World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:12, No:04, 2018

Approximate-Based Estimation of Single Event Upset Effect on Statistic Random-Access Memory-Based Field-Programmable Gate Arrays

Authors : Mahsa Mousavi, Hamid Reza Pourshaghaghi, Mohammad Tahghighi, Henk Corporaal

Abstract : Recently, Statistic Random-Access Memory-based (SRAM-based) Field-Programmable Gate Arrays (FPGAs) are widely used in aeronautics and space systems where high dependability is demanded and considered as a mandatory requirement. Since design's circuit is stored in configuration memory in SRAM-based FPGAs; they are very sensitive to Single Event Upsets (SEUs). In addition, the adverse effects of SEUs on the electronics used in space are much higher than in the Earth. Thus, developing fault tolerant techniques play crucial roles for the use of SRAM-based FPGAs in space. However, fault tolerance techniques introduce additional penalties in system parameters, e.g., area, power, performance and design time. In this paper, an accurate estimation of configuration memory vulnerability to SEUs is proposed for approximate-tolerant applications. This vulnerability estimation is highly required for compromising between the overhead introduced by fault tolerance techniques and system robustness. In this paper, we study applications in which the exact final output value is not necessarily always a concern meaning that some of the SEU-induced changes in output values are negligible. We therefore define and propose Approximate-based Configuration Memory Vulnerability Factor (ACMVF) estimation to avoid overestimating configuration memory vulnerability to SEUs. In this paper, we assess the vulnerability of configuration memory by injecting SEUs in configuration memory bits and comparing the output values of a given circuit in presence of SEUs with expected correct output. In spite of conventional vulnerability factor calculation methods, which accounts any deviations from the expected value as failures, in our proposed method a threshold margin is considered depending on user-case applications. Given the proposed threshold margin in our model, a failure occurs only when the difference between the erroneous output value and the expected output value is more than this margin. The ACMVF is subsequently calculated by acquiring the ratio of failures with respect to the total number of SEU injections. In our paper, a test-bench for emulating SEUs and calculating ACMVF is implemented on Zynq-7000 FPGA platform. This system makes use of the Single Event Mitigation (SEM) IP core to inject SEUs into configuration memory bits of the target design implemented in Zynq-7000 FPGA. Experimental results for 32-bit adder show that, when 1% to 10% deviation from correct output is considered, the counted failures number is reduced 41% to 59% compared with the failures number counted by conventional vulnerability factor calculation. It means that estimation accuracy of the configuration memory vulnerability to SEUs is improved up to 58% in the case that 10% deviation is acceptable in output results. Note that less than 10% deviation in addition result is reasonably tolerable for many applications in approximate computing domain such as Convolutional Neural Network (CNN).

Keywords : fault tolerance, FPGA, single event upset, approximate computing
Conference Title : ICDCFTS 2018 : International Conference on Dependable Computing and Fault Tolerance Systems
Conference Location : Paris, France
Conference Dates : April 19-20, 2018