故障注入機構を有するフォルトトレラントシステムの 信頼度評価システム[†]

鹿 股 昭 雄*・樋 口 龍 雄**

Reliability Evaluation System of Fault-Tolerant Systems with Fault Injector

Akio KANOMATA* and Tatsuo HIGUCHI**

This paper proposes a microcomputer-based reliability evaluation system which injects artificial fault signals into a hardware prototype under examination and periodically monitors its state. A fault injector which consists of a simple hardware, namely shift registers, a decoder and several gates can generate fault signals whose interarrival times follow a well-known Weibull distribution.

The fault injection is occurred whenever a 20-tuple Tausworthe sequence generated from a maximum length sequence of 34 degree coincides with a pre-defined bit pattern. The bit pattern can be time-variably changed under the control of a microcomputer. As a shape and slope parameter of a Weibull distribution and a simultaneous failure rate among injected signals are adjustable, we can take a heuristic prediction as to an ability and a limitation of fault-tolerance.

Last, as an example of application, evaluation tests for a Triple-Modular-Redundant microcomputer system with resynchronization are carried out. Experimental results approximately agree with analytical results.

Keyword: fault-tolerant system, reliability evaluation system, maximum length sequence, micro-computer

1. ま え が き

一般に、フォルトトレラントシステムの信頼度を評価する手段として、数学的なモデルを用いた解析的な方法¹⁾や、計算機によるシミュレーション²⁾が用いられている。これらは、さまざまなシステムの評価に容易に適用できる融通性をもっているが、プロセッサの

ような複雑なシステムの評価に際しては、現実のシステムに近いモデルを設定することは容易ではなく、必ずしも正しい結果が得られないといった問題点が指摘されている³⁾。

そこで、実際には、被試験システムのハードウェアプロトタイプに故意に間欠的な故障信号を注入し、その動作状態をモニタすることにより、定量的に信頼度を求めることのできる評価システムの実現が期待される。一方、コンピュータシステムのフィールドにおける間欠故障は、故障率が時間と共に減少するワイブル分布に従うことが報告されている⁴⁾。そこで、その信頼度評価システムでは、故障モデルとして、一般に用いられている指数分布に加え、分布の形状を自由に設定できるワイブル分布に従った故障を発生する機能を備えていることが望ましい。

本論文では、このような観点から、マイクロコンピュータに基づく新しい信頼度評価システムの提案を行い、システム構成と機能⁵⁾、およびワイブル分布に従う故障信号の簡易な発生法について述べると共に、本システムが、種々の故障条件のもとで、信頼度を定量的に評価でき、冗長機能の能力や限界を明らかにすることができることを示している。さらに、本システムは、複数の故障信号間で、一部同時故障相関をもたせることが可能なので、これを筆者らが先に提案している内部修復機能をもつ三重化システム^{6),7)}に適用した結果を示す。

2. 信頼度評価システムの概要

提案する評価システムは、各種フォルトトレラントシステムの冗長機能の効果を明らかにするため、被試験システムの状態をオンラインでモニタし、故障時間の分布から信頼度を数値的に求める装置である。

Fig. 1 に三重化システムを試験している評価システムの構成を示す。評価システムは、8ビットマイクロコンピュータを中心とするモニタシステムと故障注

[†] 第 20 回計測自動制御学会学術講演会で発表 (昭56・7)

* 仙台電波工業高等専門学校 宮城県宮城郡宮城町上愛子字北原 1

** 東北大学工学部 仙台市荒巻字青葉

* Sendai Radio Technical College, Miyagi-gun, Miyagi

** Faculty of Engineering, Tohoku University, Sendai (Received September 30, 1981)

(Revised January 18, 1982)

Fig. 1 Block diagram of reliability evaluation system

入機構(Fault injector)より構成される。

故障注入機構は、ランダムな信号をプロトタイプのバスラインなどへ注入して、レジスタやメモリーの内容を強制的に変化させ、故意に故障を誘発する装置である。注入故障信号の統計的な分布の形状や発生率は、信号 $g_1 \sim g_{16}$ を介して、モニタシステムから時变的に制御することができる。

モニタシステムの流れ図を Fig. 2 に示す。コマンド M をキーボードより入力すると、モニタシステムは初期値設定を行ったあと、モニタ動作に入る。初期値設定では、故障度数テーブルのクリアを行い、故障度数の時間きざみ ΔT 、および、制御信号 $g_1 \sim g_{16}$ の初期値とその切替え時刻 $t_{c(j)}$ を設定する。ついで、プロトタイプに restart 信号を送出し、モニタシステムは wait 状態となる。一方、プロトタイプは restart 信号を受けると、レジスタやメモリーに正しい値を書込んだあと、演算処理とその結果の I/O ポートへの出力をサイクリックに実行する。

モニタシステムは、1ms 周期で発生するタイマーからの割込みを受けると、プロトタイプの出力情報が正常か否かの判断を行う。もし、異常ならば、前回の故障時刻からの経過時間 T に対する故障度数を +1 加算し、モニタ動作を続行する。もし、正常であれば、経過時間 T を ΔT ごとに +1 進ませ、あらかじめ設定した時刻 $t_{c(j)}$ に達しておれば、制御信号 $g_1 \sim g_{16}$ を変更して注入故障信号の発生率を切替える。モニタシステムは再び wait 状態となる。

オペレータの指示でモニタ動作が打切られると、故障度数から信頼度が求められ、その数値とグラフが

(* TFF: Table of fault frequency)

Fig. 2 Flow chart of monitor system

CRT ディスプレイ上に表示される。

なお、注入故障信号は、3 ステートバッファで駆動されており、特殊なインタフェースなしで、直接プロトタイプの信号線やバスに接続できる。また、プロトタイプの出力情報の正誤を判断する条件は、キーボードより自由に定めることができるため、本評価システムは、種々のプロトタイプの評価に容易に適用することが可能である。

3. 故障注入機構の構成と性能

3.1 故障注入機構の構成

故障注入機構の構成を Fig. 3 に示す。M 系列から生成される擬似ランダム系列を用いて、互いに独立で、かつ、発生率の等しい基本故障信号 $\bar{e}_0 \sim \bar{e}_{15}$ が作られる。モニタシステムからの信号 $g_1 \sim g_{16}$ は、 $\bar{e}_j$ の発生率を決定する。したがって、 $g_1 \sim g_{16}$ を時变的に変化させることによって、 $\bar{e}_j$ の発生分布の形状を任意に指定することができる。

OR マトリクスは、 $\bar{e}_j$ から故障信号 f_i を合成する回路であり、二つの目的をもっている。第 1 は、 λ を $\bar{e}_j$ の発生率とすると、 f_i の発生率を λ の整数倍のステップで可変にするためであり、第 2 は、複数の故障信号間で同時故障の発生率を設定するためである。たとえば、 $f_0 = \bar{e}_0 \vee \bar{e}_1 \vee \bar{e}_2$ 、 $f_1 = \bar{e}_0 \vee \bar{e}_3$ の場合、 f_0 と f_1 は、それぞれ 3λ 、 2λ の発生率をもち、そ

Fig. 3 Block diagram of fault injector

の中、 λ の発生率で同時に故障信号を出力する。

注入故障信号 $z_{11} \sim z_{14}$ は、プロトタイプ of 任意の信号線にパッチコードで接続される。これらは、通常、高インピーダンスのためプロトタイプに何等影響を与えないが、故障信号 f_i が論理値 0 になると、対応する $z_{11} \sim z_{14}$ を介して異常な信号が注入される。

発生時間間隔が指数分布、および、その拡張であるワイブル分布に従う故障信号の発生法とその性能についてつぎに述べる。

3.2 指数分布に従う故障の注入

擬似不規則信号で知られる M 系列 $\{x_i\}$ から、 L ビットおきに取出した連続 k ビットの系列を x_n とする。ただし、 n は系列 x_n を取出すクロックの周期を単位とする時間を表わす。もし、 $L \geq k$ で、かつ、 L と M 系列の周期が互いに素であるならば、 x_n は、M 系列の周期と同じ周期で (00...0) から (11...1) のすべてのパターンに一樣に分布する擬似ランダム系列 (Tausworthe 系列) となる⁸⁾。

本故障注入機構では、34 ビットシフトレジスタを使用し、(1) 式の特性多項式に基づいて M 系列を発生し、ラッチ回路により、 $L=32, k=24$ の Tausworthe 系列を生成する。その系列がある特定のパターンに一致したときに基本故障信号 f_i を出力する。

$$h(x) = 1 + x + x^2 + x^{27} + x^{34} \quad (1)$$

シフトパルスの 1/32 分周器の出力信号は、Tausworthe 系列を取出すクロックとして用いられると同時に、プロトタイプにシステムクロックとして供給される。したがって、Tausworthe 系列は、 $3.2\mu s$ 周期

で、M 系列発生用シフトレジスタの出力から 24 ビット同時にラッチ回路に送られる。ただし、 $x_1 \sim x_{16}$ はモニタシステムからの制御信号 $g_1 \sim g_{16}$ と論理操作を施されたあと、デコーダのイネーブル信号としてラッチされる。

イネーブル信号が論理値 0、すなわち

$$\bigwedge_{j=1}^{16} (\bar{g}_j \vee x_j) = 1 \quad (2)$$

が成り立つとき、基本故障信号 f_i の中の 1 個が論理値 0 となる。デコーダの入力 $x_{17} \sim x_{20}$ も Tausworthe 系列の一部であり、どの f_i が選択されるかはまったくランダムである。

モニタシステムからの制御信号 $g_1 \sim g_{16}$ の重み w を (3) 式で定義すると、平均 2^w [クロック] ごとにデコーダがイネーブルとなり、デコーダの入力ビット数 4 を考慮すると、 f_i の発生率は (4) 式で与えられる。

$$w \triangleq \sum_{i=1}^{16} g_i \quad (3)$$

$$\lambda = 1/2^{(w+4)} [1/\text{クロック}] \quad (4)$$

ところで、本論文では、時間の単位としてクロック周期を用いているが、1 周期は $3.2\mu s$ であり、容易に一般の時間の単位に変更することができる。

f_i の発生を故障発生とみなした場合、 f_i の信頼度関数は次式で表わされる指数分布となる。ここで、 n はクロック数を表わす。

$$R(n) = \exp(-n/2^{(w+4)}) \quad (5)$$

発生率が $\lambda, 2\lambda, 4\lambda, 8\lambda$ の 4 通りについて、実際に故障信号を発生させ信頼度を求めた。片対数グラフ上にプロットした結果を Fig. 4 に示す。発生信号数は、おのおの約 6,000~20,000 個である。図中、実線は (5) 式より求めた理論値であり、実験値はそれによく

Fig. 4 Reliability function for injected signals (constant failure rate)

Fig. 5 Failure rate of Weibull distribution and its approximation

一致している。

3.3 ワイブル分布に従う故障の注入

ワイブル分布に従う故障率関数は、形状母数 m と尺度母数 λ を用いて、 $\lambda m n^{(m-1)}$ で表わされ、時間と共に増加 ($m > 1$ のとき)、あるいは減少 ($m < 1$ のとき) する。本故障注入機構では、制御をできるだけ簡潔にするため、 λm を基準に 2 のべき乗倍の離散的な値で故障率を近似している。Fig. 5 に $m < 1$ の場合の故障率関数とその近似を示す。 λm の 2^i 倍となる時刻 n_i は、 $n_i = 2^{i/(m-1)}$ で与えられ、したがって、故障率の切替は n_{i-1} と n_i の中間の時刻 $t_{c(i)}$ で行われる。モニタシステムは、切替え時刻に達すると、制御信号 $g_1 \sim g_{16}$ の重み w を、 $m > 1$ の場合は -1 減少させ、 $m < 1$ の場合は $+1$ 増加させる。それにより、故障率は (4) 式に従って 2 倍あるいは $1/2$ 倍となる。なお、重み w の初期値 w_0 は、 $\lambda m = 2^{-(w_0+4)}$ より決定される。

Fig. 6 は、 $m = 0.5, 0.7, 1.0, 2.0$ の場合について、おのおの 1000 個の基本故障信号を計算機シミュレーションによって発生し、発生時間ごとの累積頻度をワイブル確率紙にプロットしたものである。グラフを重ねて表わすため、時間軸は適当にスケールしてある。おのおの m の傾きを図に実線で示したが、データはそれにほぼ一致しており、故障注入信号として十分に利用することができる。

4. 三重化システムへの適用

評価システムの適用例として、筆者らが先に提案している内部修復機能をもつ三重化冗長マイクロコンピュータ^{6),7)}の信頼度評価を行った。このシステムは、

Fig. 6 Weibull plot of cumulative distribution function for injected signals

RALU (Register, Arithmetic and Logic Unit) とメインメモリーが三重化されており、データが転送されるごとに照合検査が行われる。不一致が検出されると、多数決の結果で該当アドレスの内容が自動的に修復される。以上の操作がマイクロ命令レベルで行われる。

実験は解析による評価との比較を行うため、以下の単純な条件のもとで行った。

(1) 故障はレジスタのアドレス線 3 ビットと書込み線に注入する。したがって、ランダムに選択されたレジスタにその時点の内部バスの値が書込まれる。しかし、そのとき実行中のマイクロ命令によっては、故障が誘発されない場合がある。今回の実験プログラムでは、その割合は約 30% である。

(2) 3 個の RALU に注入される故障信号は、それぞれ発生率 5λ (ただし、 $\lambda = 0.7 \times (1/2^{18})$ [1/クロック]) である。) の指数分布に従う。なお、同時故障相関として、Fig. 7 に示す 4 種類のモードについて実験する。

(3) プロトタイプは、すべてのレジスタの値を用いて論理演算を行い、その結果を I/O ポートに出力する操作をサイクリックを行う。1 サイクルのクロック数 N は 425 である。

三重化システムの信頼度評価実験の結果を Fig. 8 に示す。図中の実線は、数学的なモデルから解析的に得られた次式に基づく値であり、文献 6) から導くことができる。

$$R(n) = \exp\{-3(1-r)N\lambda_1^2 + 3\lambda_2 + \lambda_3\}n \quad (6)$$

ここで、 r は二つ以上の RALU 間で同一アドレスのレジスタが故障したにもかかわらず、誤った桁が互いに異なっているため、多数決の結果を用いて正しく修

MODE	λ_1	λ_2	λ_3
1	5λ	0	0
2	4λ	0	λ
3	3λ	λ	0
4	2λ	λ	λ

$\lambda = 0.7/2^{18} [1/\text{clock}]$

Fig. 7 Venn diagram for dependent-failures and test condition

Fig. 8 Reliability function for TMR system with resynchronization

復できる割合である。1語8ビットの場合、 r は約0.093となる。評価実験の結果は解析的な評価の値とよく一致しており、本システムの妥当性が明らかにされた。

5. む す び

本論文では、複雑なフォルトトレラントシステムの信頼度をできるだけ正確に評価するため、対象システムのプロトタイプにランダムな故障信号を間欠的に注入し、その状態をオンラインでモニタするシステムの構成について述べた。注入する故障信号としては、指数分布を拡張したワイブル分布に従う信号を扱うことができ、その分布の形状や尺度母数および信号間の同時故障相関を比較的柔軟に設定することができた。したがって、種々の条件のもとで、冗長機能の能力や限

界を発見的に評価することが可能である。具体的な適用例として、三重化システムの信頼度について評価実験を行ったところ、解析的な結果とよく一致した結果が得られた。

本評価システムでは、定量的に信頼度を評価するため、注入する故障信号を人為的に生成したが、実際の雑音（たとえば、電波雑音など）に対しても、プロトタイプでのモニタリングと信頼度の評価機能は、現行のまま直ちに適用することができ、汎用性のある信頼度評価システムとなっている。

終りに、日ごろ有益な御討論をいただく豊橋技術科学大学 秋丸春夫教授および田所嘉昭助教授に深謝する。

参 考 文 献

- 1) Y. W. Ng and A. Avizienis: ARIES-An Automated Reliability Estimation System, Proc. 1977 Annual Reliability and Maintainability Symposium, 108/113 (1977)
- 2) H. O. Levy and R. B. Conn: A Simulation Program for Reliability Prediction of Fault Tolerant Systems, in Dig. 1975 Int. Symp. Fault-Tolerant Computing, 104/109 (1975)
- 3) A. Avizienis: Fault-Tolerance: The Survival Attribute of Digital Systems, Proc. of the IEEE, 66, 10, 1109/1125 (1978)
- 4) S. R. McConnell, D. P. Siewiorek and M. M. Tsao: The Measurement and Analysis of Transient Errors in Digital Computer Systems, in Dig. 1979 Int. Symposium Fault-Tolerant Computing, 67/70 (1979)
- 5) 鹿股, 樋口: プロトタイプによるフォルトトレラントシステムの信頼度評価, 第20回SICE学術講演会予稿集, 363/364 (1981)
- 6) 鹿股, 樋口: マイクロプログラム方式による制御用マイクロコンピュータシステムの高信頼化, 信学技報, EMC 79-41, 19/24 (1979)
- 7) 鹿股, 樋口: マイクロプログラム方式による制御用マイクロコンピュータシステムの高信頼化, 信学論, (D), J64-D, 2, 174/175 (1981)
- 8) 柏木: M系列再発見, 計測と制御, 20-2, 236/245 (1981)