処理完了時限をもつマイクロプロセッサ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にともなって，マイクロプロセッサの利用範囲が拡大かつ多様化しており，その高信頼化の必要性が高まってきている．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，しばしば異常状態になる．このため高信頼性が要求されるマイクロプロセッサシステムには，これらの異常を確実に検出する機能が必要である．実際，簡単かつ小規模な副プロセッサであるウォッチドッグプロセッサが利用されている．ここでは，マイクロプロセッサとウォッチドッグプロセッサで構成される N 個のマイクロプロセッサユニットをもつシステムを考え，マイクロプロセッサにある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．マイクロプロセッサユニットはマイクロプロセッサとウォッチドッグプロセッサで構成され，処理完了時限 T までに1単位以上の処理が実行できなければ予備ユニットに切り替わる．そのとき，システムが動作障害に至るまでの平均時間とマイクロプロセッサの正常な処理回数を解析的に導出する．さらに，これらの結果を用いてコスト/有効性を表す評価尺度を定義し，それを最小にする最適なマイクロプロセッサユニットの個数を議論する．最後に，数値例を与え，種々の考察と評価を行う．

Reliability Evaluations of a Microprocessor System with Limit Processing Time

MITSUHIRO IMAIZUMI,[†] KAZUMI YASUI[††] and TOSHIO NAKAGAWA[††]

A large number of a microprocessor have been widely used in many practical fields and the demand for improvement of its reliability 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. However, it is impossible to detect any errors. Therefore, it would be necessary to develop a watchdog processor with more advanced capabilities and to improve the reliability of the whole system including a microprocessor. This paper considers reliability problems of a system with N microprocessor units where each microprocessor unit consists of microprocessor and watchdog processor. If the operating unit cannot finish one processing by errors until limit time, it changes to one of standby units. The mean time and the expected number of processings until system failure are obtained. Using these results, the cost effectiveness is derived and an optimal number of microprocessors which minimize it is discussed analytically. Finally, numerical examples are given under suitable conditions.

1. はじめに

近年，半導体集積回路技術の著しい進展とマイクロプログラミング技術の高度化にともなって，マイクロプロセッサの利用範囲が拡大している．とくに自動車や航空機，産業ロボットなど，マイクロプロセッサの広範な分野への利用の促進にともなって，その高信頼化の要求と必要性が非常に高まってきている[1)]．

一般に，マイクロプロセッサ（microprocessor: μP）は使用環境の悪化，ノイズの影響やハードウェア障害，またはプログラムバグ等によって，ある確率で異常状態になる[2),3)]．このため，高信頼性が要求される μP システムには，これらの異常を確実に検出する機能が必要であり，従来から多くの研究や提案が行われている[4)~6)]．

実際，μP の動作状態を監視する手段として，ウォッチドッグプロセッサ（watchdog processor: WDP）が幅広く用いられている．WDPは，主プロセッサの動作状態を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．

† 愛知学泉大学経営学部
School of Business Management, Aichi Gakusen University
†† 愛知工業大学経営工学科
Department of Industrial Engineering, Aichi Institute of Technology

その誤り検出は，たとえば監視対象の特徴情報を記憶して，動作時のバス情報を計算し，結果を比較することなどにより行われる．現状では，μP に発生する異常状態のすべてを検出することは不可能であり，より高機能をもつWDPの開発とともに，μP を含めたシステム全体の信頼性の向上が強く望まれている．

文献8)において，WDPの機能を簡素化したウォッチドッグタイマ（watchdog timer: WDT）をもつ μP システムが考察されており，高信頼性が重要視されるシステムに対してWDTの設定が有効であることが示されている．また，文献9)において著者らは，システムのメインプロセッサが単一で，WDPが多重化されたシステムの信頼性評価を行った．そこでは，少なくとも1個のWDPの設定が有効であることが分かった．しかし，最近では μP とWDPを一対とした μP ユニットが使用されており，さらに一般的なシステムのリアルタイム性の視点から，μP の単位処理が，ある完了時限以内に確実に終了するような機能の組込みが重要視されてきている．

ここでは，μP ユニットが μP とWDPで構成されるとき，N 個の μP ユニットをもつシステムの信頼性の問題を経済性と有効性の両面から考察する．システムは，常時は1つのユニットが動作し，他は待機状態にある．μP 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，μP に異常が発生した場合，その異常は，WDPのカバレッジと呼ばれるある確率で検出され，μP を自動リセットして初期状態へ復帰させる．μP は単位処理を繰り返し実行するが，あらかじめ設定した処理完了時限 T までに1単位以上の処理が実行できない場合は，μP を故障と判断して予備の μP ユニットに自動的に切り替わる．

以上の仮定のもとで，システムが動作障害に至るまでの平均時間と μP の正常な処理回数を，マルコフ再生過程[7]の手法を用いて解析的に求める．さらに，これらの結果を使用してコスト/有効性を表す評価尺度を導出し，それを最小にする μP ユニットの個数を議論する．最後に，具体的な数値例を与え，種々の考察と評価を行う．

2. モデルの設定と解析

μP ユニットの構成を図1に，N 個の μP ユニットをもつシステムの概要を図2に示す．

μP は単位処理（初期処理と主処理）を繰り返し実行する．その初期処理時間は指数分布 $A(t)$（平均 $1/\alpha$），主処理時間は指数分布 $B(t)$（平均 $1/\beta$）に従って行われる．

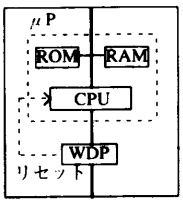

図1 マイクロプロセッサユニット
Fig. 1 Microprocessor unit.

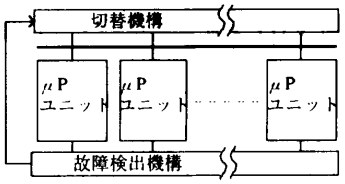

図2 N 個のマイクロプロセッサユニットをもつシステムの概要
Fig. 2 Outline of the system with N microprocessor units.

(1) μP の異常は，平均 $1/\lambda$ をもつ一般分布 $F(t)$ に従って発生する．

(2) WDPは μP の動作状態を監視し，その異常をカバレッジ $p(0<p<1)$ で検出する．
  (a) 確率 p で異常を検出したとき，μP をリセットし，主処理の初期状態へ復帰させる．
  (b) リセットに要する時間は，無視できる．
  (c) WDPは故障しない．

(3) μP が主処理開始後，時刻 T までに1単位以上の処理が実行できなかった場合，WDPは μP を故障と判断して予備ユニットへ切り替える．切替え成功確率は θ $(0<\theta<1)$ とし，切替え処理は一定時間 v で行われる．

(4) μP の異常がWDPにより検出できなかった場合，切替えに失敗した場合，あるいは，初期処理が完了する前に μP の異常が発生した場合，いずれもシステムは動作障害に至る．なお，N 個目の μP において，時刻 T までに1単位以上の主処理が実行できなかった場合も，システムは動作障害に至る．

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 μP ユニットが動作開始（$i=1,2,\cdots,N$）．

状態 F： システムの動作障害発生．

システムの状態を上のように定義するとき，各状態は状態 F を吸収状態にもつマルコフ再生過程を形成し，各状態間の推移は図3のように表される．

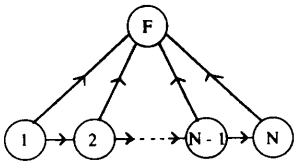

図3 システムの状態推移図
Fig. 3 Transition diagram between system states.

ここで，処理完了時限 T の分布 $U(t)$，切替えの処理時間分布 $V(t)$ を便宜上次のように定義する．

$$U(t) \equiv \begin{cases} 1: & t \geq T, \\ 0: & t < T, \end{cases} \tag{1}$$

$$V(t) \equiv \begin{cases} 1: & t \geq v, \\ 0: & t < v. \end{cases} \tag{2}$$

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・スチルチェス（LS）変換を $q_{i,j}(s)$ とする．一般に，$\Phi(t)$ の LS 変換を $\phi(s) \equiv \int_0^\infty e^{-st}d\Phi(t)$ と書き，

$$h_T(s) \equiv \int_0^T e^{-(s+\beta)t}dF(t) \tag{3}$$

とおく．そのとき，付録 A.1 より，

$$q_{i,i}(s) = \frac{\alpha\beta[1-f(s+\alpha)]}{(s+\alpha)(s+\beta)} \times \frac{1-\overline{F}(T)e^{-(s+\beta)T} - h_T(s)}{1-ph_T(s)} \quad (i = 1,2,\cdots,N), \tag{4}$$

$$q_{i,i+1}(s) = \frac{\left[\begin{array}{l} \alpha\theta(s+\beta)[1-f(s+\alpha)] \\ \times e^{-\beta T}e^{-s(T+v)}\overline{F}(T) \end{array}\right]}{\left[\begin{array}{l} (s+\alpha)(s+\beta)[1-ph_T(s)] \\ -\alpha\beta[1-f(s+\alpha)] \\ \times [1-\overline{F}(T)e^{-(s+\beta)T} \\ -h_T(s)] \end{array}\right]} \quad (i = 1,2,\cdots,N-1), \tag{5}$$

$$q_{i,F}(s) = \frac{\left[\begin{array}{l} (s+\beta)[1-ph_T(s)] \\ \times [\alpha + sf(s+\alpha)] \\ -\alpha(s+\beta)[1-f(s+\alpha)] \\ \times [1-h_T(s)-(1-\theta) \\ \times e^{-\beta T}e^{-s(T+v)}\overline{F}(T)] \end{array}\right]}{\left[\begin{array}{l} (s+\alpha)(s+\beta)[1-ph_T(s)] \\ -\alpha\beta[1-f(s+\alpha)] \\ \times [1-\overline{F}(T)e^{-(s+\beta)T} \\ -h_T(s)] \end{array}\right]} \quad (i = 1,2,\cdots,N-1), \tag{6}$$

$$q_{N,F}(s) = \frac{\left[\begin{array}{l} (s+\alpha)(s+\beta) \\ \times [1-ph_T(s)]f(s+\alpha) \\ +\alpha(s+\beta)[1-f(s+\alpha)] \\ \times [(1-p)h_T(s) \\ +e^{-(s+\beta)T}\overline{F}(T)] \end{array}\right]}{\left[\begin{array}{l} (s+\alpha)(s+\beta)[1-ph_T(s)] \\ -\alpha\beta[1-f(s+\alpha)] \\ \times [1-\overline{F}(T)e^{-(s+\beta)T} \\ -h_T(s)] \end{array}\right]} \tag{7}$$

を得る．ここで，明らかに，$q_{i,i+1}(0) + q_{i,F}(0) = 1$ $(i = 1,2,\cdots,N-1)$, $q_{N,F}(0) = 1$ が示される．さらに，式 (4) ~ (6) において，$q_{i,j}(s)$ は i に無関係であることに注意する．

最初に，システム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．

$$H_N(t) = Q_{1,F}(t) + Q_{1,2}(t) * Q_{2,F}(t) + \cdots + Q_{1,2}(t) * \cdots * Q_{N-1,N}(t) * Q_{N,F}(t). \tag{8}$$

したがって，$\ell(N)$ を次のように求めることができる．

$$\ell(N) \equiv \int_0^\infty t dH_N(t) = \lim_{s\to 0}\frac{d}{ds}[-h_N(s)] = \frac{1}{1-k(0)}\{D(1-[k(0)]^N) + E(1-[k(0)]^{N-1})\} \quad (N = 1,2,\cdots). \tag{9}$$

ここで，

$$k(0) \equiv \frac{\theta[1-f(\alpha)]\overline{F}(T)e^{-\beta T}}{\left[\begin{array}{l} 1-ph_T(0)-[1-f(\alpha)] \\ \times [1-\overline{F}(T)e^{-\beta T}-h_T(0)] \end{array}\right]}, \tag{10}$$

$$D \equiv \frac{\left[\begin{array}{l} \left\{\frac{1}{\alpha}[1-ph_T(0)] \right. \\ \left. +\frac{1}{\beta}[1-h_T(0)-\overline{F}(T)e^{-\beta T}]\right\} \\ \times [1-f(\alpha)] \end{array}\right]}{\left[\begin{array}{l} 1-ph_T(0)-[1-f(\alpha)] \\ \times [1-h_T(0)-\overline{F}(T)e^{-\beta T}] \end{array}\right]}, \tag{11}$$

$$E \equiv \frac{v\overline{F}(T)e^{-\beta T}[1-f(\alpha)]}{\left[\begin{array}{l}1-ph_T(0)-[1-f(\alpha)]\\ \times[1-h_T(0)-\overline{F}(T)e^{-\beta T}]\end{array}\right]}. \quad (12)$$

なお，$k(0) \equiv q_{i,i+1}(0)$ $(i=1,2,\cdots,N-1)$ が示されるので，$0<k(0)<1$ であることに注意する．また，$N=1,\infty$ に対して，

$$\ell(1) = D, \quad (13)$$

$$\ell(\infty) = \frac{D+E}{1-k(0)} \quad (14)$$

となる．

次に，システムが動作障害に至るまでの μP の平均処理回数を求めよう．時刻0でシステムが状態 i を出発したとき，時刻 t までに再び状態 i を訪れる平均回数 $M_i(t)$ は次のような再生形方程式で与えられる．

$$M_i(t) = Q_{i,i}(t) * [1+M_i(t)] \quad (i=1,2,\cdots,N). \quad (15)$$

よって，システムが状態1を出発してから状態 F へ吸収されるまでの平均処理回数 $M(t)$ のLS変換 $m(s)$ は，次式で与えられる．

$$\begin{aligned} m(s) &= m_1(s) + q_{1,2}(s)m_2(s) + \cdots \\ &\quad + q_{1,2}(s)q_{2,3}(s)\cdots q_{N-1,N}(s)m_N(s) \\ &= \sum_{j=1}^{N} m_k(s)[q_{i,i+1}(s)]^{j-1}. \end{aligned} \quad (16)$$

ここで，$m_k(s) \equiv m_i(s)$ $(i=1,2,\cdots,N)$ である．したがって，$q_{i,i+1}(0)=k(0)$ であるから，システムが動作障害に至るまでの平均処理回数 M を，次のように求めることができる．

$$\begin{aligned} M &\equiv \lim_{t\to\infty} M(t) = \lim_{s\to 0} m(s) \\ &= \sum_{j=1}^{N} m_k(0)[k(0)]^{j-1} \\ &= \frac{[1-f(\alpha)][1-\overline{F}(T)e^{-\beta T}-h_T(0)]}{\left[\begin{array}{l}1-ph_T(0)-[1-f(\alpha)]\\ \times[1-\overline{F}(T)e^{-\beta T}-h_T(0)]\\ -\theta e^{-\beta T}[1-f(\alpha)]\overline{F}(T)\end{array}\right]} \\ &\quad \times\{1- \\ &\quad \left[\frac{\theta e^{-\beta T}[1-f(\alpha)]\overline{F}(T)}{\begin{array}{l}1-ph_T(0)-[1-f(\alpha)]\\ \times[1-\overline{F}(T)e^{-\beta T}-h_T(0)]\end{array}}\right]^N \\ &\quad \}. \end{aligned} \quad (17)$$

3. 最適方策

一般に，あるシステムにおける期待コストとその有効性とは，相反する関係にある．実際に行われる μP の正常な処理回数を考慮してシステムの信頼性等を評価するため，ここでは，信頼性と経済性の両方を兼ね備えたコスト有効性の考え方を導入して，最適方策を議論する．まず，1 μP ユニットあたりの費用を c_1 とし，システムの動作障害にともなう損失費用を c_2 とする．そのとき，N 個の μP ユニットをもつシステムの単位時間あたりの期待コストを $\tilde{C}(N) \equiv (Nc_1+c_2)/\ell(N)$，有効性を単位時間あたりの平均処理回数 $M/\ell(N)$ と仮定し，コスト/有効性を

$$C(N) \equiv \frac{\tilde{C}(N)}{\frac{M}{\ell(N)}} = \frac{Nc_1+c_2}{M} \quad (18)$$

と定義する．すなわち，$C(N)$ は単位処理回数あたりの期待費用を表す．

式 (18) の $C(N)$ を最小にするユニットの個数 N^* を求める．式 (17) より，

$$C(N) = \frac{Nc_1+c_2}{\sum_{j=1}^{N} m_k(0)[k(0)]^{j-1}} \quad (19)$$

となる．ここで，

$$A_j \equiv m_k(0)[k(0)]^{j-1} \quad (20)$$

とおく．$0<k(0)<1$ であるから，A_j は j の単調減少関数であり，$\lim_{j\to\infty} A_j = 0$ となる．

次に，$C(N)$ を最小にする N^* を求めるため，$C(N+1)-C(N) \geq 0$ とおくと，

$$\frac{\sum_{j=1}^{N} A_j}{A_{N+1}} - N \geq \frac{c_2}{c_1} \quad (21)$$

を得る．式 (21) の左辺を $L(N)$ とおくと，

$$\begin{aligned} L(N)-L(N-1) &= \sum_{j=1}^{N} A_j\left(\frac{1}{A_{N+1}}-\frac{1}{A_N}\right) \\ &> 0, \end{aligned} \quad (22)$$

$$L(1) = \frac{A_1}{A_2} - 1 = \frac{1}{k(0)} - 1 > 0, \quad (23)$$

$$\begin{aligned} L(\infty) &= \lim_{N\to\infty}\left\{\frac{\sum_{j=1}^{N} A_j}{A_{N+1}} - N\right\} \\ &\geq \lim_{N\to\infty}\frac{A_1}{A_{N+1}} - 1 = \infty \end{aligned} \quad (24)$$

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．

以上から，次のような結論を得ることができる．

(i) もし，$L(1) \geq c_2/c_1$，すなわち $k(0) \leq c_1/(c_1+c_2)$ ならば，$N^*=1$ である．

(ii) もし，$L(1) < c_2/c_1$，すなわち $k(0) > c_1/(c_1+c_2)$ ならば，式 (21) を満たす有限で唯一の $N^*(>1)$ が存在する．

4. 数値例による考察と評価

3章で求めたコスト/有効性 $C(N)$ を最小にする最適方策について，具体的な数値を求める．ここでは，自動車などで用いられている μP の経験的なパラメータ値[8]を参考として適用する．まず，μP の異常発生の確率分布を $F(t)=1-e^{-\lambda t}$ と仮定し，μP の主処理時間の平均 $1/\beta$ をシステムの単位時間とおく．このとき，μP の平均異常発生間隔を $(1/\lambda)/(1/\beta)=3600\sim3600\times24$ ($1/\beta=1$（秒）のとき 1 ～ 24（時間）に相当)（可変)，μP の初期処理の平均を $(1/\alpha)/(1/\beta)=1$ とする．μP ユニットの切替え処理時間については，WDP 固有のクロック（たとえば30 MHz）の100倍程度として，$v/(1/\beta)=(1/30)\times10^{-6}\times100$ と仮定する．さらに，μP ユニットの切替え成功確率を $\theta=0.8\sim0.99$（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個あたりの費用 c_1 を単位費用とし，システムの動作障害にともなう損失費用を $c_2/c_1=10\sim10^3$（可変）と仮定する．

以上の仮定のもとで，μP の処理完了時限 T を μP の主処理時間の 10 ～ 20 倍に設定したとき，すなわち $T/(1/\beta)=\beta T=10\sim20$（可変）のとき，コスト/有効性 $C(N)$ を最小にする最適値 N^* の数値例を**表1**に示す．

表1によれば，N^* は βT の増大にともない減少し，$1/\lambda$，p，θ，および c_2/c_1 が大きくなるに従って増加する．たとえば，$(1/\lambda)/(1/\beta)=3600\times24$，$P=0.9$，$\theta=0.9$，$\beta T=15$，$c_2/c_1=10^2$ のとき，最適な μP の個数は $N^*=2$ であることが分かる．表1の結果から，処理完了時限 βT が小さい場合，N^* は μP の異常発生率 λ の影響を受けやすく，かつ WDP の性能 p やユニットの切替え成功確率 θ に大きく依存することが示される．しかし，$\beta T\geq15$ では，N^* は $1/\lambda$ や p および θ にほとんど依存せず，およそ 1 ～ 2 でよいといえる．

次に，$(1/\lambda)/(1/\beta)=3600$，$3600\times24$，$p=0.8$，$\theta=0.8$，$\beta T=10$，$c_2/c_1=10$ のとき，N に対する $C(N)$ の推移と最適値 N^* を**図4**に示す．

図4によれば，$C(N)$ の値は $1/\lambda$ が増大すると著しく減少することが分かる．表1において，$1/\lambda$ が大きくなると N^* が大きくなるのは，処理完了時限 βT 内における μP の単位処理回数が増大し，処理回数あたりの期待コストの低減が顕著になるためと考えられる．いわば，図4から，性能の良い μP ユニットは，有効性に対する期待コストが非常に小さくなるた

表1 $C(N)$ を最小にする最適値 N^*
Table 1 Optimal numbers N^* to minimize $C(N)$.

βT	$(1/\lambda)/(1/\beta)$	p	θ	c_2/c_1		
				10	10^2	10^3
10	3600	0.8	0.8	2	4	6
			0.9	2	4	6
			0.99	3	5	7
		0.9	0.8	3	5	7
			0.9	3	5	8
			0.99	3	6	8
		0.99	0.8	3	6	9
			0.9	4	7	10
			0.99	4	8	12
	3600 × 24	0.8	0.8	4	8	13
			0.9	5	10	16
			0.99	6	13	20
		0.9	0.8	4	8	13
			0.9	5	10	17
			0.99	6	13	22
		0.99	0.8	4	9	14
			0.9	5	11	17
			0.99	7	14	23
15	3600	0.8	0.8	1	1	2
			0.9	1	1	2
			0.99	1	1	2
		0.9	0.8	1	1	2
			0.9	1	1	2
			0.99	1	1	2
		0.99	0.8	1	1	2
			0.9	1	1	2
			0.99	1	1	2
	3600 × 24	0.8	0.8	1	2	2
			0.9	1	2	2
			0.99	1	2	2
		0.9	0.8	1	2	2
			0.9	1	2	2
			0.99	1	2	2
		0.99	0.8	1	2	2
			0.9	1	2	2
			0.99	1	2	2
20	3600	0.8	0.8	1	1	1
			0.9	1	1	1
			0.99	1	1	1
		0.9	0.8	1	1	1
			0.9	1	1	1
			0.99	1	1	1
		0.99	0.8	1	1	1
			0.9	1	1	1
			0.99	1	1	1
	3600 × 24	0.8	0.8	1	1	1
			0.9	1	1	1
			0.99	1	1	1
		0.9	0.8	1	1	1
			0.9	1	1	1
			0.99	1	1	1
		0.99	0.8	1	1	1
			0.9	1	1	1
			0.99	1	1	1

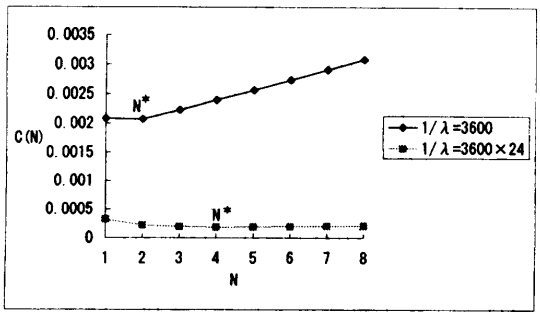

図4 $(1/\lambda)/(1/\beta) = 3600, 3600 \times 24$, $p = 0.8$, $\theta = 0.8$, $\beta T = 10$, $c_2/c_1 = 10$ のとき，N に対する $C(N)$ の値と最適値 N^*

Fig. 4 Cost effectiveness $C(N)$ for N and N^* when $(1/\lambda)/(1/\beta) = 3600, 3600 \times 24$, $p = 0.8$, $\theta = 0.8$, $\beta T = 10$ and $c_2/c_1 = 10$.

めに，最適な N^* は逆に大きくなる傾向を示すことが分かる．

5. おわりに

μP と WDP で構成される μP ユニットが N 個の待機冗長方式をとるシステムの信頼性モデルを設定した．μP ユニットの処理機能に関して，μP が故障状態であるという判断を下すためのしきい値として処理完了時限 T を設定し，μP の平均異常発生間隔 $1/\lambda$，WDP によるカバレッジ p，待機中の μP ユニットへの切替え成功確率 θ，さらに μP の平均主単位処理時間 $1/\beta$ 等を考慮することによって，システムが動作障害に至るまでの平均時間や μP の正常な処理回数を求めた．また，コスト有効性の考え方を導入し，有効性に対する期待コストを最小にする最適な μP ユニットの個数について議論した．

数値例から，コスト/有効性を最小にする最適な μP の個数 N^* は，βT の増大にともない減少し，$1/\lambda$ や p，θ，および損失費用比 c_2/c_1 が大きくなるに従って増加する傾向を示し，$\beta T \geq 15$ では，N^* はこれらの値にほとんど依存せず，およそ 1～2 でよいことが分かった．なお，βT が比較的小さい場合，性能の良い μP ユニットは単位処理あたりの期待コストがきわめて小さくなり，最適な N^* は逆に大きくなるという興味深い結果が得られた．このことは，システムの処理完了時限 T の大きさと，期待コストの設定に関して留意すべき点であると考えられる．

最近の VLSI 技術の進展により，μP はあらゆる分野で多用されてきている．ゆえに，このような μP を用いたシステム全体として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) 楠 菊信：マイクロプロセッサ，丸善 (1994).
2) 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).
3) 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).
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) Osaki, S.: *Applied Stochastic System Modeling*, Springer-Verlag, Berlin (1992).
8) 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).
9) 今泉充啓，安井一民，中川覃夫：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，情報処理学会論文誌，Vol.36, No.12, pp.2859-2866 (1995).

付 録

A.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 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．

$$Q_{i,i}(t) = \left[\int_0^t \overline{F}(t)dA(t)\right] * \left\{\sum_{k=1}^{\infty}\left[p\int_0^t \overline{B}(t)\overline{U}(t)dF(t)\right]^{(k-1)} * \int_0^t \overline{F}(t)\overline{U}(t)dB(t)\right\} \quad (i = 1, 2, \cdots, N), \tag{25}$$

$$Q_{i,i+1}(t) = \sum_{j=1}^{\infty}\left[Q_{i,i}(t)\right]^{(j-1)} * \left[\int_0^t \overline{F}(t)dA(t)\right]$$

$$* \left\{ \sum_{k=1}^{\infty} \left[p \int_0^t \overline{B}(t)\overline{U}(t) dF(t) \right]^{(k-1)} * \left[\int_0^t \overline{F}(t)\overline{B}(t) dU(t) \right] \right\} * \left[\theta V(t) \right] \quad (i = 1, 2, \cdots, N-1), \tag{26}$$

$$Q_{i,F}(t) = \sum_{j=1}^{\infty} \left[Q_{i,i}(t) \right]^{(j-1)} * \left[\int_0^t \overline{A}(t) dF(t) \right] + \sum_{j=1}^{\infty} \left[Q_{i,i}(t) \right]^{(j-1)} * \left[\int_0^t \overline{F}(t) dA(t) \right] * \sum_{k=1}^{\infty} \left[p \int_0^t \overline{B}(t)\overline{U}(t) dF(t) \right]^{(k-1)} * \left\{ (1-p) \int_0^t \overline{B}(t)\overline{U}(t) dF(t) + \left[\int_0^t \overline{F}(t)\overline{B}(t) dU(t) \right] * \left[(1-\theta) V(t) \right] \right\} \quad (i = 1, 2, \cdots, N-1), \tag{27}$$

$$Q_{N,F}(t) = \sum_{j=1}^{\infty} \left[Q_{N,N}(t) \right]^{(j-1)} * \left[\int_0^t \overline{A}(t) dF(t) \right] + \sum_{j=1}^{\infty} \left[Q_{N,N}(t) \right]^{(j-1)} * \left[\int_0^t \overline{F}(t) dA(t) \right] * \sum_{k=1}^{\infty} \left[p \int_0^t \overline{B}(t)\overline{U}(t) dF(t) \right]^{(k-1)} * \left\{ (1-p) \int_0^t \overline{B}(t)\overline{U}(t) dF(t) + \int_0^t \overline{F}(t)\overline{B}(t) dU(t) \right\}. \tag{28}$$

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，$a^{(i)}(t) \equiv a^{(i-1)}(t) * a(t)$, $a(t) * b(t) \equiv \int_0^t b(t-u) da(u)$, $a^{(0)}(t) \equiv 1$ である．たとえば，$Q_{N,F}(t)$ は，N 個目の μP が動作中のとき，時刻 t までに，(i) 初期処理が完了しないうちに μP の異常が発生する，(ii) WDP により μP の異常が検出されない，(iii) 処理完了時限がきても μP の主単位処理が終了しない，3つの場合のいずれかのために，システム故障状態へ推移する確率分布を表す．

(平成8年 9 月19日受付)
(平成8年11月 7 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，日本信頼性学会各会員．

中川 覈夫（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．