耐永久故障FPGAアーキテクチャの予備評価

岡田崇志† 喜多貴信† 五島正裕† 坂井修一†
†東京大学大学院情報理工学系研究科

1 はじめに

宇宙用途のLSIは，放射線や，激しい温度サイクルのため，過渡故障のみならず，永久故障が発生する確率も増大する．また，宇宙用途では，交換が困難であるため，1個のLSIの故障がシステム全体の運用停止につながり得る．そのため，宇宙用途のLSIには，地上用途に比べて，格段に高い信頼性が要求される．

高い信頼性を確保するため，従来用いられてきた**MIL規格品**[1]は，低性能，高価格，長納期など，通常部品に比べてデメリットを持つ．そこで，通常用途のFPGAに対して，わずかな追加ハードウェアで故障耐性を付加することを考える．このアプローチによる利点は二つある．

一つは，通常用途との両立が可能な点である．耐故障性のための追加ハードウェアが十分に小さければ，通常用途向けに大量に製造し，安価に販売しながら，その全く同一のFPGAを宇宙用途向けに使用することが可能になる．

もう一つは，性能面での優位である．通常用途のFPGAをベースにするため，民生品と同様の最先端のテクノロジを用いて製造される．したがって，FPGAであっても，MIL部品など，2〜3世代前のテクノロジで製造されるASICと比して十分な性能が提供できる．

一方で，通常用途FPGAは，最先端の微細なテクノロジを用いて製造されることが一般的であり，放射線に対する感受性は高い．そのため，故障に対しては，回避ではなく，検知，回復によって対処することになる．本手法では，**TMR**(Triple Modular Redundancy)を用いて，故障検知を行い，**動的部分再構成**を用いて故障回復を行う．

Preliminary Evaluation of Fault-tolerant FPGA Architecture
Takashi Okada †, Takanobu Kita †, Masahiro Goshima †and Shuichi Sakai †
†Graduate School of Information Science and Technology, The University of Tokyo

[1]米軍使用の高信頼部品

2 提案手法

2.1 Recovery Manager

再構成を用いた故障回復では，故障した回路を物理的に離れた別の場所に再構成する必要がある．その際に，新たに配置配線を行う必要があり，これには計算コストがかかるため，何らかの計算資源が必要である．

従来の手法[1]には，そのような計算のための専用ロジックを，ハードワイアード・ロジックで追加することを想定したものが多い．ここでは，このようなロジックをRM(Recovery Manager)と呼ぶ．RMは，一度故障すればシステム全体の故障回復能力が失われることになるため，他の回路と同程度の故障耐性を備えていなければならない．そこで，RM自体に故障耐性を付加するために冗長性を加えると，追加するハードウェア量がさらに大きくなってしまうという問題がある．

本手法では，RMをFPGAのユーザ・ロジック領域[2]に他の回路と同様に実装する．さらに，RM自身に生じた故障を自分自身で検知，修復できる仕組みを導入する．この方法によって．以下のように先述した問題を解決できる．

- RM自身にも，他のユーザ・ロジックと同様の高い故障耐性を確保できる．特に，FPGAの再構成を利用できるので，ハードワイアード・ロジックでは実現できない柔軟な故障回復が可能である．
- 追加すべきハードウェアを小さく抑えることができる．RMはユーザ・ロジックとして構成されるため，通常用途のFPGAとして使用する際はRMを構成せず，その領域を自由な用途に割り当てることができる．

2.2 全体構成

提案する手法の概略図を図1に示す．ユーザ・ロジック領域全体はタイルと呼ばれる単位で分割されており，全てのタイルが再構成ネットワークで接続された構造となっている．それぞれのタイルには，再構成ネットワークにアクセスするために，ネットワークIFが1つ

[2]FPGAにおいて，ユーザーが使用するプログラム可能な領域．

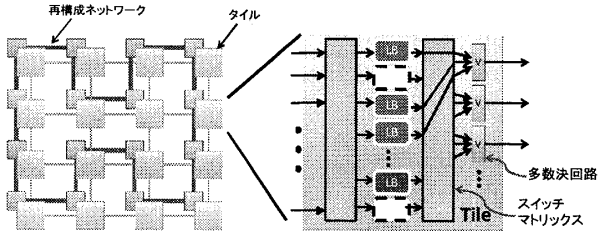

図 1: 全体構成

ずつ付属している．タイルの内部には，ロジックブロック (LB) が数百個程度含まれており，同一の機能を持つ LB を三つで TMR を構成している．ここで LB とは，一組の LUT(Look-Up Table)+FF と定義する．タイル間，LB 間での，信号のやり取りは FPGA 上の通常の配線が使用されるが，故障情報，及び再構成データの伝達に限り，特別に用意されたネットワーク IF を通して再構成ネットワーク上で伝達される．

2.3 故障回復

TMR は単一の故障をマスクすることができるが，一度故障が発生すると TMR の持つ冗長性は失われる．そこで，本手法では故障を検出した際に，故障箇所を再構成し，TMR 状態を回復する．

故障を検知すると，RM が再構成用のコンフィギュレーションデータを再計算する．過渡故障が発生した場合と永久故障が発生した場合の回復方法について説明する．

過渡故障の場合は，物理的な損傷ではないため，故障が起こった LB に，元のデータで上書きすることで過渡故障から回復する．

故障が発生した際に再構成を何度か繰り返しても，回復しない場合は永久故障と判断する．この場合には，元の LB の複製を，タイル内の別の位置にある予備の LB 上に構成し，再配線する．

なお，RM を含め，全てのロジックは三重化されており，故障が発生した際もシステム全体はオペレーションを継続できる．

2.4 再構成ネットワーク

再構成ネットワークは，故障情報と，再計算されたコンフィギュレーションデータ (CFD) を伝達するために，特別に追加するネットワークである．全てのタイルは，再構成ネットワークのノードに相当し，ネットワーク IF を通して，アクセスできる仕組みになっている．再構成ネットワークは，次の二つの機能を持つ．

一つは，故障情報と CFD の伝達である．タイル内の多数決回路から送信された故障検出信号，及び，再構成に必要な CFD は，ネットワーク IF を介して再構成ネットワーク上に，パケットの形で送信される．

もう一つは，再構成の機能である．ネットワーク IF は，自身のタイルのコンフィギュレーションメモリに対する読み書きの機能を持っている．そのため，ネットワークを通じて受信した CFD を用いてタイルを再構成することができる．

3 予備評価

本手法によって追加すべきハードウェアは，多数決回路及びネットワーク IF である．多数決回路は，3LB あたりに一つの割合で追加する必要がある．この場合，トランジスタ数換算でのオーバーヘッドは以下のように計算できる．

$$\frac{\text{多数決回路のトランジスタ数}}{1LB\text{ のトランジスタ数} \times 3}$$

LB を 4 入力 LUT + FF とすると，これは，約 200 トランジスタで構成可能である．多数決回路は 18 トランジスタなので，この際のオーバヘッドは約 3%である．

一方ネットワーク IF は，約 3600 トランジスタで実装可能であることを確認しているので，1Tile = 500LB = 10 万トランジスタとすると，オーバヘッドは，

$$\frac{\text{ネットワーク } IF\text{のトランジスタ数}}{1Tile\text{ のトランジスタ数}} = 3.6\%$$

である．実際には，これらの追加ハードウェアは，粗いプロセスルールで作ることを想定しているので，面積を考えるとトランジスタ数で比較した結果より大きなオーバヘッドになることが予想される．しかし，FPGA のチップ面積の大半が配線領域に費やされていることを考えると，チップ面積全体に対する追加ハードウェアの面積は無視できるほど小さいと考えられる．

4 おわりに

本稿では，わずかな追加ハードウェアで FPGA に高い故障耐性を付加する手法を提案した．今後は，テストベッドを用いて本手法の詳細な評価を行う予定である．

参考文献

[1] Abramovici, M., Strond, C., Hamilton, C., Wijesuriya, S. and Verma, V.: Using roving STARs for on-line testing and diagnosis of FPGAs in fault-tolerant applications, *Test Conference, 1999. Proceedings. International*, pp. 973–982 (1999).