2012 IEEE 15th International Conference on Computational Science and Engineering

Susceptibility Analysis of LEON3 Embedded Processor Against Multiple Event Transients and Upsets

Hamed Abbasitabar [a], Hamid R. Zarandi [a,b], Ronak Salamat [a]
[a] Department of Computer Engineering and Information Technology, Amirkabir University of Technology (Tehran Polytechnic)
[b] School of Computer Science, Institute for Research in Fundamental Sciences (IPM), P. O. Box 19395-5746
E-mails:abbasitabar@ce.sharif.edu, {h_zarandi, ronak_salamat}@aut.ac.ir

Abstract— **This paper presents an analysis of the effects and propagations of different faults such as Single Event Transient (SET), Multiple Event Transients (MET), Single Event Upset (SEU) and Multiple Bit Upsets (MBU) by simulation-based fault injection into Areoflex Gaisler LEON3 processor which is a 32 bit synthesizable processor based on SPARC V8 architecture. LEON3 is designed for ground-based applications. This investigation is done by injecting nearly 11200 transient faults into different components of LEON3 including flip-flops, registers, register-file and cache memories. The behavior of LEON3 processor against injected faults is reported. Besides, it is shown that nearly 52.83% of SEUs are overwritten; 31.74% of SEUs are latent and finally 15.43% of them are reported as failure while 44.74% of MBUs are overwritten; 38.42% of them are latent and 16.84 of these kind of faults are failed. Also, 98.03% of SETs are overwritten; 0.6% of them are latent and 1.36% of SETs are reported as failures. Finally, the effects of METs are as follows: 96.71% for overwritten faults; 1.15% for latent and 2.14% for failure. Moreover, integer unit and multiplier unit are the most susceptible components against single and multiple faults respectively.**

Keywords- Embedded Processor; LEON3; Transient Faults; Dependability Evaluation; Simulation-based Fault Injection

I. INTRODUCTION

Embedded systems are widely used in automotive, avionics, railways, security functionalities, robotics and military applications. Previously, they were just found in controlling physical process and now they are used everywhere [1]. In addition, several embedded processors can be exploited in FPGA chips for high performance computing [2]. Therefore, their importance in the current technology could not be ignored.

Embedded systems should be efficient enough from the power perspective, run time issues, weight and cost [3]. One of the main components of embedded systems is their processors having great impact on regulating the mentioned factors and determining the constraints of running system. Due to the considerable usage of the processors in the embedded systems, designing an efficient processor and evaluating its performance from different aspects is a great concern.

Since the processors have a critical role in the embedded systems, unique attributes of LEON3 such as the great performance up to 800MHZ, optimized power consumption which is about 0.4 watt, cost efficiency and synthesizability for FPGAs and ASIC designs causes that it will be considered by the embedded designers .

Recently, reliability has become one of the most major aspects in designing embedded systems [4]. Therefore, investigating the behavior of the system against various faults such as Single Event Upset (SEU), Single Event Transient (SET) caused by Electromagnetic Interfaces (EMI), alpha particles' and cosmic radiation would be mandatory since this investigation provides an overlook about the reliability of the system.

Reliability issues of LEON3 should not be ignored because it has been widely used in automotive, multimedia systems such as MP3 and DVD players, mobile phones, wireless and other low-end and high-end applications [5], [6]. It should be considered that a fault-tolerant version of LEON3 named LEON3FT was suggested which is used in aerospace applications [5] while LEON3 is designed for ground-based applications. Non safety-critical applications might employ LEON3 with less reliability excepting.

Second, another version of LEON3 named LEON4 processor was suggested [7]. It provides an improved pipeline structure and wider cache memories. Moreover, it increases performance 25-50% for a typical application in comparison with LEON3 at the same clock frequency while LEON4 increases cost. So, LEON4 is suitable for very high performance usage. On the contrary, LEON3 provides acceptable performance for the applications which is used for them with lower cost. Also, LEON3 is available freely under GPL license for academic researches. Hence, reliability analysis of LEON3 against faults would be possible.

In order to investigate the effects of faults, simulation-based fault injection technique would be applicable since it provides high controllability and observability in comparison with the other fault injection methods. In this technique, different faults will be injected to the desired points of the LEON3 architecture described in the VHDL language, and ultimately the effects of these transient faults will be observed.

Fault injection in LEON processors is used in several works. In [8], crash test, which is a fast FPGA-based framework, evaluates the effects of SEUs and some permanent models. It uses LEON3 as a case study. A virtual platform with fault injection capability named LEON3 ViP is presented in [9]. A modular fault injector for multiple faults and security evaluation is brought up in [10] which uses LEON3 as a case study. The effects of SEUs and the needed time for error recovery in LEON3 is presented in [11]. FPGA-based fault injection technique for SEU fault model is introduced in [12] which employed LEON2 as a case study.

978-0-7695-4914-9/12 $26.00 © 2012 IEEE
DOI 10.1109/ICCSE.2012.81

A fault injection platform for SEU faults using LEON2 as a case study is presented in [13].

In previous works, only the effects of SEUs have been investigated. Therefore, the effects of MBUs, SETs and METs have not been investigated. Moreover, SEUs cannot manifest the effect of multiple faults which are present in the actual failed circuit [14]. Therefore, the effects of SEUs, MBUs, SETs and METs in LEON3 processor are investigated. Results represents that nearly 52.83%, 44.74%, 98.03% and 96.71% are overwritten for SEUs, MBUs, SETs and METs respectively. Also, the most percentage of latent errors is reported for MBUs with 38.42%. Finally, the order of failure percentage is 16.84%, 15.43%, 2.14% and 1.36% for MBUs, SEUs, METs and SETs respectively.

The reminder of this paper is organized as follows: section 2 describes an overview of LEON3 processor; section 3 presents the characteristics of simulation-based fault injection. Fault injection results are presented in section 4 and finally section 5 concludes the paper.

II. LEON3 ARCHITECTURE

LEON3 is a 32-bit synthesizable processor which is compatible with SPARC V8 architecture (IEEE-1754). The LEON3 core has 7 pipeline stages and Harvard architecture. Also, it uses separate instruction and data cache memories and supports multiprocessors up to 4 cores.

This processor benefits the VHDL synthesizable code. Moreover, it provides full configuring core. Therefore, designers would be able to configure the processor in order to optimize the power consumption, input/output power, area and cost. Furthermore, this processor is suitable for System on Chip (SoC) designs. It would be able to be used with Gaisler Research IP Library (GRLIB).

As Figure I shows, LEON3 exploits AMBA 2.0 AHB bus to communicate with USB 2.0, PCI, CAN 2.0, Ethernet and Spacewire. Moreover, it is connected to VGA, Timers, UART and other I/O devices through APB bus.

In this study, the ASIC design of LEON3 is considered since it has low dependency to the target technology of synthesized chip. Table I summarizes the important attributes of the processor and the other attributes are set to default value. As it will be shown in Table I, the processor is used in single core mode. Furthermore, Integer unit is always active and it is able to do multiplications and divisions.

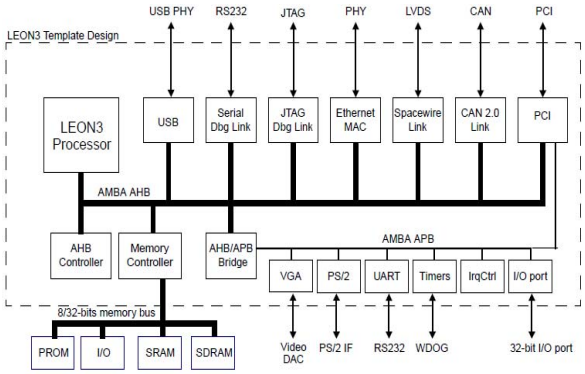

Figure I. An example of LEON3 system designed with GRLIB [5]

TABLE I. LEON3 CONFIGURATION

	Attribute	Value
Synthesis	Memory Library	UMC18
Processor	No of processors	1
	SPARC register windows	8
Integer Unit	SPARC V8 MUL/DIV instructions	yes
	Enable power down mode	no
Floating-point unit	Enable FPU	no
Data and Instruction Cache system	Enable Instruction Cache	yes
	Associativity(sets)	1
	Set size(KBytes/set)	4
	Line size(Bytes/line)	32
	Enable local instruction RAM	yes
MMU	Enable MMU	no
AMBA Configuration	32 bit program counter	no
	Round Robin arbiter	yes
	AHB split-transaction support	no
Debug Link	Enable AMBA AHB monitor	no
	Serial debug link	yes
	JTAG debug link	no

In order to investigate the behavior of the processor, Memory Management Unit (MMU), Spacewire link and Floating point Unit working as a coprocessor are inactive.

III. FAULT INJECTION

The three workloads which are considered in fault injection experiments are selected from MiBench [15] workloads. They are namely: Quick Sort (QSort), Advanced Encryption Standard (AES) and Cyclic-Redundancy Check 32 (CRC32). QSort is a kind of an industrial workload which sorts an input array. AES is an encryption algorithm which is used in security applications. Moreover, it is sometimes called Rijnadael Encryption. CRC32 is categorized in network and telecommunication workloads as an error detection algorithm.

As it was mentioned, this analysis is based on simulation-based fault injection and Modelsim [16] which is a digital ASIC simulation and verification tool is used in order to run the experiments.

Different fault models that are considered are namely: SEU, MBU, SET and MET. Script generator is used in order to generate Modelsim scripts which are able to control the flow of running program on the processor. Moreover, it selects a random point in the processor at a random time and finally applies one or more bit-flips to the desired point. One consideration is that the selected random time in which the fault is activated covers 5% to 80% of the simulating runtime because it takes nearly 5% for a processor to pass the warm up time.

Table II shows that configured processor includes 660 flip-flops and registers, one register file including 136 words, data cache including 128 words for tags and 1024 words for data and finally instruction cache including 128 words for tag and 1024 words for data. As it can be clearly seen in Table II, 660 faulty experiments are done on flip-flops and registers. Hence, one faulty experiment is done for each flip-flop and register.

TABLE II.NUMBER OF FAULT INJECTIONS IN DIFFERENT MODULES

Number of fault injections	Fault injection points
660	Flip-flops and registers
136	Register file
128	Data cache - Tag
1024	Data cache – Data
128	Instruction cache – Tag
1024	Instruction cache - Data

Furthermore, the number of fault injection experiments in the register file, data cache and instruction cache is determined according to the number of words in the modules. Since one SEU occurs in a random bit in a word situated in the register file, 136 experiments is done for register file. The fault injection experiments are done in data cache and instruction cache according to the number of their memory words. All of these experiments repeated for each workload. Generally, SEU causes bit-flip in these memory cells. One consideration is that the inverted value of the memory cell is hold for one clock period. Then, this memory cell might be driven by a new value from the combinational circuit or remained as faulty.

IV. EXPERIMENTAL RESULTS

Results of fault injection experiments are presented in this section. These results are categorized in four sections: first, investigating the effects of SEUs, second MBUs, third and forth analysis the effects of SETs and METs respectively.

In order to analyze the effects of faults, the results of faulty runs of programs is compared with the expected values in the golden run of the programs. So, three classes of results are reported as follows: recovered faults, latent errors and failures. It should be considered that what we mean recovered results are the ones in which the faulty values are overwritten during the simulation time. Consequently, in evaluation phase the final results are not different from the golden results. In some cases, the injected fault changes the behavior of intermediate signals during small or large number of clock cycles without having an effect on the final results. These kinds of faults are named latent errors which do not transform to errors during simulation time. Finally, failures are the ones in which the final compared results are different from the golden values.

Table III shows the results of SEU injection in different parts of the processor. The results of SEU injection into different applications are reported. As it can be clearly seen in Table III, the percentage of recovered faults in registers and flip-flops is much further rather than the latent error and failures since the combinational circuits between registers and flip-flops results in the fault getting overwritten. The other considerable point is that the percentage of latent errors in AES application is high in all the components since AES application writes data in different addresses in memory elements and it has less reference to it in order to write again in future. Therefore, they could not be overwritten and they remain as latent. Besides, the rate of failure in the data part of the data cache is the most because of the fact that it is targeted for reading a lot.

TABLE III. SEU ANALYSIS

LEON3 Portion	Workload	# of Injected Faults	Overwritten (%)	Latent (%)	Failure (%)
Regs & FFs	QSort	545	90.09	2.39	7.52
	CRC32	544	90.44	2.39	7.17
	AES	544	88.60	3.31	8.09
	Average	544	89.71	2.70	7.59
Reg File	QSort	136	59.56	12.50	27.94
	CRC32	136	40.44	50.00	9.56
	AES	136	16.91	72.79	10.29
	Average	136	38.97	45.10	15.93
Data Cache - Tag	QSort	128	30.47	69.53	0
	CRC32	128	55.47	44.53	0
	AES	128	8.59	90.63	0.78
	Average	128	31.51	68.23	0.26
Data Cache - Data	QSort	178	12.36	53.37	34.27
	CRC32	308	8.44	39.29	52.27
	AES	287	2.44	63.41	34.15
	Average	258	7.75	52.02	40.23
Instruction Cache - Tag	QSort	128	64.84	35.16	0
	CRC32	128	69.53	30.47	0
	AES	128	1.56	98.44	0
	Average	128	45.31	54.69	0
Instruction Cache - Data	QSort	513	65.11	20.08	14.81
	CRC32	419	83.05	13.60	3.34
	AES	613	1.14	66.39	32.46
	Average	515	49.77	33.36	16.87
Average	QSort	1628	64.50	22.24	13.27
	CRC32	1663	65.00	21.35	13.65
	AES	1836	28.98	51.63	19.39
	Average	1709	52.83	31.74	15.43

Also, the rate of failure in the tag part of the instruction cache is reported as zero due to the write through method between the processor and cache. In other words, each of the writings in the tag corresponds to writing in the related word in the memory. So, the valid data is always present in the memory. Hence, there is no failure. This is also true for the tag part of the instruction cache.

In MBU fault injection, according to [16] the effects of two to five bit-flips are investigated. The activation time for bit-flip is considered as one clock period. According to [18], for technology 150 nm SRAM cells, the pattern of fault injection experiments which should be selected for special number of bit-flips is determined according to the possibility of the occurrence of that special pattern. In other words, the number of MBU experiments is done according to the probability of the occurrences of multiple bits (number of bit flips is also selected from two to five according to [17]). Table IV represents the results of MBU fault injection. As it can be seen in Table IV, occurrence of two bit-flips has higher possibility. So, more experiments should be done for this kind of MBU rather than the other MBUs. As the number of bit-flips increases, the number of fault injection experiments for that specific bit-flip decreases since they have lower possibility.

As the results represents, the percentage of recovered, latent and failure for different number of bit-flips is the same. Consequently, the number of bit-flips has no effect on the final results. Finally, comparison among the effects of SEUs and MBUs in LEON3 concludes that this processor recovers SEU faults more than MBUs.

TABLE IV. MBU ANALYSIS

Workload	#of bit-flips	# of faulty experiments	Overwritten (%)	Latent (%)	Failure (%)
QSort	2	291	60.82	20.96	18.21
	3	119	62.18	21.85	15.97
	4	35	40	34.29	25.71
	5	22	45.45	22.73	31.82
CRC32	2	207	51.21	37.68	11.11
	3	78	58.97	29.49	11.54
	4	26	69.23	19.23	11.54
	5	19	63.16	36.84	0
AES	2	201	21.39	58.21	20.40
	3	91	16.48	58.24	25.27
	4	26	26.92	61.54	11.54
	5	19	15.79	63.16	21.05
Average	2	233	44.47	38.95	16.58
	3	96	45.88	36.53	17.59
	4	29	45.38	38.35	16.27
	5	20	41.47	40.91	17.62

The rate of recovered faults for SEUs is about 52.83% in LEON3 while it is 44.74% for MBUs. Moreover, LEON3 is a bit more susceptible to MBUs rather than SEUs since the rate of failure is nearly 16.84% for MBUs while it is 15.43% for SEUs.

In order to investigate the effects of SETs, all the signals of LEON3 were considered. In order to inject SETs, one bit signal is selected by uniform distribution from the whole signals. The SET duration is calculated by means of an exponential distribution with respect to the value of one clock period. Totally, 2585 faulty experiments were done to analyze the effect of SETs. Table V represents the effects of SET injection on different workloads.

Table VI shows the results of METs on LEON3. The number of METs is similar to MBUs. Other characteristics are similar to SET.

Comparison among the effects of SETs and METs indicated that most of the injected faults have no effect on LEON3 since nearly 98.03% of SETs and 96.71% of METS are recovered. Therefore, most of the signals have no effect on the behavior of the workloads.

As an example, if the fault injection occurs in the control parts of the interrupts, the fault injection effects which were done on the workloads having no interacts with I/Os, will be ineffective.

TABLE V. SET ANALYSIS

Workload	# of injected faults	Overwritten (%)	Latent (%)	Failure (%)
QSort	865	97.3	0.9	1.8
CRC32	862	98.18	0.68	1.14
AES	858	98.62	0.23	1.15
Average	879	98.03	0.6	1.36

TABLE VI. MET ANALYSIS

Workload	# of bit-flips	# of faulty experiments	Overwritten (%)	Latent (%)	Failure (%)
QSort	2	350	97.43	0.86	1.71
	3	238	97.06	2.10	0.84
	4	231	95.24	1.73	3.03
	5	114	98.25	0.88	0.88
CRC32	2	203	98.03	0.49	1.48
	3	160	96.88	0.63	2.50
	4	168	93.45	4.17	2.38
	5	72	93.06	2.78	4.17
AES	2	338	96.75	0.59	2.66
	3	200	98.50	0	1.50
	4	188	96.28	0	3.72
	5	108	99.07	0	0.93
Average	2	297	97.40	0.65	1.95
	3	199	97.48	0.91	1.61
	4	196	94.99	1.97	3.04
	5	98	96.79	1.22	1.99

Finally, an investigation has been done on error propagation latency and amount of error propagation in different components of the processor. Error propagation delay for SEUs compares with error propagation delay for MBUs in Figure II. Error propagation latency means the time starts from the moment that forced value is finished to the moment that one of 660 internal registers of the processor would have different values from the golden values.

Figure III compares error propagation latency in SETs versus METs. Comparison among Figure II and III represents that error propagation latency in SEU and MBU fault injections has higher values rather than SETs and METs since SETs and METs usually occur in combinational circuits. Therefore, they propagate quickly (often less than a clock period) while memory elements might not have been read for a long time for SEUs or MBUs.

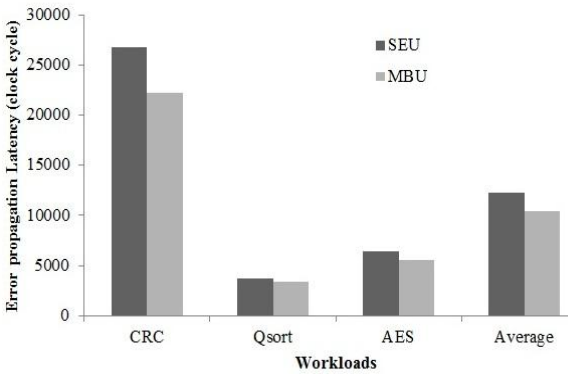

Figure II. Comparison of error propagation latency among SEUs and MBUs

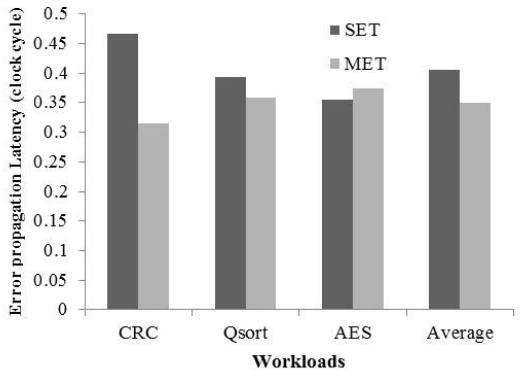

Figure III. Comparison of error propagation latency among SETs and METs

Besides, it can be clearly understood that error propagation latency for single faults is higher than multiple faults because probability of propagating multiple faults is higher than single faults.

In order to determine the most susceptible component against various faults Figure IV and Figure V is presented. In these Figures criticality of each component against various faults is measured. As it is shown in Figure IV, integer unit is the most susceptible component against SEUs and MBUs. It should be considered that the fifth group represents the criticality in a group of components. So, the criticality in each of the components is lower than the criticality in the integer unit although the total criticality is more than the integer unit. Figure V illustrates that the most susceptible component against SETs and METs is the multiplier unit.

V. CONCLUSIONS

An analysis of the effects and propagations of various fault models in Aeroflex Gaisler LEON3 processor was done in this paper.

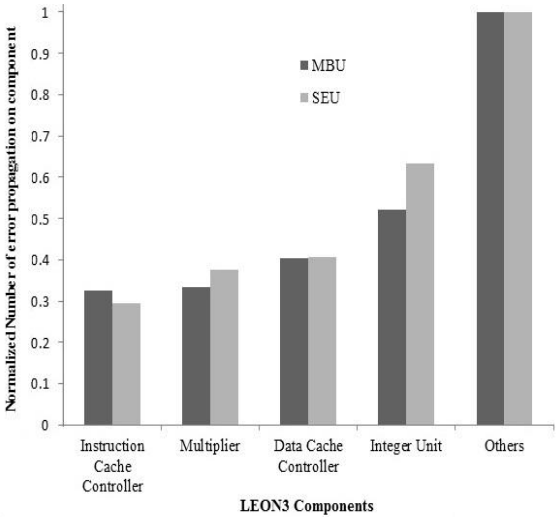

Figure IV. The normalized value of error propagation for SEUs and MBUs in different components of the processor

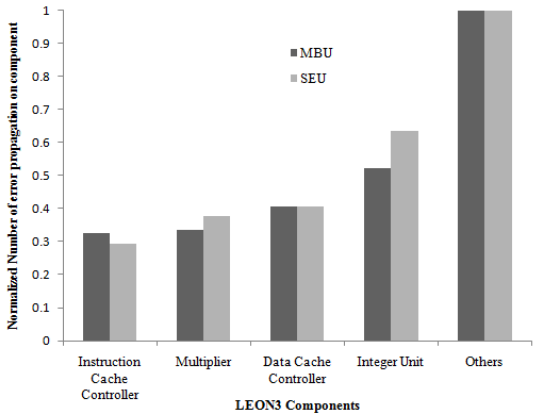

Figure V. The normalized value of error propagation for SEUs and MBUs in different components of the processor

This investigation is based on simulation-based fault injection into VHDL model of LEON3 using Modelsim tool. The fault models considered in this evaluation are namely: SEU, MBU, SET and MET. These faults are injected into different components of this processor including flip-flops and registers, register file and cache memories. Through the analysis of the behavior of LEON3 against SEUs, it was revealed that 52.83% of injected faults are overwritten; 31.74% of faults are latent and 15.43% are failed. In order to investigate the effects of multiple faults, the effects of two to five bit-flips are considered. It should be mentioned that QuickSort, CRC32 and AES are the workloads used for fault analysis. The effects of multiple faults showed that 44.74% of multiple faults are overwritten during simulation time; 38.42% of them are latent and finally 16.84% of them reported as failure. Besides, SET evaluation revealed that 98.03% of SET faults are overwritten faults, 0.6% of them are latent and 1.36% of faults are failed. Hence, most of the SET faults has no impact on LEON3. Furthermore, 96.71% of METs are recovered; 1.15% and 2.14% are reported for latent faults and the percentage of failure respectively. To conclude with, integer unit is the most susceptible component against SEUs and MBUs while multiplication unit is the most sensitive component against SETs and METs.

REFERENCES

[1] P. Marwedel, *Embedded System Design: Embedded System Foundations of Cyber-Physical Systems*,: Springer, 2010.

[2] C. Bobda, *Introduction to Reconfigurable Computing: Architectures, Algorithms and Applications*: Springer, pp. 52-55, 2010.

[3] A. Malinowski and H. Yu,"Comparison of Embedded System Design for Industrial Applications," *IEEE Transactions on Industrial Informatics*, vol. no. 7, pp. 244-254, 2011.

[4] S. K. Pedro José Marrón, Daniel Minder, Aníbal Ollero, *The Emerging Domain of Cooperating Objects*: Springer, pp. 13-15, 2011.

[5] J. Gaisler, E. Catovic, M. Isomaki, K. Glembo, and S. Habinc, "GRLIB IP Core User's Manual," *Gaisler Research*, 2012.

[6] J. Gaisler, S. Habinc, and E. Catovic, "GRLIB IP Library User's Manual," *Gaisler Research,* 2012.

[7] Gaisler Site, http://www.gaisler.com/cms.

[8] A. Pellegrini, K. Constantinides, D. Zhang, S. Sudhakar, V. Bertacco, and T. Austin, "CrashTest: A fast high-fidelity FPGA-based resiliency

analysis framework," *IEEE International Conference on Computer Design*, pp. 363-370, 2008.

[9] A. da Silva and S. Sanchez, "LEON3 ViP: A Virtual Platform with Fault Injection Capabilities," Digital System Design: Architectures, *13th Euromicro Conference on Methods and Tools*, pp. 813-816, 2010.

[10] J. Grinschgl, A. Krieg, C. Steger, R. Weiss, H. Bock, and J. Haid, "Modular Fault Injector for Multiple Fault Dependability and Security Evaluations," *14th Euromicro Conference on* Di*gital System Design*, pp. 550-557, 2011.

[11] H. Guzman-Miranda, M. A. Aguirre, and J. Tombs, "Noninvasive Fault Classification, Robustness and Recovery Time Measurement in Microprocessor-Type Architectures Subjected to Radiation-Induced Errors," *IEEE Transactions on Instrumentation and Measurement,* vol. no. 58, pp. 1514-1524, 2009.

[12] A. Mohammadi, M. Ebrahimi, A. Ejlali, and S. G. Miremadi, "SCFIT: A FPGA-based fault injection technique for SEU fault model," *Design, Automation & Test in Europe Conference & Exhibition*, pp. 586-589, 2012.

[13] J. M. Daveau, A. Blampey, G. Gasiot, J. Bulone, and P. Roche, "An industrial fault injection platform for soft-error dependability analysis and hardening of complex system-on-a-chip," *IEEE International Reliability Physics Symposium,* pp. 212-220, 2009.

[14] S. Kundu, S. Chattopadhyay, I. Sengupta and R. Kapur,"Multiple Fault Diagnosis Based on Multiple Fault Simulation Using Particle Swarm Optimization," 14th International Conference on VLSI Design, pp. 364-369, 2011.

[15] M. R. Guthaus, J. S. Ringenberg, D. Ernst, T. M. Austin, T. Mudge, and R. B. Brown, "MiBench: A free, commercially representative embedded benchmark suite," *Workload Characterization*, pp. 3-14, 2001.

[16] Modelsim Site, www.model.com.

[17] M. Juan Antonio and R. Pedro, "Study of the effects of MBUs on the reliability of a 150 nm SRAM device," *45th annual Design Automation Conference*, 2008.

[18] D. Radaelli, H. Puchner, S. Wong, and S. Daniel, "Investigation of multi-bit upsets in a 150 nm technology SRAM device," *IEEE Transactions on Nuclear Science,* vol. no. 52, pp. 2433-2437, 2005.