FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 26, N^o 3, December 2013, pp. 175 - 186
DOI: 10.2298/FUEE1303175S

FAULT-TOLERANT ASIC: DESIGN AND IMPLEMENTATION

Z. Stamenković, V. Petrović, G. Schoof

IHP, Im Technologiepark 25, 15236 Frankfurt (Oder), Germany

Abstract. *The paper presents fault-tolerant CMOS ASICs which are immune to the single event upsets (SEU), the single event transients (SET), and the single event latchup (SEL). Triple and double modular redundant (TMR and DMR) circuits and SEL protection switches (SPS) make the base for a modified fault-tolerant ASIC design flow. The proposed design flow requires the standard design automation tools and a few additional steps during logic synthesis and layout generation. An extra step is necessary to generate the redundant design net-list including voters. Other two extra steps (definition of the redundant power domains and placement of the SPS) have to be performed in the layout phase. The concept has been proven by design and implementation of the two digital circuits: shift-register and synchronous counter.*

Key words: *Single event effect, fault tolerance, TMR, DMR, latchup protection, ASIC*

1. INTRODUCTION

Malfunctions of electronic devices due to the single event effects, being an effect of radiation, are observed not only in cosmic and airborne equipment, but also in mainstream applications. Together with the progressing integration and scaling of the electronic chips their susceptibility to errors increases. The current space microelectronics development and high energy physics research require shorter design time and cheaper solutions for the radiation and fault tolerant ASIC designs [1], [2], and [3]. The main idea is to provide ASICs capable of correct and reliable functioning in the radiation environment using the standard semiconductor technologies and design flow. Therefore, the design of the advanced fault-tolerant digital integrated circuits needs scientific research and progress concerning three important aspects:

1. Analysis of irradiation effects and circuit faults.
2. Development of fault models and simulation test benches.
3. Design of fault-tolerant circuits and systems.

Definition and description of the basic irradiation effects and fault mechanisms can be found in literature [4], [5], and [6]. The thesis referenced in [7] provides an overview of different radiation environments and investigates interaction mechanisms between ener-

Received October 25, 2013
Corresponding author: Z. Stamenković
IHP, Im Technologiepark 25, 15236 Frankfurt (Oder), Germany
(e-mail: stamenko@ihp-microelectronics.com)

getic particles and the matter. It also introduces a new semi-empirical model for estimating the electronic stopping force of heavy ions in solids. The most common irradiation effect is a single event effect (SEE) induced by a cosmic particle strike. Three common types of SEE are known: single event upset (SEU), single event transient (SET) and single event latchup (SEL). A single event upset causes the change of state in a storage element. It affects the memory cells and sequential logic. A single effect transient causes a short impulse at the combinational logic output. The wrong logic state will propagate in case that it appears during the active clock edge. On the other hand, a single event latchup causes the excessive current flow through a parasitic bipolar structure in CMOS circuits (see [8], [9], [10], and [11]). We can clearly separate the known SEU, SET, and SEL fault-tolerant techniques into the two categories: circuit level techniques [12] (hardened-cell design [13], triple modular redundancy (TMR) [14], double modular redundancy (DMR) [15], and error detection and correction for memories [16]) and layout level techniques [17].

When it comes to SEU and SET, the most common fault-tolerant techniques are TMR and DMR. The triple modular redundant circuit consists of three identical modules and a 3-input majority voter. The voter's function is to pass through the major input value to the output. As we speak about digital circuits, the modules are memory elements such as flip-flops or latches. The main disadvantage of this technique is that the system fails in case of a faulty voter. Therefore, a new triple voting logic was developed to complete the circuit redundancy. Each of the three voters is fed from outputs of all three memory modules. This technique is known in the literature as the full triple modular redundancy. A detailed analysis of the triple modular redundancy was presented in [18]. The higher redundancy provides the higher fault tolerance and circuit reliability but increases the chip area, energy consumption, and costs. Therefore, the goal is to trade-off between the redundancy level and the reliability requirements taking into account the prospective application. In order to reduce the high hardware overhead produced by TMR and keep the design reliability high, the double modular redundancy with self-voting was developed [15]. A novel double/triple modular redundancy (DTMR) technique for dynamically reconfigurable devices tested on a finite state machine was presented in [19].

The SEL mitigation techniques can be classified in the three main groups. First approach uses the current sensors at board-level to detect the excessive current induced by latchup. The power supply of the affected device is switched off and, after some time, re-established again. This approach suffers from a serious drawback: the circuit state is destroyed and can't be recovered. Second approach [20] is based on introduction of an epitaxial buried silicon layer and reduction of the well resistivity. However, this modification incurs additional costs and impact circuit performance. Third approach [21] uses n-type and p-type guard rings that break the parasitic bipolar transistor structure. This solution is very efficient but can result in excessive circuit area. A new SEL mitigation scheme that combines error correcting codes with intelligent power line implementation was presented in [22].

The paper presents a design flow for fault-tolerant ASIC based on the redundant circuits with latchup protection and additional implementation steps during logic synthesis and layout generation. The proposed approach protects ASICs from the SEU, SET, and SEL faults by combining and integrating different fault-tolerant techniques. The following sections describe a SEL protection switch (Section 2), redundant (TMR and DMR) cir-

cuits with latchup protection (Section 3), a fault-tolerant ASIC design flow (Section 4), and simulation results of the implemented fault-tolerant circuits (Section 5). The conclusions are summarized in Section 6.

2. LATCHUP PROTECTION

Instead of using the external current sensors and the expensive technological modifications, we introduce a single event latchup protection switch (SPS) which can be integrated with standard cells and which can control their supply current. The proposed SEL protection switch is shown in Figure 1. It is an improved version of the switch presented in [23] and [24]. The main task of this circuit is to switch off the power supply in case of the excessive supply current. A current sensor/driver (P5 transistor) is used for supplying the power to the logic that needs to be protected from latchup. The P5 transistor operates in the linear (ohmic) region. It must provide enough current during normal operation (as a driver) and survive a potential latchup (as a sensor). When all the circuits operate correctly, both inputs of the NOR gate (P0, P7, N1, and N5 transistors) are at logic 0 and the output (B node) is therefore at logic 1. The C node is set to logic 0 because the P1 transistor is off (there is no current through the R1 pull-down resistor). This activates the P5 transistor which drives enough current (and voltage) at the VDD_a output. Logic 1 at VDD_a is inverted by the P8/N6 transistor pair and the A node is set to logic 0. The TSTART output stays at logic 1 (the N8 and N9 transistors are off) that indicates no latchup condition.

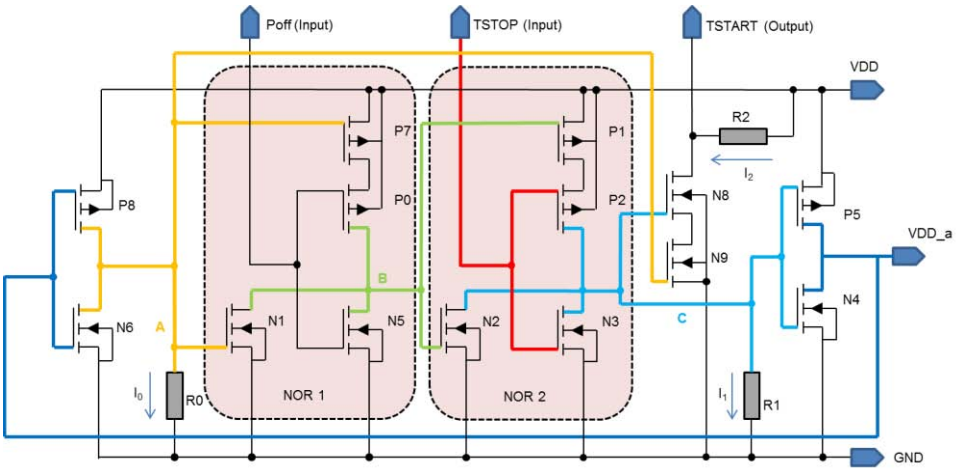

Fig. 1 Schematic of the latchup protection switch

In case of the excessive supply current, the output voltage of the P5 transistor increases what, in turns, causes the voltage drop of the transistor drain (VDD_a output). As soon as the VDD_a voltage is under the threshold voltage, the feed-back line sets the A node to logic 1. It activates the N9 transistor that sets the TSTART output to logic 0 and informs a power network controller that the latchup has occurred. On the other side, the B

node is set to logic 0 and the P1 transistor is activated. The TSTOP input is set to logic 0 by the power network controller. Therefore, after the latchup has been detected, the C node goes to logic 1 and forces the VDD_a output to logic 0 (the power supply is cut off). The power network controller switches the circuit between different operational modes (active, latchup protected, or power off) and defines their duration. It consists of three components: a programmable counter, a status/control unit, and a control register. A block diagram of the power network controller is shown in Figure 2.

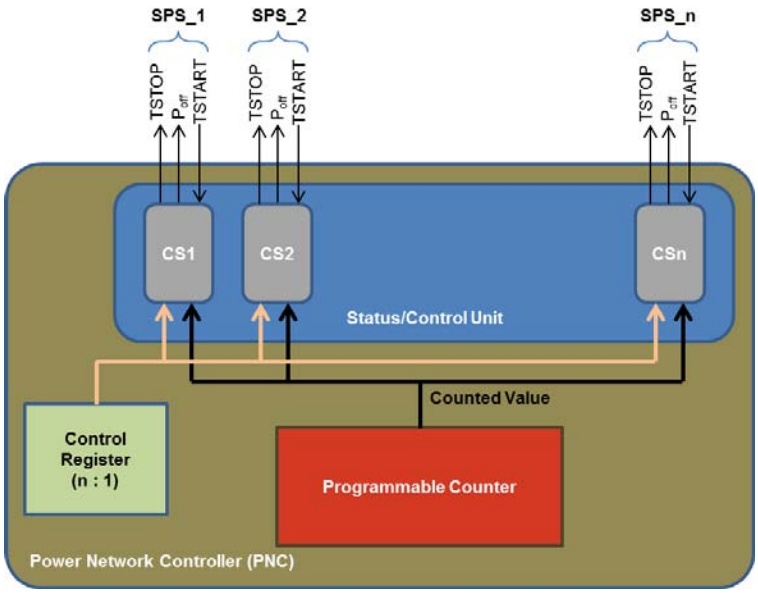

Fig. 2 Power network controller

The programmable counter sets the period of latchup protection mode depending on the chosen technology. The status/control unit is composed of control interfaces which communicate with the SPS cells via an input signal (TSTART) and two output signals (TSTOP and P_{off}). If the latchup has been detected, the TSTART signal activates the corresponding control interface which has to save the current counter value. When the counter reaches again the saved value (the protection phase is over), the control interface activates the TSTOP signal. The P2 transistor is deactivated and there is no current through the R1 pull-down resistor. The C node is again at logic 0 and the P5 transistor can supply the connected logic. In this way, it is possible to detect multiple latchup effects. If the latchup continues after the protection phase is finished, the N8 transistor keeps the power network controller informed about it and the TSTOP signal will not be activated. The control register generates the P_{off} signal and can be accessed by the system processor. The power network controller has an independent clock. If the controlled section (circuit) needs to be switched off for a longer period of time, the power network controller sets the P_{off} input to logic 1.

3. REDUNDANCY

Redundancy is always required for a fault-tolerant design. The higher redundancy, the better protection, but also the larger chip area, power consumption, and cost. Therefore, it is necessary to trade-off between the redundancy rate and the cost for each and every application. However, the redundant circuits (TMR and DMR) need to be protected from the latchup condition too. This requires significant modifications of the standard TMR and DMR circuit designs. We propose the SEL protection switch and the independent redundant power domains as a foundation of the latchup protected redundant circuits.

3.1. TMR with latchup protection

Figure 3 presents a TMR circuit with three SEL protection switches which control three independent power domains. In case of the latchup (high supply current) condition in one of the three power domains, the corresponding switch breaks off the supply line of this domain but the other two power domains (and redundant circuits) continue with normal operation. Since one of the three redundant modules is switched off, this TMR circuit operates as a DMR circuit and it stays so as far as the latchup protection is active.

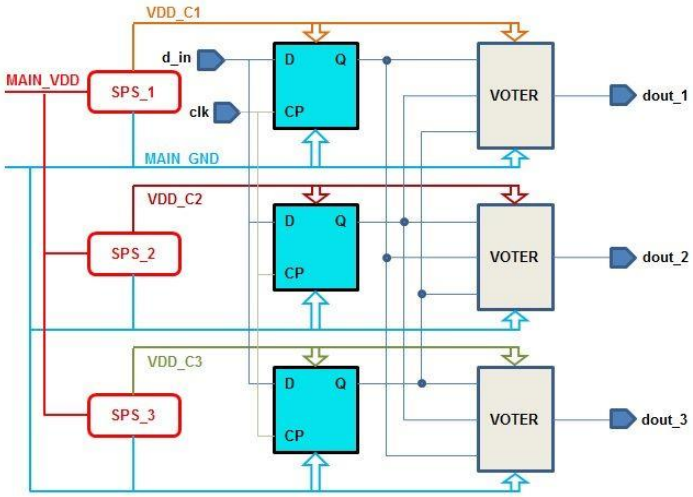

Fig. 3 TMR circuit with the latchup protection switches

3.2. Self-voting DMR with latchup protection

In order to reduce the hardware overhead produced by the TMR and to keep the design reliability high, we use the self-voting DMR (Figure 4). Self-voting is based on a 3-input majority voter configured to vote on the two external input values and its own output value. The SPS switches off the power domain (and redundant circuit) which suffers latchup. It means that the redundancy is lost during the latchup protection. However, modifications of the voter feed-back logic are necessary since the standard self-voting DMR circuit is very sensitive to a SET hitting the flip-flop data input near the active clock edge [23].

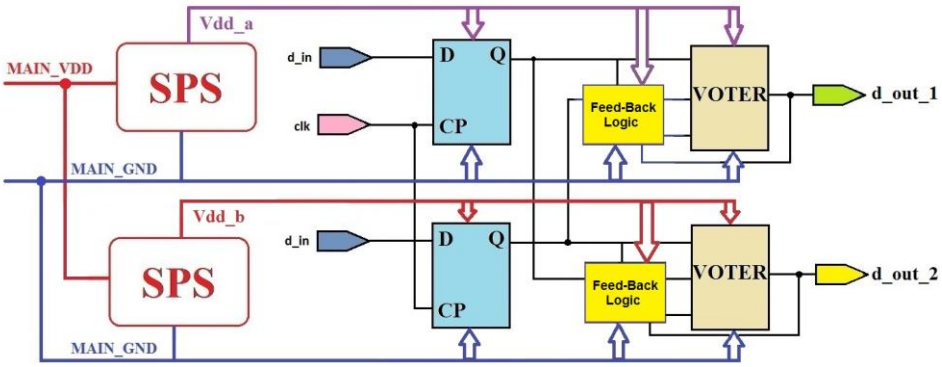

Fig. 4 Self-voting DMR circuit with the latchup protection switches

Having a SET occurred during the clock transition, the setup/hold time margins can be violated and the flip-flops are not certain about the correct output state (well-known effect of metastability). If the flip-flops are in the different logic states, a SEU occurs and propagates through the logic, causing the system failure [25]. As a remedy, we propose using the logic value of the flip-flop data input at the third voter input during the hold time. After the hold time has passed, the voter output becomes again its third input and it stays so until the next active clock edge arrives. During the clock transition, a short pulse is generated to control a multiplexer and send data from the flip-flop input to the third voter input. In case of a SET during this short period of time, regardless of the wrong state of the flip-flop output, the third voter input receives the correct logic value. This approach works fine for transient pulses of a few hundreds of picoseconds, what is limited by the flip-flop hold time. The self-voting DMR circuit with multiplexers in feed-back logic has been verified at a fault-injection testbench using gate-level simulations [26].

4. DESIGN FLOW

Fault-tolerant ASICs can be implemented using standard design automation tools [27], [28], [29] and introducing a few additional steps in design flow. An extra step compared to the standard design flow (HDL modelling, simulation, logic synthesis and technology mapping, floor and power planning, cell placement, wire routing, and, finally, design rule and layout checking) is necessary to generate a new net-list including redundant cells and voters. The other two extra steps (definition of the redundant power domains and placement of the SPS cells) have to be made in the layout phase. A modified design flow is presented in Figure 5.

Duplication (for DMR) or triplication (for TMR) of the original net-list is performed using a parsing script which can be included in the synthesis script as an optional subprogram. The parser is generated by a set of the GnuWin tools [30]. It takes care of the following:

a) The names of redundant instances in the design net-list must be unique. Identical (redundant) instances from different power domains are marked after the power domain which they belong to.

b) The inputs of a TMR voter have to be connected to the outputs of all three redundant flip-flops.

c) Two inputs of a DMR voter have to be connected to the outputs of both redundant flip-flops and the third input has to be connected to the voter's output by a multiplexer.

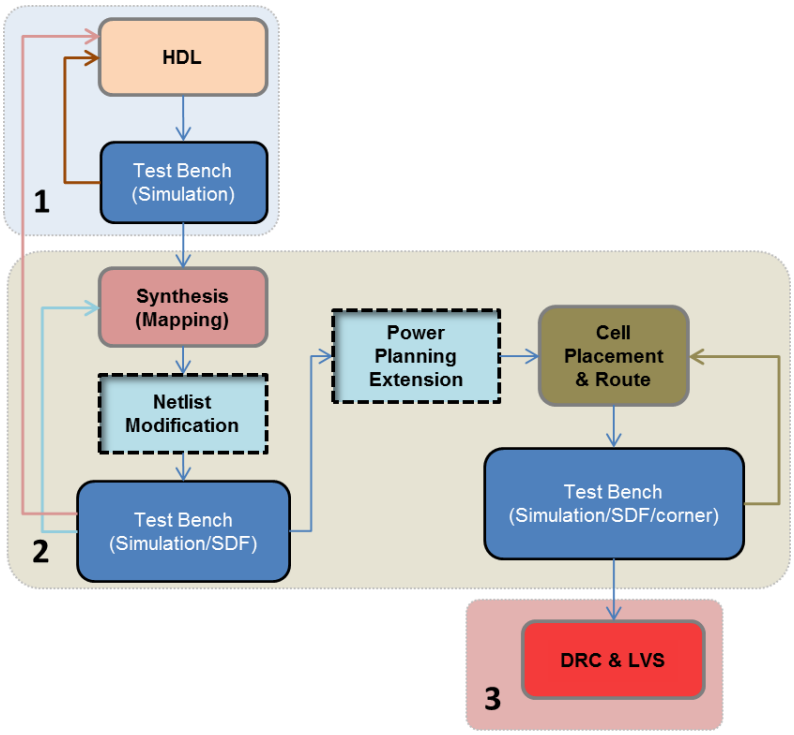

Fig. 5 Design flow for fault-tolerant ASIC

A simple modification of the technology file suffices in case of redefinition of the power domains. After the power planning has been finished, the placement of SEL protection switches (SPS) can be performed. The SPS cells are placed under the crossover points of the power stripes and cell rows (where the filler cells are usually placed). A SPS cell (or a group of SPS cells) protects only one power domain and the corresponding redundant logic. SPS cells may not be placed under all power crossover points. The maximal current needed for driving the connected logic defines the required (minimal) SPS output current.

Figure 6 illustrates a DMR circuit with placed SPS cells. A pair of SPS cells controls the power supply of all the cells in a redundant row section (the SPS 1a and 2a control the power domain VDD_a: SC1_a, SC2_a, SC3_a, SC4_a, SC5_a, and SC6_a; the SPS 1b and 2b control the power domain VDD_b: SC1_b, SC2_b, SC3_b, SC4_b, SC5_b, and SC6_b). Similar SPS placement can be done in case of the generation of a TMR layout. After the SPS cells have been placed and connected to the corresponding power domains, the design flow continues with the standard steps: cell placement, clock tree synthesis,

and wire routing with all the required timing optimizations. The flow ends by the design rule and layout-versus-schematic checks.

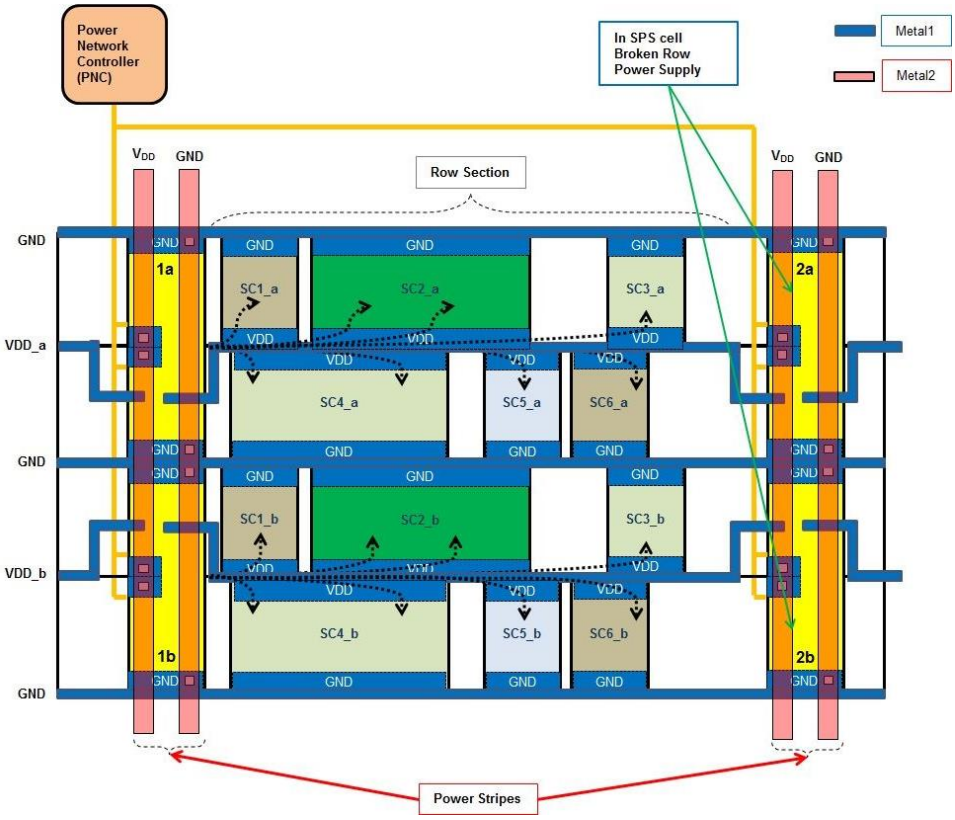

Fig. 6 Layout of a DMR circuit with integrated SPS cells

5. CASE STUDIES

In order to prove the proposed concept and protection techniques, DMR test circuits (a 4-bit shift-register and a 4-bit synchronous counter) equipped with the latchup protection have been designed, implemented, and tested.

Figure 7 shows a block diagram of the shift-register. The *dmr_ff* cell is a "half" of the circuit depicted in Figure 4 (flip-flop, voter, and feed-back logic). As it has already been explained in the previous section, a single cell does not necessarily include the protection switch. In the presented test circuits, one SPS switches two cells. Figure 8 presents simulation waveforms of the shift-register signals.

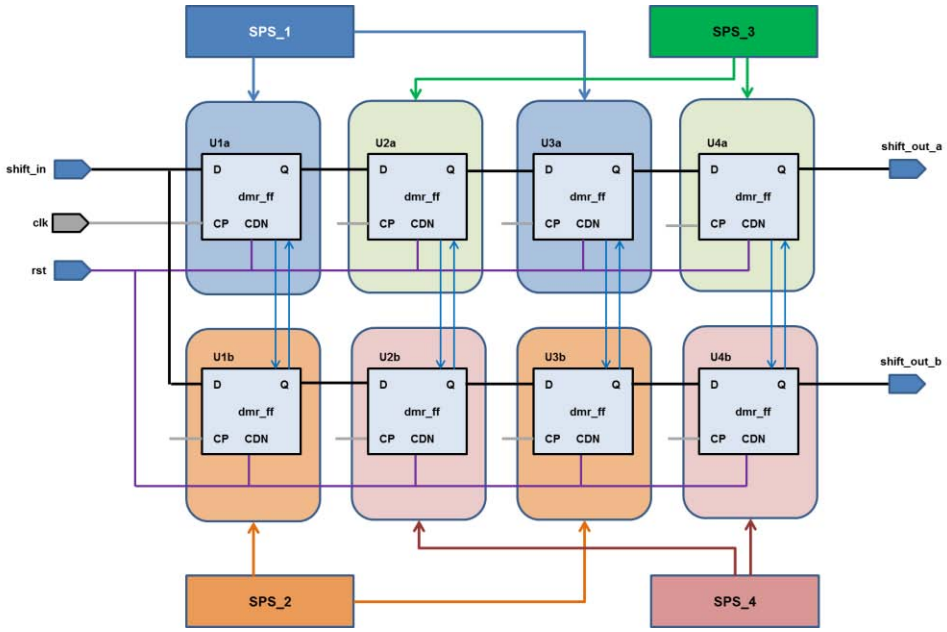

Fig. 7 Functional block diagram of the shift-register

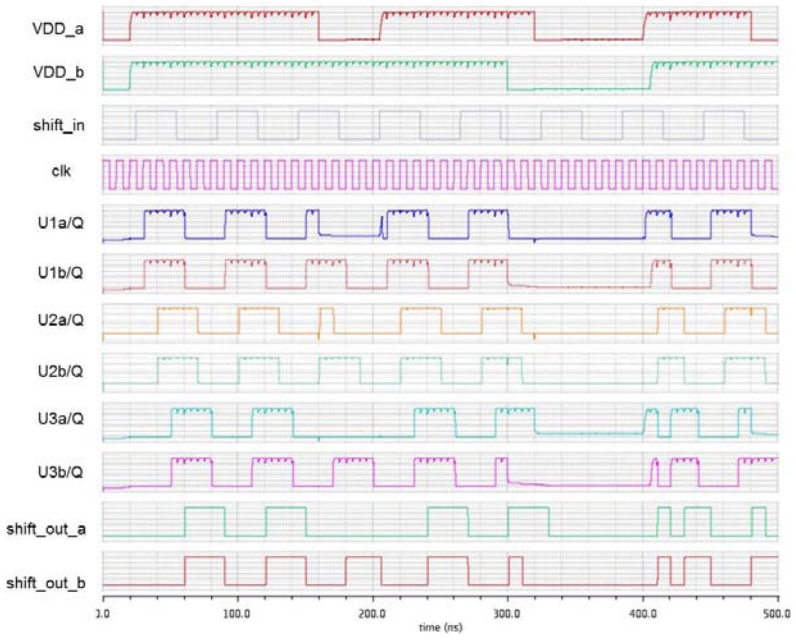

Fig. 8 Timing simulations of the shift-register signals

Figure 9 shows a block diagram of the synchronous counter. A counter cell consists of the *dmr_ff* cell and feed-back combinational logic (see the insert of the first cell). Figure 10 presents simulation waveforms of the counter signals.

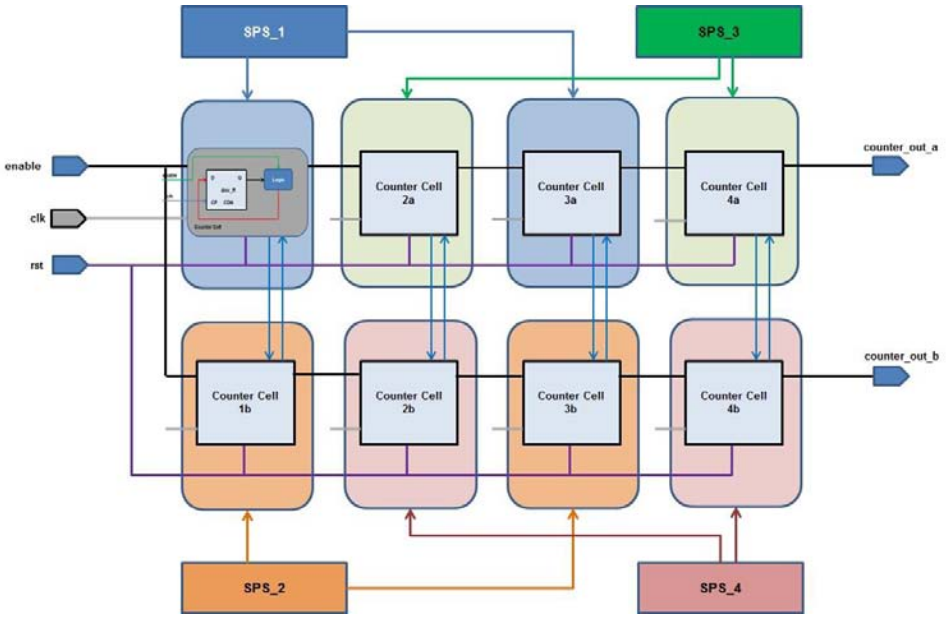

Fig. 9 Functional block diagram of the synchronous counter

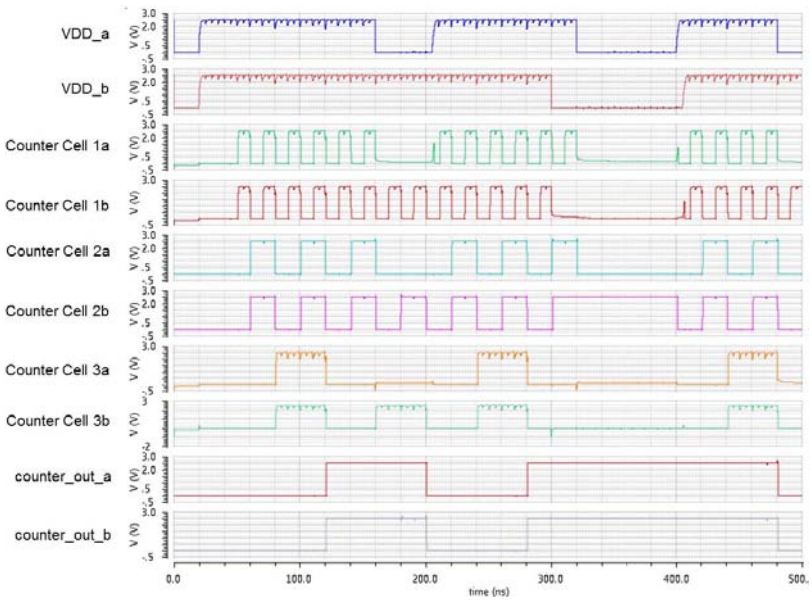

Fig. 10 Timing simulations of the synchronous counter signals

SPICE timing simulations illustrate the circuits' behaviour when one or both redundant sections suffer the latchup. The SPS 1 and SPS 3 cells control the *a* section. This section is switched off after the latchup has been triggered. The *b* section (controlled by the SPS 2 and SPS 4 cells) keeps working properly. After both sections have been switched off and, after some time, switched on again, the circuit logic states are reset and the shifting/counting process continues.

6. CONCLUSION

The standard design flow has been modified to provide the protection of digital ASICs against the known single event effects occurring in radiation environment. The results, based on the shift-register and synchronous counter simulations, have shown that the SEL protection switches integrated with TMR or DMR circuits seem to be a promising solution when it comes to the design of fault-tolerant circuits and systems. The future work will be focused on improvements of the TMR and DMR circuits, development of the redundant net-list parsers, and simplification of the SPS cell placement. Testing of more complex circuits is planned for the near future.

Acknowledgement: *The research leading to these results has received funding from the European Union's Seventh Framework Programme FP7 (2007 - 2013) under the grant agreement no. 284389 also referred as VHiSSI.*

REFERENCES

[1] N. Dressnandt, M. Newcomer, O. Rohne, and S. Passmore, "Radiation hardness: design approach and measurements of the ASDBLR ASIC for the ATLAS TRT", In the IEEE Nuclear Science Symposium Conference Record, Norfolk (USA) 2002, (pp.151-155)

[2] J. Tarrillo, R. Chipana, E. Chielle, and F. L. Kastensmidt, "Designing and analyzing a SpaceWire router IP for soft errors detection", In Proc. 12th Latin American Test Workshop, Porto de Galinhas (Brazil) 2011, (pp.1-6)

[3] Y.-K. Jung, "Fault-recovery non-FPGA-based adaptable computing system design", In Proc. Second NASA/ESA Conference on Adaptive Hardware and Systems, Edinburgh (UK) 2007, (pp.709-716)

[4] A. Holmes-Siedle and L. Adams, *Handbook of radiation effects*, Second Edition, Oxford University Press, New York, 2002.

[5] M. Nicolaidis (Ed.), *Soft errors in modern electronic systems*, Springer, New York, 2011.

[6] K. Iniewski (Ed.), *Radiation effects in semiconductors*, CRC Press, Boca Raton, 2011.

[7] A. Javanainen, *Particle radiation in microelectronics*, PhD Thesis, Department of Physics, University of Jyväskylä, Finland, 2012.

[8] R. R. Troutman, *Latchup in CMOS technology: The problem and its cure*, Kluwer Academic Publishers, Boston, 1986.

[9] S. H. Voldman, *Latchup*, John Wiley & Sons, Chichester, 2007.

[10] N. H. E. Weste and D. M. Harris, *CMOS VLSI design: A circuits and systems perspective*, Fourth Edition, Addison-Wesley, Boston, 2011.

[11] L. Ye, G. Xiaohan, X. Weiwei, H. Zhiliang, and D. Killat, "An experimental extracted model for latchup analysis in CMOS process", In Proc. 8th IEEE International Conference on ASIC, Hunan (China) 2009, (pp.1035-1038)

[12] R. C. Lacoe, "Improving integrated circuit performance through the application of hardness-by-design methodology", *IEEE Transaction on Nuclear Science*, vol.55, no.4, pp.1903-1925, 2008.

[13] M. P. Baze, S. P. Buchner, and D. McMorrow, "A digital CMOS design technique for SEU hardening", *IEEE Transaction on Nuclear Science*, vol.47, no.6, pp.2603-2608, 2000.

[14] R. E. Lyons and W. Vanderkulk, "The use of triple-modular redundancy to improve computer reliability", *IBM Journal of Research and Development*, vol.6, no.2, pp.200-209, 1962.
[15] J. Teifel, "Self-voting dual-modular-redundancy circuits for single-event-transient mitigation", *IEEE Transaction on Nuclear Science*, vol.55, no.6, pp.3435-3439, 2008.
[16] P. K. Lala, "A single error correcting and double error detecting coding scheme for computer memory systems", In Proc. 18th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems, Cambridge (USA) 2003, (pp.235-241)
[17] G. K. Maki and P.-S. Yeh, "Radiation tolerant ultra-low power CMOS microelectronics: Technology development status", In Proc. NASA Earth Science Technology Conference, Hyattsville (USA) 2003, (pp.1-4)
[18] N. Rollins, M. Wirthlin, M. Caffrey, and P. Graham, "Evaluating TMR techniques in the presence of single event upsets", In Proc. International Conference on Military and Aerospace Programmable Logic Devices, Washington DC (USA) 2003, (pp.1-5)
[19] K. Shinohara and M. Watanabe, "A double or triple module redundancy model exploiting dynamic reconfigurations", In Proc. NASA/ESA Conference on Adaptive Hardware and Systems, Noordwijk (Netherlands) 2008, (pp.114-121)
[20] D. B. Estreich, A. Ochoa, and R. W. Dutton, "An analysis of latch-up prevention in CMOS IC's using an epitaxial-buried layer process", In Proc. IEEE International Electron Devices Meeting, Washington DC (USA) 1978, (pp.230-234)
[21] R. R. Troutman, "Epitaxial layer enhancement of N-well guard rings for CMOS circuits", *IEEE Electron Device Letters*, vol.4, no.12, pp.438-440, 1983.
[22] M. Nicolaidis, "A low-cost single-event latchup mitigation scheme", In Proc. 12th IEEE International On-Line Testing Symposium, Lake Como (Italy) 2006, (pp.111-118)
[23] V. Petrovic, M. Ilic, G. Schoof, and Z. Stamenkovic, "Design methodology for fault tolerant ASICs", In Proc. 15th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems, Tallinn (Estonia) 2012, (pp.8-11)
[24] Z. Stamenkovic, V. Petrovic, and G. Schoof, "Design Flow and Techniques for Fault Tolerant ASICs (invited)", In Proc. 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits, Suzhou (China) 2013, (pp.97-102)
[25] G. Schoof, M. Methfessel, and R. Kraemer, "Fault-tolerant ASIC design for high system dependability", In Proc. 13th International Forum on Advanced Microsystems for Automotive Applications, Berlin (Germany) 2009, (pp.369-382)
[26] V. Petrovic, M. Ilic, G. Schoof, and Z. Stamenkovic, "SEU and SET fault injection models for fault tolerant circuits", In Proc. 13th Biennial Baltic Electronics Conference, Tallinn (Estonia) 2012, (pp.73-76)
[27] http://www.synopsys.com/tools
[28] http://www.mentor.com/products
[29] http://www.cadence.com/products
[30] GnuWin packages, http://gnuwin32.sourceforge.net/packages.html