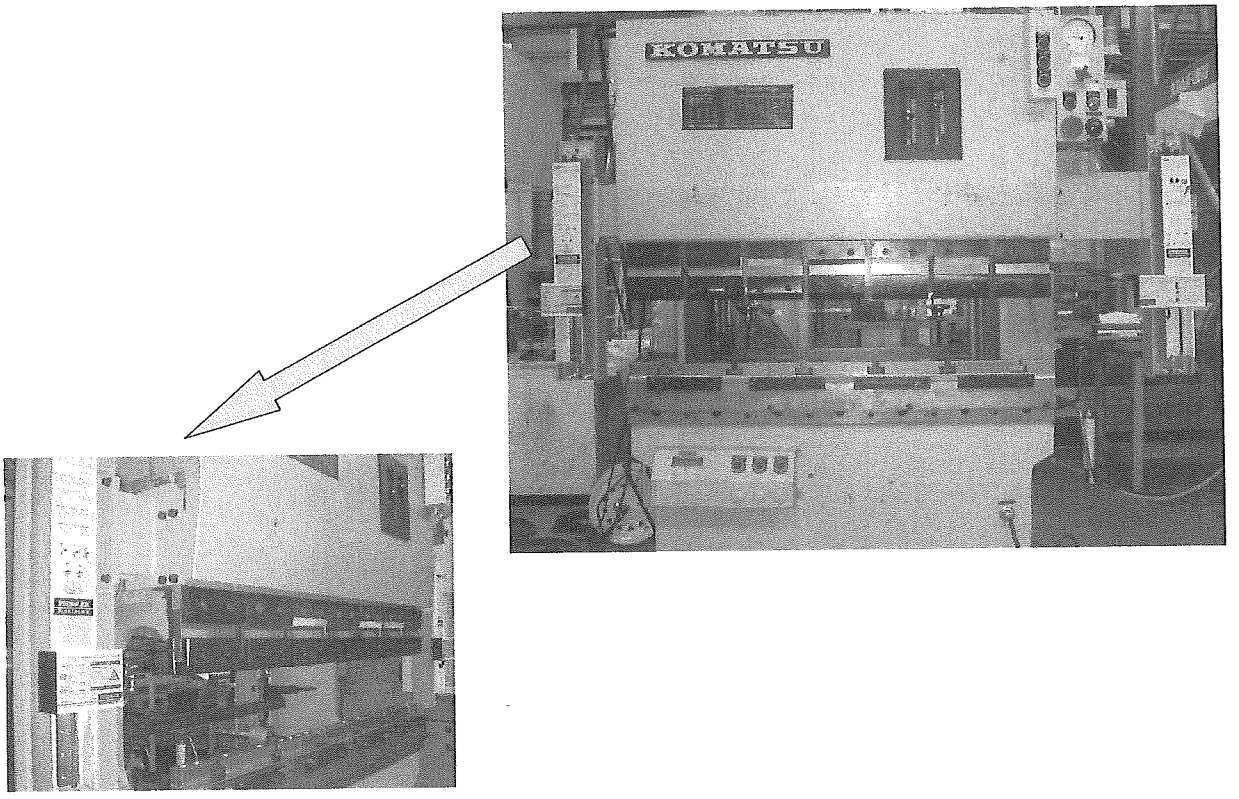

写真5-1　試験用プレスブレーキ

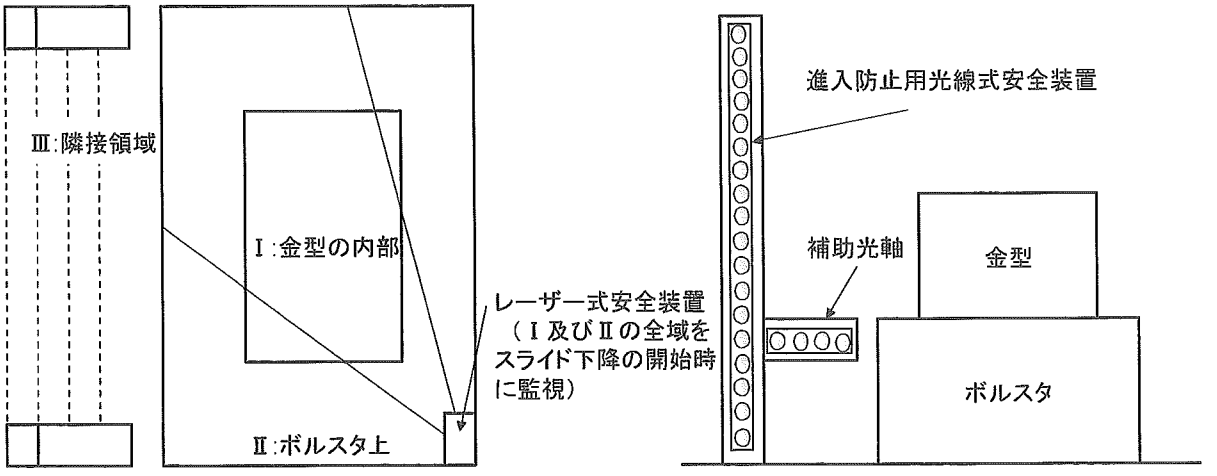

図6-1　大型プレス機械の安全システムの例

に，特定の権限を有する者（少なくともプレス作業主任者以上の管理監督者）でなければ，プレス機械のリセットやスタートができないようにする。

7. 結論

本研究では、当初、平成19年度に予定していたサーボプレスの安全要件の解明を平行して実施した。これは、交付決定書の付帯事項として「サーボプレスの安全要件の解明は平成17年度に行うことが望ましい」との指示が厚生労働省からあったためである。

また、平成18年度から労働安全衛生法にリスクアセスメント（災害防止対策を含む）に関する条項が追加されることを考慮し、プレス機械を対象としたリスクアセスメント手法と災害防止対策の検討も併せて実施した。

本研究によって得られた成果は次の通りである。

1）労働災害の分析結果では、平成11年から16年までに首都圏で発生したプレス機械による労働災害1,395件などの分析を行った。その結果、平成11年には46.8％、平成13年には44.5％であった障害部位での切断・挫滅の件数が平成15年は55.9%、平成16年は59.0％に達しており、災害の重篤化が推察された。

2）リスクアセスメント手法の開発では、最新の国際安全規格や安全技術の動向に配慮すると同時に、中小零細企業で簡単に実施できる効果的な手法の開発が要望されていた。そこで、プレス機械の種類ごとに最近の安全技術の高度化に配慮したリスク低減戦略の構築を試みた。また、労働災害の分析結果に基づく典型的災害事例を抽出し、プレス災害の多発している中小零細企業を対象に、当該事例を活用した簡単で効果的なリスクアセスメント手法の開発を進めている。

3）サーボプレスの安全要件は、きわめて単純であることが判明した。具体的には、①手指が危険限界内に進入していないか、またはスライドが下降していないことの常時監視、②サーボ制御系のフェールセーフ性の保証、③機械式ブレーキの停止性能の保証だけに集約できる。ただし、「スライドが下降していないこと」の常時監視がないと、安全要件は複雑になる。

以上のうち、①は、既存の報告書等では指摘されていないと思われる。したがって、今後の構造規格の改訂作業では、要件①の追加の必要性を検討すべきと考える。

また、②や③では、機能安全に基づく確率的なリスク低減策が必要である。そこで、②の課題の先端的研究機関であるドイツのダルムシュタット工科大学に産業安全研究所の研究官を派遣し、最新の機能安全的知見も踏まえた確率的な安全性評価手法の解明を試みた。また、③では機械式ブレーキのチェック間隔の確率的な安全性評価が課題である。

4）二次加工用プレスブレーキと大型プレス機械の安全システムの開発では、産業安全研究所が実施した大型プレス機械による死亡労働災害の調査などを活用して、安全システムの仕様検討を進めた。また、試験機を製作して問題点の解明を進めている。

今後は、以上の結果を基に産業現場で直ちに活用できるシステムや手法の開発を進めていくのが課題である。

参考文献

1)安全衛生年鑑(昭和30年代から現在まで)、中央労働災害防止協会
2)梅崎重夫・清水尚憲、産業機械の労働災害分析、産業安全研究所特別研究報告、NIIS-SRR-NO.33 (2005) pp.53-68
3)プレス事業場におけるリスクアセスメント入門マニュアル、中央労働災害防止協会 (2006)
4)社団法人日本鍛圧機械工業会、「サーボ駆動式プレス機械の規格・標準化の委員会報告書」(2005)
5)プレス技術特集号、サーボモータプレス機が実現する高付加価値加工、Vol.42, No.5 (2004)
6)社団法人産業安全技術協会、「動力プレス機械構造規格、及びプレス機械又はシャーの安全装置構造規格の国際整合化に関する調査研究委員会報告書」(2005)

付録　サーボプレスの駆動制御回路の安全性評価手法の検討

A. 1　研究目的

サーボプレスは，従来の機械プレスにおいて安全確保のために重要な役割を果たしてきたクラッチ機構やフライホイールを用いず，主駆動源であるACサーボモータを制御する駆動制御回路（サーボドライバ）によってスライドの動作が完全に支配されている点に構造上の特徴がある。このため，安全要件の解明では，サーボドライバにより実現される安全関連機能の性能を解析し，故障や障害を生じても，安全側に停止するフェールセーフ性を検証することが最も重要となる。そこで，本研究では，ドイツ第三者認証機関において現在行われている汎用サーボドライバの認証作業の実態，ならびに，安全関連機能が実装されたサーボシステムの技術動向を調査し，その結果に基づいて，サーボプレスへの適用を前提としたサーボドライバの安全性能評価手法を提案する。さらに，実際のサーボプレスの構造を模擬した実験モデルを試作し，サーボプレスの安全ドライブシステムの構築例を示すとともに，提案する評価手法と動作検証実験の結果から，実現された安全関連機能の安全性能を検証する。

A.2　サーボプレスの開発と認証の動向

ドイツにおいて機械プレス・液圧プレスの型式検定を行っているドイツ職業保険組合のプレス部門（MMBG），ならびに，金属加工部門（BGMS）をヒアリング調査した結果，現在，日本と同様，ドイツの多くのプレス機械メーカーがサーボプレスの開発に着手している状況にあり，このため，サーボプレスの安全性能評価試験方法について検討中であるとの報告を受けた。

従来の機械プレスの構造とサーボプレスの構造を，いわゆるプレス災害防止の観点から比較すると，以下の相違点が指摘できる。

1. クラッチ機構が使用されていない：クラッチ機構は，スライドの起動が阻止されるべき状況で確実な動力エネルギ伝達の遮断を実行するばかりでなく，その故障モードが，伝達可能な動力の量の減少，もしくは，動力伝達そのものが不可能になる安全側故障であるという特徴をもつ。
2. プレス用安全弁が使用されていない：上記に関連し，通常，クラッチ機構の操作を行うために使用されるプレス用安全弁（モニタ付き複式電磁弁）が使用されていない。プレス用安全弁では，スプールの不具合により両バルブの開閉動作に不一致が起こると，クラッチへの空気圧の印加が自動的に遮断される安全機能が構造的に実現されている。
3. フライホイールが利用されていない：フライホイールの慣性モーメントは，スライド又はクランクシャフトの動作方向が，瞬時には反転しないことを物理的に保障するものである。
4. ブレーキ機構の制動能力が高頻度にチェックされていない：機械プレスでは，オーバランモニタリングにより，ブレーキ機構の性能劣化が毎回のサイクル終了時に監視される。これに対し，サーボプレスでは，サイクル終了時のスライドの停止はサーボ制御により実現され，ブレーキ機構が真に使用されるのは非常停止操作等の異常時のみである。
5. カムスイッチが利用できない：カムスイッチはTDC（上死点），BDC（下死点）及びスライドの上昇／下降動作を機械的に記憶／判別するコンポーネントである。しかし，サーボプレスでは，TDC，BDCはプログラムにより容易に書き換えでき，また，スライド動作の検出はエンコーダの信号情報に依存している。

従来の機械プレスでは，上記の危険性が，電気・機械的手段を用いて合理的に解決されてきた。しかし，サーボプレスでは，サーボドライブ及びこれを含むプレス制御システム全体に実装された安全関連機能で，これらに対処しなければならない。そのための安全関連機能の実現には，マイクロプロセッサ等の電子制御装置が利用される。機械プレスの制御にプログラマブルな電子制御装置（Safety PLC）が利用されるようになって久しく，また，MMBG及びBGMSの報告によれば，ここ15年間で電子制御装置の故障や暴走が原因でプレス災害が生じたことは1件もないとのことではあるが，上述したリスク低減方策の実現原理の違い，すなわち，電子制御システムへの依存度の違いを考慮すれば，現行の機械プレスのEU内適合規格であるEN 692で述べられている確定論的安全性能評価をサーボプレスに適用することには明らかに限界がある。この問題はEU各国間及び米国ANSIでも認識されており，

現実に，先ごろ開始された EN 692 の改訂会議において，サーボプレスを今後どう扱うかが本会議期間中の主要議題の１つに挙げられているとの報告を受けた。

A.3　サーボドライバの開発と認証の動向

ドイツにおいて，サーボドライブの製品認証を行っているドイツ職業保険組合中央研究所（BGIA）をヒアリング調査した結果，既に 20 年程前から，BGIA にて認証された汎用サーボドライバが市場に登場しており，現在では，汎用サーボドライブを生産しているドイツ国内（一部，近隣 EU 諸国を含む）のほとんどのメーカーが，安全関連機能を実装した製品をラインナップしている状況にあるとの報告を受けた。現在の認証状況を表 1 に示す。これより，現在入手可能な安全関連機能を実装した汎用サーボドライバの傾向として以下の２点が指摘できる。

1. ほとんどの製品の安全制御カテゴリ（以下，Cat.と記す）は Cat.3 であり，最高ランクの Cat.4 を達成している製品は，現時点では１社に留まっている。
2. 実装されている安全関連機能は，ほとんどの製品で，非常停止操作等に対してモータの確実な停止を実行する安全停止のみであり，安全サーボドライバの特徴ともいえる機能的な安全制御機能（回転角度や回転速度が規定の範囲にあることの監視機能など）を実現している製品は極僅かである。

これらの傾向のうち，傾向 1 の理由として，従来まで安全関連機能を実装した汎用サーボドライバの用途が，主に，マシニングセンタや小型 NC 旋盤等の工作機械，据付型研削盤，産業用ロボットであったことが挙げられる。すなわち，これらの機械は，通常，インターロックガードが設置されることが前提で，このため，表 2 に示すように，駆動モータ制御系の安全関連部に要求される安全制御カテゴリは最高でも Cat.3 までであり，Cat.4 を求める需要が少なかったためと考えられる。このことは，別途訪問したサーボドライブメーカ数社からも示唆された。

次いで，傾向 2 は，従来の用途では，他の外部制御機器との関連も含めて，モータ各軸のモーションは制御コントローラにより集中制御されるのが一般的で，さらに，安全関連情報は中央の安全 PLC によって制御されるため，個々のモータ軸を駆動するサーボドライバ自体に複雑な安全関連機能を実装する必要がなかったためと推察される。

しかし，サーボプレスでは，従来の機械プレスと同等の安全性能として，そのサーボドライバにも Cat.4（もしくは，それと同等の安全性能。要求される安全性能については次節で詳述する）が要求され，さらに，安全停止だけでなく，より複雑な安全制御を実現する必要がある。この意味で，現在市販されているサーボドライバ単体では，サーボプレスの安全制御システムを構築することは大変困難であると考えられる。

市販のコンポーネントを用いてサーボプレスの制御システムを構成する例として，Cat. B の標準のサーボドライブ（コントローラとインバータ）を安全リレーユニットで制御するシステムの構成例を Fig. 1 に示す。図中，Cat. 4 の枠は，両手操作ボタン，光線式安全装置，安全リレーユニットが Cat.4 の安全要求事項を満足していることを示し，Cat. B の枠は枠内のコンポーネントが特に安全要求事項を考慮していない標準のコンポーネントであることを示している。現在，一部の光線式安全装置（ESPE／AOPD）には，例えばミューティング機能等の機能的な安全関連機能が実装されている。しかし，Fig. 1 のシステムでは，基本的には「工具区域内に手が挿入される恐れのあるとき（光線式安全装置等で手の挿入が検知されたときや，両手操作ボタンから手が離れたとき）にモータの電源を遮断する」という機能以外は実現できない。なぜなら，スライドの動作が制御システムの安全関連部にフィードバックされていないからであり，例えば，一行程一停止（シングルストローク）機能やブレーキの制動性能確認に重要なオーバラン監視は実現できない。最も重要な問題は，「モータの電源遮断」は単に「モータが回転トルクを発生しない」ことを意味するのであって，必ずしも「スライドの停止」が約束されていないことである。

他方，Safety PLC と Cat.3 の安全停止機能を有するインバータを用いて制御システムを構成する例を Fig. 2 に示す。Cat.3 の安全停止機能だけでは必ずしも十分でないため，この例では，メインコンタクタの遮断パスを追加方策として設け，モータ動力遮断手段の異種多重化を図っている。ただし，現在の Safety PLC は比較的高機能であるが，ユーザがプログラムしたスライドの動作シーケンス（特に，上死点や下死点の位置情報）を安全関連パラメータとして Safety PLC で処理するためには，後で詳し

く述べるようにシステム構成上の特別の工夫が必要となり，その実現は困難である。

以上のように，市販のコンポーネントを用いて実現できる安全関連機能には限界があり，前節で述べたサーボプレスの危険性をカバーすることは，現状では大変困難である。

A.4　サーボプレスへの適用を前提としたサーボドライバの安全性能評価指標

現在，制御系の安全関連部分の安全性能の指標には，電気・空圧・油圧システムなど比較的構造が単純な安全関連部を対象とした規格 ISO13849-1 で述べられている安全制御カテゴリ（Cat.）と，プログラマブルな電子制御システムを対象とした IEC 61508（この従属規格の一つに，機械分野に特化した規格として IEC 62061 もある）で述べられている安全完全性レベル（SIL）の 2 つがある。しかし，多くの機械制御システムは，実際には，上述した 2 種類の実現原理に基づく制御システムが機械構造部品によって組み合わされて実現されるのであって，Cat.と SIL の 2 つの指標のうち，どちらを適用するべきか一概には判別できず，各機械の構成と個別規格に左右される。これら評価指標の混在は EU 内でも混乱を生じており，現実にも，前節で述べたように既存の認証されたサーボドライブシステムは，多くが Cat.による評価であるが，BGIA とのヒアリングによれば，現在検討中のサーボドライブの安全関連機能に関する規格（CD／IEC 61800-5-2）では SIL に基づく性能評価を前提に作成作業が進行しているとの報告を受けた。

Cat.と SIL は，互いに要求事項（評価項目）が異なるために，一概に両指標を対応させることはできない。ただし，実現された安全関連システムに内包された危険側故障を徹底的に掘り下げて検証することには変わりはなく，また，その要求事項には多くの共通点を見出せる。このため，サーボプレスのリスクに相当する適切な Cat.及び SIL を選択して，両者を両立させることは必ずしも不可能ではない。そこで，本研究では，両指標の両立という方針に基づき，サーボプレスへの適用を前提としたサーボドライバの安全性能評価指標を検討した。

ハンドインダイ方式で用いられる機械プレスでは，種々の安全関連機能（安全関連装置）が ISO13849-1 で最高ランクの安全性能とされる Cat.4 の要求事項を満足しなければならない。よって，サーボプレスにも（それがハンドインダイ方式で用いられるならば）同等の Cat.4 レベルの安全性能が要求されると考えられる。Cat.4 の要求事項を簡単にまとめると以下のようになる。

1. システムの構造は吟味された安全原則に則ること，
2. 障害許容度：1 以上，
3. 危険側故障の平均時間間隔（$MTTF_d$）：30 年以上，
4. 診断有効度（DC）：99%以上，
5. 二重故障，多重故障を考慮すること，
6. 共通原因故障（CCF）及び系統的故障を考慮すること，
7. 使用する技術やシステム設計上の理論的根拠，FTA／FMEA による故障解析結果など，主張するカテゴリの妥当性確認に必要な情報を文書化すること（ISO13849-2)。

一方，今日，多くの安全制御用 PLC が SIL 3 を達成している現状を考慮すれば（IEC 62061 において機械分野で合理的に達成可能な SIL は SIL 3 が最高とされている），State of the art の観点から，サーボプレスの安全関連制御システムにも SIL 3 の達成が要求されると考えられる。所要の SIL を達成するためには，開発・製造・運用・廃棄に至る製品のライフサイクルの全てのフェーズで，仕様書及び設計コンセプトの作成，目的の実現，検証テストの実施に関し，品質管理やそれらを実行する人員のコンピテンシーまで含んだ，非常に多岐にわたる要求事項を満足する必要があるが，ハードウェアアーキテクチャに関する制約を中心に SIL 3 の要求項目を非常に簡単にまとめると以下のようになる。

1. ミッションタイム内（設定寿命内）における平均危険側故障発生率（PFH_d）が10^{-7} 以下であること，
2. 非対称故障率（SFF）が 90%以上であること（ただし，障害許容度が 1 以上の場合）
3. CCF（β ファクター）を定量的に評価すること，
4. 人的要因，外部環境要因に起因する系統的故障を回避する方策を導入すること，

5. 独立した組織によって機能安全性アセスメントを実施すること，
6. ソフトウェア安全性ライフサイクル要求事項を達成すること，
7. 安全要求仕様，ハードウェア・ソフトウェア要求仕様，機能性検査テスト計画とその結果など，安全関連機能に関わるすべての情報を文書化すること。

SIL における PFH_d の要求は，システムを構成するコンポーネントの $MTTF_d$ のみならず，DC や自己診断テストのインターバルをパラメータとした関数値の評価となるため，単に $MTTF_d$ を評価する Cat.の要求とは単純には比較できない。しかし，コンポーネントの故障率が一般的な範囲にあり，かつ，他の要求項目を満足していることを前提とすれば，両者はほぼ同じ信頼性目標であると言える。

一方，SIL における SFF と Cat.における DC との間には次式の関係がある。

$$SFF = \frac{\sum \lambda_S + DC \sum \lambda_D}{\sum \lambda_S + \sum \lambda_D} \quad \cdots(1)$$

ここで，λ_S は安全関連部の安全側故障率，λ_D は危険側故障率である。DC ＞ 99%，障害許容度 1 という Cat. 4 の厳しい要求を満足すれば，仮に $\lambda_S = 0$ であっても，SFF ＞ 90% の要求は達成される。

以上のように，Cat. 4 と SIL 3 の要求事項は，少なくともハードウェアアーキテクチャの観点からは類似点が多く，より厳しい側の指標を達成することでそれらの両立が可能である。サーボプレスの危険性からすれば，安全方策の根幹に位置づけられるサーボドライブシステムには両要求事項の両立を課す必要があると考えられる。なお，現状では，ソフトウェア（このうち，特に，OS や機能モジュールなどのプロセッサに組込みこまれるソフトウェア）に関する安全要求事項を扱っている規格は IEC 61508-3 のみであるため，ソフトウェアに関しては SIL 3 の要求事項がそのまま適用できる。

A.5　サーボドライバの安全性能評価手法の提案

複雑な電子制御システム（一般には，1000 ゲート以上もしくは 24 ピン以上の IC が使用されているプログラマブルな装置・システムを指す）の安全性能評価では，単に実現された安全関連機能の性能（例えば，急停止性能など）を外面的に評価しても，必ずしも安全性は証明できず，設計開発段階で盛り込まれた種々の安全方策の妥当性，さらに，それらが設計計画どおりに実現されることを検証することが必要である。このようなシステムの安全性能評価手法は，一般に，以下の 4 つのフェーズに大別できる。

1. 設計コンセプトの検証：システムに実現される安全関連機能が，機械のリスクを許容可能なレベルにまで低減するのに必要十分であるか，その選択の妥当性を検証する。これには，当該機械に対して実施されたリスクアセスメントの検証も含まれる。なお，HSE の報告によれば，災害発生原因となった制御システムの障害の約 65%がシステムが実際に使用される以前に“組み込まれた”ものであり，その多くが設計コンセプトや仕様設定の誤り，ならびに，危険状態の想定の不十分さによるものであるとされている。
2. 実現手法の検証：要求される安全関連機能を実現する手段・方法の妥当性を検証する。それらにマイクロプロセッサが利用される場合には，ハードウェアのみならず，組込まれるソフトウェアの内容についても精査する必要がある。
3. 実現・構築手順の検証：要求される安全関連機能が実装・構築される際に混入する可能性のある系統的エラーを防止するために，実装・構築の方法論，ならびに，そこに盛り込まれた種々の方策について選択の妥当性及びその効果を検証する。
4. 検査テスト計画とテスト結果の検証：開発過程の様々な段階で実施される種々の検査テストに関し，その結果のみならず，テストの計画と方法の妥当性についても検証する必要がある。特に，一旦開発が終了した後のシステムの変更・改造に対し，安全関連機能の性能の低下を防止する上で，これらの検査計画が非常に重要となる。

サーボプレスに実装されるサーボドライバは，マイクロプロセッサの使用を前提にした複雑な電子制御システムであり，その検証手法は，上記の一般論に則したものとならざるを得ない。ただし，本研究の期間内では上記のすべてを検討することには明らかに限界があるため，ここでは，特に上記 1）及び

2) のフェーズに着目し，サーボドライバの安全性能評価手法を検討することとした。本章では，まず，サーボプレス及びサーボドライバのモデルを想定し，次いで，これに対して必要な検証を実施していく形で，本研究で提案する安全性能評価手法（以下，本手法）を具体的に説明する。

A.5.1　システムの想定モデル

現在国内で生産されているサーボプレス及び実装されているコントロールシステムを参照し，実際的なサーボプレスシステムのモデルとして，ここでは Fig. 3 に示すシステムを想定する。サーボプレスの駆動方式には種々あるが，このシステムでは，比較的容易に高精度が得られるとして普及しているボールスクリューを利用した駆動方式を対象とした。この場合，スライドの上下動はサーボモータの頻繁な正逆転動作の繰返しによって実現される。本システムに対し，以下の仮定を設ける。

1. 想定するサーボプレスはハンドインダイ方式で用いられる比較的小型のものとする。すなわち，工具区域内に作業者が立ち入るような大型のシステムは対象にしない。
2. 煩雑になるのを避けるために Fig.3 には示していないが，側面及び背面はサーボプレス自体の構造フレーム又は固定ガードにより覆われているとし，前面開口部からのみ接近可能であるとする。
3. 作業者は１名とするが，第三者が近傍にいる場合も考慮する。
4. 開口部の防護方策として，両手操作ボタンと光線式安全装置（以下，AOPD）が併用されるものとする。
5. サーボモータには，ロータと同軸に保持用電磁摩擦ブレーキが内蔵されているとする。さらに，このブレーキはノーマルクローズ型であるとし，モータがトルクを発生できない状態（例えば，電源遮断時）には自動的に作動するものとする。
6. サーボモータの動作及びスライドの位置は，モータのロータ軸上に設置されたエンコーダとボールスクリューに設置されたエンコーダを用いて検知されるとする。これらの検知信号は，サーボモータの動作制御だけでなく，後述する安全関連機能の実現にも使用されるとする。なお，Fig. 3 のサーボプレスでは，ロータリーエンコーダの他に，スライドの位置を直接的に検出するリニアエンコーダが設置されているが，その理由については後に詳述する。
7. 上死点及び下死点（以下，TDC 及び BDC）の位置は，各々，1 サイクル中の最高位置及び最低位置とする。また，上死点を参照位置（以下，RP）とし，各サイクル終了時には必ず RP に復帰するものとする。ただし，1 サイクル中にスライドが BDC に達する回数には制限を設けない。

A.5.2　リスク解析

本手法では，まず，対象とするサーボプレスに対し，ISO 14121 で示されている種々の危険源・危険状態を予測し，その結果として人体に及ぼす傷害の酷さ及びその発生頻度や回避の可能性を推定して，サーボプレスのリスクを解析する。検討すべき危険源・危険状態については，機械／液圧プレスの C 規格である EN 692／693 にも述べられているが，すべての危険源が網羅された ISO 14121 を参照するべきである。また，前記仮定の中では，すでにいくつかの防護方策について述べているが，本来のリスクアセスメントは，防護方策が一切無い状態から解析が開始されなければならない点に注意が必要である。

予備的検討として，想定したサーボプレスに対してリスクアセスメントを実施した。その詳細については割愛するが，明らかになったリスクのうち，1) サーボドライブの危険な誤動作を主な検討対象としていること，2) 想定される傷害の酷さと頻度が共に高いことの 2 つの理由から，本研究では，「工具区域に作業者の手が入れられているにも係わらず，スライドが下降した結果として発生する挟圧の危険源」を対象に検討を進めることとした。サーボプレスの運用目的より，この挟圧の危険源は，本質的安全設計方策や防護ガードの設置では解消されない。さらに，そのリスクの高さより，この低減に関わる安全関連機能には，Cat. 4 もしくは SIL 3 の安全性能が必要となる。

なお，リスク解析より得られた知見の 1 つとして，想定したサーボプレスのタイミングベルト伝動機構に問題があり，以下の 2 つの仮定を新たに導入する必要があったことを指摘しておく。

8. タイミングベルトの破断が起こると，サーボモータに内蔵された保持用ブレーキのみでは，スライドの降下を防止できない。破断に至る過程でタイミングベルトの劣化や損傷を監視するオートモニ

タリングの実装は，現実のサーボプレスへの適用を考慮すると，非現実的であると言え，この問題は本質的安全設計方策の採用によって解決されるのが妥当である。すなわち，タイミングベルトが破断した場合にもスライドを停止・保持できるように，ブレーキの制動力がポジティブにスライドへ伝達される（バネやゴムなどの弾性体を介さず機械的に伝達される）構造でなければならない。このため，Fig. 3 のサーボプレスでは，ボールスクリューの回転を直接停止できる位置にノーマルクローズ型摩擦ブレーキを設置することとする。なお，左右のボールスクリューにブレーキが 2 重化されて設置されているが，その理由については次節で詳述する。

9. 同様に，タイミングベルトが劣化や損傷のために破断すると，伝達機構の一次側の動作検知センサの信号（Fig.3 では，サーボモータ側のエンコーダによる角度検出信号）は，スライドの動作との関連がなくなり，安全関連情報としての意味をなさなくなる。このため，Fig.3 のサーボプレスでは，ボールスクリュー軸上のエンコーダのほかに，スライド位置の検出が可能なリニアエンコーダを設置することとする。なお，スライド位置検出のためのエンコーダを冗長化する理由については次節で詳述する。

A.5.3　安全関連機能の同定

リスク解析結果に基づき，サーボプレスのリスク低減に必要な安全関連機能が同定する。ただし，ISO 12100 で述べられているように，リスク低減は，まず，本質的安全設計方策によって，次いで，固定ガード等の防護ガードの設置によって達成されなければならない。制御システムで実現される安全関連機能にリスク低減を委ねるのは，これらの方策の適用が困難と判断された場合のみである。

前述したように，サーボプレスの運用目的より，「工具区域に作業者の手が入れられているにも係わらず，スライドが下降した結果として発生する挟圧の危険源」については，Cat. 4 もしくは SIL 3 の要求事項を満足した安全関連機能の適用が必要となる。ただし，これは単一の安全関連機能ではない。なぜなら，このような挟圧はサーボプレスの種々の運用モードで発生する可能性があるからであり，また，A.2 節で述べた従来の機械プレスとの構造上の差異を考慮すれば，当該リスク低減に直接関わる安全関連機能のみならず，それらに付随した複数の安全関連機能も要求されるためである。リスク解析に基づいて，同定された安全機能を表 3 にまとめて示す。ここで，入力要素とは当該機能で使用されるセンサ及び当該機能のトリガとなるコンポーネントを指し，出力要素とは当該機能で操作の対象となるコンポーネントを指す。このうち，特に重要な機能について以下に説明を加える。

Inverter switch off monitoring：モータの安全停止は，インバータ回路内に設けられた IGBT 回路のベース電流遮断用パス（以下，Safe pulse blocking と呼ぶ）によって実現される。その詳細な構成については後述するが，Inverter switch off monitoring は，冗長化された Safe pulse blocking の不一致を検知する機能である。さらに，Cat. 4 の要求事項では Safe pulse blocking の遮断機能は，周期的にテストされなければならない。Inverter switch off monitoring は，このためのテスト周期管理機能を含んでおり，一定時間以上 Safe pulse blocking が使用されない場合には自動的にテストを実施する。

Encoder arrangement monitoring：冗長化されたエンコーダの情報を比較し，不一致がある場合には，サーボプレスの運転を停止させる。インクリメンタルエンコーダの場合，通常，電源ライン以外に 4 つ（A，B 相及びそれらの反転信号）の信号ラインが，また，アブソリュートエンコーダの場合はそれ以上の数の信号ラインがコントローラに接続される。このため，エンコーダを 1 つ設置し，それらのラインから送信される信号を比較すれば，信号ラインの断線や内部短絡，内部演算回路の機能障害は検出可能である。しかし，単一のエンコーダではエンコーダ接続部の可動部からの脱落（ロータリーエンコーダにおいては回転軸の回転円盤からの脱落も問題となる）が検出できない。よって，エンコーダ自体の冗長化が必要である。なお，冗長化されたエンコーダの角度情報の比較は，両エンコーダが動作しているときのみ（すなわち，信号が変化しているときのみ），エンコーダの正常性確認手段として有効である。このため，非常に長時間，電源が投入された状態で停止し続けた場合（例えば，1 週間）には自動的にサーボプレスの運転を停止させるなどの方策も検討する必要がある（このような状況では落下防止ブロックの使用を義務付ける等）。

Braking performance check：従来の機械プレスと異なり，ノーマルクローズ型摩擦ブレーキの制動能力は頻繁に確認されない。このため，サーボプレスでは，各サイクル開始時に制動能力をテストする機能が必要である。これには，ブレーキを作動させた状態で，モータの最大トルクを印加し（最大トルクの印加は，Safe motor torque check 機能で確認する），停止状態が維持されていることを確認する手法が適用できる。ただし，この方法で確認できるのはブレーキの静摩擦力が確認されるのみで，真に必要な動摩擦力はテストされない。一般に，ブレーキ面間の動摩擦力は静摩擦力の約 75～50%程度になる。そこで，モータの最大トルクを停止できる制動トルクを有するブレーキを 2 つ装備し，これらの静摩擦力を上記の方法で交互にテストする手法を提案する。本手法によれば，非常時に十分な動的制動力が得られることが確認できる。この目的のために，Fig.3 ではノーマルクローズ型摩擦ブレーキを両ボールスクリューに装備することを想定した。なお，本手法ではブレーキの動作時間はチェックされないため，制動時間については，別途実測に基づいて最大時間（最悪値）を決定し，安全距離の設計に反映させなければならない。

なお，表 3 の安全関連機能は，あくまでも本研究で想定したサーボプレスに対し，特にサーボドライバに関連すると考えられる機能に着目してまとめたものであり，個々のサーボプレスのすべてのリスクをカバーするものではないことを明記しておく。

A.5.4　安全性能評価

次いで，要求される各安全関連機能に対し，これらが割り当てられた安全性能を満足していることを，A.4 節で述べた定性的・定量的要求事項に照らし合わせて評価する。プロセッサを含む電子制御システムで実現される安全関連機能の検証は，ハードウェアに関する評価，ソフトウェアに関する評価，系統的故障に関する評価の 3 つに大別される。

ここで，ソフトウェアと系統的故障に関する評価は，システムの設計・実現・運用の各段階でこれらの障害に起因して安全関連機能を喪失しないためにシステムに組込まれた種々の技法や方策の妥当性を検証するとともに，組込まれた方策が有効に機能していることを種々のテストにより確認する作業である。ソフトウェアの安全性評価では，一般に V モデルのフローに則り，各実現段階において導入・実施された技法や方策の有効度を各段階ごとに検証し，さらに，最終的にシステム実装された状態で意図した障害回避特性が実現されていることを確認する。各段階で採用すべき方策は，安全関連機能に要求される安全性能に応じて異なり，その妥当性については IEC 61508-3 の付属書 A,B,C を参照して判断する。他方，系統的故障とは，電磁ノイズや温度変化といった環境要因に起因する機能障害，ならびに，安全関連機能の設計実現段階での人的ミスに起因する機能障害のことであり，これらは，設計や実現手法，管理手順を変更しない限り除去することができないことに特徴がある。系統的故障に対する方策は大きく 3 つに分けられる。

1) 系統的故障の抑制：オンラインテストの定期的な実施，適切な診断機能の実装など，
2) 系統的故障の回避：吟味された安全原則の使用，実績のあるコンポーネントの使用など，
3) 系統的故障の混入防止：機能テスト，Black Box テスト，White Box テストなど。

系統的故障に関する評価は，これらの方策が適切にシステムに導入・実施されていることを確認するもので，その妥当性の判断には IEC61508-2 の付属書 B や IEC62061 第 8.3 節を参照して判断する。

以上の 2 つの評価が定性的な妥当性の判断と実現されたシステムを用いた機能テストに依存しているのに対し，ハードウェアに関する評価では，ハードウェア構成に着目した定性的評価（ハードウェア制約）のみならず，使用されているコンポーネントの信頼性データに基づいた定量的評価を組み合わせて実施する必要がある。以下では，Inverter switch off monitoring を例に，その評価手順を説明する。

A.5.4.1　Inverter switch off monitoring 機能の定性的・定量的評価

Inverter switch off monitoring に関連するシステムの構成は，冗長系を基本とし，Cat. 4 の要求事項にある障害許容度 1 を満足するものとする。その構成を Fig.4 に示す。また，メインコンタクタの遮断は IEC 60204 の非常停止機能の要求事項に対するもので，本機能では特に必要なく，インバータ回路の安全停止は，冗長化された Safe pulse blocking によるパルス発生の抑止と冗長化されたプロセッサのリセット操作によって実現されるとする。

サーボモータが回転を行うためには，回転磁界の生成が必要である。これには，1) インバータ回路に必要な電力が供給されること，2) 回転を制御するプロセッサが設定されたフォトカプラの ON／OFF パターンを適切に生成すること，3) フォトカプラ及び IGBT 素子が入力されたパターンに従って同期して ON／OFF 動作すること，の 3 つの条件が成立する必要がある。Fig. 4 の構成では，条件 2) と 3)を抑止することで回転磁界の生成を阻止する。モータ回転中にメインコンタクタの遮断操作を実行するとインバータを破損する恐れがあり，安全関連部としてコンタクタ遮断を利用することは合理的でない。メインコンタクタが閉じ，インバータ回路に電力が供給されている状態において，仮に IGBT 素子に短絡故障が生じたとしても，容易に理解できるように，単一の素子の短絡では回転磁界は発生しない。ただし，利用されているモータが永久磁石同期モータである場合，極めて稀に複数の素子に同時多重短絡故障が生じて特定の位相の磁界が発生すると，1 極分ロータが回転する可能性はある。例えば，8 極の同期モータがサーボプレスに使用されている場合は $2\pi/8 = 0.785$[rad] (=45[deg]) 回転することになる。このため，このような異常回転に起因したスライド動作でリスクが増大する場合には別途対策が講じられる必要がある（ただし，一般的には，このために生じる下降動作は微小である。例えば，想定したサーボプレスにおいて，タイミングベルトの減速比を 1 : 5，ボールスクリューのリードを 2 mm と各々仮定すると，0.785[rad]の回転で起こりえる下降動作は高々0.05mm である)。

Inverter switch off monitoring 機能は以下の手順で実行されるとする。

1. 毎サイクルにおいて，両手操作ボタンが開放されたことをトリガにして，2 つのプロセッサが各々対応する Safe pulse blocking の半導体スイッチをターンオフする。ただし，ここでは，ミューティングは実装されておらず，通常の使用方法として，毎サイクル終了時まで両手操作ボタンは保持され続けるとする。
2. 1 つの半導体スイッチの動作は両プロセッサにフィードバックされる。両プロセッサは規定時間以内にターンオフが行われたことを検査するとともに，互いにデータを交換し，不一致がないことを検査する。
3. 異常な遅れやデータに不一致があった場合には，以後のサイクルの実行を禁止する。
4. このテストは，毎サイクルごとの実施であるので，少なくとも 20 秒に 1 回は実施される。
5. 両手操作ボタンの制御と監視は認証された Cat.4 のリレーモジュールによって実行されるとし，プロセッサによっては処理されないとする。

Inverter switch off monitoring 機能を実行するためのハードウェアの機能ブロック図を Fig 5(a)に示す。ここで安全性能評価のための仮定として，2 つのプロセッサは同じ型式ではあるが異なる配線パターンで使用されており，このため異なったプログラムが組込まれることから，異種多重系と見做せるとする。両プロセッサは個々にセルフテストを実施し，その結果は他方のプロセッサによって検査される。さらに，両プロセッサは独立した定電圧源により電力供給を受けるとし，特に，定電圧源 B はプロセッサ B とその周辺機器に対してのみ使用されるとする。各々の定電圧源の出力電圧は，電圧監視用 IC とプロセッサにより二重に監視される。

この機能ブロックに対し，Cat.4 及び SIL3 の要求事項が満足されているか検証するため，Fig.5(b)に示すように 4 つのサブシステムに分割する。ただし，簡単化のため，この分割では，メインコンタクタの接点モニタリング及びプロセッサの電源監視機能を（共に安全性能向上には寄与するが）無視して考えている。以下では，各サブシステムごとに考察を進める。

A.5.4.2 サブシステム 1

安全関連機能を実行するシステム（ここでは，サブシステム 1）に対し，まず，FTA 及び FMEA を実施して，起こり得る故障と故障同士の関連（多重故障や共通原因故障），ならびに，それら故障が意図した安全関連機能に与える影響を検討する。次いで，その結果から，安全側故障率，検出可能な危険側故障率，検出されない危険側故障率を同定し，これより，SFF と DC の値を決定する。ここでは，検討結果の一部として，サブシステム 1 の特に冗長化プロセッサについて実施した FTA の抜粋を Fig. 6 に示す。Cat.4 と SIL3 の要求事項を満足する値として，ここでは，サブシステム 1 の DC と SFF を各々DC=99%，SFF=99.5%と仮定する。

ハードウェアの検証過程においては，FTA 及び FMEA による故障解析が最も重要な作業である。特に，Cat.4 の要求事項には，すべての故障・障害が安全関連機能の実行中かそれ以前に確実に検出されることが要求されており，それを満足していることは理論的な故障解析の結果からしか判定できない。

次いで，FTA／FMEA による検討結果を評価するため，故障検出のために組込まれた各診断機構や故障を回避するための手法から，IEC 61508-2 付属書 A に記載の表を参照して，DC を見積もる。例として，サブシステム A に導入される診断機構を仮定し，それらを付属書 A を参照して評価した結果を表 4 に示す。ここでの DC の評価と FTA／FMEA で得られた結果とを比較することで，FTA／FMEA の検討結果の妥当性が判断できる。また，SFF については，すべての故障を危険側と見做して，式(1)より DC 値=SFF 値と考えることも可能ではある。

他方，安全関連機能を実現するシステムに導入された共通原因故障を防ぐ方策に対し，IEC 61508-6 付属書 D を参照して，付属書 D の表 D.1 に記載された各項目を吟味し，項目分類ごとの合計スコアから表 D.4 を使ってβファクタを推定する。例として，サブシステム 1 のβファクタを評価した結果を表 5 に示す。ここで，X 値と Y 値は，各々，導入された方策の診断機能への寄与率と系統的故障防止への寄与率を表している。合計スコアより，サブシステム 1 のβファクタを$\beta=0.02$ と仮定する。

以上のパラメータを用いて，安全関連機能を実行するシステム（ここでは，サブシステム 1）の信頼性モデルを構築し，ミッション時間内（10 年とする）の平均危険側故障率 PFH_d を推定する。信頼性モデルについては IEC 61508, IEC 62061 にいくつか例示されているが，ここではマルコフ信頼性モデルを用いて，サブシステム 1 の PFH を推定する。このために，まず，サブシステム 1 を Fig. 6 に示すように A と B の 2 つのブロックに分割する。そして，ブロック A とブロック B の危険側故障率 λ_{AD} と λ_{BD} を各々導出する。この際の故障率データには，少なくとも信頼水準 70%以上の下限推定値が与えられるだけの総運転時間に基づいたデータを用いなければならない。例えば，危険側故障率 λ_D を 10^{-6} [h]とするには，テストケースが 100 以上，個々の運転時間が 1 年以上の条件で，総運転時間が少なくとも 1.2×10^{6} [h]以上の期間中に危険側故障が発生しなかったことを示すデータが必要である。ここでは，比較的否定的な値として，プロセッサ A 及び周辺素子の危険側故障平均時間（$MTTF_d$）を 50[y]，プロセッサ B 及び周辺素子の $MTTF_d$ を 70[y]，トランジスタの $MTTF_d$ を 900[y]，フォトカプラの $MTTF_d$ を 1200[y]とおき，$\lambda_{AD}=2505$ FIT，$\lambda_{BD}=1852$ FIT と仮定する。

次いで，危険側故障のみを対象としつつ，マルコフ信頼性モデルを構築する。例として，ここでは，ブロック A とブロック B の相似性を利用して，Fig.7 に示すモデルを構築した。図中，r_{Test} は診断テスト頻度，r_{Rep} は修復時間の逆数であり，ここでは各々$r_{Test}=180$[1/h]（20 秒に 1 回），$r_{Rep}=0.125$[1/h]（8 時間）とする。このモデルにおいて，例えば，状態 S2 はブロック A に危険側故障が生じた状態であり，これが診断テストにより検出されると S5 に，検出されなければ S6 に，診断テストの実行前にブロック B にも危険側故障が発生すると S8 に状態が推移することを表している。S8 が両ブロックに危険側故障が生じた危険状態である。なお，診断テストと修復に関連する状態推移は，一定時間区間内で指数分布に従わないため，厳密にはマルコフモデルに含めることはできないが，あくまで近似モデルとして，Fig. 7 ではこれらを含めて考えている。各状態間の推移確率をC とおき，S1 から S2 への推移確率を$C_{12}(=\lambda_{AD}-\beta\lambda_{BD})$，S1 から S3 への推移確率を$C_{13}(=\lambda_{BD}-\beta\lambda_{BD})$と表すと，S1～S8 の状態確率 $P_1(t)\sim P_8(t)$ は次式で与えられる。

$$\begin{pmatrix} \frac{dP_1(t)}{dt} \\ \frac{dP_2(t)}{dt} \\ \vdots \\ \frac{dP_8(t)}{dt} \end{pmatrix} = \begin{pmatrix} -\sum_{k=2}^{8} C_{1k} & C_{21} & \cdots & C_{81} \\ C_{12} & -\sum_{\substack{k=1 \\ k\neq 2}}^{8} C_{2k} & \cdots & C_{82} \\ \vdots & \vdots & \vdots & \vdots \\ C_{18} & C_{28} & \cdots & -\sum_{k=1}^{7} C_{8k} \end{pmatrix} \begin{pmatrix} P_1(t) \\ P_2(t) \\ \vdots \\ P_8(t) \end{pmatrix} \quad \cdots(2)$$

一般に，式(2)の微分方程式を解析的に解くのは困難である。そこで，各パラメータに前述した値を各々代入し，想定ミッション時間 10 年での各時刻 t での状態確率 $P_1(t)\sim P_8(t)$ の推移を数値演算によって求めるとすると，サブシステム 1 の $PFH_{d\,ss1}$ は S8 に至る確率として次式で導くことができる。

$$\mathrm{PFH_{d\,SS1}} = \frac{1}{T_M}\int_0^{T_M}\left[\beta\,\lambda_{BD}P_1(t) + \lambda_{BD}\left(P_2(t)+P_6(t)\right) + \lambda_{AD}\left(P_3(t)+P_7(t)\right)\right]dt \quad \cdots(3)$$

式(2)及び(3)を数値演算によって求めた結果，ここで仮定したλ_{AD}，λ_{BD}，DC，βの条件では，$\mathrm{PFH_{d\,SS1}}$ $=4.07\times10^{-8}$[1/h]となった。なお，DC 及びβの値と $\mathrm{PFH_{d\,SS1}}$ との関係については，6.5.4.6節で別途改めて考察する。

A.5.4.3　サブシステム2

同様の手順で，サブシステム 2a と 2b の検証を行う。改めて，サブシステム 2a と 2b の構成を Fig.8 に示す。構成の相似性より，まず，サブシステム 2a について考察する。ここで電圧監視は専用 IC（以下，VM）で連続的に行われるとし，その診断有効度は $\mathrm{DC_{PS}}$=99%とする（IEC61508-2 表 A.9)。また，実際にはプロセッサ A による電圧監視を行っているので Cat.4 の障害許容度 1 の要求事項は満足されるが，$\mathrm{PFH_d}$ の推定では信頼性モデルの構築を容易にする目的でこれを無視し，VM 自体の診断は一切行われないものとして考える。VM 以外の素子を 1 つのブロック（以下，PS）と見做して構築したサブシステム 2a のマルコフ信頼性モデルを Fig. 9 に示す。式(2),(3)と同様の手順で，想定ミッション時間（10 年）内の各時刻 t での状態確率$P_1(t)$ ～$P_4(t)$ の推移を数値演算によって求め，さらに，危険側平均故障率 $\mathrm{PFH_{d\,2a}}$ を S4 に至る確率として次式で求める。

$$\mathrm{PFH_{d\,2a}} = \frac{1}{T_M}\int_0^{T_M}\left\{(1-\mathrm{DC_{PS}}+\mathrm{DC_{PS}}\cdot\beta)\lambda_{PSD}P_1(t) + \lambda_{VMD}P_2(t) + \lambda_{PSD}P_3(t)\right\}dt \quad \cdots(4)$$

λ_{VMD} =500 FIT，λ_{PSD} =500 FIT，β=2%，r_{Rep}=0.125[1/h]とおいた結果，$\mathrm{PFH_{d\,2a}}=2.51\times10^{-8}$ [1/h]となった。サブシステム 2b についても全く同じ数値を仮定する。目的とする安全関連機能の実行においては，2a か 2b のどちらか一方が正常であれば，システムは安全側に移行できる。ただし，2a と 2b は互いに監視しあってはおらず，さらに，その構造は同一の実現原理に基づくものである。これらを考慮し，ここでは，サブシステム 2 全体がβファクタを 5%とする 2a と 2b の並列システムで表されるとする。この場合，サブシステム 2 全体の $\mathrm{PFH_{d\,SS2}}$ は次式で求められる。

$$\begin{aligned}\mathrm{PFH_{d\,SS2}} &= (1-\beta)^2\times T_M\times\mathrm{PFH_{d\,2a}}\times\mathrm{PFH_{d\,2b}} + \beta\times0.5\left(\mathrm{PFH_{d\,2a}}+\mathrm{PFH_{d\,2b}}\right)\\ &= 1.3\times10^{-9}\,[1/h]\end{aligned} \quad \cdots(5)$$

A.5.4.4　サブシステム3

両手操作ボタンの同時 ON／OFF の確認は Cat.4 の要求事項を満足したリレーモジュールにより実現されるとした。実際には Cat.4 の評価から直ちに $\mathrm{PFH_d}$ を得ることはできず，上記と同様の手順で各パラメータを吟味する必要があるが，サブシステム 3 のように，あまり複雑でないコンポーネントに限り，EN／IEC 62061 の 6.7.9 節で述べられている系統的故障の回避に関する要求事項を満足していれば，同規格の表 7 に記載された値を $\mathrm{PFH_d}$ の推定値として利用できる。ここでは，リレーモジュールが障害許容度 1 で Cat.4 の要件を満足しているとし，表 7 より，$\mathrm{PFH_{d\,SS3}}=3\times10^{-8}$ [1/h]とする。

A.5.4.5　システム全体の評価

得られた 3 つのサブシステムの $\mathrm{PFH_d}$ から，次式により，Inverter switch off monitoring 機能に関連する安全関連部全体の $\mathrm{PFH_d}$ を求める。

$$\begin{aligned}\mathrm{PFH_d} &= \mathrm{PFH_{d\,SS1}} + \mathrm{PFH_{d\,SS2}} + \mathrm{PFH_{d\,SS3}}\\ &= 4.07\times10^{-8}+0.13\times10^{-8}+3.00\times10^{-8}=7.2\times10^{-8}\,[1/h]\end{aligned} \quad \cdots(6)$$

SIL3 の条件の 1 つである $\mathrm{PFH_d} < 10^{-7}$ [1/h]を満足している。

以上の評価結果を表 6 にまとめて示す。なお，機能全体の DC（$\mathrm{DC_{avg}}$）は次式より求めた。

$$DC_{avg} = \frac{\frac{DC_{SS1}}{MTTF_{d\,SS1}} + \frac{DC_{SS2}}{MTTF_{d\,SS2}} + \frac{DC_{SS3}}{MTTF_{d\,SS3}}}{\frac{1}{MTTF_{d\,SS1}} + \frac{1}{MTTF_{d\,SS2}} + \frac{1}{MTTF_{d\,SS3}}} \quad \cdots(7)$$

表6より，Inverter switch off monitoring機能はCat.4とSIL3の安全性能を達成していると判断できる。

以上が，安全関連機能のハードウェアに関する評価手順である。ただし，PFH_dと$MTTF_d$に関する定量的検討は，安全関連機能の安全性能を検証する上での単なる一側面に過ぎないことに注意が必要である。すなわち，FMEA／FTAによるDC及びSFFの導出，ソフトウェアの安全性検証と機能テスト，ならびに系統的故障防止方策に対する検討といった比較的定性的といえる評価段階のほうが（これらで誤った評価を与えれば，対象とする安全関連機能に致命的な欠陥を認める結果となるため）より重要である。

A.5.4.6　冗長化プロセッサの信頼性パラメータとPFH_dとの関係

Fig. 7のマルコフ信頼性モデルにおいて，仮定した信頼性パラメータを変化させたときのPFH_dの違いから，クロスモニタリングが導入された冗長化プロセッサというハードウェアアーキテクチャにおける各信頼性パラメータの影響を考察する。

A.5.4.2節で仮定したパラメータのうち，DC値，βファクタ及び診断テスト頻度r_{Test}を変化させて式(2)，(3)から導出したPFH_dの結果を表7に示す。まず，表7より，他のパラメータが同じであれば，診断テストの頻度が1時間に1回から1日に1回に低下してもPFH_dにはほとんど変化が見られないことが分かる。これは，クロスモニタリングが導入された冗長化プロセッサでは，次の診断テストが実行されるまで，どちらか一方が健全であれば，安全機能を喪失しないためである。診断テスト間隔が長ければ長いほど，故障を生じた場合，システムが単一系に縮退している時間が長くなる（これは確定論的安全の立場からは決して好ましいことではない）。しかし，6.5.4.2節では一般的な値と比較してより高い故障率を仮定したが，そのようなプロセッサの故障率でも，診断テスト間隔が1時間から1日に延長された程度ではPFH_dにはほとんど影響しない。

一方，DC値が小さく，また，βファクタが大きくなるにつれ，PFH_dは著しく増大するが，この傾向において，DC値が大きいほどβファクタの増大の影響がより顕著に表れており，特にDC=99%の条件ではβファクタにほぼ比例してPFH_dが増大しているのが分かる。これは，DC値が大きくなるにつれ，一方のブロックに故障が生じてもほとんどが検知されて状態S1に復帰するので，他のパスに比べて共通原因故障のパス（式(3)では被積分項の第1項）がより支配的になるためである。上記の結果は，Cat.4で要求される非常に高いDC値を満足するシステムでは，共通原因故障防止のための方策や技法の採用がPFH_dの改善に非常に重要になることを示唆している。共通原因故障を防止するために有効とされている主な方策を表8に示す。このうち，特に，EMC試験の実施と異種冗長化構造の採用は最も効果が高いとされ，ここで議論しているようなCat. 4／SIL 3システムには不可欠である。

A.6　サーボプレス用安全ドライブシステムの実験モデルの構築と動作検証実験

本研究で得た情報に基づき，ドイツにて入手可能なCat.3の安全停止機能が実装されたインバータユニット（BoschRexroth社製）と，本研究の研究指導者であるNeudörfer博士が現在扱っているサーボシステムの動作監視ユニット（BBH社製SP100）を使用して，サーボプレスに適用可能な安全サーボドライブシステムの実験モデルを構築した。実験モデルの概観をFig. 9に示す。前節で想定したものと同じく，ボールスクリューを用いたサーボプレスの構造を模したもので，ボールスクリューへのトルク伝達はタイミングベルト機構を介して行われる。スライドに見立てたナット部の移動量はポテンショメータにより観測される。他方，動作監視ユニットは，Cat.4の要求事項を満足するように設計開発されたもので，2つのエンコーダ入力ポートを有し，ここより入力された情報を異種冗長化されたプロセッサで処理することで，サーボシステムが予め設定した速度限界や位置限界を超える動作，あるいは規定の動作方向に反する動作を行った場合には，許可出力を停止する機能をもつ。ここでは，この許可出力をインバータユニットの安全停止機能に入力する。ただし，Cat.3の安全停止機能だけでは

Cat.4 の要求事項を満せないため，この許可出力を利用して，1) インバータユニットのイネーブル信号遮断パス，2) メインコンタクタの遮断パス（Fig.2 参照）を追加方策として設けた。また，入力ポートには，リニア／ロータリ，インクリメント／アブソリュートといった形式の異なるエンコーダが接続可能であり，冗長化されたエンコーダの信号を比較することにより，位置／角度情報の正常性が確認される。ただし，本実験モデルでは，後の動作検証実験での比較を容易にする目的で，ボールスクリュー軸上に設置されたインクリメント型のロータリーエンコーダの出力信号を両ポートに分配して入力している。

本研究の期間内に構築した実験モデルのすべての安全関連機能を吟味することは困難である。したがって，これらのうち，ここでは，エンコーダ信号の不一致検知機能（前述の Encoder arrangement monitoring 機能）を対象に，提案した評価手法及び動作検証実験（機能テスト）を実施し，その結果から安全性能を評価した。

実験モデルでは 1 つのエンコーダの信号を分配しているが，ここでは実際のサーボプレスへの適用を考慮し，2 つのエンコーダが接続されているものと見做して解析する。Encoder arrangement monitoring 機能は以下の手順で実行される。

1. エンコーダの出力信号は，プロセッサ A, B に入力される。各プロセッサは，エンコーダが出力する角度情報を比較し，不一致があれば，インバータユニットへの許可信号を遮断して，モータを停止させる。この不一致検出は 25 [ms]毎に実行される。
2. 角度情報の比較過程で，プロセッサ A, B は中間処理結果と計算結果を交換し，互いに処理の正常性を監視しあう。この方法によれば，プロセッサ A, B のいずれか一方が正常である限り，エンコーダの故障は 100%検出可能である。
3. エンコーダはインクリメンタル型とし，A 相 B 相信号及びこれらを論理的に反転した A^{-1} 相 B^{-1} 相信号の 4 つの信号が出力されるとする。
4. 許可信号遮断パスの正常性確認は Inverter switch off monitoring 機能で対処されるものとし，構成素子の故障はプロセッサの故障（遮断機能障害）として考える。
5. 動作監視ユニットは 1 時間に 1 回の頻度でセルフテストを実行する。このセルフテストは，他方のプロセッサにより制御・監視される。
6. 2 つのプロセッサともに故障した状態，及び，2 つのエンコーダがともに故障した状態を，検知できない危険側故障状態と定義する。厳密には，プロセッサやエンコーダの故障モードは必ずしも同じではないので，故障が検出され，システムが安全状態に移行する可能性もあるが，ここでは解析の単純化を目的にこの定義を採用する。
7. ミッション時間 T_M は 10 年とする。

まず，提案した評価手法を適用するため，動作監視ユニットの内部構成に基づき Encoder arrangement monitoring 機能に関連するハードウェアの機能ブロック図を作成した（Fig.10）。さらに，これを，Fig.10 に示すように，1) エンコーダ A（EA），2) プロセッサ A と許可信号遮断パス A で構成される A 系プロセッサ（PA），3) PA の定電圧源（PSA），4) エンコーダ B（EB），5) プロセッサ B 及び許可信号遮断パスパス B で構成される B 系プロセッサ（PB），6) PB の定電圧源（PSB）の 6 つのブロックに分割する（インバータユニットは安全関連機能には関係しない）。前記仮定 4 より，PA と PB の信頼性モデルは，個々のコンポーネントが直列に接続された直列モデルで表される。定電圧源 PSA, PSB で構成されるサブシステム SP の PFH_d は，前節の Inverter switch off monitoring 機能に対する評価で仮定した値がそのまま利用できるとし，$PFH_{d\,SP} = 1.3 \times 10^{-9}$ [1/h]とした。

EA, EB, PA, PB の 4 つのブロックの危険側故障率，DC 値，β ファクタを以下に示す。ただし，動作監視ユニットのすべての製品情報が公開されてはいないので，以下の値には，動作監視ユニットが Cat.4 の要求事項を満足していることに基づいた推測値を含んでいる。

EA, EB：$\lambda_{EA} = 1142$ FIT, $\lambda_{EB} = 1142$ FIT, $DC_E = 100$ %, $\beta_E = 5$ %,

PA, PB：$\lambda_{PA} = 2505$ FIT, $\lambda_{PB} = 1852$ FIT, $DC = 99$ %, $\beta_P = 2$ %

エンコーダ情報の比較頻度：r_C＝14400 [1/h],

セルフテスト頻度：r_T＝1[1/h],

修復時間間隔：r_{Rep}＝0.125 [1/h]

以上の仮定の下で構築したマルコフ信頼性モデルを Fig. 11 に，図中の状態 S1～S18 の定義を表 9 に各々示す。

計算過程の詳細は割愛するが，前節と同様の手順で，ミッション時間 10 年での各時刻 t での状態確率 $P_1(t)$ から $P_{18}(t)$ までの推移を数値演算によって求め，これらを用いて検知できない危険側故障状態に至る平均確率 $PFH_{d\,EnPr}$ を次式から導出した。

$$PFH_{d\,EnPr} = \frac{1}{T_M}\int_0^{T_M}[(\beta_E\lambda_{EB}+\beta_P\lambda_{PB})P_1(t)+(\lambda_{EB}+\beta_P\lambda_{PB})P_4(t)+(\lambda_{EA}+\beta_P\lambda_{PB})P_5(t)$$
$$+(\lambda_{PA}+\lambda_{PB})(P_6(t)+P_7(t)+P_8(t)+P_9(t))+(\lambda_{PB}+\beta_E\lambda_{EB})P_{12}(t)$$
$$+(\lambda_{PA}+\beta_E\lambda_{EB})P_{11}(t)+(\lambda_{PB}+\lambda_{EA}+\lambda_{EB})P_{14}(t)+(\lambda_{PA}+\lambda_{EA}+\lambda_{EB})P_{15}(t)$$
$$+\lambda_{PB}P_{16}(t)+\lambda_{PA}P_{17}(t)]dt \quad \cdots$$

式(8)より，$PFH_{d\,EnPr}$＝9.77×10^{-8}[1/h]となった。これに前述の $PFH_{d\,SP}$ を加えると，Encoder arrangement monitoring 機能全体の PFH_d は PFH_d = 9.9×10^{-8} [1/h]となり，SIL3 の要求事項が満足されていることを確認できた。なお，上記の値より別途導出した結果，$MTTF_d$ = 30.4[y]であった。

上記の $PFH_{d\,EnPr}$ の導出において，エンコーダ EA, EB の危険側故障寿命（$MTTF_d$）とβファクタを変えた場合の $PFH_{d\,EnPr}$ の変化を表 10 に示す。βファクタが小さくなるにつれ，$PFH_{d\,EnPr}$ におけるエンコーダの $MTTF_d$ の影響が小さくなるのが分かる。特に，βファクタが 0%の場合には，$PFH_{d\,EnPr}$ に顕著な差が表れるのは，EA, EB の $MTTF_d$ が 1 週間と極端に短くなってからである（通常，このような $MTTF_d$ の値は有り得ない）。この結果は，高い DC が実現されている上に，さらに異種冗長化などの技法によって 2 つのエンコーダの共通原因故障が完全に排除されたシステム構成の下では，システムの PFH_d はプロセッサの危険側故障のみによって支配され，エンコーダ自体の故障は無視できることを示唆している。ただし，$MTTF_d$ の導出においては診断テストの有効度や共通原因故障の発生率は考慮されないため，エンコーダの $MTTF_d$ が短くなれば，要求値を満足できなくなることに注意が必要である。

一方，Encoder arrangement monitoring 機能の機能テストとして，2 つのエンコーダ入力のうちの一方が断線した状態を擬似的に生成し，エンコーダ信号の不一致を検知し，許可信号を遮断するまでの動作監視ユニットの応答を測定する障害挿入テストを行った。測定結果の例として，2 つのエンコーダ入力の A 相信号と B 相信号及び動作監視ユニットの許可信号出力を Fig.12 に示す。この測定では，エンコーダ信号に不一致が生じてから（図中 a 点から）許可信号を遮断するまで（図中 b 点まで）約 27ms を要している。動作監視ユニットでは不一致検知のための比較が 25ms 周期のサイクルで実行されている。1 回のサイクルで不一致を見過ごすと，許可信号遮断が遮断されるのは次のサイクルであるから，最悪ケースとして応答遅れには 2 サイクル分見積もる必要がある。同様の実験を 10 回行った結果，応答時間は 22ms から 38ms の間でバラつき，平均値 29.47ms，不偏標準偏差 4.77ms であった。これより，最悪値を平均値＋3×不偏標準偏差として計算すると約 44ms であり，前述した 2 周期分（50ms）を超えないことが確認できた。

表１　これまでに認証されたサーボドライブシステム及び汎用インバータ

製造社名	型　式	実装された安全関連機能	安全性能	認証機関
ALSTOM	ALSPA MV 1000-s	Safe torque off	Cat.3	BGIA
	ALSPA MD 2000	Safe torque off	Cat.3	BGIA
Baumueller	BUM 6	Safe torque off	Cat.3	BGIA
	BUS 6	Safe torque off	Cat.3	BGIA
	BKH 6	Safe torque off	Cat.3	BGIA
	Bma BN44	Safe torque off	Cat.4	BGIA
Berger Lahr	SAW for Twin Line	Safe torque off, Safe operating stop, Safety-limited speed	Cat.3	BGIA
Bosch Rexroth	IST System 200	Safe torque off, Safe standstill, Safe operating stop, Safety interlock, Safe stop monitor, Safety-limited speed, Safe speed reduction, Safe deceleration monitor, Safety-limited increment, Safe direction, Safety-limited position, Safe-related homing, Safe diagnostic outputs, Safe brake control	Cat.3	BGIA
Control Tech.	PDS Unidrive SP	Safe torque off	Cat.3	BGIA
Danaher	ServoSter SR 300	Safe torque off	Cat.3	BGIA
Danfoss	VLT P400	Safe torque off, Safe standstill, Safe speed reduction	Cat.3	BGIA
Eurotherm SSD	Servomrichter 637f	Safe torque off	Cat.3	FA MFS
ELAU	PacDrive MC-4	Safe torque off, Safe standstill	Cat.3	FA MG
Dr.J.Heidenhain	TNC 410M	Safe torque off, Safe standstill, Safe operating stop, Safety interlock, Safety-limited speed, Safety-limited position	Cat.3	BGIA
	TNC 426M	Safe torque off, Safe standstill, Safe operating stop, Safety interlock, Safety-limited speed, Safety-limited position	Cat.3	BGIA
Lenze	Antriebsregelbaureihe 9300 & Ferquenzum-richter 8220	Safe torque off	Cat.3	FA MFS
Parker Hannifin	Compax3	Safe torque off	Cat.3	BGIA
SEW-Euro drive	MM C-503-00	Safe torque off, Safe standstill	Cat.3	MHHM
	MDX 6 B00	Safe torque off, Safe standstill	Cat.3	MHHM
Siemens	SIMODRIVE 611U	Safe torque off	Cat.3	FA MFS
	SIMOVERT Ver.1.1	Safe torque off	Cat.3	FA MFS
	SINUMERIK 840K & SIMODRIVE 611D	Safe torque off, Safe standstill, Safe operating stop, Safety interlock, Safe stop monitor, Safety-limited speed, Safe speed reduction, Safe deceleration monitor, Safety-limited increment, Safe direction, Safety-limited position, Safe-related homing, Safe diagnostic outputs, Safe brake control	Cat.3, SIL2	BGIA

表 2　EN／ISO 規格における各種機械の要求安全性能

	EN 12417(2001) Machining centers	EN 12415(2001) Small NC turning machines and turning centers	EN 13218(2002) Stationary grinding machines	ISO 11161(1994) Industrial automation systems	ISO 10218-1(2005) Robots for industrial environments
Enabling device	Cat.3	—	Cat.3 or Cat.1 only if Hardware	Cat.3	Cat.3
Deceler-Ation	Cat.3 or Cat.B & Enabling device	Spindle : Cat.3, Shaft : Cat.2	Cat.3 or Cat.B & Enabling device	Cat.3 or Cat.B & Enabling device	Cat.3
Interlock Guard	Cat.3, Guard: Cat.1	Cat.3	Cat.3, Guard: Cat.1	Cat.3, Guard: Cat.1	Cat.3
Position limiting	—	—	—	Cat.3	Cat.3
E-stop function	Cat.3	Cat.3 or Cat.1 only if Hardware	Cat.1	According to IEC60204	Cat.3

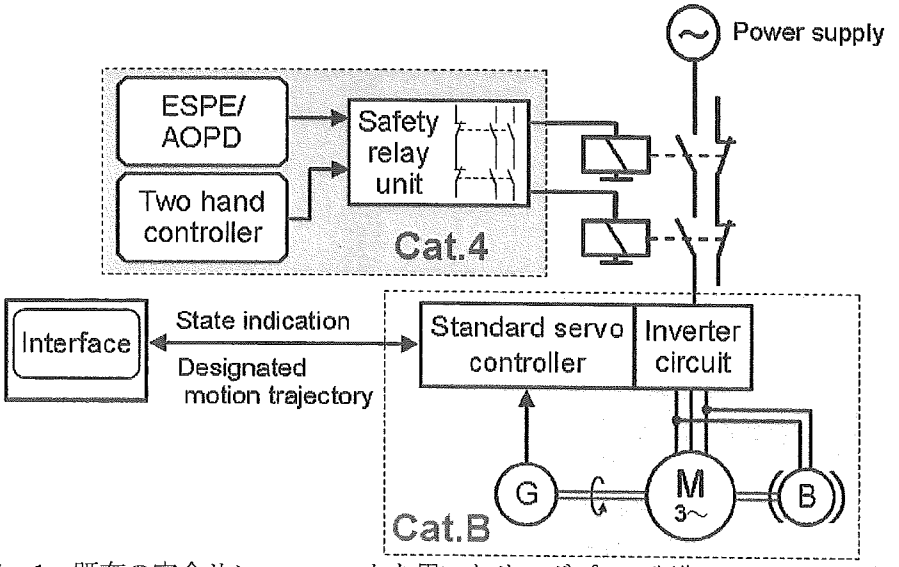

Fig. 1　既存の安全リレーユニットを用いたサーボプレス制御システムの構成例

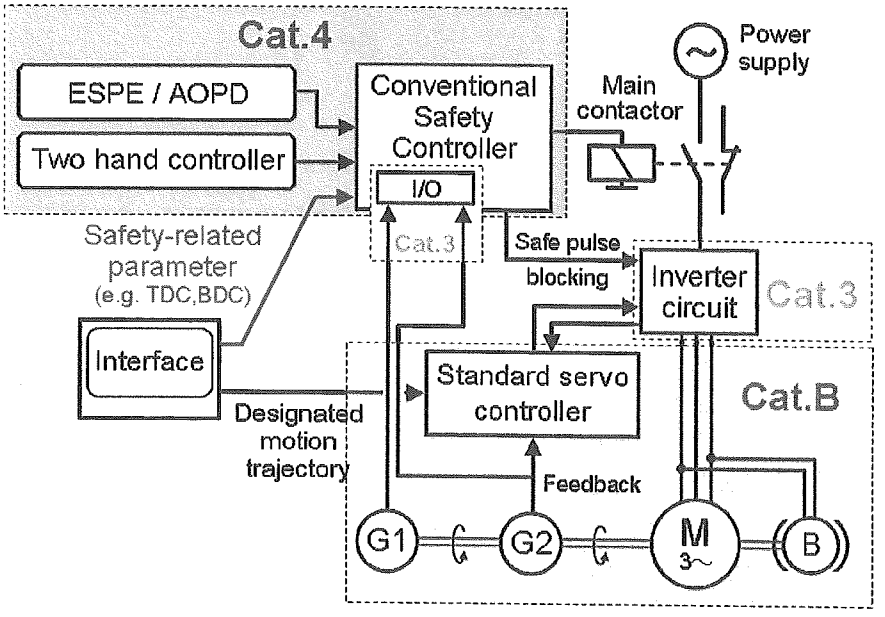

Fig. 2　Cat.3 のインバータと Cat.4 の Safety PLC を用いたサーボプレス制御システムの構成例

表3　サーボプレスコントローラに要求される安全関連機能

安全関連機能	機能の詳細	入力要素	出力要素
E-stop control	to monitor the E-STOP with monitored reset.	E-stop button	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Two hand control	to utilize the two-hand controller with automatic reset	Two-hand controller	Switching off of Inverter, Activation of N.C. brake
ESPE / AOPD control	to initiate redundant switch off and to count the number of the interventions for PSDI	ESPE / AOPD	Switching off of Inverter, Activation of N.C. brake,
Inverter switch off monitoring	to activate cyclically the redundant switch off paths of Inverter circuit to check their normalcy	Feedback loop from Inverter	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Encoder arrangement monitoring	to monitor the discrepancy among the encoders	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
SPM (Broken shear pin) monitoring	This function should be included in the above		
Position reset monitoring	to confirm the slide position returns a programmed position (e.g., TDC) by Inching for restart	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Overrun monitoring	to monitor that the slide motion stops within the designated time or distance after a stop command (Regenerative breaking)	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Braking performance check	to check the performance of normal closed type of mechanical brakes	Logic solver, Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Safe motor torque check	to check the motor torque output by using current sensor to detect the secondary current	Logic solver, Current sensor	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Standstill monitoring (Safe operation stop)	to monitor the standstill of the drive at a current position or reset position (If zero-speed is achieved by external mechanical brakes, it is not needed)	Rotary encoder, Linear encoder, Current sensor	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Safety-related parameterization	to input safety-related parameters such as TDC, Max speed, Braking distance, etc.	Interface unit, Motion controller	Prevention of startup
Single cycle operating	to enable only one cycle and to stop the slide movement at a programmed position (TDC)	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Limited movement control	to monitor that the slide motion is limited within 6 mm or 10 mm/s (i.e., Inching)	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Operating mode selector	to detect more than one inputs as a fault	Selector switch	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Motion direction monitoring	to monitor the direction of slide motion	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart
Muting function	to suspend temporally the protective devices at the upward movement of the slide	Rotary encoder, Linear encoder	Switching off of Inverter, Activation of N.C. brake, Prevention of restart

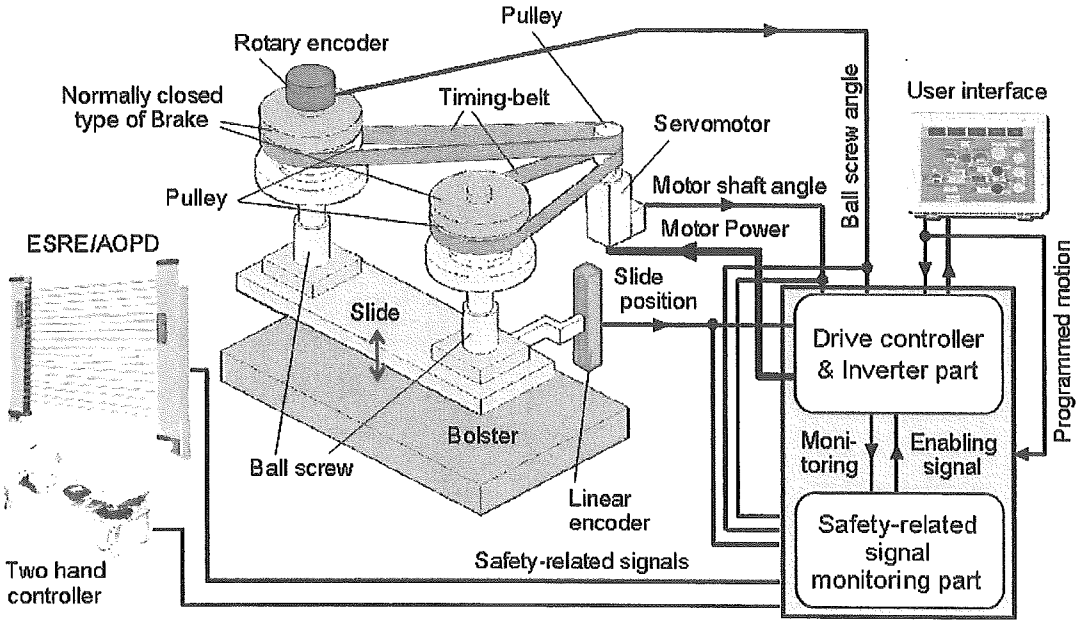

Fig. 3　想定するサーボプレスシステムの構成

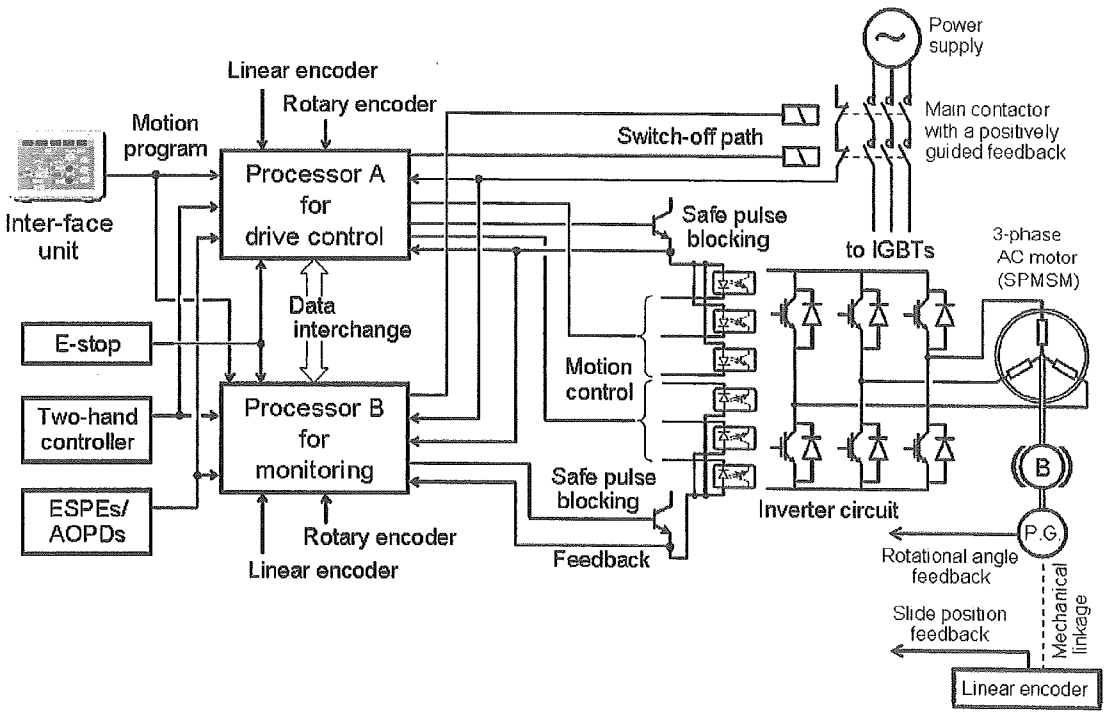

Fig.4　想定するサーボプレスの制御システムの安全関連部の構成