

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性

岩井 仁司[†]

Rockwell Personal Lab.

1. はじめに

著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。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。

文献[1]では、この方式の信頼性について、スイッチの故障率を On 故障 / Off 故障に分けずに求めていた。しかし、On 故障は機能モジュールの故障と同時に発生して障害を生じるのに対して、Off 故障は機能モジュールの故障に関係なく障害を生じるため、On 故障率と Off 故障率を分けない議論は、実用性を欠いている。また、Off 故障時の順序依存性も考慮すべき課題である。本稿では、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の信頼性について、スイッチの故障を On 故障率 / Off 故障率に分けて求める。

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。

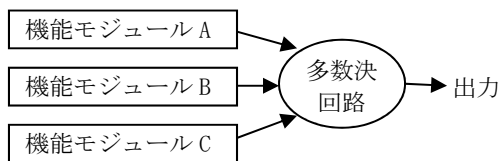


図1 Triple Modular Redundancy (TMR)

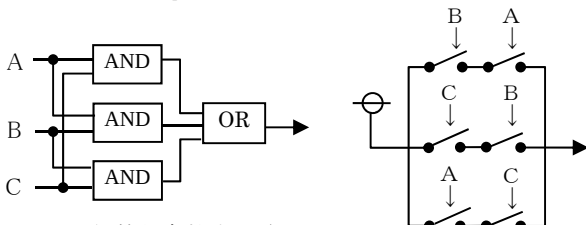


図2 一般的な多数決回路

図3 多数決スイッチ回路

ノイマンの論文[2]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。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 ON 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。([3] など)

3. 著者の提案 [1]

著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。

具体的に、2 故障のフォールトトレラントの例を図4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、故障した機能モジュールを分離し、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、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。

この構成では、高速データ通信が可能であり、また多数決スイッチ回路の冗長性を利用して、機能モジュールが Off にならないよう個々のスイッチを順に On/Off することによりスイッチの故障検知も可能である。

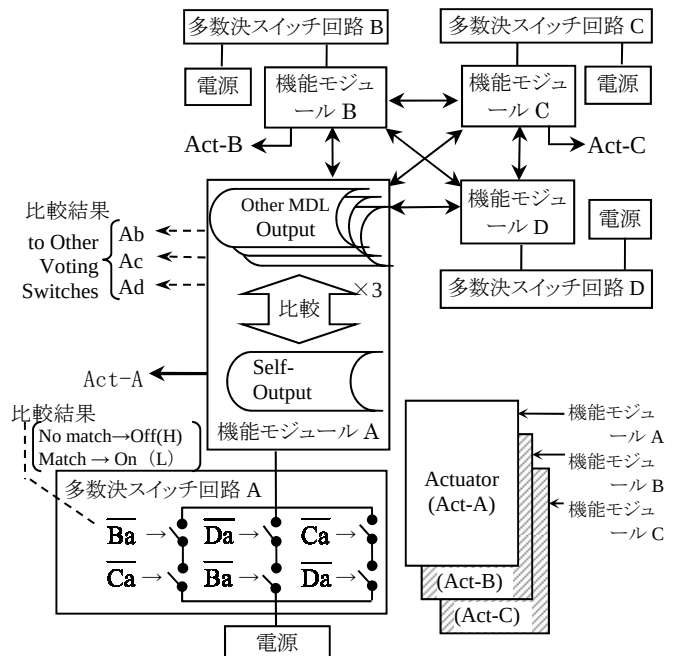


図4 2フォールトトレラント冗長系の例

(1) 構成

構成について、説明する。

- ①機能モジュールは 4 つ。
- ②各機能モジュール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 つの機能モジュールの多数決で 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各機能モジュール内アプリケーションは出力データを生成し、出力直前の状態でバッファに貯める。
- ②機能モジュールどうしが、出力データを交換する。
- ③自分の出力データと他機能モジュールの出力データと比較して、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 個の機能モジュールから 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。

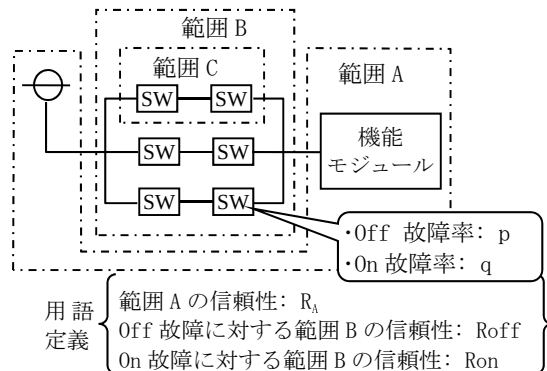
⑤多数決で OFF された機能モジュールの、他系電源スイッチ制御信号は、必然的に Low に落ちる。各多数決スイッチ回路では、Low はスイッチ ON 指令として扱う。これにより、一旦故障として OFF された CPU は、自動的に投票者から外れていく。

4. 信頼性の検討

図5は1つの機能モジュールとその機能モジュールの電源制御する多数決スイッチ回路の構成を示す。

ここで、 p を Off 故障率、 q を On 故障率とする（以降、“故障率”という語は不信頼度と同じ）。即ちスイッチ 1 個の信頼性 $s = 1 - p - q$ とする。

まず、Off 故障率とシステム障害発生率の関係を検討する。検討のための用語、範囲 A, B, C は図 5 を参照のこと。



- ①範囲CのOff故障に対する信頼性： $(1 - p)^2$
(注)「信頼性=1-故障率」なので $(1 - p - q)^2$ であるが、On 故障は故障として症状が現れないので、 $q=0$ として扱う。
- ②範囲CのOff故障率： $1 - (1 - p)^2$
- ③範囲BのOff故障率： $(1 - (1 - p)^2)^3$
- ④範囲BのOff故障に対する信頼性(Roff)：
 $1 - (1 - (1 - p)^2)^3 = 1 - p^3(2 - p)^3$

図5 信頼性検討のための用語

例えば、図 4 で多数決スイッチ回路 A の中の左下のスイッチ Ca が Off 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 Off 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[4]。障害の条件を論理式で表すと次のようになる。(pANDは優先 AND)

<機能モジュール 1 故障とスイッチ 1 故障後、機能モジュール 2 故障目により障害に至るケース>

$$= p \text{AND} (6 \times R_A^2 \times R_{\text{off}}^2 \times (1 - R_A \times R_{\text{off}}) \times p \times 2(1 - p)^2, R_A) \quad (1)$$

<スイッチ 2 故障後、機能モジュール 1 故障目により障害に至るケース>

$$= p \text{AND} (4 \times 3 \times R_A^3 \times R_{\text{off}}^2 \times p^2 \times 4(1 - p)^4, R_A) \quad (2)$$

∴ <Off 故障に対するシステム全体の障害の確率>

$$= (1 - R_A \times R_{\text{off}})^4 + 4 \times (1 - R_A \times R_{\text{off}})^3 \times (R_A \times R_{\text{off}}) + (1) \text{の確率} + (2) \text{の確率} \quad \dots \text{グラフを図 6 に示す。}$$

次に On 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 On 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、

<On 故障に対するシステム全体の障害の確率>

$$= (1 - R_A)^4 + 4 \times (1 - R_A)^3 \times R_A + 6 \times R_A^2 \times (1 - R_A)^2 \times \{2 \times \{1 - (1 - q)^3\} - \{1 - (1 - q)^3\}^2\} + 4 \times (1 - R_A) \times \{1 - (1 - q)^3\} \times R_A^3 \quad \dots \text{グラフを図 7 に示す。}$$

図 6 では、機能モジュールの信頼性が1でも、スイッチ Off 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 7 では機能モジュールの信頼性が1であれば、スイッチ On 故障率=1でも、システム障害とはならない。

スイッチの Off 故障率/On 故障率の許容基準として、「システム全体の信頼性が機能モジュール単系の信頼性より良くなること」を基準にすれば、Off 故障率、On 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性が 0.4~1.0 の範囲)

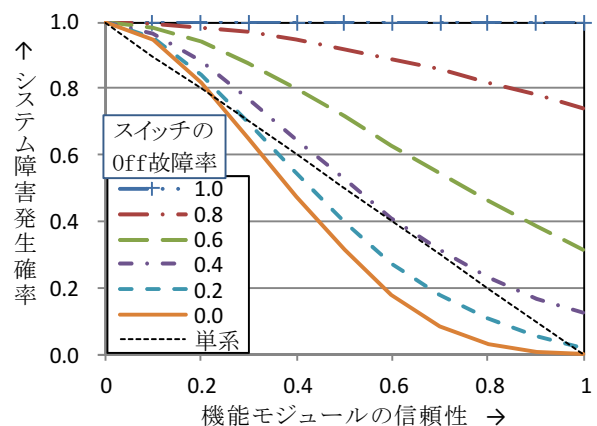


図6 スイッチ Off 故障率とシステム障害発生確率

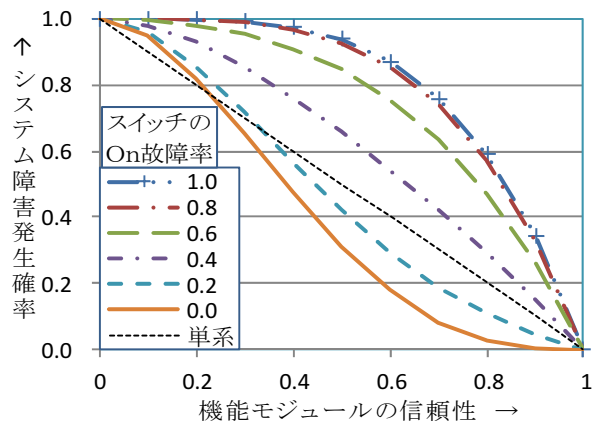


図7 スイッチ On 故障率とシステム障害発生確率

謝辞 信頼性を Off 故障と On 故障に分けて考えるよう唆していただいた金川信康様に感謝申し上げます。

文献

- [1] H.Iwai: “A Study of n-Fault Tolerant system with voting switches”, FIT2013 RC-001, (Sept. 2013)
- [2] 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.
- [3] 高江洲、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
- [4] 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)