C-018

n-フォールトトレラントシステムの提案

A Construction Method of a Fault Tolerant Voter for N-Modular Redundancy

岩井 仁司†
Hitoshi IWAI

1．まえがき

本論文では、n 個の故障を、多重化多数決冗長系で多数決回路も含めてマスクする方法を提案する。同じ処理をする機能ユニットを複数個並べて、それらの出力を多数決回路で多数決する方式は、NMR (N-Modular Redundancy) と呼ばれている。従来の方法では、多数決回路の故障に対しては、多数決回路を多重化する方法が知られているが、結局、多数決回路の多数決を行う回路が必要になり、根本的な解決にならない[1]。この問題は、多数決回路の出力が 1 故障で誤りになる、という制約から由来している。

故障があっても、なお正しい信号を出力できる多数決回路があれば、多数決回路の故障をもマスクする方法がある。スイッチのみから構成される多数決スイッチ回路を NMR に適用し、多数決回路の故障を含めて、マスクする方法を提案する。

2．課題を解決するための工夫点と効果

従来、多数決回路を AND ゲートや OR ゲートで構成することを考えられていた。その回路は図 1 のようなものである。しかし、図 2 のようにスイッチのみでも多数決回路を構成でき、素子(スイッチ)の 1 故障によっても、多重化ユニットの出力信号 A,B,C にエラーがなければ、正常のままである。

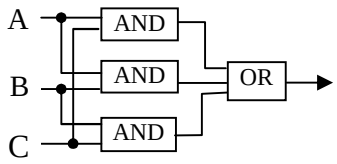


図 1 一般的な多数決回路

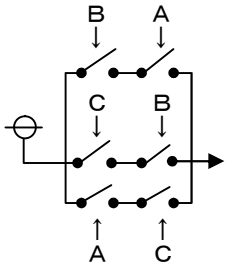


図2 多数決スイッチ回路

3. ２故障許容の検討

提案の構成では、図 2 のような多数決スイッチ回路を各多重化機能ユニットの電源 On/Off 制御に適用し、各機能ユニットから互いに制御し合い、故障発生時に当該機能ユニットを多数決で電源 OFF する。

具体的に、２故障のフォールトトレラントの例を図 3 に示す。ここで、2 故障を多数決でマスクするために必要な多重化機能ユニット数は４としている。即ち、１故障目は４つの機能ユニットの多数決で検出後、分離し、２故障目は残った３つの機能ユニットで検出できるからである。ここでは、複数の機能ユニットが同時に同じ症状で故障しないと仮定している。

†神奈川県鎌倉市在住

（１）構成
構成について、説明する。

①多重化機能ユニットは 4 つ。
②各多重化機能ユニットは多数決スイッチを具備する。
(多数決スイッチ回路は､自分以外の 3 つの機能ユニットの多数決で OFF できるように接続する。)

（２）動作
次に、動作について説明する。

①各機能ユニット内の CPU は出力データを生成し、得られた出力データに、符号を付加する。
②CPU どうしが、符号つきで出力データを交換する。
③自分の出力データと他機能ユニットの CPU の出力データと比較して間違っていれば相手の電源スイッチ OFF 指令を出す。
④多数決スイッチ回路では、2 個または 3 個の CPU から OFF 指令が出力されると、当該多数決スイッチ回路全体では、電源 OFF になる。
⑤多数決で OFF された CPU の、他 CPU 電源スイッチ制御信号は、必然的に Low に落ちる。各多数決スイッチ回路では、Low は ON 指令として扱う。これにより、一旦故障として OFF された CPU は、自動的に投票者から外れていく。

（３）故障耐性の検討
2 個の CPU から OFF 指令が出力される時は、機能ユニットが 2 個故障した場合であり、検討の条件としては、さらなる故障は、想定しなくてよい。3 個の CPU から OFF 指令が出力される時は、その機能ユニットが故障した場合である。この時、多数決スイッチ回路の 1 つのスイッチが ON 故障または OFF 故障していても、当該機能ユニットは、期待通り OFF され、システムから分離される。

機能ユニットが故障せず、多数決スイッチ回路のスイッチが 2 故障した場合は、いずれの機能ユニットも OFF されることなく、符号付きの正しい出力データを得ることができる。

一時的なソフトエラーに対して、MTBF 等の評価指標の悪化を防ぎたい場合は、CPU は自分の出力データと他機能ユニットの出力データと比較照合して一致しない時、直ちに相手の電源を OFF せずある期間待って、一方で自分以外の複数の機能ユニットの出力データが一致するのであれば、それら機能ユニットから処理に必要なデータを送ってもらって、自分のデータを更新することにより、ソフトエラーを修正してしまう方法が考えられる。

（４）応用
故障が発生しても検知できない場合は、初期には故障耐性があっても、突然サービスに障害が発生してしまうことが考えられる。このため、故障をカウントできることが重要である。

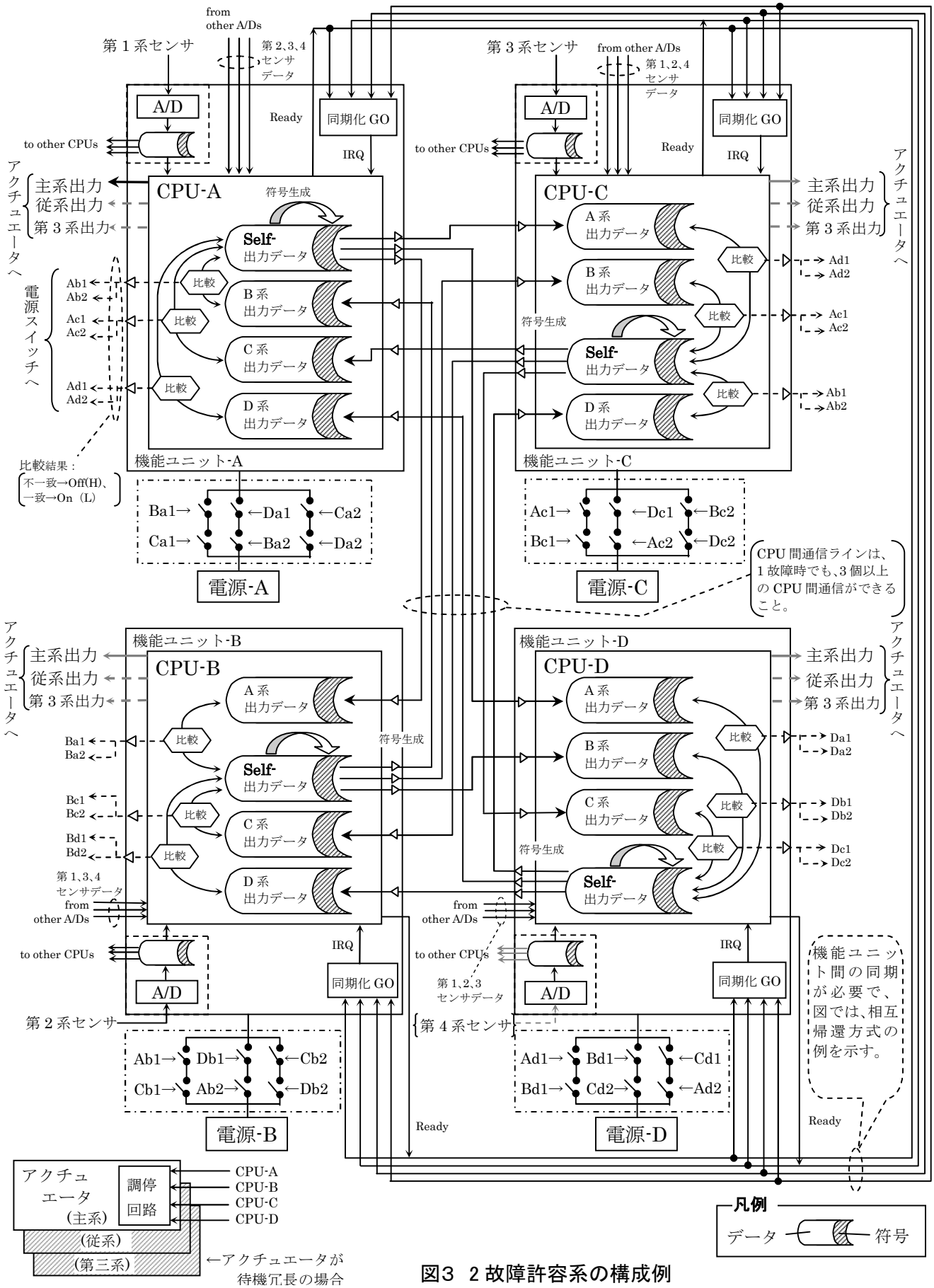
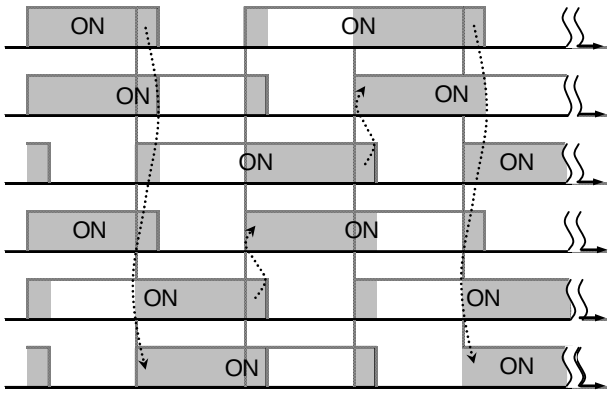
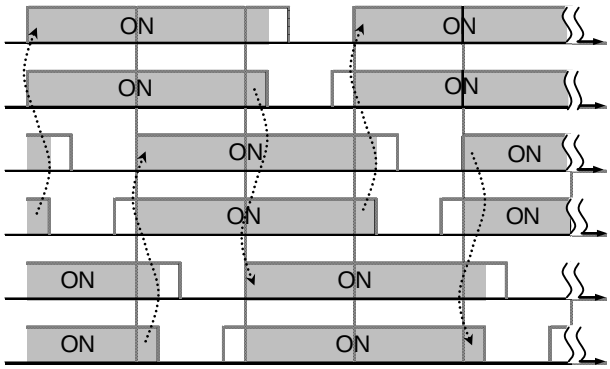


図3　2 故障許容系の構成例

表-1　並列に接続したスイッチを交互に On-Off して固着故障を検知するためのスイッチ･タイミング図

注：スイッチ番号は、図 3 の機能ユニット-A のもの

図番	説明	接続形態	スイッチ番号(注)	タイミング図
図4	＜常に1系統ONにするケース＞ 図3の構成では、同じCPUからの出力Ba1とBa2、Ca1とCa2、Da1とDa2は、独立には制御できない。 この場合、給電ルートは1列になってしまうので、6個のスイッチのうち、1つでもOFF故障があれば、機能ユニットの喪失につながる。	並列 / 直列	Ba1 Ca1 Da1 Ba2 Ca2 Da2	 図中ハッチングは通電状態であることを示す。
図5	＜常に2系統ONにするケース＞ 同じCPUからのスイッチ制御ラインを、独立に制御できるよう構成すれば、右のように、常に2並列のスイッチをONしておくことができる。 こうすれば、OFF故障のスイッチがあっても、機能ユニットを喪失せずに済む。	並列 / 直列	Ba1 Ca1 Da1 Ba2 Ca2 Da2	 図中ハッチングは通電状態であることを示す。

多数決スイッチ回路を構成するスイッチの故障を検知するために、まず各スイッチにスイッチステータス･モニタを付けることが考えられる。これにより OFF 故障を検知できる。

しかし多数決スイッチ回路のスイッチは、通常 ON なので、そのままでは ON 故障を検知することはできない。そこで多数決スイッチ回路の並列部分を利用して､いずれかの列が常に ON にしながら ON-OFF を交互に繰り返すことにより、ON 故障も検出することが考えられる。

図 4 では、常に 1 列しか ON になっておらず、6 個のスイッチのうち、1 つでも OFF 故障があれば、機能ユニットの喪失につながる。ロバスト性を維持しつつ、潜在的なスイッチの固着故障を検出するためには、常に 2 並列のスイッチを ON しておくことが考えられる。そのためには、同じ CPU からのスイッチ制御ラインは、独立に制御できるよう構成する必要がある。(図 5)

4. n 故障許容への一般化

4.1 同時故障を前提外とする場合

図 3 のような多数決スイッチ回路を用いた 2 故障許容システムから、n 故障許容の多重化多数決冗長システムを一般化できる。2 故障許容で見てきたように、複数の機能ユニットが同時に故障しないと前提できるなら、n 故障を許容する多重化システムの機能ユニットの必要数は、n+2 である。ここで“同時”とは、機能ユニットの“同じ制御周期内で”という意味になる。図 6 に、一般化した機能ユニット 1 つ分の構成を示す。各機能ユニットは、符号を付加した出力データを、相互に交換をして、自らのデータと他機能ユニットのデータを比較して、一致しない場合は、相手側の多数決スイッチ回路を OFF する。

多数決スイッチ回路のスイッチの直列数は n 個必要である。これは、直列のスイッチが全て ON 故障した場合を想定してみるとよい。この場合、接続された機能ユニットが異常動作した場合、切り替える手段がなくなる。したがって、n 故障を許容するには、n 個の直列したスイッチが必要になる。

次に並列数は、多数決の母数から直列数を選ぶ組合せになる。機能ユニットの正常/異常を多数決で判断する場合、自分自身については公正な判断ができないので、多数決の母数から除いておいた方がよい。したがって、多数決の母数は n+1 で、並列数は、$_{n+1}C_n = n+1$ になる。

また、CPU から出力されるスイッチ制御信号は、同じものを複数に分けて、多数決スイッチ回路の異なる列に分散して配線しなければならないが、この数は、(直列数)×(並列数)／(多数決の母数) = n×(n+1)／(n+1) = n になる。（便宜的に｢分岐数｣と呼ぶことにする）

さらに、多数決スイッチ回路では、Low は ON 指令、High は OFF 指令として扱う。これにより、一旦異常として OFF された CPU は、自動的に投票者から外れていく。

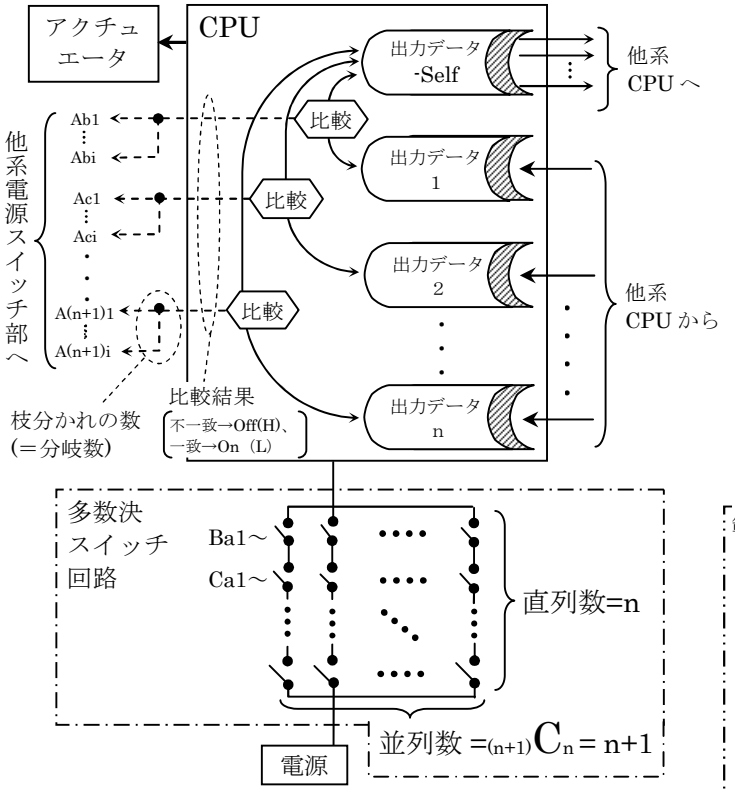
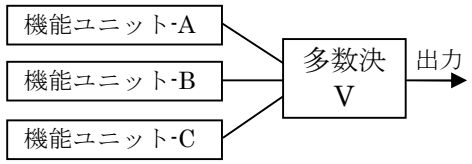


図 6　n 故障許容多数決冗長系の 1 機能ユニットの構成例
（数値は同時故障を前提外とする場合）

図 6 付表　同時故障は前提外の場合と前提とする場合の諸元

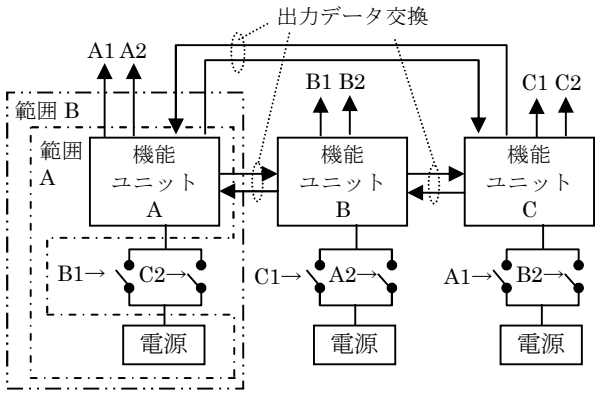
		同時故障を前提外とする場合の諸元	同時故障も前提とする場合の諸元
必要機能ユニット数		n+2	2n+1
多数決スイッチ回路	直列数	n	n
	並列数	n+1	$_{2n}C_n$
	分岐数	n	$_{2n-1}C_{n-1}$



{多数決回路 V の信頼度：Rv
機能ユニットの信頼度：R} とする時

全体の信頼度：$Rv \cdot R^2（3-2R）$ ･･･(式 1)

図 7-1　一般的な TMR の構成と信頼度



{スイッチ 1 個の信頼度＝r
範囲 A の信頼度＝R} とする時

範囲 B の信頼度 $R_B=R\{r^2+2r(1-r)\}=R(2r-r^2)$

機能ユニット 3 系共故障なし（正常）の確率 R_0

$=(R_B)^3=R^3(2r-r^2)^3$

機能ユニット 3 系中 1 故障かつ故障した機能ユニットのスイッチは 2 個とも正常の確率 R_1

$=3\times(1-R)\times R^2\times r^2=3R^2r^2(1-R)$

全体の信頼度$=(R_0)+(R_1)$

$=R^2r^2\{3(1-R)+Rr(2-r)^3\}$ ･･･(式 2)

図 7-2　多数決スイッチ回路を適用した TMR の構成と信頼度

4.2　同時故障も前提とする場合

同時故障も含めて n 故障許容とする場合は、機能ユニットの必要数は、2n+1 になる。直列数は、同時故障を前提外とする場合と同様、最悪 ON 故障が直列に並ぶことを考慮して n 個必要で、並列数は多数決の母数から直列数を選ぶ組合せで、$_{2n}C_n$ になる。分岐数は、(直列数)×(並列数)／(多数決の母数) = $_{2n-1}C_{n-1}$ となる。

以上を図 6 付表にまとめる。

5.　信頼性の検討

最後に、一般的な NMR と今回提案の NMR の信頼性を比較しておく。簡単のため、機能ユニット数が 3 のケース、即ち三重化多数決冗長系のケースで比較する。

図 7-1 に一般的な三重化多数決冗長系の構成と信頼度を、図 7-2 に提案の多数決スイッチ回路を適用した三重化多数決冗長系の構成と信頼度を示す。ここでは、多数決スイッチ回路におけるスイッチは ON 故障と OFF 故障で、症状が異なるので、大雑把な議論ではあるが、故障する場合は、障害が出る方の故障モードとして議論する。

図 7-1 の信頼度（式 1）と図 7-2 の信頼度（式 2）で、大小関係は単純ではないが、(式 2)のスイッチに信頼性の低いリレーなどを使うと、全体の信頼性も悪化することが考えられる。やはり信頼性の高い半導体スイッチなどを使用することが重要である。半導体スイッチの使用に電気的制約などある場合は、多数決スイッチ回路を、電源の代わりに、機能ユニットが確実に機能停止するようなディジタル信号などに適用してもよい。

6.　むすび

多数決スイッチ回路を用いた多重多数決冗長系は、簡単な構成で、かつ故障カウントもしやすい、実用的な方法である。

文　　献

[1] 当麻、南谷、藤原：”フォールトトレラントシステムの構成と設計”，pp103-104，槇書店，(1991)