

労働安全衛生総合研究所安全資料

SAFETY DOCUMENT

OF

THE NATIONAL INSTITUTE OF OCCUPATIONAL SAFETY AND HEALTH

JNIOOSH-SD-NO.26 (2010)

機械サーボプレスの急停止時間の
決定方法に関する研究



独立行政法人 労働安全衛生総合研究所

機械サーボプレス急停止時間の決定方法に関する研究

目 次

1. 序論	… 2
1. 1 背景と目的	… 2
1. 2 参照規格	… 3
2. 急停止時間に関する定義と諸条件の整理	… 4
2. 1 急停止時間決定法の適用範囲	… 4
2. 2 非常停止ならびに監視機能による急停止での停止時間	… 10
2. 3 急停止時間の定義	… 12
3. 急停止時間の測定条件	… 15
3. 1 急停止時のスライドの速度	… 15
3. 2 ボールスクリーを用いたサーボプレスの速度設定	… 18
3. 3 エアバランサの内圧	… 19
3. 4 機械的制動機構（メカブレーキ）の摩擦面の摩耗	… 21
3. 5 エア式メカブレーキのエア排気時間の影響	… 21
3. 6 温度条件	… 21
3. 7 情報処理負荷	… 21
3. 8 監視機能の安全性能	… 22
4. 障害の除外	… 26
4. 1 機械部品	… 27
4. 2 空圧機器	… 30
4. 3 油圧機器	… 30
4. 4 電気・電子部品	… 31
5. 解析事例	… 34
5. 1 急停止時間決定の基本的流れ	… 34
5. 2 例 1：停止カテゴリ 0 のシステム	… 36
5. 3 例 2：停止カテゴリ 0（インバータ回路遮断）＋ダイナミックブレーキのシステム	… 42
5. 4 例 3：停止カテゴリ 1 のシステム（遅延回路によって停止カテゴリ 0 に切り替える場合）	… 50
5. 5 例 4：停止カテゴリ 1 のシステム（サーボ異常検出によって停止カテゴリ 0 に切り替える場合）	… 55
6. 結論	… 63
謝辞	… 64
参考文献	… 64
付録（用語の解説）	… 65

**A Study on Procedure for Determining
the Protective Stopping Time of Mechanical Servo Presses**

CONTENTS

1. Introduction	...	2
1.1 Background and purpose	...	2
1.2 Referenced standards	...	3
2. Definition, terms and conditions of protective stopping time	...	4
2.1 Scope of proposed determining procedure	...	4
2.2 Stopping time of emergency stop and protective stop resulting from monitoring function	...	10
2.3 Definition of protective stopping time	...	12
3. Measurement conditions of protective stopping time	...	15
3.1 Motion speed of slide	...	15
3.2 Setting speed of servo press using ball screw	...	18
3.3 Pressure value in air balancer system	...	19
3.4 Frictional surface wear of mechanical brake	...	21
3.5 Influences of an increase in air exhaust time of pneumatic brake	...	21
3.6 Temperature condition	...	21
3.7 Information processing load	...	21
3.8 Safety performance of monitoring function	...	22
4. Fault exclusions	...	26
4.1 Mechanical components	...	27
4.2 Pneumatic components	...	30
4.3 Hydraulic components	...	30
4.4 Electrical and electronic components	...	31
5. Examples of procedure for determining the protective stopping time	...	34
5.1 Basic task flow	...	34
5.2 Example 1: System with stop category 0	...	36
5.3 Example 2: System with stop category 0 (inverter circuit shutdown) + dynamic brake	...	42
5.4 Example 3: System with stop category 1 (switched to stop category 0 by using a delay circuit)	...	50
5.5 Example 4: System with stop category 1 (switched to stop category 0 by detection of servo system failure)	...	55
6. Conclusions	...	63
Acknowledgments	...	64
References	...	64
Appendix (glossary)	...	65

機械サーボプレスの急停止時間の決定方法に関する研究

齋藤 剛*

A Study on a Procedure for Determining the Protective Stopping Time of Mechanical Servo Presses

by Tsuyoshi SAITO*

Abstract: “Servo press” is the name given to such an innovative power press machine that the motion of its slide can be changed flexibly and easily by the control of programmable servo drive system. A kind of the servo press which is so constructed that the power of a servo motor is transmitted to the slide by means of a mechanical rotating mechanism or a direct drive mechanism (e.g. crank, ball screw, etc.) is termed “mechanical servo press”.

In order for a safe use of the servo press to be ensured, the time interval between the actuation request for a protective stop function and the completion of a slide stoppage (i.e., the protective stopping time) is an important parameter to determine an appropriate distance to a hazard zone from the detection zone of a sensitive protective equipment or a two-hand control device. JIS B 6410 which provides safety requirements of servo presses, therefore, requires such a treatment of servo press manufacturers that the protective stopping time has to be determined by considering a single fault condition which gives the longest stopping time (i.e., the worst case). However, the extent of components and failures which may impact on the stopping time, the relationships with the required performance level, the applicability of fault exclusion and the forth are not mentioned in this standard, consequently, a common interpretation of the requirement for the protective stopping time still has not been shared.

Concrete examples of procedures to identify the worst case and to evaluate the protective stopping time for several types of the mechanical servo press are described in this document. For this purpose, at the first, the meaning of the requirement for the protective stopping time is clarified from the results of considerations about the concepts and technical requirements of the ISO/IEC international standards on functional safety and the actual approach on the Japanese construction code for power press. In the second, concrete evaluation methods for the respective single fault condition, the extent of failures to be considered and constraints for fault exclusion is discussed. System architectures related to the protective stop function shown in the examples are modeled by reference to commercially available servo presses, which is one of results of a collaborative research project by JNIOSH and six domestic servo press manufacturers.

Key-words: Servo press, Protective stopping time, Safety distance, Safety function

* 機械システム安全研究グループ Mechanical Safety Research Group

1. 序論

1.1 背景と目的

サーボプレスは我が国で開発された新しい形態の動力プレス機械である。このうち、サーボモータの動力をクランクなどの回転式機構又はボールねじなどの直動式機構によってスライドに伝達する構造のものを特に機械サーボプレスと呼ぶ(JIS B 6410 定義 3.1.1)。典型的な機械サーボプレスのシステム構成を図1に示す。

従来の機械プレス(フリクションクラッチプレス)において、スライドの停止はメカブレーキによって行われるものであり、いかなるプレスの急停止機構も方式はこの1つである。しかし、機械サーボプレスでは、スライドの減速/停止に、メカブレーキの他、サーボシステムの減速/停止制御、回生制動、あるいは、モータ端子を短絡又は抵抗素子に接続して行うダイナミックブレーキなど様々な機構が利用可能であり、現実には多種多様な急停止機能が実装されている。このため、メーカー、さらには同一業者が製造するものでも機種が異なると、急停止時のスライドの挙動が同じではなく、特に急停止時間については、メーカー毎に独自の判断基準に基づいて決定(銘板表示)しているのが現状である。

このような状況に鑑み、2009年9月に「JIS B 6410-サーボプレスの安全要求事項」が発行され、サーボプレスの安全関連機能に一定の基準が示されることとなった。JIS B 6410は、近年著しく整備が進んだISO/IECの機能安全規格の内容を取り込み、一連のISO機械安全規格の枠の中でタイプC規格の1つとなるべく各要求事項が策定されたものであり、本規格において“急停止時間”は急停止機能を実行するサブシステムに単一障害が発生した状況を想定し、急停止時間が最も長くなる場合(ワーストケース)での値として決定しなければならないことが明確に規定された。

しかし、急停止時間の定義付けは確立したものの、JIS B 6410ではワーストケースの特定において個々の故障や不具合に対する具体的な取り扱いや評価までは示しておらず、当該要求事項の解釈について統一された見解が得られているとは必ずしも言えない。

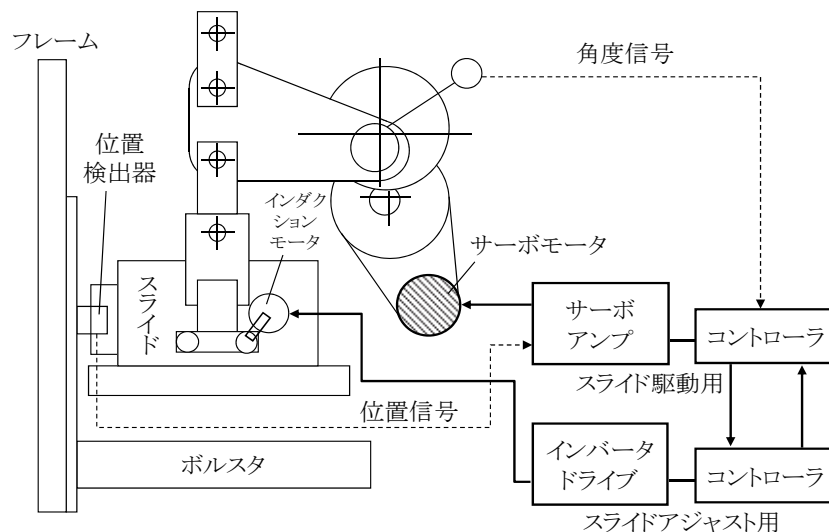


図1 機械サーボプレスのシステム構成の例 (JIS B 6410 図1)

そこで、本研究では、JIS B 6410 及び関連する上位規格(特に ISO 13849-1:2006)の要求事項、

ならびに、現行の国内での動力プレスの故障に対する取り扱いなどを考慮に入れ、JIS B 6410 が要求する“ワーストケースの特定”の意味、ならびに、そこで検討されるべき不具合（障害）の範囲について考察し、機械サーボプレスの急停止時間を決定する際の考え方を明らかにする。さらに、現在市場に投入されているサーボプレスで採用されている典型的な急停止システムの構成例を挙げ、これらについてワーストケースを特定していく具体的なプロセスを詳述する。

なお、本資料は、(独)労働安全衛生総合研究所と国内プレスメーカー6 社との共同研究課題「サーボプレスの急停止時間の決定法に関する研究」で得た知見をもとに、機械安全規格の枠組みの中でタイプ C 規格の 1 つとして発行された JIS B 6410 の解釈として筆者の見解を述べたものである。現行の動力プレス機械構造規格及びこれに関連した技術指針における機械サーボプレスの急停止時間の取り扱いを変更するものではない。

1.2 参照規格

本資料で規定の一部を引用する国内外工業標準を以下にまとめておく。引用箇条については原文を必ず参照されたい。

- 1) JIS B 6410:2009 プレス機械 - サーボプレスの安全要求事項
- 2) JIS B 9705-1:2000 機械類の安全性 - 制御システムの安全関連部 - 第 1 部:設計のための一般原則
- 3) JIS B 9715:2006 機械類の安全性 - 人体部位の接近速度に基づく保護設備の位置決め
- 4) JIS B 9960-1:2008 機械類の安全性 - 機械の電気装置 - 第 1 部：一般要求事項
- 5) JIS B 9961:2008 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
- 6) JIS C 0508-2:2000 電気・電子・プログラマブル電子安全関連系の機能安全 - 第 2 部：電気・電子・プログラマブル電子安全関連系に対する要求事項
- 7) JIS C 9730-1:2004 家庭用及びこれに類する用途の自動電気制御装置 - 第 1 部：一般要求事項
- 8) ISO 13849-1:2006 Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
- 9) ISO 13849-2:2003 Safety of machinery - Safety-related parts of control systems - Part 2: Validation
- 10) ISO/TR 23849:2010 Guidance on the application of ISO 13849-1 and IEC 62061 in the design of safety-related control systems for machinery
- 11) IEC 61800-5-2 Ed.1.0:2007 Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional
- 12) IEC 61784-3 Ed.1.0:2007 Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions
- 13) EN 692:2005+A1:2009 Machine tools - Mechanical presses - Safety

2. 急停止時間に関する定義と諸条件の整理

ワーストケース特定の具体例を示す前に、急停止時間の決定法を議論する上で前提となる JIS B 6410 及びその他安全規格の定義や要求事項について、本章で整理しておく。

2.1 急停止時間決定法の適用範囲

2.1.1 急停止システムの安全性能

JIS B 6410 において、スライドによる押しつぶしの危険源を本質的安全設計方策によって除去していない限り又は押しつぶしのリスクを適切に低減していない限り、サーボプレスは急停止機能をもたなければならないとされている。ただし、いずれの部品の単一障害も急停止時間の延長を引き起こしてはならないという JIS B 6410 の要求事項（以下、この要求事項を「急停止時間条件」という）が適用されるか否かは、あくまでもリスクアセスメントの結果として要求された急停止システムの安全性能に依拠して定まる。

急停止システムが機能不能状態に陥るような故障が起ればリスクの増大は免れない。したがって、急停止機能は JIS B 9705-1 で定義される安全機能に該当する。JIS B 9705-1 に従えば、安全機能として急停止機構を設計・実現していく際、まず次の 2 つを定めなければならない。

- 1) 安全機能仕様（急停止機能に要求される各種の特性）の決定
- 2) 安全性能（期待するリスク低減に応じた急停止機能の信用度の高さ）の決定

このうち、1) 安全機能仕様について、少なくとも以下の内容を指定しなければならないとされている。

- a) 応答時間（箇条 5.2.6）
- b) 速度、圧力などの安全関連パラメータの逸脱や変動の監視（箇条 5.2.7）
- c) 動力源の喪失、変動の影響（箇条 5.2.8）

急停止時間が上記 a) に該当するのは明らかである。すなわち、JIS B 9705-1 に従えば、急停止機能は急停止時間を含めて 1 つの安全機能として設計されるのであって、その仕様に反して急停止時間を超えることは“機能の喪失”と見なされると解釈できるのである。

サーボプレスの安全機能に対する安全性能については、JIS B 6410 の箇条 5.3 において、JIS B 9705-1 の 6.2.7 に規定されるカテゴリ 4 を標準とすることが定められている。リスクアセスメントの結果からこの基準を採用する場合、急停止システムは次のように設計しなければならない。

- a) いずれの部品の単一障害も安全機能の喪失に至らない。
- b) すべての単一障害を次の安全機能の作動要求時又はその前までに検出する。
- c) 単一障害発生時に安全機能を常に実行し、検出した障害が修復されるまで安全状態を維持する。
- d) 検出が不可能な場合、障害の蓄積が安全機能の喪失に至らない。

上記 a) から、急停止システムが JIS B 6410 の箇条 5.3 の基準に従う場合（すなわち、カテゴリ 4 を要求されている場合）、いずれの部品の単一障害も急停止時間の延長を引き起こしてはならないこととなり、これより JIS B 6410 の急停止時間条件が導かれるのである。

換言すれば、JIS B 6410 の解釈としては、リスクアセスメントの結果、急停止システムがカテゴリ 4 である必要がない場合、必ずしも急停止時間条件は要求されない。例えば、急停止システムがカテゴリ 3 に従う場合には、蓄積した障害のために安全機能を喪失しても、すなわち、カテゴリ 3 の範囲で許容されている危険側故障状態で急停止時間が銘板表示値を超えても、これは許容される。この場合、該当する障害蓄積状態はワーストケースの検討から除外し、あくまでもカテゴリ 3 の範囲で許容されない危険側故障についてのみ検討すればよい。さらに、急停止システムをカテゴリ 2 又はカテゴリ 1 とする場合は、単一障害によって安全機能を喪失すること自体が JIS B 9705-1 で許容されており、したがって、この場合のワーストケースとは、通常の使用において合理的に想定される範囲で最も急停止時間が長くなる条件を指すに留まり、故障状態下での急停止時間の延長を考慮する必要は特にない。

以上のことから、後述するワーストケース特定プロセスの例示においては、急停止システムはカテゴリ 4（以下、これを Cat.4 と記す）の要求に従って設計・構成されるという前提で議論を進める。

2.1.2 ISO 13849-1:2006 への対応

急停止時間条件が急停止システムの安全性能に依拠することを述べたが、JIS B 9705-1 の基となった ISO 13849-1:1999 は 2006 年に改定されており、いずれ旧版と置き換えられる予定である。このため、急停止システムの妥当性評価においても、改定された ISO 13849-1:2006 への対応を考慮する。

注記 1) 制御系の安全関連部に対する整合規格については、2009 年 12 月 29 日付 EU 官報において、当初 2009 年 12 月末を期限としていた EN 954-1 から ISO 13849-1:2006 への移行が 2 年間延長されることが発表されている。しかし、各種の C 規格では ISO 13849-1:2006 への移行を前提とした改定がすでに実施あるいは進行中であり、その対応は必須と考えられることから本研究でも考慮することとした。

ISO 13849-1:2006 では、新しい安全性能基準として“パフォーマンスレベル”（Performance Level：以下、PL と記す）が導入され、安全関連部で使用するコンポーネントの信頼性に対する要求がより具体的に規定されることとなった。ISO 13849-1:2006 に従えば、Cat.4 と同等な PL は“e”（以下、これを PL=e と表す）であるので、前述した旧版の規定も重複して記すと急停止システムの要件は以下ようになる。

- a) カテゴリ B の要求を満たすこと、すなわち、基本安全原則に従っていること。
- b) 十分に吟味された安全原則（該当する場合）が正しく実現されていること。
- c) 単一障害（共通モード故障を含む）で安全機能を喪失しないこと。
- d) 単一障害は、次の安全機能の作動要求時又はその前までに検出されること。
- e) d)の障害検出が不可能な場合、検出できない障害の蓄積が安全機能の喪失に至らないこと。
- f) 各チャンネルの MTTF_dが 30 年以上であること。
- g) 診断範囲の平均値が 99%以上であること。

- h) 故障率に対する共通原因故障の割合（ β パラメータ）が 2%以下であること（ISO13849-1:2006 の附属書 F に従うことで達成できる）。
- i) システム全体の 1 時間当たりの危険側故障発生確率が 10^{-7} 以下であること（ただし、一般に、 10^{-8} 以下の達成は不可能とされている）。

上記の f)～i) が ISO 13849-1:2006 で新たに追加された要件であり、これらは急停止にサーボ減速制御を利用する場合などでサーボシステム及び関連コンポーネントの妥当性を評価する際に重要な数値目標となる。

注記 2) ISO 13849-1:2006 では、安全関連部のアーキテクチャがカテゴリ 3 であっても $PL = e$ を達成できる場合が示されているが、JIS B 6410 の箇条 5.3 で謳われている“同等の安全性能”の解釈として“Cat.4 の構造要件を満たすこと”は必須である。

注記 3) プレスコントローラのように、プログラマブル電子部品又は高複雑度電子部品を用いたコンポーネントについて（特に、組み込みソフトウェア部分について）は、規格の性質上 ISO 13849-1:2006 の適用は推奨されない。このようなコンポーネントについては、 $PL = e$ (Cat.4) の認証が既になされているプレスコントローラを用いるか、又は、ハードウェア及びソフトウェアの安全性能の査定に JIS B 9961 を考慮する必要がある。なお、JIS B 6410 の箇条 5.3 で謳われている Cat.4 と同等な安全度水準は“耐故障数 1 以上の SIL 3”であって、単に SIL 3 ではない。

さらに、ワーストケースの特定プロセスにおいて、本研究では“安全関連ブロック図”の利用を推奨する。安全関連ブロック図は、ISO 13849-1:2006 において、アーキテクチャが単一系か冗長系か、あるいは、どのコンポーネントの障害が自己診断で検知可能か否かなど、安全関連サブシステムの安全性能を解析する上で重要となる事項を図式で考察できるようにする目的で導入された表現方法である。典型的な急停止システムの安全関連ブロック図については第 4 章の解析事例で改めて詳述するが、ISO 13849-1:2006 に従えば、急停止システムは一般的に図 2 の安全関連ブロック図として表現される。

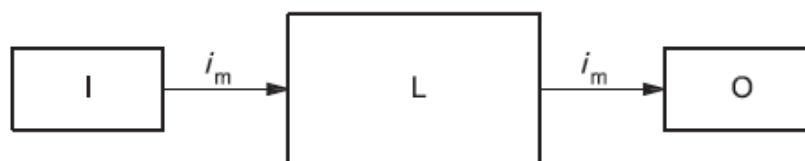


図 2 急停止システムの一般化安全関連ブロック図表現

ここで、各略語の意味は各々以下の通りである。

- “I”：入力要素（押しボタン、ガードのインターロック装置、ライトカーテンなど）
- “ i_m ”：内部接続手段（I/O インターフェースなど、信号伝達のための要素）
- “L”：論理／処理要素（安全コントローラ、安全リレーユニットなど）
- “O”：出力／動力制御要素（モータの電源遮断を行うコンタクタ、エア式メカブレーキの空気

圧を抜く電磁弁など)

具体的なコンポーネントに対応させた例として、能動的光電保護装置 (AOPD)、電子制御ロジック、液圧バルブにより構成されたインターロックシステムを安全関連ブロック図として表現したものを図 3 に示す。

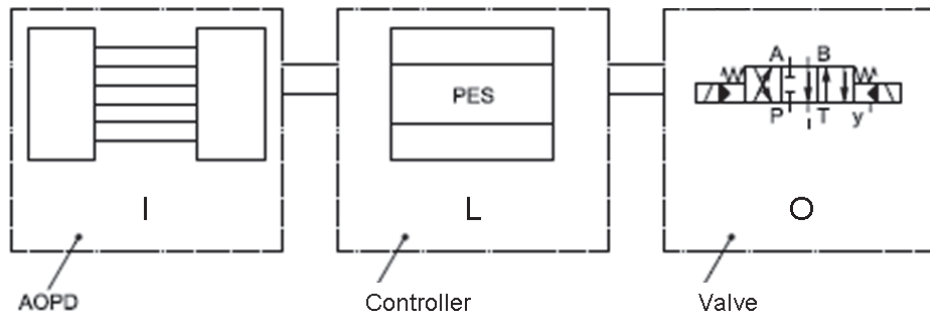


図 3 インターロックシステムの安全関連ブロック図の例

安全関連ブロック図に関する詳細な説明は、ISO 13849-1:2006 の附属書 B に記載されているが、特に注意すべきは、これは安全性能を解析することを目的にした作図法であって、必ずしも“機能ブロック図”や“信頼性ブロック図”と対応する表現ではないことである。また、上図はあくまでも“安全関連ブロック図”の最も基本的な概念を示しているもので、3 つのブロックは必ずこの数でなければならないということを意味している訳ではない。

安全関連ブロック図は以下のように解析する。

- 1 つのチャンネルは複数のブロックから構成される。ブロックは 1 つのコンポーネント又はユニットを表す。
- 直列接続されたブロックのうちの 1 つでも危険側故障すれば、そのチャンネルは安全機能を実行することはできない。
- 2 つのチャンネル (ブロック) が並列に配置されている場合、少なくとも 1 つのチャンネル (ブロック) が故障をしていないなら、安全機能を遂行できる。
- 試験目的のためだけに使用されるブロック及び別のチャンネルの安全機能の実行に影響を与えないブロックについては、分離して考えてもよい。

より詳細な解析方法については、ISO 13849-1:2006 の附属書 I を参照されたい。

2.1.3 PL=e (Cat. 4) で許容される障害

安全関連部が特定のカテゴリ又は PL に適合するか否かについて、その妥当性は ISO 13849-1:2006 及び ISO 13849-2 の規定に基づいて判断する。これらの規格には、各カテゴリで満足すべき基本安全原則の他、妥当性検証で検討すべき障害、さらに特定の条件の下で検討から除外できる障害 (障害除外) がリスト化されている。

注記 4) ISO 13849-2 は現在 DIS 段階まで改定審議が進んでおり、特に附属書 A~D の障害リストにおいていくつかの数値の見直しが検討されている。本資料では現行の ISO 13849-2:2003 を引用するが、正式改定後は最新の内容を参照されたい。

妥当性検証の結果、ISO 13849-1:2006 及び ISO 13849-2 に従って、MTTF_d、DC、CCF 等の条件を満たし、PL=e (Cat.4) に適合していると判断された急停止システムは、以下の特性を有することができる。

- 単一障害では安全機能を損なわない。
- 障害は安全機能要求前か要求時に必ず検出できる。
- 検出できない障害は蓄積するものとして考慮されている。

そして、以下に掲げるような障害状態は残留リスクとして考慮され、その平均発生確率が十分に低いことから許容される（ISO 13849-1:2006 では $10^{-7}[1/h]$ 未満とされる）。

- 一方の系が検出可能な故障を生じたとき、これを検出するまでの間又はこの状態で機能要求があって安全機能を開始するまでの間に他方が故障すること。
- 一方の系が検出できない故障を生じたとき、これがブルーフトテスト（定期自主検査のようなフルメンテナンスを含むテスト）で発見されるまでの間に他方が故障すること。
- 1 つの原因（共通原因）で両方の系が次の機能要求までの間に故障すること（ただし、ある障害の結果として他のコンポーネントが続けて故障する場合は最初の障害に続くすべての障害は単一障害と見なす。ISO 13849-1:2006 簡条 7.2 参照）。

すなわち、検証の結果から PL=e (Cat.4) に適合すると認められた急停止システムにおいては、前回の急停止時に冗長系の両方が健全であることが確認されれば、次の急停止要求時（安全機能作動要求時。このとき又はその前までに故障が検出されることが Cat.4 の条件である）には必ずどちらか一方は健全であると見なしてよい（動作要求は高頻度である）。そして、仮に一方が故障した状態で急停止要求があり、健全なもう一方の系だけがこれに応じて急停止している場合、この急停止動作が完了する前に健全な系も故障してしまう事態まで考慮する必要はない。PL=e (Cat.4) に適合した急停止システムでは、以上のような事態は想定されるも、その発生は極めて希であるとして残留リスクとして扱われるのである。

このことは、ISO 13849-1:2006 と同様に安全関連システムの条件を扱う JIS B 9961 でも示されている。JIS B 9961 に従えば、PL=e (Cat.4) と同等の SIL 3 のシステムの典型的構造である“冗長化+自己診断”の構造をもつ系は、図 4 のようにモデル化される。ここで、 λ_{De1} と λ_{De2} は各々

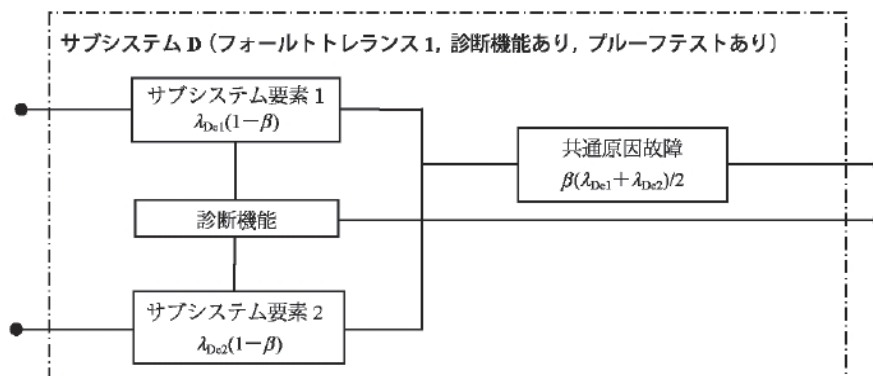


図 4 “冗長化+自己診断”の構造をもつ系 (JIS B 9961 図 9)

のサブシステム（チャンネル：これは複数のコンポーネントで構成される）の危険側故障率、 β は共通原因故障係数である。議論を容易にするために、サブシステム 1 とサブシステム 2 が同じ設計であると仮定して λ_{De1} と λ_{De2} の値が共に λ_{De} であるとする、JIS B 9961 では、システム全体の危険側故障率 λ_{DssD} [1/h] を次式で推定する（箇条 6.7.8.2.5 式 D.2）。

$$\lambda_{DssD} = \left\{ (1 - \beta)^2 \times \lambda_{De} \times [DC \times T_2 + (1 - DC) \times T_1] + \beta \right\} \times \lambda_{De} \quad \cdots(1)$$

ここで、 DC は診断範囲（すべての危険側故障のうち周期的に実行する自己診断で検出できる危険側故障の割合で、例えば 0.99）を表し、これ以外の $1 - DC$ はプルーフテストで発見されるとしている。また、 T_2 は自己診断の診断間隔、 T_1 はプルーフテスト間隔である。

SIL 3 の要件では、サブシステムの危険側故障率 λ_{DssD} [1/h] は 10^{-7} [1/h] 未満でなければならぬが、これに対し、式(1)では T_2 がかかる項で“一方の系が故障してから次の自己診断の前にもう一方の系が故障する場合”を、 T_1 がかかる項で“一方の系が故障してから次のプルーフテストの前にもう一方の系が故障する場合”を、 β がかかる項で“共通原因で両方の系が一度に故障する場合”を計算している。つまり、JIS B 9961 では、別々の原因から両系に故障が発生する場合については危険側故障の算出に含めてなく、あくまでも、以上の 3 つの場合を危険側故障として検証の対象にしているのである。

注記 5) λ_{De} は 1 つのチャンネルの（瞬間）危険側故障率、 λ_{DssD} はシステム全体の（瞬間）危険側故障率である。急停止システムの不信頼度ではなく、また、急停止の要求に対して急停止システムが機能を失敗する率でも、単位時間当たりの災害発生率でもない。なお、SIL の要件には構造上の制約（SFF：安全側故障率）もあって、単に λ_{DssD} が低いことだけでは SIL を達成できない。

注記 6) 危険側故障率 $\lambda_{DssD} < 10^{-7}$ [1/h] の要求は、安全機能を実行するシステム全体の危険側故障率の要求であって、コントローラのみに対する要求ではない。システム全体に占める割合を考慮して、コントローラの目標として 10^{-7} [1/h] よりも 1 桁以上小さい値を設定する場合もある。

2.1.4 単一障害の発生タイミング

以上のように、急停止時間の決定では、急停止システムに要求されている PL（カテゴリ）で許容される障害発生状態はワーストケースに含める必要はない。これに対して考慮しなければならない単一障害については、それが最も急停止時間が長くなるタイミングで発生することを想定しなければならない。すなわち、

- 1) 対象とする単一障害が起こっている状態で保護装置から急停止の開始が要求された。
- 2) 急停止要求があり、機能が開始した時点までは障害がなかったが、急停止が完了するまでの間（すなわち、急停止動作中の任意の時点）で対象とする単一障害が起こった。

という 2 つのタイミングを想定して急停止時間を評価する必要がある。

2.2 非常停止ならびに監視機能による急停止での停止時間

JIS B 6410 における停止機能の分類を表 1 に示す。以下では、各停止機能と急停止時間条件との関係について述べる。

表 1 停止機能で規定する要求事項の要約 (JIS B 6410 表 1)

停止機能	機能要求／開始	停止 カテゴリ	保持時の 電源遮断	保持時の 制動機構	注記 (関連する細分箇条)
非常停止機能	手動による	0 又は 1	実行	作動	5.4.2
急停止機能	監視機能による	0 又は 1	実行	作動	5.4.3.2
	保護装置による	0 又は 1	実行	作動	5.4.3.3 a)
		—	—	作動	5.4.3.3 b)
通常停止機能	プログラムによる， 意図した操作による	0 又は 1	実行	作動	5.4.5.2
		—	—	作動	5.4.5.3
		2	—	—	5.4.5.4
注記 “—” の項目は、この規格では規定しない。					

注記 7) 十分な制動能力を有する制動機構を持つために保護装置による急停止で電源遮断を必要としないサーボプレス（いわゆる F 型）においても、サーボシステム等のシステムに何らかの異常や故障を生じて監視機能により急停止する場合は電源遮断が必須である。

2.2.1 非常停止機能における停止時間

“非常停止機能” については、JIS B 6410 の箇条 5.4.3 b) でリスクアセスメントに基づいた適切な安全性能の達成が要求されているが、急停止時間条件のように停止時間に関わる規定は設けられていない。これは、保護装置（ライトカーテン、両手操作制御装置等）と異なり、非常停止ボタンの設置位置の決定が安全距離という概念の条件で制約されないことに基づく。すなわち、急停止時間条件は保護装置による急停止についてのみ要求される。非常停止装置が操作された場合は、可能な限り迅速に危険な作動を停止することが求められることに違いはないが、その際の停止時間を表示する必要はない。

このように JIS B 6410 には基準・規定がないため、非常停止機能の応答時間に関わるリスクについては、各々のメーカーが独自にリスクアセスメントを実施して検討する必要がある。少なくとも次の事項については、該当する場合、何らかの措置が必要である。

- － 非常停止時の停止時間が表示した保護装置による急停止時間よりも長いために危害を生じる又は危害が拡大する可能性
- － 単一障害下、あるいは、特定の環境条件下で、非常停止が機能しない又は停止時間が延長したために危害を生じる又は危害が拡大する可能性
- － 非常停止装置が不適切な位置に取り付けられている、あるいは、他の操作ボタンと見分けがつかない等の理由から、予見可能な作業位置で非常停止装置を操作するのに過大な時間を要するために危害を生じる又は危害が拡大する可能性

2.2.2 監視機能による急停止時間

JIS B 6410 箇条 5.6.2 で規定されている起動／停止監視として、あるいは、例えば急停止にサーボシステムを使用する場合にはエラー検知機能など、必要に応じてその他急停止機能に関わる障害を検出するために監視機能が備えられる。

監視機能による急停止については、このときの急停止時間を評価する必要はない。なぜなら、監視機能によって開始される急停止とは、ある特定の単一障害発生状態で保護装置よりも先に急停止機能を開始したことに他ならず、このような障害発生状態での急停止時間については 2.1 節で述べてきた保護装置による急停止のワーストケースの評価の中で当然検討されなければならないからである。すなわち、

- a) ある単一障害が発生しているときに、
 - a-1) 保護装置が作動する前に監視機能が障害を検出し、急停止を開始した
 - a-2) 監視機能が障害を検出する前に保護装置が作動し、急停止を開始した
→ いずれも前述 2.1.4 項の 1)と同じ
- b) 障害がない状態で急停止が要求されたが急停止の途中で単一障害が発生した場合で、
 - b-1) この急停止は保護装置が開始した → 前述 2.1.4 項の 2)と同じ
 - b-2) この急停止は監視機能が開始した → すでに別の障害が発生している状況であって、2.1.3 項で述べたように想定する必要はない。

となり、保護装置による急停止での検討が十分なされていれば、監視機能による場合の急停止時間を保護装置の場合と区別して改めて評価する必要は本来ないはずである。

注記 8) 本研究では急停止システムに PL=e (Cat.4) が要求されていることを想定しており、このため、監視機能自体もこれに準じ、単一障害では監視機能を損なわないとの前提に立っている。

2.2.3 監視機能の例外

ただし、次の 2 つの監視機能については、保護装置による急停止において、監視対象である故障や異常を検出するまでの遅れ時間(周期的な監視を行っている場合には監視実行間隔又は自己診断間隔)が急停止時間に大きく影響する恐れがある。

- ・ スライド速度の監視 (サーボ異常によるオーバースピードの監視) → 後述 3.1 節参照
- ・ エアバランスの正常性監視 (内圧又は供給圧の監視) → 後述 3.3 節参照

このため、上記 2.2.2 項で述べた解釈には含めず、急停止時間条件の検討の中で監視実行間隔の影響を考慮に入れなければならない。具体的な取り扱いについては次の第 3 章で詳述する。

また、次のようなサーボシステムの監視も診断間隔やサンプリング周期を考慮する必要がある場合があり、その取り扱いについては第 5 章 5.5 節で詳述する。

- ・ 正常時には停止カテゴリ 1 で急停止を行うサーボプレスにおいて、減速制御中、サーボシステムの異常を検知して停止カテゴリ 0 の停止に切り替える場合

2.3 急停止時間の定義

JIS B 6410 の規定をまとめると、急停止時間は次のように定義される。

急停止時間：急停止機能の作動要求があつてから次の a)～c)のすべてを達成するまでの時間

- a) スライドの移動速度を 10 mm/s 以下に減速している。
- b) 制動機構を作動している。
- c) 停止カテゴリ 0 又は 1 の停止として機能する場合、電源遮断を行っている。

以下、順に各々の解釈を示す。

2.3.1 急停止機能の開始

JIS B 6410 において、急停止時間は「JIS B 9715 の定義 3.2 の総合システム停止性能における“機械の最大応答時間 t_2 ”に相当する時間」とされる（図 5 参照，動力プレス機械構造規格第 50 条においては T_s ）。

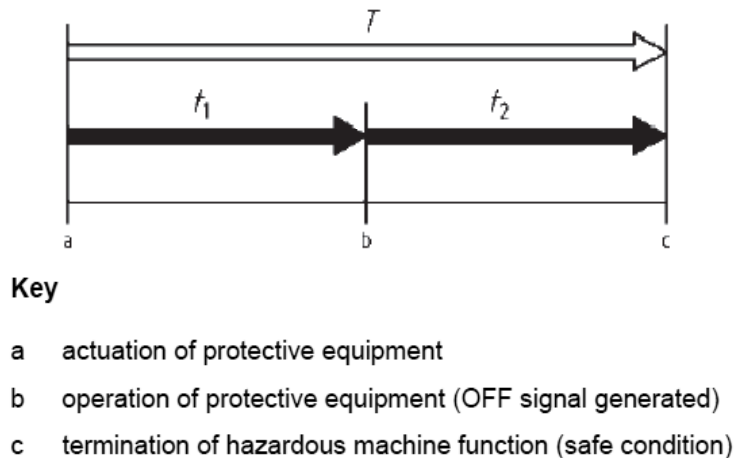


図 5 総合システム停止性能の定義

したがって、保護装置による急停止の場合，“急停止機能の作動要求”とは，保護装置の出力信号開閉機器が OFF した瞬間（図 5 の b 点）である。例えば，ライトカーテンの OFF 信号が入力されてからエア式メカブレーキの空気圧を抜く電磁弁のコイル電流を遮断するまでのプレスコントローラの遅れ時間，あるいは，OFF 信号が入力されてからプログラムシーケンスが急停止機能に処理が移行するまでのプレスコントローラの遅れ時間は t_2 に含まれる。このような遅れ時間には，処理速度の限界から生じるものの他，意図的にディレーがプログラムされている場合もある。

前述の安全関連ブロック図を用いて言えば，急停止時間の検討で対象となるのは“L”と“O”が機能に要する時間である。これは「I」（例えば，ライトカーテン）には危険を検知してからの応答時間 t_1 （動力プレス機械構造規格第 50 条においては T_I ）が製品の仕様として明示されているので，安全距離によって確保しなければならない総時間 T のうち，残りの“L”と“O”にあたる t_2 についてはサーボプレス側で表示する必要がある」という趣旨である。図 5 の b 点の位置を図 3 のインターロックシステム例で示せば，図 6 のようになる。

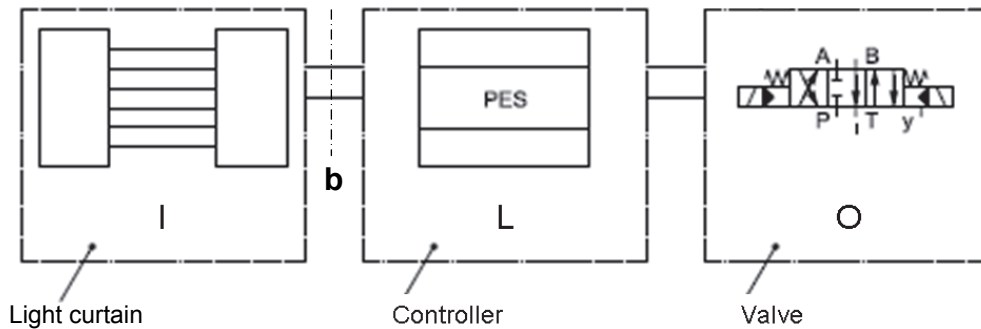


図 6 安全関連ブロック図での作動要求時 (b 点)

一方、監視機能による急停止については、2.2.3 項に掲げたものを除き、その急停止時間を評価する必要はないので、この場合の急停止機能の作動要求に関してはここでは論じない。ただし、一般的に $PL=e$ (Cat.4) の要求への適合を目標にするシステムの場合、故障検出までの遅れ時間、すなわち、自己診断機能の実行間隔（診断間隔）が問題となるのは 2.1.3 項で述べたように、この遅れ時間の間にもう一方の系も故障して安全機能を完全に喪失する危険側故障であって、結局、診断間隔はシステムを構成する各コンポーネントの故障率（信頼性）に応じて定まる。

注記 9) 診断間隔を決定する方法として、例えば 2.1.3 項で示した式(1)を利用する場合、国内のプレスの運用においては年に一度の自主検査が前提となるので、これをプルーフテスト間隔 T_1 と考え、 $T_1 = 8760$ 時間（あるいは、明確な根拠がある場合には年間の総稼働時間：例えば、2 シフト $\times$ 20 日 $\times$ 12 ヶ月 $= 3840$ 時間）とおき、さらに、対象としているコンポーネントの危険側故障率 λ_{De} と共通原因故障係数 β を代入すれば、設計目標に対して必要な診断間隔 T_2 を導出できる。

注記 10) JIS B 6410 の箇条 5.6.3 で規定されているオーバラン監視による急停止での急停止時間は「通常停止で設定された許容範囲での停止（すなわち、ノーマルな停止）ができなかったことを検出した」時点から「急停止を完了した」までの時間となる。ただし、箇条 5.4.5.5 “追加要求事項” に該当する場合は、「スライドの行き過ぎ量（オーバーシュート）が設定ストローク長さの 2 %を超えたとき」からとなる。

2.3.2 条件 a) スライドの減速

スライドが減速して特定の低速度になった瞬間をスライドの停止とする趣旨であり、10 mm/s 以下は現行の動力プレス機械型式検定ガイド¹⁾に準じた値である。

前述したように、サーボプレスにおいては種々の電氣的制動機構を利用できるため、この状態を実現する方式は複数考えられるが、実際の条件 a) の検証では、従来から機械プレスで使用されている急停止測定装置を利用することが可能である。

2.3.3 条件 b) 制動機構の作動

JIS B 6410 では、急停止においてサーボシステムの制御によるスライドの保持（停止カテゴリ 2 の停止）を認めていない。このため、スライドは必ず制動機構によって保持される必要があり、

その保持した時点をもって急停止動作の完了とするという趣旨である。厳密な解釈では保持力が発生した瞬間を指すが、等価的に、機械的制動機構についてはバネによってブレーキ面やシューが所定の位置に移動完了した時点、また、液圧的制動機構についてはロックのための電磁弁が閉じ側に作動完了した時点として解釈してもよい。

実際の条件 b) の検証では、特に機械的制動機構については、ブレーキの機械部分の動作遅れを考慮した上で排気バルブが作動完了した時点から換算する方法も考えられる。

2.3.4 条件 c) 電源の遮断

十分な制動能力を有する制動機構により実行するために電源遮断を必要としないサーボプレス（いわゆる F 型）の保護装置による急停止の場合を除き、急停止中又はスライドの減速が完了した後にサーボシステムの電源（動力）を遮断しなければならない。条件 c) はこのサーボシステムの電源遮断の完了を急停止動作の完了に含めるとする趣旨である。

注記 11) F 型においても、サーボシステム等のシステムに何らかの異常や故障を生じて監視機能により急停止する場合は電源遮断が必須である（JIS B 6410 表 1 参照）。

実際の条件 c) の検証では、サーボモータの電流（インバータ二次側電流）を計測して検証するのが望ましい。ただし、コンタクタを遮断に利用する場合は、主接点の開放（例えば、バックチェック用ミラー B 接点の ON）によって検証してもよい。一方、インバータ回路遮断（ベース電流遮断、ゲート OFF 遮断）を用いる場合は、遮断機能が作動して動力遮断が実行されたことを検証するにはサーボアンプの特性を勘案した何らかの工夫が必要になる場合がある。

注記 12) 動力遮断機能の冗長化の 1 つとしてインバータ回路遮断を利用する急停止システムにおいては、接触器のミラーコンタクトを用いたバックチェックと同じように、インバータ回路遮断が実行される度に正常に機能したことを信頼できる手段/手法で確認できなければ診断範囲 $DC \geq 99\%$ の条件を満たせず $PL=e$ (Cat.4) を達成できない。診断範囲 DC の推定方法については、ISO 13849-1:2006 の附属書 E、ISO 13849-2 の附属書 E 及び JIS C 0508-2 の附属書 A を参照。

3 急停止時間の測定条件

前章で述べたように、急停止時間の延長は急停止システムの安全機能の喪失と見なされる。しかし、急停止時間（特に、スライドを制動するのに要する時間）を延長させる要因には、システムの故障・不具合のみならず、金型重量の増加、使用環境温度、コントローラの情報処理負荷量など種々の条件も含まれてくる。ワーストケースの想定とは言え、あまりに非現実的で過剰な条件の設定では急停止時間を定められなくなるのは明らかである。

そこで、本研究では、これらスライド制動時間を測定する際の条件設定については、EN692 附属書 B での取扱いに準じ、基本的には使用上の情報の一つとして規定した使用条件に基づく正常な運転状況の範囲内で最も厳しい条件を設定することを強く推奨する（同規格 B.4 項参照）。例えば、急停止時間の測定において、金型などのスライドに付加される重量負荷は、設計仕様によって指定した最大値とする。

本章では、EN692 記載項目以外にサーボプレス固有の事項として注意すべき条件に対し、その設定の考え方について述べる。なお、いくつかの条件設定においては、例えば、サーボシステム以外のコンポーネントに障害を仮定しないなど、単一障害の取り扱いにまで言及した事項があるが、これらは従前の機械プレスの急停止時間測定の実情を踏まえた上で国内において JIS B 6410 に基づいて急停止時間を評価する方法としての本研究の見解であることに改めて留意されたい。動力プレス機械構造規格での急停止機構の故障の取り扱い、あるいは、EU 機械指令の型式試験において急停止システムの安全性能（PL、カテゴリ）の評価に関して解釈を示したものではない。

3.1 急停止時のスライドの速度

測定において、急停止機能の開始タイミングは、スライドが最大速度で作動しているときでなければならない。このときの最大速度は、基本的には、意図する使用においてプログラム設定可能な範囲での上限速度（いわゆる使用最大速度）と設定してよい。

ただし、急停止時間条件で検討する単一障害の 1 つとして、保護装置より急停止命令がなされる前にスライドの運動を制御しているサーボコントローラ（あるいは、NC コントローラ）に異常を生じて、設定した（プログラムした）速度範囲が破られる状況は想定しなければならない。この状況でのスライドの下降速度は、サーボモータの回転速度を監視する速度監視機能の有無、ならびに、サーボプレスに使用されているサーボドライブシステムの数が大きく影響する。そこで以下の 4 つの場合に分けて扱う。

注記 13) JIS B 9715 の基である ISO 13855 は 2010 年 4 月に改定され、第 2 版では附属書 D の箇条 D.1 において、機械の最大応答時間 t_2 を決定する際の機械作動部の動作速度に関して“故障を生じている状況は考慮せずに通常使用で設定された（プログラムされた）値を条件とする”ことを当該規格での原則としつつも、特定の機械における具体的な故障状態の取り扱いについては“各々の機械の個別規格（タイプ C 規格）で扱うべき問題である”とし、特段の規定は設けられていない。本研究では 2.1.1 項で述べたように 1) 急停止時間の延長は安全機能の喪失とみなされること、ならびに、2) 機械サーボプレスの急停止システムには一般に PLr=e (cat.4) が要

求されることを考慮し、本項で述べるように“保護装置から急停止命令がされる前にサーボコントローラ等に異常を生じて設定した速度範囲が破られる状況”は急停止時間の決定において考慮しなければならない条件の1つとした。

注記 14) 本項の議論は、現状のサーボドライブの技術水準を踏まえ、PL=e (Cat.4) に適合できるシステムとしてはあくまでも速度を監視する機能（すなわち、異常速度が発生した場合にこれを検知して動力遮断して停める機能であって、速度を任意に制御することとは本質的に違う）を実行するのが限界であろうとの前提に立ったものである。したがって、仮に PL=e (Cat.4) に適合できる速度制御機能を備えたサーボシステムを実装したサーボプレスが実現された場合、これについては本項はあたらず、別途個別に検討すべきである。

(1) 速度監視を行っていない場合

サーボシステム異常時の急停止時間測定でのスライド速度は、スライド動作機構の構造、動力伝達機構の構造及びサーボモータの能力的制約から、無負荷状態で物理的に発生し得る最大速度とすべきである。ただし、このような作動状態を実験することは一般に非常に困難である。1つの方法として、実験可能な範囲での最大速度で得た測定結果から機構等の制約を考慮して理論的に外挿することで制動時間を推定することが考えられる。

なお、この条件では、既にサーボシステムの制御に異常が起こっている状態であるので、サーボシステム以外のコンポーネント（例えば、メカブレーキ、エアバランサ等）は正常であると仮定してよいが、有効な急停止機能は停止カテゴリ 0 の停止としかなり得ない。

(2) サーボコントローラの自己診断機能のみで速度監視を行っている場合

サーボシステムの運動制御を行うサーボコントローラ（もしくは NC コントローラ）には、速度超過や偏差過大といった異常状態を検出する目的で自己診断機能を備えたものが多い。しかし、いわゆる標準機能として備わる自己診断機能は、処理系ばかりでなく、エンコーダ等の回転速度検出手段も含めて単一系として構成され、構造要件として Cat.4 を（あるいはカテゴリ 3 すら）満足しないものが多い。さらに、その診断有効性も低いものとされ、診断範囲 DC は 30%~60%程度とされる²⁾のが一般的である。

以上のことから、速度超過のような不具合状態にあるサーボコントローラの診断機能がその不具合の影響を受けずに正常に機能することは必ずしも期待できないため、FMEA 等に基づいてサーボコントローラの安全性能が特別に検証されている場合を除き（このときは次の (3) に該当する）、サーボシステム異常時の急停止時間測定でのスライド速度は、前述 (1) と同様に設定すべきである。

なお、この条件では既にサーボシステムの制御に異常が起こっているため、サーボシステム以外のコンポーネント（例えば、メカブレーキ、エアバランサ等）は正常であると仮定してよいが、有効な急停止機能は停止カテゴリ 0 の停止としかなり得ない。また、以上のことは、1つのサーボモータで駆動されるサーボプレスの場合を述べたものであり、複数のサーボモータで駆動されるサーボプレスの場合については (4) で述べる。

(3) 妥当性が検証された監視機能で速度監視を行っている場合

サーボコントローラとこれと独立したコントローラとで冗長化して速度監視を行う構成であって、平均危険側故障時間 $MTTF_d$ 、診断範囲 DC、共通原因故障対策等の必要な PL（カテゴリ）の要件を満足している場合、あるいは、サーボシステムとは別に製品として必要な PL（カテゴリ）への適合を宣言しているサーボコントローラや速度監視ユニット³⁾を用いている場合などにおいては、単一障害の発生で監視上限速度を越えた速度でサーボドライブが作動し続けることを想定する必要はないと言える。

ただし、この場合には、サーボドライブの異常動作を検出するまでの間に、既に速度が監視上限を超過してしまっていることは想定する必要がある。よって、この場合での急停止時間測定でのスライド速度 v [m/s]は、次式で設定すべきである。

$$v = v_{limit} + T_{test} \times a \quad \cdots(2)$$

ここで、 v_{limit} は監視機能で設定したスライドの下降速度の上限値[m/s]、 T_{test} は v_{limit} を超えた速度が発生した場合にその発生からサーボ電源遮断するまでの遅れ時間の推定最大値[s]、 a は T_{test} の間に想定されるスライドの最大下降加速度[m/s²]で正の値である。すなわち、式(2)は、異常な速度を検出した時点で、既にその前から速度が監視上限から逸脱していた場合があることを考慮して、その最悪の状況を想定することを表している。例えば、速度監視が一定周期で実行される場合には、 T_{test} は監視機能のチェック間隔[s]やサンプリング周期[s]に電源遮断の遅れ（コンタクタの動作時間あるいはインバータ回路遮断）を加えた値と考えられる。また、最大下降加速度 a の見積もりでは、モータの起動トルクで駆動されている条件でのスライド下降加速度[m/s²]を仮定してもよい。

注記 15) 別途、技術的な根拠に基づき、速度異常が一旦検出されれば、その後はモータが加速することを考慮しなくてもよい場合には、 T_{test} を監視機能のチェック間隔[s]やサンプリング周期[s]のみとしてもよい。

注記 16) サーボシステムの異常が発生してからこれを検出するまでの遅れ時間は、スライド速度 v [m/s]に影響するが、急停止時間には含めない。2.3.1 項で述べたように、この場合の急停止時間は「速度異常を検出した」時点から「急停止を完了した」までの時間となる。コンタクタの動作時間は急停止時間に含まれる。

なお、この条件では既にサーボシステムの制御に異常が起こっているの、サーボシステム以外のコンポーネント（例えば、メカブレーキ、エアバランサ等）は正常であると仮定してよいが、有効な急停止機能は停止カテゴリ 0 の停止としかなり得ない。

また、速度監視機能に要求される安全性能は、ISO 13849-1:2006 の附属書 A に従ったリスクアセスメントの結果に則して定めてもよいが、後の 3.8 節で述べる理由から、本研究では急停止システムと同等のレベル（本研究の前提の下では PL=e (Cat.4)）とすることを強く推奨する。

注記 17) 現在のところ、市場において PL=e (Cat.4) への適合を認証されている速度センサ（エンコーダ）や速度監視ユニットは一般的ではなく、PL=e (Cat.4) に適合した速度監視を実現することが極めて困難な状況であるのは事実である。しかし、3.7

項に後述するように速度監視機能の要求安全性能は急停止システムと同等と考えるのが妥当であり、また、技術的にも達成不可能な課題とは言えないと考えている。

(4) 複数のサーボモータで駆動されるサーボプレスの場合

各々独立したサーボコントローラで制御される複数のサーボモータが機械的に連結した構造のサーボプレスにおいて、仮に 1 つのサーボシステムが使用最大速度を逸脱するような異常作動をし、さらに、この異常が故障したサーボコントローラの自己診断機能で検出されなかったとしても、他のサーボシステムの作動との調和が乱れてスライドがロックするので結果的に危険な作動を防止できる場合には、擬似的に 1 つのサーボシステムを誤動作させてロックするまでの時間をもって急停止時間としてよい。このときの時間は、一般的には、他の条件での急停止時間よりも短くなると考えられ、その確認が得られれば、以後は検討から除外してよい。

また、このとき、コントローラは標準仕様のものであってもよい。これは、各々のサーボコントローラに搭載された自己診断に一定の評価を与えているのではなく、複数のサーボシステムが強調して動作する構成では、いかなる単一障害を仮定しても、少なくとも 1 つのサーボシステムは正常な作動をしているので、その結果、スライドのロックという機械的な不一致検知によって異常が必ず露呈すると言えるからである。

したがって、複数のサーボシステムを用いていても、

- 一方が主、他方が従の関係にあるマスタスレーブ系など、サーボシステム間の作動状態の不一致を許容するようなシステム構成である場合、
- 複数のサーボシステムを統率する上位コントローラが、I/O 回路の故障、CPU の異常、プログラムバグ等の単一障害によって、例えば誤った速度指令を出力する等、1 つの原因ですべてのサーボシステムが一度に異常作動する共通原因故障が想定される場合、
- 同型のサーボアンプを用いているために特定周波数の電磁ノイズや電源変動に対して共通の反応を示した結果、あるいは、同型のサーボコントローラを用いているためにスライドの振動的作動等に対して共通の応答を示した結果が異常作動につながる場合、

には、ここで意図する安全性能は達成できないので、単一障害で速度制限機能が失われることを前提として、その取り扱いは上述の (1) ～ (3) に照らして考えなければならない。

なお、スライドが突然ロックすることに起因した危険事象（例えば、金型の落下やスライドの破断）については別途そのリスクを解析評価する必要がある。

3.2 ボールスクリーを用いたサーボプレスの速度設定

サーボモータの動力をボールスクリーによってスライドに伝達するサーボプレス、あるいは、スピンドル式のサーボシステムを用いるサーボプレスにおいては、急停止時間測定の際、定格速度に達するまでスライドを下降させた時点で急停止信号を OFF 入力すると、機械ブレーキ等によってスライドが 10 mm/s 以下に減速（停止）する前にストロークの最下限に到達してしまう場合がある。

このようなサーボプレスにおいては、急停止動作の過程で最下限に達した後スライドが再び上

昇に転じて作動を継続してしまう構成のものを除き、スライドがストロークの最下限に達した時点で構造的に“スライドの停止”が達成されたと見なせる。このため、このようなボールスクリーンを用いたサーボプレスについては、急停止時間測定でのスライド速度は、最大ストローク内でスライドを 10 mm/s 以下に減速可能な（停止可能な）範囲の中での最大速度（例えば定格速度の 70%程度など）を設定してよい。

ただし、一般に急停止を停止カテゴリ 0 の停止として行うサーボプレスではストローク下限に達してもなおスライドの動作が継続することは原理的に想定されないが、これに対して、停止カテゴリ 1 の急停止を行うものにおいて上記を適用するには、サーボシステムを含む急停止システムの詳細な故障解析によって急停止動作の過程で最下限に達した後スライドが再び上昇に転じないことを検証する必要がある。また、速度監視機能を備えていることを理由に、プログラムされたさらに低い速度を設定する場合の扱いは 3.1 節に準じる。

3.3 エアバランサの内圧

急停止時間の測定において、エアバランサ内圧は、原則、設計仕様に従った正常範囲内の下限又は上限の圧力（停止時間が長くなる方の値）に設定してよい。ただし、急停止時間条件で検討する単一障害の 1 つに、エアバランサの故障、すなわち、エアバランサ内圧が低下したために重量補償能力が低下することは含めなければならない。

次の第 4 章で述べる“障害除外”の条件がすべて適用できるよう基本的な工学の原則に従って適切にエアバランサ及び関連空圧システムを設計製造しても、エアバランサのピストン内圧の低下を引き起こす障害として次のことは考慮しなければならない。

- 空圧供給系の機能停止
- 配管接続機器又は配管接続シール部分からの漏れ
- 調圧弁等の圧力機器での漏れ

ただし、ここで重要なことは、これらによる圧力低下は“ある程度の時間を要して徐々に進展する事象”として扱えるということである。基本な安全原則に従って適切に設計されており、かつ、始動前に点検され、通常運転での毎回の上昇過程で機能を果たしているエアバランサにおいて、突発的に圧力が喪失するような事態（例えば、シリンダの破裂）はこれまでに経験されたことがない（機械部品及び空圧機器が満たすべき基本安全原則については第 4 章で述べる）。

以上を考慮し、エアバランサ内圧を圧力スイッチ等によって連続的に監視している場合、すなわち、特にサンプリング周期などを設けておらず、コントローラの処理内容に関わりなく圧力低下時に直ちに急停止を開始するような構成のサーボプレスの場合では、エアバランサのピストン内圧低下時の急停止時間測定においては、内圧を監視圧力値に設定して測定してよい。ただし、圧力監視機能は、少なくともリスクアセスメント結果に従った安全性能に適合していなければならない。3.8 節に後述する理由から本研究では急停止システムと同等のレベル（本研究の前提の下では PL=e (Cat.4)）とすることを強く推奨する。これに対し、圧力監視機能の安全性能が要求されるレベルにない場合は、後述する圧力監視機能を備えていない場合として扱う。なお、この条件ではエアバランサ以外のサーボシステムを含むコンポーネントは正常であると仮定してよい。

注記 18) センサ配置位置や配管等の関係から、エアバランサのピストン内圧の変化を圧力検知装置で検知する遅れが無視できない場合には、これを連続監視とは扱わずに、次に述べる“異常を検出するまでの間に既に内圧が低下している想定”に準じる。

注記 19) 従前の機械プレスにおいても急停止時間にバランサ圧が影響することは周知されているが、現在のところ、PL=e (Cat.4) の自動監視機能として確立・要請されるまでには至っていない。また、市場を見ても、現在のところ、高 PL (あるいは高カテゴリ) への適合を認証されている圧力センサは一般的ではなく、PL=e (Cat.4) に適合した圧力監視を実現することが極めて困難な状況であるのは事実である。しかし、3.8 節に後述する理由から、監視機能の要求安全性能は急停止システムと同等とするのが妥当で、また、技術的にも達成不可能な課題とは言えないと考えている。

一方、3.1 節 (3) で述べたのと同様に、周期的に内圧を監視する場合では、異常を検出するまでの間 (例えば、サンプリング周期、あるいは、センサ配置位置や配管等の関係から生じるエアバランサのピストン内圧の変化を圧力検知装置で検知遅れの時間) に既に内圧が下限値よりも特定の割合で低下していることを想定する必要がある。このため、式(2)を準用し、エアバランサ内圧低下時の急停止時間測定においては、エアバランサのピストン内圧 P [Pa] を次式で設定する。

$$P = P_{limit} + T_{test} \times b \quad \cdots(3)$$

ここで、 P_{limit} は監視機能で設定したエアバランサのピストン内圧の下限値[Pa]、 T_{test} は内圧が P_{limit} を下回ってからこれを検知するまでの最大の遅れ時間[s]、 b は T_{test} の間に想定される毎秒当たりの最大内圧低下率[Pa/s]で負の値である。 b [Pa/s]を与える指標として、1 つは、コンプレッサの停止後の圧力低下率 (負の値) [Pa/s]がある。他には、例えば、エアバランサ及びタンク、アキュームレータを含む関連空圧系に P_{limit} の内圧を充填した状態で、空圧源からエアバランサまでのうち何れか 1 つのネジ接続された配管接続部を締め付け力を規定値の半分まで緩めてエア漏れさせる実験を行い、最も急速にエアバランサのピストン内圧が大気圧に達したときの圧力低下率 (負の値) [Pa/s]も考えられる。なお、前段落で述べたのと同様に、この条件ではエアバランサ以外のサーボシステムを含むコンポーネントは正常であると仮定してよい。

注記 20) 厳密には、内圧低下を検出した後も、サーボ減速制御が開始するまでの遅れ、あるいは、機械ブレーキが機能するまでの遅れ、さらに、その後にスライドが停止し急停止が完了するまでの間においても内圧は減り続けるが、本研究ではこれらは無視できるとした。

エアバランサ内圧をPL=e (Cat.4) の機能で監視していない場合でも、通常運転中、毎回の通常停止の度に、スライドが上昇できたという結果をもってエアバランサのピストン内圧が確認されている (これをプロセスによるモニタリングと呼ぶ) と考えることができる。このため、上式の P_{limit} [Pa] をスライドを上昇できる最低の内圧[Pa]とおき、 T_{test} [s]を通常の使用で想定される最長ストローク周期[s]とにおいてピストン内圧 P [Pa]を設定する。これに依らず、急停止時間を実験で定める方法として、スライドを上昇できる最低の内圧がエアバランサにかかっている状態で、スライドを

上死点から下降させ、スライド速度が最大に達したタイミングで、何れか1つのネジ接続された配管接続部の締め付け力を規定値の半分まで緩めてエア漏れさせ、急停止時間を測定する方法も考えられる。ただし、上昇可能な最低内圧は金型重量の違いで変化し、また、急停止時間も金型重量に依存するので、緩める配管接続部ばかりでなく、これらの条件のあらゆる組み合わせを検討し、ワーストケースを特定する必要がある。

なお、エアバランサの内圧低下については、2.2.2 項の a)に該当する“急停止機能が開始する前に既に障害が生じていた”場合のみを考慮すればよい。上述したように、圧力低下は発生から時間がより経過したほうがより影響が大きいので、急停止動作中にエアバランサに障害が生じた場合よりも、すでに障害が生じていた場合のほうが、急停止時間が長くなることが明らかであるためである。

3.4 機械的制動機構（メカブレーキ）の摩擦面の摩擦

メカブレーキで考慮すべき単一障害の詳細については次の第4章で述べる。ただし、ブレーキシュー等の摩擦面の摩擦や劣化による急停止時間の延長については、特定自主検査での扱いも含めて従前の機械プレスに準じて扱うのがよく、表示する急停止時間に適切に反映することが望ましい。

3.5 エア式メカブレーキのエア排気時間の影響

エア式メカブレーキでは、エア排気時間が作動遅れの1つの要因となる。エア排気時間については、通常の使用で合理的に想定される範囲で、これが最大となる状況を想定すべきである。この意味で、かかるエア圧と排気時間との関係は十分把握されていなければならない。

排気管に備えられた消音器の影響、急速排気バルブの不具合は、次の第4章で述べる障害除外に該当しない限り、急停止時間の延長を検討する際に検証すべき単一障害に含まれる。

3.6 温度条件

メカブレーキ、あるいはサーボシステムの電子機器では、温度の影響で制動性能や遅れ時間が変化する可能性がある。このため、スライド制動時間のみならず、電源遮断時間やブレーキ作動時間を含め、急停止時間を決定するにあたっては、通常の使用で想定される温度範囲の中で最も厳しい条件を設定しなければならない。特に、温度変化で制動性能が激変することが判明している場合には、想定範囲を外れた高温や低温のときは、これを検知して急停止機能を開始する温度監視機能を実装することが望ましく、少なくとも使用者にこのような状況での使用を制限する警告を使用上の情報として提供する必要がある。

3.7 情報処理負荷

規格に従えば、急停止システムのコントローラ部が実行する情報／論理処理は、安全関連部として生産に関わる標準機能での処理とは分離独立すべきである。しかし、現実には、標準機能との同調や連携、あるいはシステムの余裕の観点から、例えば標準機能部との相互通信などが実装されている場合もある。安全性能の妥当性検証において考慮されてさえいれば、このようなシステム構成を採用すること自体に問題はない。ただし、このような情報処理負

急停止を停止カテゴリ 1 の停止で実行する急停止システムの例を図 7 に示す。あくまでも基本要素のみを抜粋して示したものであるが、この例では、ライトカーテンから急停止開始要求として OFF 信号が出力されると、冗長化安全コントローラを介して NC コントローラの制御でサーボによるスライドの減速が実行され、スライド停止後はインバータ内の遮断回路及び安全リレー K を介してインバータ一次側で電源遮断を行い、同時にエア式機械ブレーキを作動させる。ただし、この基本的急停止機能に加え、回転速度監視とエアバルサ内圧監視に関連するコンポーネントも示してある。モータの回転速度は、エンコーダ G1 によって標準 NC コントローラと冗長化安全コントローラにフィードバックされ監視される。冗長化安全コントローラはエンコーダ G2 によりスライド位置も監視しており、クロスモニタリングによって G1 の障害を検出できる。また、圧力供給はユーザー側の設備で行われるとするが、供給圧の異常（供給停止を含む）は 2 つの圧力スイッチによってエアバルサピストン配管接続部近傍で直接監視されている。

前述した「急停止機能」の定義の議論に従えば、図 7 全体で一つの急停止システムを構成していることになる。したがって、この急停止機能の安全性能を検証する際、関連するコンポーネントを安全ブロック図で表現すると図 8 のようになる。

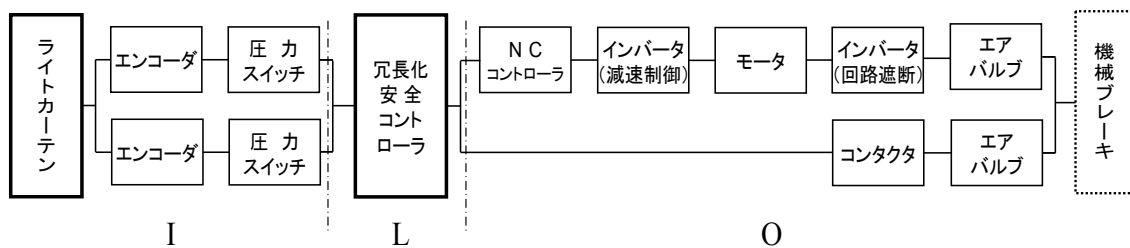


図 8 急停止システム例の安全関連ブロック図

安全関連ブロック図に基づく詳細な解析に関する説明は第 5 章の解析事例で述べるのでここでは割愛するが、仮に急停止機能が PL=e (Cat.4) を要求されている場合、その妥当性検証では図 8 に示すシステムが PL=e (Cat.4) の要求事項である平均危険側故障時間 $MTTF_d$ や診断範囲 DC 等を満足しなければならない。

しかしながら、回転速度監視機能が機能を喪失していても実際に過大な速度での回転をサーボドライブが行わなければ急停止時間の延長は起こらない。エアバルサ内圧監視機能についても同様である。PL=e (Cat.4) の達成では障害の蓄積を考慮しなければならないが、端的に言えば、単一障害が回転速度超過やエアバルサの機能喪失に至らないことが検証されていれば、それら監視のみに関わるコンポーネントを冗長化する必要は無いとも言える。ただし、本研究での調査の結果、現実には、図 8 の例に示したように、これら監視機能に関連するコンポーネントと基本的な急停止に関わるコンポーネントが共通していることが多く、両者を明確に区別して特定することが困難な場合がむしろ一般的である。

以上に鑑み、本研究では、サーボドライブの回転速度監視及びエアバルサの内圧監視に関わる部分を、各々、急停止の基本的な機能に対するサブシステムとして捉えることとし、3.1 節及び 3.3 節で述べたように、回転速度監視を実行するシステム部分及び内圧監視を実行するシステム部分については、それぞれ独立して安全性能を評価検証することとした。これは、これら監視

機能が急停止機能の危険側故障に与える影響の度合いのみならず、厳密に言えば急停止機能と一体のものとして評価すべきこれら監視機能に対し、 $MTTF_d$ に代表されるコンポーネントの信頼性評価よりも監視を実行するサブシステムの構造を重視すべきであるとの考えに依拠した措置である。さらに、この監視機能を分けて扱う考え方を導入することで、第5章の解析事例でも示すように、サーボドライブの異常動作やエアバランサの不具合といった非常に影響の大きい事象を急停止時間決定の際の検証時に個別に扱うことが可能になり、結果、他の障害を整理して解析する上で非常に有効なものと考えている。

一方、これらの監視機能の要求安全性能を本研究では急停止システムと同等とするのが妥当であるとしたが、その理由は、上記のように、本来これら監視機能は急停止機能の一部であるとの考えに沿ったからである。例えば、サーボドライブの回転速度監視について、これを独立した安全機能とし、その安全性能をISO 13849-1:2006 附属書 A のリスクグラフに従って決定するとすれば、各ノードでのリスクパラメータを以下のようにおく考え方もある：

傷害のひどさ： S2 （金型間に手指を挟まれれば、切断される）

危険源への暴露頻度： F1 （サーボドライブの異常動作に曝される頻度は希である）

回避の可能性： P2 （サーボドライブの高速動作に対して回避は困難である）

この場合、以上のパラメータから導かれる要求 PL は $PL_r=d$ である。しかしながら、本来これらの監視機能は急停止機能の一部である。一般に、システムの一部が要求性能を達成できていない場合、それらを接続したシステム全体は要求性能を達成し得ない。この観点から、本研究では、これらの監視機能については、その要求安全性能を急停止システムの要求安全性能と同等とすることを強く推奨した。

注記 21) 上記は、各コンポーネントを直列接続した場合のシステム安全性能について言っている。厳密には、冗長化といったシステムアーキテクチャ次第では総合的評価が個々のコンポーネントの評価を越える場合もあるが、結局この場合にはシステム全体を対象にした解析が妥当性検証で必要になる。

なお、本研究では、特に急停止機能に与える影響が大きいことから、サーボドライブの回転速度監視とエアバランサの内圧監視を取り上げ、それらの取り扱いを示したが、その他にもスライド制動時間を測定する際の設定条件として監視すべき状態／不具合がある場合、それらの監視機能についても同様に扱うのが望ましい。

注記 22) 以上の監視機能の取り扱いは、従前の機械プレスの急停止時間測定の実情を踏まえた上での JIS B 6410 に基づく急停止時間決定法としての筆者の見解である。機能安全に関わる B 規格あるいはプレスの個別 C 規格で明確に規定された場合は、それに従わなければならない。

また、妥当性検証の際にこれらの監視機能を急停止機能とは独立して解析する上記の考え方は、あくまでも、監視する対象である状態／障害がスライド制動時間を測定する際の設定条件として急停止時間に関与する場合に対してのみ適用するものであることに留意されたい。例えば、サーボドライブの回転速度監視に関して、通常は停止カテゴリ 1 の停止で急停止を行うシステムにお

いて、減速制御中にサーボ制御に異常が発生した場合にこれを偏差過大などの形で監視機能によって検出し、直ちに電源遮断を行う停止カテゴリ 0 の停止に切り替える場合などについては、上記で議論してきた条件設定に比して速度監視機能の急停止機能への寄与率が大きいため、ソフトウェアの検証も含め、速度監視機能を急停止機能に包含した一体のシステムとして評価すべきと考える。

注記 23) 図 7 の例は現実には上記のような切り替えが必要である。これに関する議論は本章では割愛し、後の 5.4 項で解析事例を示して詳述する。

4 障害の除外

JIS B 6410 で急停止時間は、「いかなる単一障害が起こっても（銘板に）表示する急停止時間を超えてはならない」としており、例として、急停止機能が停止カテゴリ 1 の停止として機能する場合を挙げ、このときには電源に不具合が生じたなどの影響で急停止時間が延長されることがあってはならないとしている。

ただし、関連する既存の法規や規格の要件、あるいは、一般的に受け入れられた技術的経験を十分に満足することを条件として、特定の障害については評価の範囲から除外する場合がある（ISO 13849-1:2006 箇条 7.3 参照）。例えば、クランクピンが、急停止時にその衝撃で割れて、軸の停止とは無関係にスライドが落下することを想定することは可能ではある。しかし、冗長化することが非現実的であるクランクピンについて、十分な強度を確保するよう製造されている等の技術的要求を条件にその破損を検討範囲から除外することを考慮しなければ、急停止時間を決定できなくなることは明らかである。

以上のことから、本研究では、すでに ISO/IEC 規格において安全関連システムの安全性能評価などで想定すべき障害の範囲から除外できることが明言されている障害・故障については、当該規格類を“特定の障害を除外した詳細な根拠”たる技術文書として認め、急停止時間条件を評価する際にも想定範囲から除外することを推奨する。具体的には、機械類に関連するすべての技術様式が包括的に扱われている ISO 13849-2 の附属書やサーボシステムの特異性を考慮した IEC 61800-5-2 の附属書掲載のリスト等がこれにあたる。

注記 24) 上記は、急停止時間を評価する際の障害の範囲を ISO 13849-2 及び IEC 61800-5-2 のリストに掲げられている障害に限定するという趣旨ではない。これらのリストに記載されていない障害についても、可能性があれば、その影響を検討しておく必要がある（ISO 13849-1:2006 箇条 7.2 参照）。なお、リストには除外できるときの条件が“なし（None）”とある項目があるが、これは、安全関連システムの安全性能を評価する上で、その障害を除外する理由がないことを特に強調する意味でリストに加えられていると解釈する。

本章では、機械／空圧／電気・電子コンポーネント毎に、ワーストケースの特定の際に想定から除外できる障害のリストを示す。これらの障害除外リスト又は条件の適用は、一連の ISO 機械安全規格の枠の中でタイプ C 規格の 1 つとして制定された JIS B 6410 に照らし、従前の機械プレスの急停止時間測定の実情を踏まえた上での本研究の見解であることに改めて留意されたい。動力プレス機械構造規格での障害に対する扱いや解釈、あるいは、EU 機械指令の型式試験において急停止システムの安全性能（PL, カテゴリ）を評価する際に特定の障害を除外できる可能性を示すものではない。

注記 25) ISO 13849-2 は現在 DIS 段階まで改定審議が行われており、特に附属書 A～D の障害リストにおいて、いくつかの障害除外条件で数値の見直しが検討されている。改定審議資料の入手困難さ故に以下の議論では現行の ISO 13849-2 : 2003 を引用しているが、正式改定後は最新の内容を反映されたい。

4.1 機械部品

4.1.1 基本要素事項

構造部品や動力伝達機構等の機械部分は、動力プレスに関連する既存の諸法規及び規格を遵守し、必要な強度等有するよう製造されなければならない。加えて、PL=e (Cat.4) への適合を前提とすれば、急停止機能に関連する機械部品については、ISO 13849-2 の附属書 A にある表 A.1 及び A.2 の該当する項目が正しく実現されていなければならない。同表 A.3 にある部品については、可能な限り、これを満たすものを使用するのが望ましい。

なお、機械的制動機構（メカブレーキ）については、JIS B 6410 箇条 5.10.2 に適合するように設計・製作しなければならない。

4.1.2 除外可能な障害

メカブレーキを除き、機械部品（構造部品の他、ギア、カム、カムフォロア、チェーン、クラッチ、ブレーキ、シャフト、ねじ、ピン、ガイドレール、ベアリング）については、除外できる障害及びそのときの条件を ISO 13849-2 の附属書 A にある表 A.4 に従う。ばねについては表 A.5 に照らして評価する。これらの表で障害除外（Fault exclusion）の欄に記載されている条件を満足する限り、急停止時間を検討する際には当該障害は発生しないものとして検討範囲から除外してよい。

ただし、表 A.4 は、材質を金属とする機械部品に関する一般的な工学の原則から導かれたものであり、表 A.4 を樹脂製又はゴム製の部品に対して適用する場合にはより慎重に吟味する必要がある。特に、タイミングベルトについては、別途技術的な根拠が特別にない限り、破断、歯飛び、緩み、外れ等の障害を想定しなければならない。

また、1 つのコンポーネントの中に電気・電子部品を内包する場合（信号入力部、コイル等）、電気・電子部品部分については後述する 4.4 節に従って評価する。

4.1.3 機械的制動機構（メカブレーキ）

機械的制動機構（メカブレーキ）については、以下の 1)～3) の条件を満たす場合、単一障害では所定の制動能力を失わないとし、急停止時間を延長させる要因としては除外してよい。なお、エア式メカブレーキであって、圧力供給をユーザー側の設備・装置で行う場合の取り扱いとは次節の 4.2.2 項に準じる。

注記 26) 所定の制動能力とは必ずしも新品状態を意味しない。特に、ブレーキシューの摩耗や劣化による急停止時間の延長については、特定自主検査での扱いも含め、表示する急停止時間に適切に反映することが望ましい。

注記 27) JIS B 6410 の箇条 5.10.2 は、メカブレーキを電磁弁を含む機構と解釈しているように読めるが、電磁弁や配管接続機器を含む空圧機器部分は分けて扱うべきである（解析事例 5.1 項を参照）。

条件 1) ばねについては、JIS B 6410 の箇条 5.10.2 の c) 及び d) に加え、ISO 13849-2 の表 A.5 に照らして評価し、その結果、障害を除外できれば、単一障害では急停止時間に影響を与えないと考える。圧縮ばねとして使用し、伸びる側での利用はしてはならない。なお、

機械プレスクラッチ／ブレーキに用いているばねであって、既に十分な実績を有しているものにあつては、ISO 13849-2 の表 A.5 の障害除外条件を満たすと見なしてよい。JIS B 6410 の箇条 5.10.2 の c)及び d)は満足するが、ISO 13849-2 の表 A.5 を満足しない場合には、急停止時間の検討で“ばねが 50%破損した状態”を想定する。

条件 2) 電磁弁については、プレス用安全バルブを用いている場合は、製品のスペック又は製造元の故障解析結果に基づいて、種々の単一障害がその応答時間に与える影響を評価する。方向切り替え弁を組み合わせて使用している場合は、弁、配管接続機器及び制御回路部分などに分けて、各々、4.2 節“空圧機器”及び 4.4 節“電気・電子部品”の内容に照らして検証し、メカブレーキの機械機構部分とは別にする。

条件 3) ばね・電磁弁以外の部分については、次の a)又は b)を満たす場合、単一障害では制動性能は落ちず、急停止時間には影響を与えないと見なす。

- a) クランク式等の機械プレスクラッチ／ブレーキに用いている機構・装置であつて、既に十分な実績を有している。
- b) ISO 13849-2 の表 A.4 及び次頁に示す表 2 に記載の事項に照らして障害を評価し、その結果、すべての障害が除外できる。

表 2 メカブレーキについて ISO 13849-2 の表 A. 4 に追加する項目

考慮する障害	障 害 除 外	備 考
メカブレーキに供給されるエア圧の遮断又は圧力低下	以下の条件を満たす場合、除外する。 － JIS B 6410 箇条 5.10.2 b)項	
メカブレーキへ供給されるエア圧の上昇（注 1）	なし。該当する場合、急停止時間への影響を想定する。	注 1: コンプレッサはブレーキに含まれない。3.2.2 項 4)又は 5)に照らして評価する。不具合としては、エア排気時間の延長を考慮する。
メカブレーキへの電力供給の遮断又は断線	以下の条件を満たす場合、除外する。 － JIS B 6410 箇条 5.10.2 b)項	
メカブレーキへの供給電圧の上昇等による電磁力の増加（注 2）	以下の条件を満たす場合、除外する。 － ISO 13849-2 の表 D.3 の条件を満足するヒューズ又はブレーキを用いて、コイル励磁電流が制限されている	注 2: 電源はブレーキに含まれない。これは 3.4 項で述べる“電気・電子部品”に照らして評価する。不具合としては、電磁力の増大による作動遅れ時間の延長を考慮する。
コイル・抵抗等の電気・電子部品	以下の条件を満たす場合、除外する。 － 3.4 項で述べる“電気・電子部品”に照らして評価し、すべての部品について障害が除外できること（注 3）	注 3: 障害除外条件がない部品については、その障害を除外することが認められていないと解釈されるので、本項にはあたらない。
ブレーキ摩擦面への油脂類、塵埃などの侵入	以下の条件を満たす場合、除外する。 － 従前の機械プレスのクラッチ・ブレーキと同じ又は同等の性能を有する防塵措置が講じられている	
ブレーキシュー・摩擦面の摩耗／劣化（注 4）	ISO 13849-2 表 A.4 “磨耗／腐食”の条件に従う場合、除外する。 または、以下のいずれかを満たす場合、除外する（注 5）。 － 毎回の通常停止でメカブレーキが使用され、その停止性能が JIS B 6410 の箇条 5.6.3 “オーバラン監視”に適合する監視機能で検査される － JIS B 6410 の箇条 5.6.5 “制動性能監視”に適合する監視機能で、同規定で推奨している実行頻度で制動性能が検査される	注 4: 特定自主検査での扱いも含め、従前の機械プレスに準じて、表示する急停止時間に適切に反映すること。 注 5: ブレーキの開放に電磁コイルを用いる構造の機械的制動機構では、コイル短絡等による電磁力低下によるブレーキシューの異常磨耗に対して適切な防御方策が導入されていない限り、左欄は適用されない。

4.2 空圧機器

4.2.1 基本要事項

サーボプレスの急停止システムに使用する空圧回路及び部品は、動力プレスに関連する既存の諸法規及び規格に準拠して製造されなければならない。加えて、PL=e (Cat.4) への適合を前提とすれば、空圧系の設計や部品の選択において、ISO 13849-2 の附属書 B にある表 B.1 及び B.2 の該当する項目が正しく実現されていなければならない。

4.2.2 除外可能な障害

ISO 13849-2 の附属書 B にある表 B.3～表 B.18 に従い、障害除外 (Fault exclusion) の条件を満たす限り、急停止時間を検討する際、その障害は発生しないものとしてよい。

ただし、

- (1) 空圧系 (エア圧供給源が同じ部分は 1 つの空圧系として扱う) に、十分な容積のエア圧を蓄積する部分 (タンク又はアキュムレータ) が備えられている場合には、圧力供給源 (コンプレッサ) の不具合を想定しなければならない場合にあっては、瞬間的に供給圧が大気圧に低下する障害は想定しなくてよい。
- (2) コイル、信号入力部、制御回路などについては、電気・電子部品として扱い、3.4 節に従って別途評価する。
- (3) エアバルンサのピストン部分は、機械部品として扱い、前述の 3.1 節に従って評価する。配管接続部品又は配管接続部は ISO 13849-2 の表 B.7～表 B.9 を適用する。
- (4) 圧力供給源 (コンプレッサ) については、調圧弁や圧力容器 (タンク、アキュムレータ)、フィルター、配管接続部品などの空圧機器、圧縮機構などの機械部品、駆動モータやスイッチなどの電気・電子部品に各々分解し、個々に該当する ISO 13849-2 のリストを適用して、供給圧が変動 (上昇/低下) する障害の可能性を評価する。除外条件にあらず、部品に障害を想定しなければならないときは、急停止時間が最も長くなる状況を設定する。なお、圧力を監視する機能・機構を備えるものにあつては、その遅れなどについて前述 3.3 節に準じて扱う。
- (5) 安全弁、圧力逃がし弁を空圧系に備え、これによって最大圧力を制限している場合、当該弁に ISO 13849-2 の表 B.6 を適用して評価する。ただし、表に“長期間の使用における漏れ流量の変化”とあり、圧力逃がし弁を要因とする圧力低下は除外されない。
- (6) 圧力供給をユーザー側の設備・装置で行うサーボプレスでは、急停止時間を検討する際、供給圧力の変動は検討から除外し、設計仕様の圧力が常に供給されることを仮定してよい。ただし、ユーザーが適切な措置を講じられるように、急停止時間を決定する際に設定した供給圧の条件、ならびに、供給圧が変動した場合の急停止時間に与える影響 (延長される時間) を使用上の情報として提供する。なお、圧力監視機能や圧力制限機構を別途備える場合は前記 (4) 及び (5) に準じて評価する。

4.3 油圧機器

油圧機器・油圧回路部品については基本的には ISO 13849-2 の付属書 C を適用できると考える。

しかし、本研究で調査した範囲では、急停止システムに油圧機器を利用しているサーボプレスはなく、具体的な急停止システム事例が得られていない。このため、急停止時間条件の評価における油圧機器の取り扱いについてはこれ以上言及しない。

4.4 電気・電子部品

4.4.1 基本要素事項

サーボプレスの急停止システムに使用する電気・電子回路及び部品は、動力プレスに関連する既存の諸法規を遵守し、また、JIS B 9961 の該当する規定に適合するよう適切に設計・選択されなければならない。また、ISO 13849-1:2006 の附属書 G にあるシステムティック故障を防止する方策が正しく実現されていなければならない。

加えて、PL=e (Cat.4) への適合を前提とすれば、ISO 13849-2 の附属書 D にある表 D.1 及び D.2 の該当項目が正しく実現されていなければならない。表 D.3 にある部品については、可能な限り、これを満たすものを選択するのが望ましい。

なお、ソフトウェアについては、JIS B 6410 の箇条 5.9 に適合するように設計・製作しなければならないとされており（JIS B 6410 附属書 F 参照）、本研究ではこれ以外の条件については言及しない。

4.4.2 除外可能な障害

サーボアンプ、エンコーダ、電源等の電気・電子コンポーネントは、部品毎のレベルに分解し、IEC 61800-5-2 の附属書 D にある表 D.1～表 D.16 及び ISO 13849-2 の附属書 D にある表 D.4～表 D.21 を適用して解析する。障害除外条件はどちらの規格に拠ってもよい。ただし、

- (1) 主電源の停電又は電圧低下は除外されず、そのタイミングは急停止時間が最も長くなるワーストケースを想定する。ただし、これは単一障害として扱う。すなわち、他の障害が発生している状況に加えて停電を想定すること（又はその逆）は検討する必要はない。主電源電圧の上昇も除外されず、単一障害として扱う。ただし、電流の増大については、ISO 13849-2 附属書 D の表 D.3 の記載事項に従ったヒューズ、ブレーカ、RCD を用いている場合、これらが確実に機能すると考えて、電流値をこれらの制限値に限定してよい。

注記 28) 通常、保護装置からの信号が消滅した時点で急停止機能が開始するように急停止システムは構成される。この場合には、評価すべき停電の影響は“急停止動作中に停電が発生した”という状況になる。このように、停電を単一障害と扱い、他の障害を想定しないのは、PL=e (Cat.4) が二重故障の可能性を許容しているという理由からではなく（停電は、急停止システムの片側のチャンネルが危険側故障する確率よりもはるかに高い確率で発生する）、あくまでも現行の国内での動力プレスの故障に対する扱いを反映した見解である。

- (2) その他の電源装置、電圧・電流変換装置については、各部品レベルに分解し、IEC 61800-5-2 の附属書 D もしくは ISO 13849-2 の附属書 D に記載された除外条件を満

たさない限り、単一障害によって、出力の上昇、低下、喪失および特定周波数の交流出力の発生することを想定する。

- (3) 保護装置（ライトカーテン、両手操作制御装置等）を無効化するスイッチ、操作ボタン等は安全関連部である。したがって、ISO 13849-2 の附属書 D にある表 D.8（機械部分については同規格付属書 A）を参照し、その障害の影響を評価する。システムの構成次第ではスイッチの単一障害が機能の喪失に至るとは限らない。しかし、短絡等の障害が起こった場合に、それを検出できる機構・手段あるいは障害が露呈する方策を備えていないときは、障害の蓄積を考慮し、スイッチが故障している条件で他の障害の影響を評価する必要がある。
- (4) スライドの位置検知又はモータの回転検出にポテンシオメータを用いる場合には、IEC61800-5-2 の表 D.10 に加えて表 D.16 記載の障害項目についても考慮する。
- (5) モータについては部品毎のレベルに分解し、機械部分については前述の 4.1 節に従って解析する。コイル、内部配線、電力配線接続部、信号配線接続部等の電気・電子部分については、IEC 61800-5-2 の付属書 D にある表 D.1～表 D.16 及び ISO 13849-2 の附属書 D にある表 D.4～表 D.21 を適用する。
- (6) インバータに、自身内部の処理回路を介さず、外部信号によって直接的に電源遮断を行えるインバータ回路遮断が内蔵されている場合、安全関連ブロック図においては、これに関連する素子及び回路を 1 つの機能ブロックとしてグループ化し、インバータ本体の標準制御回路部分とは分離して扱うことができる。ただし、これには遮断動作確認用のフィードバックが不可欠であり、このフィードバックに関連する回路部分もブロックに含む。

注記 29) 電子的な遮断素子はこれに相当する電気機械部品と次の点で異なる。

- 1) 小電流を回路に流す、
- 2) 電源本線の影響を受けやすい、
- 3) 温度の影響を受けやすい。

これらに対する検証事項は JIS C 9730-1:2004 箇条 H.28 を参照のこと。

- (7) ダイナミックブレーキユニットは、コンタクタ、抵抗、信号処理 IC 等に分解して評価する。
- (8) 回生制動での電気エネルギー変換の安定化などを目的として平滑用コンデンサがモータとインバータとの間に接続される場合、IEC 61800-5-2 の付属書 D の表 D.11 に掲げられているような単一障害の発生を考慮し、該当する場合はコンデンサの故障が急停止時間に与える影響、ならびに、この故障に対する検出可能性を評価する必要がある。
- (9) 安全用途で実績がなく、プログラマブルで機能的な電子回路コンポーネント（特にエンコーダ等のセンサ）については、詳細な故障解析に加え、別途その故障を検出する特別な方策によって高 DC を確保できない限り、PL=e (Cat.4) が要求されたシステムでは使用できない（アプリケーションソフトウェアが要求を満足しない場合が多い）。

- (10) 単純な ON/OFF 信号の伝送及びアナログ電圧/電流の伝送については、信号出力要素（例えば、スイッチ）、伝達媒体（例えば、導線）及び受信要素（例えば、安全リレーユニット）の故障解析に準じて評価する。
- (11) データの通信をシリアルリンク、フィールドバス等のデジタル信号処理で行う場合について、通信プロトコルが IEC61784-3 に適合する安全なもので、データ伝送誤りに対する方策（例えば、メッセージの冗長化 CRC 処理。同規格 6.2.17 参照）が十分講じられているとし、単位時間当たりの残留エラーレートが目標とする PL で要求される危険側故障率の 1%以下であれば、その障害は除外する。
- (12) 鉛フリー化に伴うウィスカの影響が想定される場合は、IEC61800-5-2 付属書 D の D.2.2 項に従うこと。
- (13) プリント配線基板上に実装された部品間の短絡は、IEC61800-5-2 付属書 D の表 D.2 に従って評価すること。

5. 解析事例

5.1 急停止時間決定の基本的流れ

急停止時間を評価する際は、保護装置によって急停止機能の作動が要求されてから以下の 3 つの条件がすべて完了するまでの時間を、原則、それぞれ個別に決定する。

条件 a) スライドの移動速度を 10 mm/s 以下に減速している。

条件 b) 制動機構を作動している。

条件 c) 停止カテゴリ 0 又は 1 の停止として機能する場合、電源遮断を行っている。

以下では、具体的な急停止システムを仮定してワーストケースを特定していくプロセスを例示する。このプロセスの基本的な流れは以下のとおりである。

- (1) サーボプレスのシステムのうち、急停止機能に関連するサブシステム（安全関連部）を明確にする。
- (2) 第 4 章で述べた障害リストに照らし、各コンポーネントでの単一障害の影響を解析する。解析の結果、障害除外の条件が適用可能で単一障害を考慮する必要のないコンポーネント、ならびに、想定される単一障害の影響がすべて安全側となるコンポーネントについては以降の検討から省いてよい。

注記 30) ここでは、人がマニュアルで設定する調節機構等のコンポーネントに対しては、適切な設定がなされることを仮定してよい。ヒューマンエラーによるリスク（安全機能の喪失）は別に評価・低減しなければならない事項である。

- (3) 3.1 節で述べた“サーボシステムの故障による異常速度の発生”及び 3.3 節で述べた“エアバランサの内圧低下の発生”について、各項で述べた条件に則して、条件 a) の“スライドの停止”に要する急停止時間を評価する。
- (4) 以上を経て、上記(2)で除いた障害及び(3)で評価した“サーボシステムの故障による異常速度”及び“エアバランサの内圧低下”以外の障害発生状態を検討していくが、ここで、要求される安全性能（PL，カテゴリ）を急停止システムが達成しているか評価しておく。これは予備的な評価であるが、要求安全性能を達成できておらず、例えば、制動機構の作動を単一障害の発生で実行できなくなってしまうシステムについて条件 b)は評価できない。このとき作成する安全関連ブロック図には、ほとんどの場合、危険側の単一障害を想定する必要のあるコンポーネント(すなわち、(2)及び(3)で除外又は評価されなかったコンポーネント)がすべて表現される。
- (5) PL=e (Cat.4) を達成している急停止システムでは単一障害で上記の条件 a)～c)が実行できなくなることはない。すなわち、“ワーストケース”とは“発生する単一障害の違いによって条件 a)～c)に要する時間が変化してしまう急停止システムにおいて最も急停止時間が長くなる状況”のことである。
- (6) 条件 a)～c)について、それぞれ個別に、保護装置からの急停止機能作動要求から完了までの急停止時間を決定していく。このときは、(5)で作成した安全関連ブロック図を利用し、図から各々の条件に関係しないコンポーネントを除いていく方法で、

ワーストケースを特定する。例えば、条件 c) に関して言えば機械ブレーキは明らかに関係しない。

- (7) 2.1.4 節で述べたように、障害の発生するタイミングには、
- 単一障害が起こっているときに保護装置から急停止が要求された場合、
 - 急停止が完了する前（すなわち、急停止動作中）に単一障害が起こった場合、
- を想定する。

5.2 例1：停止カテゴリ0のシステム

1) 想定するシステムの概要

停止カテゴリ0の停止として急停止機能を実行する急停止システムの例を図9に示す。

このシステムでは、ライトカーテンから急停止信号として OFF 信号が出力されると冗長化安全コントローラがサーボシステムを電源遮断し、同時にエア式機械ブレーキを作動させる。

スライドの減速・停止はエア式機械ブレーキだけで行われ、電氣的制動機構は一切関与しない。また、このサーボプレスでは、通常停止は、停止カテゴリ1の停止で行うものとし、毎回上死点で電源遮断と機械ブレーキの作動が実行される。

機械ブレーキの制動性能は、始動時及び24時間毎にJIS B 6410 箇条 5.6.5にある“動的な制動性能監視”を実行して検査される。なお、ここで“機械ブレーキ”とはコイルやバルブを含まない機械部品部分（ばね、ブレーキ板等）を指す。

モータの回転速度は、エンコーダ G1 によって標準 NC コントローラにフィードバックされるが、冗長化安全コントローラでは監視されていない。

圧力供給はユーザー側の設備で行われるが、供給圧の低下（含む供給停止）は考慮する。エアバルサの内圧は直接は監視されていない。機械ブレーキ系及びエアバルサ系は金属配管で配管

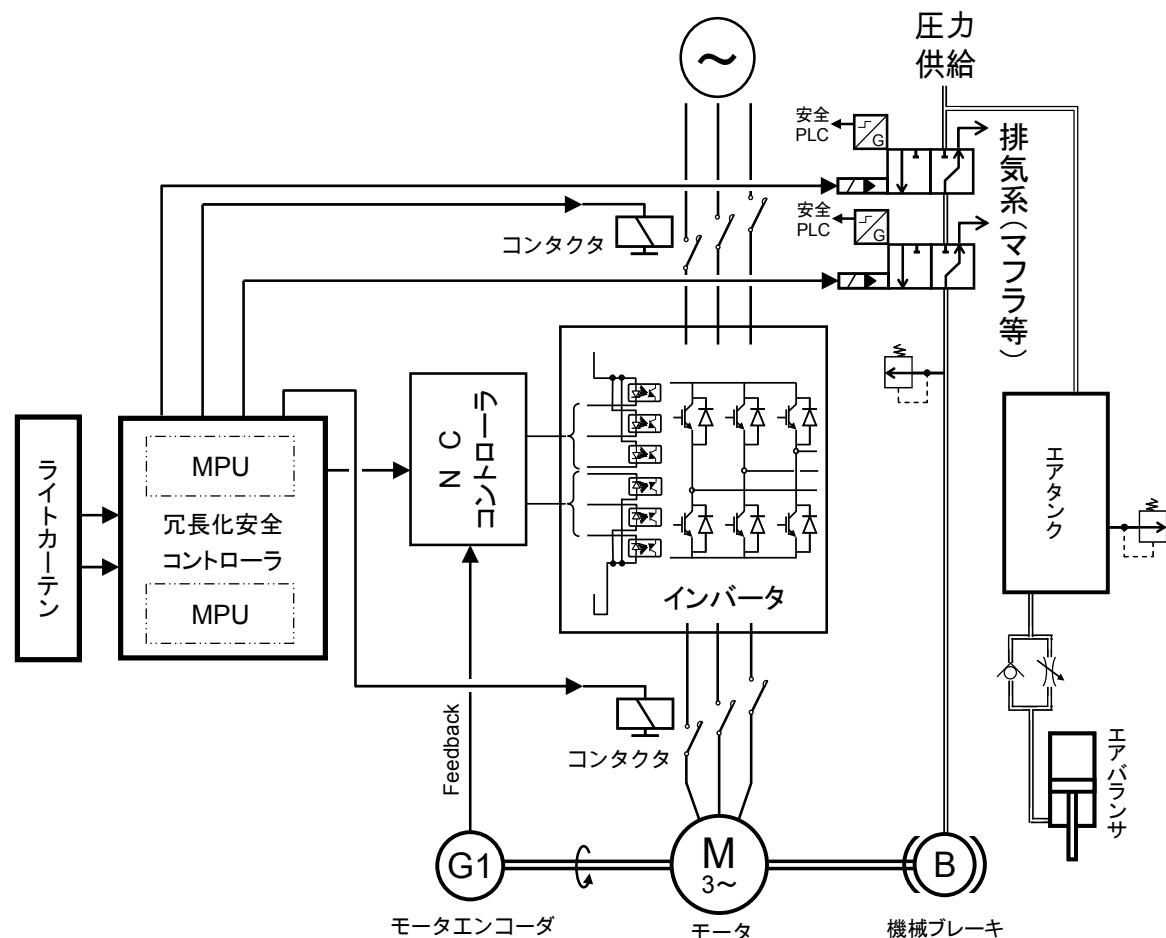


図9 システム例1

（※クランク軸以降のリンク機構、スライド、コンタクタのバックチェック用ミラーB 接点は作図を省略している。）

されている。いずれもネジ式調圧弁を備えており、このため圧力上昇は各々の調圧弁の設定圧までしか考慮しない。

2) 構成品の条件、障害の除外

この例では、以下を前提条件として仮定する。

- (1) 現行の動力プレスに関する諸法規は遵守されているとする。
- (2) 構造部品を含むすべての部品は、ISO 13849-2 の機械部品、空圧機器及び電気/電子部品に関する基本安全原則及び吟味された安全原則をすべて適切に実現しているとする。
- (3) ライトカーテンには TYPE 4 適合品を用いている。
- (4) 冗長化安全コントローラは JIS C 0508 の SIL 3 の要求事項を満足しているとする。ソフトウェアも JIS C 0508-3 Section 7 にある SIL 3 の要求事項を満足しているとする。
- (5) コンタクタの開動作は（図 9 では図示していないが）直接駆動する B 接点（：ミラーコンタクト，JIS C 8201-4-1 附属書 F 参照）を用いて冗長化安全コントローラでバックチェックされ、両者の不一致が検出される。
- (6) エア式機械ブレーキの電磁弁の動作は、ポジションセンサを用いて安全 PLC でバックチェックされ、両者の不一致が検出される。

以下の障害については、ISO 13849-2 を検討の結果、除外できると仮定する。

- (7) クランク軸以降のリンク機構部分及びスライドは十分な強度を有する設計と仮定し、表 A.4 に基づき、破断、変形等の障害は除外する。また、適切な工学の原則に則した設計方策によって金型の落下は防止できているとする。
- (8) プレスのリンク機構及びバルブに用いている“ばね”は、すべて表 A.5 (A.2) を満足していると仮定し、障害を除外する。
- (9) 機械ブレーキの機械部分は、ISO 13849-2 の表 A.4 及び本稿 3.1.3 項の表にある項目を適切に実現しているとし、障害を除外する（すなわち、エア圧が排気されれば確実に作動するとする）。
- (10) 空圧系の金属配管は表 B.7 をすべて満たすとし、障害を除外する。
- (11) エアバランサピストン及びエアタンクは、十分な強度を有する設計であり、ISO 13849-2 の表 A.4 及び表 B.14 に基づき、破裂、ひび（漏れ）、ロッドの抜けは生じないと仮定する。また、エアバランサのピストンがスティックすることは、ここでは危険側故障とならない。したがって、エアバランサピストンとエアタンクの障害としては、配管接続部について、表 B.9 を参照して“接続部での漏れ（シールの低下）”のみを想定する。
- (12) エア式機械ブレーキの排気系（マフラ等）は、表 B.7、表 B.9 及び表 B.13 に基づき、表 B.9 の“接続部での漏れ（シールの低下）”以外の障害（閉塞等）は除外する。
- (13) ネジ式調圧弁は、表 B.6 に基づき“長期使用に伴う漏れ流量の変化”以外の障害は除外する（すなわち、機械ブレーキ系には影響を及ぼさないが、エアバランサ系には圧力低下が起きる可能性がある。）
- (14) バルブに設けたポジションセンサは、故障解析の結果、本稿 3.4.2 項で述べた想定され

るいかなる障害についても，すべてエアバルブの不一致作動として検出できるとする。

3) サーボシステムの故障による異常速度時の急停止時間

サーボシステムの異常速度発生について，図 9 のシステムは 3.1 節の (2) にあたる。このため，スライド動作機構の構造，動力伝達機構の構造及びサーボモータの能力的制約から，無負荷状態で物理的に発生し得る最大速度を想定して，サーボシステム異常時の急停止時間を測定する必要がある。ただし，このような理論的最大速度を実験することは非常に困難である。このため，この例では，スライド速度と急停止時間との関係をプロットし，これに理論的な最大速度を外挿することで，急停止時間を推定することとする。なお，この例では機械ブレーキには不具合を想定しない。

4) エアバランサの故障による重量補償機能異常時の急停止時間

エアバランサの故障について，図 9 のシステムはバランサピストン内圧を監視していない場合にあたるので，1 ストロークの間に重力補償機能が損なわれることを想定する。この例では，これを実験で求めることとし，スライドを上昇できる最小限の内圧をかけた状態から，配管接続部の締め付け力を規定値の半分まで緩めてエア漏れを起こし，最も急速にピストン内圧が大気圧に達する条件でライトカーテンを作動させて急停止時間を評価することとする。なお，この例では機械ブレーキには不具合を想定しない。また，エアバランサの不具合発生については 2.2.2 項の a) に該当する“急停止機能が開始する前に既に不具合が生じていた”場合のみを考慮する。

5) PL=e (Cat.4) の検証

急停止システムの安全関連ブロック図を作成し，ISO 13849-1:2006 附属書 I を参照し，これが PL=e (Cat.4) に適合することを確認する (図 10 参照)。この例では上記 2) で除外されたコンポーネント (機械ブレーキ，排気系，調圧弁，ポジションセンサ等) 及び 3) と 4) で検討したモータ速度監視とエアバランサ内圧監視のみに関わるコンポーネント (エアバランサ，ならびに，この例ではインバータ回路遮断や減速制御を行わないためサーボシステム一式) は安全関連部に含めない。ただし，後の急停止時間評価で必要になるので機械ブレーキの機械部分は破線で示しておく。

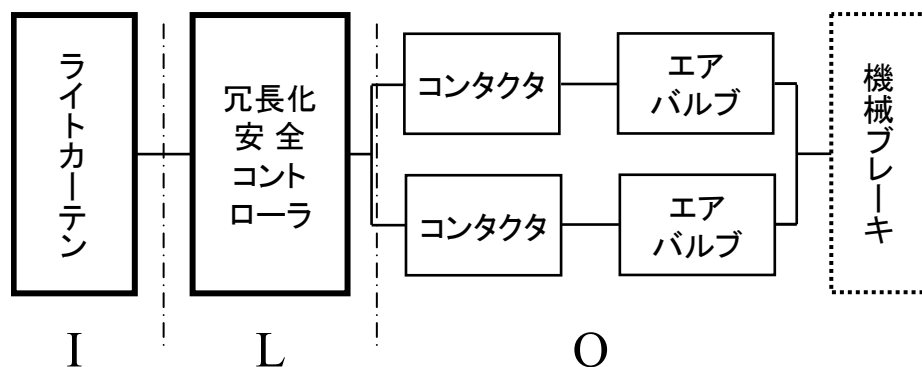


図 10 システム例 1 の安全関連ブロック図

2)で述べた仮定より、

- (15) ライトカーテンは TYPE 4 であって、製品として PL=e (Cat.4) に適合しているとする（この平均危険側故障率は最後に合算する。ISO/TR 23849 参照）。
- (16) 冗長化安全コントローラは JIS B 9961, JIS C 0508 等に基づき PL=e (Cat.4) に適合すると見なす（仮定(4)参照。この平均危険側故障率は最後に合算する。ISO/TR 23849 参照）。

したがって、ここで検討するのは、

- (17) コンタクタについては危険側となる単一障害（例えば、接点溶着）を除外できない。冗長化されているので Cat.4 の構造要件は満足している。コンタクタ単体の MTTF_d は ISO 13849-1:2006 附属書 C のコンタクタ（定格負荷）の標準 B_{10d} 値（200 万回）を適用するとし、これとコンタクタの作動頻度（1 年 240 日、1 日 16 時間稼動、平均作動周期 30 秒を仮定）から附属書 C の例 C.4.3 に従って計算し、MTTF_d=約 43[years]となったとする。DC は ISO 13849-1:2006 附属書 E の表 E.1 にある“直接監視”を適用して 99%を仮定する。
- (18) エアバルブについては危険側となる単一障害（例えば、任意の中間位置でのスティック）を除外できない。冗長化されているので Cat.4 の構造要件は満足している。バルブ単体の MTTF_d は ISO 13849-1:2006 附属書 C の空圧機器の標準 B_{10d} 値（20 000 000 回）とし、バルブの作動頻度（1 年 240 日、1 日 16 時間稼動、平均作動周期 30 秒を仮定）から附属書 C の例 C.4.3 に従って計算し、MTTF_d=約 434[years]となったとする。DC は ISO 13849-1:2006 附属書 E の表 E.1 にある“直接監視”を適用して 99%を仮定する。

注記 31) コンタクタ及びエアバルブについては、サーボプレスの運転において、急停止のほか、通常停止、非常停止等においても使用されるため、作動周期を平均 30 秒と仮定した。

となり、

- (19) コンタクタとエアバルブからなる 1 チャンネルの MTTF_d は約 39[years]（高）、また、平均 DC は 99%（高）となる。さらに、ISO 13849-1:2006 附属書 F に従って CCF に対する方策を評価し、65 点以上のスコアとなったとする。以上のことからコンタクタとエアバルブからなる出力部分 (O) は PL=e に適合すると見なせ、ISO 13849-1:2006 の表 K より、その平均危険側故障率は 7.11×10^{-8} と導かれる。

これにライトカーテンと冗長化安全コントローラの平均危険側故障率を加え、システム全体で最終的に 10^{-7} 未満であれば、この急停止システム例が PL=e (Cat.4) に適合すると見なせる (ISO/TR 23849 参照)。

6) 制動機構の作動に要する時間

図 10 の安全関連ブロック図より、“条件 b) 制動機構の作動”に関連するコンポーネントを抜き出したものを図 11 に示す。この条件ではコンタクタは関連せず、また、2.3.1 項で述べたようにライトカーテンは検討対象に含まれないことに注意されたい。

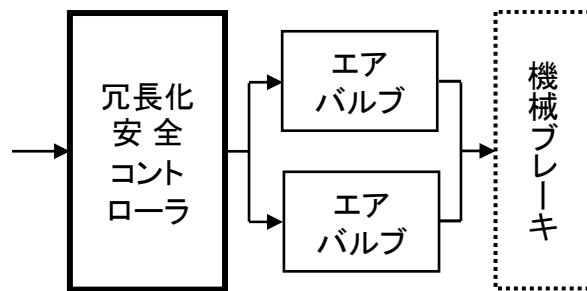


図 11 “制動機構の作動”の安全関連ブロック図

評価すべき時間は“冗長化安全コントローラの遅れ”＋“エアバルブの遅れ”＋“機械ブレーキの作動遅れ”の合計となる（ただし、冗長化安全コントローラについては、仮定(4)より単一障害では指定された安全機能を喪失しないとしたため、この例ではいわゆる“通常の遅れ時間”を考慮する）。これに対して、エアバルブについては、何れか一方のエアバルブに不具合発生を想定し、最も時間が長くなる状況が条件 b)におけるワーストケースとなる。なお、仮定(9)より、機械ブレーキのばねが 50%破損した状態は想定しない。

7) 電源遮断に要する時間

図 10 の安全関連ブロック図より、“条件 c) 電源遮断に要する時間”に関連するコンポーネントを抜き出したものを図 12 に示す。この条件では機械ブレーキは関連しない。また、インバータ回路遮断を行わないのでサーボシステムも関連しない。

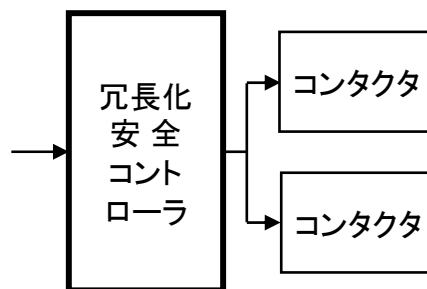


図 12 “電源遮断”の安全関連ブロック図

評価すべき時間は“冗長化安全コントローラの遅れ”＋“コンタクタの主接点 OFF 動作時間”の合計となる。ただし、冗長化安全コントローラについては、仮定(4)より単一障害では指定された安全機能を喪失しないとしたため、この例ではいわゆる“通常の遅れ時間”を考慮する。これに対して、コンタクタについては、何れか一方のコンタクタに不具合発生を想定し、最も時間が長い状況が条件 c)におけるワーストケースとなる。

8) スライドの制動に要する時間

図 10 の安全関連ブロック図より“条件 a) スライドの制動に要する時間”に関連するコンポーネントを抜き出したものを図 13 に示す。ただし、急停止時間の評価という本項の目的に則し、

安全関連ブロック図を拡張して、各コンポーネントの動作時間が容易に比較できるような表現で示している。特に図 11 と異なり、機械ブレーキの作動遅れの先に“スライドの制動・停止に要する時間”を表す破線ブロックを加えている。仮定[9]より、機械ブレーキのばねが 50%破損した状態も単一障害の 1 つに入れて評価する。

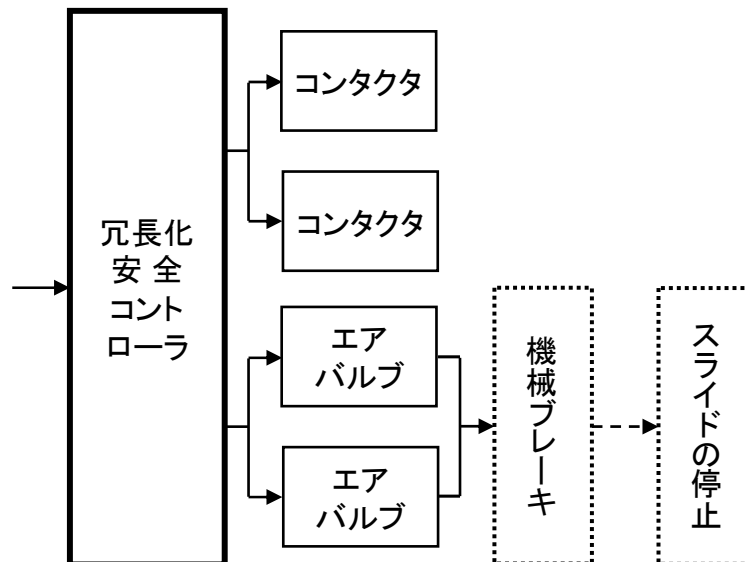


図 13 “スライドの制動”（これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない）

コンタクタの作動遅れはエアバルブの遅れよりも短いと仮定すれば、評価すべき時間は、“冗長化安全コントローラの遅れ（仮定(4)より、単一障害では指定された安全機能を喪失しないとしたため、いわゆる通常の遅れ時間）” + “エアバルブの遅れ” + “機械ブレーキの作動遅れ” + “スライドの制動時間” の合計であって、何れか一方のエアバルブに不具合発生を想定し、最も時間が長い状況が条件 a) におけるワーストケースとなる。

9) 急停止時間の決定

以上の検討から、下記の 5 つの条件に対する時間が得られる。

- ・ 3) で得た “サーボシステムの故障による異常速度時の急停止時間”
- ・ 4) で得た “エアバランサの故障時の急停止時間”
- ・ 6) で得た “制動機構の作動に要するワーストケース”
- ・ 7) で得た “電源遮断に要するワーストケース”
- ・ 8) で得た “スライドの制動に要するワーストケース”

このうち最も長い時間を対象サーボプレスの急停止時間として決定する。

5.3 例 2：停止カテゴリ 0（インバータ回路遮断）＋ダイナミックブレーキのシステム

1) 想定するシステムの概要

停止カテゴリ 0 の停止として急停止機能を実行する急停止システムの例を図 14 に示す。

このシステムでは、ライトカーテンから急停止信号として OFF 信号が出力されると冗長化安全コントローラがサーボシステムを電源遮断し、同時にエア式機械ブレーキとダイナミックブレーキ回路（DB 回路：コンタクタと抵抗で構成される）を作動させる。

ただし、DB 回路は、インバータ二次側を切る電源遮断の機能を果たすが、ここでは、電源遮断の要素としてはインバータ回路遮断とインバータ 1 次側コンタクタを考え、DB 回路は機械ブレーキとともにスライド制動の要素として捉える。

通常停止は停止カテゴリ 1 の停止で行うものとし、毎回上死点で電源遮断及びダイナミックブレーキと機械ブレーキの作動が実行される。機械ブレーキの制動性能（摩擦版の劣化）は始動時及び 8 時間毎に JIS B 6410 箇条 5.6.5 にある“静的な制動性能監視”を実行して検査される。

モータの回転速度は、エンコーダ G1 によって標準 NC コントローラと冗長化安全コントローラにフィードバックされる。冗長化安全コントローラはエンコーダ G2 によりスライド位置も

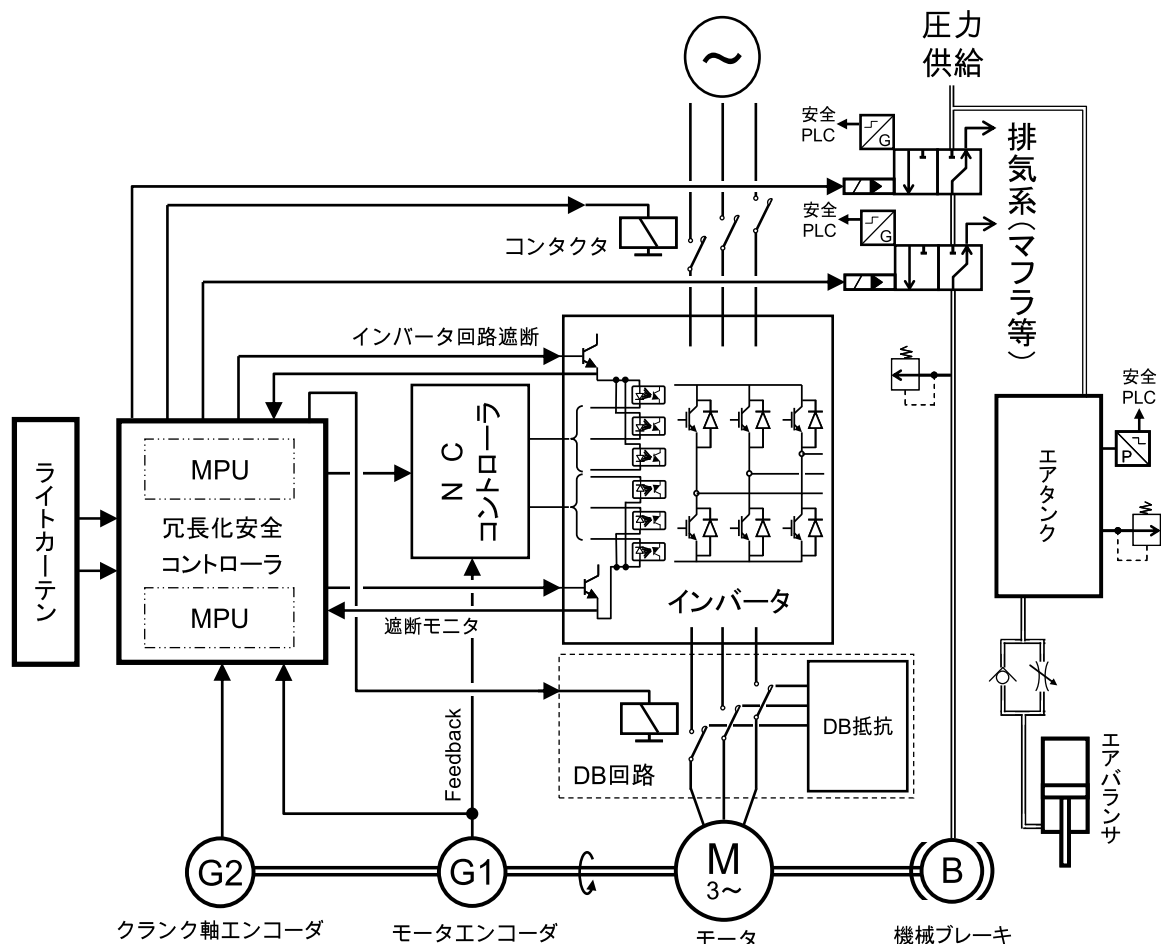


図 14 システム例 2

（※クランク軸以降のリンク機構、スライド、コンタクタのバックチェック用ミラー B 接点は作図を省略している。）

監視しており、クロスモニタリングによって、G1 の障害を検出できる。これらは、モータの速度監視だけでなく、“静的な制動性能監視”でも利用される。

圧力供給はユーザー側の設備で行われるが、供給圧の低下（含む供給停止）は考慮する。圧力スイッチによってエアタンクの内圧が監視されているが、エアバランサピストンの内圧を直接測定はしていない。機械ブレーキ系及びエアバランサ系は金属配管で配管されている。いずれもネジ式調圧弁を備えており、このため圧力上昇は各々の調圧弁の設定圧までしか考慮しない。

2) 構成品の条件、障害の除外

この例では、以下を前提条件として仮定する。

- (1) 現行の動力プレスに関する諸法規は遵守されているとする。
- (2) 構造部品を含むすべての部品は、ISO 13849-2 の機械部品、空圧機器及び電気/電子部品に関する基本安全原則及び吟味された安全原則をすべて適切に実現しているとする。
- (3) ライトカーテンには TYPE 4 適合品を用いている。
- (4) 冗長化安全コントローラは JIS C 0508 の SIL 3 の要求事項を満足しているとする。ソフトウェアも JIS C 0508-3 Section 7 にある SIL 3 の要求事項を満足しているとする。
- (5) インバータ回路遮断は、IEC 61800-5-2 に従い、SIL2 の安全性能を達成しているとする。その遮断動作は遮断モニタによって冗長化安全コントローラでチェックされ、毎回の通常停止時に不一致が検出される。なお、安全関連ブロック図においては、インバータ回路遮断及び遮断モニタに関連する素子及び回路を 1 つの機能ブロックとしてグループ化し、インバータ本体の標準制御回路部分とは分離して扱う。
- (6) インバータ回路遮断が完了してからコンタクタが開動作するように、冗長化安全コントローラのプログラムでディレーを設けている。
- (7) (図 14 では図示していないが) インバータ 1 次側コンタクタの開動作は直接駆動する B 接点（:ミラーコンタクト, JIS C 8201-4-1 附属書 F 参照）を用いて冗長化安全コントローラでバックチェックされる。
- (8) DB 回路のコンタクタはチェックされない。
- (9) エア式機械ブレーキの電磁弁の動作は、ポジションセンサを用いて安全 PLC でバックチェックされ、両者の不一致が検出される。
- (10) 静的な制動性能監視は、冗長化安全コントローラで行われる（ここでは詳細は議論しない）。

以下の障害については、ISO 13849-2 を検討の結果、除外できるとする。

- (11) クランク軸以降のリンク機構部分及びスライドは十分な強度を有する設計と仮定し、表 A.4 に基づき、破断、変形等の障害は除外する。また、適切な工学の原則に則した設計方針によって金型の落下は防止できているとする。
- (12) プレスのリンク機構及びバルブに用いている“ばね”は、すべて表 A.5 (A.2) を満足していると仮定し、障害を除外する。
- (13) 機械ブレーキの機械部分は、ISO 13849-2 の表 A.4 及び本資料 3.1.3 項の表にある項目を適切に実現しているとし、障害を除外する（すなわち、エア圧が排気されれば確実に作

動するとする)。

- (14) 空圧系の金属配管は表 B.7 をすべて満たすとし、障害を除外する。
- (15) エアバランサピストン及びエアタンクは、十分な強度を有する設計であり、ISO 13849-2 の表 A.4 及び表 B.14 に基づき、破裂、ひび（漏れ）、ロッドの抜けは生じないと仮定する。また、エアバランサのピストンがスティックすることは、ここでは危険側故障とならない。したがって、エアバランサピストンとエアタンクの障害としては、配管接続部について、表 B.9 を参照して“接続部での漏れ（シールの低下）”のみを想定する。
- (16) エア式機械ブレーキの排気系（マフラ等）は、表 B.7、表 B.9 及び表 B.13 に基づき、表 B.9 の“接続部での漏れ（シールの低下）”以外の障害（閉塞等）は除外する。
- (17) ネジ式調圧弁は、表 B.6 に基づき“長期使用に伴う漏れ流量の変化”以外の障害は除外する（すなわち、機械ブレーキ系には影響を及ぼさないが、エアバランサ系には圧力低下が起きる可能性がある。）
- (18) バルブに設けたポジションセンサは、故障解析の結果、本稿 3.4.2 項で述べた想定されるいかなる障害についても、すべてエアバルブの不一致作動として検出されることが解っているとする。
- (19) DB 回路の内部配線の短絡は ISO 13849-2 の表 D.4 より除外できるとする。
- (20) 静的な制動性能監視は、別途解析の結果、PL=e (Cat.4) に適合していると仮定する（ここでは詳細は議論しない）。

3) サーボシステムの故障による異常速度時の急停止時間

モータ回転速度監視機能に関連するサブシステムの安全関連ブロック図を図 15 に示す。

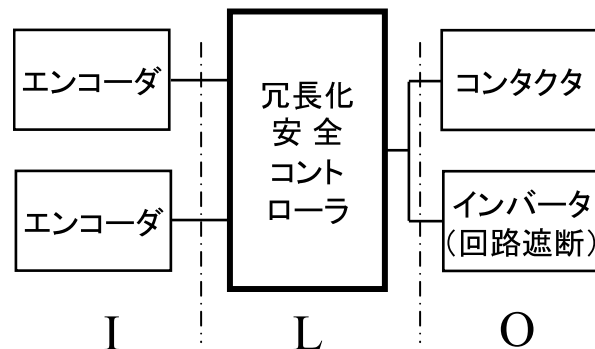


図 15 モータ回転速度監視機能の安全関連ブロック図

解析の結果からモータ回転速度監視機能が PL=e (Cat.4) の要件を満足しているとするれば、図 14 のシステムは 3.1 節の (3) にあたる。このため、サーボシステムの故障による異常速度時の急停止時間の測定ではスライド速度 v [m/s] を式(2)で設定する。

$$v = v_{limit} + T_{test} \times a \quad \dots(2 \text{ 再掲})$$

この条件では、インバータ回路遮断には不具合を想定しないので、 T_{test} は“速度監視実行周期”

+ “インバータ回路遮断の遅れ” となる。

また、ここで機械ブレーキ等の他のコンポーネントに不具合を想定する必要はないが、ダイナミックブレーキの効果については 5)での検討結果から判断した DB 回路の取り扱い方に従う。

4) エアバランサの故障による重量補償機能異常時の急停止時間

エアバランサの故障について、図 14 のシステムではエアタンクの内圧を監視しているが、エアタンク内圧監視ではバランサピストンまでの配管接続部での漏れを確実に検出し、重量補償機能の低下を防止できるとは必ずしも言えない。このため、内圧を監視していない場合と同等と見なし、1 ストロークの間に重力補償機能が損なわれる想定で評価することとする。

なお、エアバランサ以外のサーボシステムを含むコンポーネントは正常であると仮定する。また、エアバランサの不具合発生については、2.2.2 項の a)に該当する“急停止機能が開始する前に既に不具合が生じていた” 場合のみを考慮する。

5) PL=e (Cat.4) の検証

上記 2)で除外されたコンポーネント（機械ブレーキ、排気系、調圧弁、ポジションセンサ等）及び急停止機能に直接関与しないコンポーネントを除き（ただし、後の急停止時間評価で必要になるため、機械ブレーキの機械部分は破線で示しておく）、急停止システムの安全関連ブロック図を作成し、ISO 13849-1:2006 附属書 I を参照し、これが PL=e (Cat.4) に適合することを確認する。システム例 2 の安全関連ブロック図を図 16 に示す。

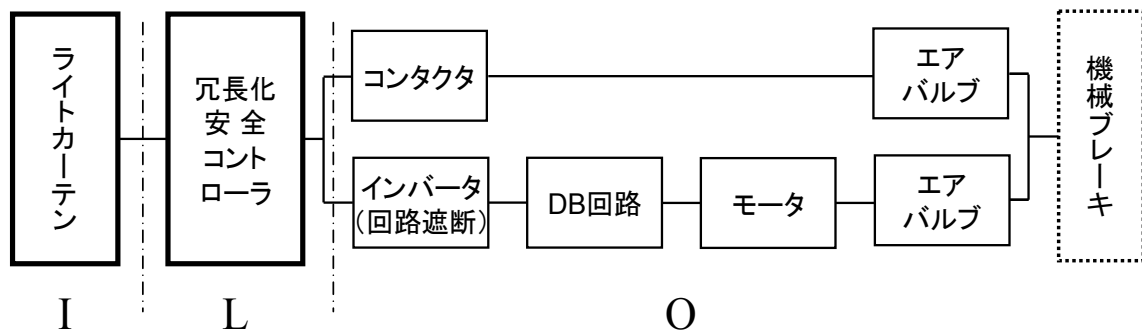


図 16 システム例 2 の安全関連ブロック図

ただし、DB 回路をインバータ（回路遮断）のチャンネルかコンタクタのチャンネルのどちらに帰属させるかについては、ISO 13849-1:2006 附属書 D の式 D.2 を用いて冗長化チャンネルの平均 $MTTF_d$ を導出した結果を比較し、平均 $MTTF_d$ がより低い値となる配置を選ぶ。

2)で述べた仮定より、

(21) ライトカーテンは TYPE 4 であって、製品として PL=e (Cat.4) に適合しているとする（この平均危険側故障率は最後に合算する）。

(22) 冗長化安全コントローラは JIS B 9961, JIS C 0508 等に基づき PL=e (Cat.4) に適合すると見なす（この平均危険側故障率は最後に合算する）。

したがって、ここで検討するのは、

- (23) コンタクタについては危険側となる単一障害（例えば、接点溶着）を除外できない。コンタクタ単体の $MTTF_d$ は ISO 13849-1:2006 附属書 C のコンタクタ（定格負荷）の標準 B_{10d} 値（2 000 000 回）を適用するとし、これとコンタクタの作動頻度（1 年 240 日、1 日 16 時間稼動、平均作動周期 30 秒を仮定）から附属書 C の例 C.4.3 に従って計算し、 $MTTF_d$ = 約 43[years] となったとする。DC は ISO 13849-1:2006 附属書 E の表 E.1 にある“直接監視”を適用して 99%を仮定する。
- (24) インバータ(回路遮断)については単一障害を除外できない(ISO 13849-2 附属書 D 参照)。信頼性解析の結果、 $MTTF_d$ = 100[years]を得たとする。DC は ISO 13849-1:2006 附属書 E の表 E.1 にある“間接監視”及び“プロセスによる障害検知”を適用して 99%を仮定する。
- (25) DB 回路については危険側となる単一障害を除外できない（ISO 13849-2 表 D.13 及び表 D.14）。そこで、パーツカウントメソッドを用い（ISO 13849-1:2006 表 D.1 参照），表 3 に示すように $MTTF_d$ = 約 42.75[years]を得たとする。ただし、DC については、その障害が毎回の通常停止でのオーバラン監視（これは“プロセスによる障害検知”にあたる）で検出できるとしても ISO 13849-1:2006 の表 E.1 に記されているように $PL=e$ に必要な条件を満足できない。このため、別途“何らかの方策”を講じてあり、抵抗値の変化を検知できるようになっていると仮定し、この仮定の上で 97.5%を想定する。

注記 32) ISO 13849-1 では“プロセスによる障害検知だけでは $PL=e$ の DC の要求を満足できない”としているので、上記の“何らかの方策”がない限り DB 回路を急停止機能に含めるべきでない。

注記 33) オーバラン監視は $PL=e$ (Cat.4) に適合する必要がある（JIS B 6410 参照）。

表 3 DB 回路の $MTTF_d$ の見積もり例

コンポーネント	使用数 N	$MTTF_d$	$N/MTTF_d$
抵抗	3	22831[y] (最悪値)	0.0001314
コンタクタ	1	43[y] (仮定 (23) 参照)	0.0232558
$\Sigma 1/MTTF_d = 0.0233872$			
DB 回路全体の $MTTF_d = 42.75[y]$			

- (26) ダイナミックブレーキではモータは正常作動しなければならない。ここでは、モータを部品毎のレベルに分解し、機械部分については 3.1 節に、電気・電子部分については 3.4 節に従って解析した結果、障害を除外できないことが判明したとし、そこで、 $MTTF_d$ については製造元より得た平均寿命 ($MTTF$) 50 年のデータを適用するとする。DC は ISO 13849-1:2006 附属書 E の表 E.1 にある“プロセスによる障害検知”を適用して 99%を仮定する。

注記 34) DC = 99%の仮定は、運転中常時動作が監視されていることを踏まえたもので

あって、あくまでも仮定である。ISO 13849-1 では「プロセスによる障害検知だけでは PL=e の DC の要求を満足できない」とされており、障害除外が適用されない限り、“モータが正常である”を急停止機能の条件に入れるべきではない。

- (27) エアバルブについては危険側となる単一障害（例えば、任意の中間位置でのスティック）を除外できない。冗長化されているので Cat.4 の構造要件は満足している。バルブ単体の $MTTF_d$ は ISO 13849-1:2006 附属書 C の空圧機器の標準 B_{10d} 値（20 000 000 回）とし、バルブの作動頻度（1 年 240 日、1 日 16 時間稼動、平均作動周期 30 秒を仮定）から附属書 C の例 C.4.3 に従って計算し、 $MTTF_d$ = 約 434[years] となったとする。DC は ISO 13849-1:2006 附属書 E の表 E.1 にある“直接監視”を適用して 99%を仮定する。

となり、

- (28) コンタクタとエアバルブからなる 1 チャンネルの $MTTF_d$ は約 39[years]、インバータ（回路遮断）、DB 回路及びエアバルブからなる 1 チャンネルの $MTTF_d$ は約 28[years] となり、これを ISO 13849-1:2006 附属書 D の式 D.2 を用いて対称化すると 1 チャンネルの $MTTF_d$ は約 33.8[years]（高）となる。また、平均 DC は ISO 13849-1:2006 附属書 E の式 E.1 を用いて 98.5%（高、許容範囲）となる。さらに、ISO 13849-1:2006 附属書 F に従って CCF に対する方策を評価し、65 点以上のスコアとなったとする。以上のことから、出力部分（O）は PL=e に適合すると見なせ、ISO 13849-1:2006 の表 K より、その平均危険側故障率は 8.57×10^{-8} 以下と導かれる。

これにライトカーテンと冗長化安全コントローラの平均危険側故障率を加え、システム全体で最終的に 10^{-7} 未満であれば、この急停止システム例が PL=e（Cat.4）に適合すると見なせる。

6) 制動機構の作動に要する時間

図 16 の安全関連ブロック図より、コンタクタ及びインバータ（回路遮断）を除く、“条件 b) 制動機構の作動”に関連するコンポーネントを抜き出したものを図 17 に示す。

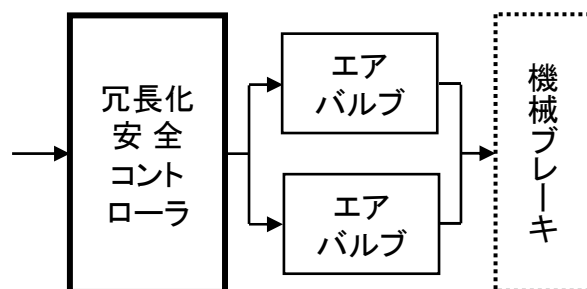


図 17 “制動機構の作動”の安全関連ブロック図

評価すべき時間は“冗長化安全コントローラの遅れ（仮定(4)より、単一障害では指定された安全機能を喪失しないとしたため、いわゆる通常の遅れ時間）” + “エアバルブの遅れ” + “機械ブレーキの作動遅れ”の合計であって、何れか一方のエアバルブに不具合発生を想定し、最も

時間が長い状況が条件 b) におけるワーストケースとなる。

7) 電源遮断に要する時間

図 16 の安全関連ブロック図より“条件 c) 電源遮断に要する時間”に関連するコンポーネントを抜き出したものを図 18 に示す。ただし、インバータ回路遮断が完了してからコンタクタが開動作するように冗長化安全コントローラのプログラムでディレーを設けていることを強調するため、これを破線で表している。

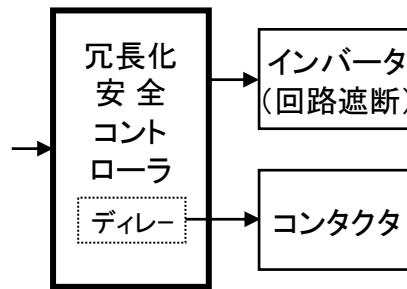


図 18 “電源遮断”の安全関連ブロック図

障害解析結果によるが、一般には“冗長化安全コントローラの遅れ（仮定(4)より、単一障害では指定された安全機能を喪失しないとしたため、いわゆる通常の遅れ時間）”＋“ディレー時間”＋“コンタクタの主接点 OFF 動作時間”の合計を評価することになり、コンタクタに不具合発生を想定し、最も時間が長い状況が条件 c) におけるワーストケースとなる。

8) スライドの制動に要する時間

図 14 の急停止システム例で“条件 a) スライドの制動に要する時間”にダイナミックブレーキの効果を必須とする場合、関連するコンポーネントを抜き出すと、図 19 に示すように DB 回路と、これに加えてモータ（特にコイル及び内部配線部分）が単独で直列接続された安全関連ブロック図となる。

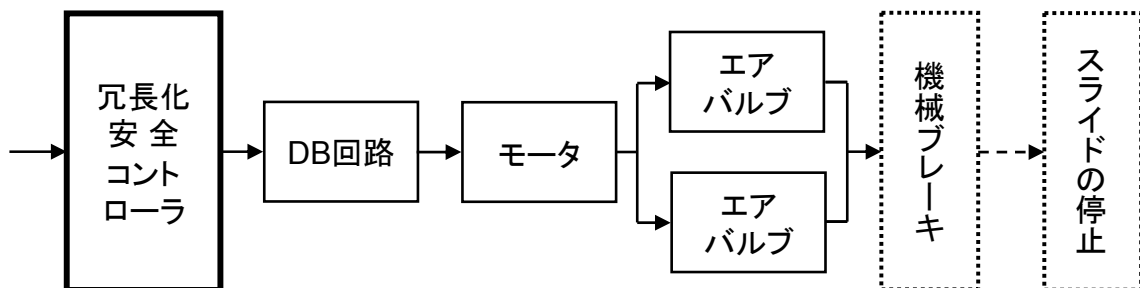


図 19 DB 回路の効果を必須とする“スライドの制動”の安全関連ブロック図

すなわち、単一障害を想定せざるを得ない DB 回路（及びモータ）の効果をスライド制動時間に必須の条件としてしまうと、ダイナミックブレーキが所定の性能を発揮しなければ急停止機能を喪失してしまうことを表している。

したがって、ここではダイナミックブレーキは機械ブレーキの摩耗を軽減する補足制動手段と位置付けることにする（この場合には **5**）の PL=e (Cat.4) の解析でも含めない）。改めて、図 14 の急停止システム例で“条件 a) スライドの制動に要する時間”に関連するコンポーネントを抜き出すと図 20 になる（急停止時間の評価という本項の目的に則し、安全関連ブロック図を拡張して、各コンポーネントの動作時間が容易に比較できるような表現としている。）なお、冗長化安全コントローラについては、仮定[4]より単一障害では指定された安全機能を喪失しないとされたため、この例ではいわゆる“通常の遅れ時間”を考慮する。

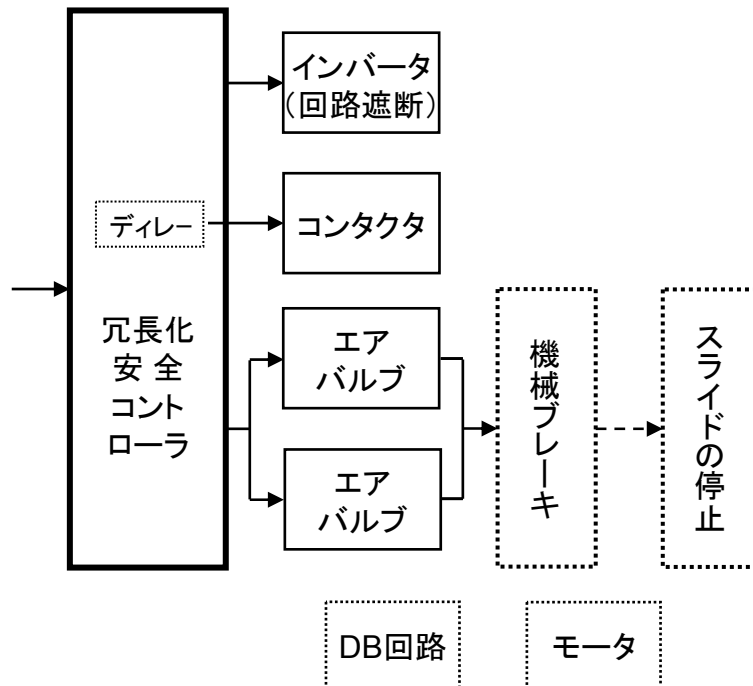


図 20 “スライド停止”（これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない）

9) 急停止時間の決定

以上の検討から、下記の 5 つの条件での時間が得られるので、

- ・ **3)**で得た“サーボシステムの故障による異常速度時の急停止時間”
- ・ **4)**で得た“エアバランサの故障時の急停止時間”
- ・ **6)**で得た“制動機構の作動に要するワーストケース”
- ・ **7)**で得た“電源遮断に要するワーストケース”
- ・ **8)**で得た“スライドの制動に要するワーストケース”

このうち最も長い時間を急停止時間として決定する。

5.4 例3：停止カテゴリ1のシステム（遅延回路によって停止カテゴリ0に切り替える場合）

1) 想定するシステムの概要

停止カテゴリ1の停止として急停止機能を実行する急停止システムの例を図21に示す。

このシステムでは、ライトカーテンから急停止信号としてOFF信号が出力されると冗長化安全コントローラからの指令を介してNCコントローラの制御でサーボによるスライドの減速が実行される。ただし、遅延回路（コンデンサC）で設定した一定時間を経過すると、安全リレーKを介してインバータ一次側で電源遮断が行われ、同時にエア式機械ブレーキが作動する。

通常停止は停止カテゴリ1の停止で行うものとし、毎回上死点で電源遮断及び機械ブレーキの作動が実行される。機械ブレーキの制動性能（摩擦版の劣化）は始動時及び8時間毎にJIS B 6410 簡条5.6.5にある“静的な制動性能監視”を実行して検査される。

モータの回転速度は、エンコーダG1によって標準NCコントローラと冗長化安全コントローラにフィードバックされる。冗長化安全コントローラはエンコーダG2によりスライド位置も監視しており、クロスモニタリングによって、G1の障害を検出できる。これらは、モータの速度監視だけでなく、“静的な制動性能監視”でも利用される。

圧力供給はユーザー側の設備で行われるが、供給圧の低下（含む供給停止）は考慮する。2

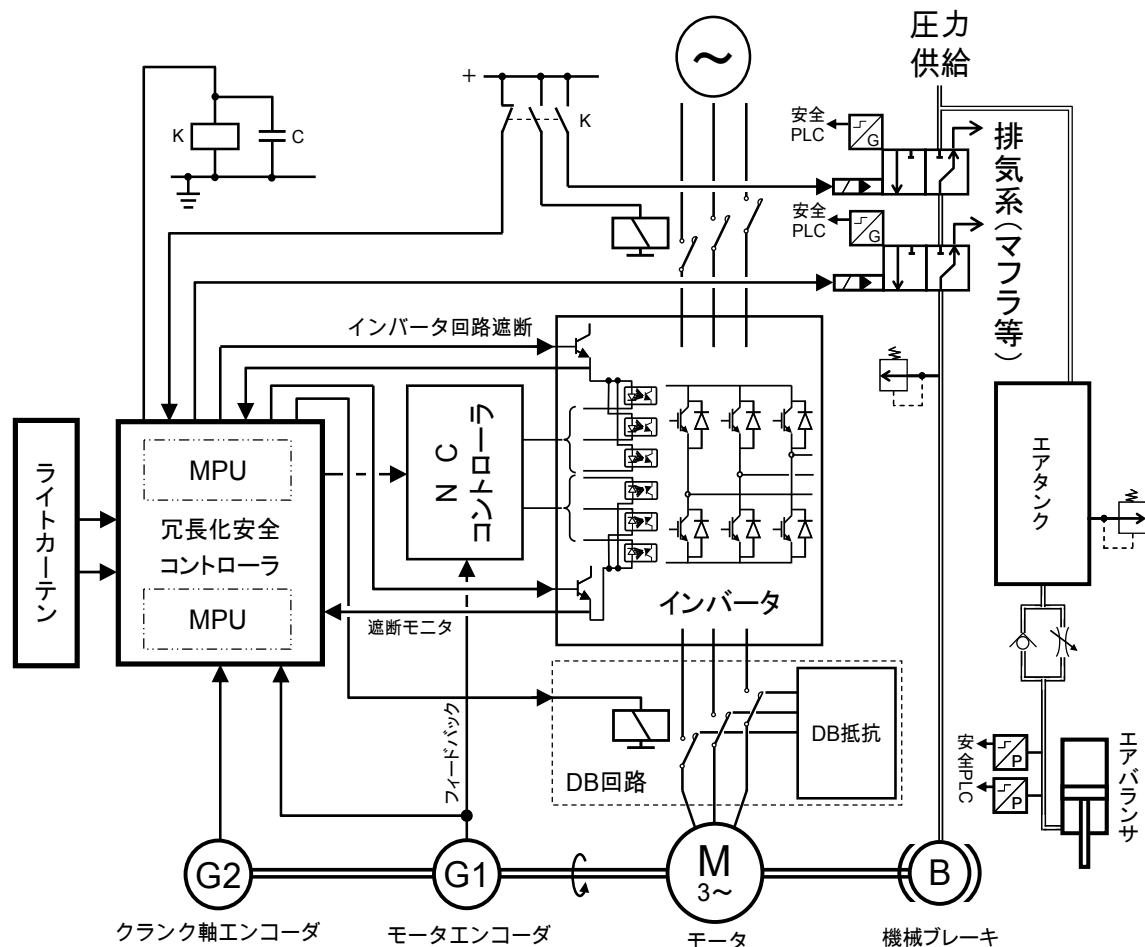


図21 システム例3

（※クランク軸以降のリンク機構、スライド、コンタクタのバックチェック用ミラーB 接点は作図を省略している。）

つの圧力スイッチによってエアバランサピストン配管接続部近傍でその内圧が直接測定される。機械ブレーキ系及びエアバランサ系は金属配管で配管されている。いずれもネジ式調圧弁を備えており、このため圧力上昇は各々の調圧弁の設定圧までしか考慮しない。

2) 構成品の条件、障害の除外

下記以外の項目は、前述した 5.3 節の 2) と同じであるため割愛する。

- (1) 安全リレー K の開動作は直接駆動する B 接点（：リンクドコンタクト，JIS C 8201-5-1 附属書 L 参照）を用いて冗長化安全コントローラでバックチェックされる。また，その B10d 値が製造元より入手できているとする。
- (2) コンデンサ C のいかなる障害も，必ず安全リレー K を OFF させるように影響し，K の OFF 動作時間延長を招かない場合には，コンデンサ C を検討から除外してもよい。
- (3) バルブに設けたポジションセンサと同様に，エアバランサピストン配管接続部近傍に設けた圧力スイッチについては，故障解析の結果，本稿 3.4.2 項で述べた想定されるいかなる障害又は両者の不一致動作が，すべて圧力異常として検出されることが解っているとする。

3) サーボシステムの故障による異常速度時の急停止時間

サーボシステムの故障がライトカーテンからの機能要求の前及び要求時に起こり，速度監視機能で検出される場合については，5.3 節の 3) で述べたのと同様に扱う。すなわち，検出及び電源遮断までの遅れを考慮して，スライド制動時間を検討する際の速度を設定する。この例では，“サーボによる減速制御は行われない”ことは前提にしなければならないが，インバータ回路遮断及びコンタクタ，機械ブレーキ，ダイナミックブレーキ等の他の要素に不具合を想定する必要はない。

急停止要求があった時点ではサーボシステムは正常であったが，一旦急停止機能を開始した後急停止が完了する前の任意の時点でサーボシステムの故障が発生した場合については，しばらくの間サーボ減速を行った後に，サーボシステムが異常加速を電源遮断されるまで続けたことを想定しなければならず，スライド動作の動的な解析が必要になる。ただし，サーボ制御によるスライド制動のほうが機械ブレーキによる場合よりも減速能力が高い場合（サーボ減速のほうがより早くスライドを停止できる場合）は，急停止要求直後にサーボシステムの異常が発生した状況がワーストケースであることが明らかなので検討を省略してよい。

4) エアバランサの故障による重量補償機能異常時の急停止時間

エアバランサの故障について，図 21 のシステムではバランサピストン内圧を監視していると見なせるため，測定実験では監視圧力値に設定して評価する。

5) PL=e (Cat.4) の検証

障害除外に該当するコンポーネント（機械ブレーキ，排気系，調圧弁，ポジションセンサ等）及び急停止機能に直接関与しないコンポーネントを除いた急停止システムの安全関連ブロック図を図 22 に示す。これまでの例と同様に，これが PL=e (Cat.4) に適合することを確認する。

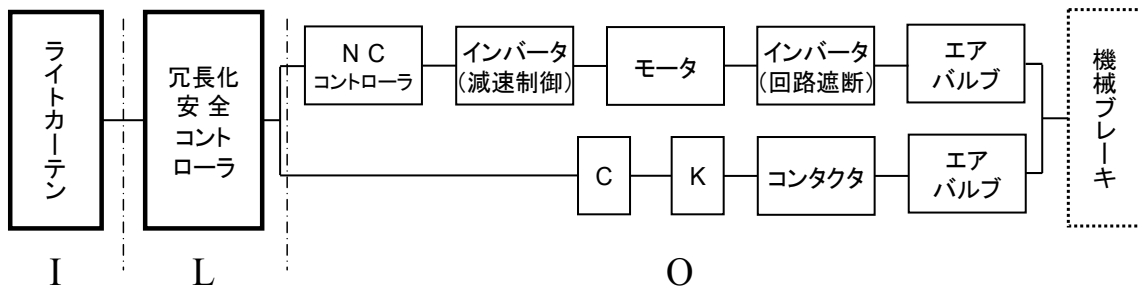


図 22 システム例 3 の安全関連ブロック図

スライドの減速・停止をサーボ制御で行う停止カテゴリ 1 の停止では、モータがトルクを失う不具合は危険側故障であり、その結果、NC コントローラ（これには組込みソフトウェアも含む）、インバータ（減速制御に関連する部分）及びモータが一方のチャンネルに直列接続されることになる。MTTF_dはもとより DC, CCF, システムティック故障抑制の点で PL=e (Cat.4) の要求を満足できず、減速制御を付加的機能と見なし、急停止システムの動作としては、一定時間後に電源遮断する停止カテゴリ 0 の停止として扱わざるを得ない場合もある。

6) 制動機構の作動に要する時間

図 22 の安全関連ブロック図より，“条件 b) 制動機構の作動”に関連するコンポーネントを抜き出したものを図 23 に示す。ただし、安全コントローラが直接作動させるバルブについては、減速制御の時間分を待機するためにプログラム上で何らかのディレーが設けられていることを仮定し、これを上側チャンネルの表現に含めている。

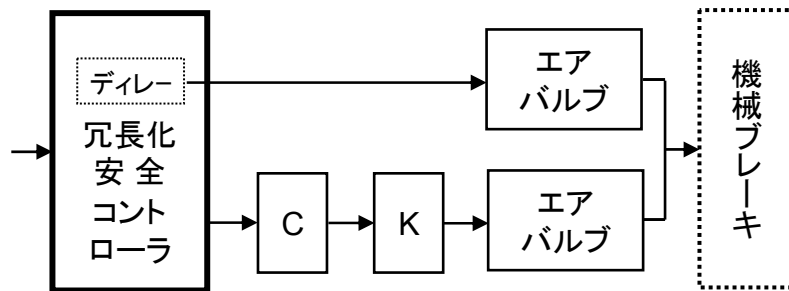


図 23 “制動機構の作動”の安全関連ブロック図

ただし、冗長化安全コントローラについては、ここでは単一障害では指定された安全機能を喪失しないことを仮定しているため、いわゆる通常の遅れ時間を考察の対象とする。それ以外のリレー K、コンデンサ C、何れか一方のエアバルブに不具合発生を想定し、最も時間が長い状況が条件 b)におけるワーストケースとなる。

7) 電源遮断に要する時間

図 22 の安全関連ブロック図より“条件 c) 電源遮断に要する時間”に関連するコンポーネントを抜き出したものを図 24 に示す。

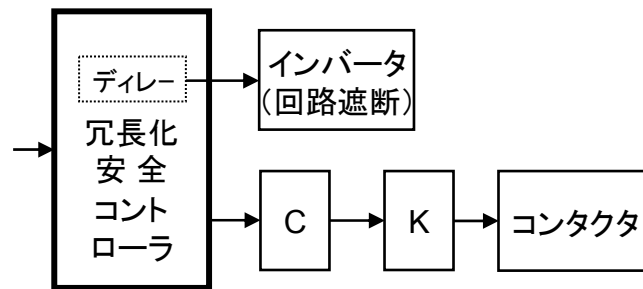


図 24 “電源遮断”の安全関連ブロック図

ただし、インバータ回路遮断については、減速制御の時間分を待機するためにプログラム上で何らかのディレーが設けられていることを仮定し、これを上側チャンネルの表現に含めている。冗長化安全コントローラについては、ここでは単一障害では指定された安全機能を喪失しないことを仮定しているため、いわゆる通常の遅れ時間を考察の対象とし、それ以外のリレーK、コンデンサC、コンタクタの何れかに不具合発生を想定し、最も時間が長い状況が条件 b)におけるワーストケースとなる。

8) スライドの制動に要する時間

図 21 の急停止システム例で“条件 a) スライドの制動に要する時間”に関連するコンポーネントを抜き出すと図 25 になる（急停止時間の評価という本項の目的に則し、安全関連ブロック図を拡張して、各コンポーネントの動作時間が容易に比較できるような表現としている）。

サーボ減速制御については、サーボシステムの故障による異常加速はすでに前述の 3) で評価しているので、ここでは障害発生による減速能力の低下（トルクフリー状態の発生）についてのみ検討する。

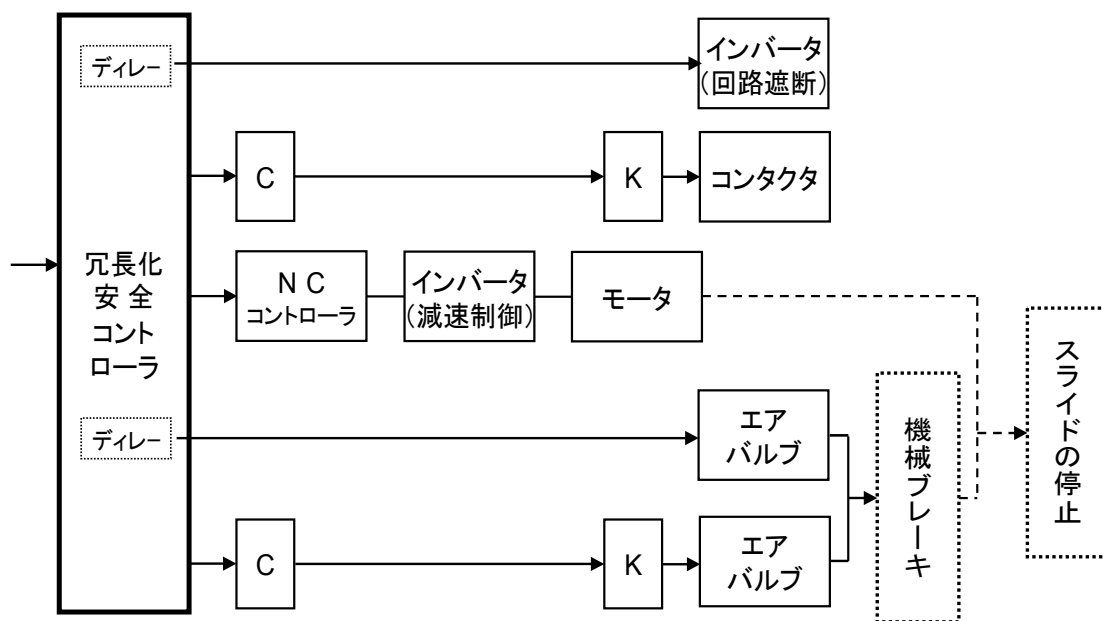


図 25 “スライド停止”（これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない）

他方、機械ブレーキについては、**5)**の検討の結果から減速制御を急停止システムに含めることができるのであれば、不具合は想定しなくてよい。単一障害の仮定から、機械ブレーキに不具合を仮定すれば減速制御は正常であるとでき、スライドを制動できることは明らかであるからである。**5)**の検討の結果、減速制御をカウントできない場合は 4.1.3 項に従って機械ブレーキを吟味し、該当する項目があれば不具合の発生を考慮する。

9) 急停止時間の決定

以上の検討から、下記の 5 つの条件での時間が得られるので、

- ・ **3)**で得た “サーボシステムの故障による異常速度時の急停止時間”
- ・ **4)**で得た “エアバランサの故障時の急停止時間”
- ・ **6)**で得た “制動機構の作動に要するワーストケース”
- ・ **7)**で得た “電源遮断に要するワーストケース”
- ・ **8)**で得た “スライドの制動に要するワーストケース”

このうち最も長い時間を急停止時間として決定する。

5.5 例 4：停止カテゴリ 1 のシステム（サーボ異常検出によって停止カテゴリ 0 に切り替える場合）

1) 想定するシステムの概要

停止カテゴリ 1 の停止として急停止機能を実行する急停止システムの例を図 26 に示す。

このシステムでは、ライトカーテンから急停止信号として OFF 信号が出力されると冗長化安全コントローラからの指令を介して NC コントローラの制御でサーボによるスライドの減速が実行される。ただし、減速制御中にサーボ制御に異常が起これ、これを偏差過大などの形でエンコーダを用いた監視機能（この機能は冗長化安全コントローラに実装）によって検出すると、安全リレー K を介してインバータ一次側で電源遮断が行われ、同時にエア式機械ブレーキ及びダイナミックブレーキ回路（DB 回路：コンタクタと抵抗で構成される）を作動させる。

通常停止は停止カテゴリ 1 の停止で行うものとし、毎回上死点で電源遮断及びダイナミックブレーキと機械ブレーキの作動が実行される。機械ブレーキの制動性能（摩擦版の劣化）は始動時及び 8 時間毎に JIS B 6410 箇条 5.6.5 にある“静的な制動性能監視”を実行して検査される。モータの回転速度は、エンコーダ G1 によって標準 NC コントローラと冗長化安全コントローラにフィードバックされる。冗長化安全コントローラはエンコーダ G2 によりスライド位置も監視し

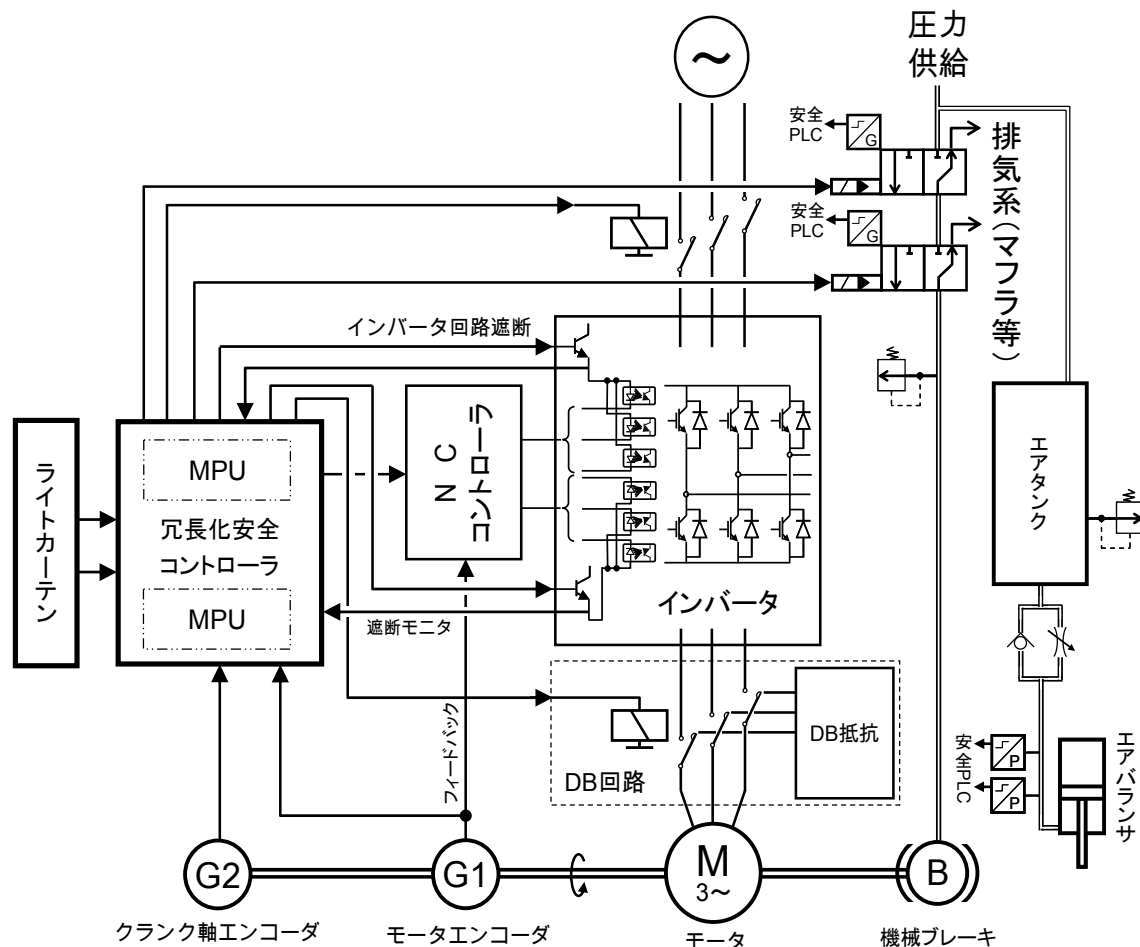


図 26 システム例 4

(※クランク軸以降のリンク機構、スライド、安全リレーのバックチェック用リンクド B 接点、コンタクタのバックチェック用ミラー B 接点は作図を省略している。)

ており、クロスモニタリングによって、G1 の障害を検出できる。これらは、安全コントローラに実装されたモータの速度監視、減速制御の正常性監視、静的な制動性能監視で利用される。

圧力供給はユーザー側の設備で行われるが、供給圧の低下（含む供給停止）は考慮する。2 つの圧力スイッチによってエアバランサピストン配管接続部近傍でその内圧が直接測定される。機械ブレーキ系及びエアバランサ系は金属配管で配管されている。いずれもネジ式調圧弁を備えており、このため圧力上昇は各々の調圧弁の設定圧までしか考えない。

2) 構成品の条件、障害の除外

該当する事項については 5.2～5.4 節で掲げた事項と同様の内容であるため割愛する。

3) サーボシステムの故障による異常速度時の急停止時間

5.4 節の 3) とほぼ同様であるが、サーボシステムの異常加速を仮定しているので、モータ自体は正常であると考えられるので、ダイナミックブレーキの効果をスライド減速時間に加味してよい。なお、モータの構造的な不具合については、後の 8) で述べるスライドの制動に要する時間で考慮する。

4) エアバランサの故障による重量補償機能異常時の急停止時間

5.4 節の 4) と同様、バランサピストン内圧を監視していると見なせるため、測定実験では監視圧力値に設定して評価する。

5) PL=e (Cat.4) の検証

障害が除外されたコンポーネント（機械ブレーキ、排気系、調圧弁、ポジションセンサ等）及び 4) で検討したエアバランサを除く、急停止システムの安全関連ブロック図を図 27 に示す。

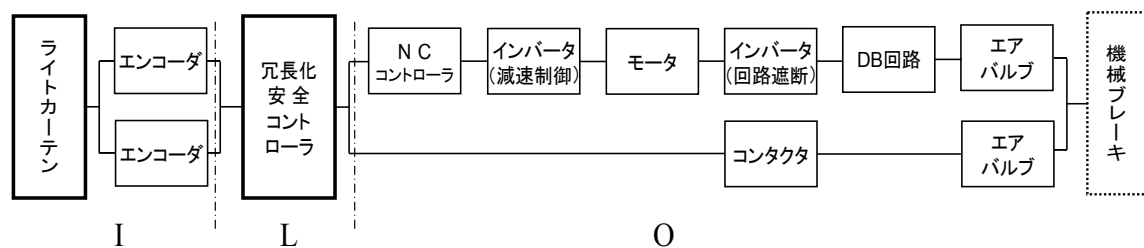


図 27 システム例 4 の安全関連ブロック図

5.4 節のシステム例 3 と異なり、このシステム例 4 では 2 つのエンコーダも安全関連部に含まれる。ただし、この例に示すように冗長化しているため、どちらかに障害が発生しても急停止機能を喪失しないことが分かる（エンコーダが 1 つだけ直列に接続されたのであれば、これに障害が起これば、入力から出力まで信号が流れきらない）。

他方、DB 回路をインバータのチャンネルかコンタクタのチャンネルのどちらに帰属させるかについては、ISO 13849-1:2006 附属書 D の式 D.2 を用いて冗長化チャンネルの平均 $MTTF_d$ を導出した結果を比較し、平均 $MTTF_d$ がより低い値となる配置を選ぶ。

PL=e (Cat.4) の検証において、4.1 項の 5)及び4.2 項の 5)と同様に、ライトカーテンと冗長化安全コントローラの平均危険側故障率を最後に加える場合には図 27 を次のように書き換えてもよい。

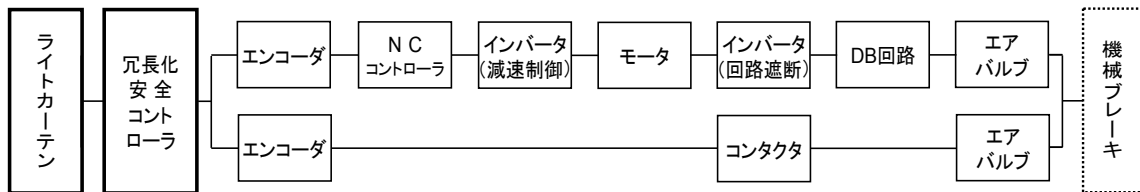


図 28 システム例 4 の安全関連ブロック図

最終的にシステム全体の平均危険側故障率が 10^{-7} 未満であれば PL=e (Cat.4) に適合すると見なせるが、NC コントローラ（これには組込みソフトウェアも含む）、インバータ（減速制御に関連する部分）及びモータが直列接続されることになり、さらに DB 回路も加わり、これらについて $MTTF_d$ はもとより DC, CCF, システマティック故障抑制の点で PL=e (Cat.4) の要求に適合するか十分な吟味が必要である。

6) 制動機構の作動に要する時間

“制動機能の作動に要する時間”は、実際には実システムの故障解析によって場合分けして評価することになる。その指針を示す意味で、ここでは典型的な故障状態を想定して述べる。

6-a) 正常に減速制御が実行された場合

このシステム例では、減速制御でスライドが停止したことを検出してから電源遮断を行うような構成がなされる。したがって、ライトカーテンからの機能開始要求に対して、急停止開始処理の遅れのみならず、停止検出処理に要する時間（あるいは、停止検出後にプログラム上で付加したディレー）を考慮する必要がある、図 29 のように表現される。

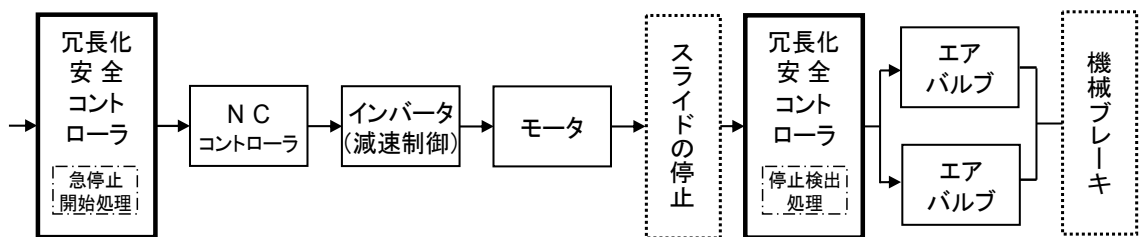


図 29 正常に減速制御が実行された場合の“制動機構の作動”
(これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない)

6-b) 減速制御に異常を生じた場合

急停止機能要求前にサーボシステムに異常が生じた場合については、すでに 3)で検討している。したがって、ここでは、急停止動作中にスライドが停止する前の任意のタイミングで減速制御が実行できなくなった状況（トルクフリーの状況）を想定するが、ここには減速制御の異常を検出するまでの遅れを含める必要がある。これを示すと図 30 のようになる。

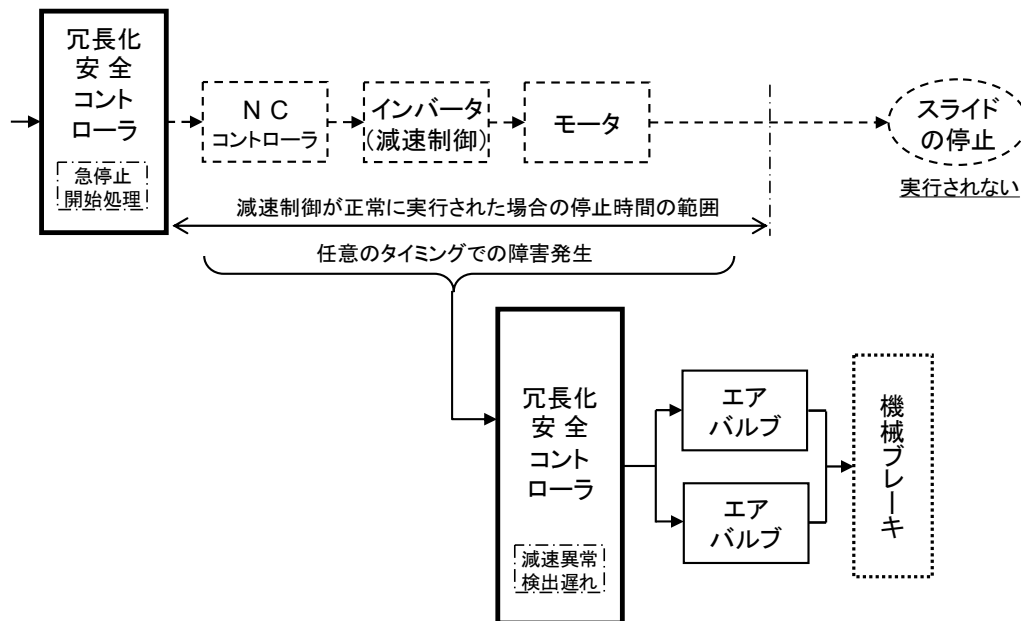


図 30 急停止機能要求前にサーボシステムに異常が生じた場合

この場合には、時間がより経過した後で減速制御に異常が発生するほうが結果的に停止カテゴリ 0 の停止に移行するのが遅くなり、機械ブレーキの作動までに多くの時間が費やされることになるのが分かる（機械ブレーキの作動までの時間であって、スライドの制動・停止に要する時間については後の 8) で述べる）。ただし、偏差異常などによる減速制御の異常検出を仮定すれば“正常時の本来のスライド停止時間が経過したのにサーボが停止していない”ということから最低限サーボ異常が判別できると考えられ、よって、障害発生を仮定する時間の範囲は本来正常に減速制御が実行された場合のスライド停止時間を超えることはないと考えることができる。この仮定が該当するのであれば、ワーストケースとしては図 31 の状況を検討すればよい。

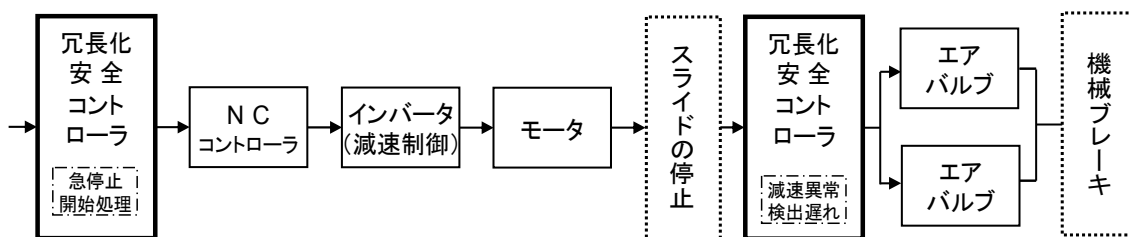


図 31 減速制御に異常が発生した場合の“制動機構の作動”のワーストケース
(これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない)

なお、図 29 との比較から、仮に減速制御異常検出処理の遅れが図 29 で示した停止検出処理に要する時間（あるいは、停止検出後にプログラム上で付加したディレー）よりも短いのであれば、6-a) の場合より時間が長くなることはないのが明らかであるので、この検討は省いてもよい。

c) エンコーダに障害が発生した場合

5) の検証で $PL=e$ (Cat.4) に適合していると見なせる場合、エンコーダについてはいずれの障害が起こっても減速制御に異常を生じたのと同様に処理されると仮定でき、したがって、6-b) に準じる。

7) 電源遮断に要する時間

6)と同様“電源遮断に要する時間”は実際には実システムの故障解析によって場合分けして評価することになるが、典型的な場合を以下に示す。

7-a) 正常に減速制御が実行された場合

このシステム例 4 では、減速制御でスライドが停止したことを検出してから電源遮断が行われる。このため、ライトカーテンからの機能開始要求に対して、急停止開始処理の遅れのみならず、停止検出処理に要する時間（あるいは、停止検出後にプログラム上で付加したディレー）を考慮する必要がある。

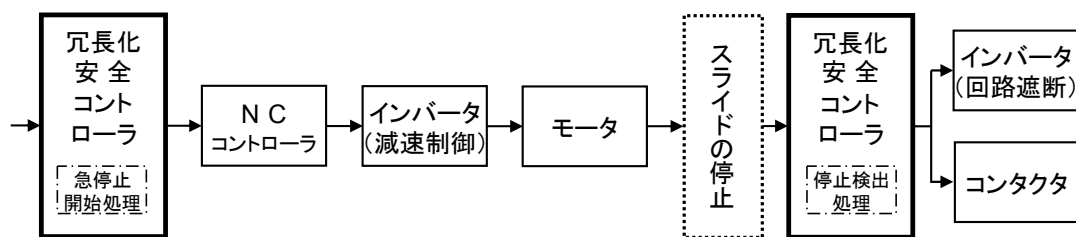


図 32 正常に減速制御が実行された場合の“電源遮断”
(これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない)

7-b) 減速制御に異常を生じた場合

急停止機能要求前にサーボシステムに異常が生じた場合については、すでに 3) で検討している。したがって、ここでは、急停止動作中にスライドが停止する前の任意のタイミングで減速制御が実行できなくなった状況を想定するが、6) で述べたようにワーストケースとしては図 33 の状況を検討すればよい。

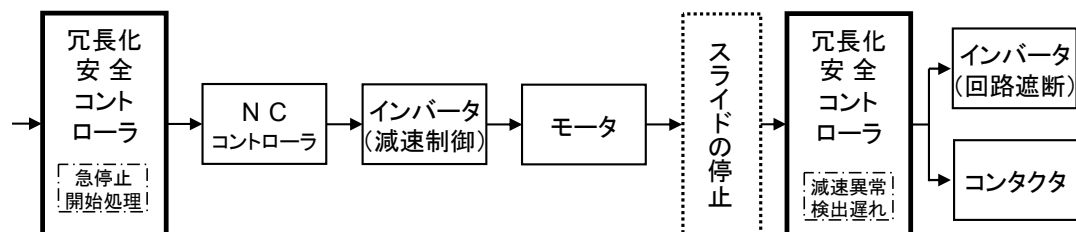


図 33 減速制御に異常が発生した場合の“電源遮断”のワーストケース
(これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない)

なお、図 32 との比較から、仮に減速制御異常検出処理の遅れが図 32 で示した停止検出処理に要する時間（あるいは、停止検出後にプログラム上で付加したディレー）よりも短いのであれば、7-a) の場合より時間が長くなることはないのが明らかであるので、この検討は省いてもよい。

c) エンコーダに障害が発生した場合

5) の検証で PL=e (Cat.4) に適合していると見なせる場合には、エンコーダについてはいずれの障害が起こっても減速制御に異常を生じたのと同様に処理されると仮定でき、b) の場合に準じる。

8) スライドの制動に要する時間

図 26 の急停止システム例 4 では機械ブレーキの制動能力よりもサーボ減速制御の能力のほうが高いことを仮定しており、また、急停止機能要求前にサーボシステムが異常加速した場合については 3) で検討しているから、ここでは“条件 a) スライドの制動に要する時間”として“急停止動作中にスライドが停止する前の任意のタイミングで減速制御が実行できなくなった状況（トルクフリー状態の発生）”に関して検討することになるが、その場合分けは、モータを部品毎のレベルに分解し、機械部分については 3.1 節に、また、電気・電子部分については 3.4 節に従って解析した結果、いかなる障害も除外できるか否かに分かれる。

モータの障害をすべて除外できる場合は、NC コントローラ及びインバータ（減速制御関連部分）に障害を仮定する（DB 回路及びモータに障害を仮定しない）ので、ダイナミックブレーキの減速効果を加味できる。また、DB 回路の作動はサーボ電源遮断も兼ねる。したがって、ここでワーストケースとして検討する状況は図 34 で表される。

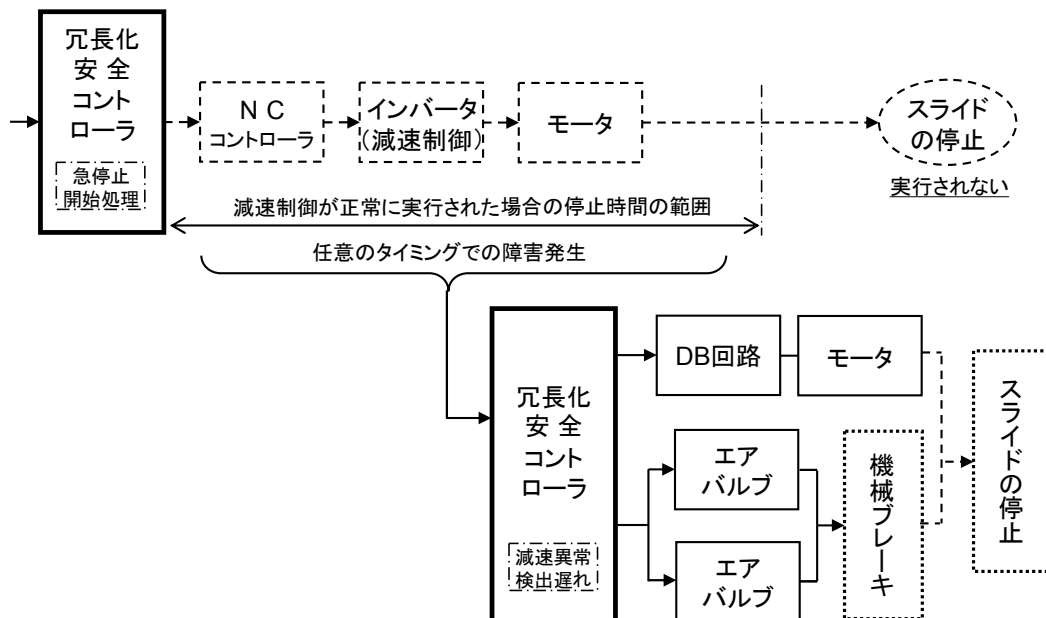


図 34 ダイナミックブレーキの効果を加味できる場合の“スライド停止”のワーストケース
(これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない)

これに対し、モータがトルクを発生できない不具合を除外できない場合は、DB 回路が正常であったとしても、ダイナミックブレーキの減速効果を加味できないので、ワーストケースとしては図 35 の状況を検討する必要がある（ただし、サーボ電源遮断は除いている）。

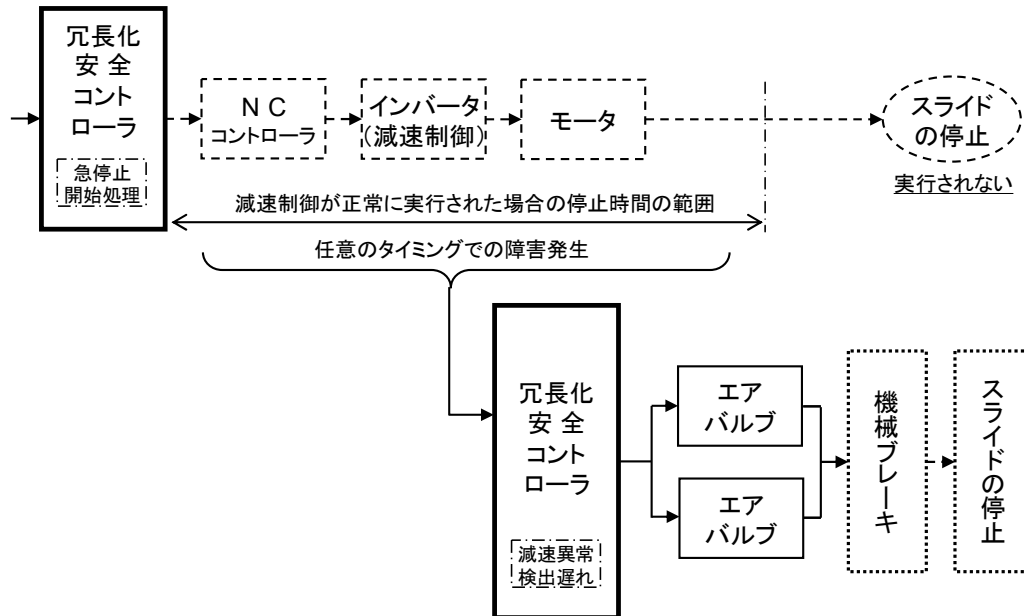


図 35 ダイナミックブレーキの効果を加味できない場合の“スライド停止”のワーストケース
(これは ISO 13849-1:2006 の安全関連ブロック図にはあたらない。)

図 34 と図 35 の状況では明らかに後者の方が制動時間を要するが、対象とする急停止システムがいずれに該当するかはモータの故障解析結果による。ただし、重要なことは、いずれの場合においても、サーボ減速制御に異常を生じるタイミングについて、

- ・急停止機能の開始直後に障害が発生したとする場合は既に 3) で検討されている。
- ・減速制御が正常に実行されたがスライドが停止する直前に障害が発生したとする場合は既に 6-b) で検討されている。

とできることである。

すなわち、ここでは上記以外のタイミングで障害が発生した状況を検討することになる。例えば、モータの障害を除外できず、ダイナミックブレーキを加味できない場合において、スライド速度をサーボ減速制御によって 50% 減速させた時点でサーボ系に障害が発生した状況を想定すると、サーボ減速制御による減速分だけ機械ブレーキによる制動時間が短縮されるので、検討する時間は図 36 のようになる。

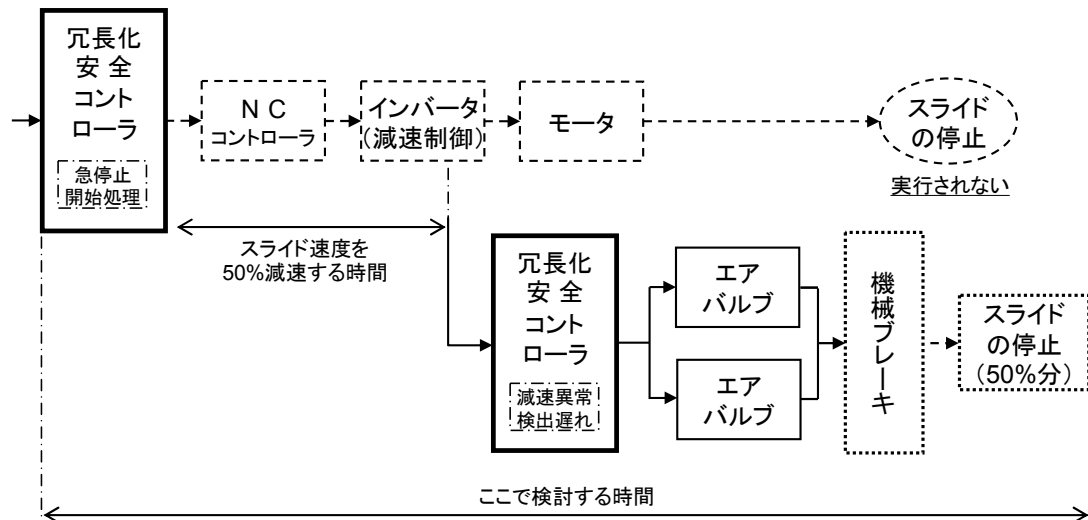


図 36 スライド速度を 50%減速した時点で障害が発生した状況を想定した“スライド制動”のワーストケース（ISO 13849-1:2006 の安全関連ブロック図にはあたらない）

9) 急停止時間の決定

以上の検討から、下記の 5 つの条件での時間が得られるので、

- ・ 3) で得た “サーボシステムの故障による異常速度時の急停止時間”
- ・ 4) で得た “エアバルブの故障時の急停止時間”
- ・ 6-a) または 6-b) で得た “制動機構の作動に要するワーストケース”
- ・ 7-a) または 7-b) で得た “電源遮断に要するワーストケース”
- ・ 8) で得た “スライドの制動に要するワーストケース”

このうち最も長い時間を急停止時間として決定する。

6. 結論

PL=e (Cat.4) を満足している急停止システムは、その定義より、単一障害が発生しても急停止を完了できる。ただし、発生した障害又は不具合を生じたコンポーネントの違いによっては、その完了時間が異なる場合があり、急停止時間には最も長い時間を明示しなければならない。

本研究では、急停止の標準化という JIS 本来の目的に照らし、このワーストケースの特定において故障や異常に対する解釈や評価に関する見解を述べ、さらに実際のシステム構成に基づいた急停止システムの例を挙げて急停止時間を決定していく具体的なプロセスを示した。

得られた結果は以下のとおりである。

- 1) ワーストケースを特定する際の基本的な考え方は、急停止時間を急停止機能の安全仕様の 1 つと捉え、急停止時間が延長されるという安全仕様に反する事態を安全機能の喪失と見なすことにある。この結果、検討すべき障害・不具合の範囲が要求される安全性能に応じて定まることになる。
- 2) PL=e (Cat.4) に適合している急停止機能は、検出可能な障害は安全機能要求前か要求時に必ず検出できることを前提にしてよい。さらに、ISO 13849-2 にリスト化された除外条件を満たす特定の障害に対しては検証の対象から外してもよい。
- 3) 急停止時間の解析において ISO 13849-1:2006 の安全関連ブロック図表現を拡張して用いることを提案した。また、急停止完了の 3 つの条件、プログラム設定を越えた異常速度の発生及びエアバランサ機能の不具合の発生については、これらを各々場合分けすることで解析を整理して実施できることを示した。

ただし、本資料で述べた諸事項、考え方及びプロセスは、あくまでも筆者の現時点までの見解であって、実際の急停止時間の評価に適用していく上で網羅されていない問題が指摘された場合には内容を修正したい。

なお、本資料で述べた急停止時間の考え方は機械サーボプレスを対象に考察したものである。したがって、特定すべきワーストケースと急停止システムの安全性能との関係についてなど参考とできる点も示してはいるが、他の構造のサーボプレス、すなわち、機械サーボプレスブレーキ、液圧サーボプレス及び液圧サーボプレスブレーキに対して本指針の内容がすべて適用できるとは言えず、別途個別に検討すべきであることに注意されたい。

さらに、法的に義務付けられている特定自主検査での急停止時間測定の取り扱いが重要な問題であるが、本研究の範囲では、これについて議論が尽くされているとは言えない。自主検査での急停止時間測定では、想定したワーストケースと同じ故障状態を擬似的に再現して仕様と比較するのが検査方法として最も厳密であるのは明らかである。ただし、この方法は検査終了後に正常な状態へ適切に復帰されない恐れを含んでおり、さらに、急停止機能の安全性能確保の意味でシステムの構成がより複雑化することは避けられず、これらの点から必ずしも実際的とは呼べない可能性がある。このため、例えば、

- 1) 機械ブレーキ動作は動的な制動性能監視で評価する。
- 2) 銘板で記す急停止時間とは別に、自主検査での評価用の急停止時間を設定しておき、その上

で、検査ではサーボ減速制御やダイナミックブレーキが正常な状態での急停止時間を評価する。

などの措置が考えられるが、結論を得るまでには至っておらず、今後の課題としたい。

謝 辞

本資料は、(独)労働安全衛生総合研究所と国内プレスメーカー6 社との共同研究課題「サーボプレスの急停止時間の決定法に関する研究」にて提供頂いた資料及び討論頂いた検討内容をもとに作成されたものである。本共同研究において、参加頂いた各メーカーの担当者各位には単なる情報提供にとどまらず、終始貴重なご指導ご助言を賜った。ここに記して深甚たる感謝の意を表す。また、本共同研究の遂行にあたっては、一般社団法人日本鍛圧機械工業会事務局に多大なご協力を頂いた。心より感謝申し上げる。

参考文献

- 1) (社)産業安全技術協会編：動力プレス機械（安全プレス）型式検定ガイド，TIIS-8，産業安全技術協会，1991
- 2) Michael Hauke, Michael Shaefer, 他：Functional safety of machine controls – Application of EN ISO 13849-, BGIA Report 2/2008, Institute for Occupational Safety and Health of German Social Accident Insurance, 2008
- 3) 梅崎重夫，清水尚憲，齋藤剛：プレス作業を対象とした安全技術の高度化に関する研究（平成 17 年度総括・分担研究報告），厚生労働科学研究成果データベース，200501018A，2006
- 4) 井上洋一，平尾裕司，蓬原弘一，川池囊，向殿政男（監修）：安全の国際規格 第 3 巻－制御システムの安全－ISO 13849-1(JIS B 9705-1), IEC 60204-1(JIS B 9960-1), IEC 61508(JIS C 0508)，日本規格協会，2007

付録（用語の解説）

以下では、本資料で用いている機械安全規格または機能安全規格特有の専門用語について解説する。ただし、これらに関してその概念や背景も含めて正確に理解できるよう詳述することは紙面の都合上限界があり、あくまでもこれらの定義を概説するにとどめる。さらに詳しい解説としては、例えば文献 4) が参考となるので参照されたい。

1) 停止カテゴリ（JIS B 9960-1 簡条 9.2.2）

停止機能はその動作特性の違いから次の 3 つに分類されており、この分類を停止カテゴリと呼ぶ。

停止カテゴリ 0：機械アクチュエータ（サーボモータ）の電源を即時に遮断することによる停止

停止カテゴリ 1：停止（減速）するために機械アクチュエータ（サーボモータ）が電源を使い、停止が完了してから電源を遮断する停止

停止カテゴリ 2：停止（減速）するために機械アクチュエータ（サーボモータ）が電源を使い、停止完了後も（静止を維持するために）機械アクチュエータに電源を供給したままにする停止

例えば、JIS B 6410 簡条 5.4.2 で、サーボプレスの非常停止機能は停止カテゴリ 2 の制御停止とすることは認めていない。なお、サーボプレスにおける電源遮断方法の分類については JIS B 6410 の付属書 D を参照されたい。

2) カテゴリ（JIS B 9705-1 定義 3.2）

障害に対する抵抗性（フォールト・レジスタンス）及び障害条件下での挙動に対する制御システムの安全関連部の分類で、表 4 に示す B、1～4 の 5 つがある。各々のカテゴリはコンポーネント（部分）の構造的配置、障害検知及び／又はこれらの信頼性により達成される。

表 4 カテゴリの概要

カテゴリ	要求事項の要約	障害に対する抵抗性	障害検出性能
B	使用中のストレスや環境、加工材料の影響を考慮。	単一障害の発生で安全機能を喪失する。	障害検出は考慮されていない。
1	十分吟味された技術（安全原則）及びコンポーネントを用いる。	故障発生率はカテゴリ B より低い単一障害で安全機能を喪失する。	障害検出は考慮されていない。
2	安全機能が適切な間隔で定期的にチェックされる。	チェックとチェックの間で障害が発生すると安全機能を喪失する。	チェックによって障害が検知される。
3	単一障害では安全機能を損なわない。	検出されない障害の蓄積で安全機能の喪失を招くことがある。	障害検出が実行される。しかし、完全ではない。
4	単一障害では安全機能を損なわず、かつ、あらゆる障害を直ちに検出できる か又は、 検出できない障害が蓄積しても安全機能を維持できる。		

3) 平均危険側故障時間：mean time to dangerous failure (MTTF_d) (ISO 13849-1:2006 定義)

制御システムの安全関連部（又はその単一チャンネル）が危険側故障するまでの推定時間の平均値。代表的な単一コンポーネントの MTTF_d 及び見積もり方法が ISO 13849-1:2006 付属書 C に、単一チャンネルの MTTF_d の推定方法が同規格付属書 D に述べられている。

4) 診断範囲：diagnostic coverage (DC) (ISO 13849-1:2006 定義 3.1.26)

周期的に実行される自動的な障害検出機能の診断効果の尺度であって、検出可能な危険側故障の発生確率を λ_{DD} ，すべての危険側故障の発生確率を λ_{Dtotal} で表すと、次式で与えられる。

$$DC = (\sum \lambda_{DD}) / \lambda_{Dtotal}$$

5) 共通原因故障：common cause failure (CCF) (ISO 13849-1:2006 定義 3.1.6)

単一の事象から生じた異なるアイテムの故障であって、これらの故障が互いの結果ではないもの。

6) システマティック故障：systematic failure (ISO 13849-1:2006 定義 3.1.7)

安全要求仕様の誤り，ソフトウェア設計の誤りなど，確定的要因に関係した故障。通常，設計，製造プロセス，運転手順，文書又は他の関連要因を変更しない限り除去することができないとされる。

7) パフォーマンスレベル：performance level (PL) (ISO 13849-1:2006 定義 3.1.23)

予見可能な条件下で制御システムの安全関連部による安全機能実行能力を指定するために用いるレベル。a～e の 5 段階があり，PL e が最も高いレベルを表す。PL は以下の項目を評価することで決定される。

- 単一チャンネルの MTTF_d
- DC の平均値
- CCF に対して適用された方策のスコア
- 安全関連部のアーキテクチャ構成及び障害条件下での安全機能の挙動（カテゴリ）
- 安全関連ソフトウェア
- システマティック故障を抑制・回避するために適用された方策
- 予期される環境条件下での安全機能遂行能力

8) 安全インテグリティレベル：safety integrity level (SIL) (JIS B 9961 定義 3.2.23)

安全関連電気制御システムの安全性能として，規定条件下で要求される安全機能を満足に実行する確率（安全インテグリティ）を指定するために用いるレベル。1～4 の 4 段階があり，SIL 4 が最も性能が高い（失敗する確率が低い）。ただし，機械におけるリスク低減要求の範囲では SIL 4 は必要ないとされ（一般に SIL4 はプロセス産業における悲劇的な事象に

対して割り当てられる), 機械の安全関連電気制御システムでは **SIL 3** を最高レベルとする。
また, 機械の安全関連電気制御システムが低頻度作動要求モードで稼働されることもないと
され, 高頻度作動要求又は連続モードのみが対象になる。

PL a～e と SIL 1～3 の単位時間当たりの危険側故障確率は互いに図 37 に示す関係にある。

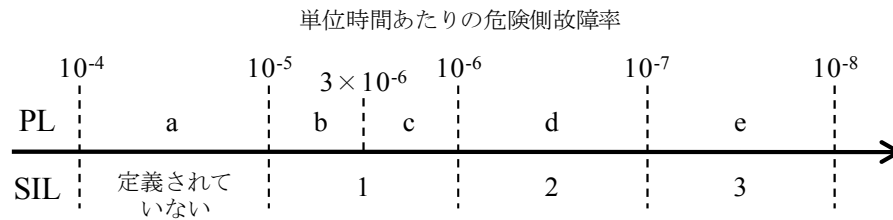


図 37 PL と SIL との対応関係

抄 録

サーボプレスの安全要求事項を示した JIS B 6410:2009 において、機械サーボプレスの「急停止時間」は急停止機能を実行するサブシステムに単一障害が発生した状況を想定し、急停止時間が最も長くなる場合（ワーストケース）での値として決定しなければならないとされている。しかし、ワーストケースを特定する際の個々の故障や障害に対する評価や考え方までは示されておらず、当該要求事項の解釈について統一された見解が得られているとは必ずしも言えない。

本資料では、JIS B 6410 及び関連する上位国際安全規格の要求事項、ならびに、現行の国内での動力プレスの故障に対する取り扱いなどを考慮に入れ、JIS B 6410 で要求される“ワーストケースの特定”の意味、ならびに、そこで対象となる障害の範囲について考察し、機械サーボプレスの急停止時間を決定する際の考え方を明らかにした。ここでの基本は、急停止時間を急停止機能の安全仕様の 1 つと捉え、急停止時間が延長されるという安全仕様に反する事態を安全機能の喪失と見なすことにある。これに従い、市場に投入されているサーボプレスにおいて採用されている典型的な急停止システムの構成例を挙げ、ワーストケースを特定していく具体的なプロセスを詳述した。

労働安全衛生総合研究所安全資料

JNIOSH-SD-NO.26 (2010)

発行日 平成22年10月12日 発 行
発行者 独立行政法人 労働安全衛生総合研究所
〒204-0024 東京都清瀬市梅園1丁目4番6号
電話 (042) 491-4512(代)

印刷所 株式会社 アトミ

SAFETY DOCUMENT
OF
THE NATIONAL INSTITUTE OF OCCUPATIONAL SAFETY AND HEALTH

JNIOOSH-SD-NO.26 (2010)

A Study on Procedure for Determining
the Protective Stopping Time of Mechanical Servo Presses



NATIONAL INSTITUTE OF
OCCUPATIONAL SAFETY AND HEALTH
1-4-6, Umezono, Kiyose, Tokyo 204-0024, JAPAN