報源について記載する。(Documentation/reasoning, Source へ記入)

②リスクグラフによる選択入力

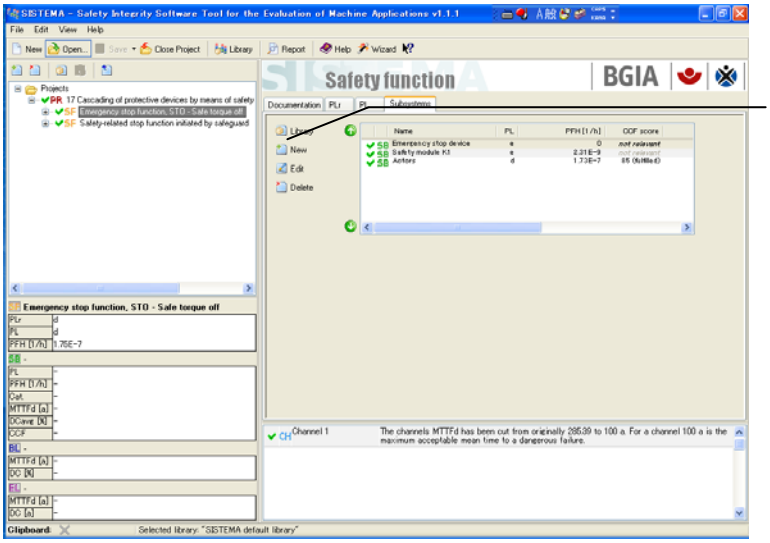
もうひとつは、要求パフォーマンス･レベルをリスクグラフ(risk graph)から求める方法である。要求パフォーマンス・レベルはどちらかの方法で入力する。

3)パフォーマンス･レベルの判定結果



この画面は、下位にあるサブシステム(subsystem)から計算されたパフォーマンス･レベルと PFH(1/h)が表示される。

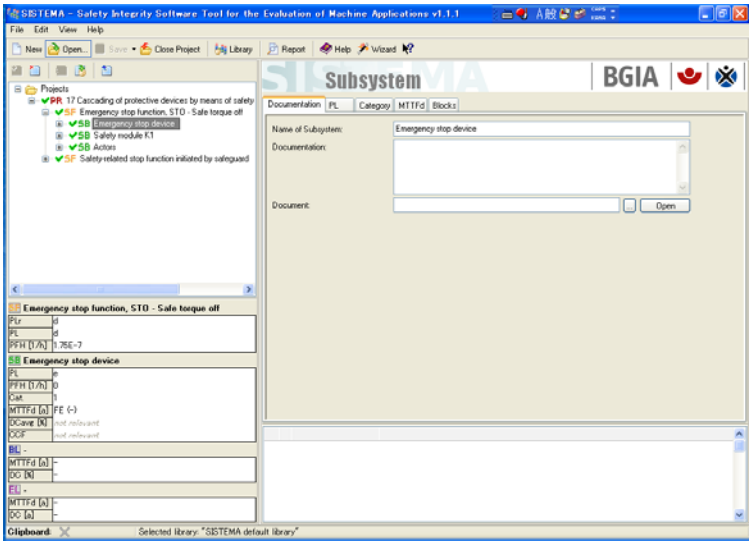
4)サブシステムの作成



セーフティ・ファンクションにサブシステム(Subsystem)の項目を作成する場合、上記画面を開いて、5 新規(New)をクリックする。もし、サブシステムが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

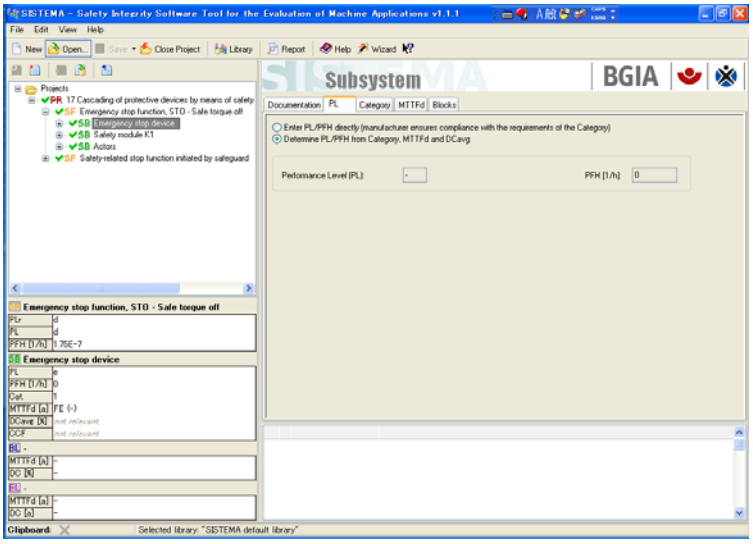
(3)サブシステム(Subsystem)

1)サブシステムのドキュメントデータの入力



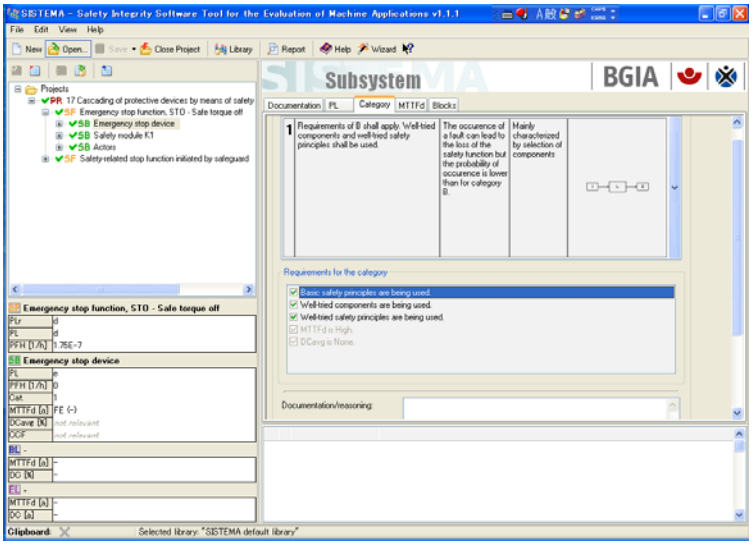
サブシステムを作成すると上記の画面が表示される。この画面の Name of Subsystem, Documentation の項目に必要事項を入力する。

2)パフォーマンス･レベルの入力、又は表示



サブシステムのパフォーマンス･レベルは、上記画面を開いて選択する。入力は、直接入力する方法とサブシステムのカテゴリ､MTTFd と DCavg より求める方法の 2 つがある。通常は、後者の方法を選択する。直接入力すると、MTTFd の入力は必要なくなる。

3)カテゴリの選択

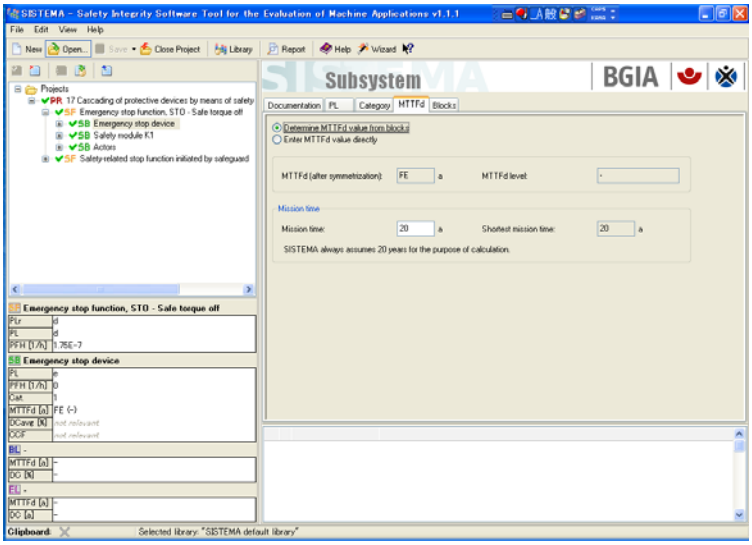


サブシステムのカテゴリ(B、1、2、3、4)を選択する場合は、上記画面を開いて選択する。要求パフォーマンス･レベルにあったカテゴリを選択し、各カテゴリ要求(Requirements for the category)を満足しているかチェックをする。必要な場合、Documentation/reasoning に記入する。カテゴリを選択すると、カテゴリに応じたチャンネルが作成される。

また､カテゴリ B や 1 では､システム内には診断範囲はなく(DCavg=0%)､そのような構造(単一チャンネルシステム)においては、共通原因故障(CCF)の考慮が不要となる。

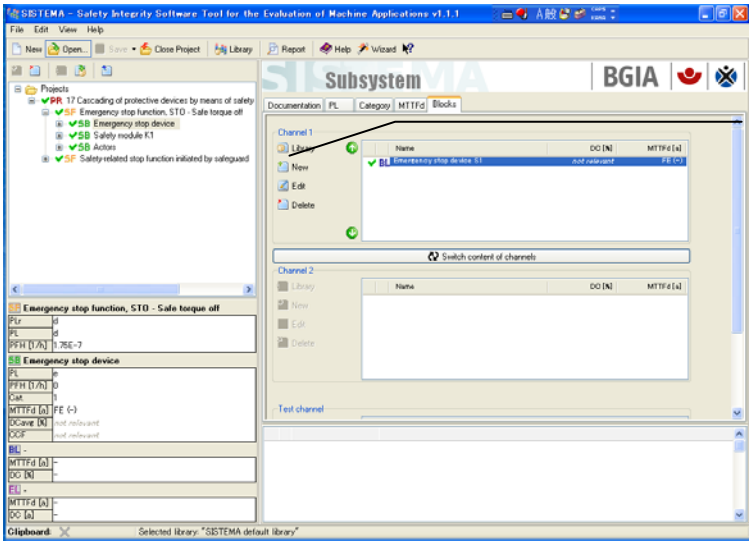
そのため SISTEMA では、カテゴリ B や 1 を選択すると DCavg と CCF の入力項目が表示されなくなる。この例では、カテゴリ 2 を選択しているのでチャンネル 1 とテストチャンネルが作成される。

4)危険側故障までの平均時間(MTTFd)の入力、又は表示



サブシステムの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とブロック(block)の MTTFd より求める方法の 2 つがある。通常は、後者の方法を選択する。

5)サブシステムからのブロックの作成

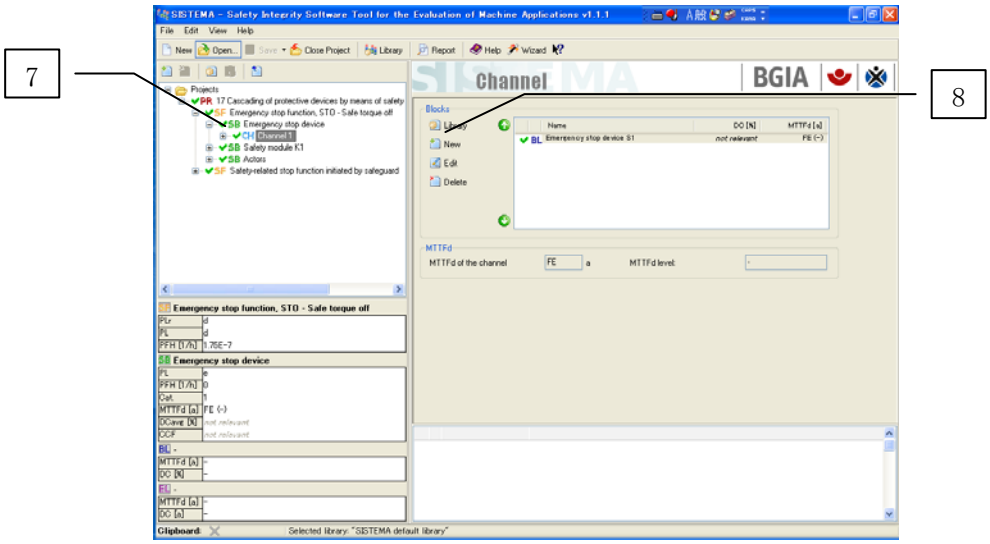


6

サブシステムにブロック(Block)の項目を作成する場合、上記画面を開いて、6 新規(New)をクリックする。もし、ブロックが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

6)チャンネルからのブロックの作成

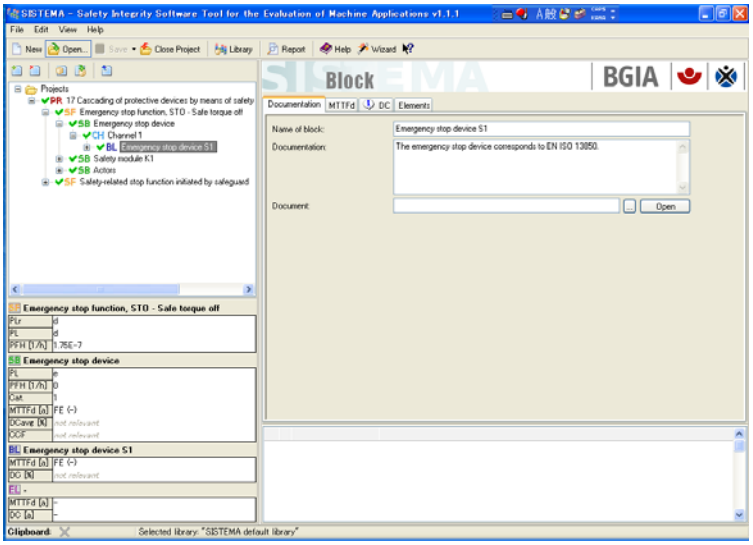
チャンネルは、サブシステムで選択したカテゴリにより、チャンネル 1、チャンネル 2、テストチャンネルが作成される。



又は、左側のディレクトリの 7 チャンネル(Channel)から上記画面を開いて、8 新規(New)をクリックし、ブロック(Block)の項目を作成する。もし、ブロックが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

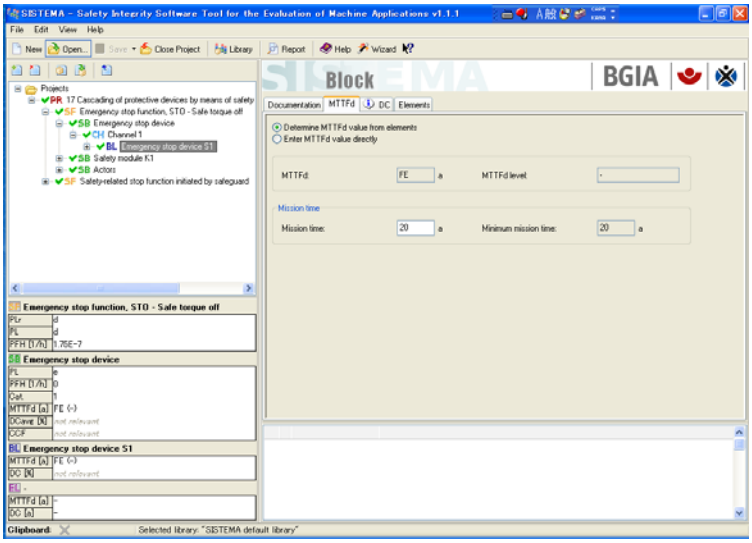
(4)ブロック(Block)

1)ブロックのドキュメントデータの入力



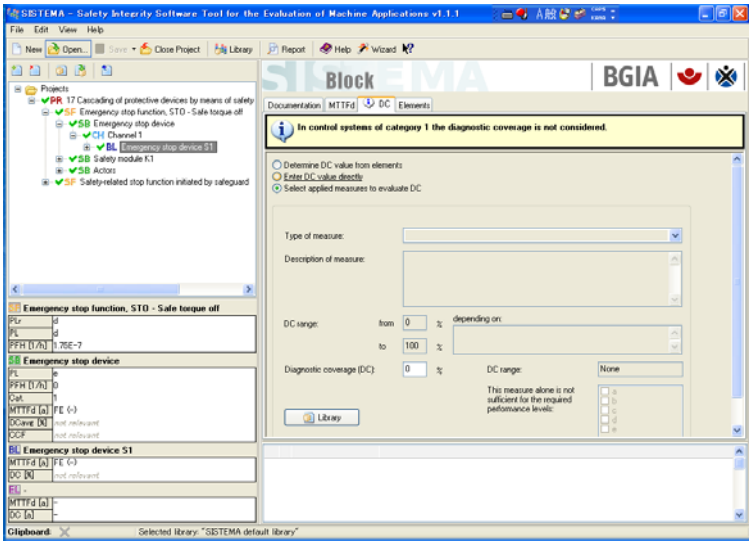
ブロックを作成すると上記の画面が表示される。この画面の Name of block, Documentation の項目に必要事項を入力する。

2)危険側故障までの平均時間(MTTFd)の入力、又は表示



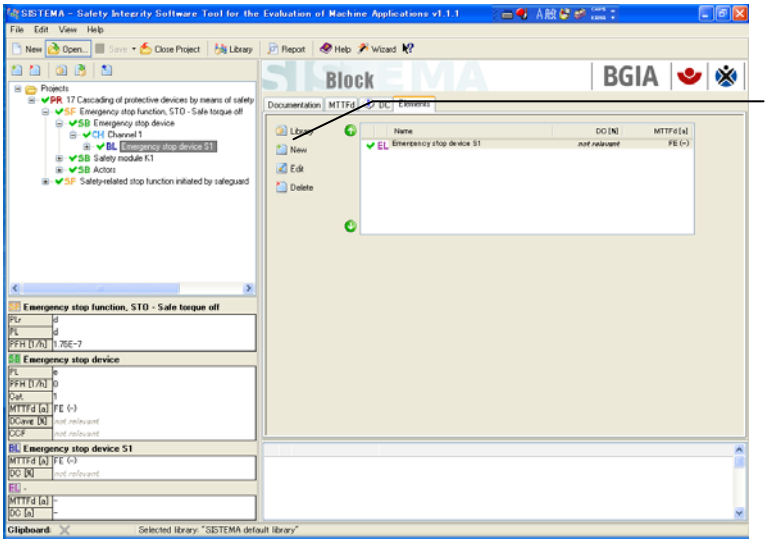
ブロックの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法とエレメント(element)の MTTFd より求める方法の 2 つがある。通常は、後者の方法を選択する。

3)診断範囲(DC)の入力



ブロックの DC の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法、エレメント(element)の DC より求める方法、ISO 13849-1 の付属書 E の表 E1 から選択する方法の 3 つがある。表 E1 からの選択方法は、上記画面で“Select applied measures to evaluate DC”を選択する。これを選択すると画面が変更される。表示された画面の下側に“Library”の表示があるので、そこを押すと表 E1 がポップアップされる。表示された表 E1 の項目を選択し、“Load Selection”を押すと DC の値が入力される。

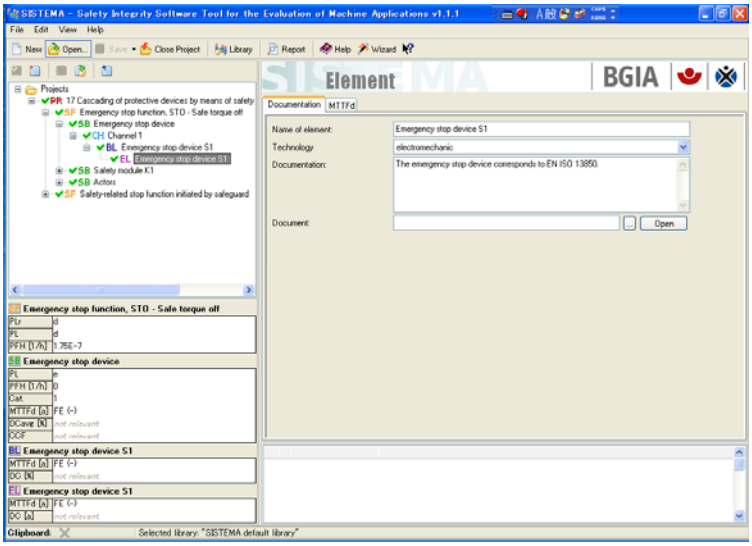
4)ブロックからのエレメントの作成



ブロックにエレメント(Element)の項目を作成する場合、上記画面を開いて、9 新規(New)をクリックする。もし、エレメントが複数ある場合は、上記画面から新規(New)をクリックして追加を行う。

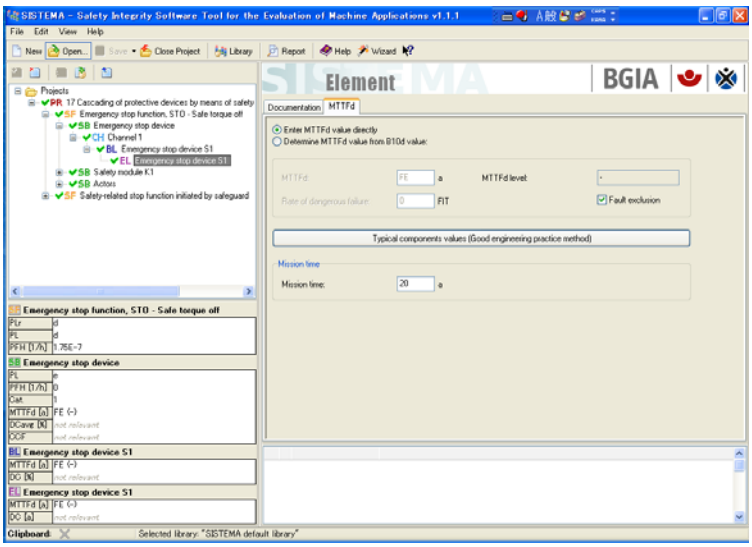
(5)エレメント(Element)

1)エレメントのドキュメントデータの入力



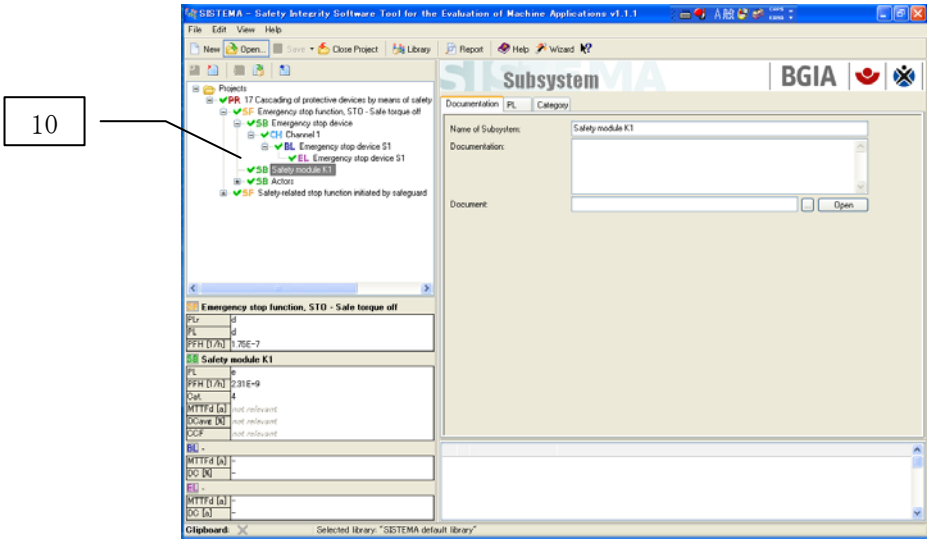
エレメントを作成すると上記の画面が表示される。この画面の Name of element, Documentation の項目に必要事項を入力する。

2)危険側故障までの平均時間(MTTFd)の入力



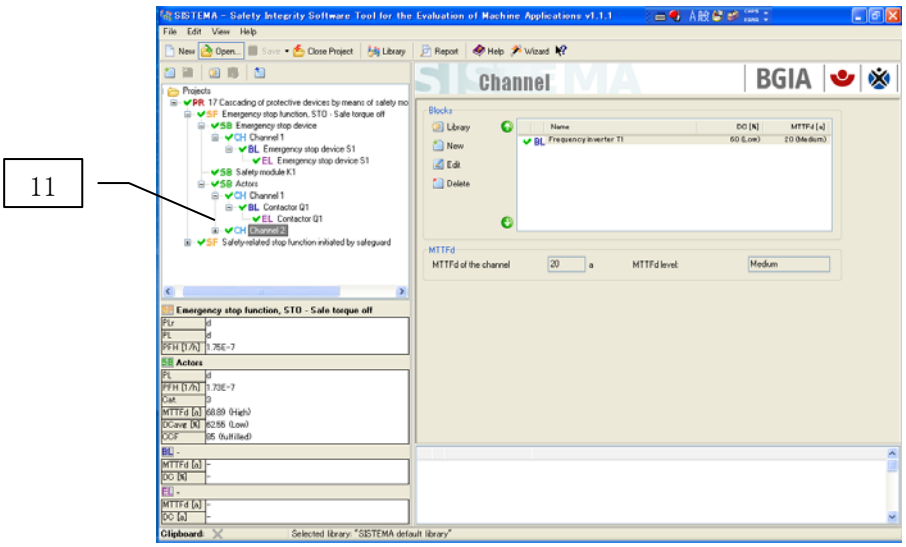
エレメントの MTTFd の入力方法は、上記画面を開いて選択する。入力は、直接入力する方法と B10d と nop の値から MTTFd より求める方法の 2 つがある。 B10d と nop の値から MTTFd を計算する場合、B10d と nop の値を直接入力する仕方と ISO 13849-1 の附属書 C の表 C1 から MTTFd や B10d を選択する仕方がある。表 C1 から選択する仕方は、上記画面の“Typical components values (Good engineering practice method)”を押す。押すと表 C1 が表示されるので、該当する項目を選択し、OK を押す。OK を押したら、選択した MTTFd や B10d が入力される。

(6)追加されたブロック(Block)の選択



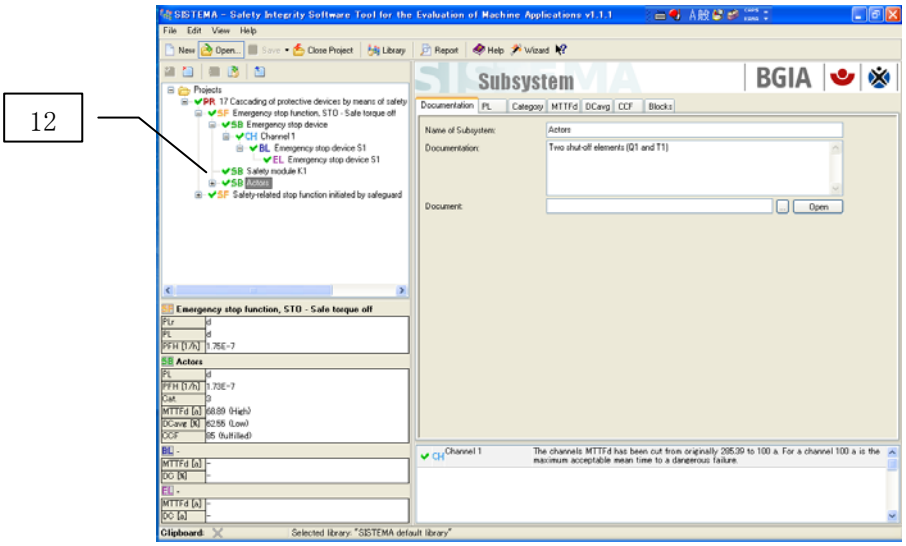
サブシステムで追加されたブロックの選択は､左側のディレクトリの10該当項目をクリックすることにより、上記画面が表示される。表示されたら、前で記載した内容と同様に必要なデータを入力する。このブロックの下位にあるエレメントも前で記載した内容と同様に必要なデータを入力する。

(7)チャンネル 2 からのブロックの作成



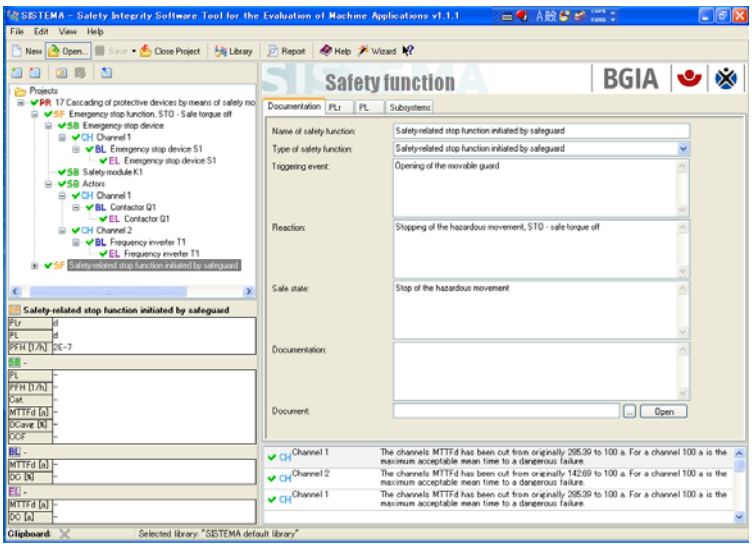
チャンネル 2 にブロック(Block)を作成する場合は、左側のディレクトリの11 CH2(チャンネル 2)から上記画面を開いて、新規(New)をクリックし、ブロック(Block)の項目を作成する。作成したブロックやエレメントのデータは、前で記載した内容と同様にて入力する。

(8)追加されたサブシステムの選択



セーフティファンクションで作成されたサブシステムの選択は、左側のディレクトリの12 該当項目をクリックすることにより、上記画面が表示される。表示されたら、前で記載した内容と同様に必要なデータを入力する。このサブシステムの下位で作成したブロック、エレメントも前で記載した内容と同様に必要なデータを入力する。

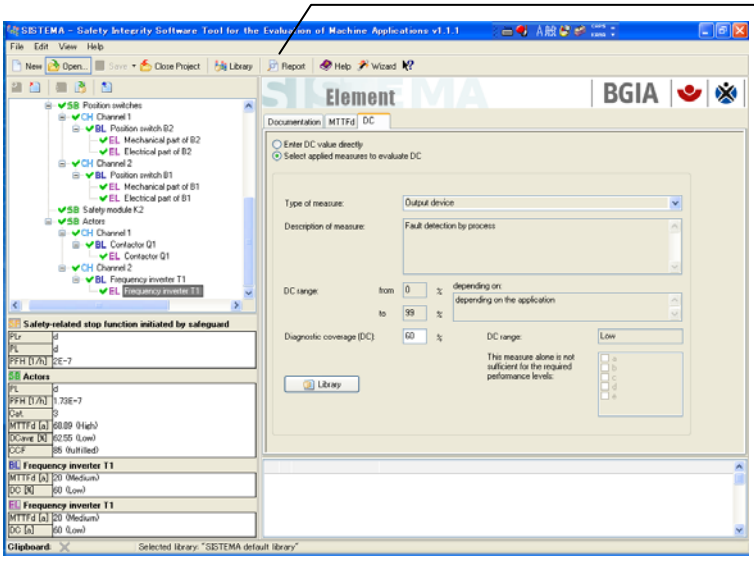
(9)追加されたセーフティファンクションの選択



プロジェクトで追加されたセーフティファンクションの選択は、左側のディレクトリの該当項目をクリックすることにより、上記画面が表示される。表示されましたら、前で記載した内容と同様に必要なデータを入力する。さらに、この下位に作成したサブシステム、ブロック、エレメントも前で記載した内容と同様に必要なデータを入力する。

(10)作成したデータのレポート印刷

13



このようにして、各項目の必要なデータを入力することにより、パフォーマンス・レベル(PL)や PFH(1/h)が計算され、要求パフォーマンス・レベルと同等になっているか自動的に計算される。計算された結果の印刷は、ツールバーの13レポート(Report)から行う。レポートを押すとプレビュー画面が開くので、左上のファイル(File)から印刷(Print)を選択して印刷する。また、ファイル(File)から“Save As”を選択すると PDF ファイルの保存ができる。しかし、“Save AS”で保存した PDF ファイルが開かない場合がある。その場合は、ファイル(File)で印刷を選択して、印刷する場合のプリンタ設定で PDF 作成や TIF 作成を行う。

3. ISO 13849-1:2006 の疑問点と BG からの回答

下表は、当委員会において抽出した ISO 13849-1:2006 の疑問点と、BG からの回答を紹介したものである。回答（その 1）の 1～16 は、当委員会から事前に BG へ質問した内容とその回答であり、回答（その 2）の 17～24 は、当委員会が実施した BG の講習会における質疑を要約して記載したものである。

ISO 13849-1:2006 Question and BG answer

No	Question	Answer
1	If MTTFd and/or B10d are not supplied from component manufacturers, may we calculate them from those components' lifetime (the values in the Annex are too big)?	1. If MTTFd and /or ß10d value are not available from the component manufacturer you can use a. methods in annexes C and D, b. Choose ten years
2	Assuming that electrical life is B10 and fault on hazardous side occurs in the percentage of 50%, may we take B10d as the twice of electrical life?	2. ß10d is estimated as two times ß10 (50 % dangerous failure see annex C)
3	If the values of MTTFd and/or B10 are not supplied from manufacturers, may we use the standard values of "Table C.1 - International Standards dealing with MTTFd or B10d for components"? If so, please advise us of what we should note.	3. see answer 1
4	When calculating MTTFd in case of using our own made circuit baords for safety-related parts, should we calculate 1/MTTFd for each component used and totaling all calculated values as described in "Table D.1 - Example of the parts list of a circuit board" of Annex D, D.1 Parts count method?	4. if you make the quantification for one channel taking into account your own circuit board you have to use the formula for the part count method.
5	Do you recommend any reliability database? If B10d, etc. are taken from such database, is suitability of selection of database required (which kind of reliability database can be used)?	5. I recommend the data base from SN 29500
6	The standard contains a method of converting SIL of subsystem to PL in case data required for calculation of PL such as MTTFd or DC is not disclosed. Is there any concern on such conversion without efforts to obtain necessary data?	6. In the case you have PFH value of category IV system you can determine the DC=99% and the MTTFd (depents of PFH value).
7	May we use data supplied from component manufacturers such as B10d as a basis of calculation as is? Please advise us of conditions of use of such manufacturers' data for calculation, if any.	7. As the result of the validation you have to check the reasonability of the released data of the manufacturer.

8	If Remote I/O Link or the like is used for PLC, can we take the PLC as a single component, or should we take each of them as separate component for calculation?	8. For bussystem you have taken to account the 1 % rule (limit the residual error rate to 1% of the maximum value permitted for the probability of a dangerous failure per hour)
9	For output components, if two safety relays are used in parallel for output and two of their contacts are used in serial connection, should we calculate as one safety relay? If the two relays are treated as component, MTTFd becomes 1/2. We think the reliability against fault becomes twice, but it has not been cleared up that MTTFd decreases.	9. Logical you have to make the calculation of MTTF d for a redundant system (single fault system).
10	Regarding the requirement of multiplying 2/3 or using lower MTBF when estimating MTBF of parallel redundant system, if the parallel redundant system is dual system, the formula is defined. How about 3-way system? At first, should we calculate for dual system, and then calculate for the first calculation and the remaining one system in the formula of dual system? Or should we select and calculate the higher two systems? It is not clear that MTTFd decreases though redundancy is provided by 3-way system.	10. My proposal is to select the channel with the highest MTTFd values and make die calculation with symmetrization formula.
11	How should we determine cycle of proximity switch detecting rotation of machine? In case of 60rpm, the cycle is one rotation per one second. This means Nop will be bigger and MTTFd will be smaller.	11. In the case the proximity switch is a wear component you have to make the calculation taking into account ß10d
12	Is it acceptable to use output results of SISTEMA for results of PL calculation to include in declaration for CE marking? Are documents of hand calculation required?	12. It is acceptable to use output results SISTEMA
13	Is there any checklist containing scores like CCF for determination of conformity to safety requirements for software (e.g. IEC 61508)?	13. Sorry at this time is no checklist for the software available
14	Is it essential to meet specified architecture? Regardless of specified architecture, if it can be verified that PL meets the Table 1, is the PL permitted? If it is essential to meet specified architecture, where is it specified in the standard?	14. Table 1 is not longer guilty. If you make the calculation according to the simplified procedure you have to consider the architectures mentioned in clause 6 of EN ISO 13849-1 : 2006
15	The standard prescribes multiplying 2/3 or use of lower MTBF when estimating MTBF of parallel redundant system. We think this denies the intention of redundancy. What do you think about this?	15. The factor 2 / 3 was introduced to give the (Symmetrization of MTTFd) the reliability not too great importance.

16	We found mission time in SISTEMA report. Is the mission time guaranteed period of machinery or period of trial use? Sometimes we have a calculation result as follows: Mission Time(a): 20 MTTFd(a) of channel (CH1): 19.88 If the MTTFd(a) is 19.88 years to the machine's guaranteed period of 20 years, is it not acceptable? Otherwise, if the total MTTFd of CH1 and CH2 exceeds 20 years, is it acceptable? Do we need to take care of it?	16. For wear components where the T10d is less then 20 years (smaller then the mission time) the wear component has to be exchange during the time T10d.

ISO 13849-1:2006 の疑問点と BG の回答(その1)(仮訳)

No.	質問	回答
1	コンポーネントメーカーから MTTFd や B10d が提示されない場合、そのコンポーネントの電気的寿命から算出してよいか？ (附属書の値があまりに大きいため)	メーカーから MTTFd または、B10d が得られないなら、 a. ISO 138949-1:2006 付属書 C または D の値を使用する。 b. 10 年を選択する。
2	電気的寿命は、B10 と考え、危険側故障が 50%と考えて、B10d は、電気的寿命の２倍としてよいか？	電気寿命の B10 データの 2 倍と見積もる。 (付属書 C 参照)
3	MTTFd や B10 の数値がメーカーから提供されない場合は、ISO 13849-1:2006 の附属書 C に記載ある「表 C.1-コンポーネントの MTTFd または B10 を扱う国際規格」の標準数値を使用してよいか。 また、使用する場合の注意点は何か。	メーカーから MTTFd または、B10d が得られないなら、 a. ISO 138949-1:2006 付属書 C または D の値を使用する。 b. 10 年を選択する。
4	安全関連部に自社基板を使用している場合の MTTFd を求める場合は、ISO 13849-1:2006 の附属書 D の D.1 のパーツ・カウント・メソッドの「表 D.1-回路基板の部品リストの例」に記載あるように使用部品ごとの 1/MTTFd を求め、合計すればよいか。	パーツカウント方法にてにより数値化する。
5	推奨データベースはあるのか。B10d などをデータベースから取ったとき、データベース選択の妥当性も認証時に問われるか (どのような信頼性データベースなら使用してもよいか)	私は SN 29500 からデータベースを推薦する。
6	MTTFd, DC などの PL を計算するのに必要なデータが開示されていない場合、サブシステムの SIL を PL に置き換えるやり方が記載されているが、必要なデータを入手する努力をせずに置き換えてしまう懸念がないのか。	カテゴリ IV システムの PFH 値を持っているという場合、DC ＝ 99%と MTTFd (PFH 値に依存) を決定することができる。
7	コンポーネントメーカーから提供される B10d などのデータはそのまま計算基礎として使用してよいのでしょうか。もし、メーカーのこれらデータを計算に使うための条件があるとしたら教えてください。	確証の結果として、製造業者からリリースされたデータの信頼性をチェックしなければならない。
8	PLC で、Remote I/O LINK 等を使用した場合、PLC は同一の１つのコンポーネントとして、考えればよいのか？ それとも、それぞれ、コンポーネントとして計算しなければならないのか？	バスシステムには、1 パーセントルールで考える (エラーレートを時間当たり 1 パーセント以内にする) 。

9	出力部品で、安全リレーを２個並列で出力し、その接点を２個シリアル接続で使用した場合、計算は、安全リレー１個として、計算するのか。２個をコンポーネントとして扱うと、MTTFd は、１／２になっていく。本来、故障への信頼性は、２倍になると思うが、MTTFd は下がっていくという点が釈然としません。	冗長システムのために MTTF ｄの計算をしなければならない（シングルシステム）。
10	並列冗長系の MTBF を評価する時 2/3 をかける、あるいは低い方の MTBF を使うこと が規定されている、という件で、並列冗長系が、２系統の場合、式が定義されていると思うが、３系統の場合などは、どうしたらよいか？まず、２系統を計算して、さらに、計算したものと残りの１系統で２系統の計算式で、計算するという方法でよいのか？それとも、選択して、高いもの２つで計算すればよいのか？３系統で冗長させているのに、MTTFd は下がっていくという点が釈然としません。	私の提案は、最も高い MTTFd 値でチャンネルを選んで、対称化公式で計算をすることである。
11	機械回転を検出する近接スイッチのサイクルは、どう判断するのか？60rpm で回転すると 1 秒間 1 回になり、Nop が大きくなり、結果、MTTFd が小さくなる。	近接スイッチは、低信頼性部品である。B10d を考慮し計算しなければならない。
12	CE マーキングの自己宣言書に PL 計算の結果として、SISTEMA の出力結果を正式文書としても問題ないか。別に手計算による書類が必要なのか。	SISTEMA から出力された結果を使うことはできる。
13	ソフトウェアの安全要求事項に関する項目についての判定ができる CCF のような点数付けされたチェックリストのようなものがないのか。例えば、IEC 61508 などに。	チェックリストはない。
14	規定アーキテクチャーを満たすことは必須か。それともそれとは無関係に ISO 13849-1:2006 の表 1 を満たしていることを立証できれば規定アーキテクチャーでなくとも PL は認められるのか。必須であるとすれば、どの規定に規定されているのか。	ISO 13849-1:2006 の表 1 は、今は使用しても問題ない。 簡略化された手順によって計算をするならば、ISO 13849-1:2006 の 6 で言及される構造を考慮しなければならない。
15	並列冗長系の MTBF を評価する時 2/3 をかける、あるいは低い方の MTBF を使うことが規定されている。このことは冗長化の意味を否定しているように思われるが、どのように考えるか。	弾力的な数値。信頼性には大きく影響しない。
16	SISTEM のレポートをみると、ミッションタイムを記入してある。これは機械（製品）保証期間（？）、試用期間（？）？ Ｍｉｓｓｉｏｎ　Ｔｉｍｅ（ａ）　　：　20 チャンネル（CH1）の MTTFd（ａ）　：　19.88 という計算になることがある。 機械（製品）保証期間 20 年に対し、19.88 年では未適合ということになるのか？ それとも、CH1＋CH2 のトータルの MTTFd が、20 年を超えていれば、よいのか？ そこまで、気にしなくてよいのか？	信頼性は低い部品で 20 年未満なら保守などによりその期間を満足させる。

ISO 13849-1:2006 の疑問点と BG の回答（その2）

No.	質問	回答
17	EN 954-1 の問題点　「カテゴリ 1 での故障除去はリスク低減の決定に不十分な階層に導かれない。」の意味は？	リスク低減を定量的に規定する時に、カテゴリ 1 の故障除去という概念では評価が適切に行えない。ISO 13849-1 では、カテゴリ 1 は最大で PL=“c”まで対応可能。
18	DC の決定（スライド 33）で、SW1 の DC が 99%で SW2 の DC が 90%である理由は？	SW1 は､強制開離機構を有するため 99%となる。
19	ガス検知器への要求事項→PL=“d”の中でセンサは 1ch でよいのか？	SIL2 なら 1ch で良い。SIL3 なら 2ch が必要。しかしキャリブレーションを頻繁に実施すれば 1ch でも可。
20	安全ドライブシステムインバーターのパルスブロックによる停止は、電源遮断による停止と同等の安全機能とみなせるのか？	同等である。残留エネルギーの問題もパルスブロック方式では回避できるという利点あり。
21	安全ドライブシステムインバーターのパルスブロックによる停止回路のカテゴリ、PL は？	カテゴリは 3。PL については自己診断機能、MTTFd（通常の PLC で 50～70 年）などを考慮して“d”.。
22	安全ドライブシステムインバーターのシャフトレス制御の場合にも適用できるのか？	適用可能、むしろ軸数の多いシャフトレス制御の場合に有効である。
23	PG が 1 個でも PL=“d”が達成できる理由は？2ch は必要ないのか？（モーター速度監視にて）	自己診断を常時実施することにより 1ch でも問題なし。
24	並列システムの MTTFd の計算式の 2/3 の意味は？	これは、たとえば MTTFd=100 年のシステムを 2ch 並列にすると通常の信頼性工学の式では、150 年になってしまう。並列の場合にもシングルの場合と同等にしたいという意図があり､2/3 を付けたもの。

非　売　品

禁無断転載

平　成　２　１　年　度

印刷産業機械の機能安全に関する

調査研究報告書

発　行　　平成２２年３月

発行者　　社団法人　日本機械工業連合会

〒105-0011

東京都港区芝公園三丁目５番８号

電　話　０３－３４３４－５３８４

社団法人　日本印刷産業機械工業会

〒105-0011

東京都港区芝公園三丁目５番８号

電　話　０３－３４３４－４６６１