Talha Ansari

CprE 583

Fall 2011

Soft Error Susceptibility in SRAM-Based FPGAs

With the increasing emphasis on minimizing mass and volume along with cost in aerospace equipment, the use of FPGAs has slowly but gradually increased over the last decade. With the SRAM-based FPGAs offering more flexibility for designers, it has quickly become one of the most common source of FPGA in the industry. However, with the selection of this type of a device, engineers have also had to integrate techniques to account for soft errors caused by the harsh environments, thirty to sixty thousand miles in the air. These environments are filled with ionized neutrons and protons that can generate soft errors in the system. There are many things that can cause a soft error, from signal noise to electromagnetic interface to alpha particles to cosmic rays creating energetic neutrons and protons. Since majority of the space in the FPGA is used as memory bits, Single Event Upsets (SEU) and Single Event Transients (SET) are more common in these devices. Also, since configuration memory in these devices is composed of static RAM cells these are more susceptible to soft errors as composed to flash based FPGAs. These errors if not detected or accounted for can cause erroneous data into the system leading to catastrophic outcomes. These devices when compared to

Application Specific Integrated Circuits (ASICs) are more susceptible to such soft errors, as majority of the FPGA is allocated to memory bits.

This paper focuses on SEU and SET errors referred henceforth as soft errors. Mitigation techniques for both will be discussed which include both analytical and real on chip solutions. Mitigation against SEU and SET can be handled at two levels, by manufacturer of the FPGA through built-in circuit techniques and by end-user through design and system techniques. Along side mitigation, detection mechanisms will also be briefly discussed for each type of soft error.

Single Event Upsets

Single event upset is a state change for a memory buffer, whether it is in a processor, a memory component of an FPGA. It is mainly caused by an ion striking the transistor and causing it to change its state. Therefore a transistor might change its state from bit 1 to bit 0, hence making the data stored in that part of the memory invalid. To address SEUs in FPGAs, it is important to handle two parts of the FPGA, the user memory and the configuration memory areas [2]. The users memory area contains information such as registers, gate information, memory arrays etc. On the contrary information in the configuration memory part of the FPGA consists of information as to which part of the FPGA implements what functions. One of the most common mechanisms for handling SEUs in FPGAs is the Triple Modular Redundancy.

Triple modular redundancy (TMR) scheme is a very creative way to harden the FPGA against SEU. The basic idea for a TMR is that three copies of the same design are copied on the FPGA along with a majority voter [1]. It is important to note that this approach is only valid for single faults. For multiple faults, this architecture might not hold true. For example if the same bit is flipped on two of the three copies of the design, then the fault can carry over. The probability of this happening however is very low. The majority voter can be either designed inside the FPGA or outside in a different circuit. When implemented inside the FPGA, this part of the circuit is also susceptible to SEU. Hence another more advanced approach is to triplicate the majority voter circuit as well [2]. Figure 1 and Figure 2 show the two different approaches of TMR with a high-level block diagram.

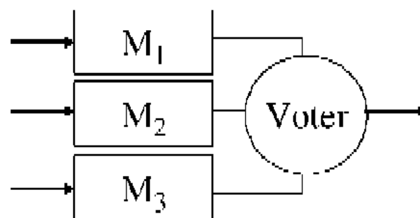

Figure 1. Basic TMR approach with code replication and single majority voter [1].

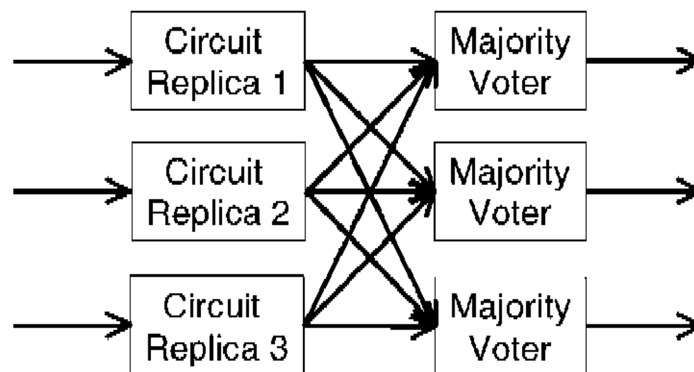

Figure 2. TMR approach where circuit and majority voter are hardened [2]

In the first figure, the design is triplicated with a single majority voter while the second figure shows the triplication of the design as well as the majority voter. Since TMR requires the design to be triplicated, more power and more footprint is utilized. Hence this impacts cost directly. In systems where cost and footprint are important, partial TMR can be implemented [3]. In partial TMR, instead of triplicating the whole design only a subset or the design is triplicated. This subset is quantified as being critical with the use of analysis and projection tools to provide a more reliable solution while minimizing cost as compared to a full TMR approach.

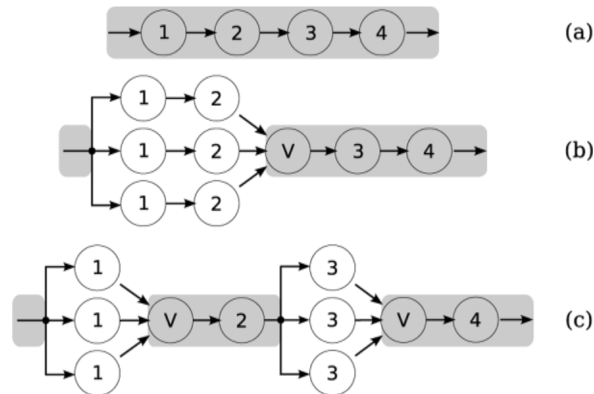

Figure 3. Partial TMR Approach. (a) No TMR applied, (b) & (c) partial TMR applied. Shaded area represents SEU sensitive areas [3].

As seen in the figure, multiple voters have to be placed after triplicating part of the circuit instead of a final voter as in the full TMR approach. This also adds more logic to the FPGA, which now becomes sensitive to SEUs therefore by concentrating on these triplicating sections more reliability gains can be achieved [3].

Single Event Transients

Contrary to SEU, Single Event Transients (SET) can also be caused through electromagnetic radiation or by a striking cosmic partible, but in this case the fault is propagated through a signal line. Generally when a particle strikes the FPGA node it produces a current pulse, which then becomes a voltage disturbance that propagates through the logic and eventually latches a fault [4]. Figure 4 shows a very general picture where SET propagates on the output of an AND gate.

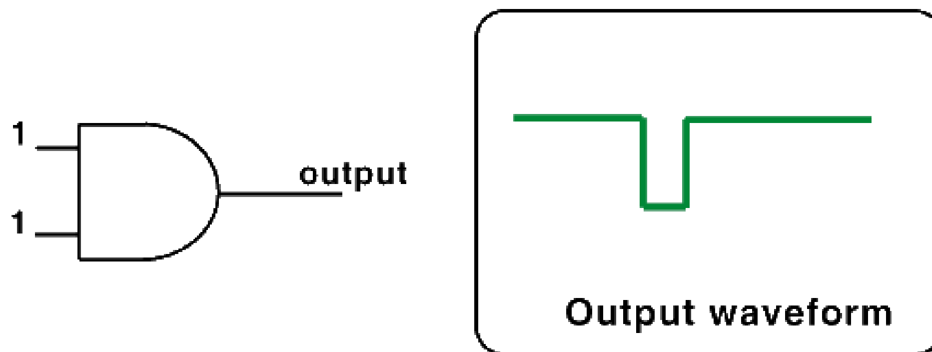

Figure 4. SET propagating through the AND gate output.

When handling SETs in FPGA, masking has to be considered. There are three types of masking effects that can prevent a transient pulse in combinational logic from propagating and being latched by a memory element; logic masking, latch window masking, and electrical masking [4]. Basically all these masking's are to protect and filter out these transients, as in electrical masking the transient goes through multiple gates until it is eventually nullified.

To add to the electrical masking part of the design, one approach suggested is the Voltage-Time Quantization (VTQ) where rising and falling edges of each

transition are sampled and rounded to points in the interval from 0 to 2^N -1, where N is the voltage resolution in bits [4]. This approach basically captures each transition and the counter counts up to a high voltage, and counts low to the low voltage. Then using synthesis delays at the electrical level are back annotated to the VTQ model for analysis. So if a SET transient occurs in the design, it can be captured by the counter implemented through the VTQ model. Experiments with such a model show promising results [4] on how the design handles SETs.

System Level Improvements to Handle SET & SEU

Apart from implementing approaches within the FPGA, end users can also implement detection schemes such as Error Detection and Correction (EDAC) or Error Checking Correction (ECC). These features not only detect, but can also correct single bit errors that may have occured due to an SET or an SEU. With these mechanism, the user can have the FPGA reload it self from an external EEPROM incase a fault is detected. These techniques are very common in the aerospace industry as a mechanism to counter both types of soft errors.

With systems used in mission critical and aerospace industries, it is important to detect soft errors caused by single event upsets and single event transients to prevent the system from displaying or computing erroneous data. With the flexibility and popularity of SRAM-based FPGAs, designers have to be aware of such faults and need to design systems that are more robust through techniques like TMR and VTQ.

Reference:

[1] L. Sterpone; M Violante, “Analysis of the Robustness of the TMR Architecture in SRAM-Based FPGAs”, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, Vol. 52, No. 5, October 2005.

[2] L. Sterpone; M Violante, “A New Analytical Approach to Estimate the Effects of SEUs in TMR Architectures Implemented Through SRAM-Based FPGAs”, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, Vol. 52, No. 6, December 2005.

[3] B. Pratt; M. Caffrey; J.F. Carroll; P. Graham; K. Morgan; M. Wirthlin, “ Fine-Grain SEU Mitigation for FPGAs Using Partial TMR”, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, Vol. 55, No. 4, August 2008.

[4] L. Entrena; M. Valderas; R. Cardenal; M. Garcia; Celia Ongil, “SET Emulation Considering Electrical Masking Effects”, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, Vol. 56, August 2009.

[5] S. Liu; G. Sorrenti; P. Reviriego; F. Casini; J. Antonio; M. Alderighi, “Increasing Reliability of FPGA-Based Adaptive Equalizers in the Presence of Single Event Upsets”, IEEE TRANSACTIONS ON NUCLEAR SCIENCE, Vol. 58, No. 3, June 2011.

[6] H. Asadi; M. Tahoori; B. Mullins; D. Kaeli; K. Granlund, “Soft Error Susceptibility Analysis of SRAM-Based FPGAs in High-Performance Information Systems”, IEEE TRANSACTION ON NUCLEAR SCIENCE, Vol. 54, No. 6, December 2007.