設 計 自 動 化 77－21
(1995. 10. 20)

ハードウェア・ロールバック機能を持つシステムによるデジタル信号処理

石井 信　松原 隆　古賀 義亮

防衛大学校 情報工学教室
〒239 横須賀市走水1-10-20
E-Mail: mako@cc.nda.ac.jp

あらまし：ハードウェア・ロールバック機能を持つ高信頼システム用マイクロプロセッサGMICRO/100 for Fault Tolerant Systemが試作された．その特徴として，汎用32ビットマイクロプロセッサGMICRO/100と２重系を構成し，従来ソフトウェアで行っていたロールバックをハードウェアで自動的に行うことができることがある．その高信頼化動作がデジタル信号処理には影響を及ぼすことがある．そこでデジタル信号処理における処理中断の影響程度を明らかにし，その影響を軽減する一方法として，ＦＩＦＯバッファを用いることが有効であることを示す．

キーワード：ロールバック，デジタル信号処理

Digital Signal Processing on hardware rollback system

Makoto Ishii　Takashi Matsubara　Yoshiaki Koga

Department of Computer Science, National Defense Academy
1-10-20,Hashirimizu,Yokosuka,Japan

E-Mail: mako@cc.nda.ac.jp

Abstract : The microprocessor GMICRO/100 for fault tolerant systems has been developed for highly-reliable system equipped with built-in coincidence checker, hardware rollback operation and recovery functions. For a real time fault-tolerant system, a duplex system is composed by GMICRO100FTS and GMICRO/100 for general use.

We show that the check point setting up and the rollback operations affect to digital signal processing and also show that a FIFO buffer is effective to reduce distortions in digital signal processing.

key words : rollback operation, digital signal processing

1. はじめに

近年，コンピュータ技術の発展により家電製品やＯＡ機器をはじめとして，様々な分野の多種多様な機器にコンピュータが組み込まれ運用されている．それらは，システムの自動化・省力化に大きく貢献しているが，航空機の制御や銀行の現金自動支払いシステムなどの分野においては，故障が生じた場合に，誤動作によって重大な障害をもたらす恐れがあり，障害に強いコンピュータシステムの研究・開発が進められている[1]．

その様な中で，通産省・工技院委託研究である「電力用リアルタイム制御システムの信頼性向上に関する調査研究」において，三菱電機により，自動障害検出/障害訂正機能を持たせることを目的とした高信頼システム用マイクロプロセッサGMICRO/１００ for Fault Tolerant System（以下G/１００ＦＴＳと略記する）が試作された．このプロセッサは，ロールバック機能[2]~[5](システム障害が発生した場合に同じ処理を再実行する機能，主として瞬時故障のリカバリに使用)・オンチップの自己診断機能等により高い信頼性を得ている．

本報告では，早いリアルタイム動作環境での性能を検証するために，デジタル信号処理における高信頼化動作，特にロールバック機能・動作による問題を明らかにする．

2. 高信頼マイクロプロセッサG／１００ＦＴＳについて

2.1 G／１００ＦＴＳの概要と特徴[3][4]

本研究で使用した高信頼マイクロプロセッサG／１００ＦＴＳは，トロン仕様に基づく汎用３２ビットマイクロプロセッサGMICRO／１００(以下G／１００と略記する）をコア・プロセッサとしたＡＳＩＣマイコンであり，特に高信頼システムを構築する場合に有効な機能を備えている．

G／１００ＦＴＳではソフトウェアに負担をかけることなく信頼性の高いシステムを構築することを目的としており，わずかなハードウェアの付加を行うことによってシステムが構成できる．従来ソフトウェアに依存している機能をプロセッサ内部のハードウェアで実現することにより，プログラムの作成に負担をかけずに高信頼コンピュータ・システムを実現可能としている．

G／１００ＦＴＳとG／１００を用いて構成した２重系コンピュータシステムの特徴を以下簡単に記述する．

（1）G／１００とソフトウェア的に等価

命令セットレベルでG／１００ＦＴＳはG／１００と互換があり，G／１００用に開発されたプログラムの大部分をG／１００ＦＴＳを用いたシステムで使用が可能である．

（2）バスサイクル毎の監視

データバス，アドレスバスをはじめとし，制御信号線についてもG／１００の出力信号とG／１００ＦＴＳ内部のコア・プロセッサの出力信号の一致／不一致をバスサイクル毎に検出する．データの保証は出力信号の一致確認後にデータ・ストローブ信号を出力することによって行い，誤ったデータが周辺デバイスに対して書き込まれることを防ぐ．

（3）ハードウェアによるロールバック

従来ソフトウェアで行っていたロールバックをハードウェアで実現しており，G／１００で開発された既存のソフトウェアを大幅に手直しすることなくG／１００ＦＴＳを用いた高信頼コンピュータ・システムに組み込める．また，ロールバック機能は外部メモリ，Ｉ／Ｏ等になんら影響を与えることなく実行されるため，メモリ回路や周辺Ｉ／Ｏに関しても特に再設計を行う必要がない．

（4）オンチップの自己診断

２重系システムにおいても不良マイクロプロセッサの特定を可能にするため，オンチップ診断機能を備える．永久的な故障が発見された場合には各々の診断を独立して行うため，G／１００ＦＴＳ内部のコア・プロセッサ，及びG／１００の双方を診断するための機能を有している．診断は，G／１００ＦＴＳ内部の診断プログラムより行い，単にバスサイクル毎だけではなく，全てのマシンサイクルにおける信号の診断を行う．

（5）縮退動作

診断結果によっては，システムをコア・プロセッサ単体で動作させたり，G／１００単体で動作させたりする縮退動作を可能としている．縮退動作時は高信頼システムではなく通常の単体システムと同様であり，外部に対しては縮退動作を行っていることを信号によって知らせる仕様になっている．

（6）少ない部品点数

高信頼化動作のためのハードウェアを，一つのＬＳＩであるプロセッサ周辺に作り込むことにより，多くの部品で構築する必要があった制御回路を少ない部品数で実現している．これらは部品点数の削減によるシステムの高信頼化にも貢献している．

また今回の応用ボードには，コンピュータ・システム中でのG／１００ＦＴＳの機能評価，性能評価をおこなうため，故意に障害を発生させるための障害発生回路，動作状態表示機能等を備えている．

図１に今回の実験に用いたシステム構成を示す．

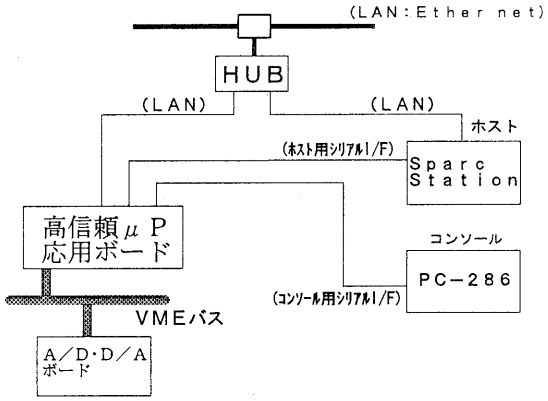

図1　システム構成

2.2　G／１００ＦＴＳの実時間処理について

実時間処理を行うにあたり，G／１００ＦＴＳの高信頼化（ロールバック機能）がもたらす影響について調べた．処理速度については，表１のように高信頼化動作のため，処理速度の低下がみられた．この理由については後述の(1)(2)などが考えられる．

表１　タイマによる命令実行時間測定結果

内　容	２重系 [μS]	縮退 [μS]	比 縮退/2重系	
add 命令	0.35	0.22	0.63	
scb 命令	0.49	0.44	0.90	
pib 命令	1.47	1.14	0.78	
mov 命令	2.21	1.45	0.66	VME への出力
mov 命令	2.21	1.45	0.66	VME からの入力
mov 命令	2.47	1.56	0.63	ﾒﾓﾘへの出力
mov 命令	2.47	1.56	0.63	ﾒﾓﾘからの入力
mov 命令	0.35	0.22	0.63	ﾚｼﾞｽﾀ→ﾚｼﾞｽﾀ
平　均			0.69	

(1)パイプライン処理について
マイクロプロセッサ内部処理はパイプラインで行われており，パイプラインの状態はそれ以前のパイプライン状態と実行する命令に依存する．
従ってやり直しを開始する時点で，それ以前のパイプライン状態を再現することは不可能である．
G／１００ＦＴＳでは処理再開のためのコンテキスト情報を蓄積する度にパイプラインをすべてパージし，処理のやり直し時に全てパイプラインがパージされた状態から開始している[3]．通常処理中のコンテキスト待避処理毎にパイプラインが全てパージされパイプライン処理プロセッサの機能を一時的に低下させる．

(2)コンテキストセーブによる処理速度の低下

ロールバックを行うためには，ある時点での正しいマイクロプロセッサの内部のレジスタの値とその時点以降のマイクロプロセッサが読み込んだ情報が必要となる．このマイクロプロセッサ内部のレジスタ値をメモリに退避した時点を以下チェックポイント，その時のマイクロプロセッサ内部のレジスタ値をコンテキストと称し，さらに内部レジスタの値をメモリ（ＲＡＭ）に退避することをコンテキストのセーブと称する[3]．

G／１００ＦＴＳは，マイクロプロセッサ内部のレジスタ値と，チェックポイント以降にマイクロプロセッサが読み込んだデータを，全てG／１００ＦＴＳと同一ＬＳＩ上のメモリ(ＲＡＭ)に格納する．チェックポインティングを頻繁に行うと，実行速度が遅くなり，一方，チェックポインティングが少なすぎると，システム障害が発生したときのリカバリに多大な時間がかかると共に，データの保存領域の確保が問題となる．チェックポイント設定条件は，エラーの発生頻度や処理系などにより定まる．今回のG／１００ＦＴＳは約５１２バスサイクル（約３２０μｓ）毎にチェックポイントを設けている[5]．これはメモリ空間の制限によるものである．このチェックポイント生成に要する時間はG／１００ＦＴＳでは約２１μｓであり，これは，ＭＰＵの実効速度の低下を生じさせる．図２にスループログラム（Ａ／Ｄ入力データをそのままＤ／Ａに出力）における出力写真を示す．コンテキストセーブによる処理の中断がわかる．

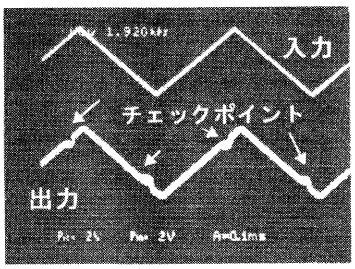

図２　ｽﾙｰﾌﾟﾛｸﾞﾗﾑによる入力と出力

3.　ロールバックによる処理中断の影響

3.1　ロールバックによる処理の中断

ロールバック動作では，内部ＲＡＭに貯えられた情報を用いて，外部メモリ（主記憶）や周辺機器を一切アクセスすることなく，ロールバック前と全く同一の動作を再現する．しかし，これらの間は，外部からの割り込みや，データを受付ない．同様にチェックポイントにおけるコンテキストセーブ，２重系から単体への縮退動作時は，ユー

ザプログラム等の処理は中断される．図３は差分方程式による正弦波の出力中に，ロールバックが発生したものである．その中の直線部分が処理中断時間を表す．また図３より，中断後正常に動作を継続していることがわかる．

図３の出力における横の直線はロールバックによる処理の中断を示しているが，ロールバックに要する時間は，チェックポイントとエラー発生時点によって定まるため，プログラムやエラーの発生した場所によって異なっていることが，図より確認できる．

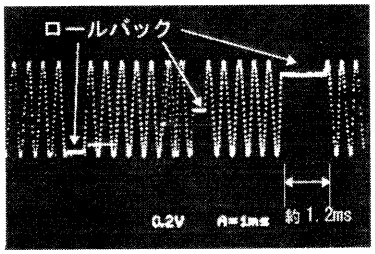

図３　処理中断が生じた正弦波出力

3.2　ロールバックによる出力の変化

3.1で示したようにG／１００ＦＴＳは，ロールバック等の実施間は外部メモリ（主記憶）や周辺機器を一切アクセスしないため，その間外部データに対しては未処理期間が生じてしまう．

数値演算等時間的要因に影響されない処理系や，データのサンプリング速度が十分に遅い処理系では問題は生じないが，より高いリアルタイム性を要求するシステムでは影響を受けることが予想された．

そこでこのシステムに対して，リアルタイム性を検証するため，速い応答速度を要求する，デジタルフィルタを用いた．今回は２次のＩＩＲフィルタ（ＢＰＦ）[6]を用いた．その伝達関数は

$$H(z)=\frac{a_0+a_1z^{-1}+a_2z^{-2}}{1+b_1z^{-1}+b_2z^{-2}} \qquad (1)$$

であり，Z^{-1}は単位遅延を表すので，差分方程式は

$$y(nT)=\sum_{k=0}^{2}a_k u(nT-kT)-\sum_{k=1}^{2}b_k y(nT-kT) \qquad (2)$$

である．フィルタ構造は図４のようになっている．

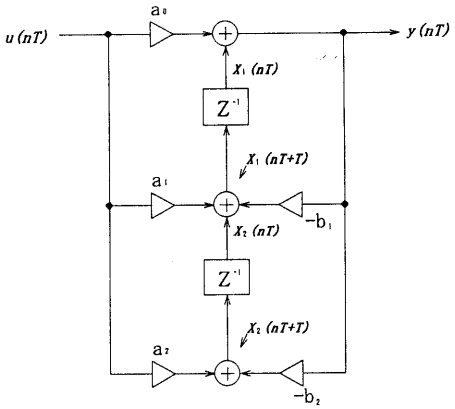

図４　フィルタ構造

これを状態空間表現すると
状態方程式：

$$\begin{bmatrix}x_1(nT+T)\\x_2(nT+T)\end{bmatrix}=\begin{bmatrix}-b_1 & 1\\-b_2 & 0\end{bmatrix}\begin{bmatrix}x_1(nT)\\x_2(nT)\end{bmatrix}+\begin{bmatrix}a_1-a_0b_1\\a_2-a_0b_2\end{bmatrix}u(nT) \qquad (3)$$

出力方程式：

$$y(nT)=\begin{bmatrix}1 & 0\end{bmatrix}\begin{bmatrix}x_1(nT)\\x_2(nT)\end{bmatrix}+\begin{bmatrix}a_0\end{bmatrix}u(nT) \qquad (4)$$

である．

上記のようなフィルタを用いた結果，ロールバックによる中断が生じると図５（中心周波数付近での入力），図６（通過帯域の上）の写真のような出力差を生じることが観測される．これは，ロールバックによる処理の中断が影響しているものと考えられる．

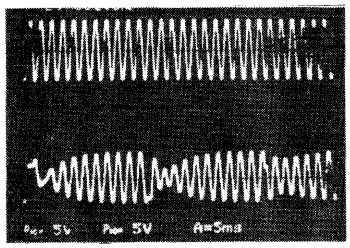

図５　ﾛｰﾙﾊﾞｯｸが発生したBPF出力
（中心周波数付近）

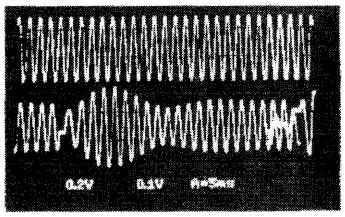

図６　ﾛｰﾙﾊﾞｯｸが発生したBPF出力
（通過帯域の上）

そこで，図５の写真について，異常出力の原因を明らかにするため，ロールバックによるデータの抜けのみを考慮し，Mathematicaにより，式(2)の形でシミュレーションを行うと，図７のような結果が得られた．図８に図５，７を重ね合わせて表示した．これにより，処理中断の影響の原因は主に，データの抜けであることが明らかになった．

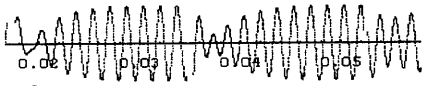

図７　処理中断のシミュレーション

図８　シミュレーションと写真の合成

ロールバック時の内部状態について考慮し，デジタルフィルタ出力についてさらに解析する．

デジタルフィルタの線形性から，図７について考える．最初のロールバックの時点における内部状態，$x_1(0)=0.57$ と $x_2(0)=-0.52$ が与えられ，入力がないときの出力は，図９のようになる．

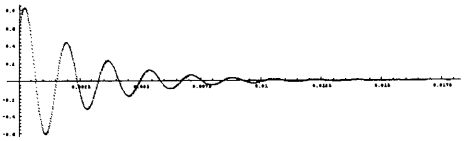

図９　内部状態のみによる出力

これは，インパルス応答と同様に個々のフィルタ特有の振動を表す．

また，$x_1(0)=0$ と $x_2(0)=0$ で，図７の最初のロールバック後の時点での正弦波が入力された時の出力は，図10の様になる．

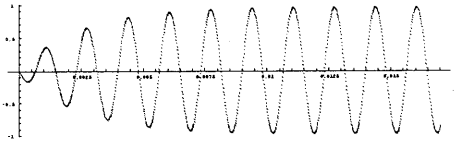

図10　正弦波入力による初期応答

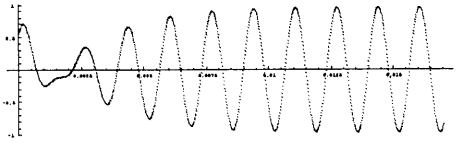

図11　出力の和

これも　図９と同じで，個々のフィルタ特有の振動であり，入力により変化する．図９と10の出力の和を求めると，図11のようになり図７の出力と一致する．

これにより，このような異常な振動現象がおきるのは，ロールバックによる中断毎に，入力が無い内部状態のみによる出力と，新たな入力によるフィルタの過渡応答の和が出力されるためであることがわかる．

よって，ロールバック後の出力は，ロールバック時に遅延素子に残っている内部状態と，新たな入力によって，変化するものと考えられる．

3.3　中断時間と出力

次に入力周波数の１周期に対して，どの程度の処理の中断を許すことができるのかを調べた．

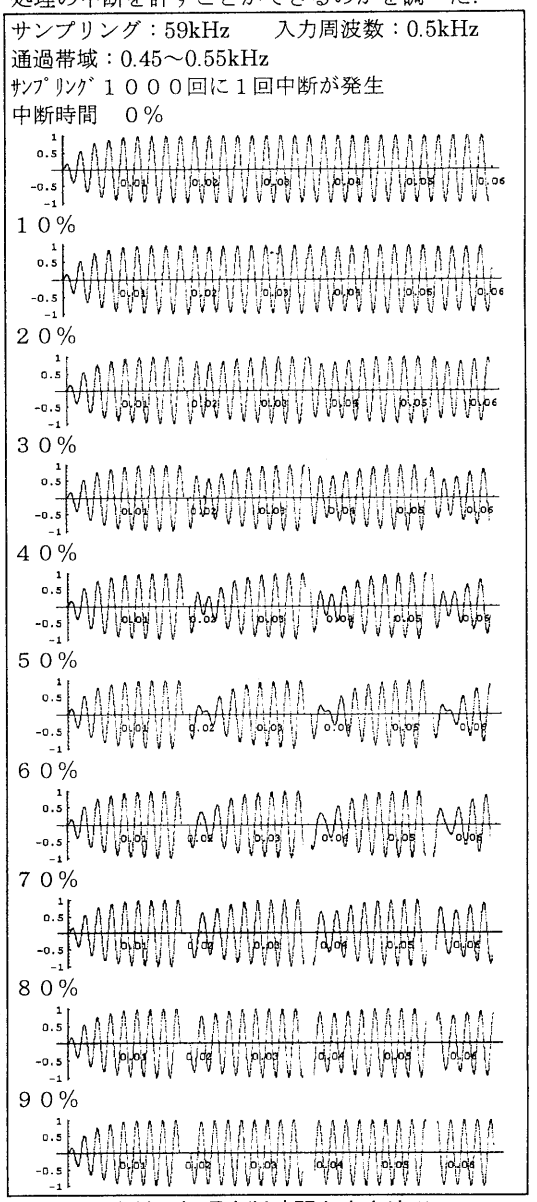

図 12　処理中断時間と出力波形

処理中断時間を入力周波数の１周期の０～９０％まで１０％づつ変化させた時の出力の変化をシミュレーションすると図12になる．

図12により，処理中断時間の変化が出力波形に及ぼす影響がわかる．

処理中断後の出力は，十分に時間が経過すると正常な状態の値に戻る．中断によってどれだけ出力波形が変化したかを，式（５）のように求めることにより，処理中断時間と出力変化の関係を，いろいろな条件のもとに調べた．

$$\frac{\sum_{t=a}^{t=b}|y(t)-y'(t)|}{\sum_{t=a}^{t=b}|y(t)|} \qquad (5)$$

y(t)は正常出力，y'(t)は中断がある時の出力

aは中断後新たに処理が始まった時点

bは(5)式を入力の1/2周期毎行い，

その値が1%以下になった時刻

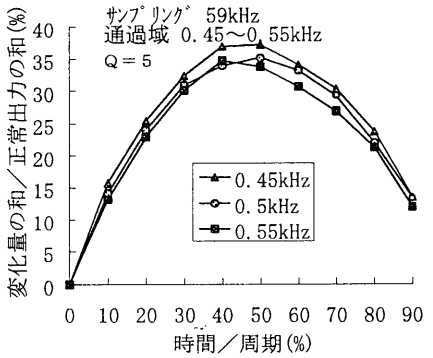

図13　入力による中断時間と出力の変化

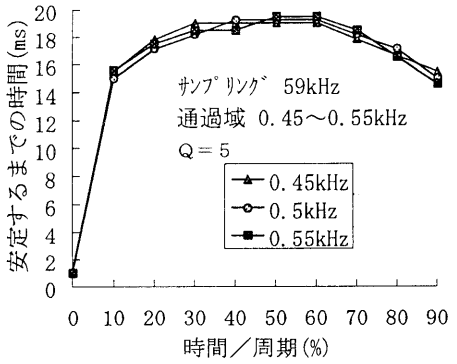

図14　入力による中断時間と安定時間

通過帯域の中心，上限下限周波数が入力された場合の，処理中断時間と出力変化の関係は，図13のグラフになる．処理中断時間と安定するまでの時間の関係は，図14のグラフとなる．

図13のグラフより，入力周波数により多少のずれはあるが，入力周波数の１／２周期程度の中断が生じた時，最大の影響が生じることがわかる．また図14より，出力が安定するまでの時間は，中断時間により，多少変動するが，ほぼ一定である．また，図16，17にQ（$Q=f/\Delta f$）が一定で，目的周波数が変化した時のグラフを示す．ただし，それぞれの入力周波数は，通過帯域の中心周波数とした．

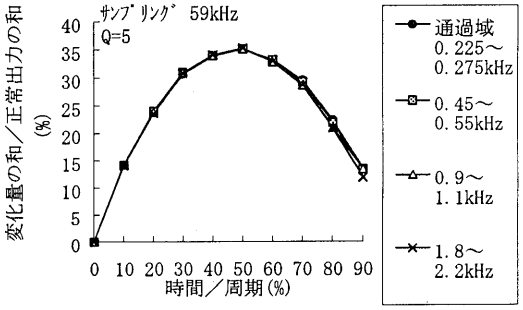

図15　各周波数における中断時間と出力の変化

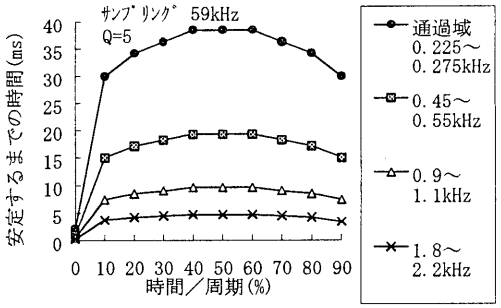

図16　各周波数における中断時間と安定時間

図15，16より，周波数が変化しても，入力周波数の１／２周期の中断時間が生じた時が最も影響が大きく，また周波数にほぼ反比例して，時間，変化量が増大するため，図16のように，同一の変化特性をもつことがわかる．

4.　問題対策

処理中断後の誤差をもたらす出力を防ぐ方法としては，

(1)同じ位相のところまで入出力しない．

応用ボード上のシステムコントロールレジスタのロールバック履歴を用い，サンプリングサイクル毎にこれを監視し，ロールバックが発生した際

に，ロールバック発生時と同じ位相のところまで入出力を行わない．これについては，最大で中断時間+1周期程の時間で復帰が可能である．しかし雑音に弱い，データの欠落が生じる等の問題がある．

(2) 目的周波数を低い範囲に限定する．

入力周波数を低くすることにより，中断時間を相対的に短くすることができる．G／１００ＦＴＳの２重系動作におけるコンテキストセーブの時間は，21μｓと短いため，1kHz程度までは影響は見られない．

実際に，現システムで実験し，比較するにあたり，フィルタ特性を等しくするため，Qを一定にし，サンプリング速度を落とす事により，係数はそのままで，目的周波数を低くして，実験を行った．基準に，サンプリング59kHz，通過帯域0.45～0.55kHz（Q＝５）のＢＰＦのプログラムを用い，これに遅延のために無意味なadd命令を挿入し測定を行った結果，図17，18の出力になった．ただし，入力周波数は，それぞれ通過帯域の中心周波数付近とした．

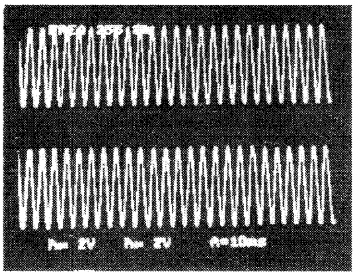

図17　無意味なａｄｄ命令によって
サンプリングを落とした出力
(ｻﾝﾌﾟﾘﾝｸﾞは30kHz，入力周波数0.26kHz)

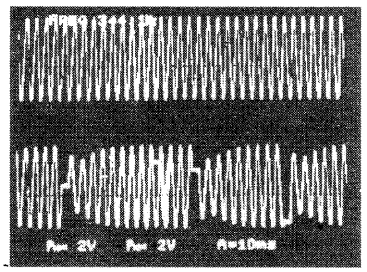

図18　無意味なａｄｄ命令によって
サンプリングを落とした出力
(ｻﾝﾌﾟﾘﾝｸﾞは40kHz，入力周波数0.35kHz)

以上のことから，十分に低い周波数(0.2kHz程度以下)であるなら中断の影響を受けないで動作が可能である．しかし，現システムの0.3%程度の能力しか出せない．

(3)　プロセッサの動作速度を上げる．

（２）と反対に，Ｇ／１００ＦＴＳの動作速度を上げることにより，高信頼化のためのチェックポイントの形成やロールバックなどの絶対時間は減少する[4][5]．それにより，入力周波数に対して，相対的に，中断時間を短くできる．例えば，動作速度が，３倍になれば，ロールバックなどの高信頼化のための時間は３分の１になる．図５の写真のロールバック時間が３分の１になった時をシミュレーションすると図19のようにになる．

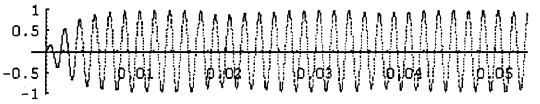

図19　中断時間が1/3のｼﾐｭﾚｰｼｮﾝ

このように，動作速度があがることにより，応用できる範囲が広がることが予想される．

(4)ＦＩＦＯバッファ等を利用

通常動作時の処理速度を下げ，中断時間のA/Dボードのデータを FIFOバッファ等に一時蓄えておき，処理中断後に処理速度を上げて処理する．

FIFOデータ処理の間は処理中断が生じない，データの送受信時間は十分に小さいものとし，サンプリング周期T_s [sec]，１入力に対する処理時間T_{work} [sec]で，$T_s > T_{work}$という条件のもとで考えると，中断時間T_{stop} [sec]に必要なFIFOバッファの量Wは，式(6)で表される．

$$W = T_{stop}/T_s \quad \text{[word]} \qquad (6)$$

FIFOバッファのデータを処理している最中も周期T_sで入力データがあるので，ロールバック後バッファのデータの処理が完了するまでの時間tは式(7)であらわされる．

$$t = T_{stop} \times T_s/(T_s - T_{work}) \quad \text{[sec]} \qquad (7)$$

入力側のみにFIFOバッファを入れた動作について，図５の写真の状態をシミュレーションした結果を図20に，また，入出力側にFIFOバッファを入れた動作について図21に示す．

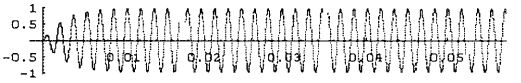

図20 入力にFIFOﾊﾞｯﾌｧを利用した
中断時間対策のｼﾐｭﾚｰｼｮﾝ

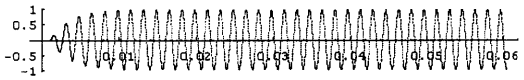

図21 入出力にFIFOバッファを利用した
中断時間対策のシミュレーション

入力側にFIFOバッファを用いることにより，入力データの抜けが生じず，振幅の変動も無くすことができる．さらに出力側にFIFOバッファを用いることにより，外部に中断の影響を及ぼすことなく，動作の継続が可能であることがわかる．

今回の実験での概略の値でFIFOバッファの必要量及び時間を計算してみる．

T_{stop} = 1ms，T_{work} = 1.8 × 10^{-2} ms (55kHz) とし，T_s = 2 × 10^{-2} ms (50kHz) とするとFIFOバッファの量は５０(word)以上必要であり，A/Dボードが16 bit幅であるものとすると100byte程度必要となる．処理時間は10ms程度である．この時間は，処理速度と中断時間に比例し，Qによって変化しないため，Qが高いフィルタ程効果が発揮される．

しかし，実際のハードウェアを設計するためには入出力側のサンプリング速度とＭＰＵ側の処理速度の同期が問題となる．これは，ＭＰＵの動作速度が，チェックポイントの形成のため一定ではないためＢＰＦのサンプリング速度が変化するので入出力側のサンプリング速度とＭＰＵの同期が困難である。

この対策の一つとしては，今回はＶＭＥバスを利用しているので，そのバス上のＤＴＡＣＫ信号等を利用することにより，入出力側のサンプリング速度に，ＭＰＵ側の速度を合わすことが可能と思われる(7)．

5. まとめ

本論文では，Ｇ／１００ＦＴＳの高信頼化動作による処理の中断がデジタル信号処理に与える影響について問題を明らかにし，その影響を軽減する一方法としてFIFOバッファを利用することが有効であることをシミュレーションにより示した．今後は，実システムにおけるFIFOバッファ及びその周辺回路の高信頼化を検討する必要がある．

参考文献

(1)当麻善弘：“フォールトトレラントコンピュータ”，信学誌,70,1,pp.289-339(1993)

(2)K.M.Chandy and C.V.Ramamoorthy：“Rollback and Recovery Strategies for Computer Programs”,IEEE Trans.Comput,**C-21**,pp.546-556(1972)

(3)“電力用リアルタイム制御システムの信頼性向上に関する調査研究報告書”，日本電機工業会，pp.289-339(1993)

(4)“電力用リアルタイム制御システムの信頼性向上に関する調査研究報告書”，日本電機工業会，pp.559-611(1994)

(5)“電力用リアルタイム制御システムの信頼性向上に関する調査研究報告書”，日本電機工業会，pp.624-673(1995)

(6)樋口龍雄：“デジタル信号処理の基礎”，昭晃堂(1992)

(7)“ＶＭＥbusアーキテクチャ・マニュアル”，ＣＱ出版株式会社(1984)