5H－6

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*

安井一民† 中川覃夫† 原田義久††
愛知工業大学 豊田中央研究所

1. はじめに

マイクロプロセッサ (microprocessor : μP) の動作状態を監視する簡便な方法として，比較的安価なウォッチドッグタイマ (watchdog timer : WDT) が多く用いられており，高機能をもつ WDT の研究・開発 [1] や，さらに，μP を含めたシステム全体の信頼性の向上が望まれている．ここでは，μP と WDT とが，それぞれ独立なプロセスを実行するとき，ある確率分布に従って異常状態が発生すると仮定した確率モデルを設定し，μP が暴走状態または障害発生に至るまでの平均時間や μP の平均有効時間の割合，さらに，コスト有効性等の尺度を導出し，WDT をもつことによって，μP の信頼性がどの程度向上するかなどについての考察と評価を行う．

2. モデルと解析

(1) μP には，ハードウェア障害やメモリアクセスミス等により，平均 $1/\lambda_1$ をもつ確率分布 $F_1(t)$ に従って異常状態が発生する．(i) μP の異常は WDT により確率 p $(0 < p < 1)$ で検出可能であり，確率 $1-p$ で検出できない．(ii) WDT は平均 $1/\mu$ をもつ確率分布 $G(t)$ に従って μP の異常を検出し，μP を初期状態へリセットする．

(2) WDT は自己のハードウェア障害等により，指数分布 $(1-e^{-\alpha t})$ に従って異常状態となる．この場合，μP の異常状態は検出できないものとする．(i) WDT は自己検査機能をもち，自己の異常状態を確率θ で検出する．(ii) WDT の異常は，人間系によって指数分布 $(1-e^{-\beta t})$ に従って検知され，WDT の取り替えを含む修復によって正常状態へ復帰する．

(3) μP の異常状態が WDT で検出不可能な場合，μP は平均 $1/\lambda_2$ をもつ確率分布 $F_2(t)$ に従って障害発生に至る．

以上のような仮定のもとで，μP が動作を開始した後，障害発生に至るまでの平均時間 (MTTF) を解析的に求める．最初に，WDT が障害発生や修復を繰り返す状態を，

状態0 ：WDT 正常，
状態1 ：WDT 異常（検出可），
状態2 ：WDT 異常（検出不可）．

と定義すると，WDT の状態確率分布 $P_{0j}(t)$ $(j=0,1,2)$ は，

$$P_{00}(t) = \frac{1}{a-b}\Big[(\beta-b)e^{-bt} -(\beta-a)e^{-at}\Big], \qquad (1)$$

$$P_{01}(t) = \frac{\alpha\theta}{a-b}\left[e^{-bt}-e^{-at}\right], \qquad (2)$$

$P_{02}(t) = 1 - P_{00}(t) - P_{01}(t)$ ，で与えられる．ここで，

$$a \equiv [(\alpha+\beta)+\sqrt{(\alpha-\beta)^2+4\alpha\beta\theta}]/2,$$
$$b \equiv [(\alpha+\beta)-\sqrt{(\alpha-\beta)^2+4\alpha\beta\theta}]/2,$$

とおく．

次に，μP の各状態を次のように定義する．

状態5 ：μP が動作開始，
状態6 ：μP の異常状態が発生（検出可），
状態7 ：μP の異常状態が発生（検出不可），
状態8 ：μP の障害が発生．

ここで，WDT は時刻 0 で状態0にあり，μP は状態5から出発する．

各状態間の推移確率時間分布を $Q_{ij}(t)$ $(i=5,6,7; j=5,6,7,8)$ とすると，次式を得る．

*Reliability Evaluations of Microprocessor System with Watchdog Timer
†Kazumi Yasui and Toshio Nakagawa, Aichi Institute of Technology
††Yoshihisa Harata, Toyota Central Research & Development Labs., Inc.

$$Q_{56}(t) = p\int_0^t P_{00}(t)dF_1(t), \quad (3)$$

$$\begin{aligned} Q_{57}(t) &= (1-p)\int_0^t P_{00}(t)dF_1(t) \\ &\quad + \int_0^t [1-P_{00}(t)]dF_1(t), \end{aligned} \quad (4)$$

$$Q_{65}(t) = \int_0^t P_{00}(t)dG(t), \quad (5)$$

$$Q_{68}(t) = \left[\int_0^t [1-P_{00}(t)]dG(t)\right] * F_2(t), \quad (6)$$

$$Q_{78}(t) = F_2(t). \quad (7)$$

ここで，$*$ は分布関数の畳み込みを表す．

さて，一般に，$\Phi(t)$ のラプラス・スチルチェス変換を$\phi(s) \equiv \int_0^\infty e^{-st}d\Phi(t)$ と定義する．μP が動作を開始してから，障害発生に至るまでの平均時間 (MTTF) ℓ は，次のように求めることができる．

$$\ell = \frac{\begin{bmatrix} (1/\lambda_1 + 1/\lambda_2)(a-b)^2 \\ -p \times KF_1 \times \{(1/\lambda_2) \times KG \\ -(1/\mu)(a-b)\} \end{bmatrix}}{(a-b)^2 - p \times KF_1 \times KG}. \quad (8)$$

ここで，

$$KF_1 \equiv (\beta - b)f_1(b) - (\beta - a)f_1(a),$$

$$KG \equiv (\beta - b)g(b) - (\beta - a)g(a),$$

とおく．

3. μP の信頼性評価

3.1 MTTF

μP が WDT をもたない場合，障害発生までの平均時間 MTTF は $1/\lambda_1 + 1/\lambda_2$ となる．従って，WDT をもつ場合の MTTF の増分を ℓ_W とおくと，

$$\ell_W = \frac{\begin{bmatrix} p \times KF_1 \times \{(1/\mu)(a-b) \\ +(1/\lambda_1) \times KG\} \end{bmatrix}}{(a-b)^2 - p \times KF_1 \times KG}, \quad (9)$$

を得る．

3.2 アベイラビリティ

μP の平均有効時間 ℓ_A を μP が正常状態にある平均時間と定義し，アベイラビリティを $A \equiv \{$ μP の平均有効時間 $\}$ / MTTF $= \ell_A/\ell$, とおく．平均有効時間 ℓ_A は，(8) 式で $1/\mu = 0$, $1/\lambda_2 = 0$ とおくことによって容易に求められる．また，μP が WDT をもたない場合のアベイラビリティは，$(1/\lambda_1)/(1/\lambda_1 + 1/\lambda_2)$ となる．よって，WDT によるアベイラビリティの増分を A_W とおくと，

$$A_W = \frac{\begin{bmatrix} [p/(\lambda_1 + \lambda_2)] \times KF_1 \\ \times\left\{KG - (\lambda_2/\mu)(a-b)\right\} \end{bmatrix}}{\begin{bmatrix} (1/\lambda_1 + 1/\lambda_2)(a-b)^2 \\ -p \times KF_1 \times \left\{(1/\lambda_2)\right. \\ \left.\times KG - (1/\mu)(a-b)\right\} \end{bmatrix}}, \quad (10)$$

で与えられる．

3.3 コスト有効性

ここでは，有効性をシステムのアベイラビリティと考え，コスト / アベイラビリティ比について考察する．WDT に関わる全費用を c_1, μP の障害発生に伴う損失費用を c_2 とするとき，コスト有効性 $\equiv (c_1 + c_2)/A$ とおく．なお，μP が WDT をもたない場合のコスト有効性は，明らかに $(1/\lambda_1 + 1/\lambda_2)c_2/(1/\lambda_1)$ である．この尺度は，小さい程良いから，その差分を U_W とおくと，

$$\begin{aligned} U_W &= \frac{\lambda_1}{(a-b)^2}\Bigg[p \times KF_1 \\ &\quad \times\left\{\frac{1}{\lambda_2}KG - \frac{1}{\mu}(a-b)\right\}(c_1 + c_2) \\ &\quad - \left(\frac{1}{\lambda_1} + \frac{1}{\lambda_2}\right)(a-b)^2 c_1\Bigg], \end{aligned} \quad (11)$$

を得る．

参考文献

[1] 並木・古賀：自己検査性ウォッチドッグタイマの一構成法，信学論 (D), J68-D, 8 , pp. 1543-1544(1985) .