New solutions for the design of hardened hardware components, from circuit to processor level.

6.7 Hardening Approaches at Different Design Levels

Date: Wednesday 26 March 2014
Time: 11:00 - 12:30
Location / Room: Konferenz 5
Chair: Lorena Anghel, TIMA, FR
Co-Chair: Cecilia Metra, University of Bologna, IT

New solutions for the design of hardened hardware components, from circuit to processor level.

6.7.1 NOSTRADAMUS: LOW-COST HARDWARE-ONLY ERROR DETECTION FOR PROCESSOR CORES

Speakers: Ralph Nathan and Daniel Sorin, Duke University, US

Abstract: We propose a new, low-cost, hardware-only scheme to detect errors in superscalar, out-of-order processor cores. For each instruction decoded, Nostradamus compares what the instruction is expected to do against what the instruction actually does. We implement Nostradamus in RTL on top of a baseline superscalar, out-of-order core, and we experimentally evaluate its ability to detect injected errors. We also evaluate Nostradamus’s area and power overheads.

6.7.2 WORD-LINE POWER SUPPLY SELECTOR FOR STABILITY IMPROVEMENT OF EMBEDDED SRAMS IN HIGH RELIABILITY APPLICATIONS

Speakers: Bartomeu Alorda, Cristian Carmona and Sebastia Bota, Balearic Islands University, ES

Abstract: Embedded SRAM yield dominates the overall ASIC yield, therefore the methodologies centered on improving SRAM cell stability will be introduced in the design as a mandatory. Word-line voltage modulation has shown that it is possible to improve cell stability during access operations. The high variability of physical and performance parameters introduce the need to adopt adaptable solutions to adequately improve SRAM cell stability. In this work, we present a word-line voltage selector circuit designed to modulate power-supply word-line voltage at each individual embedded SRAM block. The final area overhead is minimal and several strategies can be implemented with the embedded SRAM allowing adjust word-line voltage value during the life of ASIC, taking into account different operation, aging and degradations effects.

6.7.3 A HIGH PERFORMANCE SEU-TOLERANT LATCH FOR NANOSCALE CMOS TECHNOLOGY

Speaker: Zhengfeng Huang, Hefei University of Technology, CN

Abstract: This paper presents a high performance latch to tolerate radiation-induced single event upset in 45 nm CMOS technology. The latch can improve robustness by masking the soft errors utilizing Muller C-element and dual modular redundancy hardening. The power dissipation, propagation delay and reliability of the presented SEU-tolerant latch are analyzed by SPICE simulations. The results show that the presented latch provides a higher robustness and lower power-delay product than classical implementations and alternative hardened solutions.

6.7.4 A LOW-COST RADIATION HARDENED FLIP-FLOP

Speakers: Yang Lin, Mark Zwolinski and Basel Halak, University of Southampton, GB

Abstract: The aggressive scaling of semiconductor devices has caused a significant increase in the soft error rate caused by radiation hits. This has led to an increasing need for fault-tolerant techniques to maintain system reliability. Conventional radiation hardening techniques, typically used in safety-critical applications, are prohibitively expensive for non-safety-critical electronics. This work proposes a novel flip-flop architecture named SETTOFF which significantly improves circuit resilience to radiation hits over previous techniques. In addition, compared to other techniques such as a TMR latch, SETTOFF reduces the area and performance overhead by up to 50% and 80%, respectively; the power consumption is also reduced by up to 85%. In addition, a novel reliability metric called radiation-induced failure rate is developed which can be a valuable tool to predict the impact of radiation hits and quantitatively compare the reliability of various radiation hardened techniques. Our analysis shows that the proposed technique can achieve zero SEU failure rate, and significantly reduce the SET failure rate.

6.7.5 PSP-CACHE: A LOW-COST FAULT-TOLERANT CACHE MEMORY ARCHITECTURE

Speakers: Hamed Farbeh and Seyed Ghassem Miremadi, Sharif University of Technology, IR

Abstract: Cache memories constitute a large fraction of processor chip area and are highly vulnerable to soft errors caused by energetic particles. To protect these memories, most of the modern processors employ Error Detection Codes (EDCs) or Error Correction Codes (ECCs). EDCs/ECCs impose significant overheads in terms of area and energy; these overheads increase as a function of interleaveing EDCs/ECCs to detect/correct multiple errors. This paper proposes a new cache architecture to minimize the area and energy overheads of EDCs/ECCs in set-associative L1-caches. Simulation results for a 4-way set-associative cache show that the proposed architecture reduces both the area and static power overheads of parity code by about 75% and the dynamic energy overhead by about 73% in comparison to conventional cache architecture. These reduction figures are about 68% and about 66%, respectively, for SEC-DED code. The above reductions are achieved without affecting the error coverage.
A HYBRID NON-VOLATILE SRAM CELL WITH CONCURRENT SEU DETECTION AND CORRECTION

Speakers:
Pilin Junsangsri, Fabrizio Lombardi¹ and Jie Han²
¹Northeastern University, US; ²University of Alberta, CA

Abstract
This paper presents a hybrid non-volatile (NV) SRAM cell with a new scheme for SEU tolerance. The proposed NVSRAM cell consists of a 6T SRAM core and a Resistive RAM (RRAM), made of a 1T and a Programmable Metallization Cell (PMC). The proposed cell has concurrent error detection (CED) and correction capabilities; CED is accomplished using a dual-rail checker, while correction is accomplished by utilizing the restore operation; data from the non-volatile memory element is copied back to the SRAM core. The dual-rail checker utilizes two XOR gates each made of 2 inverters and 2 ambipolar transistors, hence, it has a hybrid nature. Extensive simulation results are provided. The simulation results show that the proposed scheme is very efficient in terms of numerous figures of merit such as delay and circuit complexity and thus applicable to integrated circuits such as FPGAs requiring secure on-chip non-volatile storage (i.e. LUTs) for multi-context configurability.