マイクロコンピュータによる実時間ディジタル信号処理装置の高信頼化

亀山 充隆　樋口 龍雄
（東北大学工学部）

1. まえがき

マイクロプロセッサを用いた実時間ディジタル信号処理装置は，その低価格性，柔軟性のため，広く計測・制御の分野で使用されつつあり[1][2]，最近では，LSI化された信号処理専用のプロセッサも出現している[3][4]。このような中で，マイクロプロセッサを厳しい環境中で動作させたり，また，故障が重大な事態を引き起こすようなシステムにマイクロプロセッサを使用する場合がますます多くなってきていることは周知の通りである。プロセス制御，自動車の電子制御などは，その典型的な例であり，今後，マイクロコンピュータシステムの高信頼化は，ますます重要な問題となることが予想される。

ディジタルシステムの信頼性を高める1つの方法として，同じ機能モジュールを3重化して，これらの多数決によって最終出力を決定する方式すなわちTMR（Triple-Modular Redundancy）の有効性が知られており，多くの実用システムに取り入れられている[5]～[10]。TMRにおいては，1回の間欠故障がシステムの内部状態を変化させることにより，その後も誤動作が継続する可能性がある。このような場合，3つのモジュールの内部状態を一致させ，間欠故障の影響を排除する操作，すなわち内部修復（Resynchronization）が有効となる。しかしながら，TMRにおいては，3個のモジュール全てが同一環境中に設置される場合がほとんどであり，間欠故障が複数個のモジュールに同時に起こる可能性がある。例えば，インパルス状の雑音がいくつかのモジュールに同時に印加され，システムダウンとなるような場合である。従って，通常のTMRにおいては，同時故障相関が強い場合，内部修復を最適に行ったとしても，信頼度をある一定の値以上に改善することはできないことが知られている[11][12]。

本論文では，以上のような観点から，同時故障相関の影響を排除した新しい方式に基づくディジタル信号処理用マイクロコンピュータシステムの構成法が示されている。通常の多重化システムに対する誤り検出では，対応するデータのビットごとの不一致を論理的に検出しているが，ここでは，ディジタル信号処理特有の新しい誤り検出及び内部修復の概念が提案されている。この結果，従来のTMRと比較して，故障相関が強い環境中でも，信頼度を大幅に向上できることを明らかとしている。

2. 高信頼化のためのアーキテクチャの概要

本システムでは，図1の基本構成図のように3重化されたモジュールにより，ディジタル信号処理をサンプリング周期T_sで独立に実行する。各プロセッサの入力信号は，外部タイマにより一定周期T_sで割込みをかけてサンプルされ，また，信号処理された3つの出力は，ある1つのモジュールからD-A変換器を通して出力されることになる。

同時故障相関の影響を排除した本システムの動作タイミングチャートが，図2，図3に示されている。サンプリング周期T_sの間に，3つのCPUがそれぞれ1回ずつ等間隔に入力信号をサンプリングする。従って，2つのCPUで行われる信

号処理は，システム全体で見れば冗長であると考えられる。1つのCPUが信号処理を実行している間は，他の2つのCPUは何も実行していない'No Operation'の状態であり，このとき，後の信号処理に引き続き使用される内部状態は全てメモリに格納されているものとする。例えば，ディジタルフィルタリングにおいては，遅延(z^{-1})の出力が内部状態であり，これらの全てが'No Operation'の間メモリに格納されている。1つのCPUにおいて，$N=T/T_s$個のサンプル入力が処理された後，他の2つのモジュールとのデータの授受を行うことにより，誤り検出が行われる(図3は，$N=1$の場合を示している。)。'No Operation'の間，内部状態が格納されているメモリ領域は，データの値が変化しないものと仮定する。もし，3つのCPUに，図3で示されるように同時に雑音が入り，CPU内の内部状態が変化したとしても，このとき行われている信号処理結果に対する内部状態の誤りは，1つのCPUのみに限定される。すなわち，他の2つの冗長な信号処理が誤動作なく行われれば，誤った内部状態が検出されるとともに，内部修復が3つのプロセッサによって独立に行われることになる。以上のようにして，同時故障相関の影響を排除したシステムが構成される。なお，本システムでは，単一モジュールの永久故障に対しても，フォルトトレラント性を有していることは，当然である。

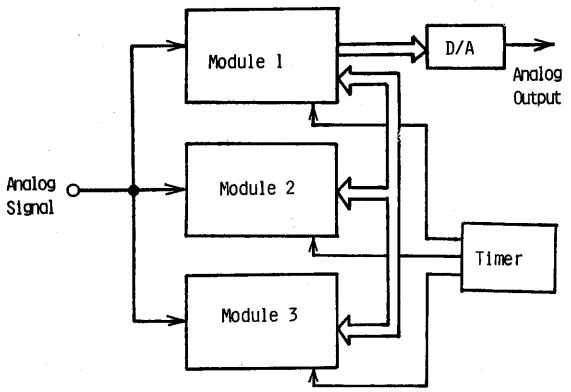

図1　高信頼化ディジタル信号処理プロセッサ

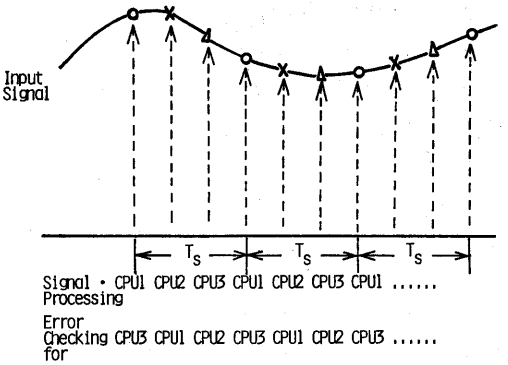

図2　入力信号のサンプル

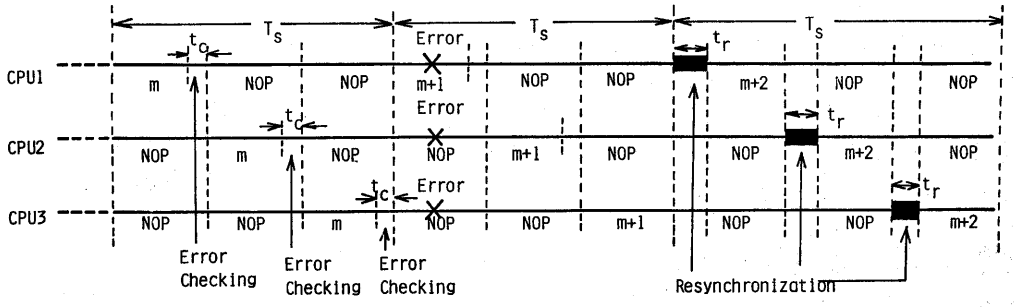

図3　タイムチャート

3. ディジタル信号処理における新しい誤り検出法と内部修復法

本システムは，3つのプロセッサにおいて，入力信号が異なる時間にサンプルされるため，通常のビットごとの論理的不一致を検出するような方法は適用することができない。このため信号処理特有のいわばアナログ的な新しい誤り検出法を提案する。

データが局所的に奇数次の多項式であると見なすことにより，2つの連続したデータの間の3分割された点における値は，補間公式を用いて求めることができる[13]。最も一般的方法は，式(1)で示される線形補間である。

$$y = (y_{n-1} + 2y_n)/3 \qquad (1)$$

但し，y_nは時間nT_Sにおける出力を示している。このような補間による最大誤差を式(1)より求めたのが式(2)である。

$$\varepsilon(f) = \frac{M}{3}\sqrt{14 - 6\cos\frac{4\pi f}{3f_S} + 4\cos 2\pi\frac{f}{f_S} - 12\cos\frac{2\pi f}{3f_S}} \qquad (2)$$

但し，fは入力信号の周波数，f_Sはサンプリング周波数$1/T_S$，Mは出力データのダイナミックレンジ±Mを示している。図4は，式(2)に基づき正規化した($M=1$)場合のεの値を示している。例えば，$f/f_S \leq 0.15$ならば，誤差は0.1M以下となる。従って誤り検出のアルゴリズムは，次のように表わすことができる。

$|y - y_{n-1/3}| \leq \varepsilon(f)$ならば，誤りはない。その他の場合，誤りが存在する。 (3)

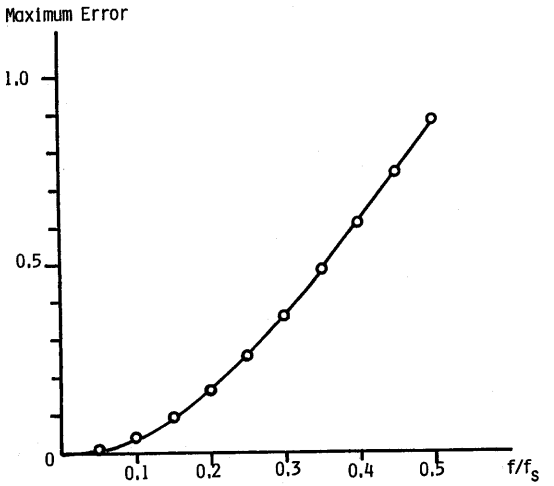

図4　線形補間の誤差

全てのデータの誤りが必ずしも式(3)により，検出されるわけではないが，たとえ誤りが式(3)により検出されない場合でも，fが十分小さければこのときの誤差の値は小さいと考えられ，ディジタル信号処理においては誤りの影響を無視できると考えられる。

誤りが検出されたならば，間欠故障によって引き起こされた内部状態を正しい値に回復する必要がある。このような内部修復のアルゴリズムを示したのが式(4)(5)である。ここでは，$y^3 \equiv y_{n-1/3}$に対する回復された値yを示している。

$$y^1 = (y_{n-1} + 2y_n)/3, \quad y^2 = (2y_{n-2/3} + y_{n+1/3})/3 \qquad (4)$$

$$y = \mathrm{Median}(y^1, y^2, y^3) \qquad (5)$$

すなわち，補間されたデータを含めた対応する3つのデータを比較し，これらの中央値(Median)に内部状態を設定することを示している。このように，多数決ではなく，中央値を用いることも本方式の特徴である。

4. 3重化システムのハードウェアとソフトウェアの構造

図5は，本システムの各モジュールを示している。各モジュールは，マイクロプロセッサ，メモリ，6つのI/Oポート，A-D変換器とから構成されていると

ともに，独立した電源とクロックを有している。入力信号は，外部タイマの割込みにより，サンプリング周期T_Sで各モジュールごとにA-D変換される。また，出力信号は，I/Oポート(3)から，D-A変換器に入力される。I/Oポート(1)(2)は，他のモジュールとの非同期的なデータの授受をハンドシェークで行うためのポートである。I/Oポート(6)は誤り検出結果を他のモジュールに送出したり，他のモジュールから入力するためのポートである。メモリ内のプログラムなど処理中に変化しないデータに関しては，間欠故障が起っても誤った状態のままにならないようにROMに格納する。

図6は，本システムのフローチャートの概略を示している。図7,8,9は，それぞれ，タイマ割込みルーチン，誤り検出，内部修復のソフトウェアを示すフローチャートである。パラメータK，Nは，それぞれ，現在処理すべき入力サンプル数と誤り検出を行ってからの信号処理の回数を表わしている。Kの値は，割込みルーチンが行われるごとにインクリメントされ，この入力信号に対する処理が終了した後にディクリメントされる。従って，K=0の間は，プロセッサはアイドル状態(No Operation)にある。信号処理がある所定の回数$N=T/T_S$に到したならば，前述したような方式に基づく誤り検出が行われる。このとき，誤

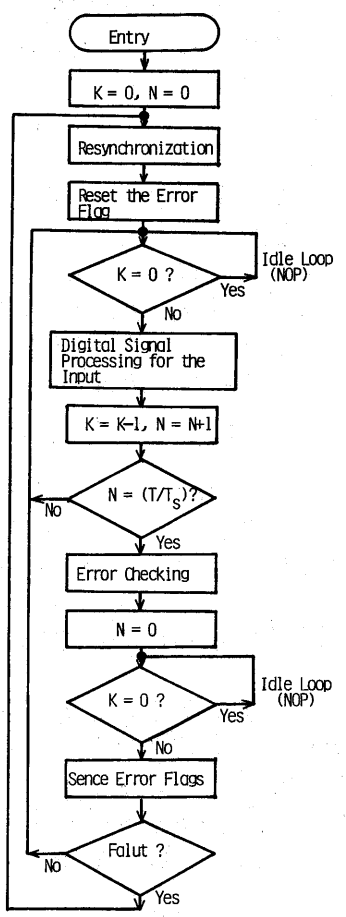

図6　ジェネラルフローチャート

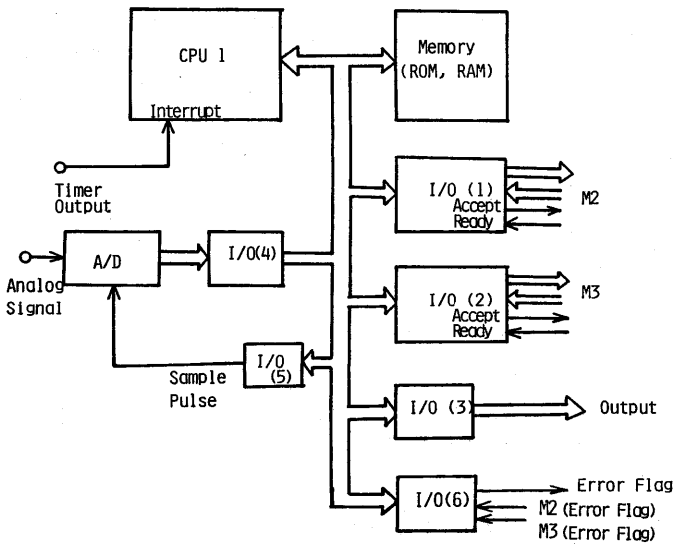

図5　各モジュールの構成図

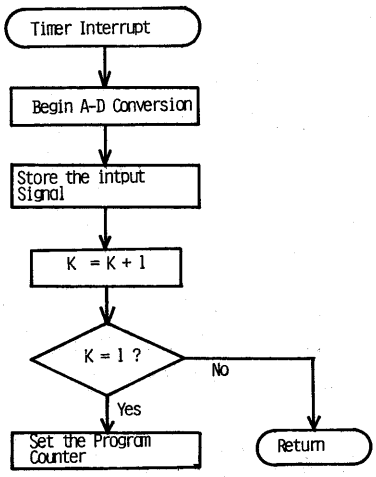

図7タイマ割込みルーチン

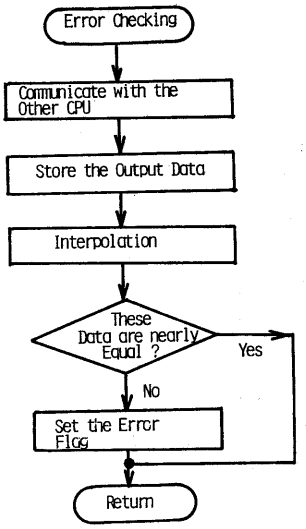

図8　誤り検出

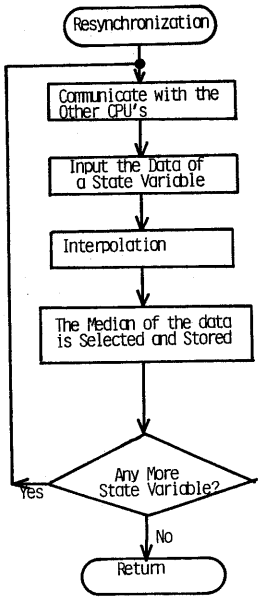

図9　内部修復

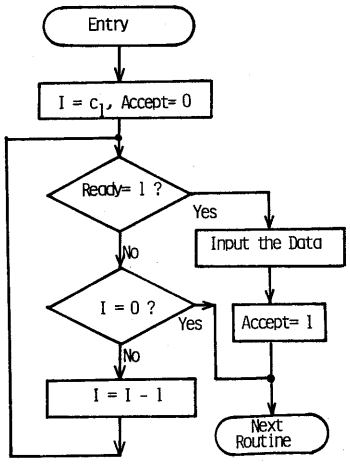

図10　ハンドシェーキング

りが検出されたならば，I/Oポート(6)の中の誤りフラグ(Error Flag)を"1"にして，この状態を他のモジュールもセンスすることになる。誤りフラグが少なくても1つ以上のモジュールで立って入れば，次の入力信号のサンプルを行った後，間欠故障の影響を除去するため内部修復を行う。内部修復は，引き続く信号処理に影響を与える全ての内部状態に対して行われる。

以上のソフトウェアにおいて，他のモジュールとのデータの授受をハンドシェークにより行うとき，1つのモジュールの誤り(プログラムの暴走など)の影響が他のモジュールに波及しないことが必要である。図10は，このようなことを考慮したデータの授受を示すフローチャートである。すなわち，定数C_1をReady="1"の信号を他のモジュールが送出するのに要する十分な値に設定することにより，他のモジュールが誤った状態にあり，Ready="0"のままでも，ループカウンタがI="0"になった時点で，次のルーチンへの分岐が可能となる。

5. 単一のCPUによる高信頼化

上述したシステムは，永久故障に対しても，単一モジュールまでの故障ならば，誤りはマスクされる。しかしながら，間欠故障のみを問題にするシステムでは，図11のように単一のCPUによる構成法も可能である。すなわち，前述のシステムと同様に，異なる時点の入力信号に対して3回，ディジタル信号処理を1つのCPUが行うことになる。異なる入力の信号処理に対して，内部状態は，それぞれ，別のRAM領域に格納される。ある時点の入力信号の処理中に，プログラムが暴走するなどして，他のRAM領域の内容が破壊されないように，タイマを入力とする制御回路を構成し，これらのRAMチップをセレクトしないようなタイミングを発生させる。従って，インパルスノイズがシステムに印加された場合でも，影響を受けるのは，その時点で実行されている信号処理のみに限られ，他の2つの信号処理が正しく行われれば，システムを再び回復させることができる。

6. 信頼度解析

以下，3重化システムの間欠故障に対する信頼度のみを考察する。本システムの信頼度関数 $R_0(t)$, $R_1(t)$ を次のように定義する。

$R_0(t)$: 時間 t において，全ての3つのモジュールが正しい確率

$R_1(t)$: 時間 t において，3つのうち1つのモジュールだけが誤まっている確率

DSPを時間 T の間の信号処理，EDを誤り検出，RSYNを内部修復で表記すると，$R_0(mT)$ と $R_1(mT)$ の関係は，次のような線形差分方程式で与えられる。

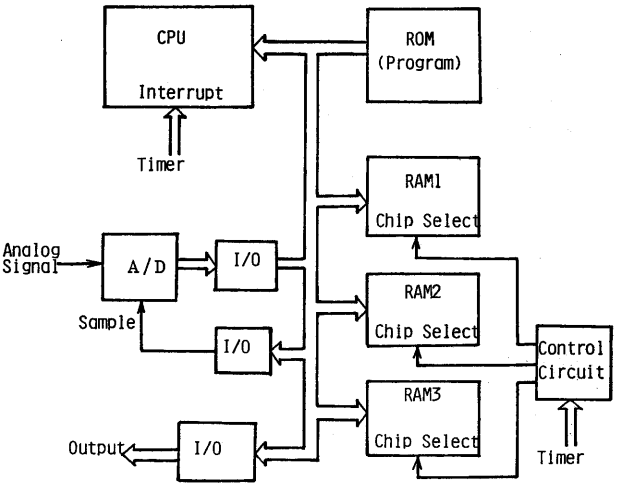

図11　1個のCPUによる構成

$R_0((m+1)T)=R_0(mT)\cdot\{$DSPとEDが3つのモジュール全てにおいて正しく行われる確率$\}+[R_0(mT)\cdot\{$DSPが2つのモジュールのみで正しく行われる確率$\}+R_1(mT)\cdot\{$他の2つのモジュールでDSPが正しく行われる確率$\}]\cdot\{$EDとRSYNが3つのモジュール全てにおいて正しく行われる確率$\}$ (6)

$R_1((m+1)T)=R_0(mT)\cdot\{$DSPが3つのモジュール全てにおいて正しく行われる確率$\}\cdot\{$EDが2つのモジュールのみで正しく行われる確率$\}+[R_0(mT)\cdot\{$DSPが2つのモジュールのみで正しく行われる確率$\}+R_1(mT)\cdot\{$DSPが他の2つのモジュールで正しく行われる確率$\}]\cdot\{$EDとRSYNが2つのモジュールのみで正しく行われる確率$\}$ (7)

式(6)(7)より，R_0 と R_1 は次のように表現できる。但し，$R_0(0)=1$, $R_1(0)=0$.

$$R_0((m+1)T)=aR_0(mT)+bR_1(mT),\ R_1((m+1)T)=cR_0(mT)+dR_1(mT) \quad (8)$$

内部修復を行わないときの信頼度関数 $f_0(t)$, $f_1(t)$, $f_2(t)$ を次のように定義する。

$f_0(t)$: 3つのモジュール全てが正しい確率　$f_1(t)$: 3つのうち1個だけのモジュールが誤る確率　$f_2(t)$: 2つのモジュールのうち全てが正しい確率

従って，a, b, c, d は，式(9)で与えられる。

$$\left.\begin{aligned} a&=f_0(T)+f_1(T-t_c)\cdot f_0(t_c+t_r),\quad b=f_2(T-t_c)\cdot f_0(t_c+t_r)\\ c&=f_0(T-t_c)\cdot f_1(t_c)+f_1(T-t_c)\cdot f_1(t_c+t_r)\quad d=f_2(T-t_c)\cdot f_1(t_c+t_r)\end{aligned}\right\} \quad (9)$$

但し，t_c, t_r はそれぞれ，誤り検出と内部修復の実行時間を示している。同時故障相関が本システムでは完全に避けられるとすると，f_0, f_1, f_2 は，λ_0 を単一モジュールの故障率とし，式(10)で与えられる。ここで，故障の発生は時間的にランダムとし，指数分布をとるものとする。

$$f_0(t)=\exp(-3\lambda_0 t),\ f_1(t)=3\exp(-2\lambda_0 t)-3\exp(-3\lambda_0 t),\ f_2(t)=\exp(-2\lambda_0 t) \quad (10)$$

本システムの信頼度 $R(t)$ は，式(8)より，式(11)で与えられる。

$$R(mT)=R_0(mT)+R_1(mT)=(1/2)\{1+(2c+a-d)/\sqrt{(a-d)^2+4bc}\}p_1^m+(1/2)\{1-(2c+a-d)/\sqrt{(a-d)^2+4bc}\}p_2^m \quad (11)$$

但し，$p_1=\{a+d+\sqrt{(a-d)^2+4bc}\}/2$, $p_2=\{a+d-\sqrt{(a-d)^2+4bc}\}/2$ である。

$\lambda_0(t_c+t_r)$が十分小さいとき，$a, b \gg c, d$であり，$R(mT)$は $R(mT)=a^m$ で近似される。高信頼度区間での信頼度を示す基準として，信頼度がR_fまで低下する時間であるMission Timeがある。冗長なシステムと非冗長なシステムのMission Timeの比はMTIF(Mission Time Improvement Factor)と定義される。式(9)(10)より，Mission Time t_mは，式(12)で近似される。

$$t_m=-(\log_e R_f/3\lambda_0^2)T/\{(T-t_c)^2+(t_c+t_r)/\lambda_0\} \quad (12)$$

t_mを最大にする最適な周期Tとそのときの MTIFは，式(13)で与えられる。

$$T=\sqrt{(t_c+t_r)/\lambda_0+t_c^2},\ MTIF=[t_c/(t_c+t_r)+\sqrt{t_c^2/(t_c+t_r)^2+1/\{(t_c+t_r)\lambda_0\}}]/6 \quad (13)$$

7. 通常のTMRとの比較

従来のTMRにおける同時故障を示すパラメータ $\lambda_{p\,of\,q}$を，q個のモジュールのうちp個同時に故障するような故障率と定義する。図12は，これらの相互関係を示すベンダイアグラムである。$\lambda_2 \equiv \lambda_{2\,of\,3}$，$\lambda_3 \equiv \lambda_{3\,of\,3}$ とすると，式(10)に対応する$f_0(t)$と$f_1(t)$は，次式で与えられる[12]。

$$\left.\begin{aligned} f_0(t)&=\exp\{-\lambda_0 t(3-\lambda_2/\lambda_0-2\lambda_3/\lambda_0)\} \\ f_1(t)&=3\cdot\exp\{-\lambda_0 t(2-\lambda_2/3\lambda_0-\lambda_3/\lambda_0)\}-3\exp\{-\lambda_0 t(3-\lambda_2/\lambda_0-2\lambda_3/\lambda_0)\} \end{aligned}\right\} \quad (14)$$

式(12)と同様にして，Mission Timeを求めたのが式(15)である。

$$t_m=-(\log_e R_f)T/\{\rho_c\lambda_0(T-t_c)+A\lambda_0^2(T-t_c)^2+(3-\lambda_2/\lambda_0-2\lambda_3/\lambda_0)\lambda_0(t_c+t_r)\} \quad (15)$$

但し，$\rho_c=(\lambda_2+\lambda_3)/\lambda_0$，$A=3+(5/6)(\lambda_2/\lambda_0)^2+(5/2)(\lambda_3/\lambda_0)^2-4(\lambda_2/\lambda_0)-6(\lambda_3/\lambda_0)+3(\lambda_2\lambda_3/\lambda_0^2)$ である。ρ_cの値は，単位時間に2個以上同時に故障する確率と単一モジュールの故障率の比である。t_mを最大にする最適な周期とそのときのMTIFは，式(16)で与えられる。

$$T=\sqrt{t_c^2+\{(3-\lambda_2/\lambda_0-2\lambda_3/\lambda_0)(t_c+t_r)-\rho_c t_c\}/(A\lambda_0)}$$

$$MTIF=1/\{\rho_c-2A\lambda_0 t_c+2\sqrt{A\lambda_0\{(3-\lambda_2/\lambda_0-2\lambda_3/\lambda_0)(t_c+t_r)-\rho_c t_c+A\lambda_0 t_c^2\}}\} \quad (16)$$

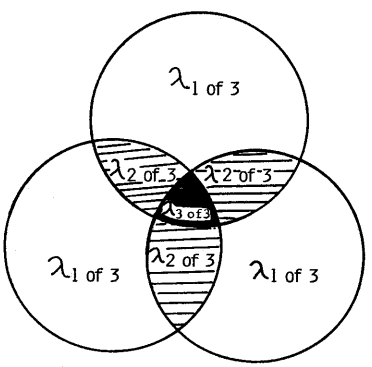

図12 故障相関を示すベンダイアグラム

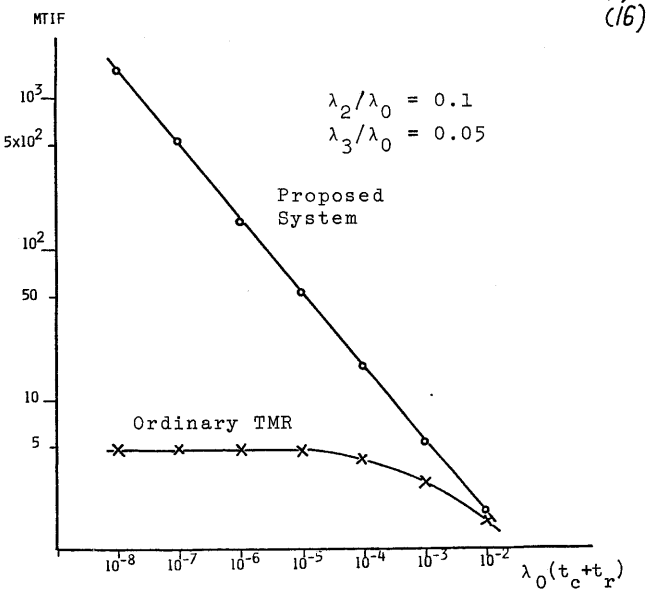

図13 MTIFの比較

従って，MTIFは，最適な周期Tで誤り検出を行った場合でも1/危以上に改善できないことがわかる。

以上の比較を図示したのが，図13であり，この場合，$\lambda_2/\lambda_0=0.1$，$\lambda_3/\lambda_0=0.05$，$t_c=t_r$にパラメータを設定してある。通常のTMRでは，故障率λ_0が十分小さくても，信頼度を1/危=6.7以上向上できないのに対し，本システムは信頼度を大幅に向上させることができることが明らかとなった。

8. むすび

本論文では，ディジタル信号処理特有の新しい誤り検出及び内部修復法に基づく高信頼化を目的としたマイクロコンピュータシステムを提案した。複数個のモジュールの故障相関が強い環境中において，従来のTMRと比較して大幅に信頼度を向上できることを明らかとした。

信号処理の多くの応用においては，入力信号はセンサを通してマイクロプロセッサに取り込まれる。このとき，プロセッサとの接続配線が長くなることなどにより，入力信号に雑音が重畳する可能性が多いと考えられる。本システムでは，このような場合でも，異なる時間の入力信号をそれぞれのプロセッサが処理しているため，このような誤りも検出できるという特長を有している。

文献

(1) L. R. Rabiner and B. Gold, Theory and Application of Digital Signal Processing, New Jersey: Prentice-Hall, Inc., 1975.

(2) T. Higuchi, T. Saito and A. Kanomata, "A Microprocessor-Based Digital Filter Programmed in a Block Diagram Language," IEEE Trans. Ind. Electron. Contr. Instrum., vol. 24, pp. 231-234, Aug. 1977.

(3) M. Townsend, M. E. Hoff, Jr., and R. E. Holn, "An NMOS Microprocessor for Analog Signal Processing," IEEE Trans. Comput., vol. 29, pp. 97-102, Feb. 1980.

(4) T. Nishitani, Y. Kawakami, R. Maruta and A. Sawai, "LSI Signal Processor for Communications Equipment," in Proc. Int. Conf. on Acoustic Speech and Signal Processing, pp. 386-393, April 1980.

(5) A. Avizienis, et al., "The Star Computer: An Investigation of the Theory and Practice of Fault-Tolerant Computer Design," IEEE Trans. Comput., vol. 20, pp. 1312-1321, Nov. 1971.

(6) J. A. Abraham and D. P. Siewiorek, "An Algorithm for Accurate Reliability Evaluation of Triple Modular Redundancy Networks," IEEE Trans. Comput., vol. 23, pp. 682-692, July 1974.

(7) J. F. Wakerly, "Transient Failures in Triple Modular Redundancy Systems with Sequential Modules," IEEE Trans. Comput., vol. 24, pp. 570-573, May 1975.

(8) J. F. Wakerly, "Microcomputer Reliability Improvement Using Triple-Modular Redundancy," Proc. IEEE, vol. 64, pp. 889-895, June 1976.

(9) J. H. Wensley, et. al., "SIFT: Design and Analysis of a Fault-Tolerant Computer for Aircraft Control," Proc. IEEE, vol. 66, pp. 1240-1255, Oct. 1978.

(10) I. Koren and S. Y. H. Su, "Reliability Analysis of N-Modular Redundancy Systems with Intermittent and Permanent Faults," IEEE Trans. Comput., vol. 28, pp. 514-520, July 1979.

(11) 亀山、樋口、"TMRによるフォルトトレラントマイクロコンピュータシステムの一構成法、"信学技報 EMCJ78—57、pp. 11—16、Jan. 1979.

(12) M. Kameyama and T. Higuchi, "Design of Dependent-Failure-Tolerant Microcomputer System Using Triple-Modular Redundancy," IEEE Trans. Comput., vol. 29, pp. 202-206, Feb. 1980.

(13) R. W. Hamming, Digital Filters, Prentice-Hall, Inc., 1977.