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

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，$PFH_{d\,SS1}$ $=4.07\times10^{-8}$[1/h]となった。なお，DC 及びβの値と $PFH_{d\,SS1}$ との関係については，6.5.4.6節で別途改めて考察する。

1.5.4.3 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 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，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 $PFH_{d\,2a}$ を S4 に至る確率として次式で求める。

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

λ_{VMD} =500 FIT，λ_{PSD} =500 FIT，β=2%，r_{Rep}=0.125[1/h]とおいた結果，$PFH_{d\,2a}=2.51\times10^{-8}$ [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 $PFH_{d\,SS2}$ は次式で求められる。

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

1.5.4.4 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 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 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，$PFH_{d\,SS3}=3\times10^{-8}$ [1/h]とする。

1.5.4.5 システム全体の評価

得られた 3 つのサブシステムの 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 PFH_d を求める。

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

SIL3 の条件の 1 つである $PFH_d < 10^{-7}$ [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（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。

1.5.4.6　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。

6.5.4.2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。

1.6　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

本派遣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，本派遣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。

本派遣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，$PFH_{d\,SP}=1.3\times10^{-9}$ [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。

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

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 $PFH_d = 9.9\times10^{-8}$ [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

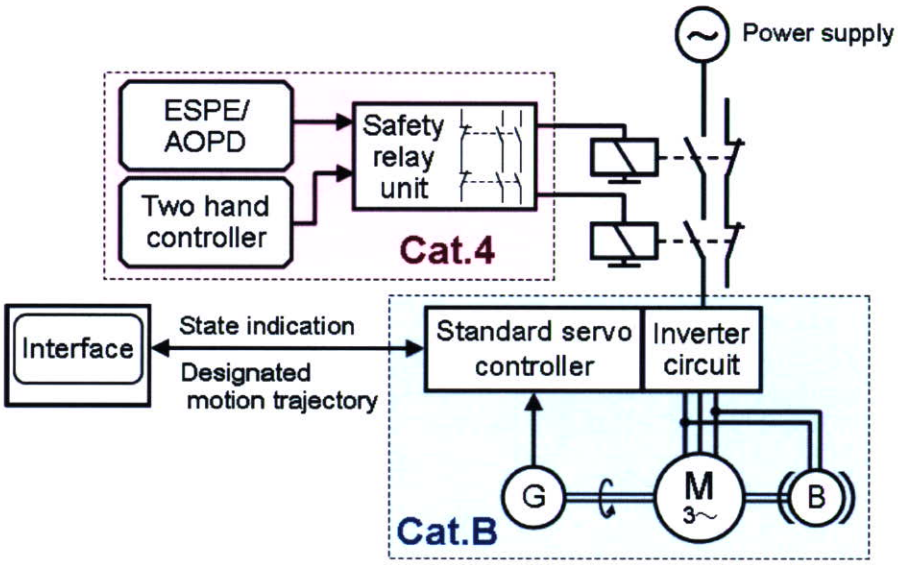


Fig. 1　既存の安全リレーユニットを用いたサーボプレス制御システムの構成例

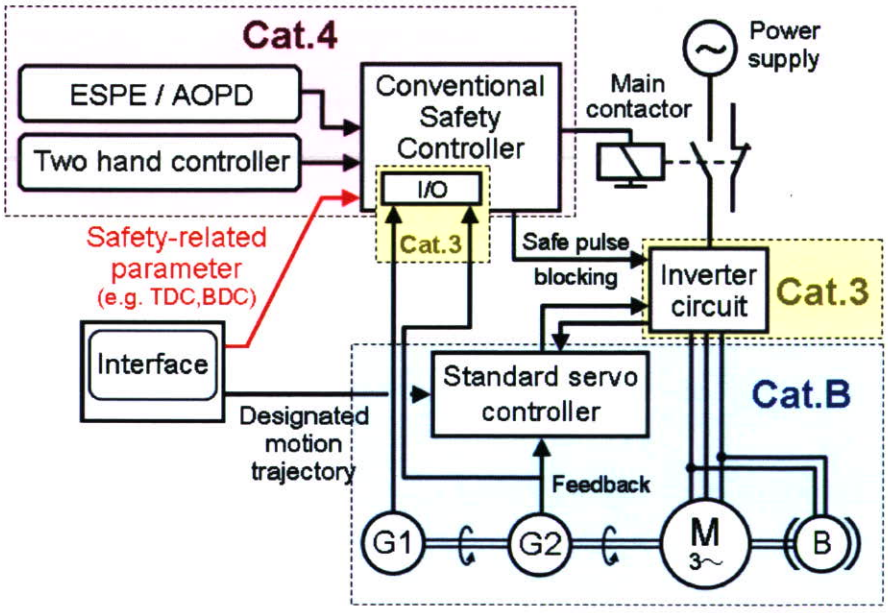


Fig. 2　Cat.3 のインバータと Cat.4 の Safety PLC を用いたサーボプレス制御システムの構成例

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

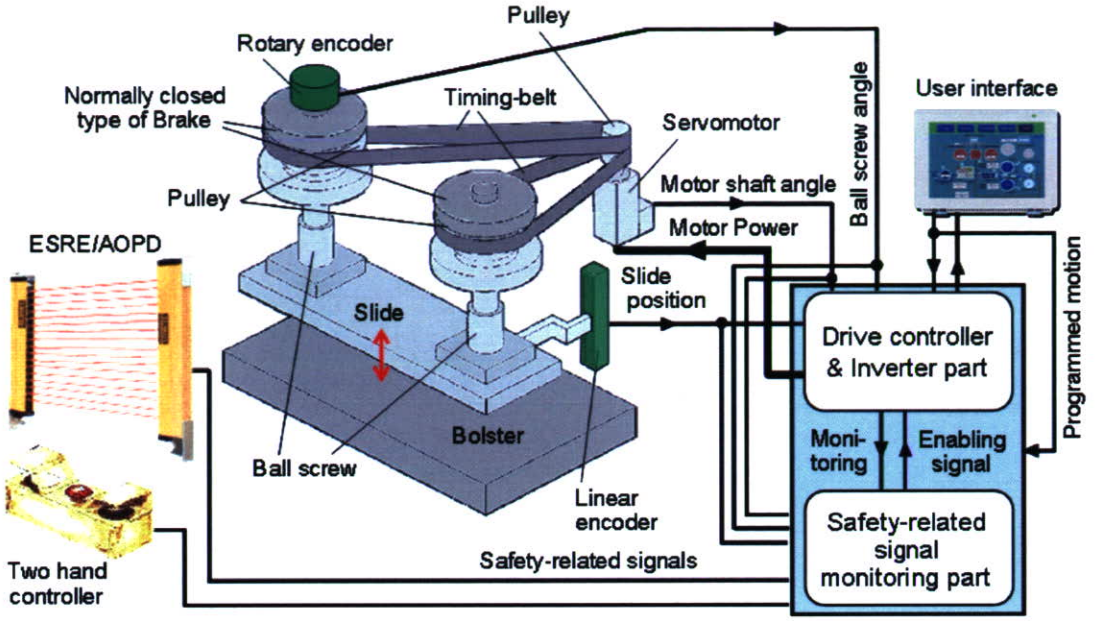


Fig. 3　想定するサーボプレスシステムの構成

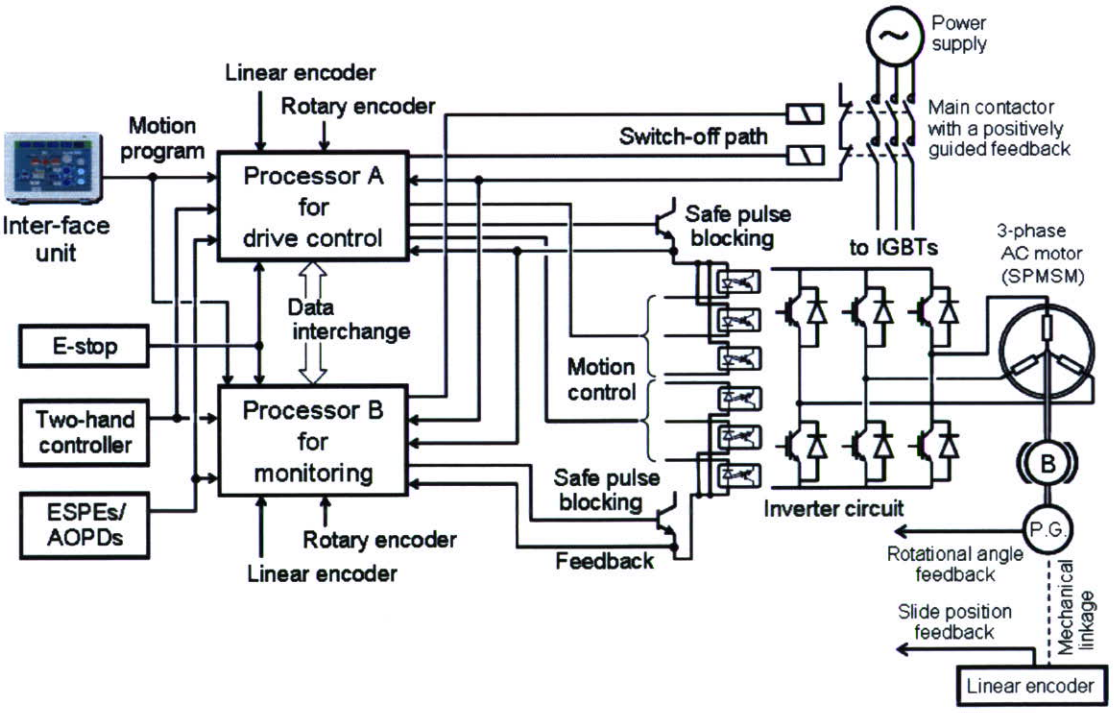
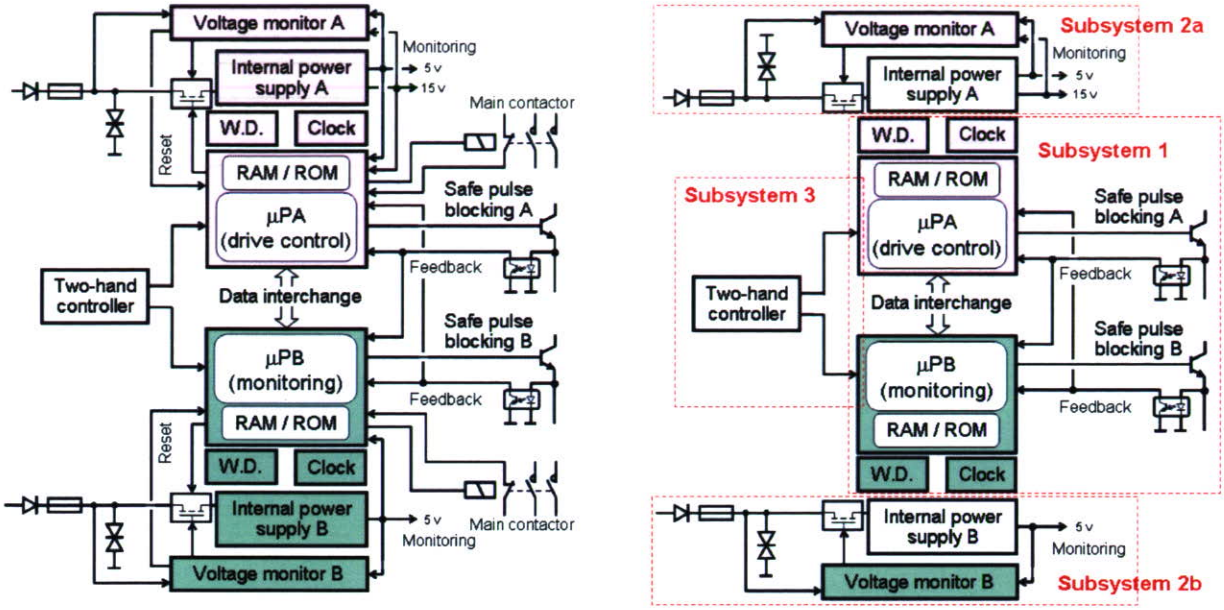


Fig.4　想定するサーボプレスの制御システムの安全関連部の構成



(a) 機能ブロック図　　(b) サブシステムへの分解

Fig.5　Inverter switch off monitoring 機能に関連するハードウェアの機能ブロック

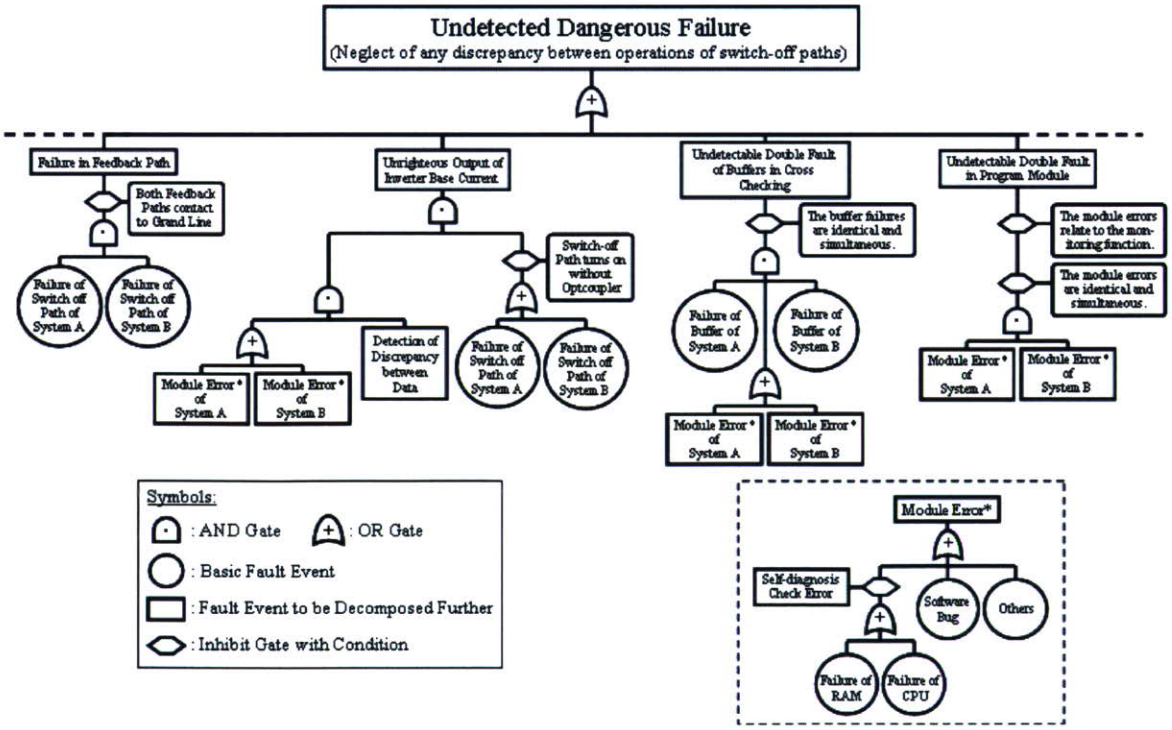


Fig.6　遮断パスの動作不一致の見過ごしをトップイベントとする FTA（抜粋）

表 4　診断有効度（DC）の推定例

診断機構・手法（IEC 61508-2 annex A）	主張される DC	手法の説明
A.3 Failure detection by online monitoring	Medium	cyclic test checks redundant channels
A.3 Monitored redundancy	High	cyclic test checks redundant channels
A.4 Self-test "Walking bit"	Medium	self-test of μP
A.4 Reciprocal comparison by software	High	intermediate and test results are exchanged
A.5 Block replication	High	data are replicated and compared
A.6 RAM test "Galpat"	Medium	done by μPs
A.8 Inspection using test patterns	High	cyclic communications including test pattern on data bus connecting μPs
A.10 (A.12) Watchdog with separate time base and time window	Medium	monitoring of cyclic test result can act as watchdog with different time base
A.10 (A.12) Combination of temporal and logical monitoring of program sequence	High	done by data exchange at every check point on program sequence
A.13 Separation of electrical energy line from information line	High	considered in circuit design
A.15 Cross monitoring of multiple actuators	High	cyclic test checks both switch off actuators
		Result : DC = High (99%)

表 5　βファクタの推定例

評価項目の分類	評価値	
	X 値	Y 値
Separation, Segregation, etc	3.50	1.50
Diversity, Redundancy, etc	10.00	3.00
Complexity, Design, etc	2.75	2.25
Assessment, Analysis, etc	0.25	4.75
Procedures, Human interface, etc	3.50	3.00
Competence, Training, etc	1.25	3.75
Environmental control	2.75	2.25
Environmental test	5.00	5.00
Total	29.00	25.50
Score (S = X+Y)		54.50
βfactor		2 %

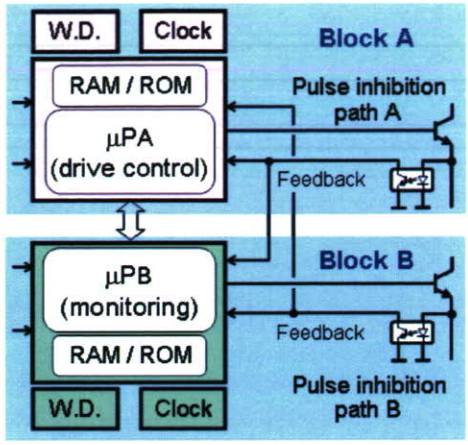


Fig.6　サブシステム 1 の分割

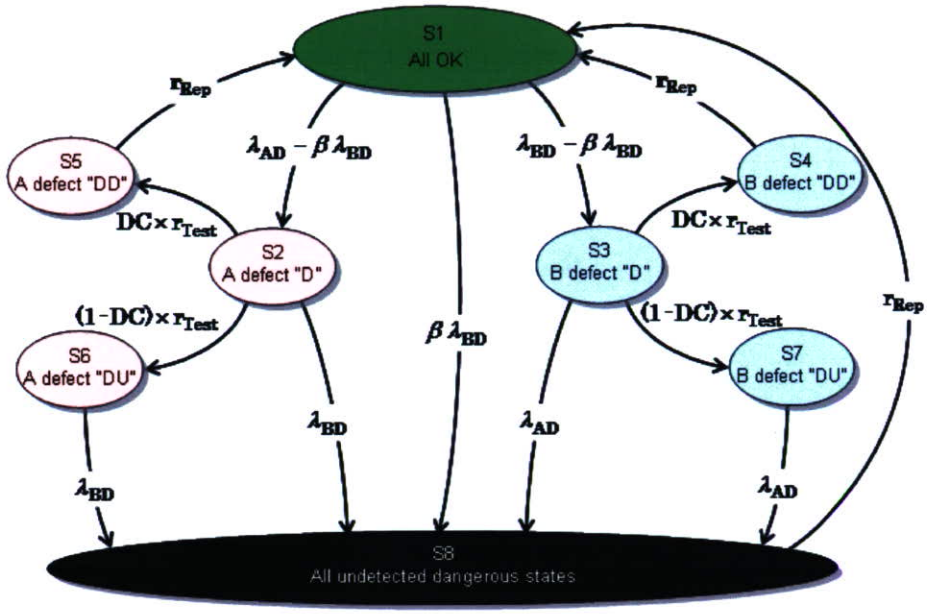


Fig.7　サブシステム 1 のマルコフ信頼性モデル

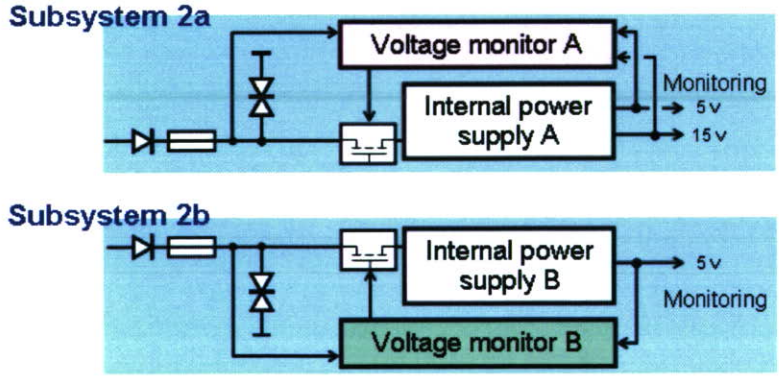


Fig.8　サブシステム 2 の構成

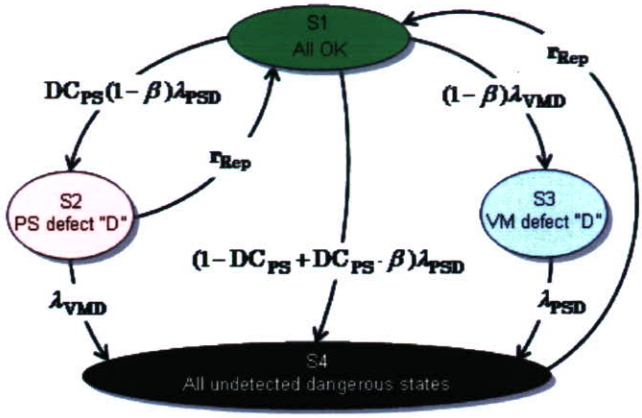


Fig. 9　サブシステム 2a のマルコフ信頼性モデル

表 6　Inverter switch off monitoring 機能の安全性能評価結果

要求項目	Cat.4 の要求値	SIL3 の要求値	Inverter switch off monitoring 機能の評価結果
障害許容度	≧1	−	1
DC_{avg}	≧99%	−	99%
SFF	−	≧90%	99%
$MTTF_d$	≧30[y]	−	43 [y]
PFH_d	−	$<10^{-7}$ [1/h]	7.2×10^{-8} [1/h]

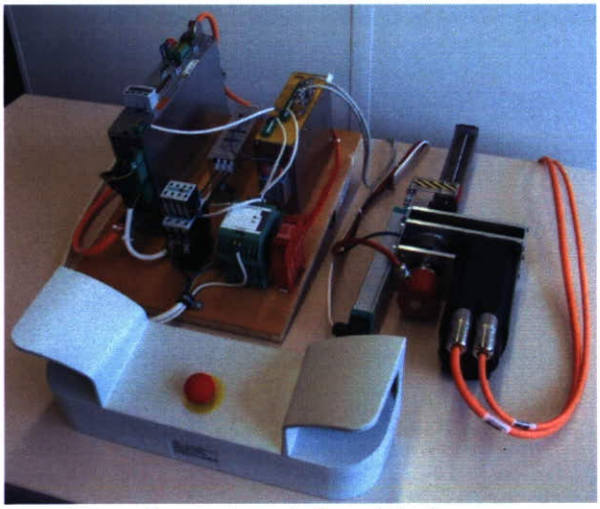
表 7　DC, β ファクタ, r_{Test} とサブシステム 1 の PFH_d との関係

DC	β	r_{Test} [h^{-1}]	PFH_d $\times10^{-8}$ [h^{-1}]	DC	β	r_{Test} [h^{-1}]	PFH_d $\times10^{-8}$ [h^{-1}]	DC	β	r_{Test} [h^{-1}]	PFH_d $\times10^{-8}$ [h^{-1}]
0.99	0.02	1	4.073	0.90	0.02	1	7.349	0.60	0.02	1	17.767
		1/8	4.079			1/8	7.354			1/8	17.777
		1/24	4.094			1/24	7.367			1/24	17.778
	0.05	1	9.610		0.05	1	12.714		0.05	1	22.602
		1/8	9.616			1/8	12.720			1/8	22.605
		1/24	9.630			1/24	12.732			1/24	22.612
	0.10	1	18.838		0.10	1	21.668		0.10	1	30.699
		1/8	18.844			1/8	21.673			1/8	30.702
		1/24	18.856			1/24	21.684			1/24	30.709

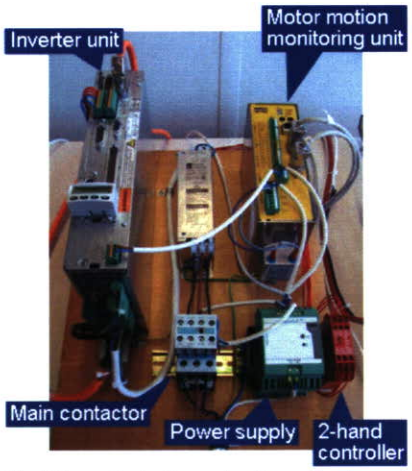
表 8　主な共通原因故障防止方策

項　　目	説　　明
Separation, Segregation	Physical separation between signal paths, e.g. separation in wiring. Sufficient clearances and creepage distances on printed-circuit boards.
Diversity	Different technologies/design or physical principles are used (e.g. first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, measuring of distance and pressure, digital and analogue, components of different manufactures).

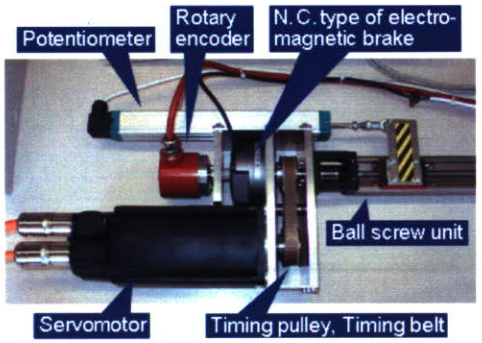
Design, Application, Experience	Protection against over-voltage, over-pressure, over-current, etc.
Use of well-tried components	Occurred components are successful used for several years under consideration environmentalinfluences.
Assessment, Analysis	The results of a failure mode and effect analysis (FMEA) are taken into account to avoid common-cause-failures in design.
Competence, Training	Designers/ maintainers have been trained to understand the causes and consequences of commoncause failures.
Electromagnetic compatibility	The system has been checked for EMC-immunity (e.g. as specified in relevant product-standards).
Other influences	The requirements for immunity to all relevant environmental influences like, temperature, shock,vibration, humidity (e.g. as specified in relevant standards) are considered.



(a) Composition of experimental model of servo press system



(b) Safety related part of control system



(c) Mecanical part including servo motor

Fig. 9　サーボプレス用安全ドライブシステムの実験モデル

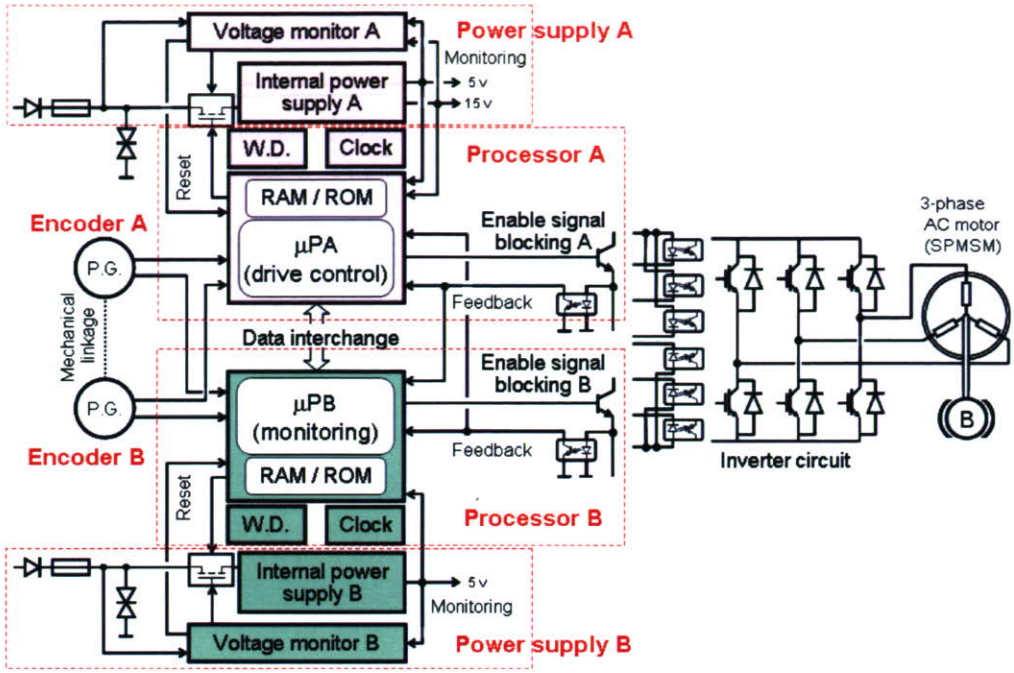


Fig.10　Encoder arrangement monitoring 機能に関連するハードウェアの機能ブロック

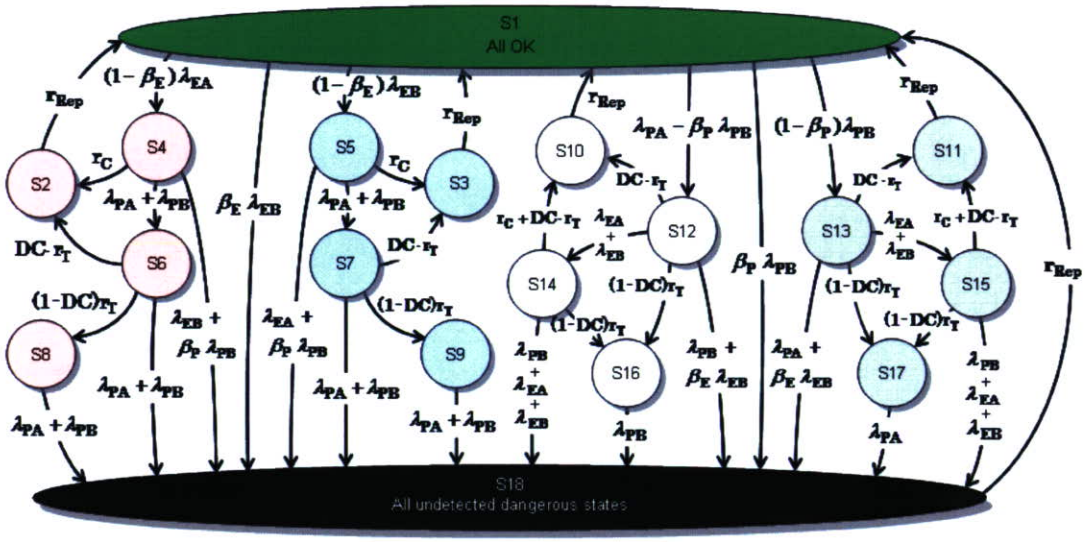


Fig.11　EA, EB, PA, PB で構成されるサブシステムのマルコフ信頼性モデル

表 9　状態 S1～S18 の定義

状 態	定　義
S1	すべてのコンポーネントが正常に稼働している
S2	EA の故障が検出された又は EA が故障した状態で PA か PB の故障が検出された
S3	EB の故障が検出された又は EB が故障した状態で PA か PB の故障が検出された
S4	EA が故障した（EB は正常）
S5	EB が故障した（EA は正常）
S6	EA が故障した状態で PA 又は PB が故障した
S7	EB が故障した状態で PA 又は PB が故障した
S8	EA が故障した状態で PA 又は PB が故障したが検知されなかった

S9	EB が故障した状態で PA 又は PB が故障したが検知されなかった
S10	PA の故障が検出された又は PA が故障した状態で EA か EB の故障が検出された
S11	PB の故障が検出された又は PB が故障した状態で EA か EB の故障が検出された
S12	PA が故障した（PB は正常）
S13	PB が故障した（PA は正常）
S14	PA が故障した状態で EA 又は EB が故障した
S15	PB が故障した状態で EA 又は EB が故障した
S16	PA の故障が検知されなかった
S17	PB の故障が検知されなかった
S18	危険側故障状態：両エンコーダ又は両プロセッサが故障した

表 10　エンコーダ EA, EB の危険側故障率と β ファクタを変えた場合の $PFH_{d\ EnPr}$

EA, EB の危険側故障寿命	EA, EB の危険側故障率	β ファクタ		
		5 %	0.5 %	0 %
100 years	1142 FIT	9.77×10^{-8}[1/h]	4.64×10^{-8}[1/h]	4.07×10^{-8}[1/h]
10 years	11420 FIT	61×10^{-8}[1/h]	9.77×10^{-8}[1/h]	4.07×10^{-8}[1/h]
1 year	114200 FIT	573×10^{-8}[1/h]	61×10^{-8}[1/h]	4.07×10^{-8}[1/h]
1 week	5952381 FIT	16652×10^{-8}[1/h]	2570×10^{-8}[1/h]	4.16×10^{-8}[1/h]

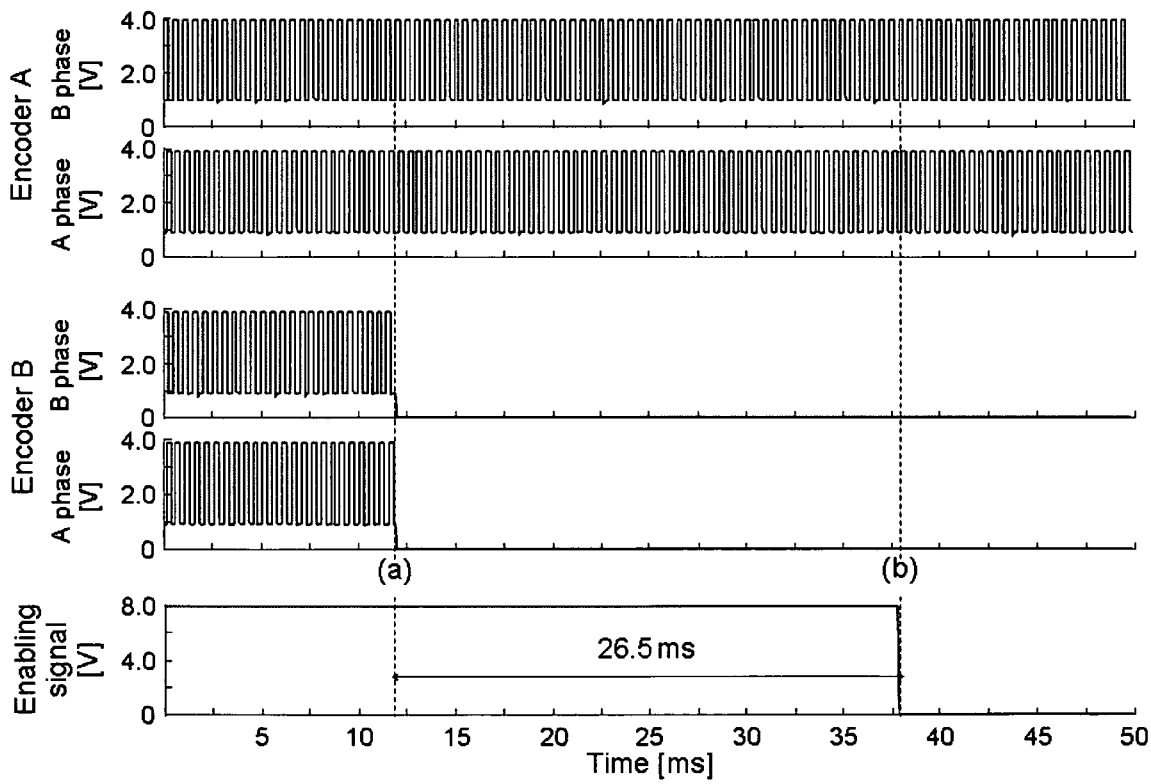


Fig.12　Encoder arrangement monitoring 機能の動作検証実験結果の一例

2. まとめ

本研究によって得られた成果は以下のとおりである。

1. 現在，日本と同様，ドイツ国内の複数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，サーボプレスの安全性能評価試験方法の確立がドイツ国内においても求められていることを明らかにした。
2. ドイツ国内では，安全関連機能が実装されたサーボドライブシステム／インバータシステムがすでに普及しているが，従来の製品を単に使用するだけでは，サーボプレスに適用可能な安全なサーボドライブシステムを構築することは困難であることを明らかにした。
3. 従来の機械プレスの構造とサーボプレスの構造の比較から，サーボプレスの危険性を指摘した。
4. ISO13849-1 のカテゴリと IEC61508 の安全完全性レベルを比較し，サーボプレスに適用されるサーボドライブシステムの安全性能評価指標を検討した。
5. サーボドライバの安全関連機能を検証するための評価手法を提案した。この中で，特に，サーボプレスに要求される種々の安全関連機能を明らかにするとともに，ハードウェアの危険側平均故障率の定量的評価法について示した。
6. ドイツ国内にて入手可能なインバータユニットとサーボシステムの動作監視ユニットを用いた実験モデルの構築を通じて，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構成例を示した。
7. 実験モデルに実装された安全関連機能のうち，エンコーダ信号の不一致検知機能を取上げ，提案する評価手法に基づいて安全性能を評価するとともに，動作検証実験より検知応答性能を調べ，以上の結果から所要の安全性能が実現されていることを確認した。

提案するサーボドライブシステムの安全性能評価手法において，PFH_d の導出にマルコフ信頼性モデルを用いたが，PFH_d の計算自体はあくまでも安全性能評価の一側面でしかないことに注意が必要である。すなわち，FMEA／FTA の結果から DC やβパラメータを導く比較的定性的な評価の過程（すなわち，すべての故障の予測とそれに対する方策の妥当性の検証）のほうが検証過程ではより重要な位置を占める。同時に，これらは，ソフトウェアの妥当性検証，系統的原因故障の検証にも密接に関連している。なお，安全性能評価の過程では，このような検証作業を行う解析者のコンピテンシー（技量・知識・実績）も問われ，その意味で，今後は，より実際的なシステムに本評価方法を適用し，安全性能評価の根幹となる基礎データの蓄積に精励していきたい。