Dependability Computations for Fault-Tolerant System Based on FPGA

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

Abstract

The methods how to design a fault-tolerant system based on FPGAs is presented. The evaluation of the whole design according the computations of reliability and dependability characteristics is described. The formal dependability model and computations obtained on the base of this model is summarized.

1. Introduction

The “dependability” is currently used to express the ability of a system or of a component of a system to correctly perform its function, or “mission” over time, [10]. This paper presents the methods how to design fault-tolerant system based on FPGAs and presents the evaluation of the whole design based on formal dependability modeling and computations.

The radiation impact on integrated circuits grows and the FPGA circuits are more sensitive to radiation than ASICs. Concurrent error detection (CED) techniques allow faster detection of soft errors (errors which can be corrected by reconfiguration) caused by Single Event Upsets (SEU) [1, 2]. SEU can change the embedded memory or Look-up Tables (LUTs) used in the design. These changes are not detectable by off-line tests, therefore some CED techniques have to be used. The probability of a SEU appearing in random access memory (RAM) is described in [3].

Our structure increases dependability parameters together with ensuring a relatively low area overhead as compare with the classical methods such as duplication or triplication.

Our solution assumes the possibility of 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 surrounding environment. Our methodology enables cooperation between on-line diagnostic methods and off-line BIST for fault detection and localization.

Our previous research shows the relation between the area overhead and the fault coverage [4]. Due to the requirement of small area overhead the fault coverage for most circuit is less than 100%. The fault coverage varies typically from 75% to 95%. Therefore we must use an additional method to ensure full fault coverage and to increase reliability parameters.

The paper is organized as follows: firstly the basic terms are presented in Section 2. The proposed structure to be implemented in FPGAs is described in Section 3. The dependability models and computations are presented in Section 4. Section 5 summarizes the results obtained from these models and Section 6 concludes the paper.

2. Basic dependability terms

There are three basic terms in a field of CED: fault security (FS), self-testing property (ST) and totally self-checking (TSC). These three terms have to be used in an on-line testing field to evaluate the level of safeness of the designed or modeled system.

To determine whether the circuit satisfies TSC properties, detectable faults belonging into one of four groups A, B, C and D [5] have to be calculated. The hidden faults belong to the class A. This fault classification can be used to calculate how much the circuit is FS or ST and than calculate TSC properties. Typical results of ST and FS properties are shown in table 1.

Table 1. Single even parity – PLA

Circuit	Parity nets	Original [LUT]	Parity [LUT]	Overhead [%]	FS
apla	1	46	23	50	82,6
b11	1	37	3	8	77,3
br1	1	54	10	19	62,1
al2	1	52	4	8	91,7
alu3	1	26	32	123	92

In our research, parity predictors are used to generate proper output code of the circuits. These techniques ensure a small area overhead with higher fault coverage but the fault coverage reached is not hundred percent [6, 7, 8].

3. Proposed structure

Due to our previous results showing the difficulty to fully satisfy TSC properties (100%), we have proposed a new structure based on two FPGAs, Fig.1. Each FPGA contains a TSC circuit and a comparator. The TSC circuit is composed of small circuits where every block satisfies the TSC property. The methods how to satisfy TSC property for the compound design is described in [9].

Every FPGA has one primary input, one primary output and two pairs of checking signals OK/FAIL. The first checking signal generated by the TSC circuit serves as additional information.

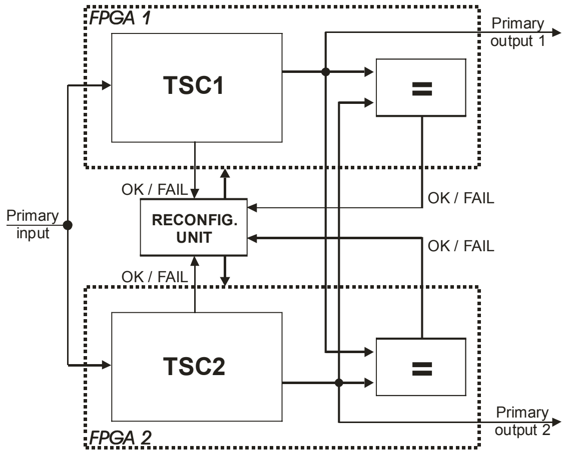

Figure 1. Reconfigurable duplex system

The probability of the information correctness depends on the TSC properties. When the TSC property is satisfied only in 75% the correctness of checking information is also 75%. It means that signal OK is correct for 75% of occurred errors (same probabilities for both signals OK and FAIL). To increase the reliability parameters we must add two comparators, one for every FPGA. The comparator compares outputs from both FPGAs. When these outputs are different the fail signal is generated. But this information is not sufficient to say, 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 TSC properties and in many cases is higher than 75%. In a case when outputs are different and one of circuits generates the fail signal, the wrong circuit is correctly detected. Correct outputs can be 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 into the calculation of reliability parameters.

When the outputs are different and both circuits signalize a correct function, we must stop the circuits and fault detection must be processed for both circuits.

4. Dependability analysis

To evaluate the influence of a sequence of transient faults, a more precise definition of "single fault" is needed. In the following text we will assume a single data damaging a transient fault that is defined as follows:

- It will occur at a single time instant that is arbitrarily located at the time axis
- The fault can destroy a data item located within a FPGA configuration memory. Both FPGAs can be attacked with the same probability. The assumed "width" of a fault is one bit in a configuration memory. Every bit of the FPGA bit-stream memory can be attacked with the same probability.
- The time distance between any two successive transient faults is as large as to recover from the previous fault (otherwise it is a multiple fault).

It is an abstract (logical) model of a kind of real faults. The physical fault that fits well to the defined fault model is a radiation (e.g. a neutron) that can randomly disturb a memory bit. The radiation impact due to its nature can come repeatedly, randomly attacking any part of the configuration memory with the uniform distribution concerning the place of the impact, and with an exponential distribution concerning the "inter-impact" time.

Some basic rules were defined to calculate reliability parameters. We assume that:

- There is at least one vector coming between two SEUs, which cause a different output from the normal operation.
- SEUs impacting an unused logic do not change function of the used part. These faults are described as hidden faults.
- The hidden faults are not considered in our calculation.
- Maximum usable area of FPGA is less than 75%.
- The comparator is fully TSC.
- The checker is fully TSC.
- The reconfiguration unit is fully TSC.

- The area overhead of the comparator, the checker and the reconfiguration unit is negligible.
- The reconfiguration unit loads a correct configuration data after a fault is detected. Time needed to reconfigure the faulty part depends on the configuration data size.

The model in Fig. 2. describes our architecture.

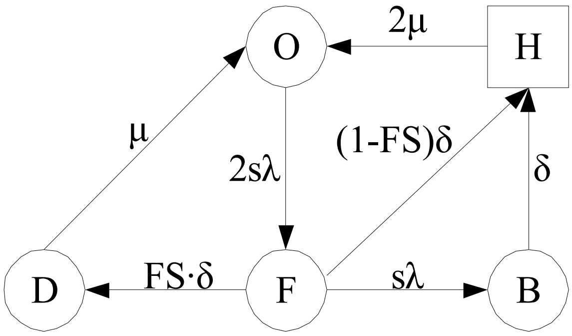

Figure 2. Model of duplex system with parity check

There are five states (**O**, **F**, **D**, **B**, **H**). **O** state (operational) means the normal fault-free state of the system, where both FPGAs operate correctly.

F state (one FPGA is faulty) is entered when a fault occurs in one FPGA (λ is the failure rate for one bit of a configuration memory and s is the size of a configuration memory). The system works and still does not detect a fault; the system contains the latent fault. The self-test of the system using all inputs vector needs time; the respective self-test rate is labeled $\boldsymbol{\delta}$. Some faults are not detected, because the output vector is a correct code word. The probability that an occurred fault causes it, is equal to **1-*FS***. In this case the system comes to the state **H**. When the fault is detected by a non-code word in the output vector, the system comes to the state **D**. If some fault occurs in the second FPGA, the system comes to the state **B**.

D state (detected) means that an occurred fault was detected and it is possible to reconfigure the part of an FPGA, where this fault is located. The repair rate is represented by $\boldsymbol{\mu}$.

B state (both FPGAs faulty) means that the fault occurred in the second FPGA. The system still works but if the output vectors are not identical the system immediately comes to the **H** state. It is quick process, but as a worst case can be substituted by self-test rate $\boldsymbol{\delta}$.

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. In this case both FPGA have to be reconfigured. The repair rate is represented by $\boldsymbol{2\mu}$.

The described model introduces four constants: a failure rate (λ), a repair rate ($\boldsymbol{\mu}$), a fault security (***FS***), the configuration memory size ($\boldsymbol{s}$) and a self-test rate ($\boldsymbol{\delta}$). These parameters are discussed in the next section. Now let us transform the Markov model into a system of equations describing the steady state probabilities of every state. The system of equations is completed with a normalisation condition.

$$
\begin{aligned}
&2s\lambda\, p_O - \mu\, p_D - 2\mu\, p_H = 0\\
&FS\,\delta\, p_F + (1-FS)\delta\, p_F + s\lambda\, p_F - 2s\lambda\, p_O = 0\\
&\mu\, p_D - FS\,\delta\, p_F = 0\\
&\delta\, p_B - s\lambda\, p_F = 0\\
&2\mu\, p_H - \delta\, p_B - (1-FS)\delta\, p_F = 0\\
&p_O + p_F + p_D + p_B + p_H = 1
\end{aligned}
$$

The value of the steady-state availability A_{SS} is a sum of probabilities for all working states:

$$A_{SS} = p_O + p_F + p_D + p_B$$

To compare our design the following models of Duplex and Triplex system was taken into account:

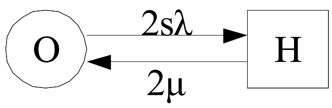

Figure 3. Model of duplex system

The model of duplex system (see Fig. 3) consists of two states (**O**, **H**), which have mostly the same meaning as in the previous model. The main difference is that if a fault occurs in one of two FPGAs it is immediately detected by comparators. Because there is not possible to detect which FPGA contains this fault, both FPGAs need to be reconfigured.

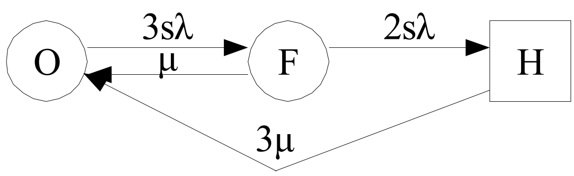

Figure 4. Model of triplex system

The model of triplex system (see Fig. 4) consists of three states (**O**, **F**, **H**). When a fault occurs in one of three FPGAs, The reconfiguration process starts when comparators detect a fault in one from three FPGA. During the reconfiguration process a second fault can occur in one of two remaining FPGAs. This fault is also detected in this case but it is not possible to detect which FPGA is faulty; all FPGAs need to be reconfigured.

5. Results

Firstly we discuss the model parameters. The failure rate (*λ*) depends on the fault hypothesis. Because the SEU fault is supposed, we took into account the result in [3] and set the fault rate to:

$$\lambda=2e^{-5}\,[h^{-1}]$$

The repair rate (***μ***) depends on the time needed for the reconfiguration of an FPGA. The operational frequency was set on 25 MHz. The configuration memory size (needed for each benchmark) was calculated as a product of the configuration memory size for AT94K40 ATMEL FPSLIC and the area overhead.

The self-test rate (δ) depends on the real application and also on the frequency of occurrence of the input vector detecting the fault. The self test rate was calculated for every circuit individually.

The fault security (***FS***) and the used bit-stream size (***s***) is summarised in Table 2, where the results obtained from the computation of the models is also included. Here "C" is benchmark circuit, "FS" is a probability that a fault is detected by code words, "S(b)" is configuration memory size for one FPGA, "Ass" is the steady-state availability.

Table 2. Availability parameters

C	SINGLE PARITY			DUPLEX		TRIPLEX	
	FS	S[b]	Ass	S[b]	Ass	S[b]	Ass
alpa	83	349k	0.9_5787	233k	0.9_5184	233k	0.9_8986
b11	77	252k	0.9_5856	233k	0.9_5412	233k	0.9_8993
br1	62	257k	0.9_5750	233k	0.9_5402	233k	0.9_8992
al2	92	242k	0.9_5951	233k	0.9_5434	233k	0.9_8993
alu3	92	520k	0.9_5783	233k	0.9_4879	233k	0.9_8970

6. Conclusion and future work

Our structure was design to increase the dependability parameters. This paper computes these characteristics from the formal reliability models. These models include the possible reconfiguration of faulty parts.

The proposed structure has been implemented in one and in two special hardware kits AT94K40. The relationship between the implementation and formal models has been searched for and improved with respect to low area overhead.

Our future work will be intended mainly to the improvements of reliability models credibility, to more precise computations by using different formal models and software tools and finally to the optimization of the whole design.

7. Acknowledgement

This research has been in part supported by the GA102/03/0672 grant and MSM6840770014 research program.

8. References

[1] QuickLogic Corporation.: Single Event Upsets in FPGAs, 2003, www.quicklogic.com

[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] Normand, E.: "Single Event Upset at Ground Level," IEEE Transactions on Nuclear Science, vol. 43, 1996, pp. 2742-2750.

[4] Kubalík, P., Kubátová, H.: "Minimization of the Hamming Code Generator in Self Checking Circuits", Proceedings of the International Workshop on Discrete-Event System Design - DESDes'04. Zielona Gora: University of Zielona Gora, 2004, s. 161-166.

[5] Kafka L., Kubalík P., Kubátová H., Novák O.: "Fault Classification for Self-checking Circuits Implemented in FPGA.", Proceedings of IEEE Design and Diagnostics of Electronic Circuits and Systems Workshop. Sopron University of Western Hungary, 2005, s. 228-231.

[6] Drineas, P., Makris, Y.: "Concurrent Fault Detection in Random Combinational Logic.", Proceedings of the IEEE International Symposium on Quality Electronic Design (ISQED), 2003, pp. 425-430.

[7] Mitra, S., McCluskey E. J.: "Which Concurrent Error Detection Scheme To Choose?" Proc. International Test Conf. 2000, pp. 985-994.

[8] Mohanram, K., Sogomonyan, E. S., Gössel, M., Touba, N. A.: "Synthesis of Low-Cost Parity-Based Partially Self-Cheking Circuits", Proceeding of the 9th IEEE International On-Line Testing Symposium 2003, pp. 35.

[9] 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.

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