RC-002

多数決スイッチ回路による n-フォールトトレラントシステムの設計考察

Design Considerations of n-Fault-Tolerant system with Voting Switches

岩井 仁司
Hitoshi Iwai

1． まえがき

筆者は、多数決回路を含めて故障をマスク（＝誤ったデータをシステムから外に出さないこと）する多重多数決冗長系を提案している[1,2,3]。この方式は多数決のために、スイッチのみから構成される多数決スイッチ回路を利用している。

本稿では、有人宇宙船のように制御系とセンサ、アクチュエータを備え、ハザードに関係する閉システムを例に提案の方法を説明する。ハザードを取り扱うシステムでは、一般的に TTE（Time To Effect：障害が発生してからハザードが発生するまでの時間）を設計要求条件として決めておく必要がある。つまり、障害が発生してもシステムが TTE までにハザード回避処置をとることができれば良いと考える。したがって、n-フォールトトレラントシステムにおいても、ｎ故障まで全く障害を出さない必要性はなく、ｎ回障害を出してもその度に TTE までに故障を検知し正常な処理に戻ってハザード回避処置をとり、ミッションに戻ることを必要条件と考える[16]。TTE はアプリケーションによって変わってくるが提案の方法では、”1 制御周期より長い”ことを前提とする。制御周期は通常正常な制御が持続できるよう十分短く設定されているので、この前提は多くのケースで問題なく受け入れられるはずである。

ただし、提案の方法が、金融のようにディジタルデータを取り扱い障害が全く許容されないシステムに適用できない、ということではない。処理データに符号を付けること、および最後に出力データを外部に取り出す際の通信に多少の工夫を加えることで、金融システムにも十分適用できると考えるが紙面の都合で本稿では割愛する。

ハザードを取り扱うシステムでは単に信頼度が高いことよりも、どこが壊れても許容でき、かつ故障数がカウントできるということが非常に重要である。本稿では、順序依存性故障の論理を指摘して、故障カウントのルールと信頼度について検討する。

2. 従来の多重多数決冗長系の問題点

フォン・ノイマンは、多重多数決冗長系の解として、Triple Modular Redundancy (TMR) を提唱した(図１)。このシステムでは、機能モジュールが１つ故障した場合でも、システムとして正しい出力を出すことができる。

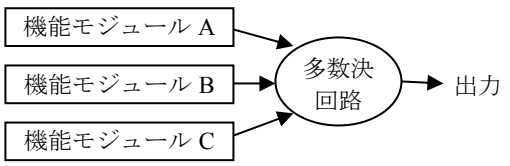


図 1 Triple Modular Redundancy (TMR)

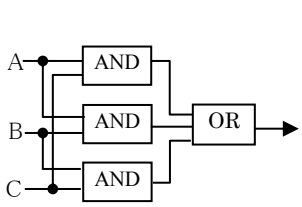


図２ 一般的な多数決回路

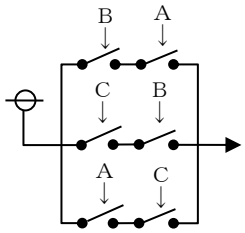


図３ 多数決スイッチ回路

ノイマンの論文[4]では、多数決回路によるエラーはマスクできないとしている。これは彼が多数決回路として、図２のような論理ゲートからなる回路を想定していたためである。この回路では、例えば AND ゲートが 1 固定故障を起こすと、システムの出力は必ず 1 となり、データ訂正はできない。しかし、一方でスイッチだけから構成される図３の回路も知られていた[7,8]。この回路の場合、多数決回路が 1 故障しても、なお正しい出力を得ることができる。但し、この回路は、”高速データ通信に向かない”、”スイッチオン故障が内在していても検知できず、結局は故障が増えて障害が出るまでわからない”、といった欠点があり、多くの人は注目しなかった。近年でも「多数決回路自体の故障によるエラーの訂正はできない」という前提の論文が多数発表されている。([10]など)

筆者は多数決スイッチ回路による n-フォールトトレラント冗長系を提案している。提案の構成では、図 3 のような多数決スイッチ回路を各多重化機能モジュールの電源 On/Off 制御に適用し、各機能モジュールから互いに制御し合い、故障発生時に当該機能モジュールを多数決で電源 OFF する。

3. 提案システムの説明

本稿で説明に用いるシステム構成図（図4～8）は、機能モジュールとアクチュエータの接続を 1 対 1 にしている。これはアクチュエータの故障時の FDIR（故障検知→故障部位隔離→機能回復の一連の処理フロー）が簡単なためであるが、これがクロス接続であっても、本稿提案の方法の有効性に影響しない。本稿提案方法の特長は、機能モジュールとアクチュエータが直結していることである。これが TMR では機能モジュールとアクチュエータの間に必ず多数決回路が介在するのと対照的である。機能モジュールとアクチュエータの接続形態と、アクチュエータの FDIR の方法は、そのシステム設計時に各々のケースとして検討する必要がある。

提案システムの構成には、同一制御周期内で発生する故障数が 1 以下であるという前提が”必要な構成”と”必要としない構成”がある。文献[2]では、それぞれ必要な機能モジュール数によって、この前提が必要な構成を(n+2)MR、必要としない構成を(2n+1)MR と呼んでいる(n は故障許容数)。この前提は一般的に非常に確率が小さいので、より少ないリソースで、信頼度も高く有用性が高いのは、前提を必要とする(n+2)MR の方である[2,7]。スイッチ単体の故障率は非常に小さいので、細かな議論はあまり意味がないと思われる。しかし敢えて厳密に議論すると、(n+2)MR には、スイッチ

のオフ故障と機能モジュールの故障には、順序依存性故障の論理があって、故障カウントのルールや信頼度の計算を複雑にしている。（本稿 5 節と 6 節で後述）

3.1 故障許容ケース（3 重多数決系）[2]

最初に提案の方法を図４に示す。もし１つの機能モジュールが故障起こすと、その機能モジュールは他の２つの機能モジュールによって無効化される。

図４について、以下に説明する。

1) 各モジュールは図３のような多数決スイッチを電源制御回路として具備している。あるモジュールは、他のモジュールが同時にオフ信号を送ることによって、電源オフすることができる。多数決スイッチは 2 並列 1 直列のスイッチで構成されている。それぞれのスイッチは異なるモジュールによって制御される。図 4 で、スイッチ制御信号の大文字は、その信号の出力元の機能モジュールを表している。小文字はその多数決スイッチのグループ番号を表している。
2) 全ての機能モジュールはデータの交換ができるよう通信ラインで相互に接続されている。
3) 機能モジュール間の同期機構が必要である（たとえば相互帰還法[5,pp.126] [7]）

次に動作について説明する。

1) 各々の機能モジュールは同じ制御周期で同じ処理を行う。
2) 機能モジュールは各自の出力データを、出力前に相互に他の機能モジュールと交換する。そして、交換されたデータと自分のデータとを比較する。
3) もし違いが見つかれば、その機能モジュールは電源オフ信号を、相手側の多数決スイッチ回路に送信する。多数決スイッチ回路が２つの機能モジュールからオフ信号を受け取ったとき、その機能モジュールは電源オフされる。
4) 電源オフされなければ、機能モジュールは出力データを外部機器に出力する(たとえばアクチュエータ)。アクチュエータは、物理的な制約から１つを動作中、他の冗長系を待機としなければならないことが多い。アクチュエータの動作／待機の区別は、機能モジュールが互いに通信を行い、予め定めた優先順位に従って決めることができる。機能モジュールは、同一の処理を並行して行うのが原則であるが、アクチュエータの動作／待機の決定は、各々の機能モジュールが制御する。
5) ステップ 1)へ戻って周期的に処理を継続する。

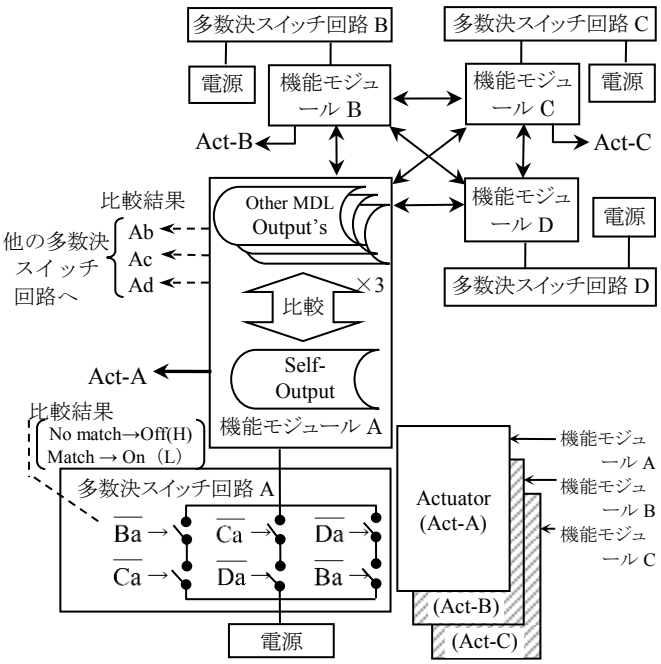


図5．2 故障許容冗長系の例(機能モジュール数は4つ)[1,2,3]

3.2 同時2故障は起こらないという前提での2故障以上許容ケース(4重多数決系)[1, 2, 3]

故障率が十分小さいとき、同一周期内で２つ以上の故障が同時に起こらないという前提は適切であろう。この前提の場合、２故障許容システムは少なくとも４つの機能モジュールから構成される。なぜなら最初に故障した機能モジュールを無効化した後、残りの３つの機能モジュールで１故障許容の多数決系を構成できるからである。この構成を図５に示す。各多数決スイッチ回路は３並列２直列の６個のスイッチから構成され、給電対象の機能モジュールを除く他の３つの機能もモジュールから制御される。図でスイッチ制御信号の大文字は、その信号の出力元の機能モジュールを表している。小文字はその多数決スイッチのグループ番号を表している。図で１つの多数決スイッチ回路の箱の中には、同じ制御信号名称が２つある。多数決スイッチ回路に接続された３つの機能モジュールの内２つ以上の機能モジュールが、各自の出力データと異なると判断した場合、それらの機能モジュールは当該機能モジュールを電源オフしにいく。

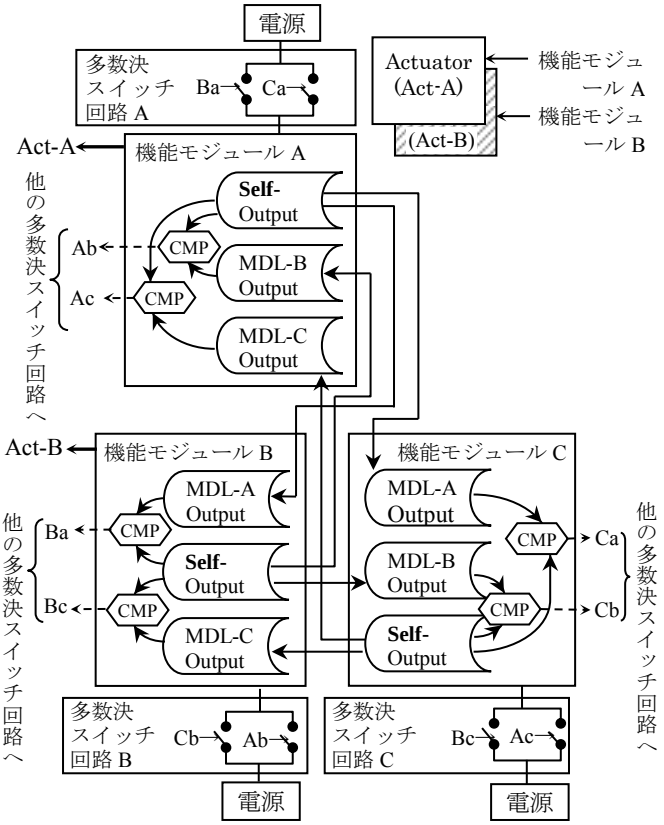


図４　1故障許容冗長系の例(機能モジュール数は3つ)

電源オフされた機能モジュールによる他モジュール電源制御機能を無効化するために、そのモジュールによって制御される全スイッチをオン側に倒す必要がある。オン側に倒すことによって、他の機能モジュールが当該多数決スイッチの機能モジュールと出力データが一致していれば正常、不一致であればオフするという制御に引き続き使うことができる。このために、機能モジュールから出力された制御信号は、Low 側がスイッチオフとなるようにするとよい。スイッチの制御は個別パルス信号で制御する方法があるがこの構成ではあまり適さない。図でスイッチ信号の上のバーは論理の反転（一致の場合 L、不一致の場合 H）を意味している。

次に機能モジュール５つによる３故障許容ケースの構成を図６に示す。

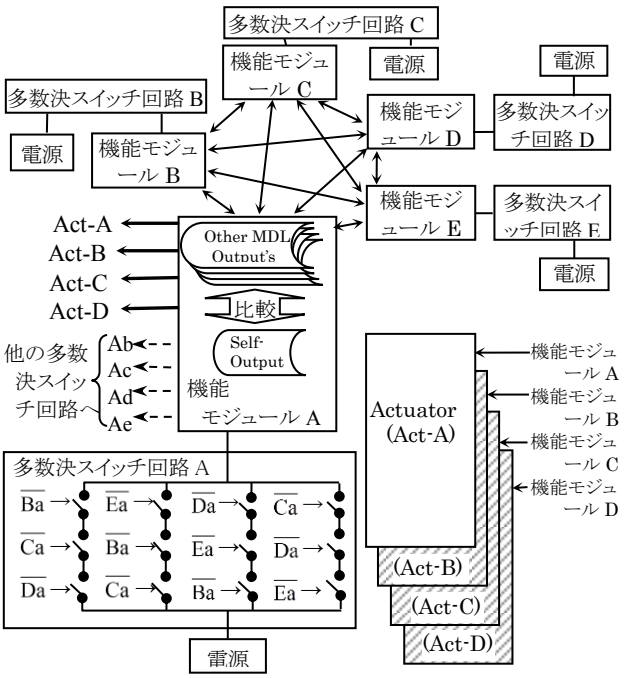


図6．3 故障許容冗長系の例(機能モジュール数は 5 つ) [2]

最後に(n+2)個のモジュールによる n-FT ケースを図７に示す。本稿ではこのケースを(n+2)MR と呼ぶことにする。

このケースでは、多数決スイッチ回路の直列数は n か、それ以上でなければならない。なぜなら、機能モジュールが誤作動した場合、その機能モジュールをオフするスイッチが必要である。この場合、機能モジュールが 1 故障しているので、(n-1) 故障しても確実にオフするためには n 個の直列に並ぶスイッチが必要である。

多数決スイッチの並列数は、多数決の母数から直列数を選ぶ組合せ数と同じになる。多数決の母数とは多数決スイッチ回路に接続された機能モジュール数であり、”n+1”である。したがって並列数は $_{n+1}C_n$ (= n+1) となる。

そして、機能モジュールから出力されるスイッチの制御ラインは、同一多数決スイッチ回路内の異なるスイッチを制御するために分岐がある。この分岐数は、(直列数)×(並列数)／(多数決の母数) = n×(n+1)／(n+1) = n. と等しい。

電源オフされた機能モジュールから出ているスイッチの制御ラインの影響を無効化するためには、High 側をスイッ

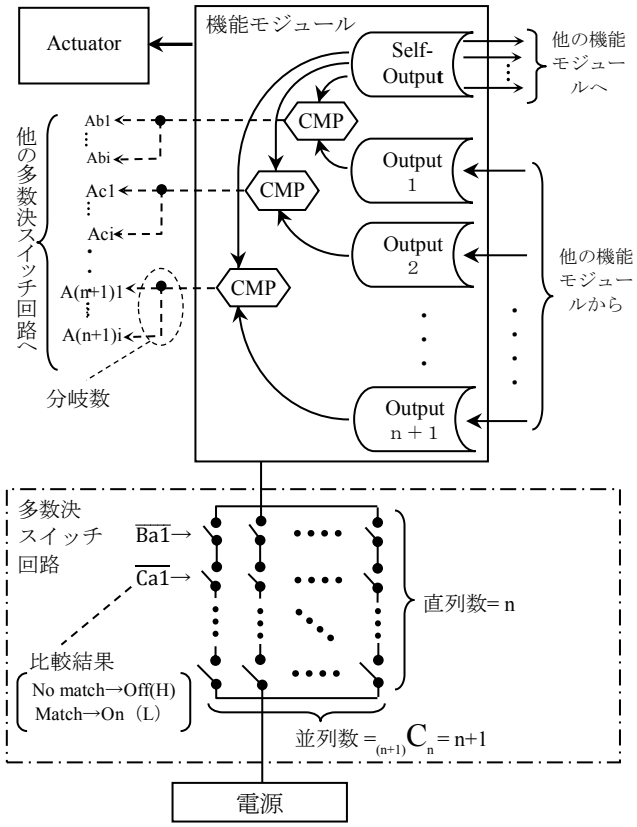


図7．同一制御周期内で複数故障が起こらないと仮定した場合の n 故障許容冗長系の例 [1][2]

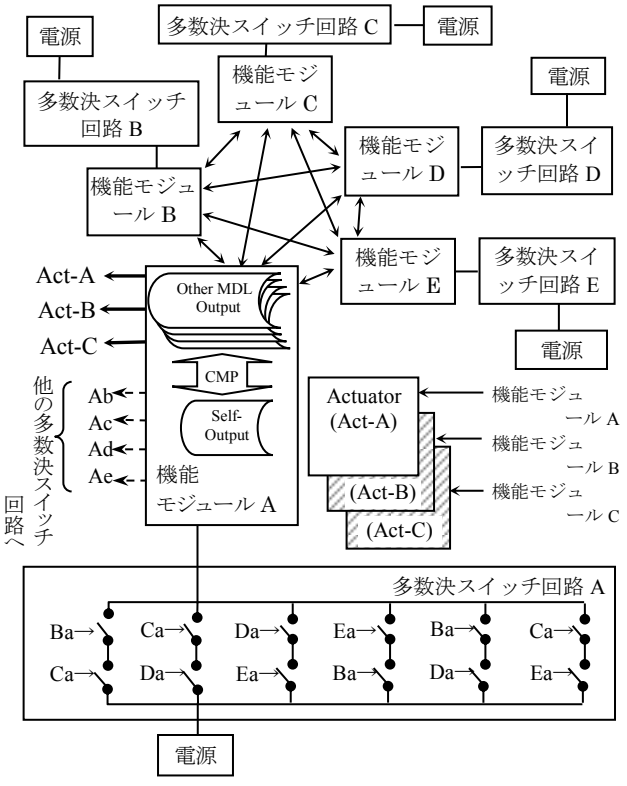


図8 多数決は常に正しいと仮定した場合の 2故障許容冗長系の例[2]

チオフ、Low 側をスイッチオンするとよい。このルールにより、自動的に電源オフされた機能モジュールの影響を排除できる。

3.3 多数決は常に正しいという前提での2故障以上許容ケース（5重多数決系）[8]

次に 1 制御周期内に複数の故障が同時に起こりうるが、多数決の結果は常に正しいという前提で検討を行う。例えば 2 故障許容システムは機能モジュールを５個必要とする。この場合のシステムの構成例を図７に示す。

一般的に、n 個の故障を許容するには(2n+1)個の機能モジュールが必要になる。機能モジュールが誤作動する場合に備えて、“n”直列のインヒビットが必要になる。そして、${}_{2n}C_n$ 並列のスイッチが必要になる(多数決の母数は自機能モジュールを除く 2n になるので、並列数は ${}_{2n}C_n$)。したがって、各多数決スイッチ回路の構成は、図８に示すように、2 直列 6 並列の構成となる。

本稿では、この前提の冗長系のタイプを(2n+1)MR と呼ぶことにする。(n+2)MR のタイプとは逆に、電源オフされた機能モジュールの影響を排除するために、スイッチ制御信号の High はスイッチオン、Low はスイッチオフとすべきである。あるいは個別パルス信号でスイッチ制御が可能である。以上を要約すると表１に示す。

4. 内部故障検出のための周期的点検[1]

もしシステム内部の故障を検出できなければ、故障は次第に増加し、突然システム障害を起こすであろう。したがって、故障を検出し、カウントできることが必要である。多数決スイッチ回路内の故障を検出するために、すべてのスイッチにスイッチ状態モニタが必要である。これによりオフ固着故障の検出は可能になる。しかしスイッチは通常オン状態なのでオン固着故障については検出できない。したがって、多数決スイッチ回路の並列部分を使って交互にスイッチをオン/オフし、一方常に 1 系統は給電を維持するよう制御することによりオン固着故障を検出できる。

本稿では、少ないリソースで高い信頼性を実現する 4 重系 2 故障許容システム（図５）を採りあげて、そのスイッチ制御のタイミングチャートを図９に示す。このようなスイッチ制御によるオン固着故障の検出を、周期的点検と呼ぶことにする。

表１． 多数決スイッチ冗長系の諸元
(1 制御周期内で 2 故障以上発生しないと前提した場合と多数決は常に正しいとのみ前提とした場合)[2]

略称		(n+2)MR	(2n+1)MR
前提		1 制御周期内で 2 故障以上の故障は発生しないと前提した場合	多数決の結果は常に正しいことのみ前提とした場合
スイッチ制御信号の極性		High: Switch-Off Low: Switch-On	High: Switch-On Low: Switch-Off
機能モジュールの最小数		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	${}_{2n-1}C_{n-1}$

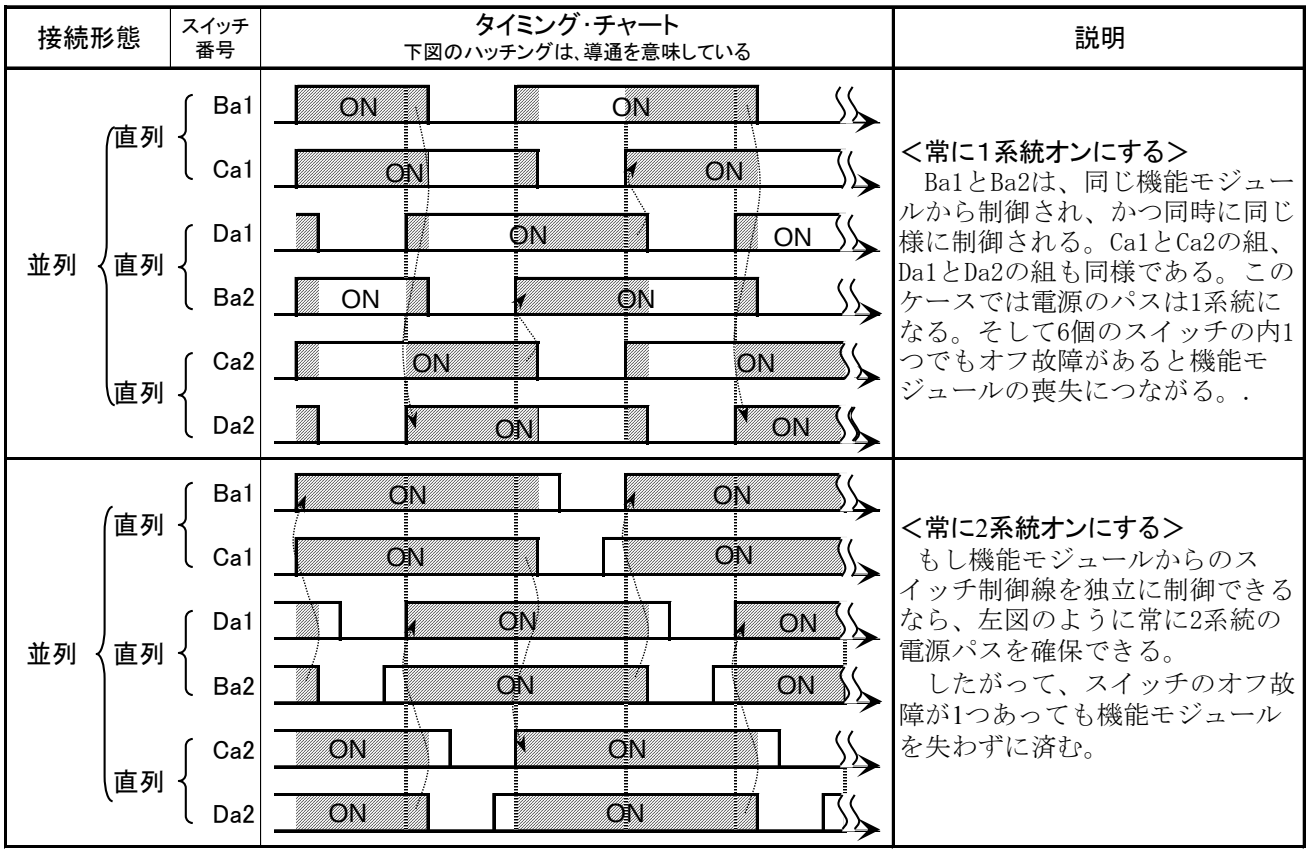


図9．4重系2故障許容システム(図5)のスイッチのための周期的点検のタイミングチャート.[1]

5. 多数決スイッチ回路の故障カウント

多数決スイッチ回路の故障カウントには注意が必要である。例えば 2FT のシステムで 2 故障後、まだ故障許容性がある場合がある。このような場合は 2 故障目をカウントしないほうが良い。故障カウントのルールは明確にする必要がある。

(1) 故障モードの定義

-**定義 A**: スイッチは､2 つの故障モードを持っている; オン固着故障／オフ固着故障。（本稿では、簡単にそれぞれオン故障／オフ故障と呼ぶ）

-**定義 B**: スイッチ状態モニタは､2 つの故障モードを持っている; オン表示固着故障／オフ表示固着故障（本稿では簡単にそれぞれオン表示故障／オフ表示故障と呼ぶ）

(2) 周期点検中の故障モードの特定

論理 A: スイッチ 1 個に 1 つのスイッチ状態モニタを実装した場合、周期的点検で、スイッチ状態モニタの故障の可能性もあるので、オン故障かオフ故障か判別することはできない。

スイッチ 1 個に 2 つのスイッチ状態モニタを実装し、同時複数故障はないと前提すれば、周期的点検でオン固着故障かオフ故障か判別することはできる。逆に同時故障あると前提すれば、周期的点検でオン故障かオフ故障か判別することはできない。 (表 2 参照)

表 2．周期的点検によるオン故障／オフ故障識別可否
（スイッチ状態モニタ 2 本時）

		スイッチ状態モニタ故障モード		
		故障なし	1 故障	複数故障
スイッチ故障モード	オン故障	特定可能	特定可能	特定不可
	オフ故障	特定可能	特定可能	特定不可

(3) (1 系統常時オンでの周期点検中の)オフ故障に対する故障カウント

論理 B: 如何なるオフ故障も故障としてカウントする必要がない。

→ 理由：1 オフ故障は、周期的点検により機能モジュールの喪失に引き起こすから､機能モジュールの故障のみをカウントすればよい。

(4) (2 系統常時オンまたは周期的点検しない場合の)オフ故障に対する故障カウント

下の論理 C は 1 つ目の故障カウント、論理 D～F は、先行するオフ故障が原因で機能モジュールが 2 つ以上同時に失われてしまう、というものである。

(4-1) **論理 C**: 全システム中、1 つ目のオフ故障は、故障カウント 1 としてカウントしなければならない。

→ 理由：例えば図 10 で Ca1 がオフ故障した後、機能モジュール D の故障により､Da1 と Da2 がオフされ、機能モジュール A と D が同時に喪失され、故障カウント 2 になるので、その前に故障カウントを 1 にしておかなければならないから。

(4-2) **論理 D**: オフ故障を含む多数決スイッチ回路では、2 つ目以降のオフ故障はカウントアップする必要はない。

→ 理由：オフ故障が 1 多数決スイッチ回路内で増殖しても､対応する機能モジュール 1 つの喪失の原因にしかならないため。

(4-3) **論理 E**: オフ故障のスイッチに直列につながるスイッチ全てに関係しない機能モジュールを洗い出す。洗い出された機能モジュールの多数決スイッチ回路のオフ故障は、故障カウントする必要がない。

→ 理由：洗い出された機能モジュールの多数決スイッチ回路にもオフ故障がある場合、他の機能モジュールの故障により、同時に両方の機能モジュールが失われ、故障カウントが 2 になる可能性がある。しかし、最初のオフ故障で故障カウント 1 をカウントしているので、2 つ目のオフ故障はカウントする必要がない。

(4-4) **論理 F**: 上記論理 E の最初にオフ故障を起こした機能モジュールと、洗い出された機能モジュールを除く多数決スイッチ回路では、洗い出された機能モジュールによって制御されるスイッチと、そのスイッチに直列に繋がるスイッチの故障はカウントする必要がない。

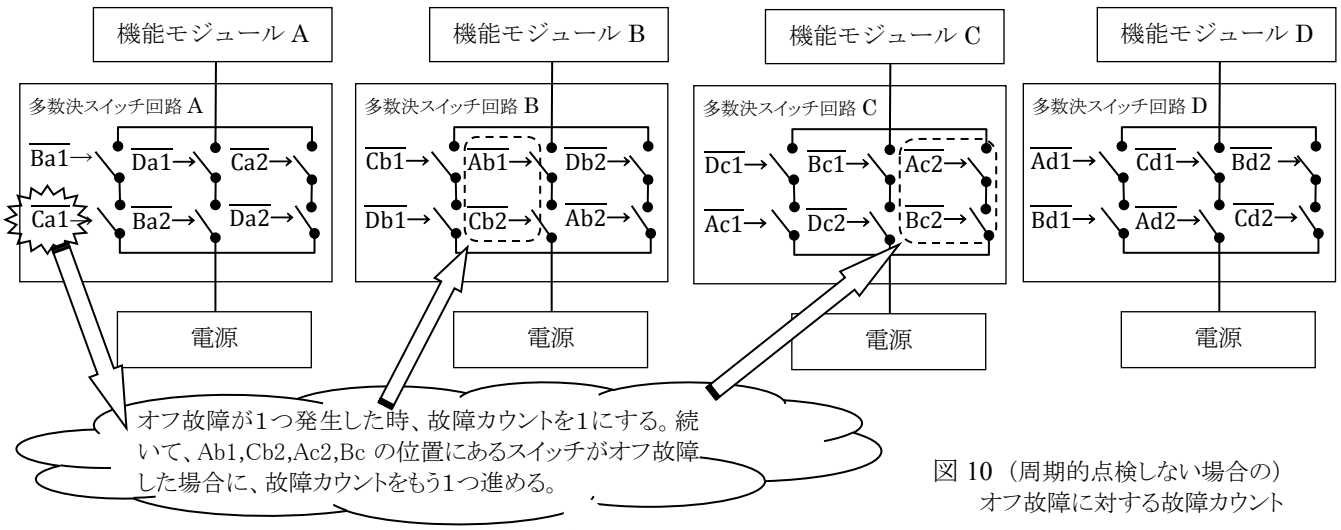


図 10（周期的点検しない場合の）
オフ故障に対する故障カウント

→ 理由: 洗い出された機能モジュールによって制御されるスイッチは、洗い出された機能モジュールの出力結果異常時に、スイッチオフになる。このオフになるスイッチと直列に並ぶスイッチがオフ故障であっても、他の導通パスが健全であれば、機能モジュールの喪失が伝搬することはない(故障カウントが 1 から 3 に飛ぶことはない)。

例えば、図 10（4 重系 2 故障許容システム)でスイッチ Ca1 が最初にオフ故障したときに、故障カウントを 1 にする（論理 C）。そして、同じ機能モジュール内の次の故障はカウントアップする必要がない（論理 D）。次に Ca1 および同じ直列上の Ba1 に関係しない機能モジュールを捜し出す。それは機能モジュール D であり、その多数決スイッチ回路のオフ故障はカウントする必要はない（論理 E）。モジュール D によって制御される直列上のスイッチのオフ故障はカウントする必要がない。つまり Cb1 と Db1, Db2, Ab2, Dc1, Ac1, Bc1, Dc2 のオフ故障はカウントする必要がなく、Ab1 と Cb2, Ac2, Bc2.のオフ故障をカウントすれば良いことになる（論理 F）。

(5) オン故障に対する故障カウント

論理 G: 同じ直列上のオン故障の数をカウントすべきである。

→ 理由：直列に全てオン故障を起こし､次に対応する機能モジュールが誤作動すると､その機能モジュールを切り離す手段がなく、システム障害に至るため。

(6) 直列上のスイッチのオフ故障

論理 H: オフ故障 1 つある場合、その直列上の全てのスイッチについて故障カウントする必要がない。

→ 理由：直列上に並んだスイッチの 1 つでもオフ故障があると、他のスイッチがどうであろうと電気が流れることはない。

実際のフォールトトレラントシステムを設計する場合は、以上の”論理”が必要になるであろう。論理 E､論理 F と論理 G が特に重要である。また、スイッチ状態モニタ 1 本のケースでは、オン故障とオフ故障の識別はできないということが大きな制約となる。

6. 多数決スイッチ冗長系の信頼度

6.1 (n+2)MR と(2n+1)MR の信頼性の比較

まず、表 1 の(n+2)MR のタイプと(2n+1)MR のタイプの信頼性の比較を行う。簡単のため、ここでは多数決スイッチ回路の信頼性は 1 とする。

図 5 のような機能モジュール 4 つの(n+2)MR の信頼性は次のようになる。(R は機能モジュール 1 個の信頼性)

$$R^4 + 4 \times R^3(1-R) + 6 \times R^2(1-R)^2 = 3R^4 - 8R^3 + 6R^2$$

さらに、モジュール数 n の場合に(n+2)MR の信頼性を一般化すると次式のようになり、グラフは図 11 のようになる。

$$R_{(n+2)MR} = \sum_{i=0}^{n} {}_{n+2}C_i \times R^{n+2-i} \times (1-R)^i$$

(2n+1)MR の信頼性を一般化すると次式のようになり、グラフは図 12 のようになる。

$$R_{(2n+1)MR} = \sum_{i=0}^{n} {}_{2n+1}C_i \times R^{2n+1-i} \times (1-R)^i$$

(2n+1)MR の場合、機能モジュール 1 個の信頼性が 0.5 より大きければ、システムの信頼性はそれよりは大きくなる。しかし、0.5 より小さい場合はシステムの信頼性は 1 台の時より悪化してしまう。一方、(n+2)MR の場合は、機能モジュール 1 個の信頼性が 0.5 より小さくても、システムの信頼性は良くなる可能性がある。

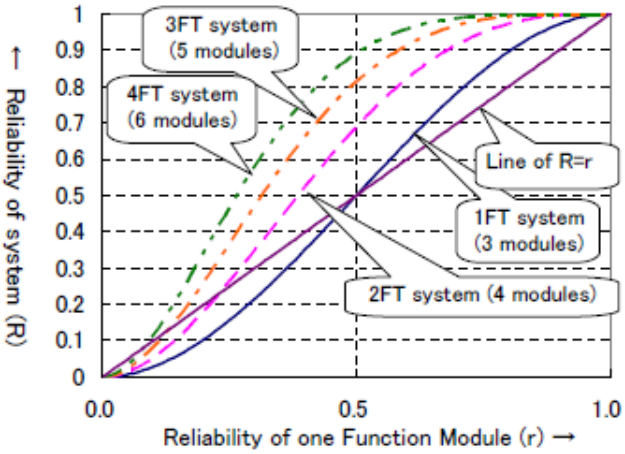


図11 (n+2)MRの信頼性

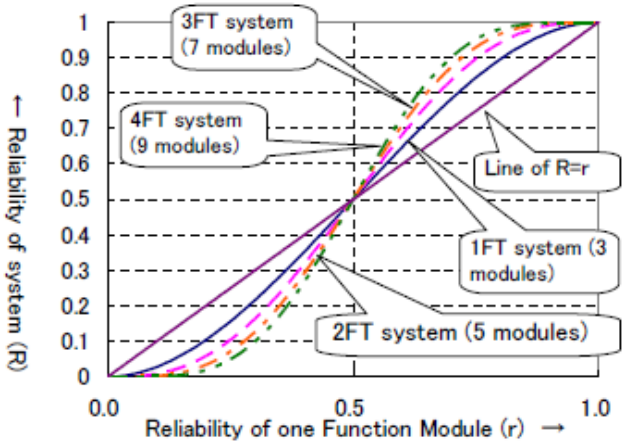


図12 (2n+1)MRの信頼性

(n+2)MR は、1 制御周期内に同時に機能モジュールが複数故障しないという前提付きの構成である。その確率は、一般的には非常に小さく無視可能であることが多い[2]。したがって、(n+2)MR の方が少ないリソースで高い信頼性を実現するもので、有用性が高いと言える。

6.2 多数決スイッチ回路を含めた信頼性

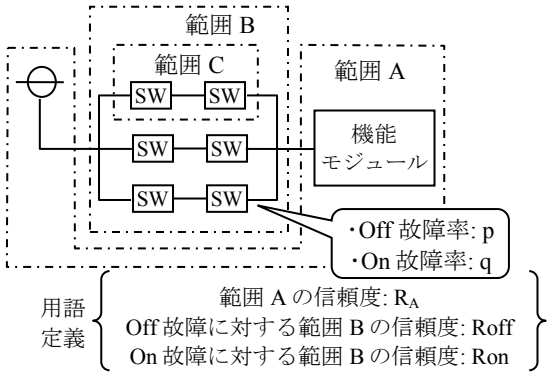
ここでは 4 機能モジュールによる 2 故障許容構成（図 5）に絞って議論をすすめる。

スイッチには故障モードが 2 つある。オン故障とオフ故障である。片方が起きればもう片方は起こらない。また、オン故障とオフ故障で、システム障害が起こるまでのメカニズムが異なる。即ち、スイッチのオン故障のみでシステム障害に至ることはなく、ある機能モジュールに接続され

たスイッチが直列に全てオン故障した場合で、かつその機能モジュールが誤作動した場合にのみシステム障害が起きる。一方、オフ故障は並列に接続された系統のいずれもオフ故障した場合に、機能モジュールの１つが喪失されるが、他の機能モジュールが残っていればシステム障害には至らない。

このようにオン故障とオフ故障では、システム障害の現れ方、信頼度計算式まで異なることから、オン故障率とオフ故障率で分けて考える必要がある。

検討のための用語、範囲 A, B, C は図 13 を参照のこと。



●範囲 C のオフ故障に対する信頼度： $(1-p)^2$
（注）「信頼度＝1－故障率」なので $(1-p-q)^2$ であるが、オン故障は故障として症状が現れないので、q=0 として扱う。
●範囲 C のオフ故障率： $1-(1-p)^2$
●範囲 B のオフ故障率： $(1-(1-p)^2)^3$
●範囲 B のオフ故障に対する信頼度(Roff):
$1-(1-(1-p)^2)^3=1-p^3(2-p)^3$

図 13　信頼度検討のための用語

(a) オフ故障率とシステム障害発生確率

まず、オフ故障率とシステム障害発生率の関係を検討する。例えば、図 10 で多数決スイッチ回路 A の中の左下のスイッチ Ca がオフ故障後に、機能モジュール D が誤動作して、多数決スイッチ回路 A の 2 つの Da を Off すると、機能モジュール A は Off されてしまう。結局、機能モジュール D 一つの誤動作によって、機能モジュール２つが Off される。一方、機能モジュール D 誤動作後に Ca がオフ故障した場合は、機能モジュール A の動作に影響はない。即ち、故障の順序に、システム障害の確率が依存している。このような事象を順序依存形故障論理という[11,12]。

図 10 の 2FT システムの場合、順序依存形故障論理により 1 つの機能モジュール故障で、2 つ以上の機能モジュールが同時に喪失されるケースとして、次の 2 ケース考慮する必要がある。

①機能モジュール 1 故障とスイッチ 1 オフ故障の後、機能モジュールの 2 故障目により、新たに機能モジュール２つが同時に失われ、システム障害に至るケース
②２つの機能モジュールのスイッチが１つずつオフ故障後、３つ目の機能モジュールの故障により、機能モジュールが３つ同時に失われ、システム障害に至るケース

①の条件式は式(1)で、②の条件式は式(2)で表すことができる。 (pAND は優先 AND)

$$pAND(6\times R_A^2\times Roff^2\times(1-R_A\times Roff)\times p\times 2(1-p)^2,\ 1-R_A) \quad (1)$$

$$pAND(4\times 3\times R_A^3\times Roff^2\times p^2\times 4(1-p)^4,\ 1-R_A) \quad (2)$$

順序依存形故障論理の定量化の方法には、多重積分による方法やマルコフモデルを用いる方法などが知られている。次式(3)は、多重積分法の公式[11]である。

$$\Pr\{N\}=\int_0^t f_1(t_1)\int_0^{t_1} f_2(t_2)\int_0^{t_2}\cdots\int_0^{t_{n-1}} f_n(t_n)dt_n\ldots dt_2dt_1 \quad (3)$$

ここで、
Pr：事象発生確率（本稿ではシステム障害率に同じ）
n ：順序依存形故障論理の入力数
N： ベクトル[n, n-1, n-2, …,1]
$f_i(t_i)$: $\lambda_i\exp(-\lambda_i t_i)$。累積故障率。
λ_i: 入力事象 i の故障率（時間当たり）

式(1)で、pAND()の第 1 引数”$6\times R_A^2\times Roff^2\times(1-R_A\times Roff)\times p\times 2(1-p)^2$” の各構成事象に順序依存性はない。順序依存性が存在するのは、第 1 引数の条件成立後、第 2 引数の条件即ち機能モジュールが誤動作する場合のみである。したがって、式 (3) のベクトル [n-1, n-2, …,1] の部分 $\int_0^{t_1} f_2(t_2)\int_0^{t_2}\ldots\int_0^{t_{n-1}} f_n(t_n)\,dt_n\ldots dt_2$は、順序依存性のない単なる掛け算$f_2(t_2)\cdots f_n(t_n)$でよい筈である。

したがって、式(3)の代わりに、式(4)が使える。

$$\Pr(\lambda_1,\lambda_2)=\int_0^t f_1(t_1)\int_0^{t_1} g(t_2)\,dt_2dt_1 \quad (4)$$

ここで、$g(t)=f_2(t)\times\ldots\times f_n(t)$

式(4)を解くと[11]、

$$\Pr(\lambda_1,\lambda_2)=\frac{\lambda_2}{\lambda_1+\lambda_2}-\exp(-\lambda_1 t)+\frac{\lambda_1}{\lambda_1+\lambda_2}\exp(-(\lambda_1+\lambda_2)t) \quad (5)$$

＜機能モジュールとスイッチのオフ故障に対するシステム障害の確率＞は、機能モジュールが 4 つ故障する場合と、機能モジュールが 3 つ故障する場合と、式(1)の確率と式(2)の確率の和であり、次式の通り。

$(1-R_A\times Roff)^4+4\times(1-R_A\times Roff)^3\times(R_A\times Roff)$＋式(1)の確率
＋式(2)の確率 (6)

式(1)の確率と式(2)の確率は、式(5)により求まるので、式(6)のグラフは、図 14 になる。

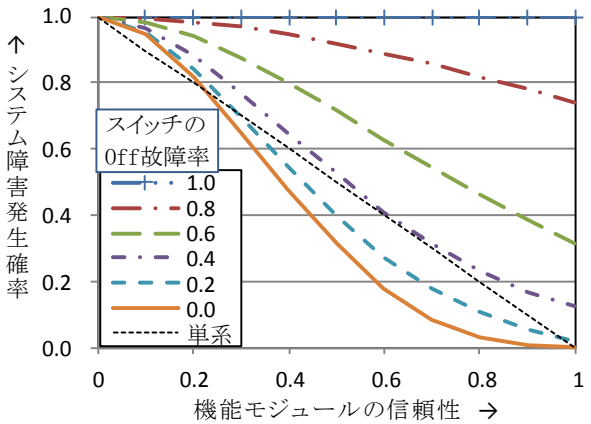


図 14　スイッチオフ故障率とシステム障害発生確率

一般的に順序依存形故障論理の定量化は複雑な問題であり、図 14 の結果も検証すべきと考えているが、現状検証できていない。多重積分法以外にマルコフモデルを用いる方法[6, 13, 15]などがある。マルコフモデルを用いる方法は、正確な議論が可能になるが、かなり複雑になる傾向がある。本問題にマルコフモデルを適用しようとすると、まず状態遷移図が複雑になり過ぎて、記述が不可能であると考える。

(b) オン故障率とシステム障害発生確率

次にオン故障率とシステム障害発生率の関係を検討する。範囲 B のオン故障は、対応する機能モジュールの故障と同時に発生した時に、システム障害を生じる。したがって、

＜オン故障に対するシステム障害の確率＞

$$=(1-R_A)^4+4\times(1-R_A)^3\times RA+6\times R_A^2\times(1-R_A)^2 \times(2\times\{1-(1-q^2)^3\}-\{1-(1-q^2)^3\}^2)+4\times(1-R_A) \times\{1-(1-q^2)^3\}\times R_A^3$$

・・・ グラフを図 15 に示す。

前項の図 14 では、機能モジュールの信頼度が 1 でも、スイッチオフ故障率＝1 なら、結局機能モジュールの電源が入らないので、システム全体では障害が必ず出てしまうことを表している。図 15 では機能モジュールの信頼度が 1 であれば、スイッチオン故障率＝1 でも、システム障害とはならない。

スイッチのオフ故障率／オン故障率の許容基準として、「システム全体の信頼度が機能モジュール単系の信頼度より良くなること」を基準にすれば、オフ故障率、オン故障率共に 0.2 程度以下である必要がある。（ただし機能モジュール単系の信頼度が 0.4～1.0 の範囲）

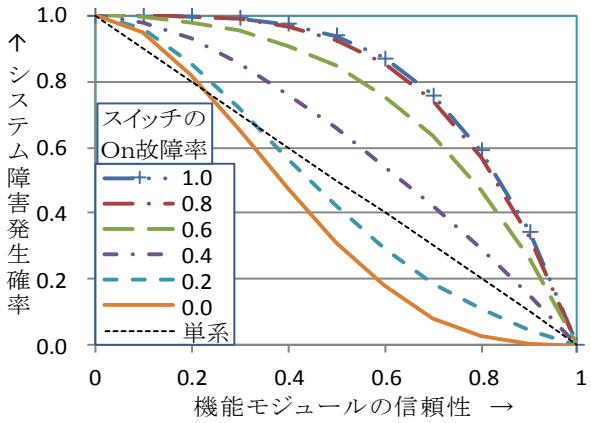


図 15　スイッチオン故障率とシステム障害発生確率

7. おわりに

筆者の提案しているn-フォールトトレラントシステムは、多数決手段も含めてシステム全体でフォールトトレラントを実現している。また、このシステムは障害を起こす前に故障数をカウントすることができる。

スイッチ単体の故障率は非常に小さいので、実用上あまり問題がないかもしれないが、厳格な議論が必要な場合は、故障カウントのために、スイッチの周期的点検（強制オン/オフ）が必要である。

故障カウントでは、スイッチのオフ故障が、機能モジュールの切り離しロジックを誤動作させるので、カウントルールが複雑になる。しかし、本稿で検討の「論理」によって解決することができるだろう。

信頼度の計算は、スイッチのオフ故障時に順序依存形論理の関係が存在し、非常に複雑になっている。本稿の方法は別途厳密な議論が必要だと感じている。

ハザードを取り扱うシステムでは単に信頼度が高いというよりも、平易に理解しやすい安全性のストーリーが重要になってくる。本稿提案のシステムは、多数決回路を含めて、どこが壊れても許容でき、かつ故障数がカウントできるので、運用中でも安全かどうかが判断できる。また、機能モジュールにCPUを搭載しているシステムであれば、ソフトエラーに対して、ロールバックやロールフォワードによりデータの修復も可能である。機能モジュールが4つ以上あれば、ハイブリッド冗長のように3つ以外を待機冗長にして、故障した機能モジュールを交代することで、ロバスト性を高めることもできる。

このシステムは、必ず世の中に普及していくであろう。

文　献

[1] 岩井仁司: “多数決スイッチ回路による n フォールトトレラントシステムの提案”, FIT2010 C-018, (Sept. 2010)

[2] H. Iwai: “A Study of n-Fault-Tolerant System with Voting Switches”, FIT2013 RC-001, (Sept. 2013)

[3] 岩井仁司: “多数決スイッチ回路による n フォールトトレラントシステムの信頼度”, 第 76 回情報処理学会全国大会 2A-6, 2014 年 3 月

[4] J. Von Neumann: “Probabilistic Logics and the synthesis of reliable organisms from unreliable components,” *Automata Studies*, *Ann. of Math. Studies*, no. 34, C. E. Shannon and J. McCarthy, Eds., Princeton University Press, pp. 43-98, 1956.

[5] 南谷崇: “フォールトトレラントコンピュータ”, Ch.4, オーム社, 1991

[6] University of Houston-Clear Lake: “Fault Tolerant Computing”, Lectures and research projects, CENG5334, 2008.

[7] D. Davies and J.F. Wakerly: “Synchronization and matching in redundant systems”, Trans. Compt., Vol.C-27, No.6, pp531-539 (June 1978).

[8] 駒嵜克郎, 池田章弘, 稲田昭夫: “フェールセーフ出力装置”, 特開平 10-340101

[9] 牧野明寛, 江花稔, 野田喜美雄, 金盛正至, 佐々木喬: “異常検出装置”, 特開昭 58-169079

[10] 髙江洲、吉田: “多数決冗長系における多数決回路の高信頼化に関する一検討”, 信学会論文誌, J84-D-1(4), 378-388, Apr. 2001

[11] J.B.Fussell, E.F.Aber and R.G. Rahl: “On the Quantitive Analysis of Priority-AND Failure Logic”, IEEE Trans. Reliability, 25, (1976), 324-326

[12] 佐藤吉信、井上紘一、熊本博光:”人間－ロボット系の安全性評価(第 3 報、順序依存型故障論理の定量化について)”日本機械学会論文集、52 巻 475 号、No.85-0454A, 1986-3

[13] 龍偉、佐藤吉信:”マルコフモデルを用いた順序依存形故障論理の定量化”, 信学技報 Vol.99 No.258 pp.1-6 (1999-8)

[14] 龍偉、佐藤吉信:”順序依存形故障論理の FTA への適用”, 信学技報 R99-25 SSS99-29 pp.7-12 (1999-12)

[15] 大村、下平、陶山、佐藤: “修理系順序依存型論理に関する一考察”, 信学技報 sss2003-26(2003-12)

[16] National Aeronautics and Space Administration: “Computer-Based Control System Safety Requirements”, International Space Station Program SSP-50038B, November 17, 1995, “3.1.2.1.6 Respond to loss of function”, p3-3