A Comprehensive Approach to Fault Tolerance: Device, Circuit, and System Techniques

Z. Stamenkovic and V. Petrovic
IHP
Frankfurt (Oder), Germany
{stamenkovic,petrovic}@ihp-microelectronics.com

In spite of the huge research efforts and respectable scientific achievements, there are still challenges regarding the use of commercial ASIC technologies in space and safety-critical applications. This work presents a design methodology for fault-tolerant ASIC that is based on radiation-hard technology, redundant circuits with latchup protection, additional implementation steps during logic synthesis and layout generation, and power gating. Enhancements have been made within the standard ASIC design flow in order to incorporate redundancy and power-switch cells and, consequently, enable protection against single-event upset (SEU), single-event transient (SET), and single-event latchup (SEL). In order to validate the proposed fault-tolerant circuits, a fault-injection environment including fault models has been developed. The fault occurrence and its duration are modeled according to the real effects in actual hardware. Some of these techniques are being exploited and implemented in the SEPHY project (http://www.sephy.eu), which aims to increase the European competitiveness in the field of fault-tolerant ASIC by developing a radiation-hard PHY layer of the 10/100-Base-T Ethernet transceiver. The radiation-hard PHY layer ASIC will be fabricated in Atmel’s 150 nm technology. This device will enable the use of Ethernet in space systems and also provide the base to implement a radiation-hard Gigabit Ethernet PHY layer for space applications. Additionally, the developed techniques and devices can be of interest in other critical applications like automotive or industrial systems.

In order to automate a design flow of the fault-tolerant circuits, it is essential to design specific cells which are not present in the standard or radiation-hard design kits. A SEL protection switch (SPS) is described first. It consists of a current sensor/driver, feedback block, control block, and communication interface for a power network controller. Afterwards, the details of triple-modular redundant (TMR) and double-modular redundant (DMR) circuits with latchup protection and separated power domains are presented.

Fault-injection models for TMR and DMR circuits are developed in order to simulate and verify the fault-tolerant designs. Functional simulation of a digital design at the gate level suffices in case of the single-event transient and upset effects. However, in order to provide the information about design behavior during latchup effect, it is required to functionally simulate the design at the transistor level. We present TMR and DMR circuit simulation results with the implemented fault-injection models for all three types of the mentioned single-event effects.

Fault-tolerant ASICs can be implemented using the standard design automation tools and introducing a few additional steps in the standard design flow. An extra step is necessary to generate a modified design netlist including redundant cells, voters and required protection for memory blocks. The other two additional steps (definition of the power domains and placement of the SPS cells) have to be undertaken in the layout phase. The SPS cells are placed under the crossover points of the power stripes and cell rows. A SPS cell protects just one power domain and corresponding redundant logic.