5Y-10

動的部分二重化を用いた自己組織化HWの故障検出機構について

奥村 謙一† 張替 拓真† 新井 浩志†
千葉工業大学 大学院 工学研究科†

1. はじめに

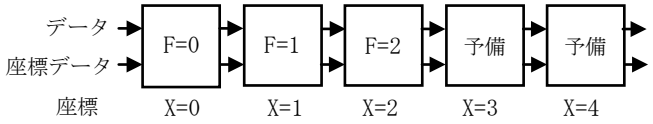
宇宙用途等で使用されるハードウェアシステムは人手による故障の修復が困難である．そのため動的部分書換え可能デバイスを用いたFTS(Fault Tolerant System)に関する研究[1]が行われている．我々は，従来より FTS を実現する手法の 1 つとして自己組織化ハードウェアに注目している．自己組織化ハードウェアは，セルと呼ばれるデバイスを複数用いて構成される進化型ハードウェアの一種である．各セルはシステム上の相対的な位置に応じた座標を持ち，実行する機能を座標に応じて動的に変化させることによって障害から回復する．このような FTS では故障からの回復方法に加えて，故障の検出が課題である．従来研究の多くは故障検出機構として TMR(Triple Moduler Redundancy) [2]やBIST(Bult-In Self Test)を前提としている．しかし TMR は耐故障回数に比べて回路規模が大きくなってしまう．一方，BIST は故障検出中にハードウェアの動作を停止させなければならない．

そこで本報告では，自己組織化ハードウェアの特徴であるセルの自律的な再構成機能を用いて故障の検出と回復を行う手法を提案する．

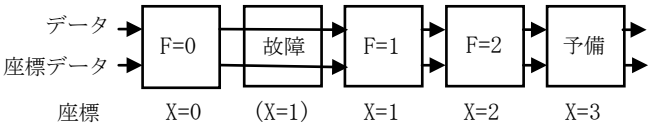
2. 自己組織化ハードウェア

本研究で提案する自己組織化ハードウェアは，セルを1次元状に接続したものである．例として，3つの機能セルと2つの予備セルから構成されるシステムを図1(a)に示す．ここで，機能セルは機能番号Fに基づく処理を行うセル，予備セルは別の機能セルが故障した時に処理を代替するセルである．データは左端のセルから入力され，各セルで処理を行い，右端のセルから出力される．同様に座標Xも左端のセルから入力され，各セルは入力された座標をインクリメントして右隣のセルに渡す．この時機能番号は座標によって決定され，機能番号＝座標となる．

X=1 のセルに故障が発生した場合に自己修復した結果を図1(b)に示す．故障したセルはセル間の接続をバイパスする．バイパス処理によって座標が変化するため，座標に応じて新たに機能が再構成される．



(a) システム構成図



(b) 故障発生

図 1 自己組織化ハードウェア

3. 動的部分二重化

3.1 故障検出

提案手法では，全てのセルのうちの座標が隣接した特定の 2 つのセルに同じ機能を持たせて処理を実行する．そして座標の大きい方のセルが自身の出力と左側のセルの出力を比較することで故障検出を行う．さらに同じ機能を持たせるセルを t クロック毎に変更することで全セルの故障検出を可能とする．これを動的部分二重化と呼ぶ．動的部分二重化を実現するために，従来のシステムに新たに冗長番号 R を導入する．R はどの機能を二重化するかを表す．各セルは，もし F が R より大きいか等しいならば F＝X，そうでなければ F＝X－1 として F を決定し，自身の機能を再構成する．

動的部分二重化の故障検出動作を図 2 に示す．この例では 5 つの機能セルから構成されている．R を 0 から F_{max} まで，t クロック毎にインクリメントすることにより，全セルを時分割で二重化し故障の検出を行う．ここで F_{max} は機能番号の最大値である． R を順次インクリメントし，F_{max} になった時は R を 0 に戻す機能を外部に設ける．

R が F_{max} から 0 に戻った時には，F_{max} クロックの間だけ右端のセルから不正なデータが出力されるという問題がある．これは，各セルが常に一つ小さい座標のセルの出力を入力としており，冗長番号がより小さい値に切り替わる時には適

Dynamic DMR : A fault detection mechanism for Self-organization hardware.
† Keinichi Okumura, Harigae Takuma, Hiroshi Arai Graduate School of Engineering, Chiba Institute of Technology.

切な機能番号のセルの出力を受け取れないためである．この問題は R が 0 になるタイミング，即ち t×F_{max} クロック毎に発生する．しかし，最終出力段に不正なデータを破棄する機能を持たせれば，ストリーミング処理の様な用途に使用する場合無視できるレベルであると考えている．

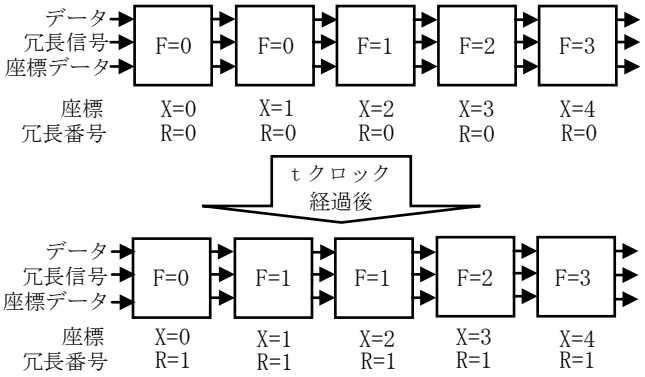


図 2　故障検出動作

動的部分二重化では，故障検出に 1 つ以上の予備セルを必要とする。そのため，予備セルが存在しない状況での故障検出は不可能である．

3.2　故障回復

図 3 は機能セル 3 個，予備セル 2 個の時の構成例である．図 3(a)で，出力の比較によって X=2 のセルが故障を検出した場合，X=1 のセルに故障信号を送信する．故障信号を受取ったセルは自身を故障状態とする．その結果 X=1 と X=2 のセルの 2 つが故障扱いとなる． これは二重化による出力の比較では，二つのセルのどちらが故障したかの判断ができないためである．

また，図には示していないが各セルは左隣のセルに故障状態を伝えるための機能を持つものとする．

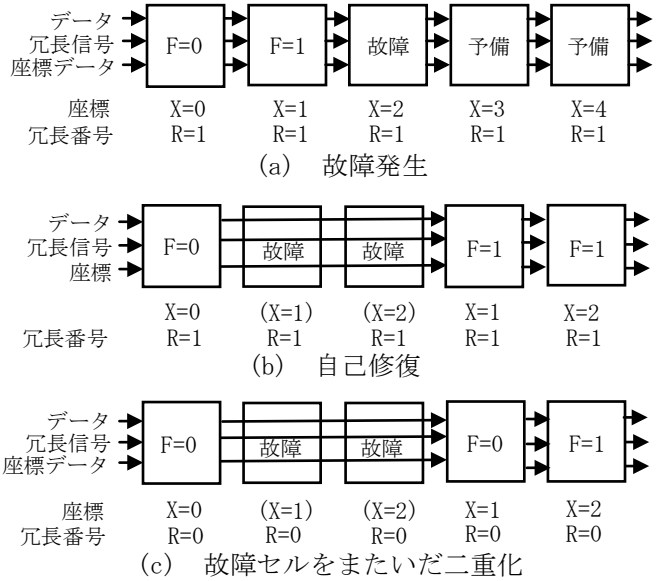


図 3　故障回復動作

故障セルがセル間の接続をバイパスすることにより，右側のセルの座標が変化し，機能が再構成されて故障から回復する(図 3(b))．

また，提案手法では故障回復後の故障検出で，故障セルをまたいで二重化される場合がある(図 3(c))．この場合も故障セルはセル間の接続をバイパスするため，通常通り故障を検出することが出来る．

本手法では，1 回の故障につき故障の回復に 2 つの予備セルを消費する．そのため，耐故障回数は予備セル数÷2 となる．

4.　考察

動的部分二重化と従来の故障検出手法の比較を表 1 に示す．

表 1　各故障検出手法の比較

	TMR	動的部分二重化	BIST
1 回の故障回復に必要な予備セル数	3	2	1
全セル数 (x=機能セル数, y=耐故障回数)	3(x+y)	x+2y	x+y
故障検出のタイムラグ	なし	あり	あり
故障検出中の動作	可能	可能	不可能

提案手法により，必要な全セル数，即ち回路規模が TMR に比べて減少している．しかし BIST と同様に故障検出時にタイムラグが生じてしまうという問題がある．しかし，BIST に比べて提案手法のタイムラグは非常に短い．また，BIST よりも故障回復に必要な予備セル数は多いが，故障検出中にも動作を続けることが可能である．

提案手法の動作を検証するために，VHDL によるセルの設計とシミュレーションを行った．冗長番号の変更による機能セルの再構成機能や故障時のバイパス機能が問題なく動作することを確認した．

5.　終わりに

本研究では，自律的な再構成機能を用いた故障検出手法を提案した．また，VHDL によるシミュレーションを行い，提案手法の動作を確認した．今後の課題として，冗長番号が 0 に戻した時に不正な値が出力されないようにする機構の検討があげられる．

参考文献

[1]　金丸 敦礼,他,“書き換え可能ハードウェアを用いた耐故障性能向上手法の研究”,信学技報,RECONF,リコンフィギャラブルシスシステム Vol.108,No.220,pp.81-86,2008.

[2]　椿 龍也,新井 浩志,“自己組織化ハードウェアによるフォールトトレラントシステムのための自律制御機構についての研究”,情処全国大会講演論文集,Vol.67,No.1,pp.143-144,2005.