A New Protection Technique for Finite Impulse Response (FIR) Filters in the Presence of Soft Errors

P. Reyes[1], P. Reviriego[2], J.A. Maestro[1], O. Ruano[1]

[(1)] Universidad Antonio de Nebrija
Madrid, Spain
Email: {preyes, jmaestro,oruano}@nebrija.es

[(2)] Universidad Carlos III de Madrid
Madrid, Spain
Email: revirieg@it.uc3m.es

***Abstract* - Traditional techniques to protect digital circuits against soft errors normally result in a significant area and power overhead. Some of those techniques may also reduce the maximum frequency of operation of the circuit as they introduce additional delays in the critical paths. In this paper we propose a circuit specific technique to protect digital finite impulse response (FIR) filters from soft errors. The idea behind our approach is to use the knowledge of the structure of those filters to provide effective protection against soft errors with lower area and power overhead than that of traditional techniques, like Triple Modular Redundancy (TMR) and Error Detection and Correction (EDAC). The whole study will be focused on Space applications, since the problem of radiation is a key issue, using a soft error simulation platform implemented by the European Space Agency.**

I. INTRODUCTION

When a radiation particle strikes on a semiconductor device and it goes through the electric field region, it generates a large number of electron-hole pairs. If such an event occurs near the depletion region of a reverse biased p-n junction, the free carriers are efficiently collected, increasing the electric field across the mentioned junction. Therefore, a noise transient pulse is generated because of the current flowing through the device. When this transient pulse or soft error, known as Single Event Effect (SEE), occurs in or is registered by a storage element, it causes a functional or data result error in the circuit which is referred to as Single Event Upset (SEU) [1][2].

Moreover, as the microelectronic industry technology processes reduce the size of the devices, lower operation voltages are needed, and the reduction of the charge stored on the circuit nodes increases the failure rate of the semiconductor devices due to soft errors. The main reason for this is that under these circumstances, even low energy particles (which have a greater frequency of occurrence than the high energy ones) can cause upsets. Many application fields are affected by these phenomena, especially those where radiation is strongly present. The Space field, which has been the focus of this paper, is especially interesting due to its inherent constraints on performance, area and power [3].

Most soft errors occur in memory arrays, DRAM and SRAM cells, but with the reduction of device sizes, soft errors will be more related to Single Event Transient (SET) events [4][5] when using a 45nm technology.

To mitigate the effects of this kind of soft errors (SEEs), a number of techniques can be used at the physical level (device size and structure) [6]. In addition to those techniques, redundancy can be introduced in the design so that it can detect and correct SEEs [7]. To deal with SEUs, a common approach is Triple Modular Redundancy (TMR), which triplicates the flip-flops in the design and adds logic to vote in case of conflict. If SETs are also to be considered, Functional Triple Modular Redundancy (FTMR, which also triplicates the combinational logic) can be used [7].

Other general techniques to deal with SEUs by introducing redundancy are Error Detection and Correction (EDAC), like Hamming codes, where one encoder, one decoder and several additional registers to store redundancy are introduced in each register.

On the contrary, the approach to deal with SEUs presented in this paper is based on applying circuit specific techniques that exploit the inherent redundancy or fault tolerance of some circuits [8][9], what we call *to apply the system knowledge*. The advantage of this is the production of custom-tailored solutions for each family of circuits, with good protection levels and a quasi-optimal implementation, something that general techniques like TMR or Hamming coding cannot achieve.

Objectives. First, a new technique to protect FIR filters against SEUs will be presented. This technique will be put in perspective with other existing solutions, uncovering some weaknesses associated to these schemes. Afterwards, we will evaluate the proposed technique using a soft error simulation platform implemented by the European Space Agency [10][11]. Finally, the different approaches will be compared in terms of protection effectiveness, impact on the maximum operating speed of the circuit and area as figure of merit for complexity.

II. RELATED WORK

The problem of radiation on electronic devices has been traditionally addressed in literature.

This work was supported by the Spanish Ministry of Science and Education under Grant ESP-2006-04163.

A classic reference by J.F. Ziegler is offered in [12], where the basic physics of radiation effects is detailed. Different rates of errors at several terrestrial positions are described, providing a quantitative analysis of the radiation effects.

A reference that deals with a similar problem to the one stated in this paper is [13]. A formal solution is proposed in order to detect errors in linear digital state variable systems. The error propagation along the circuit paths is analyzed, and although the results are promising, nothing is said about the implementation cost of the solution.

One of the factors that measure the sensitivity of circuits to radiation is the error rate. Several works try to provide models for this error rate, in order to foresee the behavior of the circuit in a particular environment. A Soft Error Rate computation algorithm is presented in [14], which can be applied to combinational circuits. The parametric waveform model is based on the Weibull function. Experiments show that the algorithm is linear in the number of nodes, and results are close to SPICE simulations.

A methodology to compute the effects of charged particle inducing delay errors (Soft Delay Errors) is presented in [15]. The different node sensitivity is computed in order to employ node hardening techniques, and therefore, increase the reliability of CMOS circuits.

Techniques to detect and correct errors are very common too. The goal of such techniques is to mitigate the effects of radiation, both by detecting errors when they happen, and by trying to correct them, thus getting rid of the negative effect. In [16], the problem of Concurrent Error Detection (CED) is discussed in Burst-Mode machines. An enhanced duplication process is proposed in order to give a solution to this problem, showing an interesting saving in hardware.

A technique to minimize the impact of soft errors in circuits is presented in [17]. Through the use of complementary pass transistor devices, those gates affected by SEUs are isolated, and therefore their negative effect is removed. This is achieved with limited area, delay and power overheads.

In [18], the problem of sub-65nm designs is described. Since it is stated that classical fault-tolerance techniques for soft error detection are expensive, a recently developed Built-In-Soft-error-Resilience (BISER) technique is proposed, which seems effective for soft error blocking or detection.

III. Soft Error Protection Technique

Traditional techniques like Triple Modular Redundancy and Error Detection and Correction codes are usually employed to deal with SEUs in several application fields, like avionics, space and medical areas. This section describes conventional generic techniques, as well as the technique proposed in this paper.

A. Conventional techniques

Triple Modular Redundancy, TMR, enhances the fault tolerance of the target circuit by triplicating the storage elements (registers, flip-flops, memories…) and adding a voting logic that selects the majority value of each set of replicated storage units (See Figure 1).

Using TMR, the highest number of SEUs that the protected circuit can support in an n-bit register without errors in its behaviour would be n, providing that each SEU occurs in different bits of the register.

If two simultaneous SEUs occur on the same set of registers used to store and protect a single bit, the error is propagated and it can cause a functional/data failure.

If it is necessary to deal with SETs the use of Functional TMR, FTMR, which also triplicates the combinational logic, must be considered.

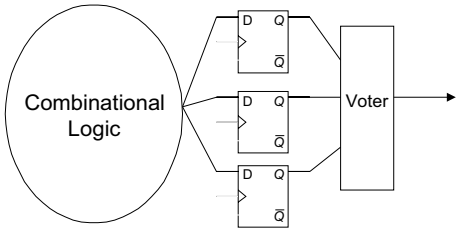

Figure 1. Illustration of TMR

Similarly, error detection and correction codes, sometimes referred as parity codes, could be used in place of TMR in order to protect the circuit against SEUs. One example are Hamming EDAC codes [19], which are named as *Hamming (n,k)* where *n* represents the number of bits of the coded word (the word with parity and data bits) and *k* is the number of data bits of the initial word, as it is illustrated in Figure 2.

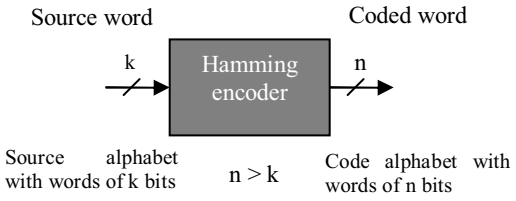

Figure 2. Hamming Encoder

The main properties of Hamming codes are that they can detect double errors and correct single errors (SEC-DED). The correction and detection capabilities are determined by different properties of the code, as the hamming distance. This kind of parity check codes has been recently used to protect FIR filters from the effects of SEUs [20].

There are many ways to protect FIR filters using Hamming codes. The most intuitive and effective one consists of adding one Hamming encoder and one decoder to each register of the electronic circuit. For an 8-bit width datapath, a (12,8) code would be needed, that implies 4 additional registers per tap plus one encoder and one decoder. However, the use of Hamming codes to protect FIR filters from the effects of soft errors has some drawbacks. First, the decoder of each register is in the critical path to the output and therefore it decreases the maximum frequency of operation of the circuit; and second, the area consumed in the case of using one encoder and decoder into each tap of the delay line can be higher than TMR in some cases, as reported in [20].

B. Knowledge-based Proposed Technique

It is clear that any protection mechanism added to a circuit will incur a higher area in exchange for its extra functionality. Traditional techniques, as the ones explained in the previous section, usually try to achieve this protection level focusing strictly on the circuit itself. However, the same circuit, implemented in different applications

and under different conditions, may require distinct protection levels. If, instead of always aiming at the same protection level, customer-tailored solutions are studied, taking the application and environment requirements into account, then the extra hardware added to achieve this protection will be minimal. This is what we call, in a generic way, to apply the *system knowledge*. Although this design philosophy can be extrapolated to any kind of circuit, the proposed technique (first introduced in our previous work [21]) will be applied to general FIR filters in this paper.

The motivation to study this kind of filters is their high presence in Space application, due to the importance of signal processing in this environment [3][22][23]. Because of this intensive use and the criticality of operations, a reliable protection against the effect of radiation is fundamental.

These filters consist of one set of shift registers interconnected, together with some adders and multipliers which performs a specific operation to the input signal represented by the next equation.

$$y[n] = \sum_{i=0}^{N-1} x[n-i] \cdot h[i] \qquad \text{(Eq.1)}$$

Two possible structures for FIR filter are depicted in Figure 3.

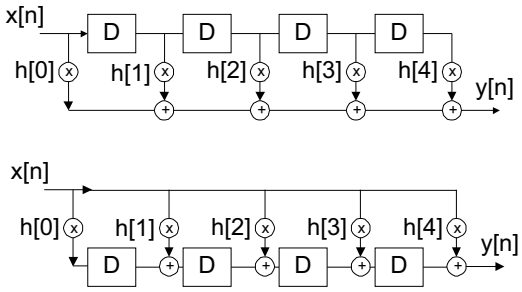

Figure 3. Different structures for FIR filters

The knowledge-based proposed technique represents one alternative to the use of TMR in all registers taking advantage of the fact that the registers for the FIR implementation are connected in such a way that their values do not suffer changes as they move across the delay line. This can be used to compute a two-dimensional parity as follows:

- For each input value, compute a parity bit, named Pv (vertical). This bit is stored with the input value and it moves across the delay line. So, an extra register to store the Pv bit per tap in the delay line is needed.
- For each bit position in the input value, compute another parity bit, known as Ph (horizontal), across all the bits that have that position on the registers of the delay line. Ph values are stored in another set of registers.

Pv is only computed once, when the input arrives and enters the delay line. However, Ph is updated every clock cycle with the bit of the new value entering the delay line and the one leaving it. These two sets, Pv and Ph, form the accumulated parity of the circuit, which is constantly being updated (See Figure 4).

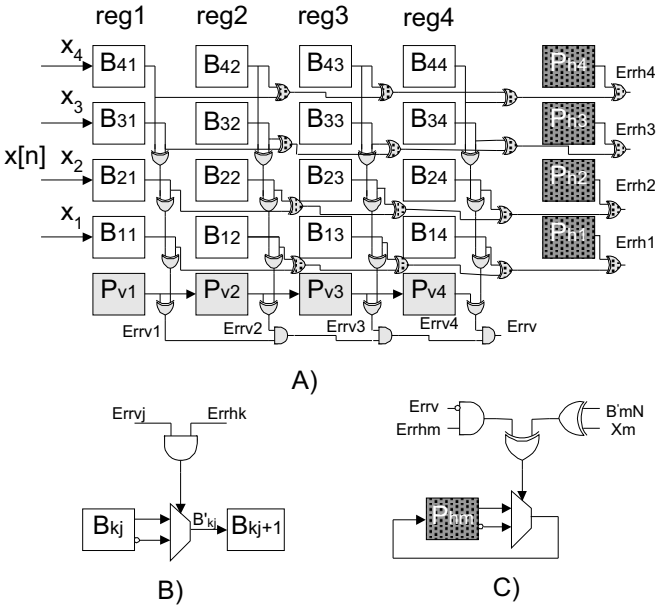

Figure 4. Proposed Implementation for protection against SEUs in FIR structures

For the example shown in Figure 4, with an input word of four bits and four taps in the delay line, sixteen one-bit registers to store data bits would be needed, plus eight more single registers, four to store Pv parity bits and other four for Ph parity bits.

Dynamically, each time a new value reaches the circuit, both the horizontal and vertical parity are re-checked and compared with the accumulated values.

Notice that the added Ph and Pv bits may also be affected by SEUs, and therefore, they should also be protected from them. Taking this into account, several situations can arise. The possible errors could be classified into single SEUs events (only one bit-flip per cycle), and multiple SEUs ones (more than one bit-flip per cycle):

1. No errors. The actual and accumulated values are the same. There is no problem with the system and its behavior can be taken as correct.

2. Single SEU. Three scenarios:
   a) There is a discrepancy between a bit of the accumulated and actual Ph and between a bit of the accumulated and actual Pv. If both differences happen, that means a SEU has affected a register in the delay line, specifically, the bit located at the crossing point of the mentioned Ph and Pv (see correcting logic in Figure 4B).
   b) There is a discrepancy between a bit of the stored and actual Ph value, but the accumulated and actual Pv bits are identical. If this happens, the SEU has occurred in the stored Ph that is discrepant, and should be corrected (see correcting logic in Figure 4C).
   c) Same situation as the previous one but the discrepancy is in Pv (while Ph remains correct). Then, the SEU has affected that Pv. In this case, the Pv bit is not corrected, since this value will be shifted out of the delay line (together with the data bits), and the cost overhead incurred by the correcting logic can be saved. However, if while that Pv error is present, another SEU causes a

different error in a given Ph (producing a 2.b scenario), the combination of both events will confuse the system into a false 2.a scenario, triggering a wrong data correction. Nevertheless, considering the very low probability of such consecutive SEUs, this risk is acceptable if compared to the savings in correcting logic.

3. Multiple SEUs (some non-exhaustive scenarios):
   a) There is a discrepancy between a bit of the accumulated and actual Ph and between a bit of the accumulated and actual Pv. If both differences happen and simultaneous SEUs have occurred, that means that, probably, soft errors have affected the Ph and Pv discrepant registers.
   b) There is a discrepancy between more than one bit of the stored and actual Ph value, but the accumulated and actual Pv bits are identical. Then:
      i. If the number of discrepant Ph bits is odd, the errors have occurred over several data bits and at least over one Pv bit.
      ii. If the number of discrepant Ph bits is even, the errors have occurred over several data bits.
   c) There are differences between more than one bit of the accumulated and actual Pv, but the Ph bits have no discrepancy. In this case, the error situations could be the same as in the previous case.
   d) If there is a discrepancy between an odd number of bits of the accumulated and actual Ph and between only one bit of the accumulated and actual Pv, the same odd number of SEUs has occurred over the different bit positions into the same four-bit data register of the delay line.
   e) If there is a discrepancy between an odd number of bits of the accumulated and actual Pv and between only one bit of the accumulated and actual Ph, the situation is reciprocal to the previous case.
   f) If there is a discrepancy between two or more bits of the accumulated and actual Pv and between two or more bits of the accumulated and actual Ph, there is no way to determine univocally where the errors have happened.

All the previous double errors in data bits are never corrected, because they are not univocally located. This is not a major drawback, due to some reasons:

- The probability of multiple (simultaneous) SEUs is reasonably low, as stated in several research sources, as [24]. This means that the number of uncorrected error will also be low.
- No technique is 100% safe against multiple SEUs. For example TMR could suffer as much as the other techniques, as the redundant flip-flops would normally be close together, and therefore, if a double SEU happens, it is likely that two of the three TMR voters in a single bit are the affected ones.

Another different problem of this technique, which is also presented when using Hamming codes, is the extra addition of combinational logic to the critical path that increases its delay, reducing the maximum operation frequency of the protected circuit. An interesting question is related to what happens if the error correction is active so late in the clock cycle, that correction cannot take place in time, and the error is propagated to the next stage of the delay line. This implies a time percentage of the clock cycle when the system is vulnerable to the error propagation. Next section includes explanations to these considerations.

IV. Experimental Results

In this section, the three protection techniques (TMR, Hamming codes and the proposed one) will be studied, in terms of area, protection effectiveness and critical path vulnerability. These techniques have been implemented in VHDL and then synthesized for a commercial ASIC library. Three experiments have been carried out on the circuits:

1. Using a simulation platform*, several SEUs campaigns have been inserted, and the effectiveness of the protection techniques has been put in perspective.
2. The circuits have been synthesized, and their complexity has been compared.
3. Study of the vulnerability that could cause error propagation in the delay line for the proposed technique and Hamming.

In this way, the quality of the proposed techniques is both measured in effectiveness and complexity.

The circuit chosen for the comparison process of the examined techniques to deal with the soft errors that generate bit flips in storage elements is the low pass FIR filter evaluated in [20]. The coefficient values for this specific filter in the Eq.1 are:

$$h[n] = [-1 \quad 24 \quad 50 \quad 50 \quad 24 \quad -1] \qquad \text{(Eq.2)}$$

The selected FIR filter has simple and symmetric coefficients, what reduces the complexity of multipliers (they are optimized to multiply constant values) and allows sharing them between taps of the delay line. Moreover, this structure is generic enough to consider the extracted results of the study as general conclusions about the compared techniques, considering general FIR implementations.

Figure 5 shows the structure of the low pass FIR filter used in the experimental process.

In all the experiments, 8-bit input and output signals, x[n] and y[n], are considered. In the case of Hamming, the code used was (12,8).

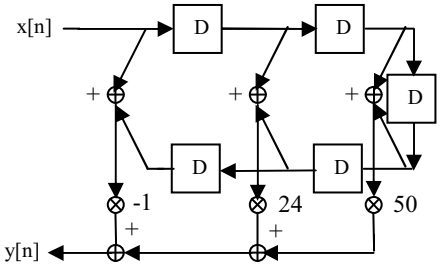

Figure 5. Low pass FIR filter structure

*This simulation platform has been built in order to easily simulate SEUs in circuits. It uses Modelsim to hold the VHDL description of the circuit, Matlab to generate the reference input and output signals (which are compared with the actual behavior of the system to determine its correctness), and the Single Event Upset Simulation Tool (SST) developed at the European Space Agency [10] to insert SEUs and study the response of the circuit. A detailed description of this platform can be found in [11].

A. Effectiveness

From the whole set of test scenarios, particular cases have been chosen for all the compared techniques, in order to evaluate the behavior of the system.

First, a random input sequence of 15.000 samples formed by pulses plus noise have been generated through Matlab, and then several sequences of 100 SEUs in random time instants have been inserted into the different techniques. These instants were selected using an equally distributed probability function, with the particularity that the maximum number of bit flips that can occur during each clock cycle is one.

Results of these tests on the three protection techniques, show the same conclusions: the three techniques are totally effective against single SEUs (no errors propagated to the output).

B. Complexity

In order to compare the complexity of the knowledge-based proposed technique with TMR and Hamming codes, the three systems have been synthesized. The area results in equivalent gates (see Table I) have been generated for a TSMC 0.25um library using Leonardo (by Mentor), assuming a 50 MHz clock and an 8-bit datapath.

As it can be seen in the table below, the proposed technique is the one with less area cost, followed by the Hamming protection methodology.

TABLE I

COMPARISON OF TMR AND HAMMING WITH THE PROPOSED TECHNIQUE FOR A SIX-COEFFICIENT FILTER

FIR WITH 6 TAPS	Frequency	Gates	DFFs
FIR with TMR	117.1	1704	168
FIR with Hamming	105.5	1476	80
FIR using system knowledge	104	**1363**	70
FIR without redundancy	137.8	791	56

The area overhead can be extrapolated for a FIR filter with more than six taps. If the number of taps is ten, the increment of area for the three techniques is illustrated in Table II. In this case, the coefficients for the FIR filter with ten multipliers are shown in Eq.3.

$$h[n] = [-1\ 3\ 50\ 64\ 96\ 96\ 64\ 50\ 3\ -1] \qquad \text{(Eq.3)}$$

TABLE II

COMPARISON OF TMR AND HAMMING WITH THE PROPOSED TECHNIQUE FOR A TEN-COEFFICIENT FILTER

FIR WITH 10 TAPS	Frequency	Gates	DFFs
FIR with Hamming	94.6	2405	128
FIR with TMR	104.2	2619	264
FIR using system knowledge	90.4	**2114**	106
FIR without redundancy	114.4	1279	88

Again, the proposed technique has the lowest area cost, what implies that it is scalable as the size of the filter grows.

C. Vulnerability

Another interesting issue related to the correction logic of the proposed technique and Hamming consists of the time that the logic needs to execute the correction. Due to the extra combinational logic added, if the correction comes so late in the cycle, the error will not be corrected, and it will go through the delay line.

Let us define the vulnerability of the technique as the percentage of the cycle when a sudden error is not corrected, due to the time issues defined before. In this way, if e.g. the vulnerability is 25%, that means that a SEU would be corrected during the first 75% of the cycle time, but it will be propagated to the next stage if it happens in the last 25%. Obviously, the lower the vulnerability is, the better. Table III shows the results after comparing the vulnerability of the proposed technique and Hamming, by performing an analysis on the critical paths. Two experiments have been conducted, with frequencies of 10 MHz and 100MHz. As it can be seen in this table, the vulnerability is worse for Hamming codes than for the proposed technique.

TABLE III

VULNERABILITY OF HAMMING AND THE PROPOSED TECHNIQUE DUE TO EXTRA LOGIC IN THE CRITICAL PATH

Frequency (MHz)	FIR with Hamming	FIR using system knowledge
100	21%	14%
10	2.1%	1.4%

Finally, to conclude the section, a summary of all the conducted experiments in this paper is offered in Table IV. This allows a quick comparison of the three techniques for area, effectiveness and vulnerability.

TABLE IV

FINAL COMPARISON

	Total area	Effectiveness	Delay
TMR	High	**Good**	N/A
Hamming	Average	**Good**	Average
Proposed Technique	**Best**	**Good**	**Good**

V. CONCLUSIONS AND FUTURE WORK

In this paper, a new protection technique for FIR filters has been presented. Several experiments have been conducted in order to compare this technique with TMR and Hamming codes. It has been showed that the new technique, while providing a similar protection level to the others, incurs a lower area overhead, what makes it more convenient.

The following topics will be considered in future works:

- Extension of the proposed knowledge-based technique to work with other kinds of digital structures. A more general methodology will be presented in order to prove the convenience of the knowledge-based approach for non-specific circuits. A study of the 8051 microcontroller is under way.
- Study of detailed modeling of soft errors generated by radiation in space. An extension of the current methodology to deal with SETs will be provided.
- Study of several statistical functions to foresee soft errors rates in different environments. In this way, a proper modeling of Space applications will be achieved.

REFERENCES

[1] D. Schrimpf, D.M. Fleetwood, "Radiation effects and soft errors in integrated circuits and electronic devices", World Scientific Publishing, 2004.

[2] P. E. Dodd, LL. Massengill, "Basic Mechanisms and Modeling of Single-Event Upset in Digital Microelectronics", IEEE Trans. on Nuclear Science, Vol 50, No 3, June 2003.

[3] E. R. Prado, J. P. Prewitt, "A High Performance COTS based Vector Processor for Space", Military and Aerospace Applications of Programmable Devices and Technologies Conference, 1999 (MAPLD '99).

[4] R. R. Rao, K. Chopra, D. Blaauw, D. Silvestre, "An Efficient Static Algorithm for Computing Soft Error Rates of Combinational Circuits", DATE 2006.

[5] U. Krautz, "Evaluating Coverage of Error Detection Logic for Soft Errors using Formal Methods", DATE 2006.

[6] M. P. Baze, S. P. Buchner, D. McMorrow, "A Digital CMOS Technique for SEU Hardening", IEEE Trans. on Nuclear Science, Vol 47, No 6, December 2000.

[7] S. Hanbic, "FTMR: Functional Triple Modular Redundancy", ESA Report FPGA-003-001, December 2002.

[8] B. Shim, N.R Shanbhag, S. Lee, "Energy-efficient soft error-tolerant digital signal processing", Signals, Systems and Computers, Conference Record of the Thirty-Seventh Asilomar, Nov. 2003.

[9] A. Reddy, P. Banarjee, "Algorithm-based fault detection for signal processing applications", IEEE Trans. on Computers Volume 39, Issue 10, Oct. 1990.

[10] D. Gonzalez-Gutierrez, "Single Even Upset Simulation Tool Functional Description", ESA Report TEC-EDM/DCC-SST2, July 2004.

[11] Computer Architecture and Technology Group Web Page, Universidad Antonio de Nebrija. Available: http://www.nebrija.es/~jmaestro/esa

[12] J.F. Ziegler, "Terrestrial cosmic rays", IBM Journal of Research and Development, vol 40, #1, 1996.

[13] A. Chatterjee, M. A. d'Abreu, "The Design of Fault-Tolerant Linear Digital State Variable Systems: Theory and Techniques", IEEE Transactions On Computers, Vol. 42, No. 7, July 1993.

[14] R.R. Rao, K. Chopra, D. Blaauw, D. Sylvester, "An Efficient Static Algorithm for Computing the Soft Error Rates of Combinational Circuits", Proceedings of Design Automation and Test Conference, 2006.

[15] B. S. Gill, C. Papachristou, F. G. Wolff, "Soft Delay Error Analysis in Logic Circuits", Proceedings of Design Automation and Test Conference, 2006.

[16] S. Almukhaizim, Y. Makris, "Concurrent Error Detection in Asynchronous Burst-Mode Controllers", Proceedings of Design Automation and Test Conference, 2005.

[17] J. Kumar, M.B. Tahoori, "Use of pass transistor logic to minimize the impact of soft errors in combinational circuits", Workshop on System Effects of Logic Soft Errors (SELSE), 2005.

[18] S. Mitra, T. Karnik, N. Seifert, M. Zhang, "Logic Soft Errors in Sub-65nm Technologies Design and CAD Challenges", Proceedings of Design Automation Conference, 2005.

[19] P. Sweeny, "Error control coding, from theory to practice", John Wiley and Sons, 2002.

[20] R. Hentschke et al., "Analyzing area and performance penalty of protecting different digital modules with Hamming code and triple modular redundancy", Integrated Circuits and Systems Design, 2002.

[21] P. Reyes, P. Reviriego, J.A. Maestro and O. Ruano "New Protection Techniques against SEUs for Moving Average Filters in a Radiation Environment", IEEE Transactions on Nuclear Science, 2007 (in press).

[22] C. Lambert-Nebout, G. Moury, "On-Board Digital Signal Processing for IASI Mission", 6th International Workshop on Digital Signal Processing Techniques for Space Applications, Noordwijk, The Netherlands, September 1998.

[23] S.M. Parkes, "DSP (Demanding Space-based Processing!): the Path Behind and the Road Ahead", 6th International Workshop on Digital Signal Processing Techniques for Space Applications, Noordwijk, The Netherlands, September 1998.

[24] H.C. Koons et al., "The Impact of the Space Environment on Space Systems", Space and Missile Systems Center - Air Force Materiel Command, Report No. TR-99(1670)-1, July 1999.