CC-001

汎用半導体によるフェールセーフ実現のための一提案

A proposal for realization of fail-safe using commercially off-the-shelf semiconductors

金川　信康†
Nobuyasu Kanekawa

1. はじめに

鉄道の安全を守るしくみであるフェールセーフ方式は，1999 年に制定された RAMS 規格 EN50126:1999，これを受けた国際規格 IEC62278:2002 に定められているが，EN50126:1999 制定以前からの各国の安全文化，歴史によるところが大きい。例えばフランスでは，VCP (Vital Coded Processing) [1]が LAAS (Laboratoire d'analyse et d'architectures des systèmes)の後押しもあり標準方式となっている。

近年になって，特殊なデバイスやをなるべく使用せずに汎用部品や FPGA (Field-Programmable Gate Array)を使って，これらのフェールセーフ方式を実現しようする動きがみられ、報告者らも FPGA によるフェールセーフ方式の実現方法[2]などを提案している。

そこで本研究では，特殊なフェールセーフ素子を用いずにフェールセーフ機能を実現する方法を提案し，欧州の標準方式である VCP 方式を例に説明する。

2. 汎用半導体によるフェールセーフ方式

2.1 VCP 方法とその課題，解決方法

先に述べた VCP 方式は，入力信号に冗長符号として剰余符号，実行されたオペレータの履歴を表す符号，そして時刻またはループ実行回数を表す符号を付加する方式で，演算結果に付加された冗長符号部を検査することにより入力信号に付加された剰余符号により情報処理過程における加算，乗算での誤りを検出でき，さらに実行されたオペレータの履歴を表す符号によりオペレータの誤りを検出でき，時刻またはループ実行回数を表す符号により条件分岐やループ制御における誤りを検出できる。

なおこの場合，入力信号に冗長符号を付加する回路，および演算結果を検査する回路は危険側故障を避けるためにフェールセーフ性が本来備わっている回路（原文では“Intrinsic Fail Safe”）とすることが必要である。現在までに様々な「フェールセーフ性が本来備わっている回路」が提案されている。例えば，リレーを用いたものや，トランスの巻き線を利用したもの，配線間隔や配線経路，配線層数などの特殊な設計制約や特殊な製造プロセスにより作られた半導体素子などが挙げられる。これらの回路は最新の半導体による論理回路と比べて寸法が大きなものであったり，動作速度が遅いものであったりすることが多く，製造方法や用途の特殊性から生産中止になりやすい可能性もある。そこで以上挙げた従来技術では，入力信号に冗長符号を付加する回路，および演算結果を検査する回路を最新の半導体による論理回路で実現可能にして小型化，高速化，さらには低コスト化，製造プロセスの汎用化を図るための更なる考慮が望ましい。

そこで本研究では，入力信号に冗長符号を付加する回路，および演算結果を検査する回路を最新の半導体による論理回路で実現可能にして小型化，高速化，さらには低コスト化，製造プロセスの汎用化を図ることを目的とする。

上記目的を達成するために本研究では以下の手段をとる。なお，Figure 1 (a)に従来の VCP 方式，(b)に提案方式，多重交互冗長符号化方式 (Multi-alternating redundant coding scheme)をそれぞれ示す。

(1) 入力信号に少なくとも 2 系列の冗長符号を時系列的に交互に付加する。（VCP 方式では 1 系統のみ）

(2) 入力信号の処理結果を少なくとも 1 系列の冗長符号の検査部で検査する。

(3) 上記検査部の出力が(1)の切り替えに同期して正常→異常→正常…と時系列的に交互に変化することをもって正常と判断する。（VCP 方式では時系列変化なし）

(4) さらに望ましくは，入力信号の処理結果を少なくとも 2 系列の冗長符号の検査部で検査する。（VCP 方式では 1 系列のみ）

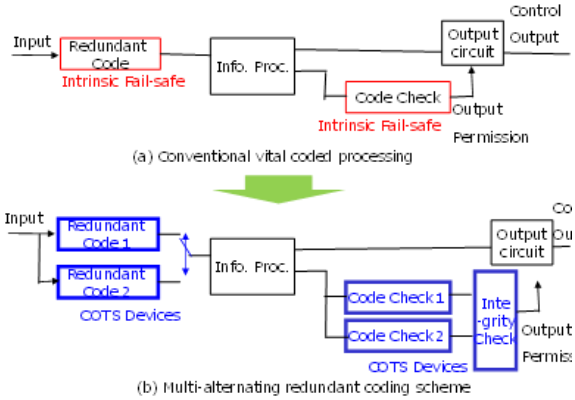

Figure 1 Conventional Vital Coded Processing and Proposed Architecture

手段(3)において，「正常」出力が得られることにより手段(1)のための冗長符号化部，手段(2)のための検査部，それらの間の情報処理部の動作の正常性を確認することができる。さらに，手段(3)において，「異常」出力が得られることにより手段(1)のための冗長符号化部の切り替え部，手段(2)のための検査部の異常検出能力が正常であることを確認することができる。従って，信号の入力から処理のための機能の正常性を確認できるだけでなく，正常と判断するための検査機能の正常性も同時に確認することができる。

なお，手段(3)において，「異常」出力が得られているときには，情報処理結果が正常であるという保証がないので

† 株式会社日立製作所, Hitachi, Ltd.,

情報処理結果を採用することができないため，情報処理結果が正常であるという保証を得るためには，手段(1)において同一の入力信号について時系列的に２系列の，即ち 2 度にわたって冗長符号を付加して情報処理を実行する必要がある。そこで手段(4)のように少なくとも２系列の冗長符号の検査部で検査することにより，一方の系列の冗長符号の検査部で「異常」出力が得られときにも，他方の系列の冗長符号の検査部で「正常」出力が得られるので，先に述べたような 2 度にわたって冗長符号を付加して情報処理を実行する必要がなくなり，処理性能を向上させることができる。なお，合理性チェック部で２系列の冗長符号の検査部での検査結果を総合的に判定して出力許可信号とする。

以上述べたような手段により，汎用半導体による回路であっても信号入力から処理のための機能の正常性を確認できるだけでなく，正常と判断するための検査機能の正常性も同時に確認することができる。

2.2 多重交互冗長符号化方式 (Multi-alternating redundant coding scheme)

多重交互冗長符号化方式の基本的な構成は Figure 1 (b)の通りである。

入力信号は冗長符号化部１および冗長符号化部２に入力され，それらの冗長符号化部の出力は切り替え部により時系列的に交互に切り替えられる。冗長符号部で付加する冗長符号は従来技術に基づくものでよい。例えば，最も簡単なものでは偶数，奇数パリティ，それぞれ法（入力数値を除算する数値）が異なる剰余符号や，生成多項式が異なる冗長符号とすることが考えられる。また VCP 方式では，剰余符号，実行されたオペレータの履歴を表す符号，そして時刻またはループ実行回数を表す符号の一部または全部を異なる系列とすることが考えられる。例えば，時刻を表す符号として異なる系列の疑似乱数を用いることが考えられる。なお，冗長符号の誤り検出能力は一般に，２－ｎ（ｎ：冗長ビットの数）とあらわされるため，１ビットだけのパリティよりはより多くのビットを付加した冗長符号の方の検出能力が高まることは勿論のことである。

情報処理部では冗長符号化された入力信号を装置の目的を達成するために予め定められたアルゴリズムに基づき処理を実行しその結果を冗長符号検査部１と冗長符号検査部２，出力回路部に出力する。合理性チェック部は，冗長符号検査部１と冗長符号検査部２が切り替え部での切り替えに同期して互い違いに，かつ時系列的に正常，異常出力を繰り返したときに正常と判断して出力許可信号を出力して，出力回路部は合理性チェック部から出力許可信号が出力されているときに制御出力を出力する。

Figure 2～4 にセルフチェッキング演算回路の動作を情報処理部における情報処理を入力から出力への写像として説明する。

セルフチェッキング演算回路では Figure 2 に示すように入力に冗長符号が付加され，情報処理（演算）される。この際，情報処理の過程でその符号規則が保たれる冗長符号を用いれば，情報処理結果が冗長符号の符号規則に則っている（符号語）か否（非符号語）かをチェックすることで情報処理の過程での誤りを検出することができる。例えば，符号語である入力 x1 が正常に情報処理された場合には結果として符号語である出力 y1 が得られる。万一情報処理の過程で何らかの誤りが生じた場合には確率（$1-2^{-n}$，但し，*n*: 冗長ビット数）で非符号語の出力 y1**となり，不正な符号語の出力 y1*となる確率は 2^{-n} となる。ここで VCP 方式の場合，n＝40 程度であり，極めて高い確率で非符号語の出力 y1**となり，不正な符号語の出力 y1*となる確率は極めて低い。以上のようにして，情報処理の過程でその符号規則が保たれる冗長符号を入力し，情報処理結果である出力が符号語か否かをチェックすることにより情報処理の過程での誤りの発生を検出することができる。

また，入力への冗長符号付加の過程に誤りがあった場合には，非符号語の入力 x2 が与えられ，その演算結果として非符号語の出力 y2 が得られる。このとき情報処理の過程で何らかの誤りが発生した場合に不正な符号語 y2*となる確率も同様に 2^{-n} と極めて低い。

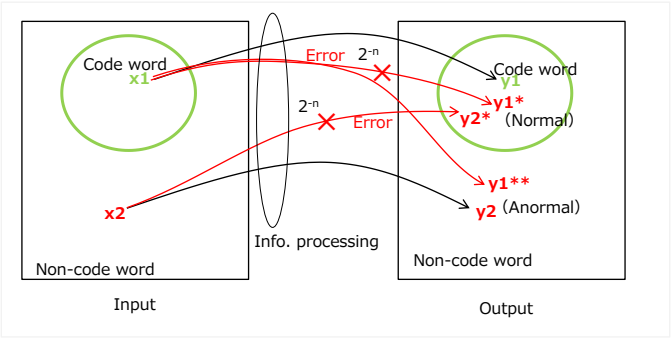

Figure 2 Interpretation of the Self-checking operation as a mapping from input to output

続いて，Figure 3 (b)に示す提案方式の動作を同様に Figure 3～5 に示す。

Figure 3 に示すように冗長符号化部１，２では入力信号に系列１，２の異なる冗長符号を付加して切り替え部によって時系列に交互に切り替えられる。このとき，情報処理部が正常な場合には，系列１の冗長符号を付加された入力信号 x1 は情報処理部における情報処理により系列１の冗長符号の符号語 y1 に変換され，系列２の冗長符号を付加された入力信号 x2 も同様に情報処理部における情報処理により系列２の冗長符号の符号語 y2 に変換される。

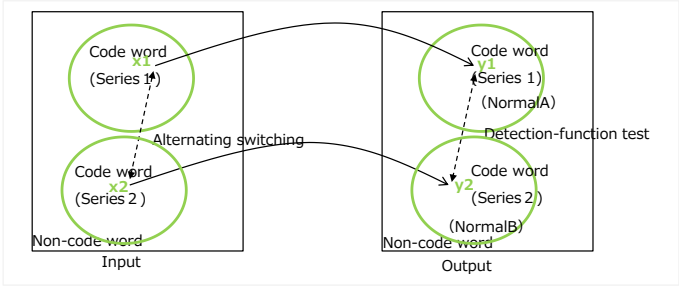

Figure 3 Operation in the Multi-alternating redundant coding scheme

ここで，情報処理部で異常が発生した場合には情報処理結果として符号語出力が得られなくなるので，処理結果を冗長符号検査部１と冗長符号検査部２で検査することに

より情報処理部の異常を検出することができる。また，冗長符号化部１および冗長符号化部２，切り替え部で異常が発生した時も同様に情報処理結果として符号語出力が得られなくなるので，処理結果を冗長符号検査部１と冗長符号検査部２で検査することにより冗長符号化部１および冗長符号化部２，切り替え部の異常を検出することができる。

続いて，Figure 4 に冗長符号検査部１の動作，Figure 5 に冗長符号検査部２の動作を示す。Figure 4 に示すように冗長符号検査部１は冗長符号化部１により符号化された入力 x1 に基づく情報処理結果 y1 は符号語と見なし，冗長符号化部２により符号化された入力 x2 に基づく情報処理結果 y2 は非符号語と見なすために，切り替え部により x1，x2 を時系列的に交互に切り替えられることにより，正常，異常の出力を交互に繰り返すことになる。その結果，正常と判定する機能だけでなく異常と判定する機能も常時確認できるだけでなく出力の H,L 固定故障も検出することができる。

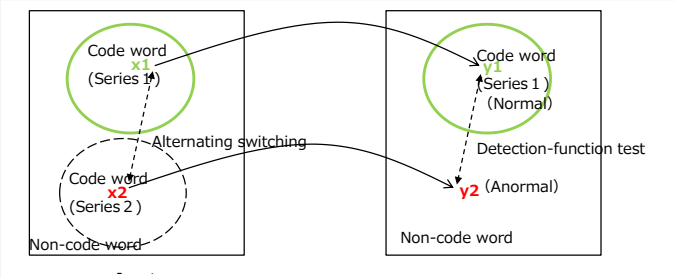

Figure 4 Operation of the Code Checker 1

同様に Figure 5 に示すように冗長符号検査部２は冗長符号化部１により符号化された入力 x1 に基づく情報処理結果 y1 は非符号語と見なし，冗長符号化部２により符号化された入力 x2 に基づく情報処理結果 y2 は符号語と見なすために，切り替え部により x1，x2 を時系列的に交互に切り替えられることにより，正常，異常の出力を交互に繰り返すことになる。その結果，正常と判定する機能だけでなく異常と判定する機能も常時確認できるだけでなく出力の H,L 固定故障も検出することができる。

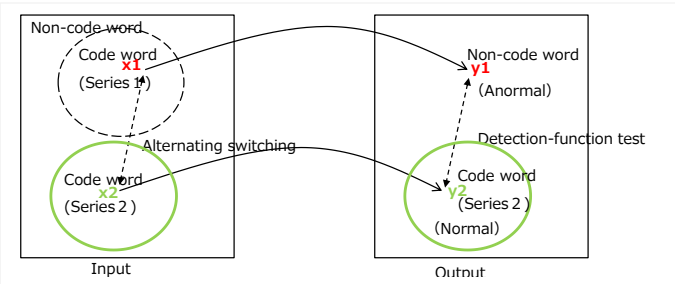

Figure 5 Operation of the Code Checker 2

本方式の正常時の動作波形を Figure 6 に示す。切り替え部からは符号系列１による入力と符号系列２による入力（図中ハッチングで示す）が交互に出力される。その結果，情報処理部のからも符号系列１による出力と符号系列２による出力（図中ハッチングで示す）が交互に出力される。情報処理部のからの信号が入力される冗長符号検査部１，冗長符号検査部２は Figure 6 に示すように時系列的に交互に，互い違いに正常，異常を示す信号を出力する。合理性チェック部では，冗長符号検査部１，冗長符号検査部２から時系列的に交互に，互い違いに正常，異常を示す信号が出力されたときにのみ正常と見なして合理性チェック部も交番信号を出力する。

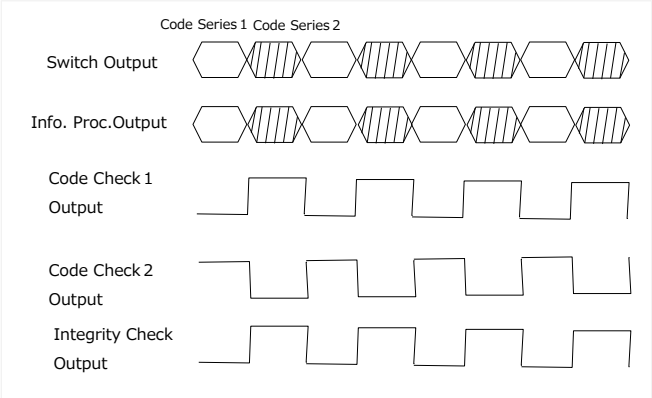

Figure 6 Operation waveforms (Normal)

ここで，Figure 7 に示すように情報処理部において異常（X）が発生した場合には，冗長符号検査部１，冗長符号検査部２のいずれかで異常が検出されて，合理性チェック部は交番信号の出力を停止する。

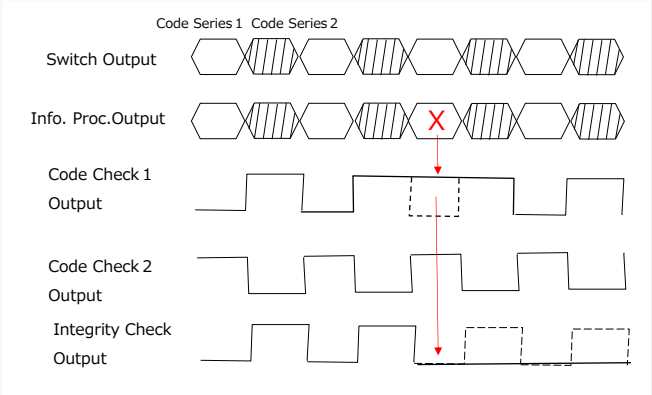

Figure 7 Operation waveforms (Anomaly in Info. Proc.)

続いて，冗長符号化部１または切り替え部で異常が発生した場合には，Figure 8 に示すように異常（X）は切り替え部の出力から情報処理部の出力に伝搬し，冗長符号検査部１，冗長符号検査部２のいずれかで異常が検出されて，合理性チェック部は交番信号の出力を停止する。これは冗長符号化部１で異常が発生した場合も同様に検出可能であることは言うまでもない。

次に切り替え部の固着故障（X）で冗長符号検査部２の出力から冗長符号検査部１の出力に切り替えられなくなった場合も，Figure 9 に示すように切り替え部は本来冗長符号検査部１の出力であるべき時に冗長符号検査部２の出力となり，情報処理部の出力も来冗長符号検査部１の出力に基づく出力であるべき時に冗長符号検査部２の出力に基づく出力となり，冗長符号検査部１，冗長符号検査部２で異常が検出されて，合理性チェック部は交番信号の出力を停止する。

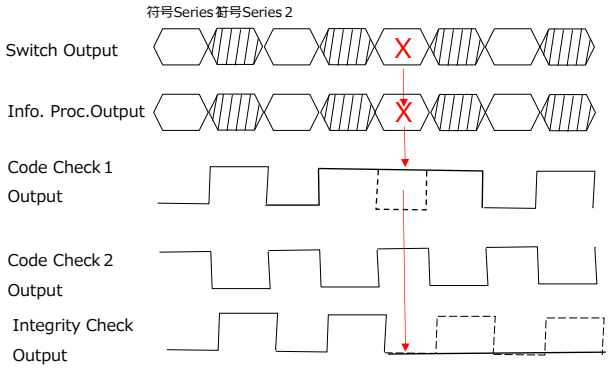

Figure 8　Operation waveforms (Anomaly in Code)

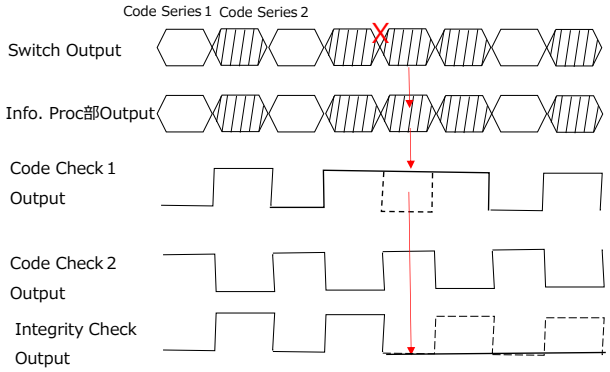

Figure 9　Operation waveforms (Anomaly in Switch)

また，Figure 10 に示すように，冗長符号検査部２で異常（X）が発生した場合には，合理性チェック部は交番信号の出力を停止する。なお，冗長符号検査部１で異常が発生した場合も，合理性チェック部は交番信号の出力を停止して異常を検出できる。

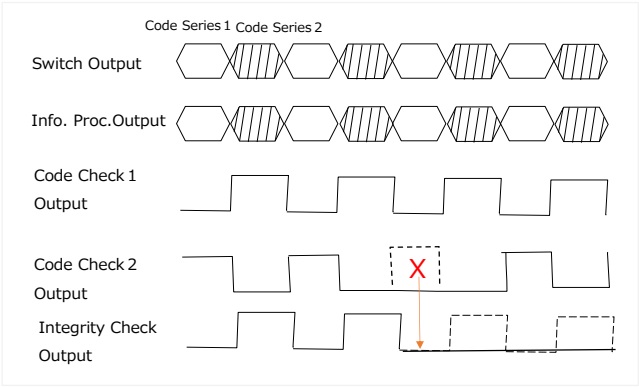

Figure 10　Operation waveforms (Anomaly in Code Checker 2)

以上述べたように本方式によれば，システムを構成する冗長符号化部１，冗長符号化部２，切り替え部，情報処理部，冗長符号検査部１，第の冗長符号検査部２のいずれかで異常が発生しても，合理性チェック部は交番信号の出力を停止し，異常を検出することができる。

本方式を用いた高安全制御システムの構成を Figure 11 に示す。出力回路からの制御出力はリレーを駆動する。なおこのとき，出力回路は最終段にフェールセーフアンプを用いるのが H,L 固着故障による誤動作も起こりにくい構成となるので望ましい

リレーが駆動されている（扛上している）間は車輪を制動するブレーキは動作せず，リレーが駆動されずに落下した場合には車輪を制動するブレーキが動作する。または，リレーが駆動されている（扛上している）間は加速動作を許可し，リレーが駆動されずに落下した場合には加速動作を許可しない。

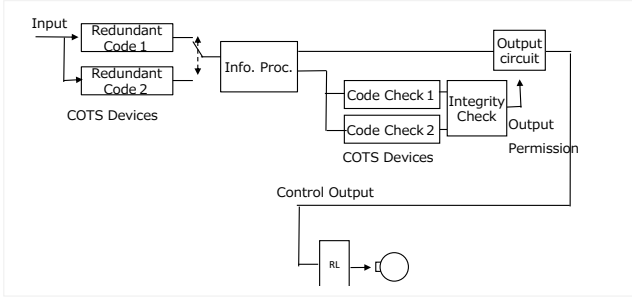

Figure 11　Safety Control System

以上、欧州の標準方式である VCP 方式を例に説明したが、本提案方式は広く高安全装置に応用が可能である。

3. おわりに

本報告では，特殊なフェールセーフ素子を用いずにフェールセーフ機能を実現する方法を提案し，欧州の標準方式である VCP 方式を例に説明した。

本方式では，入力信号に系列１，２の異なる冗長符号を付加して切り替え部によって時系列に交互に切り替えることにより，冗長符号の検査部からは「正常」，「異常」を示す出力が交互に得られる。検査部から「正常」出力が得られることにより冗長符号化部，検査部，それらの間の情報処理部の動作の正常性を確認することができる。さらに，検査部から「異常」出力が得られることにより冗長符号化部の切り替え部，検査部の異常検出能力が正常であることを確認することができる。

さらに望ましくは，入力信号の処理結果を少なくとも２系列の冗長符号の検査部で検査することにより，一方の系列の冗長符号の検査部で「異常」出力が得られときにも，他方の系列の冗長符号の検査部で「正常」出力が得られるので，先に述べたような 2 度にわたって冗長符号を付加して情報処理を実行する必要がなくなり，処理性能を向上させることができる。

参考文献

[1] Forin P. (Matra Transport, Montrouge, FRA), Vital coded microprocessor principles and application for various transit systems, IFAC-CCCT'90, Vol.23, Issue 2, pp.79-84 (1990)

[2] Y. Kanno, T. Toba, K. Shimamura and N. Kanekawa, "Design Method for Online Totally Self-Checking Comparators Implementable on FPGAs," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 3, pp. 726-735, March 2020