FPGAによるリアルタイム制御回路用のFail Safe回路

中條 直也† 橋山 智訓†† 古橋 武†† 大熊 繁†††‡

†(株)豊田中央研究所 〒480-1192 愛知県長久手町
Tel 0561-63-4599, E-mail chujo@iclab.tytlabs.co.jp

††(財)名古屋産業科学研究所 〒463-0003 名古屋市守山区下志段味
Tel 052-739-1889, E-mail hashiyama@nisri.moriyama.nagoya.jp

†††名古屋大学 〒464-8603 名古屋市千種区不老町
†††Tel 052-789-2792, E-mail furuhashi@nuee.nagoya-u.ac.jp
‡Tel 052-789-2775, E-mail okuma@okuma.nuee.nagoya-u.ac.jp

あらまし

動的書換え可能なFPGAを利用したリアルタイム制御回路用のFail Safe回路を提案する．最近のFPGAの中にはチップ全体の書換えを1 ms以内で行うことが可能なデバイスが開発されている．この高速な書換え機能を生かして，正常動作時にはFPGAを故障検出回路として構成し，故障検出後にはFPGAをBack Up回路に再構成するFail Safe回路を提案する．複数のリアルタイム制御回路に対して一つのFPGAでFail Safe機能を提供できるため，提案する回路を利用した場合，個別にFail Safe回路を用意する従来に比べ，低コスト化，小型化が可能である．

キーワード FPGA，動的再構成，リアルタイム制御回路，フェールセーフ

A Fail Safe Circuit for Real-time Controllers Using FPGA

Naoya Chujo†, Tomonori Hashiyama††, Takeshi Furuhashi††† and Shigeru Okuma††† ‡

†Toyota Central R&D Labs., Inc., Nagakute, Aichi, 480-1192
†Tel 0561-63-4599, E-mail chujo@iclab.tytlabs.co.jp

††Nagoya Industrial Science Research Institute, Shimo-Shidami, Moriyama, Nagoya, 463-0003
††Tel 052-739-1889, E-mail hashiyama@nisri.moriyama.nagoya.jp

†††Nagoya University, Furo-cho, Chikusa, Nagoya, 464-8603
†††Tel 052-789-2792, E-mail furuhashi@nuee.nagoya-u.ac.jp
‡Tel 052-789-2775, E-mail okuma@okuma.nuee.nagoya-u.ac.jp

Abstract

We discuss an improved fail-safe circuit for real-time controllers using dynamically reconfigurable FPGA. A kind of FPGAs can be reconfigured in one millisecond. In the proposed circuit, one FPGA is set up to be fault detectors of real-time controllers. After detecting one fault of such controllers, the FPGA is quickly reconfigured to be a back up circuit of the faulty controller. The proposed fail-safe system can be relatively low price and small compared with usual fail-safe systems, because one FPGA is reconfigured to be any of back up circuits of these controllers.

key words FPGA, Dynamic Reconfiguration, Real-time Controller, Fail Safe

1. まえがき

近年，半導体技術の発展により FPGA(Field Programmable Gate Array)の高集積化，高機能化が進んでいる．とりわけ，高速な再構成や，実行中の部分的な再構成機能を提供する動的再構成可能な FPGA (Dynamically Reconfigurable FPGA)が利用可能となってきた[1][2][3]．このような動的再構成可能な FPGA の登場により，従来，専用回路を必要とした処理に対しても，必要なときだけ処理回路を構成することで柔軟な処理を行うことが可能になる．

一方，自動車などの民生機器用のリアルタイム制御回路においても安全性向上のため，Fail Safe 機能などの信頼性の高い制御回路などが求められている．しかしながら，従来，民生機器用のリアルタイム制御回路においては，個別に多重系や Fail Safe 回路を付加した構成にするには，コストおよび小型化の点で問題があった．

そこで，本報告では動的再構成可能な FPGA を利用したリアルタイム制御回路の Fail Safe 回路を提案する．提案回路では，複数の制御回路に対して動的再構成可能な FPGA を使用した Fail Safe 回路が用意される．通常の動作時には，FPGA は故障検出回路として動作し，複数の制御回路に対して故障の監視を行う．制御回路に故障が検出された場合には， FPGA は故障検出回路の構成を破棄して，故障した特定の制御回路に対する Back Up 回路に動的に再構成される．このような構成により Fail Safe System の低コスト化，小型化が可能になると考える．

回路例として自動車用の制御回路(ECU, Electronic Control Unit)に対して動的再構成可能な FPGA を用いて Fail Safe 回路を設計したので報告する．

2. FPGA の高機能化

FPGA の発展の方向は基本的には，大規模化，高速化である．規模の面では 100K ゲートを超えるデバイスが利用でき，速度の面でも，クロック周波数は数 10MHz まで到達している[1]．また，機能の面でも，再構成速度の高速化と同時に，実行中の部分的な再構成ができるようになってきた．この部分的な再構成可能な FPGA が提供する機能は RADD（Reconfigurable Architectures on DemanD[1]）,Virtual Logic[2]，Configurable Computing[3]などの名前で呼ばれる．この部分的な再構成可能な FPGA を使用することにより，シリコンチップ上に処理の必要に応じて回路を構成し，必要がなくなれば他の回路に再構成することができる．これにより，効率的にシリコンチップの面積を使用することができると考えられている．

これらの部分的な再構成可能な FPGA によって，ハードウェアの高速性を持ちながら，柔軟な計算処理を比較的小さな回路で実現できると考えられている．処理速度としては汎用的なマイクロプロセッサによるソフトウェア処理と専用に作られた ASIC による処理の中間に位置すると考えられる．ただし，部分的な再構成可能な本質的な利用法については，現在，検討が行われている段階である[3][4][5]．

上述の部分的な再構成可能な FPGA の代表例には，例えば，Xilinx の XC6200 シリーズがある．これは部分的な再構成が可能なデバイスである[1]．基本論理セルはプログラム可能な 2 入力ゲートと F/F(図 1　参照)からなっている．XC6200 シリーズのデバイス XC6216 の仕様を表 1 に示す．

表 1 XC6216 の概略仕様

セル機能	2入力ゲート＋ F/F
セル数	4,096
書換え速度	40ns/Cell, ~200 μ Sec/Chip

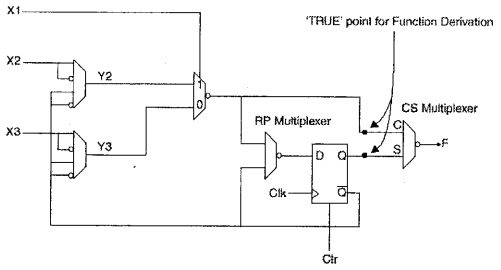


図 1　XC6200 シリーズの単位セルの構成

3.　リアルタイム制御と提案する Fail Safe 回路

3.1 リアルタイム制御回路

リアルタイム制御システムは，外部環境に対して一定時間内の応答を保証するシステムと定義されている．リアルタイム制御システムの例としては，ほとんどの組込み用制御回路があげられる．例としては，航空機，鉄道，自動車などの輸送関連システム，プラント制御システムがある．

特に航空機，鉄道，自動車など輸送関連のリアルタイム制御システムでは，乗客の安全に関わるため，システムに高い信頼性が必要とされている．このため，従来から航空分野では多重系を用いた Fault Tolerant System が採用されている．

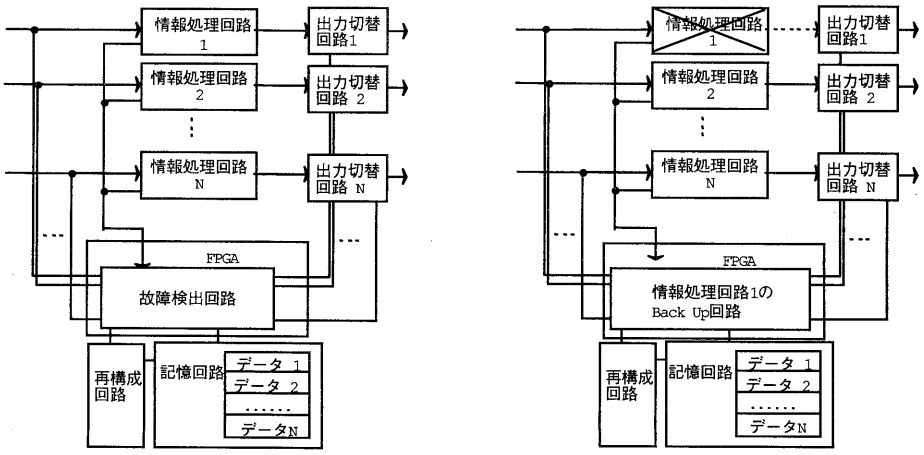
しかしながら，自動車などの民生品では低コストであることも重要な要件である．このため高コストになりがちな Fault Tolerant System の例は少なく，より低コストな Fail Safe System が採用されることが多い．Fail Safe System では故障が発生した場合には安全性を確保した上で一定の機能低下を容認する．

3.2 提案する Fail Safe 回路

ここでは提案する Fail Safe 回路の基本的な考え方について説明する．

従来の Fail Safe System の考え方では，複数の制御回路からなるシステムを対象と考えた場合，個別の制御回路ごとに Fail Safe 回路を用意する必要があった．なお本報告では Fail Safe 回路とは故障検出回路と Back Up 回路からなるものと定義する．

これに対して，提案する回路では，複数の制御回路をもつシステムに対して動的再構成可能な FPGA を使用した Fail Safe 回路が一つだけ用意される(図 2　参照)．通常の動作時には，FPGA は故障検出回路として構成しておき，複数の制御が検出された場合には，FPGA は故障検出回路の構成を破棄して，故障した特定の制御回路に対する Back Up 回路に動的に再構成される．この



(a) 正常動作時の構成　　(b) 正常動作時の構成

図2. FPGAによるFail Safe回路を用いた制御システム

ように提案する回路では，動的再構成可能なFPGAの回路書換え能力を生かしてFail Safe機能を提供する．この構成により，チップ上の素子を有効に利用できるため，Fail Safe Systemの低コスト化と小型化が可能になると考える．

4. 自動車用電子制御回路への適用検討

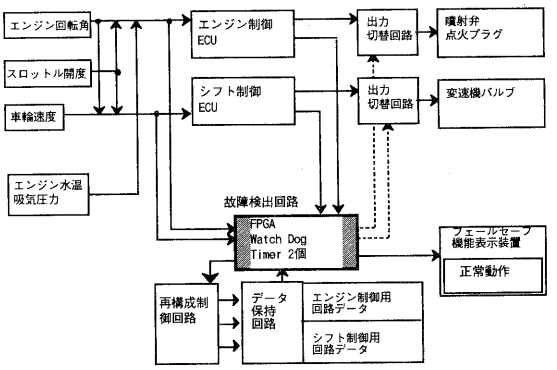
ここでは例として自動車用の電子制御回路を対象にしたFail Safe Systemの検討を行った(図3 参照)．

自動車用の電子制御回路は ECU(Electronic Control Unit)と呼ばれることが多い．現在のエンジン制御などに使用される自動車用ECUは以下のような構成が一般的である．CPU および周辺回路(入力信号処理回路，出力信号処理回路)で構成されるリアルタイム制御回路である．

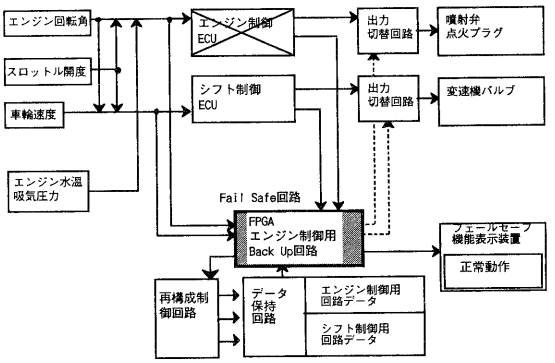
- CPU は16-32bitのプロセッサが一般的に使用される．
- 入力信号はアナログセンサ信号を扱うこともあるためA/D変換が含まれることも多い．
- 出力信号処理回路には外部アクチュエータを駆動するための駆動回路が含まれる．

ここではエンジン制御(EFI)とシフト制御(ECT)の2つからなるシステムに対して Fail Safe 機能を付加することを考えた．図に示すように動的に再構成可能な FPGA を使用することで，2つのシステムに対して一つの Fail Safe 回路で対応できるようにした．つまり，通常動作時は，FPGAは故障検出回路として動作し，2つの制御回路に対して故障の監視を行う．故障検出後は，FPGAは故障検出回路の構成を破棄して，故障した特定の制御回路に対する Back Up 回路に動的に再構成される．なお，このとき単一故障を仮定する．

今回，例として動的再構成可能なFPGAには，通常動作時の故障検出回路として Watch Dog Timer を，故障検出時用の Fail Safe 回路として



(a) 通常動作時の構成



(b) 故障検出時の構成

エンジン制御用 Back Up 回路を考えた．

図3 FPGAを用いた自動車用制御回路の Fail Safe System

5. 回路設計と評価

5.1 回路設計

動的再構成可能な FPGA として Xilinx の XC6216 を使用した開発システム(HOT Works)を利用して評価を行った．1個の XC6216 回路上に，通常動作時には故障検出回路(WDT: Watch Dog Timer 2個，図4参照)を，故障検出時にはエンジン制御用の Back Up 回路（図5参照）をインプリメントすることができた.故障検出回路と Back Up 回路は，開発システムの PC の CPU を利用して PCI バス経由で切替えを行った．

5.2 回路のデータ量と再構成時間

回路の再構成に要する時間については，Back Up 回路のデータ量と，書換え用データ転送の時間に依存する（表2参照）．データ量は Back Up 回路で 48Kbyte（CAL フォーマット）であった．この回路の書換え時間は，開発システムのバスのデータ転送レート約 8MB/sec から約 6ms 程度と推定される．実際の Fail Safe System ではバス構成が異なると考えられるため，この書換え時間は参考程度の値であるが，実際の制御回路でも十分実用に耐える値であると考えている．

表 2. 設計結果

WDT (x2)	
No. of Cell	320 Cells
Size of Data	39 KB(CAL format)
Back Up回路	
No. of Cell	504 Cells
Size of Data	48KB(CAL format)
再構成時間	6 ms (Estimated)

6. 考察

ここでは，N個の制御回路からなるシステムに提案する Fail Safe 回路を付加することを考え，従来の回路と回路規模を比較する．

i番目の故障検出回路(Fault Detector)を *FDi*, Back Up 回路(Back Up Circuit)を *BUCi* とする．従来の回路では，付加する回路はこれらすべてを足した面積が必要となり，式(1)となる．これに対して，今回提案する回路では，式(2)となる．第1項は再構成される FPGA のチップ面積であり，N個の故障検出回路の総和と，最大の Back Up 回路の大きい方のチップ面積になる．また別に Back Up 回路用の回路構成データを記憶するメモリ回路，再構成を制御する回路(RC)のための面積が必要である．

具体的な数字を挙げることは難しいが N が小さい場合には，提案する回路は FPGA を使用するため，チップ面積の有利さを主張することは難しいと思われる．

$$A_1 = \sum_{i=1}^{N} A(FDi) + \sum_{i=1}^{N} A(BUCi) \quad \text{(1)}$$

$$A_2 = \max\left(\sum_{i}^{N} A^f(FDi), \max_i\left(A^f(BUCi)\right)\right) + \sum_{i}^{N} A^m(BUCi) + A(RC) \quad \text{(2)}$$

FDi: 故障検出回路i
BUCi : Buck Up 回路i
RC: Reconfiguration Controller回路
A(X): 回路XのASIC上でのチップ面積
A^f(X): 回路XのFPGA上でのチップ面積
A^m(X): 回路XをFPGA上に構成するために必要なメモリのチップ面積

Nが大きくなり，Back Up 回路の面積の和が大きくなると提案する回路の方が有利になると思われる．更に Nが大きくなり，N個の故障検出回路が FPGA に入らなくなる場合，これを ASIC で別に構成することが必要になる．このとき，式(2)は式(3)のようになる．

$$A_2' = \sum_{i}^{N} A(FDi) + \sum_{i}^{N} A^m(BUCi) + \max_i\left(A^f(BUCi)\right) + A(RC) \quad \text{(3)}$$

式(1)と式(3)を比較すると，従来の回路(1)では N個の Back Up 回路の面積が必要であるのに対して，提案する回路では N個の Back Up 回路の回路構成を記憶したメモリと FPGA の面積が必要になっている．Back Up 回路の実際のチップ面積より，Back Up 回路を FPGA 上に構成するためのメモリの面積の方が小さいと思われる．このため，提案する回路の面積 A_2'の方が従来の回路の面積 A_1に比べ小さくなると思われる．

また提案する回路は，専用回路を開発する必要が小さいため，開発費用の点でも有利であると思われる．

今後の課題としては，FPGA の複数使用による Fault Tolerant 回路への拡張，FPGA 上の回路の自己診断化による信頼性向上などがあると考える．

7. むすび

動的再構成可能な FPGA を利用したリアルタイム制御回路に対する Fail Safe 回路を提案した．提案する回路により，従来に比べて低コストで小型な Fail Safe System が構成できる．回路例として自動車の制御回路に対して動的再構成可能な FPGA を用いて Fail Safe 回路を設計した．今後の課題としては，再構成の制御を行う回路の検討，部分的な書換えによる多重故障への対応などがある．

この研究は（財）名古屋産業科学研究所の主催する創発型ソフトコンピュータ開発プロジェクトの一部として行われた．

文　献

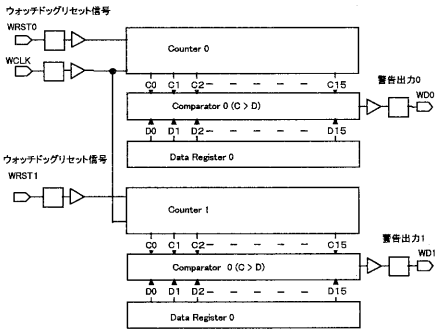
[1] S. Shiratsuchi, "FPGA as a Key Component for Reconfigurable System, " Int. Conf. on Evolvable Systems from Biology to Hardware, ICES 96, Oct 1996.

[2] 末吉　敏則，"リコンフィギャラブル・コンピューティング，" 5th Japanese FPGA/PLD Design Conference & Exhibit 予稿集，pp. 139-148，Jun 1997.

[3] J. Villasenor, W. H. Mangione-Smith, " Configurable Computing, " Scientific American, pp. 66-70, Jun 1997.

[4] 市川　周一，島田　俊夫，"パーソナルコンピューティング指向の動的再構成可能 PCI カード，" 5th Japanese FPGA/PLD Design Conference & Exhibit 予稿集，pp. 269-277, Jun 1997.

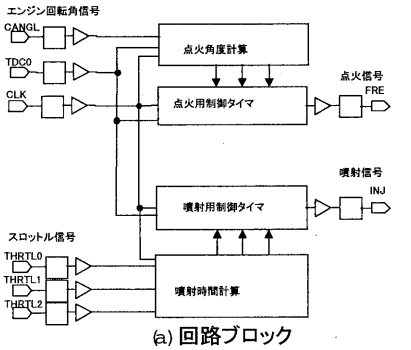
[5] R. Woods, D Trainor and J. P. Heron, "Applying an XC6200 to Real Time Image Processing, " IEEE Design & Test of Computers, Vol. 15, No. 1, pp. 20-38, Jan 1998.



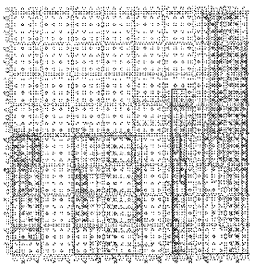
(a) 回路ブロック

(b) レイアウト

図 4　WDT 回路とそのレイアウト



(a) 回路ブロック



(b) レイアウト

図 5　WDT 回路とそのレイアウト