IP for Embedded Robustness

Michael Nicolaidis
IRoC Technologies
michael.nicolaidis@iroctech.com

1. VDSM Reliability Issues in the Field

Drastic device shrinking, power supply reduction, and increasing operating speeds that accompany the technological evolution to very deep submicron, reduce significantly the noise margins and affect the reliability of very deep submicron ICs. Timing faults escaping timing closure analysis and/or manufacturing testing, as well as soft-errors, are creating reliability issues in the field.

Soft Errors: In this context, single event upsets (SEUs) are becoming one of the major signal integrity problems. Atmospheric neutrons have become a major source of SEUs in modern VDSM technologies. An SEU is the consequence of a single event transient (SET) created on a sensitive node by a particle striking an integrated circuit. When an SET occurs on a memory-cell node and flips the state of the cell it is transformed to a single event upset (SEU). An additional problem is that in today technologies, soft errors concern not only memories (which has been the case so far) but also logic. An SET, occurring on a node of a logic network, is transformed to an SEU when a latch captures it.

One basic reason for increased sensitivity to SEUs, is the reduction of both the device size and the Vdd voltage. Since both the Vdd level and the circuit node capacitance $Cnode$ are reduced, the charge stored on a circuit node ($Q = Vdd * Cnode$) is reduced drastically. Consequently, a significantly lower charge deposed by a particle strike suffices to flip the logic value of a node, creating a transient pulse (single event transient or SET). The transient pulse, after propagation through the logic network, can be captured by a latch to create an SEU. In the past, the probability of occurrence of an SEU in logic parts was drastically lower than in memories, due to the following reasons: (i) the propagation through logic gates can filter the induced transient pulse, and (ii) a transient pulse propagated through a logic network can result in a logic error if it reaches the input of a latch in coincidence with the set up or the hold period of the clock cycle. Unfortunately, in VDSM the transient pulses become wider than the logic transition time of the logic gates. Thus, they are propagated through the logic network without attenuation. In addition, as the clock frequencies increase, the probability of latching a transient pulse increases as well. Due to these trends, the error rates in logic parts become as high as the error rates in memories.

Timing faults: Such faults can be the consequence of a signal integrity problem such as cross talk or ground bounce. In fact, the complexity of signal integrity verification in VDSMs SOCs increases the chances that a design, which under some circumstances exceeds its timing budget, is not detected as such by the signal integrity verification process. Timing faults can also be the consequence of the combination of a signal integrity issue with a fabrication defect. Process parameter variations and various defects (shorts, opens…) often increase the path delays of a circuit. In multi-MHz circuits, even short delay variations may result on timing faults. Eliminating such defects during fabrication testing requires to test the timing faults under the worst delay conditions, such as the excitation and propagation of the defect together with worst cross talk and/or ground bounce conditions. Testing the huge number of paths in modern circuits for such complex test conditions makes the test generation process computationally unfeasible and the test length unrealistic. Thus, circuits with timing faults can be declared fault-free by fabrication testing.

2. Fault Tolerant SOC Design

In this context, it becomes mandatory to evaluate the sensitivity of combinational and sequential logic blocks, and eventually eliminate the effect of SEU and/or of timing faults by modifying the design.

SEU sensitivity is increasing drastically from one process generation to another, and is going to become a major reliability problem. For 0.13 micron process the typical SEU sensitivity level seems to be a few thousand FIT per Mbit SRAM (but this is a raw estimation since the SEU sensitivity can be different from one fabrication process to another). This level corresponds to one failure every 10 days for a 128 Mbyte SRAM. Thus, 0.13 micron is becoming the starting point for integrating SEU protection at ground level, for at least some applications. Fault tolerant design is one of the best-suited approaches for coping with SEUs. As predicted several years ago [1], designing fault tolerant circuits is the only way to continue the progress of technological scaling. Thus, we need a new design paradigm to integrate fault tolerance at the chip level and at low cost [2]. Memories are the first parts to be

protected, since they represents the largest parts of a system, but logic protection will also be needed soon. Fault tolerant design is also suitable for correcting errors produced by timing-faults during lifetime.

Fault tolerant memories: Hardened memory cells can be employed to protect memories against SEUs. However hardened cells require a high area cost and may not be acceptable for large memories. Lower area cost can be achieved by means of error correcting codes (ECC). For instance, for the Hamming code, the percentage of extra bits is about 20% for 32-bit word length memories, and 12.5% for 64-bit word length. ECC has also several drawbacks:

- The cost for memories with short word length can be high (50% for 8-bit word length, 75% for 4-bit word length).
- Embedded memories with maskable operations are very frequent in SOCs. Traditional ECC cannot be used with such memories (unless using ECC at bit level, which results on bit triplication).
- ECC generation and ECC control add a significant delay to the read and write cycle, resulting on a significant speed penalty for the system.

New proprietary ECC solutions achieve low cost of ECC for memories with short word length and/or maskable operations and eliminate the speed penalty incurred by the generation and control of the ECC.

Fault tolerant logic: The simpler fault tolerant approach for logic is TMR (triple modular redundancy). However, area cost of TMR is not acceptable for a majority of applications. Error detection and correction can reduce the cost significantly. Low cost error detection can be achieved by means of time redundancy (a 15% area cost can be achieved by means of this technique for a processor core). Time redundancy can be done without speed penalty, for low and medium speed designs. But as the clock period is approaching the duration of SETs (e.g. in multi-MHz designs), speed penalty cannot be avoided. For multi-MHz designs, space redundancy based on error correcting coding of the outputs of combinational or sequential blocks, is becoming the best alternative. This technique requires a particular logic synthesis process to guaranty that the code detects the large majority of the errors produced on the block outputs. After error detection, the correct results must be computed. For single event transients (SETs), this can be done by means of a retry procedure that repeats the most recent operations. For timing faults, error correction can also be achieved by means of retry, but the clock frequency has to be reduced during the retry phase. Performance lost involved by the activation of the retry phase is insignificant, since error occurrence is not a frequent event.

CAD and Embedded Robustness IP: Traditional CAD does not support this kind of design. However, CAD tools making fault tolerant design compatible with traditional CAD are rapidly emerging and some tools are already available by some specialized companies, enabling SEU characterization of complex designs and automatic insertion of the fault-tolerant mechanisms. IP infrastructure for fault tolerance insertion in complex SOCs is also mandatory. Such infrastructure includes IP blocks for ECC generation and control for embedded memories, considering both conventional ECC solutions as well as new low-cost ECC solutions for memories with short word length and/or maskable operations, IP blocks interfacing processors with embedded memories for eliminating speed penalty incurred by ECC, IP blocks for controlling the retry process, as well as IP blocks for saving the context sensitive state to be used during the retry phase. In addition, IP blocks interfacing SOCs with stand-alone memories, for performing ECC generation and control and for eliminating speed penalty. Developing fault tolerant processor cores is a further step that greatly enhances the design of robust SOCs.

[1] M. Nicolaidis, "Design for Soft-Error Robustness to Rescue Deep Submicron Scaling", In proceedings ITC 98, October 1998, Washington DC.
[2] Contribution of M. Nicolaidis in the Rountable of the October-December 1999 issue of IEEE Design & Test of Computers.