Research Report

Fail-safe ECU System Using Dynamic Reconfiguration of FPGA

Naoya Chujo

動的再構成型FPGAによるフェールセーフECUシステム

中條直也

Abstract

ECUs (Electronic Control Units) are embedded controllers in automobiles. The number of ECUs in each automobile is increasing and their functions are becoming more complex in order to meet environmental requirements and satisfy market needs. It is important to make these ECUs reliable for the sake of customer safety. Since space and cost reduction are high priorities for automobile applications, there is a demand for improved circuit reliability with the minimum amount of hardware addition.

This paper presents a fail-safe ECU system using dynamically reconfigurable FPGA (Field Programmable Gate Array). The FPGA is configured to be fault detectors and functions as a monitor for the control circuits under normal operating conditions. If a fault in one ECU is detected, the FPGA is dynamically reconfigured to be a backup circuit for the faulty control circuit. Because of this dynamic reconfiguration it is possible for the proposed fail-safe ECU system to be small, compared with conventional hardware. Example fail-safe circuits using dynamically reconfigurable FPGA, such as the Xilinx 6200 series, have been designed and evaluated.

Keywords FPGA, Dynamic reconfiguration, Real-time controllers, Fail-safe circuit, Hardware design

要　旨

自動車の組込型制御装置としてECU (Electronic Control Unit)は広く使用されている。高まる環境や安全などのニーズに対応するために，自動車一台当たりのECU数は増加し続けており，その機能は複雑化している。複雑化するECUシステムでは信頼性向上が重要となってきているが，組込装置として実装面から小型であることも重要であるため，最小限の付加ハードウェアで信頼性を向上させることが求められている。本報告では動的再構成可能なFPGA (Field Programmable Gate Array) を使用したフェールセーフ機能付きのECUシステムを提案する。通常動作時にはFPGAを故障検出回路として構成しECUの故障を監視させる。故障検出時にはFPGAを故障したFPGAのバックアップ回路として動的に再構成する。動的再構成によりフェールセーフ用の専用回路を個別に装備する必要がなくなり，ECUシステムの小型化と信頼性向上が可能となる。例として，Xilinx 6200シリーズを用いた回路設計を行って，リアルタイム制御ECUへの適用評価した結果を示す。

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，回路設計

1. Introduction

ECUs (Electronic Control Units) are embedded controllers in automobiles. The number of ECUs in each automobile is increasing and their functions are becoming more complex in order to meet environmental requirements and satisfy market needs. It is important to make these ECUs reliable for the sake of customer safety. Generally, additional hardware is required to make ECUs fault tolerant or fail-safe. Since space and cost reduction are high priorities for automobile applications, there is a demand for improved circuit reliability with the minimum amount of hardware addition.

The reconfiguration of processors is regarded as one important technology for fault tolerant or fail-safe systems [1]. One of the reconfigurable devices, FPGA (Field Programmable Gate Array), is promising due to the development of semiconductor technology, and dynamically reconfigurable FPGAs with high speed and partial reconfigurations have also become available [2-4]. Processors that are more flexible than fixed and dedicated processors can be applied to the use of the field in question, because dynamically reconfigurable FPGAs provide designers with processing hardware whenever it is necessary. Research reports have been conducted on the utilization of FPGA [4-6]. Most of them have focused on customized computing in order to achieve high performance in fields such as image processing.

This paper presents a fail-safe circuit for a real-time ECU using dynamically reconfigurable FPGA [7]. The FPGA is configured to be fault detectors and functions as a monitor for the control circuits under normal operating conditions. If a fault in one ECU is detected, the FPGA is dynamically reconfigured to be a backup circuit for the faulty control circuit. Because of this dynamic reconfiguration, it is possible for the proposed fail-safe system to be small and inexpensive compared with conventional hardware. As an example, fault detection and backup circuits have been designed utilizing dynamically reconfigurable FPGA for a real-time ECU system in an automotive application.

In the following sections, the concept of the proposed fail-safe technology, the reconfigurable FPGA, a circuit example and conclusions will be described in order.

2. Fail-safe technology using FPGA

The concept of fail-safe technology using dynamically reconfigurable FPGA is described in this section. The reconfiguration is categorized into local redundant and processor switching types [1]. The fail-safe system is defined so as to allow function degradation after a fault, but it prevents the system from suffering fatal problems. The fault tolerant system possesses robustness against faults and maintains the specified functions. This fail-safe system can be made simpler than the fault tolerant system. In this paper, a fail-safe circuit is defined to include a fault detector and a backup circuit for one controller.

When the system has many real-time controllers, which are common in recent automobiles, it is generally necessary for a fail-safe function to be provided for each controller. Backup circuits are widely used to provide these controllers with fail-safe functions.

Backup circuits are not necessary when the system works normally. However, they are needed to provide the system with minimum functions when a fault is detected. Therefore, it is effective to configure the FPGA so that it becomes the backup circuit for the faulty controller at the moment a controller fault is detected. When the reconfiguration of the FPGA is fast enough, it is possible to apply this architecture to real-time controllers. This is the concept of the proposed fail-safe technology using dynamically reconfigurable FPGA.

In addition, in a case where only a single fault is considered and multiple faults are not, fault detectors can be configured by the FPGA under normal operating conditions. As a fault detector such as a watchdog timer can generally be much simpler than a backup circuit, several fault detectors can be reconfigured as one backup circuit.

Consequently, the proposed fail-safe technology consists of real-time controllers and dynamically reconfigurable FPGA, which is configured as fault detectors for the controllers under normal operating conditions. The moment a fault in these controllers

is detected, the FPGA is quickly reconfigured from acting as fault detectors to being a backup circuit for the faulty controller.

3. Dynamic reconfiguration of FGPA

FPGAs and FPLDs (Field Programmable Logic Devices) have been improved so that they are larger, faster, and more flexible. At present, they have over one million gates and work with a 100 MHz system clock. **Figure 1** shows that the development of FPGA has increased application areas. The flexible architecture of FPGA and HDL (Hardware Description Language) synthesis technology can realize complex functions such as ALU and DSP, and micro controllers available as IP (Intellectual Properties) function on FPGA. In addition, sophisticated reconfiguration of FPGA is also available. The time required for full-chip reconfiguration is less than one millisecond. Quick reconfigurable devices such as this are called Dynamic Reconfigurable type (DR-type). By using dynamic reconfiguration, the processing module in the FPGA can be swapped during system operation. There are also two types of dynamic reconfiguration; one is full chip reconfiguration and the other is partial reconfiguration. Other function concepts are RADD (Reconfigurable Architectures on DemanD[2]), Virtual Logic[3], and Configurable Computing[4]. These DR-type FPGAs reconfigure the logic or processing circuits dynamically from one to another on demand. The latest DR-type devices with multiple sets of configuration memory on the chip can be reconfigured within 5 nsec[8]. This sophisticated reconfiguration uses the silicon area efficiently.

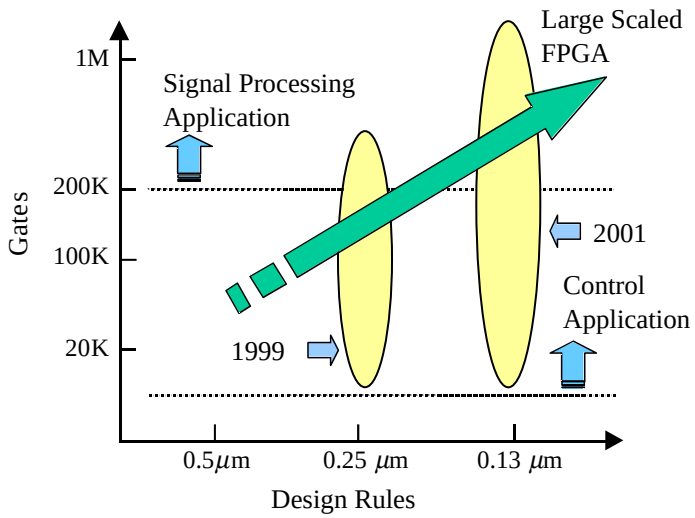

Fig. 1 Evolution of FPGA.

4. Application of fail-safe technology to ECUs

In this section, the proposed fail-safe technology is applied to an embedded system for an automobile.

4. 1 Real-time control system for automotive electronics

The definition of a real-time control system is a control system that responds to its inputs within a fixed time. This term is often used for systems that respond to inputs at very high speed. Most of the embedded control systems commonly used in automobiles are real-time control systems.

It is important to make these systems highly reliable, because they have an impact on passenger safety. Fault tolerant systems based on redundant architecture are used for control systems such as those in aircraft, which require high security. However, fail-safe systems are preferred over fault tolerant systems for automotive electronics, because low cost is also important in automotive applications.

Today's embedded control systems in automotive applications such as the engine control system have the following hardware.

- The real-time controller consists of a microprocessor and I/O peripheral circuits.
- Generally, the microprocessor is 16-32 bit.
- Analogue circuits are incorporated in some cases to handle analog sensor inputs.
- Output drive circuits are incorporated in some cases to drive actuators.

The proposed fail-safe technology was applied to a system consisting of the engine controller (EFI, Electronic Fuel Injection) and the transmission controller (ECT, Electronically Controlled Transmission). See **Fig. 2** and **Fig. 3**.

Two controllers are provided with a fail-safe circuit using dynamically reconfigurable FPGA. The FPGA is configured in advance to be fault detectors for these controllers. Two watchdog timers (WDT) are installed on the

FPGA as fault detectors for these controllers. After detecting a fault, the FPGA is quickly reconfigured as the backup circuit (BUC) of the faulty controller. In Fig. 3, the FPGA is the backup circuit for the engine controller, and it performs the fuel injection and electronic spark advance controls to enable the vehicle to continue running. This function only guarantees minimal engine performance, which is poorer than that obtained using the original engine controller. The configuration data for the FPGA is memorized on the configuration ROM.

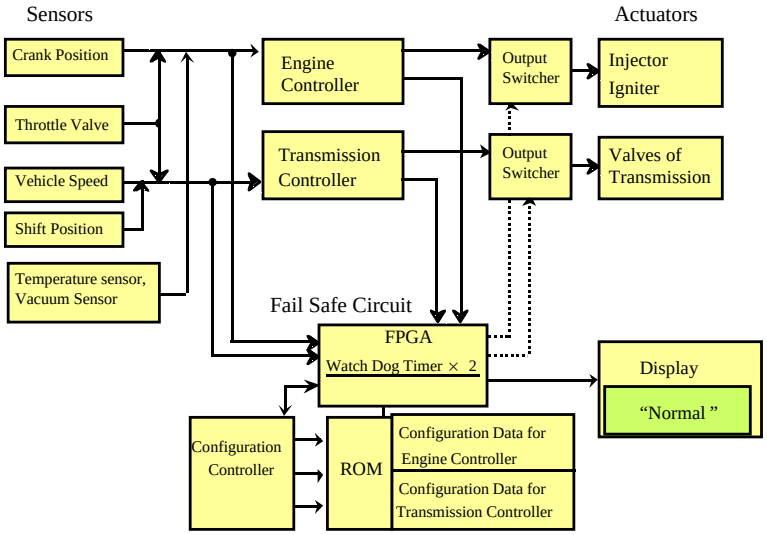

Fig. 2 Engine and transmission control system under normal operations.

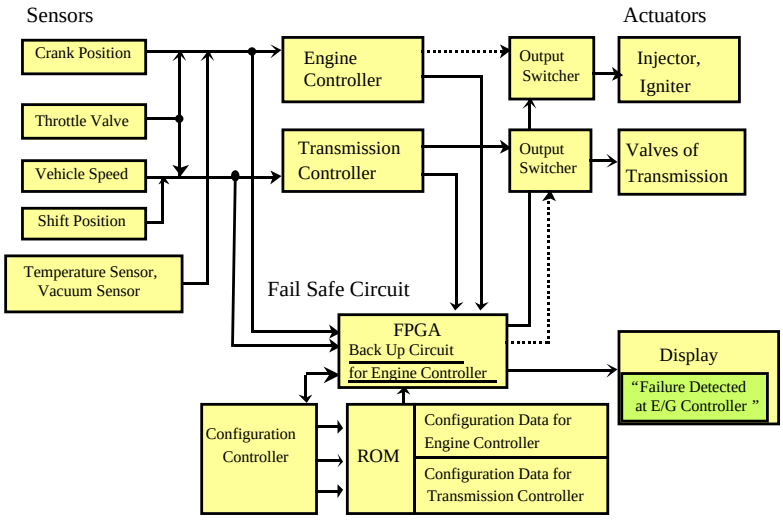

Fig. 3 Engine and transmission control system in case of a fault of engine controller.

4. 2 Circuit design and evaluation

Circuit design and evaluation were conducted using the HOT Works development system that has an integrated XC6216 and PCI-bus interface [9]. XC6216, made by Xilinx, is a kind of DR-type FPGA, which is capable of performing partial reconfiguration during operation and has short programming times. The basic cell of the XC 6200 series consists of a programmable 2-input gate and F/F. The specifications of device XC6216 of the XC6200 series are shown in **Table 1**. **Figure 4** and **5** show the schematics and layouts of the two WDTs. **Figure 6** and **7** show the schematic and layout of the backup circuit for engine control. The dynamic reconfiguration that switches from the WDT to the backup circuit was performed through the PCI bus.

The time taken for reconfiguration is important for real-time controllers. This depends on the data size of the circuit and the transmission rate. **Table 2** shows the results achieved by the design. Binary data was used and the time for the reconfiguration was 440 μsec.

The time taken for reconfiguration was

Table 1 Outline of XC6216.

Time for Configuration	~200 μsec/chip 40 ns/cell
Program mode	Parallel / Partial
No. of cell	4096 (64×64)cells

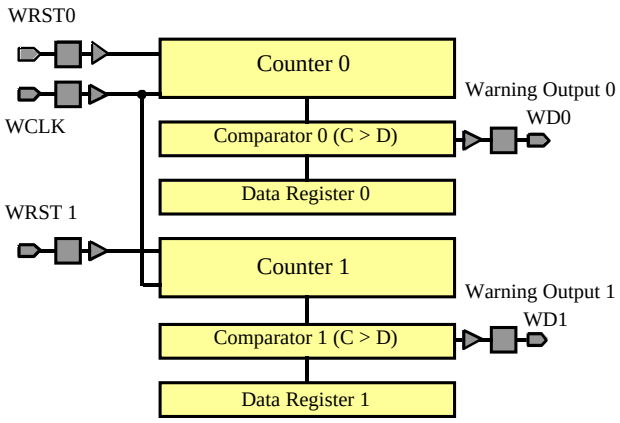

Fig. 4 Schematics of two WDTs.

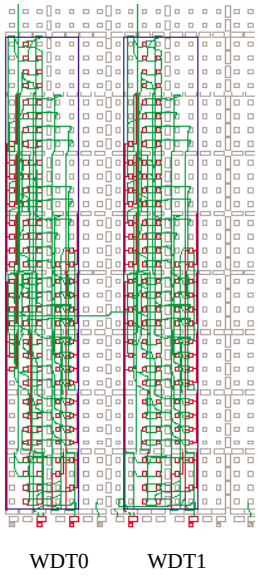

Fig. 5 Layout of two WDTs.

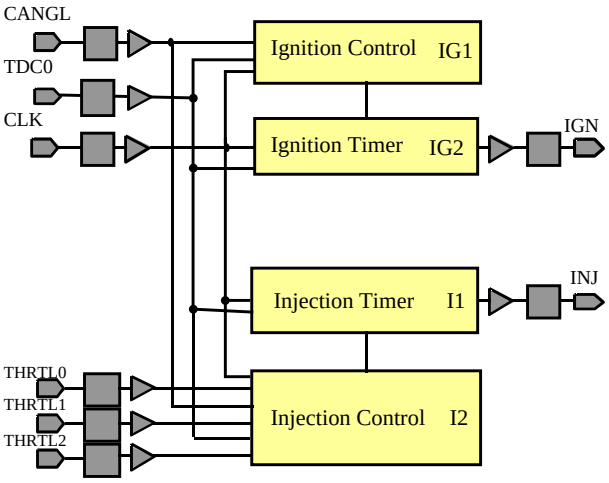

Fig. 6 Schematics of BUC.

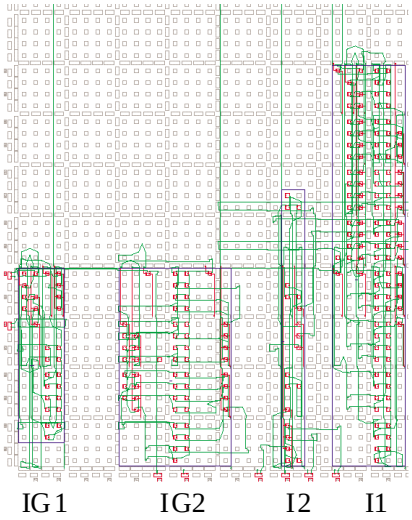

Fig. 7 Layout of BUC.

Table 2 Results of example design.

WDT (× 2)	No. of cell	320 cells
	Size of data	39 KB (CAL format) 1.0 KB (binary data)
BUC	No. of cell	504 cells
	Size of data	48KB (CAL format) 1.1 KB (binary data)
Time for configuration		440 μsec

fast enough for the real-time controller, but it should be noted that the time taken for reconfiguration depends on the reconfiguration method used. According to the specifications of XC6216, the full chip design can be reconfigured within around 200 μsec.

5. Discussion

The proposed technology was able to provide the real-time controllers with a fail-safe function using the single fail-safe circuit. The proposed fail-safe circuit eliminates the need to develop backup circuits by ASIC technology that requires wafer process and test costs. However, it does require ROM to memorize the configuration data and one reconfiguration controller to make data transmissions, which can be independent of system functions.

The silicon areas of the conventional circuit and the proposed fail-safe circuit for the system of N controllers.were compared. FD_i and BUC_i denote i-th fault detector and backup circuit, and $A^a(x)$ and $A^f(x)$ denote the silicon areas of the circuit x designed by ASIC technology and FPGA technology respectively. $A^m(x)$ is the area of memory (ROM), which is necessary to store the configuration data of circuit x for the FPGA.

The area of the conventional fail-safe circuit is:

$$A_1 = \sum_{i=1}^{N} A^a(FD_i) + \sum_{i=1}^{N} A^a(BUC_i) \qquad \cdots\cdots(1)$$

It is the sum of the areas of the ASICs for the fault detectors and the backup circuits.

The area of the proposed fail-safe circuit is:

$$A_2 = \max\left(\sum_{i=1}^{N} A^f(FD_i),\ \max_i\left(A^f(BUC_i)\right)\right) + \sum_{i=1}^{N} A^m(FD_i) + \sum_{i=1}^{N} A^m(BUC_i) + A^a(RC) \qquad \cdots\cdots(2)$$

where RC denotes the reconfiguration controller. The first term of (2) is the area of one FPGA and the second and the third terms denote the area for storing the configuration data in the ROM. The last term denotes the area for the reconfiguration controller.

When N is large enough, it is necessary to make fault detectors that are designed as ASIC circuits. In this case, the expression shown in (2) is rearranged so that:

$$A'_2 = \sum_{i=1}^{N} A^a(FD_i) + \sum_{i=1}^{N} A^m(BUC_i) + \max_i\left(A^f(BUC_i)\right) + A^a(RC) \qquad \cdots\cdots(3)$$

The second term of (1) and (3) become significant when N is large. The second term of (1) is larger than the second term of (3), because the area of the ASIC is normally larger than the area of the configuration ROM. As a result of this comparison, the silicon areas of the proposed fail-safe circuit can be smaller than the silicon areas of the conventional circuit.

Therefore, it was concluded that a fail-safe system that has multiple controllers can be made comparatively less expensive and smaller if the proposed circuit is used, in comparison with conventional fail-safe systems which require a fail-safe circuit for each controller.

It is desirable for fail-safe systems to handle multiple faults. The FPGA's capacity for partial reconfiguration can be used for handling multiple faults. Even after detecting a fault when the FPGA is partially reconfigured, it is possible for the FPGA to maintain its fault detection capability using the rest of the area of the FPGA. However, dynamic routing of the FPGA is a difficult problem for real-time systems.

The functions of fault detectors and backup circuits depend on the resources of the FPGA, which are the numbers of logic gates, routing tracks etc. The restrictions on these resources are vanishing with the advance of semiconductor technology. Some types of FPGA provide designers with several sets of memories for reconfiguration, which are switched simultaneously. As a result, circuit size and the speed of reconfiguration will be improved.

The development of the self-checking capability of the fail-safe circuit will also become possible when larger and more complex FPGAs are used.

6. Conclusions

Due to the rapid improvement of FPGAs, promising reconfigurable ECU systems are being developed in the field of real-time ECU systems. A fail-safe ECU system using dynamic reconfiguration of FPGA has been proposed. The FPGA is configured to be fault detectors and functions as a monitor for the control

circuits under normal operating conditions. The proposed fail-safe ECU system has the potential to be smaller and less expensive than conventional hardware. Example circuits for fail-safe ECUs utilizing dynamically reconfigurable FPGA have been designed and evaluated, and it has been shown that dynamic reconfiguration is fast enough for real-time ECU systems. Fault tolerant controllers and the handling of multiple faults by larger FPGAs will be discussed in our future work.

Acknowledgements

This work was supported by Emergent Soft Computer Development Project of Nagoya Industrial Science Research Institute, Japan.

References

1) Chean, M. and Fortes J. A. B. : “A Taxonomy of Reconfiguration Techniques for Fault-Tolerant Processor Arrays”, IEEE Comput., **23**-1(1990), 55
2) Shiratsuchi, S. : “FPGA as a Key Component for Reconfigurable System”, Proc. Int. Conf. Evolvable Systems from Biology to Hardware (ICES 96),(1996)
3) Sueyoshi, T. : “Reconfigurable Computing”, Proc. 5th Jpn. FPGA/PLD Design Conf. & Exhibit, (1997), 139-148
4) Villasenor, J. and Mangione-Smith, W. H. : ”Configurable Computing”, Sci. Am., No.6(1997), 66
5) Buell, D. A., Arnold, J. M. and Kleinfelder, W. J. : “SPLASH 2: FPGAs in a Custom Comput. Machine”, (1996), IEEE Comput. Soc. Pr.
6) Woods, R., Trainor, D. and Heron, J. P. : “Applying an XC6200 to Real Time Image Processing”, IEEE Design & Test of Comput., **15**-1(1998), 20
7) Chujo, N., Hashiyama, T., Furuhashi, T. and Okuma, S. : “A Fail-safe Circuit for Real-time Controllers Using Dynamic Reconfiguration of FPGA”, Design Autom. and Test in Europe, User’s Forum, (1999), 59
8) Fujii, T., et al. : “A Dynamically Reconfigurable Logic Engine with a Multi-Context/Multi-Mode Unified-Cell Architecture”, ISSCC Digest of Techn. Pap., 21.3, (1999)
9) Virtual Computer Corp. : “H.O.T. User’s Guide Rev. 1.0”, (1998)

(Report recieved on April 17, 2002)

Naoya Chujo　中條直也
Year of birth : 1958
Division : Research-Domain 24
Research fields : Automotive Electronics, Optical devices and systems for automotive LAN
Academic society : IEEE, IEE of Jpn., Inst. of Electron. Inf. Commun. Eng., Inf. Process. Soc. of Jpn.
Received the Best ASIC Prize in 1999 DATE Conf.