Specific Research Report of the National Institute
of Industrial Safety, NIIS-SRR-No.19 (1999)
UDC 62-192 ; 681.5.09 ; 681.518.5

2．コンピュータを利用した安全制御技術の実態調査

池田博康*

2.1 はじめに

最近の機械類は，NC工作機械や産業用ロボットをはじめとして，プログラムを変更するだけで多様な作業に対応できる汎用機としての能力を備えているものも多い。このような機械では，プログラムを適切に組むことによって，機械の多様な作業であっても運用効率の良い運転をすることが可能である。また，機械の機能的な有利さのみならず，安全の機能についても，運転条件が変更される毎にプログラム上で随時安全の条件を更新しながらインタロックを組むことができれば，生産性を阻害することのない機械の運用が期待できる。

以上のような理由から，近年，PLC（プログラマブル・ロジック・コントローラ）やマイクロ・プロセッサ（MP）搭載の制御装置などのコンピュータを利用したプログラマブルな電子制御装置が，機械のフレキシビリティと運用効率を高めるための制御だけでなく，安全の制御の用途にも利用され始めてきている。

しかし，プログラマブルな電子制御装置によって制御される機械では，プログラムのバグや電子制御装置の故障，ノイズの影響等によって，機械が不意作動したり，最悪暴走する危険性は常に残る。このため，プロセッサの多重化や自己故障診断システムの適用等によって高信頼化を図り，安全性により配慮した制御装置の構成手法が採られている。

ここでは，このような手法の実態を把握するために，ドイツのピルツ社が開発した三重化安全コントローラ[1),2)]及びハネウェル社が開発したフェールセーフ・コントローラ[3),4)]の調査を行った。

2.2 三重化安全コントローラの実態調査

2.2.1 開発の経緯

ドイツのピルツ社では，安全制御のための古典的な機器として，各種のリレーユニットやリレーモニターを開発してきた。一方，同社では，従来のリレー制御方式に代わって，安全制御に適用するためのPLCを10年ほど前から開発研究してきている。このPLCの構成原理はアーヘン工科大学で提唱され，それがBG(ドイツの同業者傷害保険組合）で検証されて後，同社で実際に開発がスタートしたという経緯があった。最近になって，従来のリレーロジックをソフトウェアで記述したプログラマブルな安全コントローラ（PSSシリーズ）として製品化され，我が国でも1997年から販売されるようになった。

このコントローラは，元々はプレス機械のPSDI(光線式安全装置による起動）への適用を目的としたものであった。これは，PSDIの制御を従来からプレス機械の制御に用いられてきたリレー回路で実現しようとする場合，制御装置が大型化・複雑化することになり，信頼性とコストの面で問題があったためである。そこで，PSDIの機能を含めてプレス制御機能をすべてプログラム化し，従来のリレー回路と同等の安全性及び従来以上の高い信頼性を実現しようとした。

このような経緯から本コントローラは開発され，現在では汎用の安全コントローラとして，様々な機械に適用分野を広げつつある。

2.2.2 安全コントローラの概要

本コントローラには，本来対象機械が目的とする作業を実現するための標準制御機能と，安全関連部分を担当する安全制御機能が独立して組み込まれており，安全制御機能は標準制御機能に優先して安全側，すなわち機械を停止させる側への処理を実行する。

図1に，本コントローラの基本構成を示す。このコントローラの最大の特徴は，安全制御のためのプログラムを実行するプロセッサが独立して三重化されているという冗長構造を持つことにある。

この三重化は多数決演算で一般的である2 out of 3（3つの結果の内2つ以上が同じならば結果を出力する）とは異なり，3 out of 3（3つの結果が全てが同じでなければ結果を出力しない）という考えに基づくものである。すなわち，同一接点入力に対して3つの独立したプロセッサが並列に信号処理を行った後，各プロセッサの出力信号を照合用メモリDPR（デュアル・ポート・ラム）を介して相互に比較し，出力信号が全て同じ場合のみを駆動するための運転許可信号（例え

*機械システム安全研究部　Mechanical and System Safety Research Division

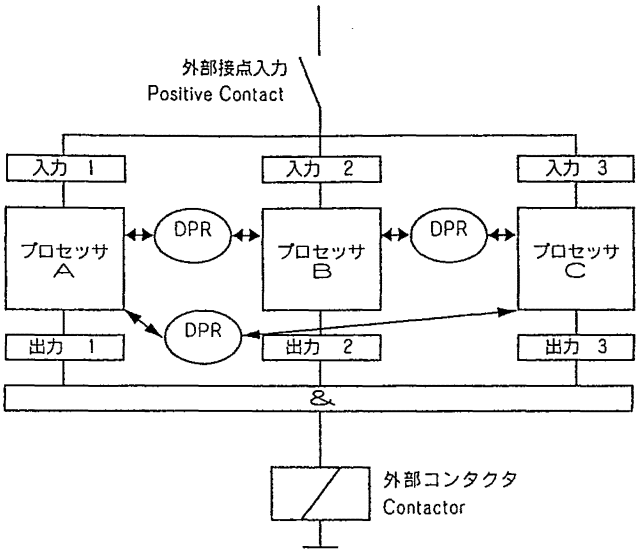

図1　三重化安全コントローラの基本構成

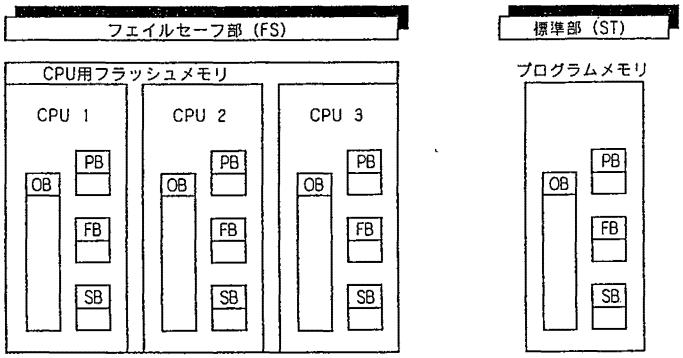

図2　多重化メモリ構造
OB, PB, FB, SBはプログラムブロックを表す。

ば外部コンタクタ駆動信号）を出力する。しかし，もし一つでもプロセッサの出力信号が異なっていれば，信号処理過程で何らかのハードウェアあるいはソフトウェアの誤りが生じたものとして，運転許可信号は出力されない。この後，運転の再開のためには，リセット操作により誤りが回復あるいは除去される必要がある。

実際のコントローラを運用する上では，プログラムのバグや電子回路素子の故障，ノイズの影響等が想定されるため，冗長化構造をもってしても誤った運転許可信号を出力してしまう可能性は避けられない。例えば，冗長化構造により誤りが検出されたとしてもそれが確実に出力オフとなるのか，あるいは，各々のプロセッサに同じタイミングでノイズが侵入したら同じ誤りを呈してしまうのではないか，といった懸念が残ることになる。

このため，本コントローラでは，次のような機能や構造を持たせて，誤った運転許可信号による機械の暴走や不意作動を防いでいる。

1）ダイバシティ（多様性）構造

冗長化プロセッサ各々に異なった種類のものを使用するため，プロセッサの特性(特に処理速度)，プログラム及びその処理方法等も異なる。したがって，このような構造とすれば，ハードウェア的にもソフトウェア的にもダイバシティを持たせることができる。ダイバシティを持つ冗長構造においては，プログラムのバグ，プロセッサの故障が各々のプロセッサチャンネルの同じ場所に同時に起こることは考えにくい。

また，ノイズが各プロセッサチャンネルに同時に侵入した場合を想定しても，全てのチャンネルが同時刻に同じ誤りを生じて，誤った運転許可信号を発生させてしまう可能性は，単一種類による冗長構造に比べれば著しく低くなる。

2）メモリエリアの多重化

図2に示すように，各々のCPU（中央処理装置，一般にプロセッサと同義語として扱う）に独立して別々のメモリエリアを割り付けている。各メモリ内に格納されるプログラムブロックやデータは，機能的には同等であるが，CPUが異なるためにその形態やアドレス等が同じというわけではない。したがって，メモリ内に異常が生じた場合でも，全てのメモリにおいて同時刻に同じ誤りを生じる可能性は極めて小さいと見なせる。

なお，安全制御機能部（フェイルセーフ部）と標準制御機能部（標準部）間でも，独立したメモリ構成となっている。

3）自己診断機能

単一プロセッサであっても，自己診断機能はプロセッサの高信頼化には必須の機能とされる。通常，自己診断機能は電源投入時だけでなく，プログラム実行中にも随時働くように組み込まれる。すなわち，電源投入時に全ての項目の診断を行い，全て正常であるならばプログラムが実行されて，図3に示すような1スキャン毎に診断を繰り返すことになる。

しかし，本コントローラのような冗長構造の場合，診断項目は多くなり，全ての項目の診断に30秒程度かかるために，スキャン毎の診断は診断項目（データ）を時分割した一部分（約5 ms）を行っている。このテクニックにより，プログラム実行中の自己診断時間は5～6分以内に収まっている。

4）入出力信号のチェック

入出力信号はI/O（入出力）インタフェースを通してCPUとやり取りされるが，CPU側でいくら対策を施して正常動作を保証しても，誤った信号が入力されたり

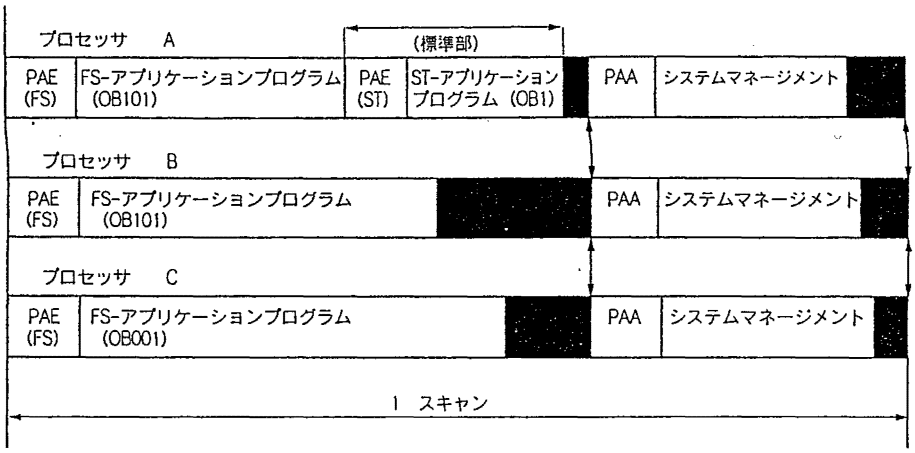

図3　3つのプロセッサによる自己診断タイミング
PAEは入力処理を，PAAは出力処理を表し，塗りつぶし部分は同期のための時間調整を示す。

出力段階で誤った信号を出力してしまうかもしれない。そのため，入出力段階での信号チェックは特に重要となる。

本コントローラの重要な入力信号には，8種類の異なるタイミングのテストパルス・クロックが重畳される。これにより，予め登録されたクロック以外の入力信号は，配線異常（例えば短絡，断線，誤配線等）として検出されることが可能となる。

一方，出力信号は，図4に示すようなトランジスタ（T^+，T^-）が駆動されて出力される。この出力回路の特徴は，各トランジスタの動作状態を常時モニタしていることにあり，トランジスタや外部配線の短絡と断線故障をCPUへフィードバックして通報できる。なお，重要な出力信号は図4の回路を2個利用して出力される。

以上のような多重化構造と自己診断機能により，本コントローラはドイツのBG電気専門委員会から，機械に関する欧州安全規格EN954で規定される最高レベルのカテゴリー4を認定されている。

2.2.3　安全水準の認定

本コントローラはプレス機械への適用を最初に想定していたため，BGによる認定は機械安全規格であるEN954で行われた。この規格では，安全水準がカテゴリーB，1～4まで規定されており，プレス機械のような危険な機械で利用される機器には最高のカテゴリー4が要求されている。

このカテゴリー4では，多重故障が起こっても安全機能を損なわないよう要求されており，最初の故障を漏れなく速やかに検知して安全側への処理を行う必要がある。したがって，強力な自己診断機能と高速な処理時間（スキャンサイクル）が必要となるが，これら

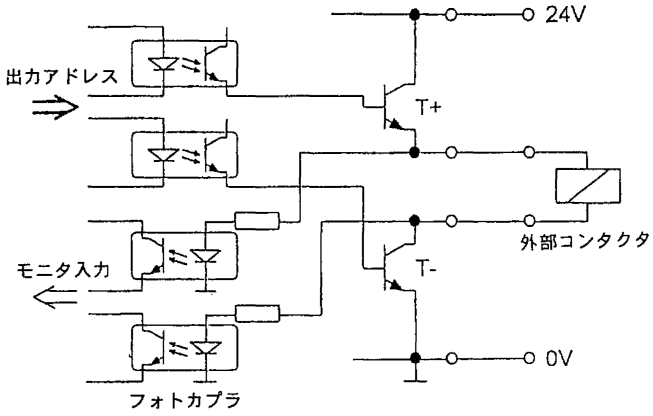

図4　モニタ付き出力回路

両者は相反する関係にあり，従来の二重系構造の場合（例えばシーメンス製の二重化コントローラ）はカテゴリー4をクリアはするが，両者のトレードオフを考慮するために適用範囲が限定される。一方，本コントローラは，3つのチャンネルの内最悪でも2つの故障が発生している間に故障を検知できればよいことから，自己診断時間のマージンをとることができ，診断処理時間を犠牲にしないで自己診断機能を強力にすることが可能となる。この点は，本コントローラの高信頼化の現実的な選択であると思われる。

また，ソフトウェアの問題として，プログラム変更で機能を容易に書き換えることができる反面，その安全機能が維持される保証がないことが挙げられる。そこで，本コントローラでは，従来の安全リレー回路と同等機能を持つ安全制御機能の基本的なプログラムが，ハードウェアと同様に検査，認証されて，ユーザーが変更できないようブロック化される。

本コントローラは，TUV（ドイツ技術検査協会）や

スイスの認証機関であるSUVAでも同様に認証されているが，今後は現在審議中のプログラマブルな機器に対する国際規格IEC61508及び62061への適合も検討されている。

2.2.4　検討課題

本コントローラの設計思想は，欧州規格でも規定されているように完全に同時に発生する二重故障は有り得ず，単一の故障が発生した後，次の故障が発生するまでに対処すれば，カテゴリー4の安全性レベルは確保できるという考え方に基づいている。ほんの僅かでも二重の故障発生の時間差があれば，その時間内に最初の故障を検知して出力オフあるいは故障からの修復が実行され，安全性は確保されるという論理である。したがって，少なくとも二重系構造にしてあれば同時ではない二重故障に対処することは可能であり，さらにダイバシティのある冗長構造であるならば，同時多重故障が起こる可能性はほとんど無いと考えられる。

しかし，最初の故障が潜在して，それが顕在化するときに次の故障が同時に起こる可能性も否定できず，ダイナミック・フェイルセーフの考え方ではそのような同時多重故障も考慮して設計される。また，原子力発電所におけるシステムでは，同時多重故障が起こり得ると考えて対策を講じる場合も多い。現実に本コントローラで同時多重故障が起こる確率は算出されておらず，この同時多重故障に対して合理的に説明するまでに至っていない。

また，本コントローラの信号出力段階における同時多重故障を考えると，仮に一つの出力素子（図4におけるT^+あるいはT^-）が短絡故障を起こしても他の素子が出力遮断してくれる仕組みとなっているが，全ての出力素子が同時に故障するか，あるいは同時でなくとも発生した故障が検出されなかった場合には出力遮断ができない恐れがある。実際には，同時多重故障も配慮しているためか，最後に出力を遮断するための有接点リレーが電源ラインに装備されていた。ただし，この場合，接点に溶着が起こると出力をオフできないという問題が生じる。この問題は，本装置だけでなく他のコントローラに共通する問題であり，今後の検討が必要とされる。

2.3　フェールセーフ・コントローラの実態調査

2.3.1　開発の経緯

ドイツでは，機械設備や産業用プラント装置の安全制御のために，従来のリレーロジック回路に代わってPLCを利用する技術の開発を進めてきた。この技術は，1980年代の初期には汎用のPLCと2 out of 3構成のリレーを組み合わせるという方式であったが，このような方式はドイツ規格では安全性が高いとは認められなかった。

このため，1986年頃からTMR（Triple Modular Redundant：2 out of 3方式による三重化）技術を利用したPLCが実用化されるようになり，高水準の安全性が達成された。これは，トライコン（TRICON）システム[5]のものが有名であり，三重化されたCPU間で通信を行って相互の処理結果の照合を2 out of 3方式で行う仕組みである。このような構成のPLCは，DIN V 19250（安全クラスを決定するためのドイツのガイドライン）の安全度要求でクラス5に適合するとTUVから認証されている（ちなみにこのクラスは1から8までであり，8が最高レベルである）。

これに対し，ハネウェル社は，TMR技術で構成されたPLCは複雑でコストがかかるとして，基本的に単一CPU構成で充実した自己診断機能を盛り込んだ基本PLCシステムを開発し，主にプロセス制御用コントローラとしてTUVからDIN V 19250のクラス4までの認定を取得した。さらに現在では，対象アプリケーションの規模や要求される安全性と稼働性のレベルに応じて，基本システムを組み合わせて高度なシステム構成を可能としている。例えば，信号出力にQMR(Quadruple Modular Redundancy：四重化）技術を適用し，CPU自体も二重化を図り，さらにこの二重化CPU自体を冗長構成として，最高クラス6と認定されたPLCを提供している。

2.3.2　フェールセーフ・コントローラの概要

ハネウェル社では，多重化構成と自己診断機能を有するPLCシステムをFSC（フェイルセーフ・コントローラ）あるいはSM（セーフティ・マネージャー）と称しており，高水準の安全性と稼働率を両立させた高信頼なコントローラという位置付けをして，一般の汎用PLCとは区別している。

このFSCは，設備・プラント等の制御対象の機能的制御部分は従来のコントローラにまかせて，安全関連部分の制御だけを管理する機能を持つ。すなわち，汎用PLCの作動中に危険側となる故障や異常があれば直ちに安全機能が働くという階層化制御システムとなっている。

以下にFSCの構成と特徴を記す。

1）基本構成

基本的なFSCは，単一CPUを用いた汎用PLCと同じ構成要素から成り立ってはいるが，メモリを二重化し，また自己診断機能であるWD（ウォッチドッグ）を三重化して，この3つのWDによる診断結果を比較照合するという構成である。実際には，稼働率向上のために，図5に示すような並列冗長化構成とした二重化CPU

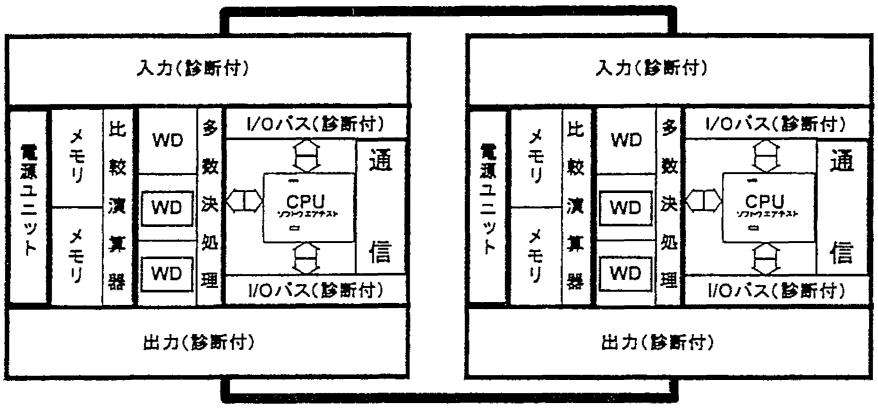

図5　FSC（フェイルセーフ・コントローラ）の基本システム

と二重化I/Oシステムをとるのが一般的であり，基本FSCシステムが電源まで含めて独立して機能し，相互の診断と同期のためにCPUは相互に通信を行う。結局，CPU，電源，通信バスを二重化し，メモリは二重化を2組，WDは三重化を2組装備するという多重化構成によって，潜在化しやすい故障を高い確率で検出し，なおかつ，一個のCPUが故障診断中であっても他のCPUで機能を維持することによって，高稼働率を実現できる。このような構成にすることによって，DIN V 19250の安全度要求でクラス1から4に相当するとされる。

2）故障検知方法と処理

FSCの出力モジュールには，図6に示すような出力用トランジスタT1とSMOD（二次的遮断手段）と呼ばれる安全機能用トランジスタが直列接続され，さらに診断回路の付加により出力用トランジスタの動作状態を監視できる。この診断回路は，出力用トランジスタが正常にオフになることを周期的にチェックし，短絡故障が起こるとSMODにより出力を遮断する。

また，特に重要な信号出力部に対しては，上記の出力モジュール構成を2組並列接続したQMR（四重化）構成とすることで，出力をオフにできない危険側故障の検出だけでなく，稼働率の低下要因となる安全側故障の減少を図っている。

3）高度なシステム構成

図5の基本システム及び二重化CPUと非冗長I/Oからなるシステムを組み合わせることによって，様々なパフォーマンスを持つFSCシステムを構成することができる。例えば，図7は，図5のシステムに加えてI/Oを直列冗長化構成としたシステムであり，同時二重故障にも耐故障性のあることから，DIN V 19250の安全度要求でクラス6に相当する。

なお，FSCシステム開発のためのソフトウェア上の

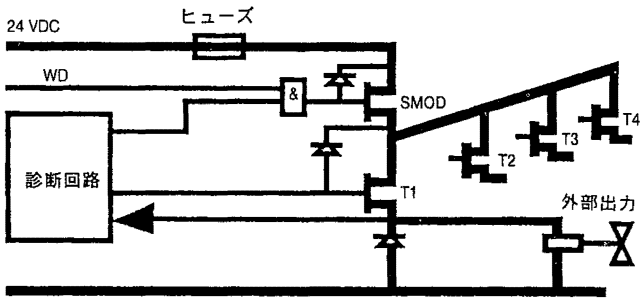

図6　SMODを用いた出力モジュール

配慮として，安全に関わる重要な機能に対してはパスワードによる制限やプログラムの照合機能を持たせることによって，プログラムのオンライン変更が可能となっている。

FSCは既に世界中に1000システムほど稼働されているという実績があるが，適用例はプラントの緊急遮断システム，ボイラの燃焼管理，防災システムのシーケンス管理が多い。FSCは，故障診断時間が比較的余裕のある用途に適しているようである。

2.3.3　安全水準の認定

前述したように，FSCはTUVにより最高クラス6という安全度が認定されている。このクラス分類は，ドイツ規格DIN V 19250，DIN V 0801等によりその要件が規定され，現在ではこれらを基にした国際規格IEC61508（機能的安全）に引き継がれようとしている段階である。このIEC61508では，安全度の水準は4レベルに分類され，DIN V 19250のクラス5，6がIEC61508のレベル3に相当し，DIN V 19250のクラス7，8がIEC61508のクラス4（最高レベル）に相当する。IEC61508はソフトウェア分野などまだ審議が継続しているが，現行の安全に配慮したプログラマブルな機器が最高でもIEC61508レベル3とされていることから，ＦＳＣは現在では極めて高水準の安全性が達成

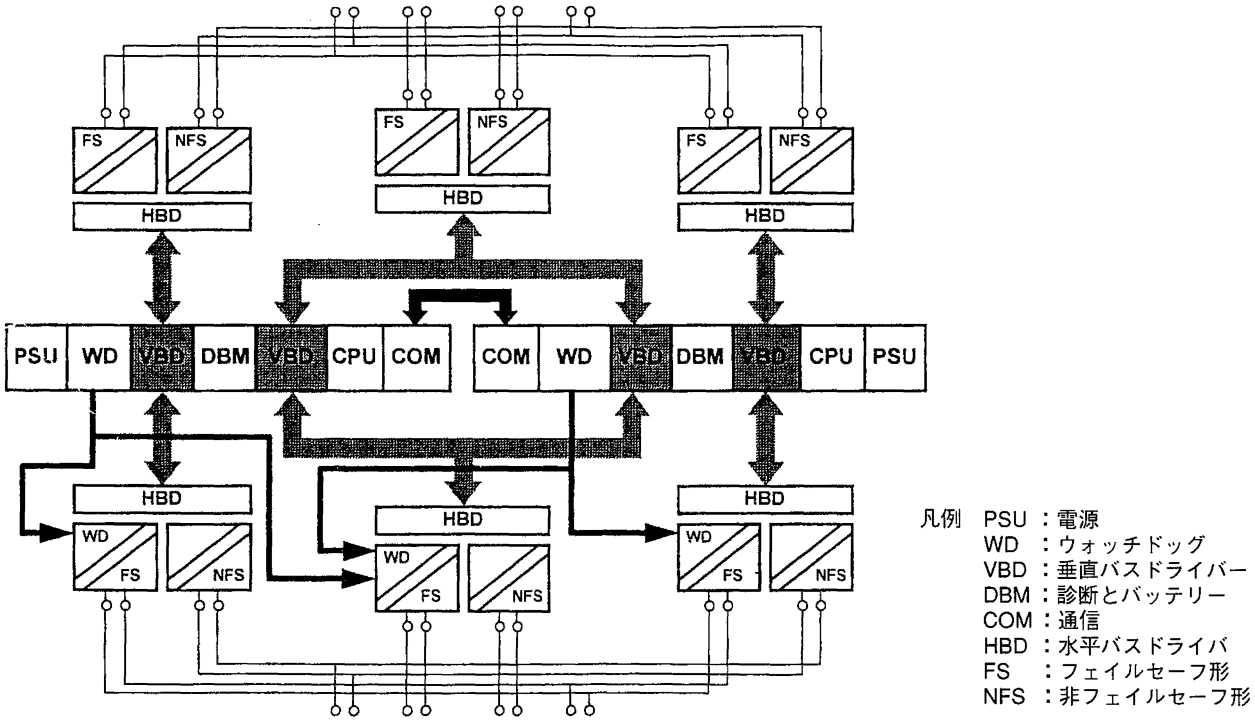

図7　出力を直列冗長化したFSCシステム構成

されていると言える。

ドイツのTUVでは，DIN V 19250の要件として，プログラマブルな機器で起こり得る故障は，ハードウェアのランダム故障，システマティックな故障，ミスやヒューマンエラーによる故障の3種類と定めて，これら全ての故障がPST（プロセス・セーフティ・タイム，図8参照）内で検出されることを求めている。このPSTとは，自己故障診断時間と故障の訂正時間の合計であり，実際のボイラ設備では1秒程度，石油プロセスでは20秒程度とされている。FSCのPSTは1または2秒であり，この周期でI/O部が診断されて，またCPU部も1秒毎に自己診断される。その結果，プロセス設備には有効であるが，人間が介在する可能性のある高速な機械設備（例えばプレス機械等）への適用は，診断周期を短縮しないと難しいと考えられる。

2.3.4　検討課題

マイクロプロセッサを利用するプログラマブルな機器の安全性を向上させるため，強力な自己診断機能と多重化構成は常套手段となっているが，FSCは制御対象が要求する安全度と稼働度に応じて冗長レベルを対応させることで，広範なユーザーの要求に応じることのできる合理的なシステムである。また，制御の対象

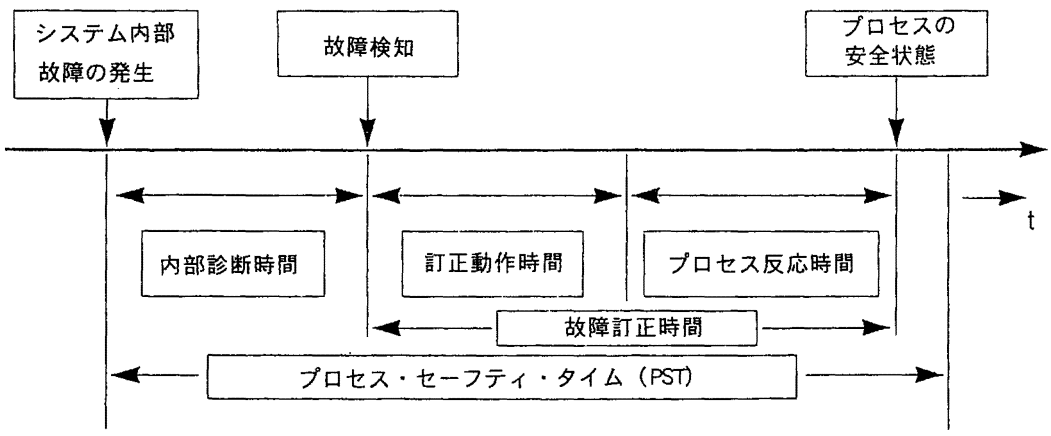

図8　PST（プロセス・セーフティ・タイム）のタイミング図
（1チャンネルシステムの場合）

を機能的部分と安全関連部分とに明確に分けて，FSCは安全関連部分だけに独立して責任を持つという考え方が確立している。しかし，高度なシステム構成にするとコストがかかってしまうことが避けられず，大規模なプロセス設備関連の用途向きとも言える。

現在のFSCは，全ての診断を行うためのPSTが１秒であるために，制御対象はやはりプロセス制御等が中心とならざるを得ず，機械設備の制御への適用にはこの遅さが問題となりそうである。このため，現在の技術では，ある程度稼働率を犠牲にしても，冗長度を落として診断間隔を短くし，より高い安全度を追求する方向が望ましいと考えられる。

また，このFSCの冗長化は，通常は同一種類のもので実現されており，ダイバシティ構造を持たせていない。しかし，同一種類の多重化は，同じ要因で故障が同時に起こる可能性があることが指摘されており，この同時多重故障への対応が今後の安全水準をもう一段向上させるためのポイントになると考えられる。今後，そのような効果を評価できるような定量的な評価手法が必要となると思われる。

2.4 おわりに

近年の電子技術・コンピュータ技術の進展は機械制御の安全関連部分にまで及び，もはやその使用は避けては通れない時代となりつつある。最近では，バスシステムの冗長化により，スタンドアロンのシステムだけでなくより大規模・広範囲に渡る安全制御のための情報をやり取りしようとする試みも始まっている。

このような新技術や新技法の乱立する状況の中で，IEC61508及び62061等の規格がようやく時代に追いついてまとまりつつある。ソフトウェアの安全性に関する論議は依然として残ってはいるが，安全性の評価指標の一つに危険側故障率を取り入れたり，冗長ダイバシティ構造や自己診断機能を重要なキーワードとして評価しており，この分野では事実上唯一の安全に関する規格として運用されることが期待されている。

今回調査した安全指向型のコントローラは多重化と自己診断機能に優れたものであり，高信頼化技術ではあるがシステム的にフェイルセーフ化を目指したアプローチを採っており，一般の高信頼性コントローラとは異なる設計思想を持っている。上記の規格案と照らし合わせても，本コントローラは現時点で最高の安全水準に到達しているものと思われる。しかし，安全性と信頼性の立場での評価の仕方や定量的評価のためのデータが不足しているなど，実際に本コントローラの認証を行った機関以外には具体的な評価が難しい。

今後は，従来からのフェイルセーフ技術と高信頼化技術との評価体系が統一され，合理的で理解しやすい評価が行われると予想される。特に，自己診断機能とダイナミック・フェイルセーフ技術とは，時間軸上の多重化という観点で体系化された評価が可能と思われ，より厳密で合理的な評価からさらに安全性を高める技術や手法が誕生することを期待する。

参考文献

1) ピルツ社, プログラマブル安全コントローラ（PSS3000, PSS3056）のカタログ
2) 三平他, PSDIに何が起こっているか, プレス技術, 35-10（1997）pp.116-121.
3) 山武ハネウェル社, セーフティ・マネージャー/フェールセーフ・コントローラのカタログ
4) 林, 安全性と稼働率向上を目指したコントロール・システム, 防災システム, 20-3/4 pp.12-15.
5) Triconex社資料, A Common Sense Approach to Safety Systems

（平成10年7月22日受理）