LC-4 シングルチップフェールセーフプロセッサの開発と安全性検証
Development and Safety Verification of a Single-chip Fail-safe Processor

高橋 聖† 平 宗久‡ 三枝 秀隆‡ 星野 武彦‡ 中村 英夫†
Sei Takahashi Munehisa Taira Hidetaka Saegusa Takehiko Hoshino Hideo Nakamura

1 まえがき

日本の鉄道信号保安装置では，バス同期式と呼ばれるフェールセーフ（FS）コンピュータシステムが用いられている [1]. 本論文では，バス同期式 FS コンピュータのシングルチップ化について報告する.

従来のバス同期式 FS コンピュータにおいて独立のチップの冗長構成であったものを一つの LSI に組み込むには，共通モード故障に対する対策が必要となる．筆者らは，内部の故障診断に M 系列符号語出力を利用するなどの新たな概念を導入し，フェールセーフ化を図った.

2 バス同期式フェールセーフコンピュータの概要

図 1 にバス同期式 FS コンピュータの構成を示す．バス同期式 FS コンピュータではフェールセーフ照合回路が診断の核となる．フェールセーフ照合回路は，バスに挿入され，バスデータを常時照合することで誤りを検出する回路であり，図 2 に示すように 2 線式検査回路（code-disjoint combinational circuit: CCC）と誤り表示回路（error indication circuit: EIC）によって構成されている．バスに挿入する検査回路が具備すべき性質としては，回路自身が totally self checking（TSC）[2] であることと code disjoint（CD）性を満足することであり，2 線式検査回路はこれらの条件を満足しているものとして知られている [3].

この検査回路は，非符号語が与えられた場合には必ず非符号語を出力するが，再び符号語が入力されると出力も符号語に戻る．したがって，誤りが発生したことを後段の回路で確実に検知し記憶するためには，何らかの仕組みが必要となる．このために設ける回路が誤り表示回路である.

3 FS プロセッサのシングルチップ化

今回開発する FS プロセッサには，従来のバス同期式 FS コンピュータを構成する二つのプロセッサ（MPU）及び照合回路を一つの LSI に組み込む.

3.1 照合回路において配慮すべき事項

従来のバス同期式 FS コンピュータでは，正常時の照合回路出力を交番信号とし，不一致発生時や，比較回路，誤り表示回路の故障時には出力が固定されることでフェールセーフ性を確保してきた．しかし，今回は一つの LSI の中に二つの MPU と，検査回路及び誤り表示回路により構成される照合回路のすべてを組み込むため，次の事項に対する配慮が必要となる.

†日本大学理工学部電子情報工学科
‡日本信号株式会社

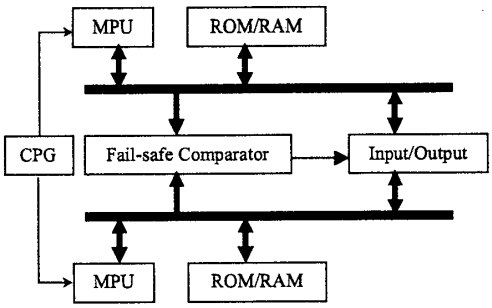

図 1: バス同期式 FS コンピュータの構成

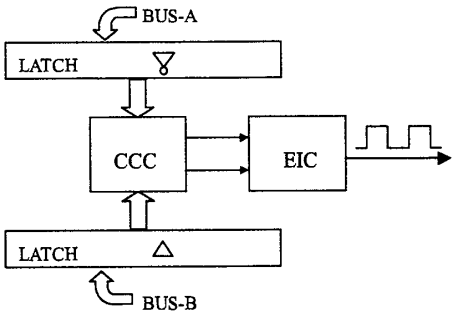

図 2: フェールセーフ照合回路の構成

1. 照合処理起動に対するセルフチェック機構
2. クロック信号等配線のショートによる偽交番出力の防止

照合処理の開始は，バス上にデータが出力されたタイミングとなる．しかし，プロセッサは二つであるから，このタイミング信号はいずれか一方の MPU からの信号を用いる．この結果，万一そのプロセッサからの信号が read（write）信号でしか生成されなければ，write（read）時に発生したバス上の不一致を見逃す恐れがある．したがって，このような故障を検出するセルフチェック機構の組み込みが要求される．また，内部クロック信号が照合回路の出力信号と混信した場合にも，外部で検知できる機構の組み込みが要求される.

3.2 M 系列擬似ランダム符号による診断機構

従来の照合回路においては，正常時には確実に交番信号が得られるように，それぞれのプロセッサから生成される照合ビットに，パーミュタと呼ばれる機構によるパーミュテーション操作を施していた [4]. 図 3 に示すように，2 線式検査回路の正規入力符号語空間は，検査出力が（1,0）となる符号語サブ空間（奇空間）と，（0,1）となるような符号語サブ空間（偶空間）の二つに分けられる．従来のパーミュタは，ある期間，入力符号語が片方の符号語サブ空間内のものしか与えられなかった場合，その期間内は 2 線式検査回路の出力値が変化しないた

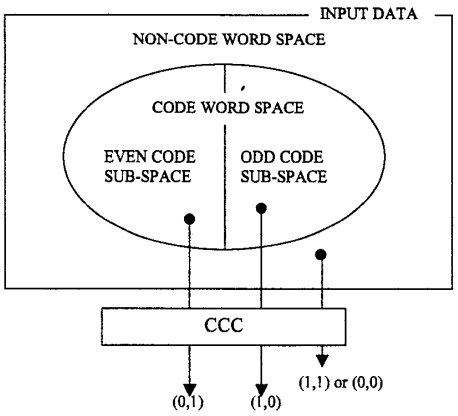

図 3: 符号検査回路に対する入力データ空間と符号サブ空間の概念

め，固定故障と判別できなくなることを懸念して考えられたものである．したがって，パーミュタ機構が作動していれば正常時には交番信号が得られ，異常時の固定出力との識別が可能であった．

しかし，不一致発生で交番出力が停止したとしても，比較出力信号線にクロック信号が混信していると，交番信号が得られる可能性があり，このパーミュタでは不一致を見逃すおそれがある．そこで，単なる交番信号の出力をもって正常とするのではなく，ある定められたビットパターンが出力されているときのみ正常とみなすことでより厳格な診断を実現することを考えた．この機構は，ノイズ等のコモンモードの外乱に対しても有効に作用することが期待できる．今回の検討では，定められたビットパターンとして，32 ビットの M 系列擬似ランダム（PN）符号語を用いることとした．

図 4 に今回提案する M 系列 PN 符号語を用いた FS 照合回路の構成を示す．検査回路の入力は一旦パリティチェック回路に分配され，パリティチェック回路の出力と PN 符号語生成器の排他的論理和出力により，最下位ビットがモディファイされる．その結果，生成される符号語も奇空間に属するものと偶空間に属するものが，PN 符号語生成器のビット配列と同期して切り替わり，2 線式検査回路の符号語入力として与えられることになる．また，照合起動のタイミング生成に関する問題について考えると，万一何らかの故障により，両系のタイミングがずれた場合には，PN 符号系列生成の同期が外れるため，非符号語が 2 線式検査回路に与えられることになる．

以上のように，回路が正常であり，かつ，二つのプロセッサの処理も正常に行われていた場合には，誤り表示回路（EIC）からの出力信号は M 系列の PN 符号語となる．この PN 符号語は既知であるから，外部に M 系列 PN 符号語検査回路を設けることによって，単なる交番信号と内部の正常性を保障する PN 符号語の識別ができる．

4 FPGA による FS プロセッサの実現と検証

上記バス同期式 FS プロセッサを FPGA により実現することとした．CPU コアは 32 ビット RISC プロセッサであり，β 版には機能試験を実施するために故障注入ブロックを組み込

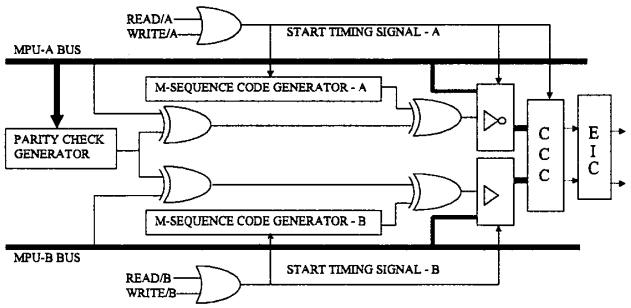

図 4: 提案する FS 照合回路の構成

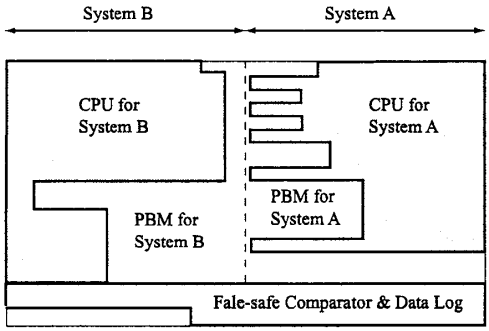

図 5: FPGA 内の回路配置

み，0/1 固定故障や反転モード故障，配線短絡故障など考え得る故障 675 件を順次発生させて挙動を評価した．この結果，誤り表示回路における A 系，B 系の配線短絡以外は所期の機能を満足することが確認された．この配線短絡に関しては，物理的に回路を分離することで対応させた（図 5 参照）．なお，これらの開発や評価は国際規格 IEC61508 および EN50126 の要件を遵守して行った．

5 むすび

バス同期式二重系 FS プロセッサをシングルチップ化することに成功した．FS 性に配慮し，従来の交番出力に代えて M 系列の符号語出力を正常出力とした．この結果，LSI 内部の配線短絡やコモンモード故障に対するテスト性が向上した．今後鉄道信号分野への利用を考えている．

参考文献

[1] 中村英夫，武子淳，“次世代運転制御システム CARAT 用マルチプロセッサシステムのディペンダブル設計，” 電学論 (D)，vol.114-D，no.5，pp.499–504，May 1994.

[2] D.A. Anderson and G. Metze, “Design of totally self-checking check circuits for m-out-of-n codes,” IEEE Trans. Comput., vol.C-22, no.3, pp.263–, March 1973.

[3] W.C. Carter, et al., “Error-free decoding for failure tolerant memories,” IEEE Int. Comp. Group Conf., 229, 1970.

[4] J.L.A. Hughes, et al., “Design of totally self-checking comparators with an arbitrary number of inputs,” FTC-13, pp.169–, 1983.