Triple Modular Redundancy using Fault Tolerant Technique– Review

Pratiksha P Kolte[1], Rashmi Maheshwari[2],Shubham Ajankar[3]
Lecturer, Assistant professor,Student[1]Department of Electronics, Shree L.R.Tiwari College of Engineering Miraroad,Thane,India
[2]Department of Electronics, Shree L.R.Tiwari College of Engineering Miraroad,Thane,India
[3]Department of Electronic and Telecommunication, MIT ,Pune,India

***Abstract* :** Redundancy is a technique to improve the reliability and availability of a system. Triple Modular Redundancy (TMR) uses three functionally equivalent units to provide redundant backup. Fault Tolerance is a high performance system and they have ability of system to continue error-free operation in presence of unexpected fault. TMR defend the FPGA circuit by creating three copies of a circuit and choosing the output based on a majority vote between the three. For making a fault tolerant system Triple Modular Redundancy (TMR) is used. Triple Modular Redundancy (TMR) is commonly used in dependable systems design to ensure high reliability against soft errors. This review paper focuses on the use of TMR for different FPGA based applications.

Keywords:*FPGA, single event upsets (SEUs), SRAM, Single Event Transients (SETs), Triple Modular Redundancy (TMR).*

*****

1. INTRODUCTION

Redundancy is a common approach to improve the reliability and ease of use of a system. The system will be expensive while Adding redundancy and complexity of a system increases with the high reliability of modern electrical and mechanical components, many applications do not need redundancy in order to be successful. However, redundancy may be an attractive option but in case of failure it is very expensive.

On the way to clarify Triple Modular Redundancy, it is necessary to elaborate the idea of triple redundancy. Triple modular redundancy (TMR) is a technique commonly used to provide design hardening. It is used to protect sequential circuits, or storage elements. Conventional TMR technique has been proved effective in protecting sequential circuits [1].

Fault Tolerance is a high performance system and they have ability of system to continue error-free operation in presence of unexpected fault. The system must not suddenly fail but continue executing part of its workload. A fault occurs within some hardware or software component. A fault is due to radiation effect, external disturbance, wearout failures. A fault might not always results in an error, but the same fault may outcome in numerous errors. Similarly a single error may arise a numerous failures.

Triple Modular Redundancy (TMR)is the most widely adopted one for hardening circuits implemented on SRAM-based FPGAs. Triple Modular Redundancy (TMR) is used for making a fault tolerant system and it can be applied based on different granularities, such as device redundancy, system redundancy, module redundancy or logic element redundancy. The Triple Modular Redundancy (TMR) technology allows protection of the functionality of FPGAs against single event upsets (SEUs). Field-programmable gate arrays (FPGAs) gives high-performance for digital signal processing and real-time communication systems. Triple Modular Redundancy (TMR) is the most popular SEU mitigation technique for FPGAs. TMR safeguards the FPGA circuit by creating three copies of a circuit and choosing the output based on a majority vote between the three. TMR also masks the effects of SEUs as well as the less critical transient and soft data errors. While TMR is very effective at protecting FPGA circuits from soft errors, it is expensive in terms of the circuit area, power, and circuit timing. FPGAs are progressively more used in space for reconfigurable radios and other high-performance computing tasks.

The use of TMR with FPGA based application is discussed in the next sections.

2. SECTIONS

Triple modular redundancy (TMR)is the most widely adopted one for hardening circuits implemented on SRAM-based FPGAs. For digital circuits mapped on FPGAs, the flip-flops (FFs) to form the feedback path of sequential circuits, and the logic gates in combinational and sequential circuits are need to be hardened. For this the reason is that the logic gates are mapped on the FPGA using look up tables (LUTs), which consist of SRAM cells. Even the interconnection is also controlled using the data stored in SRAM cells. In the system level TMR system, the original system is reapeated three times and obtain the output from a majority voter. Each replica of the system works independently and is named domain. If an SEU occurs in

one domain, TMR masks the fault by majority voting and thus propagates the correct output [2].

Triple Modular Redundancy is widely used in dependable systems design to ensure high reliability against soft errors. Conventional TMR is effective in protecting sequential circuits but can't recover soft errors in combinational circuits. A new redundancy technique called the Space-Time Triple Modular Redundancy is discussed in this paper, which improves the soft error tolerance of the combinational circuit. Triple modular redundancy (TMR) is a technique commonly used to provide error free circuit. It is used to protect sequential circuits, or storage elements. Conventional TMR technique has been proved effective in protecting sequential circuits [3].

TMR in FPGAs a Space application must consider the effect energetic particles (radiation) can have on electronic components.SEUs may modify the logic-state of any static memory element (latch, flip flop, or RAM cell) or cause transient pulses in combinatorial logic paths. Since the user-programmed functionality of an FPGA depends on the data stored in millions of configuration latches within the device, an SEU in the configuration memory array might have adverse effects on the expected functionality of the user implemented design. Similarly, Single Event Transients (SETs) have a high probability for recognition at flip flop inputs where, if registered, causes a soft-error in the user data. Static upsets in the configuration memory are not necessarily synonymous with a functional error; however, soft-errors are by definition a functional error. Upsets might or might not have an effect on functionality. However, an gathering of upsets in the configuration memory is eventually certain to lead to a functional failure. Design mitigation techniques, such as triple module redundancy, can harden functionality against SEUs and SETs, while the SEUs are corrected so that static-errors do not accumulate and soft-errors do not propagate. Implementing triple redundant circuits in other technologies, such as ASICs, is traditionally limited to protecting only the flip flops of the user's design from SEU, because logic paths in linking the flop-flops are typically hard-wired, non-reconfigurable gates. For such fixed logic technologies, this is sufficient protection from SEUs, but can still leave the circuitry vulnerable to SETs. For a technology that is vulnerable to SETs, further protection can be achieved through full module redundancy. Full module redundancy is the required implementation of TMR in FPGAs, because all the logic paths, not just the flip flops, are susceptible to SEUs. This means that three full copies of the base design will be implemented to protect circuit functionality from SEUs, as well as SETs. However, the method for constructing TMR circuitry for Virtex FPGAs provides the additional advantages of complete data retention and independent recovery. The correct implementation of TMR circuitry within the Virtex architecture depends on the type of data structure to be mitigated. These data structures can have categorize into four different types like throughput logic, state-machine logic, I/O logic, and special features [4].

Field-programmable gate arrays (FPGAs) are an attractive target for high-performance digital signal processing and real-time communication systems. FPGAs have been used to implement communication-specific processors for well over a decade. Their ability to combine flexibility with good performance makes FPGAs popular for software-defined radios. Reconfigurable radios are also becoming more attractive for space-based applications. The ability to reconfigure the FPGA resources with an updated radio configuration reduces the amount of hardware needed on the spacecraft. FPGAs are increasingly used in space for reconfigurable radios and other high-performance computing tasks.

The problem with using the popular SRAM- (static-random-access-memory-) based FPGAs in space is the presence of high-energy particles that may alter the operation of the digital circuitry or the state of static memory cells. These errors, called soft errors, do not cause any physical damage to the device but interact with state of memories or other digital circuits. For example, charged particles can occasionally invert the contents of a memory cell. Such an event is called a "single event upset" (SEU).

Because most of the FPGA area is devoted to static memory cells to store the FPGA configuration memory, FPGAs are very sensitive to radiation. Any FPGA design operating in space must consider the effects of high-energy radiation and implement some form of SEU mitigation. Triple modular redundancy (TMR) is the most popular SEU mitigation technique for FPGAs. TMR protects the FPGA circuit by creating three copies of a circuit and choosing the output based on a majority vote between the three. TMR masks the effects of SEUs as well as the less critical transient and soft data errors. Although TMR is very effective at protecting FPGA circuits from soft errors, it is costly in terms of the circuit area, power, and circuit timing [5].

Hung-Manh Pham et. al. propose a new approach to implement a reliable softcore processor on SRAM-based FPGAs, which can mitigate radiation-induced temporary faults (single-event upsets (SEUs)) at moderate cost. A new Enhanced Lockstep scheme built using a pair of MicroBlaze cores is proposed and implemented on Xilinx Virtex-5 FPGA [6].

Conclusion

This paper provides the review on the fault-tolerant and repairing technique using Triple modular redundancy (TMR). This Literature survey gives many concepts in both TMR design and FPGA selection. Traditional solutions for radiation effects were introduced including hardware redundancy and software improvement for fault tolerance, like time redundancy or software redundancy.

REFERENCES

[1] http://www.ni.com/white-paper/6874/en/,NI-Tutorial-6874-en.pdf

[2] Y. Rui, C. Qinqin, L. Zengwu, S. Yanmei, "Multi-objective evolutionary design of selective triple modular redundancy systems against SEUs," Chinese Journal of Aeronautics 28,(2015)

[3] C. CARMICHAEL, "Triple Module Redundancy Design Techniques for the Virtex TM Series," Xilinx Application Note xapp197, 2001.

[4] http://www.xilinx.com/support/documentation/application_notes/xapp197.pdf

[5] Brian Pratt, Megan Fuller, and Michael Wirthlin, "Reduced-Precision Redundancy on FPGAs" International Journal of Reconfigurable Computing, Volume 2011 (2011),

[6] Hung-Manh Pham, Se´ bastien Pillement, and Stanisław J. Piestrak, "Low-overhead fault-tolerance Technique for a Dynamically Reconfigurable Softcore Processor" Transactions on Computers, VOL. 62, NO. 6, JUNE 2013