ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

INTENSIFYING REDUNDANT TECHNIQUE FOR EXTENUATION OF SINGLE EVENT UPSET SENSITIVITY

I.Ilayaranimangammal[1], R.Sornalatha[2]

PG Scholar [VLSI Design], Dept. of ECE, Shanmuganathan Engineering College, Pudukkottai, Tamilnadu, India [1]

Assistant Professor, Dept. of ECE, Shanmuganathan Engineering College,Pudukkottai,Tamilnadu, India [2]

ABSTRACT: To detect and correct the errors in the Flow diagram of all digital systems using RAPTOR.By analysing the characteristics of PAD and structured flowchart, and a structure identification and coding algorithm are put forward for structured flow diagram and PAD. Finally a integrated development platform is developed using such algorithms, including flowchart modelling, code automatic generation Fault tolerance technique using TMR for exposure and expulsion the soft errors in the digital systems. Faults are detected and eliminated without interrupting the normal functioning of the circuit. Single point of failure, is eliminated and implemented as a fault tolerant using a Triple Modular Redundancy (TMR). Conventional lockstep scheme uses duplication with comparison (DWC), the presence of fault is detected, but it fails to indicate the location of fault which is overcome in enriched lockstep by triple modular redundancy (TMR). TMR technique incorporates both transient and permanent faults. The new intensifying lockstep scheme requires significantly shorter recovery time than conventional lock step. It uses significantly less number of slices.

Keywords*:* Structured Flow chart, Fault tolerance, Single-Event Upset (SEU), Triple Modular Redundancy (TMR),problem analysis diagram, integrated development platform.

I.INTRODUCTION

Flow chart describes the control logic of a program by top-down process. For PAD (problem analysis diagram),it has the capability of top-down and left-right. So we can say if flowchart is a one-dimension chart, then PAD is a two-dimensional chart[1]. The basic idea of redundancy is to implemented multiple copies of the same circuit, and compare the outputs of each circuits. Disparity in these outputs indicates the occurrence of an error. Redundancy technique can be implemented at various levels such as circuits, systems etc. This process of switching is a simple process when both the designs meet the system restrictions identically [2]. Logic paths in between the flip-flops are composed of hard-wired, non-reconfigurable gates. Hence they are immune to SEUs. A fully fault tolerant system has the ability to detect and then corrects the hardware occurrence and return the system to its normal functionality.

An optimal design will minimize the amount of extra logic required to detect and then correct the occurrence of the fault An extreme temperature change is one of the reasons in which fault tolerance is necessary for devices operating in harsh operating environments, as found, for example, in space and military applications[13][6]. Faults are separated into two categories: Permanent and Transient [8]. Permanent faults that exist in logic circuits are normally identified during offline testing by the manufacturer of the IC, so the transient fault is of major concern after a chip is in the hands of the consumer. The ability to simulate the occurrence of a transient fault in the VHDL description of a system is extremely important to verify the performance of an on-line testable system.

In this paper section II focus on single-event upsets (SEU) and types of upsets. Then SEU mitigation techniques were discussed. In section III proposed method IV, the experimental & results are discussed V. Finally, the paper was concluded in section

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

II SINGLE EVENT UPSET MITIGATION TECHNIQUES

It is a process of applying design techniques to strengthen the functional integrity of the circuit, and protect it from the effect of any Single Event Upset. Fault-tolerant methods [6], [8] used to mitigate logic errors in FPGA based on redundancy technique are as follows. **RAPTOR** for detect & correct the error in the flow diagram of digital systems. **Duplication with Comparison (DWC)** for detecting faults and **Triple Modular Redundancy (TMR)** with majority voter for masking fault.

❖ RAPTOR Tool using DWC Technique for testing the Flow Chart

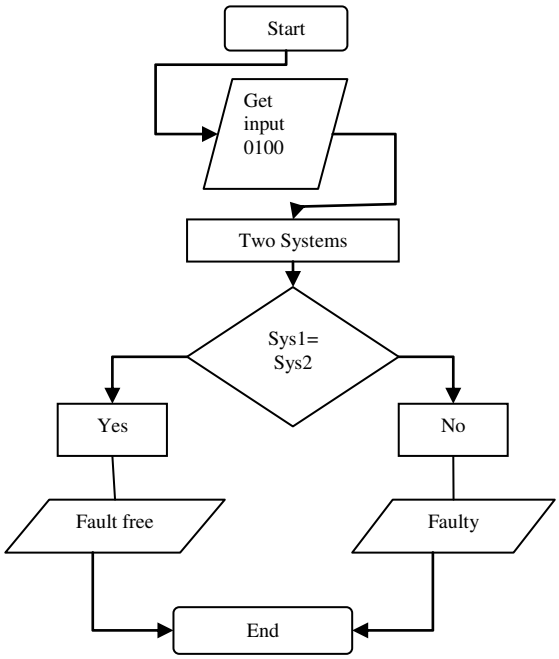
RAPTOR Tool is used to verify the DWCflow chart, each symbols are checked whether its suitable or not thenThis tool is used to all the digital circuits. This step is very important in testing field. its beginning step of testing. To detect and correct the errors in the Flow diagram of all digital systems using RAPTOR. By analyzing the characteristics of PAD and structured flowchart, and a structure identification and coding algorithm are put forward for structured flow diagram and PAD. Finally a integrated development platform is developed using such algorithms, including flowchart modeling, code automatic generation

ALGORITHM

****The following steps are first step in testing****

- Start the system design.
- Give input to the circuits (Both the circuits are accept same input value).
- Check both the circuit outputs; if output is mismatching its Faulty else fault free.
- This Flow Diagram is draw by RAPTOR Tool.
- Simulate the flow chart & evaluate each symbol.
- Run the flow chart.

FLOW CHART-DWC



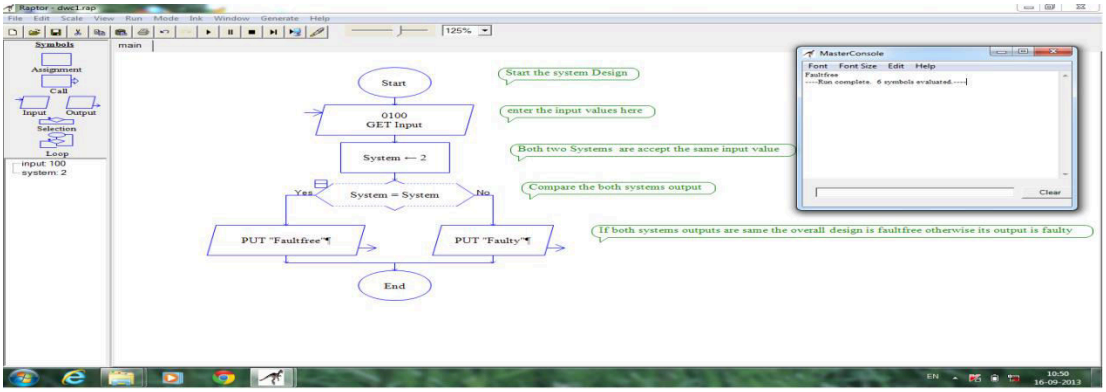
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

✓ **Result of Duplication with Comparison Flow Chart**



Design the system for Duplication with Comparison

Duplication with Comparison (DWC) is a detecting technique, in which the circuit to be protected is replicated twice and the results produced by the original circuit and the outputs of replicated circuits are compared to detect faults is given in figure 1. The implementation of DWC at processor level, supported by Xilinx ISE.

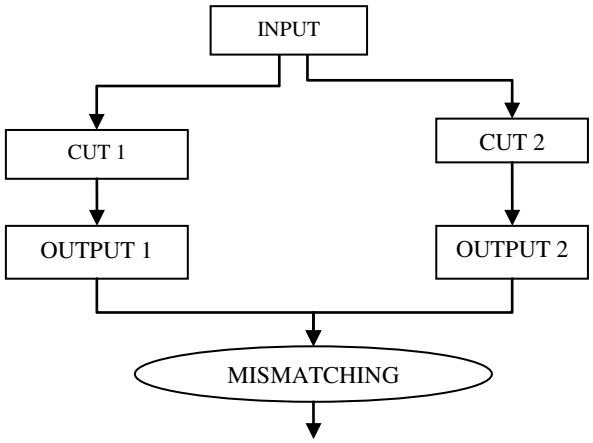


Figure 1 Duplication with Comparison (DWC)

Two identical circuits CUT1 and CUT2 receive the same inputs and simultaneously execute the same instructions, their results are compared step by- step at each clock cycle. Circuit CUT2 generates the reference results to be compared against those of CUT1 that provides the system output. Basically, DWC is able to detect but not to correct errors and also fails to indicate the fault location, since it cannot point out the faulty circuit. However, it could be capable to tolerate temporary faults, provided that it is supported by some re-execution procedure. In case of FPGA implementation, the system needs also to be reconfigured to recover correct functionalities.

III TRIPLE MODULAR REDUNDANCY TECHNIQUE

Triple Modular Redundancy (TMR) is the most reliable safeguard for total device failure as it rapidly detects and corrects SEUs.Three copies of the same circuit are connected to a "majority voter" which is used to obtain the fault free output.It operates withthe main aim of removing all single points of failure from the circuit. Each set of the triplicated circuit has its own set of inputs, to avoid errors occurring due to propagation of wrong inputs.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

❖ **RAPTOR Tool using TMR Technique for testing the Flow Chart**

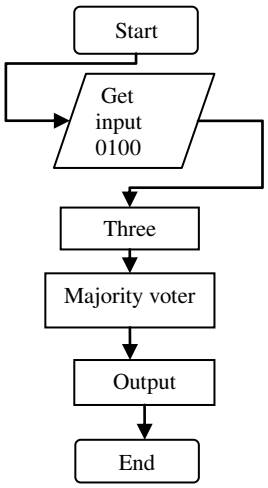
RAPTOR Tool is used to verify the TMR flow chart, each symbols are checked whether its suitable or not thenThis tool is used to all the digital circuits. This step is very important in testing field. its beginning step of testing. To detect and correct the errors in the Flow diagram of all digital systems using RAPTOR. By analyzing the characteristics of PAD and structured flowchart, and a structure identification and coding algorithm are put forward for structured flow diagram and PAD. Finally a integrated development platform is developed using such algorithms, including flowchart modeling, code automatic generation.

ALGORITHM -TMR

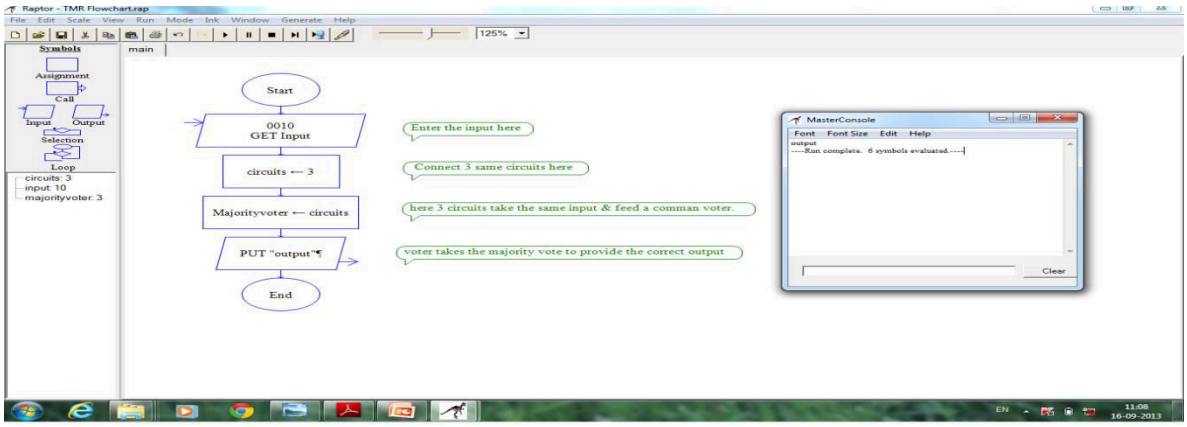
****The following steps are first process in testing****

- Start the system design.
- Give input to the circuits (All three circuits are accept same input value and feed a common voter).
- The Voter takes a majority vote to provide the correct output.
- This Flow Diagram is draw by RAPTOR Tool.
- Simulate the flow chart & evaluate each symbol.
- Run the flow chart

FLOW CHART-TMR



✓ **Result of Triple Modular Redundant Technique Flow Chart**



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

❖ **Design the System for Triple Modular Redundancy Technique**

Triple Modular Redundancy (TMR) is the most reliable safeguard for total device failure as it rapidly detects and corrects SEUs[10], [11], [12].Three copies of the same circuit are connected to a "majority voter" which is used to obtain the fault free output is shown in figure 2. This method works as long as all the faults are confined to one of the redundant blocks. The latency will be increased because of the voter in the circuit's critical path.

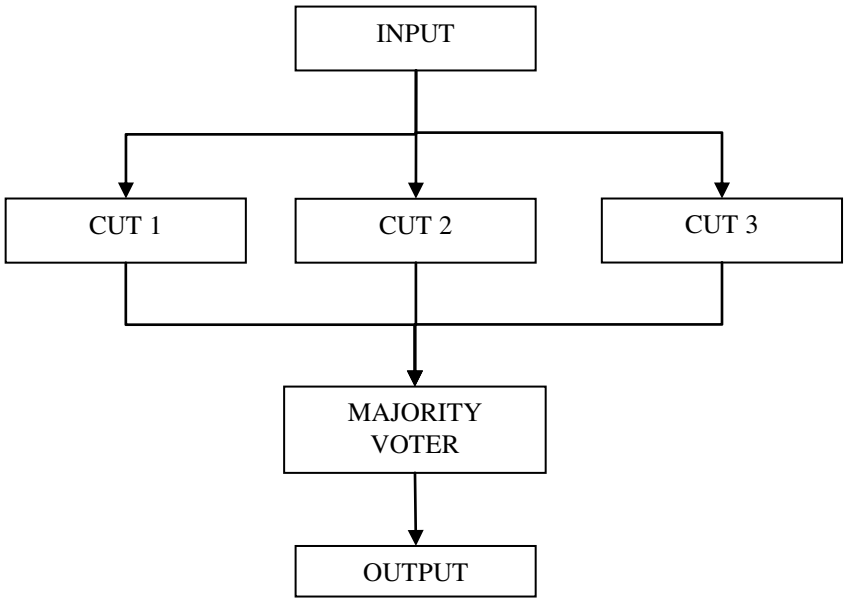


Fig 2 Triple Modular Redundancy (TMR)

TMR has a capability to protect both sequential and combinational circuits. A more efficient implementation of the TMR is focused in the sensitive logic, for example the memory cells to be protecting again SEU . It operates withthe main aim of removing all single points of failure from the circuit. Each set of the triplicated circuit has its own set of inputs, to avoid errors occurring due to propagation of wrong inputs.

The block diagram of the TMR adder circuit

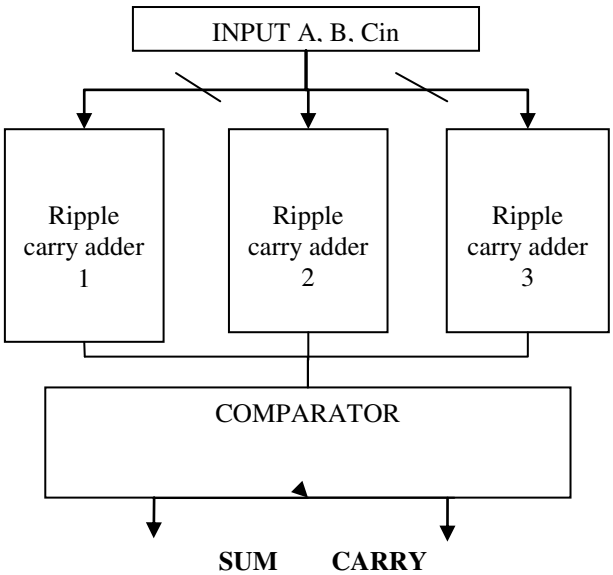


Figure 3 TMR adder circuit using ripple carry

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

The triple modular redundant ripple carry adder (TMR-RCA) is used as the reference circuit. This adder is the simplest approach for both detecting and correcting faults. using the ripple carry adders is shown in Figure 3. The technique involved in information redundancy includes the use of error-correcting codes. Fault occur in any one of the adder is compared with the fault-free adders, in order to indicate the faulty one.
TMR has a capability to protect both sequential and combinational circuits. A more efficient implementation of the TMR is focused in the sensitive logic, for example the memory cells to be protecting again SEU is shown in figure 4. It operates with the main aim of removing all single points of failure from the circuit. Each set of the triplicated circuit has its own set of inputs, to avoid errors occurring due to propagation of wrong inputs.

Enhanced Lockstep Architecture

The basic lockstep scheme [7] uses the realization of DWC at the processor level. Unfortunately, it can only detect errors without indicating the faulty module. In order to alleviate this limitation, the new Enhanced Lockstep scheme is shown in Figure 3, which provided with the mean to identify the faulty circuit. It allows continuing the execution with the remaining fault-free circuit.
This technique involves with the operation of two identical circuits with synchronized clocking. A mismatching between the output values of the circuit indicates the occurrence of SEU. Recovery actions such as reinitializing and switching to safe mode are implemented. Figure 7 shows the architecture of the fault-tolerant system, whose two main blocks are Enhanced Lockstep scheme and the fault-tolerant (FT) Configuration Engine. Error Correcting Code (ECC) is used for detection and identification of single and double-bit errors in the given data.
The reset input may be tied to logic 0 for free-running SEU detection and correction in the circuit that do not require access to the configuration memory during normal operation.[12] Two identical circuits CUT1and CUT2 and are the most essential part of the Enhanced Lockstep scheme. Their outputs are identical during fault-free functioning, any mismatching indicating error(s). If there is an error indication, the output signals of the PLB bus and the peripheral outputs are compared by the Comparator/Multiplexer (COMP MUX). If there is a mismatching occurs between any of the two circuits, a signal will be generated. When an error is detected between the circuits, since all the resources of two circuits are blended together it, there is no possibility of differentiating the faulty circuit.

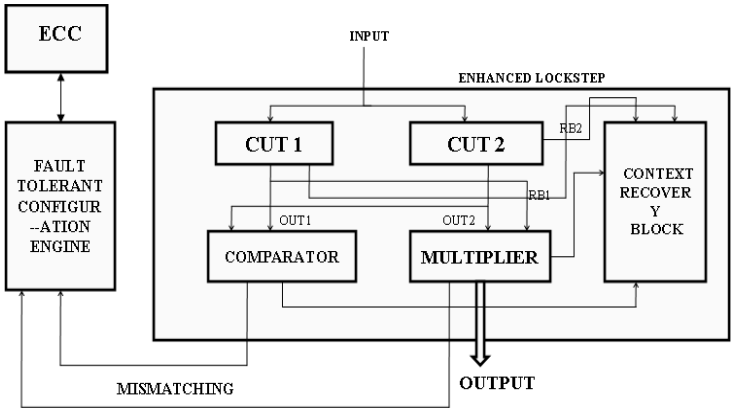


Fig 4 Enhanced Lock Step Scheme

In order to distinguish the faulty circuit, two blocks are used are the Comparator (COMP) and Multiplier (MUX). COMP that indicates any mismatch between the outputs Out1 and Out2 of CUT1 and CUT2 (containing the PLB and final output signals). [14] And the MUX, which connects one of the circuit to the system output, so that if one of them is reported to be faulty, the other is switched on. The switching is an atomic operation executed in one clock cycle. Once the error is localized by the FT Configuration Engine the affected processor is reconfigured to eliminate its configuration upset. Synchronization process is used for the newly reconfigured one to the same state as the correct one, thus enabling them to continue executingthe same task in lockstep again. The recovery process of the Enhanced Lockstep scheme is handled by the Context Recovery Block (CRB).

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

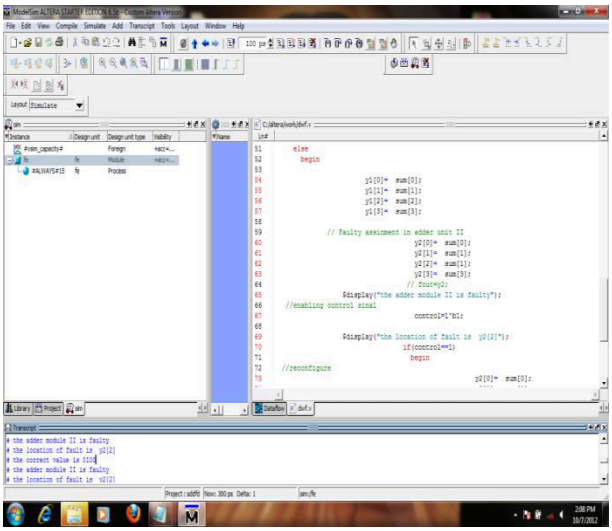
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

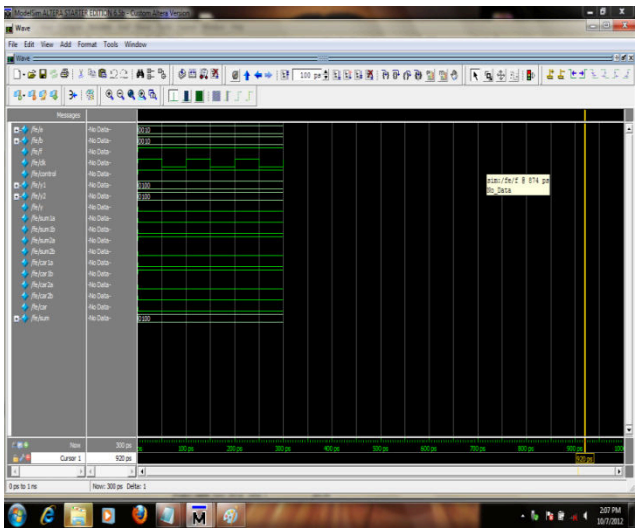
(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

IV RESULTS& IMPLEMENTATION

✓ **Ripple Carry Adder verilog codingOutput Waveform**





✓ **Table 1 Enhanced lockstep scheme**

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	17	960	1%
Number of 4 input LUTs	31	1920	1%
Number of bonded IOBs	50	66	75%
Number of GCLKs	1	24	4%

The performance analysis of enhanced lockstep scheme technique based on time, area, numbers of slices used are given in the tables. Table 1 shows the device utilization and the simulation time s 15.925.

V CONCLUSION

Conventional lockstep scheme uses duplication with comparison (DWC), the presence of fault is detected, but it fails to indicate the location of fault which is overcome in enriched lockstep by triple modular redundancy (TMR).Enhanced lockstep scheme uses triple modular redundancy (TMR) as a fault tolerant to detect and eliminate transient faults. It reduces both area and time consumption considerably. The errors can be reduced, performing the previous technological considerations, to sets of bits which are candidate to flip at the same time. The performance and efficiency of the circuit can be improved and the simulation time is reduced.

REFERENCES

[1] Y. Futamura, T. Kawai, H. Horikoshi etal. Developmentof computer programs by problem analysis Diagram(PAD). International Conference on SoftwareEngineering archive Proceedings of the 5th international conference on Software engineering. San Diego,California, United States, 1981: 325-332

[2] M. Lanuzza., "An efficient and low-cost design methodology to improve SRAM-based FPGA robustness in space and avionics applications," *Proc. Int. Workshop on Reconfigurable Computing: Architectures, Tools and Applications, Lect. Notes on Comput. Sci.*, vol. 5453, pp. 74–84, 2009.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2013

[3] H. Quinn, K. Morgan, P. Graham, J. Krone, M. Caffrey, and K. Lundgreen,"Domain crossing errors: Limitations on single device triple modular redundancy circuits in Xilinx FPGAs," *IEEE Trans. Nucl. Sci.*, vol. 54, no. 6, pp. 2037–43, Dec. 2007.
[4] L. Sterpone, M. Violante, R. H. Sorensen, D. Merodio, F. Sturesson,R. Weigand, and S. Mattsson, "Experimental validation of a tool for predicting the effects of soft errors in SRAM-based FPGAs," *Trans.Nucl. Sci.*, vol. 54, no. 6, pp. 2576–2583, Dec. 2007.
[5] P. Bernardi, L. Bolzani, M. Rebaudengo, M. S. Reorda, F. Vargas, and M. Violante, "Hybrid fault detection techniques in systems-on-a-chip," *IEEE Trans. Computers*, vol. 55, no. 2, pp. 185–198, Feb. 2006.
[6] M. Pignol, "DMT and DT2: Two fault-tolerant architectures developed by CNES for COTS-based spacecraft supercomputers," in *Proc. IEEE Int. On-Line Testing Symposium 2006*, 2006, pp. 10–12.
[7] PPC405 Lockstep system on ML310 Xilinx App. Note, XAPP564
[8] S. Rezgui, G. Swift, K. Somervill, J. George, C. Carmichael, and G. Allen, "Complex upset mitigation applied to a re-configurable embedded processor," *IEEE Trans. Nucl. Sci.*, vol. 52, no. 6, pp. 2468–2474, Dec. 2005.
[9] B. Pratt, M. Caffrey, P. Graham, E. Johnson, K. Morgan, and M.Wirthlin, "Improving FPGA design robustness with partial TMR,"presented at the IRPS Conf., Mar. 2006.
[10] N. Rollins, M. Wirthlin, M. Caffrey, and P. Graham, "Evaluating TMR techniques in the presence of single event upsets," in *Proc. 6th Annu. Int. Conf. Military and Aerospace Programmable Logic Devices (MAPLD)*, NASA Office of Logic Design, AIAA, Washington, D.C., Sep. 2003, p. P63
.[11] C. Carmichael, "Triple module redundancy design techniques for Virtex FPGAs," Xilinx Corp., Tech. Rep. XAPP197 (vl.O), Nov. 1, 2001.
[12] J. Arlat *et al.*, "Fault injection for dependability validation: A methodologyand some applications," *IEEE Trans. Softw. Eng.*, vol. 16, no. 2, pp. 166–182, Feb. 1990.
[13] P. K. Samudrala, J. Ramos, and S. Katkoori, "Selective triple modular redundancy for SEU mitigation in FPGAs," in *Proc. 6th Annu. Int. Conf. Military and Aerospace Programmable Logic Devices (MAPLD)*, NASA Office.
[14] D. Bhaduri and S. Shukla, "NANOLAB—A tool for evaluating reliability of defect-tolerant nanoarchitectures," *IEEE Trans. Nanotechnol.*, vol. 4, pp. 381–394, 2005
[15] X. Liu, Q. Wang, S. Gopalakrishnan, W. He, L. Sha, H. Ding, and K. Lee, "ORTEGA: An efficient and flexible online fault tolerance architecture for real-time control systems," *IEEE Trans. Ind. Informat.*, vol. 55, no. 4, pp. 213–224, Oct. 2008.
[16] Haissam Ziade, Rafic Ayoubi and Raoul Velazco, "A Survey on Fault Injection Techniques" *The International Arab Journal of Information Technology, Vol. 1, No. 2, July 2004*

BIOGRAPHY

I.ILAYARANIMANGAMMAL received her B.E degree in Engineering from Sethu Institute of Technology, Kariyapatti, Virudhunagar Dist, and Tamil Nadu in 2010. Currently she is pursuing her M.E (VLSI Design) in Shanmuganathan Engineering College, Thirumayam, Pudukkottai Dist, Tamil Nadu. She has presented more than 5 papers in the National & International Conferences. She got Best Paper award for international conference in the field of power system. Her research interest is design for fault tolerance, design verification, area and power reduction then web application related programming development, and web publishing in .NET domain.

Mrs.R.SORNALATHA received her B.E. Instrumentation & Control Engineering from Arulmigu Kalasalingam College of Engineering and ME (VLSI Design) from Kings College of Engineering, Thanjavur (Dt). She is presently working as an Assistant Professor in the department of Electronics and Communication Engineering in Shanmuganathan Engineering College, Pudukkottai Dist, Tamilnadu. She has presented more papers in the National & International Conferences. Her research interest in medical image processing, VLSI design &Testing Domain.