Fault Recovery Method of Modular Systems based on Reconfigurations

Jaroslav Borecký, Pavel Vít and Hana Kubátová
Department of Digital Design
Faculty of Information Technology
Czech Technical University in Prague
Email: {borecjar; pavel.vit; kubatova}@fit.cvut.cz

***Abstract*—This paper presents the method of dependability parameters improvement for systems based on unreliable components such as Field Programmable Gate Arrays (FPGAs). It combines Concurrent Error Detection (CED) techniques [4], FPGA dynamic reconfigurations and our previously designed Modified Duplex System (MDS) architecture. The methodology is developed with respect to the minimal area overhead. It is aimed for practical applications of modular systems. Therefore it is applied and tested on the safety railway station system. This Fault-Tolerant (FT) design is tested to fulfill strict Czech standards [7]. The proposed method is based on static and partial dynamic reconfiguration [5] of totally self-checking blocks which allows a full recovery from a Single Even Upset (SEU).**

I. Introduction and Motivation

Systems realized by programmable hardware like FPGAs are widely used in all of applications due to their capability to implement complex circuitry within a very short development time, together with the potential for an easy change of a design by reconfiguration.

Thanks to the Partial Dynamic Reconfiguration (PDR) the FPGAs will be more applied because a part of the circuit can be changed without disturbing of a rest of the functional FPGA. But PDR can be applied in a different way and it can help us to increase dependability parameters.

Most of modern FPGAs are based on SRAM memories. These logic arrays can not be used in mission critical applications without any additional protection due to their high sensitivity to the radiation effects. For example a Single Event Upset (SEU) changes one bit of configuration memory, that causes a radical change of an implemented circuit. Applications used in space missions or public transport need to satisfy strict safety standards to avoid tragic consequences. We propose on-line testing method, because these critical applications must not be interrupted by any tests.

The method described below can be used in highly reliable modular systems which are based on these unreliable components.

II. Theoretical Background

Whole device is composed of different modular system blocks. Each part of a block has to be secured, because a SEU can occur. A change of one bit leads to a modification of the circuit function, often drastically. That causes unpredictable behavior in practical applications, for example the control device can change signals to green in all traffic lights of a crossroad.

Therefore we must guarantee continuous function without interruption, and it is possible only by on-line tests. Our method is based on methods which follows.

A. Totally Self-checking Circuit

Every Totally Self-checking Circuit (TSC) is composed of three small parts, where each block corresponds the TSC property. The universal structure of the compound design satisfying the TSC property is shown in Fig. 1.

You can see six places where an error can occur in the TSC block diagram shown below. The idea is, that if an error is in the check bits generator, it will be observable on the check bits wire (the wire number 1). When an error is in the original combinational circuit, it will be observable on the primary output (the wire number 5). This implies that the checker in block N will detect an error on the wire number 1, 2, 4 or 5. Or if an error occurs on the wire number 3 or 6, it will be detected in the next block (N+1) by its checker. The method used to satisfy the TSC property for the compound design is described in detail [2].

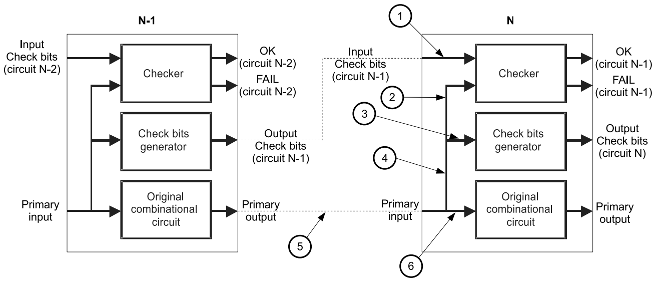

Fig. 1. The structure of compound system corresponding the TSC property

Not every TSC block (in the compound design) satisfies the fault coverage to 100%. The TSC structure, which uses only one copy of the TSC circuit is not sufficient to increase dependability parameters. Thus, we assume to use our Modified Duplex System (MDS) architecture [1], [2], which has a parity generator in all TSC.

B. Modified Duplex System

Modified Duplex System (MDS) architecture uses two instances (instead of mostly used TMR architecture like e.g.

[8]) of design that may be not fault tolerant. The purpose of MDS architecture is to achieve the whole circuit including all checkers and comparators to be fault tolerant. The MDS block diagram is shown in Fig. 2.

If an error (caused by SEU) is not detected inside the system by some TSC block, it is detected by comparators. The error detected by comparators triggers initiate the reconfiguration of both blocks (outputs from blocks are different, but the source of the error cannot be determined). But this full reconfiguration is a time demanding process and can cause synchronization problems and therefore leads to decrease of the whole system availability. Due to it the Partial Dynamic Reconfiguration (PDR) is used in our improved architecture.

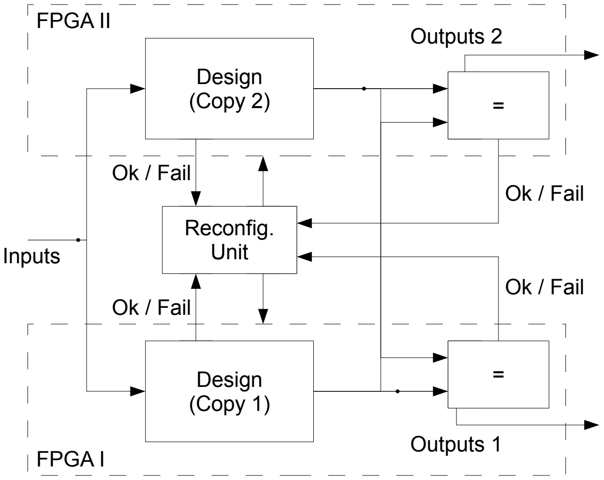

Fig. 2. The block scheme of Modified Duplex System

III. Upgraded Modified Duplex System

Mission critical systems have to run with high availability. It is necessary to develop a methodology how to repair soft errors immediately during their normal operational process. We propose to use an architecture composed of blocks which is derived from practical applications. These blocks will be utilized by partial reconfiguration to repair their transient faults. One big block or few small blocks will be placed in one Reconfiguration Module (RM).

Our method is capable to secure any modular circuit. It was evolved during the evolution of the railway station safety system in our department [3]. This system is modular and based on five types of blocks. This method reduces recovery time, because it uses partial reconfiguration often and whole FPGA reconfiguration only in critical situations. Availability of the whole system increases thanks to a short time of partial reconfiguration. System designed in this way uses less area overhead compared to other methods like TMR or NMR.

A. Basic Scheme

In Fig. 3, you can see our proposed system. It uses two boards with one FPGA, where the same design is loaded. It simplifies the systems design and reduces time of developement. There are two main parts (Reconfiguration area and Static area) in each FPGA.

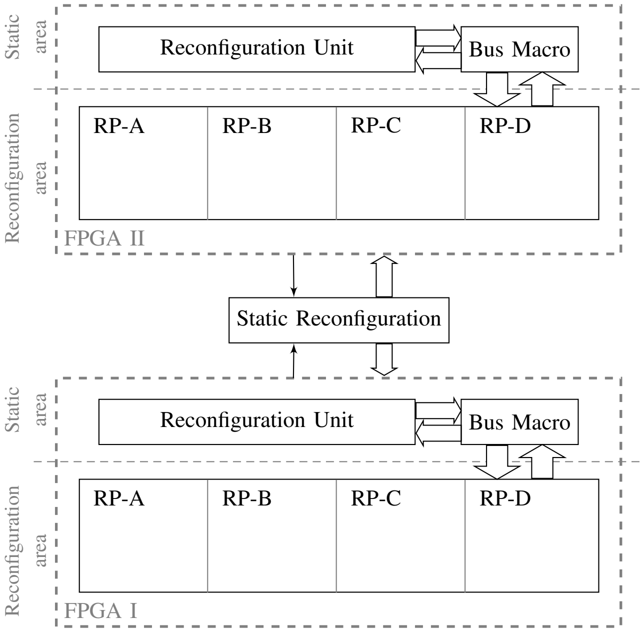

Fig. 3. Upgraded MDS Architecture

You can see in Fig. 2 that each FPGA in MDS is composed of a design and a comparator. These parts are divided into blocks and placed into Reconfiguration Area in UMDS (bottom part of each FPGA shown in Fig. 3). UMDS uses simpler static reconfiguration unit than the MDS, which is placed between FPGA boards.

The top part of the design is innovated and it improves reliability by performing partial reconfiguration of faulty part when it is needed.

1) Reconfiguration area: is a part of FPGAs which we divided into several Reconfiguration Partitions (RP). The number of RP depends on used application and their size depends on the specific architecture of an FPGA. In one RP, there is also a comparator derived from MDS. One set of RMs is prepared for both FPGAs, where each RM belongs to pertinent RP.

2) Static area: is composed of two parts. The Reconfiguration Unit is constructed by FSM, which controls the status of each TSC block in the reconfiguration area. The Bus Macro is a bridge between reconfiguration and static areas and is here present for compatibility with older FPGAs.

3) Static reconfiguration: is the control logic which performs reconfiguration of the whole FPGA (one or both in the same time). The reconfiguration is initiated by checkers from Reconfiguration Units and Comparators.

B. Fault Recovery Flow

An error can occur in every part of an UMDS and change the functionality some block. This method achieves 100% of fault cover as described below.

When an error is in the static area, the Static Reconfiguration unit performs reconfiguration of the whole FPGA, where the error was detected. When an error is in Reconfiguration area, it could be in the secured design or in the comparator. Errors in secured design are detected by checkers. An error in the comparator is detected by Static reconfiguration unit or checkers. Static reconfiguration unit reconfigures both FPGAs.

When an error is detected by some checker, then Reconfiguration unit reconfigures only this RM. For example RP-A part detects the error and RM-A is loaded into RP-A, where the broken block is placed. Other blocks in different parts (RP-B, RP-C, etc.) are able to work at this time.

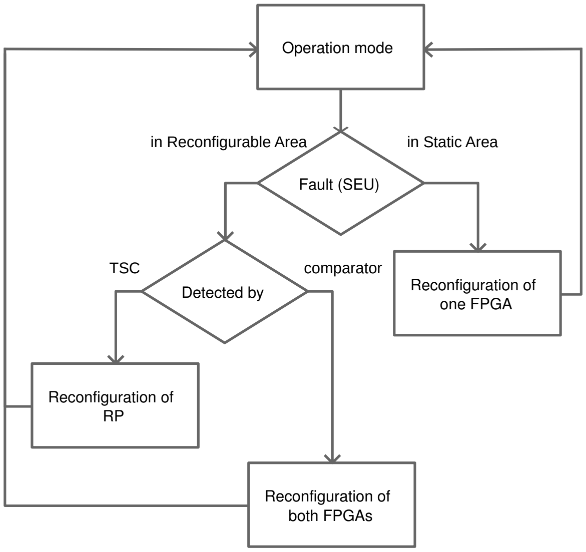

Fig. 4. The block diagram of the Fault Recovery Flow

IV. Conclusions

Our new method of fault recovery of safety systems was presented in this paper. The method is based on two independent FPGA boards with the same design. The FPGA is divided into two main parts. Whole system is placed in the reconfiguration area and static area checks failure signals and immediately repairs soft errors in RPs. Our method is aimed for modular systems which are composed from blocks. Every block is designed as TSC, also the static area satisfies TSC property.

Whole system is derived from MDS and is innovated. The main improvement is in usage of the partial reconfiguration and a block structure of the design. This allows faster detection and correction of faults. Reconfiguration of only one RP is faster than load a whole FPGA. It leads to increase availability and security within minimal area overhead. Most of dependable systems are based on TMR which uses more than three times more area of an FPGA than the original circuit.

Our method was simulated by using Markov model and failure distribution function was calculated. Comparison with original MSD is in Fig. 5.

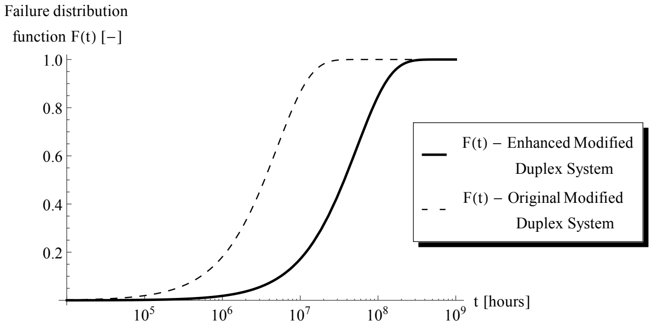

Fig. 5. The block diagram of the Fault Recovery Flow

A. Future work

An implementation of proposed method on the railway station safety device is in progress. We use two XUPV505-LX110T boards with Virtex 5. First tests will check the functionality of whole system and correct function of each block. Finally the verification of our technique will be performed by implementing errors directly into bitstream. One random bit will be changed in the bitstream of one FPGA by a testing device (simulation of SEU). Behavior of the whole system will be monitored and checked.

Another tests and simulations of faults are subscribed in [6]. An insertion of the error will be performed by changing of configuration bits in the FPGA by a neutron beam. A probability of fault will be recalculated in natural environment and compare it with [7].

Acknowledgment

This research has been partially supported by the project SGS14/039/OHK3/1T/18.

References

[1] Kubalik, P., Dobias, R., Kubatova, H.: *"Dependable Design for FPGA based on Duplex System and Reconfiguration"*, In Proc. of 9th Euromicro Conference on Digital System Design. Los Alamitos: IEEE Computer Society, 2006, pp. 139–145

[2] Kubalik, P., Kubatova, H.: *"Dependable design technique for system-on-chip"*, Journal of Systems Architecture, no. 54, 2008, pp. 452–464. ISSN 1383-7621

[3] Borecky, J., Kubalik, P., Kubatova, H.: *"Reliable Railway Station System based on Regular Structure implemented in FPGA"*, Proc. of 12th EUROMICRO Conference on Digital System Design, Los Alamitos, IEEE Computer Society, 2009, pp. 348–354.

[4] D. K. Pradhan. *"Fault-Tolerant Computer System Design"*, Prentice-Hall, Inc., 1996

[5] XILINX *"Xapp864: Seu strategies for virtex-5 devices."*

[6] Vanat, T. and Kubatova, H. *"Experiments with Physical Error Injection into FPGA Circuits"*, Work in Progress, DSD 2011, Oulu, 30.8. - 2.9.2011

[7] SN EN 50126, Czech Technical Norm
"http://nahledy.normy.biz/nahled.php?i=59709", 2011

[8] M. Lanuzza, P. Zicari, F. Frustaci, S. Perri, and P. Corsonello. 2010. *Exploiting Self-Reconfiguration Capability to Improve SRAM-based FPGA Robustness in Space and Avionics Applications* ACM Trans. Reconfigurable Technol. Syst. 4, 1, Article 8 (December 2010), 22 pages. DOI=10.1145/1857927.1857935 http://doi.acm.org/10.1145/1857927.1857935