VULNERABILITY STUDY OF EMBEDDED CIRCUITS TO SPACE RADIATIONS SINGLE EVENT PHENOMENA

S. KAROUI
USTO, University of Sciences and Technology of Oran (Algeria)
P.O. Box 1505 El M'naouer, Oran, Algeria
Tel: 0021341560329
Fax: 0021341560329
Email: sd_karoui@yahoo.com

Abstract:
The radiations in space environment with can induce failures disturbing the functionalities of the space applications embedded VLSI circuit. None means of prevention provide a total immunity. A solution consists to study and predict the sensitivity of components to be used in such applications, with an aim of choosing the least sensitive circuits. The objective of this work is to present a global methodology of heavy ions testing as well as obtained results for various VLSI circuits.

Keys Words:
Space environment / Heavy Ions / Upset / SEP Phenomenon / Functional Testers.

Résumé :
Les systèmes digitaux embarqués à bord d'applications spatiales sont constamment soumis aux radiations spatiales induisant des dégradations pouvant affecter les fonctionnalités de ces circuits. Aucun moyen de prévention ne permet a priori une immunité totale. Une première solution consiste donc à étudier et prédire la sensibilité, aux effets singuliers, des composants susceptibles d'être utilisés, ceci dans le but de choisir les circuits les moins sensibles. L'objectif de ce travail est de présenter une méthodologie globale pour la réalisation de tests aux ions lourds ainsi que des résultats obtenus pour différents circuits.

Mots clés :
L'environnement spatial / ions lourds / basculement de point mémoire / effets singuliers / Testeurs fonctionnels.

1. Introduction

The space radiations interact with the electronics components of the digital systems embedded on space board applications according to known rules of physics, resulting in effects such as: excitations, ionizations, displacements of atoms and by consequence by electric deposits of charges. These charges can induce transient or permanent degradations such as [1]:

- background noise,
- effect of accumulated dose: a accumulation of charge at the glassivation layers causing drifts and degradation of the characteristics and thus a permanent loss of functionality,
- singular effects, SEP ("Single Event Phenomena") due to radiations of high energies.

The singular effects are located phenomena, i.e. started by the channel of ions in sensitive areas of the circuit. So that the singular effect takes place, the charge deposited must be higher than a breaking value (critical charge), which implies that the radiation has a LET (transfer of energy per unit of length) higher than a threshold value. The singular effects are of several types:

- burnout, is creation and the breakdown of a way slightly resistive between the grid and the substrate of a FET transistor, the components sensitive to this phenomenon are transistors power MOSFET and NMOS structures.
- snapback is a locking of a N type FET transistor. This locking is the consequence of an avalanche current in the drain due to the presence of a parasitic bipolar transistor.
- latch up: activation of a parasitic structure PNPN in a CMOS bulk component. The continuance of a conduction of this structure can lead to a thermal destruction of the component. This problem can be avoided by use of a substrate insulating (Silicon-one-Saphire for example).
- upset: inopportune modification (flip) of the information stored in a memory element. The consequences of this phenomenon depend on the quality of modified information [2] [3]; its random nature (as well in the moment as in the place of occurrence) makes it critical.

Various means of prevention such shielding, the use of hardened components, the detection and the correction of errors, the redundancy, can be employed to deal with the effect induced by the space environment on the digital systems. None of these means, which can be expensive and/or bulky, does not allow a total immunity if we consider the upset phenomenon.

A first solution thus consists to study and predict the sensitivity to the upsets

components to be used, starting from a simulation on the ground, this with an aim of choosing the least vulnerable circuits.

Setting up such a test raises the following problems:

- The simulation of the authentic environment if necessary,
- The generation of the test stimuli,
- The application of test stimuli to the circuit to be tested and the evaluation of results, by means of a suitable test system,

In the case of vulnerability studies for circuits devoted to operate in harsh conditions, the simulation of the authentic environment becomes mandatory. The DUT (Device Under Test) is placed in an adequate chamber (a vacuum chamber if needed), where it is submitted to the environment constraints (radiation, temperature cycles, etc.). To protect the test system, the connection between the DUT and the system should be realized by a shielded cable (Fig. 1).

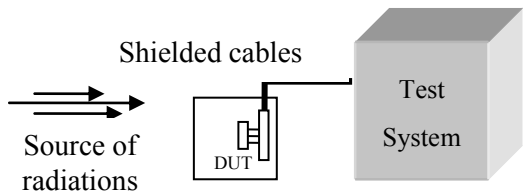

Figure 1: Set up for vulnerability studies in harsh conditions

2. Test system design

Concerning the test system design, different approaches have been proposed [4][5]. They can be distinguished by the methods used for the test stimuli application and the response evaluation.

2.1. Stimuli application

The application of the test stimuli can be realized according to two principles:
- *Dominated control*: the stimuli are stored in the tester memory as binary values. The tester converts them to electrical signals and separately applies them at the DUT inputs. The sequencing of these stimuli is totally controlled by the tester (it emulates the environment needed for the DUT operation). When the DUT is a microprocessor, the tester provides the data and instructions at the proper timing.
- *Assisted control*: the DUT is in a "natural" environment, the stimuli are stored in the tester memory as a sequence of instructions (object code). To apply the stimuli, these instructions are executed by the DUT itself (if it is a microprocessor) or by an associated microprocessor (if the DUT is other than a microprocessor). The DUT, or its associated microprocessor, accedes normally to the tester memory to fetch data and instructions.

2.2. Response evaluation

The evaluation of the DUT responses is made by comparison to a reference. Two solutions frequently used are:

- *Well-known responses*: the reference values are established before the test, either by the application of the test stimuli to a "good" circuit or by simulation or computation.
- *Golden chip method*: the reference values are the output responses of a "good" chip (or an emulator) receiving the same stimulus as the DUT.

2.3. Choice of a test system

Testers implementing the *dominated control* strategy allow performing efficient parametric and logic tests for all kind of circuit types. Commercially available testers are generally designed using this strategy. Nevertheless, using these testers requires a precise analysis of the DUT timings to prepare the test sequences and to analyze the responses when a precise diagnosis is looked for. Moreover this strategy leads to bulky equipment.

An *assisted control* strategy allows working in microprocessor native languages. The test writer can think more naturally and efficiently. The test meaning is clearer to others who may need to understand, modify or make additions to the test program. It leads to low cost, compact and portable test equipment. Nevertheless a specific interface board has to be developed for every new DUT.
Concerning the response evaluation, the use of the *golden chip* method needs complicated hardware developments (comparators, tri-states encoding, etc.) particularly to enable the comparison only when the signals are stable. Moreover the reference must have a high quality, to avoid uncovering of a similar design or masking flaw in both the reference and the DUT.
As the *well-known responses* can be correctly established (emulation for instance) and easily modified if it is needed, the *well-known responses* strategy is generally preferred.

We have designed and realized a tester, the FUTE16 system, according to the DUT *assisted control strategy with well-known response evaluation.*

The FUTE16 tester (Functional/Upset TEster) [6], has been developed with the collaboration of the French Space Agency (CNES), to cope with both functional tests and vulnerability studies against radiation in space environment.

2.4. Test system architecture

The architecture of FUTE16 is organized around a VME bus.

A specific interface board has to be realized for every new DUT. Its function is to produce a DUT minimum environment, to adjust the DUT signals timing to those of the memory and to allow the handshake between the DUT and the CPU, through a parallel I/O port.

Different mechanisms (watch-dog, address control, illegal op-code detection, etc.) have been implemented to detect some critical errors.

2.5. Operation principle

The test program is written in a high level language on the host, the obtained object code is transmitted to the tester's mass-memories. The object code is then downloaded at the tester RAM. Test stimuli application is achieved by the execution of the test program by the DUT (or the associated microprocessor) after an assertion of the "reset" signal by the CPU via the PIO. During the test program execution, the test results are stored in the tester RAM. A "test end" signal is then sent by the DUT to the CPU via the PIO. Finally, to detect the errors the CPU compares the obtained results to predetermined reference values.

Various hardware and software mechanisms allowing the detection of different error types produced by the heavy-ion beam have been implemented:

- a programmable *watch-dog*, that triggers when the device under test looses its normal program sequencing.
- an *address decoder*, which allows to control the DUT access to the different tester memory areas. If addressing errors occur, this circuit activates a specific DUT input signal that will start the execution of an exception routine (writing an associated message in the tester memory).
- specific internal mechanisms of the DUT have been used for error detection and diagnosis purposes.

In order to protect the DUT against latch-up risk and to determine the latch-up rate, the DUT current consumption should be permanently controlled.

2.6. Test monitor program

The monitor program, written in C language, takes over the control and the management of all operations related to the test as well as the user interface. The user interface allows an easy manipulation of the machine. It is realized by a high-level commands organized as a hierarchical system menus.

2.7. Main features

The features of tester can be summarized as follow:

- Universality: it allows testing almost all digital circuit types (processors, peripherals, memories, etc.).
- Portability: it is autonomous, compact, and monitored by a terminal or a PC compatible.
- Flexibility: a specific board is to be realized for each new DUT, the test program can be developed on the tester

directly as an object code file or in a high level language on a host (PC computer).
- Low cost.

3. The simulation of the environment

Data presented in this paper has been obtained using three different irradiation facilities:

- The Tandem Van de Graaff heavy-ion accelerator of the IPN (Orsay, France). We have used beams of carbone, fluorine, chlorine and nickel. Effective LETs values ranging from 1.7 to 64 Mev/mg/cm2 were obtained by varying the beam incidence angle (Table1).

$$LET_{eff} = \frac{LET_i}{\cos \theta_i} \qquad (1)$$

- A Californium 252 fission-decay source equipment, developed by the CERT/DERTS (Toulouse, France) [5].

Ion	Energy (MeV)	LET ($MeVmg^{-1}cm^2$)
12C	84	1.7
19F	111	4.0
35Cl	153	12.7
58Ni	179	27.0

Table 1: Accelerator ion energies and LET

4. The generation of the test stimuli

The strategy to characterize the vulnerability of a circuit in an irradiative environment is the ground simulation. It consists of exposing the DUT circuit, while it executes a test sequence, to a radiation close to that of the final environment.
Because of the complexity of current microprocessors, designing and performing SEU tests on them has become a non trivial task. As different programs activate in a different way the sensitive parts of a given processor, the total upset cross-section will strongly depend on the test program executed. Therefore, there is no standard way to test microprocessors and no absolute value for the SEU cross-section.

An accurate method to evaluate the upset sensitivity of microprocessors, that take into account the structure of the final application program, has been proposed in [7]. For each of the memory elements the upset sensitivity is first calculated by means of an appropriate program enumerating the bit flips occurring during the irradiation. For each of these memory elements is then determined a "duty factor" representing the period, for the considered program, in which the element is vulnerable to upsets. The global sensitivity is finally computed from the individual sensitivities and duty factors. The duty factors cannot be readily evaluated due to the complexity and the unavailability at the SEU test stage, of software used in space applications. So this approach is quite difficult to be used in the practice.

Published data on the upset sensitivity of various processors [8][9][10] has been generally obtained from irradiation experiments in which the test program executed by the DUT consists of checking sequentially in a continuous loop until an error is detected, each of the sensitive memory element accessible to the user. Typically considered memory elements are: general purpose registers, special registers such as the stack pointer and the status register, the internal Ram… Such test programs, called here "register test programs".

5. Obtained results

The setup was used to test several circuits. The Motorola MC68020 microprocessor and the floating point units MC68881 and 68882, the Sparc MHS90C601 and 602, the Idt R3000 and 3010, and finally the transputer Inmos T805.

The obtained upset and latch up cross sections using the Tandem heavy ions accelerator, are plotted in Figure 2 and Figure 3. The cache of the MC68020 is disabled. The cross sections obtained by means of the Californium fission-decay source equipment are presented in Table 2. The cache of the MC68020 is disabled.

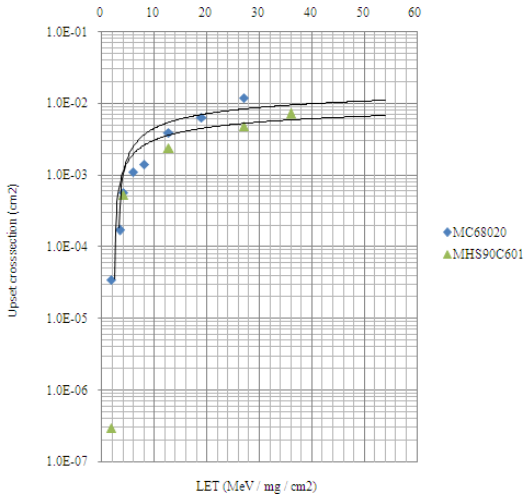

Figure 2: Upset cross sections

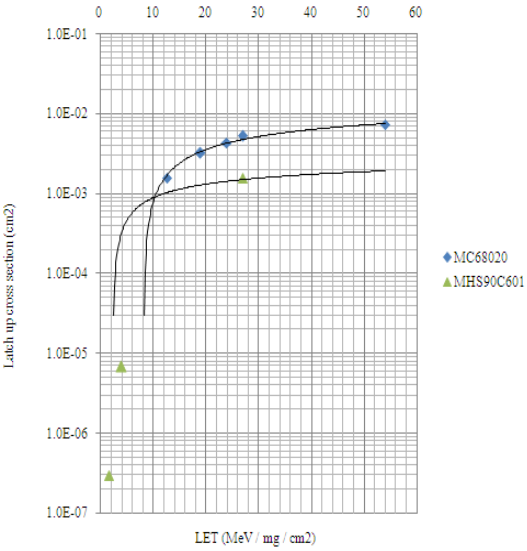

Figure 3: Latch up cross sections

DUT	σL (cm^2)	σU (cm^2)
MC68020	6.2E-04	5.1E-03
MC68882	8.5E-05	1.9E-03
MC68881	8.4E-04	4.3E-03
IdtR3000	-	6.1E-04
IdtR3010	-	6.1E-04
Inmos T805	-	1.4E-02
MHS90C601	5.5E-05	2.5E-03
MHS90C602	1.1E-04	7.0E-04

Table 2: Californium test results

6. Conclusions

This study has allowed us to validate the experimental test setup for protons and heavy ions testing. The vulnerability of various VLSI circuits was completely evaluated. The obtained results are comparable to the presented data on the similar circuits [11] and [12].

We should note also the flexibility and the versatility of the developed tester used to perform functional testing of integrated circuits [13].

Despite the larger number of tested memory points of the SPARC601 processor, estimated to 4352, compared to the MC68020 with only 480 points. The SPARC601 appears as less vulnerable to the upset phenomenon than the 68020.

The SPARC601 has a latch up saturation cross section bit smaller to the one of the MC68020 but has a LET threshold smaller. It seems to be more sensitive to the latch up phenomenon.

The discrepancies between the Californium 252 data and the accelerator data could be explained by a weaker penetration depth of the ions produced with the Californium (i.e. limited funneling). The extrapolated equivalent LET from the heavy ions cross section is around 15 Mev / mg /cm2.

These circuits are sensitive to the upset and latch up effects. The use of such circuits for space applications involve the use of means of prevention techniques such shielding, the use of hardened components, the detection and the correction of errors, the redundancy, to reduce those effects.

REFERENCES

[1] S. Karoui, "*Etude du comportement de circuits complexes en environnement radiatif spatial*", Thèse de Docteur INPG, Grenoble, December 1993.

[2] D. Binder, E. C. Smith and A. B. Holman, "*Satellites anomalies from galactic cosmic rays*", IEEE TNS, Vol. 32, December 1975.

[3] C. S. Guenzer, A. B. Campbell and P. Shapiro, "*Single event upsets in NMOS microprocessors and logic devices*", IEEE TNS, Vol. 32, December 1981.

[4] R. Koga, W. A. Kolasinski, M. T. Marra and W. A. Hanna, "*Techniques of microprocessors testing and SEU rate prediction*", IEEE TNS, Vol. 32, December 1985.

[5] R. Huston, "*Microprocessor testing: a testing turnaround - smart DUT runs the tester*", Fairchild Systems, Technical Bulletin, n° 5, 1975.

[6] S. Karoui and al, "*Design and development of the FUTE16 tester*", LGI Final Report of Grant (1990).

[7] H. Elder and al, "*A method for characterizing a microprocessor's*

vulnerability to SEU", IEEE TNS, Vol. 35, No. 6, December 1988.

[8] J. Cusik and al, "*SEU vulnerability of the ZILOG Z-80 and NSC-800 microprocessors*", IEEE TNS, Vol. 32, No. 6, December 1985.

[9] R. H. Sorensen and al, "*The SEU risk assessment of the Z80, 8086 and 80C86 microprocessors intended for use in low altitude polar orbit*", IEEE TNS, Vol. 32, No. 6, December 1986.

[10] R. Koga and al, "*Heavy-ion induced upsets of microcircuits: a summary of the Aerospace Corporation test data*", IEEE TNS, Vol. 32, No. 6, December 1984.

[11] "*SEU test of Motorola 68020 Microprocessor*", COL/TREP/0034/SAAB, July 1988.

[12] R. H. Sorensen and A. T. Sund, "*Radiations pre-screnning of R3000/R3000A Microprocessors*", IEEE Radiation Effects Data Workshop, July 1992.

[13] B. Martinet and al, "*Laser injection of spot defects on integrated circuits*", Asian Test Symposium, Hirochima, Japan November 1992.