単一故障に対してフォールトトレラントなフェールセーフCPUの開発

小川　泰生*　（日本信号株式会社）
中村　英夫　（日本大学）

Development of fault-tolerant fail-safe CPU for a single failure.

Yasuo Ogawa*, (The Nippon Signal CO.,LTD)
Hideo Nakamura, (Nihon University)

キーワード：安全性，信頼性，フェールセーフ，フォールトトレラント
(safety, reliability, fail-safe, fault-tolerant)

1. 概要

高度な安全性が要求される鉄道信号保安装置には，バス同期2重系方式のフェールセーフコンピュータシステムが多用されている。これは，CPUの動作クロックごとにCPUのデータバスをフェールセーフ（FS）バス照合回路で比較し，不一致時には安全側に遷移させることでフェールセーフを実現している。この方式は，一過性のノイズや，素子故障による誤りは確実に検出し，安全性を保証するものの，機器故障として鉄道の運転阻害につながる問題がある。事業者によっては，予備系を備えることで稼働率を向上させているが，コスト増等の問題がある。本発表は，シングルチップのFPGA内に3個のCPUを搭載し，故障発生時に自動的に系の再構成を行うことで，単一故障に対してフォールトトレラントな構成を実現するものである。

2. 従来の技術

電子連動装置を例に，CPUの構成と冗長化，フェールセーフ実現手法について述べる。

1985年に実用化されたI型電子連動装置SMILEでは，3つのCPUをクロックレベルで完全に同期して動作させ，CPUのデータバスに対して多数決照合を行っている。この方式では，3つのうち1つが故障した場合においても残った2つの系が一致していれば動作を続けることができるが，ハードウェア量が多くなる問題があった。

このため，II型電子連動装置以降は，2つのCPUで構成されるバス同期2重系構成が主流となった。この中のFSバス照合回路は，A/B系CPUが正常に動作している場合，交番信号を出力し，リレードライバによって正常リレーを動作させている。この方式では，1箇所でも故障すると，システムが停止してしまう。このため，稼働率を向上させるには予備系を持つなどの冗長化が必要とされた。

近年では，バス同期2重系フェールセーフCPUをシングルチップFPGA上にて実現する方式が開発され，実用化されている(図1)。

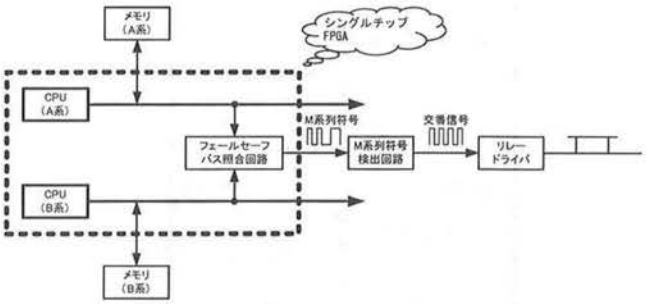

図1　FPGAによるバス同期2重系フェールセーフCPU構成

シングルチップ化の実現においては，クロック信号線などが照合出力ラインに混信し，バス不一致時にも交番信号が停止しないといった危険側への障害が懸念される。このため，2つのCPUが正常に動作している場合，ある定められたパターン（擬似ランダム信号）を出力し，外部で診断できる構成としたFSバス照合回路を開発した。擬似ランダム信号には，M系列符号を用い，FPGA外部に擬似ランダム信号を検査する回路を設け，正常である場合にだけ交番信号出力を出力するような構成としている。

3. 基本構成

シングルチップバス同期2重系フェールセーフCPUは，回路規模の縮小化と部品点数削減による高信頼化を達成し，広く用いられることとなった。しかし，上述したように故障時を想定した冗長化が必要となる問題があった。筆者らは，フェールセーフ性を確保しつつ信頼性を高めるため，シングルチップに3個のCPUを搭載することで高信頼化を実現する手法を開発した。その基本構成について説明する。

FPGA内に3つのCPUとメモリを配置し，それぞれをA系，B系，C系と呼ぶことにする。A系，B系については，バス同期2重系CPU構成のA系・B系と同等である。C系は高信頼化を意図して新たに追加する予備系で，A系またはB系のCPUあるいはメモリなどが故障した時に用いられる。FPGA内には3つのCPU相互のCPUデータバス（A

系 CPU データバス，B 系 CPU データバス，C 系 CPU データバス）を比較する回路（比較回路①／②／③）を設ける。これらの比較回路は，後述するバス切替回路（A 系切替回路，B 系切替回路）を制御するために用いる。バス切替回路は，C 系 CPU データバスを A 系データバスまたは，B 系データバスに接続するためのものである。3 つの CPU に接続されているバスは，初期状態では，A 系と B 系の CPU が FS バス照合回路に接続されている。一方，C 系は，A 系／B 系と同一クロックにより同期動作をしているものの FS バス照合回路には接続されていない（図 2）。

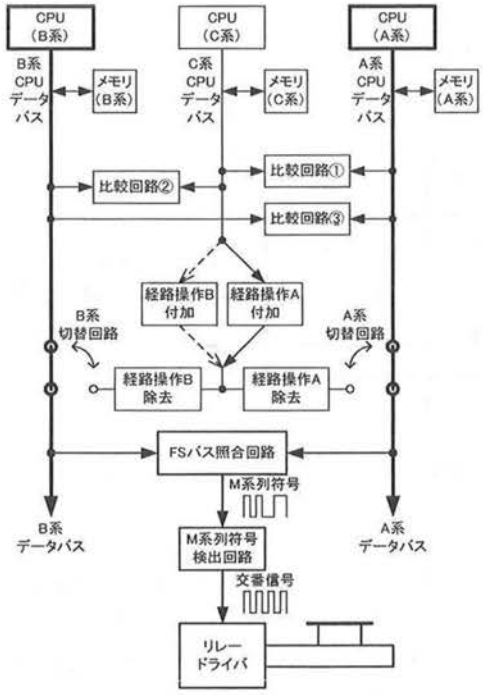

図 2　バス同期 3 重系切替方式フェールセーフ CPU 構成

4. 基本動作

次に，A 系メモリにて故障が発生した場合の基本的な動作を説明する。A 系 CPU データバスに異常データが乗るため，比較回路①／③でデータ不一致を検出する。このとき，比較回路②がデータ一致を示していれば，これらの結果を A 系切替回路，B 系切替回路の切替条件として使用することで，C 系 CPU が，A 系 CPU の代わりになるようバス切替回路を切り替える(図 3)。A 系の代わりにする場合には，経路操作 A を施し，A 系切替回路の手前で付加した経路操作 A 除去を行い，A 系データバスから FS 照合回路に入力する。

この切り替えは，FS バス照合回路にデータが入力される前にハードウェアにて実施するため，動作を停止させることなく，切り替えを行うことが可能である。その後は，C 系と B 系を新たな動作系として，動作を継続する。さらに新しい動作系にて故障が発生した場合には，FS バス照合回路にてデータの不一致を検出し，システムを停止する。

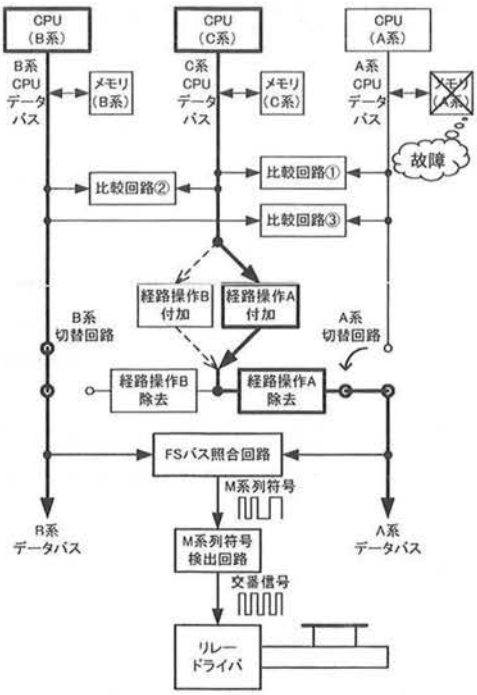

図 3　A 系 CPU またはメモリ故障時動作

5. 安全性と信頼性

シングルチップ上にバス同期 2 重系を構成する 2 つの CPU と FS バス照合回路を搭載するための手法として実績を積んできた「照合出力に擬似ランダム信号を用いる方式」を採用し，安全性は従来と同等レベルを確保する。但し，単一故障発生時には，即時システム停止しないことから，保全性を考慮し，単一故障で動作していることを通知する表示もしくは伝達する機能を搭載する。また，信頼性については，3 つの CPU あるいはメモリなどのうち，いずれか 1 箇所の故障が発生した際に，バス切替回路によって，正常動作している 2 つを新たな動作系として，FS バス照合回路に接続し，外部とのインタフェースを行うものである。これにより，単一故障による即時システム停止となる事象が減少し，稼働率の向上が見込める。

6. おわりに

単一故障に対してフォールトトレラントなフェールセーフ CPU として，3 重系切り替え方式の基本コンセプトを確立した。現在，CPU ユニットとして開発中であり，性能評価ののち，各種装置に展開していく予定である。

文　献

(1)　日本鉄道電気技術協会：「信号概論 連動装置」
(2)　シングルチップフェールセーフ RISC-CPU ボードの開発，日本信号技報 Vol.27 No.1