n 個のウォッチドッグプロセッサをもつフォールトトレラントシステムの信頼性評価

今泉充啓† 安井一民† 中川覃夫†

近年，半導体集積回路技術の著しい進展と共に，マイクロプロセッサの利用が広範な分野で促進されており，その高信頼化への要求が高まっている．マイクロプロセッサは，使用環境の悪化やノイズの影響，ハードウェア障害，またはプログラムバグ等によって，ある確率で異常状態となる．このため，高信頼性が要求されるマイクロプロセッサには，これらの異常を確実に検出する機能が必要であり，比較的安価なウォッチドッグタイマが利用されている．ウォッチドッグプロセッサは，このウォッチドッグタイマの機能を拡張したものであり，対象とする主プロセッサの動作状態を，処理プロセスにおける特徴情報のオンライン監視によって，システムレベルの誤り検出を行う簡単かつ小規模な副プロセッサである．ここでは，n 個のウォッチドッグプロセッサをもつフォールトトレラントシステムの信頼性と経済性の問題を考察する．すなわち，主プロセッサとウォッチドッグプロセッサが，独立な確率分布に従って異常状態が発生すると仮定した信頼性モデルを設定する．そのとき，主プロセッサが動作障害に至るまでの平均時間や信頼度の導出，さらに期待費用を最小にする最適なウォッチドッグプロセッサの個数を議論し，数値例による考察と評価を行う．

Reliability Evaluations of a Fault-Tolerant System with n Watchdog Processors

MITSUHIRO IMAIZUMI,† KAZUMI YASUI† and TOSHIO NAKAGAWA†

As computer technology has remarkably developed, the demand for detection of errors in a microprocessor has increased. A watchdog processor is a small and simple coprocessor that detects errors by monitoring the behavior of a microprocessor, i.e., it detects a large number of errors by monitoring the control flow and memory access behavior. It is an interesting problem to know how much the reliability of a microprocessor with watchdog processors improves. This paper considers a fault-tolerant system where a main processor has n watchdog processors with self-checking. When errors of the main processor have occurred, a watchdog processor detects them with a certain probability and resets the processor to an initial state. Otherwise, the processor goes to a fault state. If a watchdog processor fails, it detects failure with itself and one of other processors in standby begins to monitor the processor again. The above procedures are repeated until n watchdog processors have failed. We derive the reliability measures such as mean time, reliability and expected cost until the fault of the main processor. An optimal number n^* of watchdog processors which minimizes the expected cost is discussed analitically. Finally, numerical examples are given.

1. はじめに

近年，半導体集積回路技術の著しい進展と共に，マイクロプロセッサの利用が広範な分野で促進されており，その高信頼化への要求が一段と高まっている．一例を挙げると，自動車のようにシステム故障が人命に係わるようなシステムにも，マイクロプロセッサは数多く使用され，その高信頼化は不可欠な要素となっている．

† 愛知工業大学経営工学科
Department of Industrial Engineering, Aichi Institute of Technology

一般に，マイクロプロセッサ（microprocessor: μP）は使用環境の悪化やノイズの影響，ハードウェア障害，またはプログラムバグ等によって，ある確率で異常状態となる[1),2)]．このため高信頼性が要求される μP には，これらの異常を確実に検出する機能が必要であり，従来，比較的安価なウォッチドッグタイマ（watchdog timer: WDT）が利用されている[2),3)]．ウォッチドッグプロセッサ[4)~6)]（watchdog processor: WDP）は，この WDT の機能を拡張したものであり，対象とする主プロセッサ（main processor: MPu）の動作状態を，処理プロセスにおける特徴情報のオンライン監視によって，システムレベルの誤り検出を行う，簡単か

つ小規模な副プロセッサである[1].

ここでは，n 個の WDP をもつフォールトトレラントシステムを設定し，信頼性と経済性の問題を考察する．一般的な高信頼化システムに対する評価の問題は，従来から広範に取り扱われているが，その評価モデルの多くは，対象システム自身における各種の冗長性を含めた高機能化によるものが中心であり，シミュレーション手法を用いて評価したものが，その主流である[7)~9)].

ここでのモデル化は，システムの実行系（MPu）が単一で，その障害処理系（WDP）が多重化されたシステム構成であり，実行系を含むシステム全体の信頼性の向上を主目的として，その評価尺度を解析的に導出し，考察を行う．ここで，単一の WDP が MPu の異常状態を検出できない場合，MPu は結果として暴走状態に陥ると考えられ，それを防止するための WDP の多重化の個数を，経済的・信頼性的な評価尺度として示すために，n 個の多重化構成としてモデルを設定する．

MPu には，ある確率分布に従って異常状態が発生し，WDP によりその異常を検出する．すなわち，MPu に異常が発生した場合，その異常は，ある確率（WDP のカバレッジと呼ぶ）で検出され，MPu を自動リセットし，初期状態へ復帰させる．WDP は全部で n 個あり，常時は 1 個が MPu を監視し，他は待機状態にある．WDP は自己検査機能によって，自己の異常を検出し，予備の WDP に自動的に切り替わり，MPu の監視を再開する．そのとき，MPu が動作障害に至るまでの平均時間や信頼度の導出，さらに期待費用を最小にする最適な WDP の個数を議論し，数値例による考察と評価を行う．

2. モデルの設定と動作障害発生までの平均時間

モデルの概要を**図 1** に示す．ここでは，MPu の各処理プロセスにおける特徴情報を WDP によってオンライン監視し，その一致・不一致によって MPu の正常・異常を判定する．もし，MPu を異常と判定（異常検出）した場合，その異常の同定（診断による異常箇所・原因の特定）をするのではなく，MPu が異常状態にあるという現状から速やかに MPu をリセット（異常状態の復旧）し，処理プロセスの初期状態に復帰させる．いわば，コンピュータシステムにおける再試行（retry）と同様の手法によって，MPu の異常状態からの回復を行うこととする．

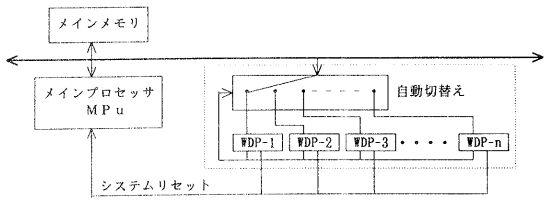


図 1 n 個の WDP をもつモデルの概要
Fig. 1 Outline of the model with n watchdog processors.

(1) MPu は，メモリアクセスミスやコントロールミス等により，一般分布 $F(t)$（平均 $1/\lambda$）に従って異常状態になる．
  (a) MPu の異常は，監視用の WDP によりカバレッジ p $(0 < p < 1)$ で検出され，システムリセットによって初期状態へ復帰する．
  (b) システムリセットに要する時間は，便宜上無視できる．

(2) WDP は，自己のハードウェア障害等により，指数分布 $(1-e^{-\alpha t})$ に従って異常状態になる．この場合，MPu の異常を検出することはできない．
  (a) WDP は，自己検査機能をもち，自己の異常状態を確率 θ で検出し，待機中の WDP に自動的に切り替わる．新しい WDP は，MPu をリセットして監視を再開する．この一連の自動切替え処理時間は，指数分布 $(1-e^{-\beta t})$ に従って行われる．一般に，この平均時間 $1/\beta$ は $1/\alpha$ よりも小さいと考えられるので，$\beta > \alpha$ と仮定する．
  (b) 待機中の WDP には，異常は発生しない．

(3) MPu の異常を WDP が検出できない場合，あるいは MPu が異常状態となったとき，WDP に異常が発生中または切り替え中の場合，MPu は動作障害に至る．

以上の仮定のもとで，システムの各状態を次のように定義する．

状態 i: i 個目の WDP が MPu を監視 $(i = 1, 2, \cdots, n)$.

状態 F: MPu の動作障害発生．

システムの状態を上のように定義すると，各状態は状態 F を吸収状態にもつマルコフ再生過程[10)]を形成し，各状態間の推移は**図 2** のように表される．

マルコフ再生過程における 1 ステップ推移確率時間分布を $Q_{i,j}(t)$ $(i = 1, 2, \cdots, n;\ j = 1, 2, \cdots, n, F)$ とし，そのラプラス・スティルチェス（LS）変換を $q_{i,j}(s)$ とする．そのとき，付録 1 より，

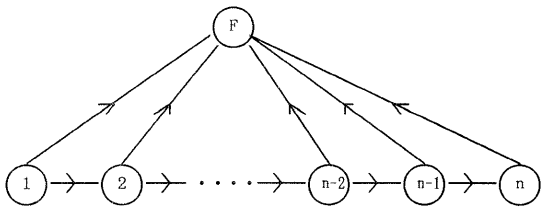


図2 システムの状態推移図
Fig. 2 Transition diagram between system states.

$$q_{i,i}(s) = pf(s+\alpha) \qquad (i = 1,2,\cdots,n), \quad (1)$$

$$q_{i,F}(s) = \frac{1}{1-pf(s+\alpha)}\left[(1-p)f(s+\alpha) + (1-\theta)(f(s)-f(s+\alpha)) + \frac{\alpha\theta}{\alpha-\beta}(f(s+\beta)-f(s+\alpha))\right] \qquad (i = 1,2,\cdots,n-1), \quad (2)$$

$$q_{i,i+1}(s) = \frac{1}{1-pf(s+\alpha)} \cdot \frac{\alpha\beta\theta}{\alpha-\beta}\left[\frac{1}{s+\beta} \times (1-f(s+\beta)) - \frac{1}{s+\alpha}(1-f(s+\alpha))\right] \qquad (i = 1,2,\cdots,n-1), \quad (3)$$

$$q_{n,F}(s) = \frac{1}{1-pf(s+\alpha)}(f(s)-pf(s+\alpha)), \quad (4)$$

を得る．ここで一般に $f(s)$ は $F(t)$ の LS 変換を表し，$f(s) \equiv \int_0^\infty e^{-st}dF(t)$ とおく．

次に，MPu が動作障害に至るまでの平均時間 $\ell(n)$ を求めよう．システムが時刻 0 で状態 1 から出発したとき，時刻 t までに初めて状態 F へ推移する経過時間分布 $H_n(t)$ は，次式で与えられる．

$$H_n(t) = Q_{1,F}(t) + Q_{1,2}(t) * Q_{2,F}(t) + \cdots + Q_{1,2}(t) * \cdots * Q_{n-1,n}(t) * Q_{n,F}(t). \quad (5)$$

式 (5) を LS 変換し，式 (1)～(4) を用いて整理することによって，

$$h_n(s) = \sum_{j=0}^{n-2}\left[\frac{\alpha\beta\theta}{\alpha-\beta} \cdot \frac{1}{1-pf(s+\alpha)} \times \left\{\frac{1-f(s+\beta)}{s+\beta} - \frac{1-f(s+\alpha)}{s+\alpha}\right\}\right]^j \times \frac{1}{1-pf(s+\alpha)} \cdot \left[(1-p)f(s+\alpha) + (1-\theta)(f(s)-f(s+\alpha)) + \frac{\alpha\theta}{\alpha-\beta}(f(s+\beta)-f(s+\alpha))\right] + \left[\frac{\alpha\beta\theta}{\alpha-\beta} \cdot \frac{1}{1-pf(s+\alpha)} \times \left\{\frac{1-f(s+\beta)}{s+\beta} - \frac{1-f(s+\alpha)}{s+\alpha}\right\}\right]^{n-1} \times \frac{1}{1-pf(s+\alpha)}(f(s)-pf(s+\alpha)) \qquad (n = 1,2,\cdots), \quad (6)$$

を得る．ここで，$\sum_{j=0}^{-1} \equiv 0$ とおく，したがって，MPu が動作障害に至るまでの平均時間 $\ell(n)$ を，次のように求めることができる．

$$\ell(n) \equiv \int_0^\infty t dH_n(t) = \lim_{s\to 0}\frac{d}{ds}[-h_n(s)] = \frac{1}{1-pf(\alpha)}\left[\frac{1-A^{n-1}}{1-A}B + \frac{1}{\lambda}A^{n-1}\right] \qquad (n = 1,2,\cdots). \quad (7)$$

ここで，

$$A \equiv \frac{\theta}{\alpha-\beta} \cdot \frac{\alpha(1-f(\beta)) - \beta(1-f(\alpha))}{1-pf(\alpha)},$$

$$B \equiv \frac{\theta}{\alpha-\beta} \cdot \left[\frac{\alpha(1-f(\beta))}{\beta} - \frac{\beta(1-f(\alpha))}{\alpha}\right] + \frac{1}{\lambda}(1-\theta).$$

なお，$A = q_{i,i+1}(0)$ であるから，$0 < A < 1$ である．明らかに，$n = 0$ のとき，いわば WDP を考慮しないとき，$h_0(s) = f(s)$，$\ell(0) = 1/\lambda$ を得る．

3. 信頼度に関する解析

MPu が，時刻 t までに動作障害に至らない確率を $R_n(t)$ とし，$R_n(t) \equiv 1 - H_n(t)$ と定義する．いわば $R_n(t)$ は，MPu が n 個の WDP をもつときの信頼度関数を表している．

特に，MPu の異常状態発生時間分布が指数分布 $F(t) = 1 - e^{\lambda t}$ に従うとき，式 (6) の $h_n(s)$ は付録 2 により，次式のように書き直される．

$$h_n(s) = \frac{\lambda}{s+\lambda}\left\{1 - \frac{sp}{s+\alpha+\lambda(1-p)} \times \sum_{j=0}^{n-1}\left[\frac{\alpha\beta\theta}{\{s+\alpha+\lambda(1-p)\}(s+\beta+\lambda)}\right]^j\right\} \qquad (n = 1,2,\cdots). \quad (8)$$

よって，$h_n(s)$ をラプラス逆変換することにより，付録 3 から，$R_n(t)(n = 0,1,2,\cdots)$ を順次求めることができる．例えば，$R_1(t)$ は，

$$R_1(t) = e^{-\lambda t} - \frac{p\lambda}{\alpha-\lambda p}(e^{-\{\alpha+\lambda(1-p)\}t} - e^{-\lambda t}), \quad (9)$$

と表される．特に，$n \to \infty$ のとき，付録 4 から，

$$R_\infty(t) = \lim_{n\to\infty} R_n(t)$$
$$= e^{-\lambda t} + p\lambda\left[\frac{\beta+\lambda-v_1}{(v_1-v_2)(v_1-\lambda)}e^{-v_1 t} - \frac{\beta+\lambda-v_2}{(v_1-v_2)(v_2-\lambda)}e^{-v_2 t} + \frac{\beta}{(v_1-\lambda)(v_2-\lambda)}e^{-\lambda t}\right], \quad (10)$$

となる．ここで，

$$v_1 \equiv \frac{1}{2}\left\{\alpha+\beta+\lambda(2-p) + \sqrt{(\alpha-\beta-\lambda p)^2+4\alpha\beta\theta}\right\},$$
$$v_2 \equiv \frac{1}{2}\left\{\alpha+\beta+\lambda(2-p) - \sqrt{(\alpha-\beta-\lambda p)^2+4\alpha\beta\theta}\right\},$$

とおく．

4. 期待費用を最小にする最適方策

最初に，単位時間当たりの期待費用を求めよう．1個当たりのWDPの費用をc_1とし，MPuの動作障害に伴う損失費用をc_2として，n個のWDPをもつときの単位時間当たりの期待費用$C(n)$を次のように定義する．

$$C(n) \equiv \frac{nc_1+c_2}{\ell(n)}. \quad (11)$$

式(11)の期待費用$C(n)$を最小にするWDPの個数n^*を求める．式(7)から，

$$C(n) = \frac{nc_1+c_2}{\frac{1}{1-pf(\alpha)}\left[\frac{1-A^{n-1}}{1-A}B+\frac{1}{\lambda}A^{n-1}\right]} \quad (n=1,2,\cdots). \quad (12)$$

不等式$C(n+1)-C(n)\geq 0$とおくと，

$$\frac{\frac{B}{1-A}(1-A^{n-1})+\frac{1}{\lambda}A^{n-1}}{A^{n-1}(1-A)} - (n-1)\cdot\left[\frac{B}{1-A}-\frac{1}{\lambda}\right] \geq \frac{c_1+c_2}{c_1}\left[\frac{B}{1-A}-\frac{1}{\lambda}\right], \quad (13)$$

を得る．式(13)において，$B/(1-A)-1/\lambda\leq 0$，すなわち$\lambda B\leq 1-A$の場合，$C(n)$はnの単調増加関数となり，$n^*=0$となる．

さらに，$\lambda B>1-A$の場合，式(13)を簡単化して，

$$\frac{1-A^{n-1}+D}{A^{n-1}(1-A)} - (n-1) \geq \frac{c_1+c_2}{c_1}, \quad (14)$$

と表す．ここで，

$$D \equiv \frac{1-A}{\lambda B-(1-A)},$$

とおく．式(14)の左辺を$L(n)$とおくと，

$$L(n)-L(n-1) = \frac{1-A^{n-1}+D}{A^{n-1}} > 0, \quad (15)$$

となり，

$$L(1) = \frac{1}{\lambda B-(1-A)}, \quad (16)$$

$$L(\infty) = \infty, \quad (17)$$

であるから，$L(n)$は$L(1)$から∞までのnの単調増加関数となる．よって，$L(1)<(c_1+c_2)/c_1$，すなわち$\lambda B-(1-A)>c_1/(c_1+c_2)$ならば，式(14)を満たす$n^*(>1)$は必ず存在する．逆に，$L(1)\geq(c_1+c_2)/c_1$，すなわち$\lambda B-(1-A)\leq c_1/(c_1+c_2)$ならば，$n^*=1$である．

以上より，次のような結論を得ることができる．

(i) もし，$\lambda B-(1-A)\leq$ならば，$n^*=0$，期待費用$C(0)=\lambda c_2$であり，WDPを使用しないほうがよい．

(ii) もし，$0<\lambda B-(1-A)\leq c_1/(c_1+c_2)$ならば，$n^*=1$である．

(iii) もし，$\lambda B-(1-A)>c_1/(c_1+c_2)$ならば，式(14)を満たす有限で唯一の$n^*$ (>1)が存在する．

5. 数値例による考察と評価

3章で求めた$R_n(t)$，および4章で求めた期待費用$C(n)$を最小にする最適方策について，具体的な数値を求めよう．ここでは，自動車などに使用されているμPやWDTの経験的なパラメータの値[11]を適用し，解析で得られた方策についての大略の傾向を把握することとする．まず，MPuの異常発生の確率分布を$F(t)=1-e^{-\lambda t}$と仮定し，MPuの平均異常発生間隔として，μPの平均ハングアップ間隔（1日～10日）を対応させ$1/\lambda=1$（日）とする．WDPの平均異常発生間隔は，WDTの平均異常発生間隔（1か月～1年）を対応させて$1/\alpha=30\sim365$（日）（可変）とする．なお，WDPの平均切替え処理時間については，便宜的に，WDP固有のクロック（30 MHzと仮定）の100倍程度と考えて，$1/\beta=(1/30)\times10^{-6}\times100$（秒）と仮定する．さらに，WDPの自己異常検出確率を$\theta=0.8\sim0.99$（可変），WDPによるカバレッジを$p=0.8\sim0.99$（可変）とする．期待費用を求めるため，WDPの1個当たりの費用c_1を単位費用とし，MPuの動作障害に伴う損失費用を$c_2/c_1=10\sim10^7$（可変）と仮定する．

以上の仮定のもとで，$1/\alpha=30$（日），$p=0.99$，$\theta=0.8$のとき，信頼度$R_n(t)$の推移を**図3**に示す．

図3によれば，明らかに$R_n(t)$はnの増大に伴っ

て大きくなる．$n=0$，いわばWDPを使用しない場合に比べ，$n \geq 1$ の場合，$R_n(t)$ は急激に増加するが，その増加率は n の増大とともに次第に小さくなり，やがて $R_\infty(t)$ に収束する．いわば，期待すべき $R_n(t)$ の大きさにもよるが，この数値例から，有効な n の値は，大略3個位までで十分であろうと推測される．

次に，$1/\lambda = 1$（日），$p=0.8$，$\theta=0.8$ のとき，期待費用を最小にする最適な n^* の数値例を**表1**に示す．

表1によれば，n^* は $1/\alpha$ の増大に伴い減少し，c_2/c_1 が大きくなるに従って増加する．例えば，$1/\alpha = 180$（日），$c_2/c_1 = 10^3$ のとき，最適なWDPの個数は $n^*=2$ であることがわかる．

なお，システムにスペース上の制約を受ける場合や，システムを簡潔に設計したい場合，表1の結果から，$1/\alpha$ の大きさに対応した性能をもつWDPを適宜組み合わせることによって，n^* を小さくできることもわかる．

また，$1/\lambda = 1$（日），$1/\alpha = 180$（日）のとき，WDPのカバレッジ p，自己検出確率 θ を可変としたときの n^* に対応して，MPuが動作障害に至るまでの平均時間 $\ell(n^*)$ の数値例を**表2**に示す．

表2によれば，$\ell(n^*)$ は，c_2/c_1，p，θ が大きくなるに従って増大する．また，MPuが動作障害に至るまでの平均時間への寄与は，WDPの自己異常検出確率 θ よりも，カバレッジ p の方が，より大きいことがわかる．すなわち，WDPに関して，MPuの信頼性を向上させるためには，θ の向上よりもカバレッジ p の向上がより重要であるといえる．

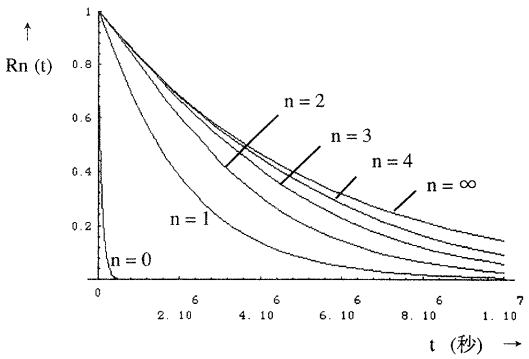


図3 $p=0.99$，$\theta=0.8$ のとき，信頼度 $R_n(t)$
Fig. 3 Reliability $R_n(t)$ when $p=0.99$ and $\theta=0.8$.

表1 $1/\lambda = 1$（日），$p=0.8$，$\theta=0.8$ のとき，$C(n)$ を最小にする最適な n^*
Table 1 Optimal number n^* to minimize $C(n)$ when $1/\lambda = 1$ day, $p=0.8$ and $\theta=0.8$.

$1/\alpha$	c_2/c_1						
（日）	10	10^2	10^3	10^4	10^5	10^6	10^7
30	1	2	4	5	6	7	8
60	1	2	3	4	5	5	6
90	1	2	3	3	4	5	6
180	1	2	2	3	3	4	5
365	1	1	2	2	3	3	4

6. おわりに

MPuの信頼性向上問題については，従来，諸種の方法が提案されているが，ここでは，MPuの動作状態を n 個の待機冗長方式によるWDPで監視するモデルを設定した．MPuおよびWDPの異常発生間隔，WDPによるカバレッジ，待機中のWDPへの切替え処理時間等を考慮することによって，MPuが動作障害に至るまでの平均時間を求め，信頼度関数の導出や，単位時間当たりの期待費用を最小にする最適なWDPの個数について議論した．

数値例による信頼度関数の推移から，より高い信頼度が要求される場合，少なくとも1個のWDPの設定が有効であることが示された．また，期待費用を最小にする最適なWDPの個数は，$1/\alpha$ の増大に伴い減少し，c_2/c_1 が大きくなるに従って増加する傾向を示した．さらに，WDPの機能・性能に関して，MPuの高

表2 $1/\lambda = 1$（日），$1/\alpha = 180$（日）のとき，$\ell(n^*)$ の数値例
Table 2 Numerical values for $\ell(n^*)$ when $1/\lambda = 1$ day and $1/\alpha = 180$ days.

p	θ	c_2/c_1						
		10	10^2	10^3	10^4	10^5	10^6	10^7
0.8	0.8	0.423	0.430	0.430	0.430	0.430	0.430	0.430
	0.9	0.423	0.431	0.431	0.431	0.431	0.431	0.431
	0.99	0.423	0.432	0.432	0.432	0.432	0.432	0.432
0.9	0.8	0.823	0.854	0.855	0.855	0.855	0.855	0.855
	0.9	0.823	0.858	0.860	0.860	0.860	0.860	0.860
	0.99	0.823	0.861	0.863	0.864	0.864	0.864	0.864
0.99	0.8	7.156	7.733	7.780	7.784	7.785	7.785	7.785
	0.9	7.353	8.103	8.181	8.189	8.190	8.190	8.190
	0.99	8.217	8.546	8.587	8.592	8.593	8.593	8.593

$\times 10^6$（秒）

信頼化のためには，WDP の自己検査機能 θ よりは，カバレッジ p の向上が，より重要であることがわかった．なお，システム設計上の要請から WDP の個数を小さくするためには，MPu の性能に対応した WDP を組み合わせることが有効である．

このような MPu の信頼性評価の問題は，その利用分野の拡大とともに今後ますます重要な課題となることが考えられ，この方面に対する多くの研究が期待される．

参考文献

1) 南谷 崇：フォールトトレラントコンピュータ，p.272，オーム社 (1991).
2) 不破 泰，中村八束：ウォッチドッグタイマの有効性に関する統計的考察，信学論 (D)，Vol.J71-D，No.11，pp.2414–2423 (1988).
3) 並木好弘，古賀義亮：自己検査性ウォッチドッグタイマの一構成法，信学論 (D)，Vol.J68-D，No.8，pp.1543–1544 (1985).
4) Mahmood, A. and McCluskey, E.J.: Concurrent Error Detection Using Watchdog Processors—A Survey, *IEEE Trans. Comput.*, Vol.37, No.2, pp.160–174 (1988).
5) Lu, D.J.: Watchdog Processors and Structural Integrity Checking, *IEEE Trans. Comput.*, Vol.C-31, No.7, pp.681–685 (1982).
6) Saxena, N.R. and McCluskey, E.J.: Control-flow Checking Using Watchdog Assists and Extended-precision Checksums, *IEEE Trans. Comput.*, Vol.39, No.4, pp.554–559 (1990).
7) 電子情報通信学会編：電子情報通信ハンドブック，p.3052，オーム社 (1988).
8) 情報処理学会編：情報処理ハンドブック，p.1596，オーム社 (1989).
9) 情報システムハンドブック編集委員会編：情報システムハンドブック—情報システムの実際，p.2-513，培風館 (1989).
10) Osaki, S.: Applied Stochastic System Modeling, Springer-Verlag, Berlin (1992).
11) 安井一民，中川覃夫，原田義久：ウォッチドッグタイマをもつマイクロプロセッサシステムの信頼性評価，信学論 (A)，Vol.J77-A，No.11，pp.1510–1516 (1994).

付　録

1. $Q_{i,j}(t)$ $(i=1,2,\cdots,n;\ j=1,2,\cdots,n,F)$ の導出

システムが時刻 $t=0$ で状態 i から出発し，時刻 t までに次の状態 j へ推移する確率分布 $Q_{i,j}(t)$ は次式で表される．

$$Q_{i,i}(t)=p\int_0^t e^{-\alpha t}dF(t) \quad (i=1,2,\cdots,n), \tag{A.1}$$

$$\begin{aligned}Q_{i,F}(t)=&\left[\sum_{j=1}^{\infty}Q_{i,i}^{(j-1)}(t)\right]\\&*\left[(1-p)\int_0^t e^{-\alpha t}dF(t)\right.\\&+(1-\theta)\int_0^t(1-e^{-\alpha t})dF(t)\\&\left.+\int_0^t\frac{\alpha\theta}{\alpha-\beta}(e^{-\beta t}-e^{-\alpha t})dF(t)\right]\\&(i=1,2,\cdots,n-1),\end{aligned} \tag{A.2}$$

$$\begin{aligned}Q_{i,i+1}(t)=&\left[\sum_{j=1}^{\infty}Q_{i,i}^{(j-1)}(t)\right]\\&*\left[\int_0^t\frac{\alpha\beta\theta}{\alpha-\beta}(e^{-\beta t}\right.\\&\left.-e^{-\alpha t})(1-F(t))dt\right]\\&(i=1,2,\cdots,n-1),\end{aligned} \tag{A.3}$$

$$\begin{aligned}Q_{n,F}(t)=&\left[\sum_{j=1}^{\infty}Q_{n,n}^{(j-1)}(t)\right]\\&*\left[(1-p)\int_0^t e^{-\alpha t}dF(t)\right.\\&\left.+\int_0^t(1-e^{-\alpha t})dF(t)\right].\end{aligned} \tag{A.4}$$

ここで，$*$ は分布関数のたたみこみを表し，一般に $a^{(i)}(t)$ は分布 $a(t)$ の i 重たたみこみを表す．すなわち，$a^{(i)}(t)\equiv a^{(i-1)}(t)*a(t)$，$a(t)*b(t)\equiv\int_0^t b(t-u)da(u)$ である．

たとえば，$Q_{n,F}(t)$ は，n 個目の WDP が MPu を監視中のとき，MPu に異常が発生し，WDP は正常であるが MPu の異常を検出できない，または，MPu が正常動作中に WDP の異常が発生し，その後 MPu に異常が発生した，のいずれかのために，MPu が動作障害状態 F へ推移する場合の確率分布を表す．

2. 式 (8) の導出

式 (6) において，$F(t)$ の LS 変換を $f(s)=\lambda/(s+\lambda)$ とし，式の簡単化のため，$x\equiv\alpha+\lambda(1-p)$，$y\equiv\beta+\lambda$ とおくと，

$$
\begin{aligned}
h_n(s) &= \sum_{j=0}^{n-2}\left[\frac{\alpha\beta\theta}{(s+x)(s+y)}\right]^j \\
&\quad\times\left[\frac{\lambda}{s+\lambda}-\frac{sp\lambda}{(s+x)(s+\lambda)}\right. \\
&\quad\left.-\frac{\lambda\alpha\beta\theta}{(s+x)(s+y)(s+\lambda)}\right] \\
&\quad+\left[\frac{\lambda}{s+\lambda}-\frac{sp\lambda}{(s+x)(s+\lambda)}\right] \\
&\quad\times\left[\frac{\alpha\beta\theta}{(s+x)(s+y)}\right]^{n-1} \\
&= \frac{\lambda}{s+\lambda}\left[\sum_{j=0}^{n-2}\{\frac{\alpha\beta\theta}{(s+x)(s+y)}\}^j\right. \\
&\quad\times\{1-\frac{sp}{s+x}-\frac{\alpha\beta\theta}{(s+x)(s+y)}\} \\
&\quad\left.+\{1-\frac{sp}{s+x}\}\cdot\{\frac{\alpha\beta\theta}{(s+x)(s+y)}\}^{n-1}\right] \\
&= \frac{\lambda}{s+\lambda}\left[1-\frac{sp}{s+x}\right. \\
&\quad\left.\times\sum_{j=0}^{n-1}\{\frac{\alpha\beta\theta}{(s+x)(s+y)}\}^j\right] \\
&\qquad (n=1,2,\cdots). \qquad \text{(A.5)}
\end{aligned}
$$

3. $R_n(t)$ の導出

式 (8) の $h_n(s)$ をラプラス逆変換することによって，$R_n(t)$ $(n=0,1,2,\cdots)$ を順次求めることができる．なお，x，y は付録 2 の定義による．

(i) $n=0$ のとき，明らかに，

$$h_0(s)=\frac{\lambda}{s+\lambda}.$$

よって，

$$R_0(t)\equiv 1-H_0(t)=e^{-\lambda t}. \qquad \text{(A.6)}$$

(ii) $n=1$ のとき，

$$h_1(s)=h_0(s)-\frac{sp\lambda}{(s+x)(s+\lambda)}.$$

よって，

$$
\begin{aligned}
R_1(t) &\equiv 1-H_1(t) \\
&= R_0(t)+B_1e^{-xt}+B_2e^{-\lambda t}. \qquad \text{(A.7)}
\end{aligned}
$$

ここで

$$B_1\equiv-\frac{p\lambda}{\alpha-\lambda p},$$

$$B_2\equiv\frac{p\lambda}{\alpha-\lambda p}.$$

(iii) $n=2$ のとき，

$$h_2(s)=h_1(s)-\frac{sp\lambda\alpha\beta\theta}{(s+x)^2(s+y)(s+\lambda)}.$$

よって，

$$
\begin{aligned}
R_2(t) &\equiv 1-H_2(t) \\
&= R_1(t)+c_1te^{-xt}+c_2e^{-xt} \\
&\quad +c_3e^{-yt}+c_4e^{-\lambda t}, \qquad \text{(A.8)}
\end{aligned}
$$

を得る．ここで，

$$c_1\equiv-\frac{p\lambda\alpha\beta\theta}{y-\lambda}\left[\frac{1}{x-\lambda}+\frac{1}{y-x}\right],$$

$$c_2\equiv\frac{p\lambda\alpha\beta\theta}{y-\lambda}\left[\frac{1}{(x-\lambda)^2}+\frac{1}{(y-x)^2}\right],$$

$$c_3\equiv-\frac{p\lambda\alpha\beta\theta}{(y-x)^2(y-\lambda)},$$

$$c_4\equiv\frac{p\lambda\alpha\beta\theta}{(x-\lambda)^2(y-\lambda)}.$$

以下同様にして，$n=3,4,\cdots$ のとき，$R_n(t)$ を順次計算することができる．

4. $R_\infty(t)$ の導出

付録 2 より，$n\to\infty$ とすることによって，

$$
\begin{aligned}
h_\infty(s) &\equiv \lim_{n\to\infty}h_n(s) \\
&= \frac{\lambda}{s+\lambda} \\
&\quad\times\left[1-\frac{sp}{s+x}\sum_{j=0}^{\infty}\{\frac{\alpha\beta\theta}{(s+x)(s+y)}\}^j\right] \\
&= \frac{\lambda}{s+\lambda}\left[1-\frac{sp(s+y)}{(s+x)(s+y)-\alpha\beta\theta}\right].
\end{aligned}
$$

よって，$h_\infty(s)$ をラプラス逆変換し，$R_\infty(t)$ を求めると，

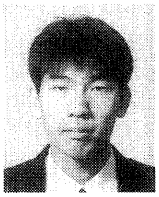
$$
\begin{aligned}
R_\infty(t) &\equiv 1-H_\infty(t) \\
&= R_0(t)+p\lambda\left[\frac{y-v_1}{(v_1-v_2)(v_1-\lambda)}e^{-v_1t}\right. \\
&\quad-\frac{y-v_2}{(v_1-v_2)(v_2-\lambda)}e^{-v_2t} \\
&\quad\left.+\frac{y-\lambda}{(v_1-\lambda)(v_2-\lambda)}e^{-\lambda t}\right]. \qquad \text{(A.9)}
\end{aligned}
$$

ここで，

$$v_1\equiv\frac{1}{2}\{x+y+\sqrt{(x-y)^2+4\alpha\beta\theta}\},$$

$$v_2\equiv\frac{1}{2}\{x+y-\sqrt{(x-y)^2+4\alpha\beta\theta}\}.$$

(平成 7 年 2 月 27 日受付)
(平成 7 年 10 月 5 日採録)



今泉　充啓

昭和43年生．平成7年愛知工業大学大学院工学研究科修士課程生産システム工学専攻修了．同年愛知学泉大学TA．コンピュータシステムの信頼性に興味をもつ．

安井　一民（正会員）

昭和11年生．昭和49年名城大学理工学部数学科卒業．工学博士．昭和30年中部電力（株）入社．平成元年愛知工業大学経営工学科助教授．信頼性理論および計算機システムの信頼性の研究に従事．電子情報通信学会，日本OR学会各会員．

中川　覃夫（正会員）

昭和17年生．昭和42年名古屋工業大学大学院工学研究科修士課程計測工学専攻修了．工学博士．昭和42年名城大学理工学部助手．昭和63年愛知工業大学経営工学科教授．信頼性理論および計算機システムの信頼性の研究に従事．電子情報通信学会，日本OR学会，日本信頼性学会各会員．