C-18 単一CPUによるフェールセーフ計算機の開発

Development of the fail-safe computer by single CPU

神宮 雅昭† 高橋 聖† 中村 英夫†
Masaaki Jingu Sei Takahashi Hideo Nakamura

1．まえがき

安全性が重視される産業用計算機は、故障時に必ず安全側に遷移するフェールセーフ（FS）性が要求される。本発表では、経済性を配慮して開発した、単一 CPU による FS 計算機の概念を紹介し、筆者らが開発している M 系列を用いた診断機構を述べる。さらに、シミュレーションを用いて行った有効性検証結果について報告する。

2．既存の FS 照合回路の特徴

計算機の FS 化は

(1) ＣＰＵのデザイン故障
(2) ＣＰＵの偶発故障
(3) ＣＰＵ以外のハードウェアの偶発的故障
(4) 電源やノイズ等の外乱による一過性故障
(5) ソフトウェアのバグ
(6) ソフトウェア仕様のミスマッチ

といった障害に対し安全性を確保する機構を組み込むことが要求されるが、「従来、処理の異常を外部に伝達する機構として WDT の組み込みがあった。しかし、WDT は単なる交番信号であり、デッドロックやオーバー負荷にはなっていないということは伝達できても、処理そのものの正当性を保障するものではない。」という問題があった。筆者らは、ソフトウェアのコピーモジュールを再度実行させ比較することで処理の正当性を検証する方法を取ることとした。しかも、このモジュールの照合の都度各モジュールに対応して割り当てられたデータを出力することで、各モジュールのスケジューリング(切り替え）が正常かつ処理結果の照合が全て OK のときに M 系列のデータが生成されるようにした。モジュール相互の照合はソフトウェアに委ねることとしたが、この部分は入念な設計と徹底した試験により高信頼度を保障する。なお、この照合部を準カーネルと呼ぶ。筆者らはコスト低減を意図し、単一 CPU による FS 化を検討してきた。

3．単一 CPU による FS 計算機の概念

筆者らが提案する単一系 FS 計算機は、図 1 に示すようにソフトウェアに two copy programming の概念を用い、外部に safety function としての安全関連ブロックを有する。ハードウェアには汎用の単一系 CPU を用いる。安全関連ブロックは、アプリケーションの論理からは独立であり、単一系計算機（計算機本体）の安全性検証のみを目的としている。ただし、安全関連ブロックによる診断は、内部の two copy programming と協調し、アプリケーションプログラムの正常な動作検証もできる。

ソフトウェアの動作は、入出力時に行われる入出力ポート診断と、一定周期で実行される CPU 機能のテスト処理、さらにアプリケーションのモジュール実行時に、異なるメモリに格納された同一処理ルーチンの二重実行を行うこととし、これらが一連の処理の基本動作となる。このうち、入出力ポート診断や、メモリ診断を含めた CPU 機能のテストは、アプリケーションによらず共通なものであるため、準カーネルとして用意されている。

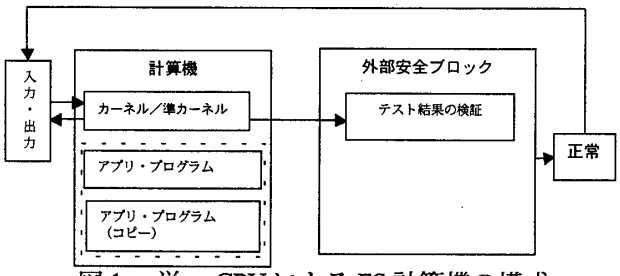

図 1 単一 CPU による FS 計算機の構成

準カーネルの機能として重要なものは、two copy programming モジュール（タスク）の管理と FS 化された入出力、そして CPU の健全性のチェックである。また、準カーネルの処理が一定周期で行われることのチェックについても、外部安全関連ブロックで行う。

また、準カーネルの起動応答のみが繰り返されるような異常状態が発生した場合には、この概念で安全性を保証することはできない。例えば、起動応答出力をした後 HALT するような処理に書き換えられたとするなら、割込レベルの高い準カーネルのみが割込周期で起動応答を行うことになり、アプリケーションは起動されない。もちろん CPU 診断やタスク管理も起動されない。従って、起動監視がウォッチドグタイマのような一定周期での起動をチェックするものであれば、FS コンピュータの要件を満足し得ない。

準カーネルのチェックポイントから固有のデータを出させ、このシーケンスが例えば最大周期シフトレジスタ系列（M 系列）になるようにすると、外部では振り子回路でシリアルに照合できる。

ただし、ここで用いる準カーネルのゴールド性が問題になる。筆者らは、「準カーネルは、よく検査されたソフトウェアルーチンであり、ハード的な故

障以外にはこの機能を全面的に信用してよいという立場」を取ることとした。

この概念の立場に立つと、どうしても外部でなければならないという機能は、準カーネルの起動監視のみになる。

次にM系列を用いた診断機構について述べる。

4．M系列を用いた診断機構

準カーネルは各チェックポイントにおいて、対応するモジュールの照合が合格したときに、あらかじめ埋め込まれているデータを読み出し、外部安全ブロックのバッファに書き込む。バッファはパラレルインシリアルアウトレジスタ(PSR)で、書き込まれるとそのビット数だけ押し出しが行われる。一方、外部安全ブロックには PSR の他に線形帰還シフトレジスタ(LFSR)からなる M 系列生成器と振り子回路が配置され、PSR の出力と LFSR の出力が振り子回路で照合される。なお、回路はチェックポイントを９箇所とし、一回のチェックポイントで７ビットのデータを出力することを想定しており、合計 63 ビットのM系列符号が生成されるとしている。

5．診断機構の作成と検証

M 系列を用いた診断機構を FPGA で構成し、有効性をシミュレーションで検出した。シミュレーションには、ターゲット計算機としてチェックポイント同期で M 系列を出力するモジュールを用いることとした。

図２にシミュレーションの構成と M 系列生成回路を示す。

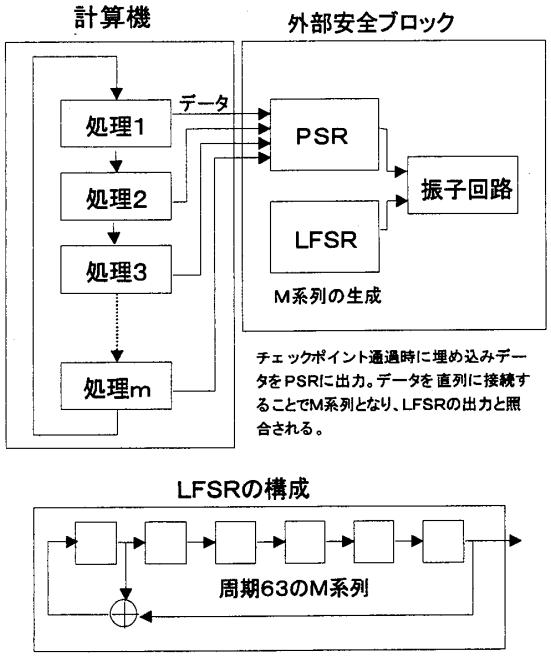

図２　M系列を用いた診断機構

シミュレーションによる検証の結果、外部安全ブロックが確実に不一致を検出することが確認された。（図３、図４）

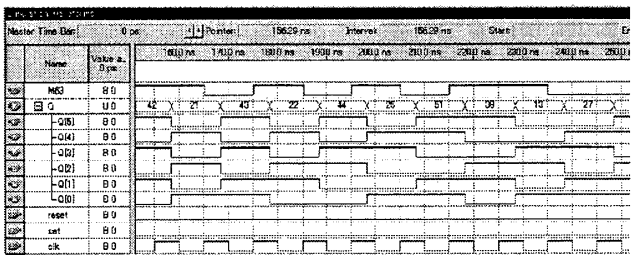

図３　M系列を用いた診断機構シミュレーション

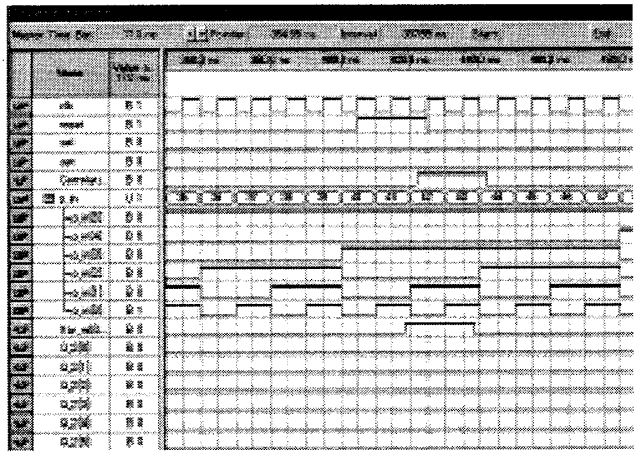

図４　M系列を用いた診断機構シミュレーション

6．まとめ

単一ＣＰＵによる FS コンピュータの開発に必要な、診断回路についてM系列を用いた診断機構を、紹介した。今後は、実際のアプリケーションに組み込み有効性を確認する予定である。

参考文献

[1]　数野・中村・山本・西牧・角山：「単一系コンピュータの高安全化手法」，信頼性学会誌 '99vol.21

[2]　中村・高橋：「鉄道信号用フェールセーフ計算機に関する考察」，信学技報　FTS2001-76 (2001-12)