High-Performance SET Hardening Technique for Vision-Oriented Applications

High-Performance SET Hardening Technique for Vision-Oriented Applications

Corrado De Sio, Luca Sterpone
Dipartimento di Automatica e Informatica
Politecnico di Torino
Turin, Italy

***Abstract*— The decreasing feature size of VLSI circuits has led to a rise in Single Event Transients (SETs), making them the dominant cause of errors in modern VLSI devices, especially Flash-based FPGAs. The combinational logic in these devices is particularly vulnerable to SETs, making efficient SET hardening techniques essential. Given the demanding performance requirements for vision-oriented benchmarks, finding an efficient hardening technique that does not exceed area and performance limitations is challenging. This paper presents a SET hardening workflow based on an accurate SET analysis aimed at identifying vulnerable circuit nodes for selectively applying hardening techniques to Microchip RTG4 radiation-hardened Flash-based FPGAs. Results from experiments comparing plain, Global hardening, and proposed selective hardening techniques show the high efficiency of the proposed solution.**

Keywords—Single Event Transient, RTG-4 Flash-based FPGA.

I. Introduction

The aggressive scaling trend in nanometer technologies has significantly impacted the rates of Single Event Transient (SETs) faults within the electronic circuit [1]. When a highly charged particle crosses the silicon junction and releases its energy, it can create an undesired voltage pulse known as a Single Event Transient. The SET pulse can propagate through the logic and routing of the circuit while broadened or filtered. If the pulse reaches a memory element and is latched, it can cause a Single Event Upset (SEU), causing wrong functionality of the system [2].

Considering reprogrammable devices such as Flash-based FPGAs, transient error affecting the combinational logic is nowadays the main concern for safety-critical applications such as aerospace. Therefore, it is crucial to evaluate the SET generation, and propagation in routing and logic cells of the circuits implemented in Flash-based FPGAs to perform an accurate SET sensitivity analysis [3] and, consequently, adopt an efficient mitigation technique [4].

Several mitigation solutions have been adopted for logic, memory, and registers, such as Triple Modular Redundancy (TMR) and Error Correction Code (ECC) [5]. However, these techniques are not always able to mitigate SET effects. Therefore, techniques such as the insertion of filtering logic and charge sharing have been evaluated to protect the sampling of SET by memory elements [6]. Though, adopting these techniques brings area and performance overhead which is not always matched with the recent requirements of mission-critical applications. To cope with the increasing aerospace requirements, this industry has moved toward the development of radiation-hardened FPGAs, for example, the RTG4 family manufactured by Microchip [9]. The standout feature of this Flash-based FPGA technology is its tolerance against Total Ionizing Dose (TID), which exceeds 100 krad. In addition, the RTG4 family also boasts embedded SEU and SET mitigation strategies based on Triplicated Flip-Flop architecture and internal SET mitigation, making it even more resistant to transient radiation effects [10]. Even though the advantages provided by the RTG4 family are notable, the commercial design toolchain does not support fine-grained and selective hardening. To elaborate more, the current design tool allows the designer to insert the SET mitigation filtering logic globally to all the Flip-Flops (FFs) of the circuit with the same filtering capability, even though performing an accurate SET sensitivity analysis shows that not all the FFs are sensitive and not all of them have the same sensitivity level [12]. Therefore, adopting the same filtering capability for all the memory elements of the circuit significantly increases the area overhead and, more importantly, performance overhead which is a substantial limitation when selecting mitigation techniques. For example, even if the state-of-the-art vision-oriented algorithms demand high-performance computational capability, they are becoming popular in space applications, where radiation-induced errors are a primary concern [13]. Moreover, they require a high resource availability. Consequently, efficient mitigation techniques to be applied to vision-based circuits implemented on FPGAs should provide low resource and performance overhead.

This paper proposes a selective mitigation technique adopted not globally but selectively to sensitive circuit nodes implemented on radiation-hardened Flash-based FPGAs, particularly the RTG-4 family. The ZFNet Convolutional Neural Network (CNN) has been implemented on the FPGA to be adopted as a benchmark circuit [14].

We performed an accurate SET analysis on the plain version of a circuit implementing ZFNet, identifying the vulnerable circuit nodes and applying filtering logic to the selected sensitive nodes. Comparison among the reliability of the plain circuit, the circuit including global adoption of the filtering logic gate to all the memory elements, and our proposed selective circuit solution has been performed, which shows a negligible reduction in the reliability with respect to the global mitigation technique while the area and performance overhead reduced drastically.

The paper is organized as follows. Section II describes the related works, while Section III provides an overview of the RTG-4 Flash-based FPGA family. Section IV elaborates on the developed framework for analyzing and mitigating SET pulses, while Section V reports the experimental results. Finally, conclusions and future works are drawn in Section VI.

978-1-6654-6703-2/22/$31.00 ©2022 IEEE

II. Related Works

Many works have investigated Single Event Transient Effects in digital circuits. Among various approaches, several works have been dedicated to the SET effects on Flash-based FPGAs, focusing on the evaluation of SET propagation using electrical simulation [11], which is shown to be efficient for analyzing the propagation of SET pulse. However, they do not consider the SET pulse's broadening or filtering effect while traversing combinational logic and interconnection of implemented circuits. Moreover, these approaches are time-consuming and not applicable to an industrial design with huge amount of resources. Therefore, developing an accurate and fast Single Event analyzer is important to reach an efficient SET mitigation and hardening technique [7]. Different mitigation solutions have been proposed in the literature [6][5][8]. One traditional method is based on redundancy, such as Triple Modular Redundancy (TMR) which is typically available on commercial FPGA design flow. Moreover, considering the new radiation-hardened FPGA family, the RTG-4, a new mitigation technique is available through the commercial design, which is based on the insertion of filtering logic globally to all the FFs of the implemented circuits.

However, since methods based on replication or global filtering insertion introduced significant resource and performance overhead, we aim to overcome this problem by performing an accurate SET sensitivity analysis in order to apply hardening techniques, not globally but selectively, to the identified sensitive circuit nodes.

III. Background on the Radiation-Hardened Flash-based FPGAs

RTG-4 is a radiation-hardened flash-based field-programmable gate array (FPGA) designed to withstand the high levels of radiation found in space, making it suitable for use in satellites and other space-based applications. The RTG-4 is equipped with Error Correction Code (ECC) for Single Event Upsets (SEU) protection. It consists of a logic element array of 4-inputs Look-Up Tables (LUT-4) and separate Flip-Flop that can be used independently from the LUT-4.

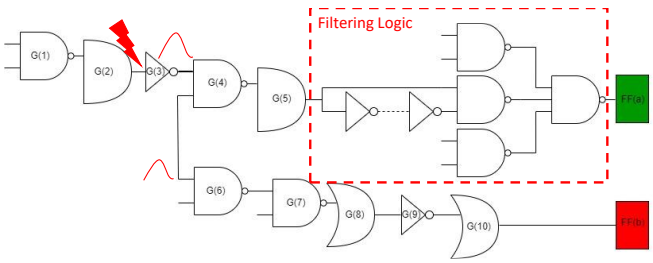

Fig. 1. SET Filtering Scheme inserted by the Commercial Tool

The main specific unique feature of the RTG4 logic cell is based on the SET-filtering self-correcting TMR-D Flip-Flop (S-TMR), which ensures SEU immunity, while SET pulses with a particular width at the input D of the functional logic block are filtered by user-defined SET filtering delay. Figure 1 represents the SET filtering logic preventing the propagated SET pulse from being captured by the storage element (FF_a). However, please note that the commercial design tool for RTG-4 allows the insertion of filtering logic globally to all or none of the Flip-Flops of the design. Moreover, the filtering delay is constant, decided by the designer, and cannot be tuned with respect to the particular sensitivity of each specific Flip-Flop. Therefore, for example, even though between two FF, one might not be vulnerable with respect to the other one, means it is expected to receive SET pulse with a smaller duration, therefore less probability to be captured by the storage element, both of them will include filtering logics with the same filtering capability.

For this reason, relying on global insertion of the filtering logic introduces significant disadvantages, especially considering that the insertion of filtering logic not only introduces area overhead but also delays that can drastically reduce the timing performances of the circuits. This is a significant limitation, especially with respect to the recent drastic usage of vision-oriented algorithms, which require high performance. Therefore, we propose a comprehensive SET analysis to first of all identify the sensitive FFs of the circuit and then insertion of selective filtering logic to the identified sensitive FF while the filtering capability is tuned with respect to each sensitivity of each individual FF.

IV. The SET Hardening Workflow

The developed Integrated Design Flow includes two phases: Firstly, a comprehensive SET analysis is performed, taking into account different SET creation and propagation scenarios in order to identify the sensitive nodes of the DUT. Secondly, a selective mitigation technique is performed by modifying the netlist and inserting a filtering logic to the identified sensitive circuit node while the filtering capability is tuned with respect to sensitivity level. The flow of the approach, which is integrated within the standard FPGA design flow, is represented in Figure 2.

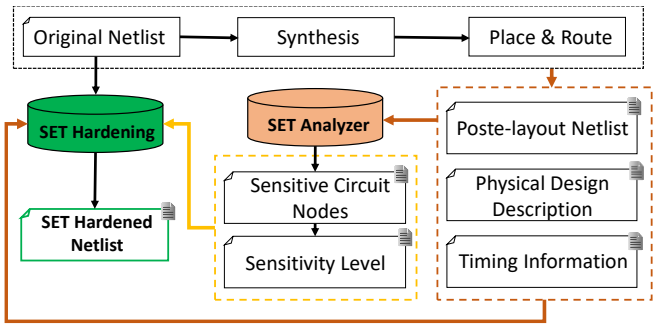

Fig. 2. The SET Hardening Workflow

A. Single Event Transient Analysis

The SET analyzing phase starts from the Hardware Description of the design, going through netlist synthesis, mapping, and place and route, generating the post-layout netlist along with the Physical Design Description (PDD) of the circuit and timing information. The SET analyzer starts by elaborating the post-layout netlist and PDD; it considers all the combinational logic as *intermediate nodes* connecting through routing segments, while I/O pins and sequential components are considered as *terminal nodes*. The SET analyzer performs SET analysis by inserting SET pulse in each input and output of the intermediate nodes, propagating the pulse until it reaches terminal nodes while considering the propagation-induced pulse broadening effects. At the end of the analysis, a list of FF facing propagated SET together with the characteristics of the pulse reached to the FF, such as amplitude and duration of the pulse, is reported. Itis exploited in the next phase for performing a selective SET filtering logic insertion. More details about the Single Event Transient Analyzing tool are provided at [15].

B. *Single Event Transient Hardening Technique*

The SET hardening technique modifies the original netlist by inserting the SET filtering logic structure. As represented in Figure 1, the filtering structure is composed of a 3-input NAND gate, three 2-input NAND gates, and parameterized number of inverters INVD gates determined by desired SET filtering capability. The SET hardening algorithm exploits the reports provided by the SET analyzer regarding the list of vulnerable FFs of the netlist as well as the maximum duration of the SET pulse expected to be received by each FF and then calculates the number of inverters required for filtering the SET pulse arriving at each individual FFs of the netlist. Later, the algorithm modifies the netlist, inserting the logic gates with the calculated filtering capability, and provides the SET-hardened netlist. This solution with respect to the global insertion of filtering logic approach offers two advantages: Firstly, the SET filtering logic is inserted not in all the FFs but only in the ones identified as sensitive ones. Secondly, the SET filtering capability is not constant for all the FFs, but it is tuned with respect to the sensitivity level of each FFs individually.

V. Experimental Results

The developed SET hardening workflow has been applied to a circuit implementing a ZFNet CNN architecture on RTG4G150 Radiation Tolerant Flash-based FPGAs manufactured by Microchip.

A. *The Benchmark Implementation*

As an application benchmark, we selected the ZFNet CNN adopting a 16-bit parallelism data size, five convolutional layers, and three fully connected layers. The input data stream consists of a 224 by 224 image convolved with 96 filters at the first layer. The feature map is then passed through a linear rectifier function, max pooled with a 3x3 matrix with stride 2, normalized across feature maps, generating a 55 x 55 elements feature map. The intermediate layers 2 to 5 repeat the same operation, while the final two layers are fully connected and elaborate the features from the top convolutional layer. Finally, the last layer is a soft-max function. Considering the resource requirements of ZFNet, the total number of routing channels required for all layers is 37,062, with an SRAM memory requirement of 124,688 KB.

While implementing the ZFNet CNN design in the RTG4 development kit manufactured by Microchip, we faced the challenge of fitting the selected CNN into a single FPGA chip and yet having some resources available to insert the filtering logic. In order to meet this challenge and implement the CNN on a single FPGA device, we applied a pruning method to the original ZFNet implementation. Pruning is an approach for reducing the number of nodes of the neural network architecture by removing weights, neurons, or even the entire channels of the neural network without suffering drastic accuracy loss. We chose selective pruning based on random removal among neurons characterized by weight values below a given threshold. Applying pruning, we achieved a 39.19% reduction of parameters while the test accuracy dropped about 10%, from 99.26% to 88.87%.

Thanks to the pruning, we reduced the required combinational and sequential resources for implementing all the ZFNet layers on a single chip and the number of needed SRAMs for the weight storage. Table I reports the resource usage in implementing the pruned version of ZFNet on RTG-4 FPGA.

TABLE I. Resource Utilization for ZFNet Implementation on RTG-4

Resource	Utilization	
	[#]	[%]
Combinational Logic	120,904	85.9
Sequential Elements	123,084	81.1
Memory	202	96.7

B. *The Single Event Transient Analysis*

The single event transient analysis has been performed on the plain implementation without applying any SET hardening technique of ZFNet circuit implemented on the RTG-4 to identify the implemented circuit's sensitive sequential elements. A SET pulse is injected in an input, output, or intermediate node of the circuit and propagated through the resources, considering the broadening or filtering effect, until it reaches a storage element, usually a FF. We modeled four different SET pulses with durations of 200 ps, 300 ps, 400 ps, and 500 ps. For each SET, 10,000 pulses are injected randomly in all the intermediate nodes of the circuit.

The RTG-4 Family FPGAs are manufactured using 65 nm technology [10], which, based on previous analysis, expects that pulses with a duration greater than 450 ps will be captured if they arrive during the sampling window of the FF. Therefore, an FF is considered sensitive if it receives pulses with a duration greater than 450 ps, while it is labeled as partially sensitive if the pulses propagate to that FF but with a duration lower than 450 ps. Not sensitive nodes refer to the cases the pulse is not propagating to the FFs. Table II represents the Single Event Transient Sensitive nodes for the injected SET pulses.

TABLE II. Single Event Transient Sensitive nodes report considering 10,000 Random Injections for the Total Number of 123,084 Nodes

SET Pulse [ps]	Sensitive Nodes [%]	Partially Sensitive Nodes [%]	Not Sensitive Nodes [%]
200	37.00	22.40	40.60
300	51.60	15.30	33.10
400	57.60	12.42	29.98
500	65.30	10.03	24.67

As it can be noticed from Table II, the ZFNet original implementation has from 37.0% to 65.3% of circuit nodes potentially sensitive to SET ranging from 200ps up to 500ps. Moreover, the SET analyzer identifies not only the sensitive nodes but also the sensitivity level, which means the maximum duration of the pulse reaching each FFs, which is used for calculating the filtering capability for each FF. This information is reported to the hardening algorithm to insert the SET filtering logic.

C. *The Single Event Transient Analysis on SET Hardened Circuits*

Based on a comprehensive SET analysis performed in the previous phase, we insert the SET filtering logic tuned with respect to the sensitivity level of the identified sensitive FFs.

Please note that in high-performance applications such as the one under study, it is crucial to meet the performance requirements that often have a small margin. To elaborate more, the insertion of hardening techniques leads to performance overhead which should be considered. This challenge was considered during the calculation of filtering capability, where a threshold was set to reduce the SET sensitivity while still holding to the application's performance

requirements. This approach ensures that the application remains reliable and meets its performance goals.

In order to verify the effectiveness of the implemented hardening technique, we performed the SET analysis on four different implemented circuits:

1. Plain: Original implementation without applying any SET hardening technique.
2. Global Hardened: Inserting SET Filtering logic in all the FFs of the circuit with the filtering capability of 600ps available from commercial tool design.
3. Proposed Selective Hardened (1): Inserting SET filtering logic to the identified sensitive FFs with the tuned filtering capability, considering the maximum filtering capability of 600ps.
4. Proposed Selective Hardened (2): Inserting SET filtering logic to the identified sensitive FFs with the tuned filtering capability, considering the maximum filtering capability of 300ps.

Figure 3 represents the SET sensitivity comparison for the four mentioned implementations. As it can be observed, the ZFNet global hardened implementation is drastically decreasing the sensitive nodes, showing reduction 41.35% reduction in the number of sensitive nodes, while the ZFNet proposed selective hardening (1) and proposed selective hardening (2) represents a reduction of the sensitive nodes equal to 34.86% and 31.35 % respectively.

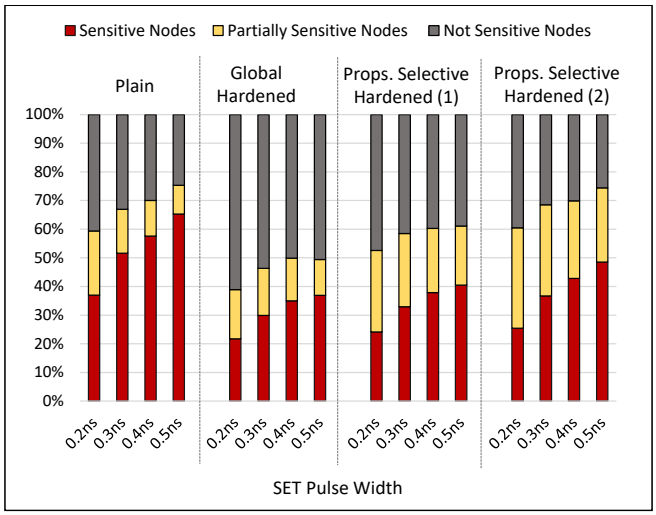

Fig. 3. SET Sensitivity comparison for the plain, global hardened, selective hardened (1) and selective hardened (2) circuit versions.

However, it is crucial to choose an efficient hardening method to fulfill the circuit's requirements. Therefore, as it is represented in Table III, even though the Selective Hardened (2) presents a slightly lower resiliency with respect to others, it is the one with the lowest frequency degradation.

TABLE III. TIMING ANALYSIS DIFFERENT IMPLEMENTATIONS

Implementations	Frequency Overhead [MHz]
Plain	82.665
Global Hardened	69.845
Selective Hardened (1)	75.148
Selective Hardened (2)	78.59

VI. CONCLUSIONS

In this paper, we present a workflow for selective hardening of vulnerable circuit nodes implemented on state-of-the-art RTG-4 radiation-hardened Flash-based FPGA which a vision-oriented benchmark, ZFNet CNN algorithm, with high performance and area requirement is selected. Comparison between the SET sensitivity analysis of three versions of the implemented circuit, plain, global hardening and selective hardening represent the efficiency of the proposed method, causing a negligible reduction of robustness with the lowest performance overhead.

REFERENCES

[1] D. Rizzieri, et al, “A comparative radiation analysis of reconfigurable memory technologies: Finfet versus bulk cmos,” in Elsevier Microelectronics Reliability. Elsevier, 2022, pp. 1–6.

[2] V. Ferlet-Cavrois, L. W. Massengill and P. Gouker, "Single Event Transients in Digital CMOS—A Review," in IEEE Transactions on Nuclear Science, vol. 60, no. 3, pp. 1767-1790, June 2013.

[3] B. Du et al., "A Novel Propagation Model for Heavy-Ions Induced Single Event Transients on 65nm Flash-based FPGAs," 2020 20th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Toulouse, France, 2020, pp. 1-4, doi: 10.1109/RADECS50773.2020.9857686.

[4] N. Battezzati et al., "On the Evaluation of Radiation-Induced Transient Faults in Flash-Based FPGAs," 2008 14th IEEE International On-Line Testing Symposium, Rhodes, Greece, 2008, pp. 135-140.

[5] Sayil, S. “A survey of circuit-level soft error mitigation” in Analog Integrated Circuits and Signal Processing, 2019, pp. 63-70, doi: 10.1007/s10470-018-1300-8.

[6] S. Azimi and L. Sterpone, "Digital Design Techniques for Dependable High Performance Computing," 2020 IEEE International Test Conference (ITC), Washington, DC, USA, 2020, pp. 1-10, doi: 10.1109/ITC44778.2020.9325281.

[7] S. Azimi, B. Du, L. Sterpone, D. M. Codinachs and L. Cattaneo, "SETA: A CAD Tool for Single Event Transient Analysis and Mitigation on Flash-Based FPGAs," 2018 15th International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD), Prague, Czech Republic, 2018, pp. 1-52, doi: 10.1109/SMACD.2018.8434897.

[8] S. Azimi, B. Du and L. Sterpone, "On the mitigation of single event transients on flash-based FPGAs," 2018 IEEE 23rd European Test Symposium (ETS), Bremen, Germany, 2018, pp. 1-2, doi: 10.1109/ETS.2018.8400715.

[9] N. Rezzak, J. -J. Wang, D. Dsilva and N. Jat, "TID and SEE Characterization of Microsemi's 4th Generation Radiation Tolerant RTG4 Flash-Based FPGA," 2015 IEEE Radiation Effects Data Workshop (REDW), Boston, MA, USA, 2015, pp. 1-6, doi: 10.1109/REDW.2015.7336739.

[10] UG0574 Userguide, “RTG4 FPGA Fabric”, 114 pp, 2015.

[11] N. Battezzati, L. Sterpone and V. Ferlet-Cavrois, "Analysis of SET propagation in flash-based FPGAs by means of electrical pulse injection," 2009 European Conference on Radiation and Its Effects on Components and Systems, Brugge, Belgium, 2009, pp. 87-90, doi: 10.1109/RADECS.2009.5994559.

[12] L. Sterpone, et al, "A selective mapper for the mitigation of SETs on rad-hard RTG4 flash-based FPGAs," 2016 16th European Conference on Radiation and Its Effects on Components and Systems (RADECS), Bremen, Germany, 2016, pp. 1-4, doi: 10.1109/RADECS.2016.8093152.

[13] C. De Sio, et al., "FireNN: Neural Networks Reliability Evaluation on Hybrid Platforms," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 549-563, 1 April-June 2022, doi: 10.1109/TETC.2022.3152668.

[14] Matthew D. Zeiler and Rob Fergus, "Visualizing and Understanding Convolutional Networks," *Lecture Notes in Computer Science*, vol. 8689, pp. 818-833, 2014, Springer.

[15] S. Azimi, et al., “A new CAD tool for Single Event Transient Analysis and mitigation on Flash-based FPGAs”, in Integration, the VLSI journal, vol 67, 2019, pp 73-81, doi: 10.1016/j.vlsi.2019.02.001.