# Dependability Computation for Fault Tolerant Reconfigurable Duplex System

Pavel Kubalík, Radek Dobiáš, Hana Kubátová
Department of Computer Science and Engineering
Czech Technical University in Prague
Karlovo nam. 13, 121 35 Prague 2
e-mail: (xkubalik, dobiasr, kubatova)@fel.cvut.cz

*Abstract* - **This paper describes a design method for highly reliable digital circuits based on totally self checking blocks implemented in FPGAs. The dependability model and dependability calculations are proposed. The self checking blocks are based on a parity predictor. These blocks are linked together to form a compound design. Our adapted duplex system is used as a basic structure to increase availability parameters and protect system against Single Even Upsets (SEUs). This adapted duplex system is realized by two FPGAs, where each FPGA can be reconfigured when a fault is detected. Availability parameters have been calculated by dependability Markov models.**

## I. Introduction

This paper presents a method how to design the fault-tolerant system based on FPGAs and the evaluation of the whole design based on formal dependability modeling and computations.

Our structure increases availability parameters together with ensuring a relatively low area overhead compared with classical methods such as duplication or triplication [1]. Our solution assumes a possibility of the dynamic reconfiguration of the faulty part of the system. The most important criterion is the speed of the fault detection and the safety of the whole circuit with respect to the application requirement.

The FPGAs are based on SRAM memories sensitive to Single Even Upsets (SEUs), therefore simple usage of FPGA circuits in mission critical applications without any method of SEUs detection is impossible. The evaluation the effect of SEUs on FPGAs are described in [2,3]. A design flow for protecting FPGA-based systems against single event upsets is described in [4].

The term dependability is used to encapsulate the concepts of reliability, availability, safety, maintainability, performability, and testability. Availability is a function of time, A(t), defined as the probability that a system is operating correctly and is available to perform its function its functions at the instant of time ,t [5]. We use availability computation to compare our modified duplex system with standard duplex system.

The following structures are vulnerable to SEUs: mux select lines, programmable interconnect point states, buffer enables, LUT values, and control bit values. Any changes of a mux select lines, programmable interconnect point states or buffers lead to a significant circuit function change but the function change is hardly detected for SEUs impacted in LUTs [3].

## II. Proposed Structure

Our previous results show that to fully satisfy TSC property (100%) is difficult, so we have proposed a new structure based on two FPGAs, see Figure 1.

Each FPGA has one primary input, one primary output and two pairs of checking signals OK/FAIL. The probability of the information correctness depends on the FS property. When the FS property is satisfied only to 75%, the correctness of the checking information is also 75%. It means that the signal "OK" give a correct information for 75% of occurred errors (the same probabilities for both signals "OK" and "FAIL"). To increase the dependability parameters we must add two comparators, one for each FPGA. The comparator compares outputs of both FPGAs. The fail signal is generated when the output values are different.

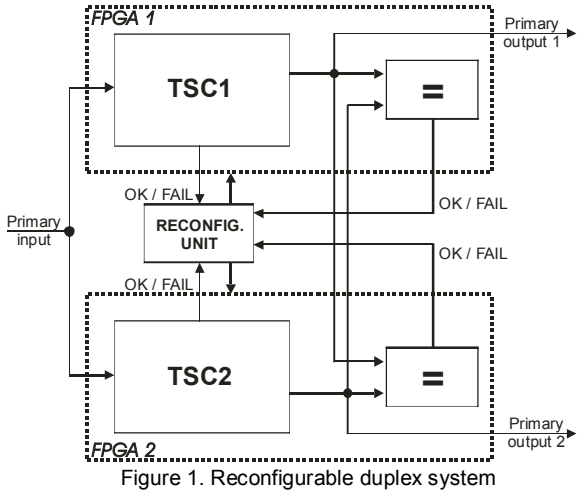


Figure 1. Reconfigurable duplex system

But this information is not sufficient to determine, which TSC circuit is wrong. Additional information to mark out the wrong circuit is generated by the original TSC circuit. The probability of the information correctness depends on the FS property and in many cases it is higher than 75%. In a case

when outputs are different and one of the TSC circuits signalizes fail function, the wrong FPGA is correctly recognized. Correct outputs are processed by the next circuit.

The reconfiguration process is initiated after a fault is detected. The reconfiguration solves two problems: localization and correction of the faulty part. The time needed to localize the faulty part is not negligible and must be included in the calculation of dependability parameters. We only detect the faulty FPGA and we reconfigure it completely. It means that we do not localize the faulty block inside the compound design. The time to localize a fault and to reconfigure the faulty part can be similar to the time to reconfigure the whole FPGA. The whole FPGA reconfiguration also masks a fault which occurred in an unused logic. The reconfiguration process can be initiated also when one of the two FPGAs signalize the "FAIL" signal. This situation occurs when a fault is detected by one of the small TSC blocks inside the compound design. The fault propagation to the primary outputs may take a long time.

When the outputs are different, and both circuits signalize a correct function, we must stop the circuit function and the reconfiguration process is initiated for both circuits. After the reconfiguration process is performed, states of both FPGAs are synchronized. It means that our adapted duplex system can be used in an application where the system reset synchronization is possible.

Each FPGA contains a TSC circuit and a comparator. The TSC circuit is composed of small blocks where each block satisfies the TSC property. The structure of the compound design satisfying the TSC property is shown in Figure 2.

We can assume six places where an error can be observable for this compound design. We assume, for simplicity, that an error occurring in the check bit generator will be observable at the parity nets (number 1) and an error occurring in the original circuit will be observable at the primary outputs (number 5).

The checker in the block N will detect the error if it occurs in net number 1, 2, 4 or 5. If an error occurs in the net number 3 or 6, it will be detected in the next checker (N+1). The method used to satisfy the TSC property for the compound design is described in [6] in more detail.

Every small block (in compound design) does not satisfy TSC property to 100%. The TSC property depends on FS and ST properties which are also not satisfied to 100%. For dependability computations, we find the block with the lowest FS property value in the compound design.

## III. Dependability Analysis

The model shown in Figure 3 describes model of our architecture.

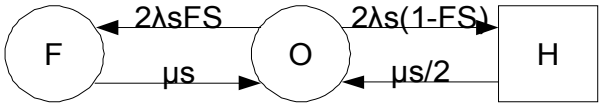


Figure 3. Model of our modified duplex system

There are three states (**O**, **F**, **H**).

The **O** state (operational) represents the regular fault-free state of the system, where both FPGAs operate correctly. It means that the fail function is signalized neither by TSC circuit, nor by comparator.

There is transition from **O** to **F** state (one FPGA is faulty) corresponding to the situation when a fault occurs in one FPGA and this fault is detected by one of TSC circuits. The system enters this state with a probability FS. $\lambda$ is the failure rate for one bit of a configuration memory and $s$ is the size of a configuration memory. Number 2 (in the 2λsFS expression) means that 2 FPGAs can be affected with SEUs. The reconfiguration process is initiated only for the faulty FPGA. The repair rate is represented by $\mu$. The second FPGA is running correctly and performs the function of the system.

Some faults are not detected, when the output vector is an incorrect codeword. The probability that an occurred fault causes incorrect codeword is equal to **1-*FS***. In this case the system comes to the state **H**.

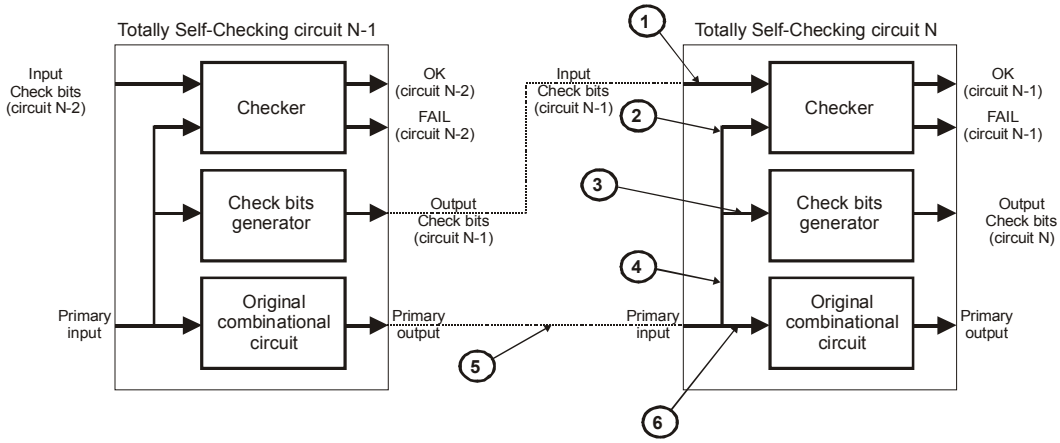


Figure 2. Proposed structure of TSC circuits implemented in FPGA

The **H** state (hazard) means that the system is in the hazard state. The hazard state is detected (e.g., by comparators), because the output vectors are not identical.

Both FPGAs have to be reconfigured in this case. The repair rate is equal to $\mu/2$, because we are reconfiguring each FPGA separately. If we are able to reconfigure both FPGAs at the same time, the availability parameters will increase.

$$\begin{aligned} 2s\lambda p_O - \mu s p_F - \frac{\mu s p_H}{2} &= 0 \\ \mu s p_F - 2s\lambda FS p_O &= 0 \\ \frac{\mu p_H}{2} - 2s\lambda(1-FS)p_O &= 0 \\ p_O + p_F + p_H &= 1 \end{aligned} \quad (1)$$

$$A_{SS} = p_O + p_F \quad (2)$$

The value of the steady-state availability $A_{SS}$ is a sum of probabilities for all working states (Equation 2).

## IV. Results

The failure rate ($\lambda$) depends on the probability that the impacting SEUs will change a bit in the FPGA configuration memory. Due to this fact we took into account the result presented in [3] and set the failure rate to:

$$\lambda = 1.8e^{-5}\ [h^{-1}]$$

The repair rate ($\mu$) depends on the time needed for the reconfiguration of an FPGA. The clock frequency was set to 25 MHz. The configuration memory size $s$ (needed for each benchmark) was calculated as a product of the configuration memory size for AT94K40 ATMEL FPSLIC and the circuit area overhead (AO[%]).

$$s = 233k \cdot AO\,[bits] \quad (3)$$

The results obtained by our case study were validated on MCNC benchmarks. Our results are shown in Table 1.

TABLE 1.
AVAILABILITY PARAMETERS

| CIRCUIT | AO [%] | FS [%] | ASS [%] |
|---|---|---|---|
| alu11 | 687,5 | 100 | 1 |
| apla | 53,3 | 82,8 | 0.9999912 |
| b11 | 7,9 | 75,5 | 0.9999938 |
| br1 | 20,0 | 62,9 | 0.9999847 |
| al2 | 11,5 | 94,3 | 0.9999985 |
| alu2 | 140,0 | 92,5 | 0.9999906 |
| alu3 | 121,4 | 90,3 | 0.9999897 |

Here "CIRCUIT" is benchmark circuit, "AO" is the area overhead, "FS" is a probability, that a fault is detected by code word and "Ass" is the steady-state availability.

## V. Conclusions

Our presented structure has been designed to increase the dependability parameters of a circuit implemented in FPGA. We figured out that the availability parameter depends on the FS property more than on the area overhead. But if the FS is not 100%, the area overhead parameter value is strictly limited by the availability value of the standard duplex system. When this value is surpassed, the availability is inferior to the standard duplex system. We can summarize that for the tested benchmarks the availability parameters have increased. E.g., "apla" with 82.8% of FS and 53% of area overhead the time, when the system is unavailable is about 2.5 shorter than for the standard duplex system.


## Acknowledgement

This research has been supported in part by the GA102/04/2137 grant and MSM6840770014 research program.


## References


[1] Dobiáš, R., Kubalík, P., Kubátová, H.: "Dependability Computations for Fault-Tolerant System Based on FPGA", In Proceedings of the 12th International Conferrence on Electronics, Circuits and Systems, IEEE Circuits and Systems Society, 2005, vol. 1, s. 377-380.

[2] Bellato, M., Bernardi, P., Bortalato, D., Candelaro, A., Ceschia, M., Paccagnella, A., Rebaudego, M., Sonza Reorda, M., Violante, M., Zambolin, P.: "Evaluating the effects of SEUs affecting the configuration memory of an SRAM-based FPGA." Design Automation Event for Electronic System in Europe 2004, pp. 584-589.

[3] Graham, P., Caffrey, M., Zimmerman, J., Sundararajan, P., Johnson, E., Patterson, C.:"Consequences and Categories of SRAM FPGA Configuration SEUs", Military and Aerospace Programmable Logic Devices International Conference, Washington DC, MAPLD 2003 Paper C6.

[4] Sterpone, L., Violante, M.: "A design flow for protecting FPGA-based systems against single event upsets ", DFT2005, 20th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, pp. 436 – 444.

[5] Pradhan, D. K., Fault-Tolerant Computer System Design, Prentice-Hall, Inc., New Jersey, 1996.

[6] Kubalik, P., Kubatova, H.: "High Reliable FPGA Based System Design Methodology." Work in Progress Session of 30th EUROMICRO and DSD 2004, Universitat Linz 2004 pp. 30-31.