Self-Repair Modified Duplex System Architecture 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 describes our aims, how to increase dependability parameters (safety and reliability) of a system based on programmable hardware (FPGAs) against transient faults like a Single Event Upset. We combine Concurrent Error Detection (CED) techniques, FPGA reconfigurations and our Modified Duplex System (MDS) architecture. Our new methodology is developed for industrial practical FPGA applications and is proposed to reach the minimal area overhead for the possible future low-power SoC (System on a chip) design. It is aimed especially for modular systems. The method uses static and partial dynamic reconfiguration of FGPAs where a design is decomposed into totally self-checking blocks. The type and size of blocks to reconfigure depends on the used architecture and on the particular construction of a secured sytem.**

I. Introduction

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 reconfiguration or for other actual changes of the implemented circuit.

But the SRAM-based FPGA circuits can not be used in mission critical applications due to their high sensitivity to the radiation effects such as Single Event Upsets (SEU). The Concurrent Error Detection (CED) techniques allows detection of soft errors (errors which can be corrected by reconfiguration) caused by SEUs. Changes of the content of embedded memory Look-Up Tables (LUTs) and other configuration bits are not detectable by off-line test methods. Therefore we use CED technique in all our methods.

The self-checking (SC) structure, which uses only one copy of the SC circuit is not sufficient to increase dependability parameters. Thus, we assume to use our Modified Duplex System (MDS) architecture [1], [2].

MDS architecture uses only two blocks (instead of mostly used TMR architecture like e.g. [6]) and checkers of each block to ensure a minimal area overhead.

The reconfiguration of the whole FPGA is performed when an error (caused by SEU) is detected by checkers in MDS architecture. But this full reconfiguration is a time spending 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 described in this paper.

II. Motivation and Background

This paper presents our new technique of increasing reliability and dependability parameters of the system based on FPGAs. We propose block architecture which is derived from practical experiments in the railway station safety system design. The system is based on safety blocks realized by a finite state machine (FSM). Each block is designed as a totally self-checking circuit (TSC) [7]. This architecture ensure testability of all blocks inside and makes possible to join them. Our aim is to develop the design technique for scalable structures with defined dependability parameters, which can be used for different railways system based on FPGA. These methods are used to protect the circuits implemented in FPGA against Single Event Upsets (SEUs) and the whole system against faults.

MDS architecture, the partial and static reconfigurations are used to improve fault coverage and to increase Fault Security (FS) and Self-Testing (ST) property up to 100%. These basic criteria are in a field of CED [4].

The TSC property depends on the FS and ST properties, which are also not satisfied to 100%. For availability computations, we find the block with the lowest FS property value in the compound design.

III. Upgraded Modified Duplex System

It is necessary to create a regular structure that will use partial reconfiguration to repair transient faults. Due to the retention of reliable parameters it is important to develop a methodology how to make the reconfiguration part secure and how to observe fault-security parameters. When the fault has been localized in this part, then it has to be repaired via the reconfiguration of an external circuit or by the reconfiguration of the whole FPGA.

A. Basic Schema

In Fig. 1, you can see our proposed system, which uses TSC and MDS methods to detect and to repair possible faults caused by SEU. The upgraded MDS is based on [7], where the system uses two FPGAs with the same design. CED schema is used for all parts of the design. MDS system is extended by reconfiguration areas, where PDR is performed when an error is detected by ECC. This device contains blocks, which are all designed as TSC ones.

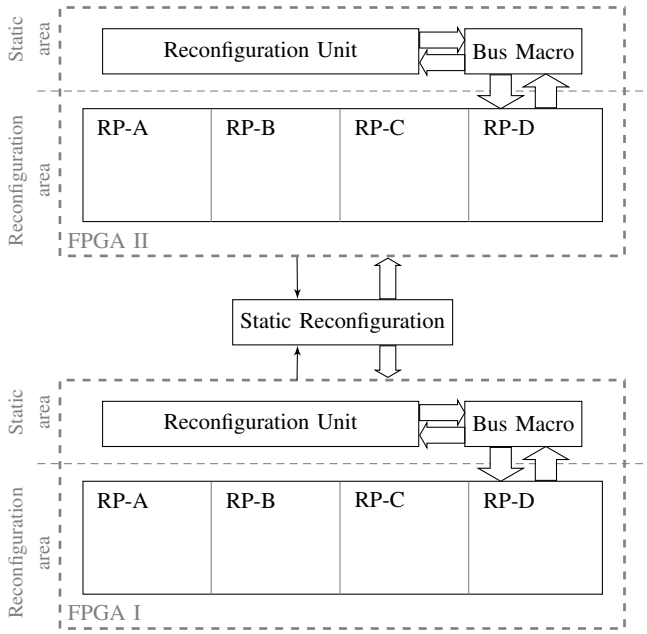

Fig. 1. Upgraded MDS Architecture

1) Reconfiguration Unit: is constructed by FSM in the static area, which controls the status of each TSC block in the reconfiguration area. When an error is occurred e. g. in RP-A part, the proposed logic detects which part does not work well and performs the partial dynamic reconfiguration of the part, where the broken block is placed. Other blocks in different parts (RP-B, RP-C, etc.) are able to work at this time. The size of blocks depends on the specific architecture of a FPGA.

2) Static Reconfiguration: is the control logic in Fig. 1, which compares wires between FPGAs and controls the function of both reconfiguration units. When an error of the function of the reconfiguration unit is detected, the "Static Reconfiguration" unit performs reconfiguration of the whole FPGA. The soft error in a static area is repaired and the device is in the default configuration with default values.

IV. Experiments

A. Practical Application - the Railway Station Safety Device

The design method of the railway station safety device is presented as a practical application here. The device is based on five types of safety blocks, each realized by a finite state machine (FSM). Each block is designed as a totally self-checking circuit (TSC). The final dependability design is based on the MDS architecture principles [1], [2].

The method of fault detection in FSM is described in [3] where the simulation of these blocks was performed. The innovation of the railway stations safety device is not so easy because of the predefined dependability properties. It must fulfil strict railways norms [5]. Therefore the dependability model has to be constructed according the real failure rate, so the fault classes have to be find out and real dependability parameters have to be compute.

B. SEU detection and future work

We would like to test our techniques in mission critical environment, e.g. high energy neutron beam and recalculate probability of fault into nature environment.

There will be some simulations in cooperation with Faculty of Transportation Sciences, Institute of Experimental and Applied Physics at Czech Technical University in Prague and Nuclear Physics Institute. Other simulations and tests have performed by injecting errors into bitstream. These experiments are in progress.

V. Conclusions

The method of creation of safety systems based on FPGA was presented. On-line testing methods were used to achieve reliable blocks. Our aim is to develop dependable systems with a minimal size of designed circuits (the minimal area overhead). The main difference is in using of our MDS architecture, which is upgraded to increase dependability parameters. The minimal area overhead is ensured by MDS architecture, which is based only on a duplex system, when classical TMR uses triplications.

Some practical tests will be performed with the cooperation with Faculty of Transportation Sciences and company AZD Praha, it means on their real model of safety railway station system, where the reliability, availability, maintainability and safety (RAMS) parameters computed according Czech standard [5] should be fulfilled.

Finally the simulation of the correct function of our technique will be performed by implementing errors directly into bitstream via the partial dynamic reconfiguration.

Acknowledgment

This research has been partially supported by the project SGS13/101/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] SN EN 50126, Czech Technical Norm *"http://nahledy.normy.biz/nahled.php?i=59709"*, 2011

[6] 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

[7] J. Borecky, M. Kohlik , P. Kubalik and H. Kubatova: *"Faults Coverage Improvement based on Fault Simulation and Partial Duplication"* In Proceedings of the 13th Euromicro Conference on Digital System Design. Los Alamitos: IEEE Computer Society Press, 2010, p. 380-386. ISBN 978-0-7695-4171-6.