

A NEW METHODOLOGY FOR THE SIMULATION OF SOFT ERRORS  
ON MICROPROCESSORS : A CASE STUDY

S. REZGUI, R. VELAZCO,

TIMA Laboratory  
46, Av. Félix Viallet  
38031 Grenoble (France)

R. ECOFFET  
CNES

18, av. Edouard Belin  
31055 Toulouse (France)

S. RODRÍGUEZ

INTA  
Torrejón de Ardoz 28850 (Spain)

*Abstract*

*This paper presents a new methodology for the simulation of soft errors on digital architectures. Bit flips are injected, concurrently with the execution of a program, on potentially sensitive memory locations. Result analysis of the soft error injection on a board based on a 68332 processor will illustrate the potentialities of this new method.*

Contact Author:

S. Rezgui

E-mail: sana.rezgui@imag.fr

Phone: +33 4 76 57 46 26

Fax: +33 4 76 47 38 14

If accepted, the authors wish to have the paper published at peer-reviewed publication and oral presentation.

This paper could be included in one of these sessions:

- Radiation Effects, Device Reliability and Element Characteristics
- Use of COTS Devices in the Military and Spaceflight Environment
- Aeronautics and Space Applications
- Advanced Devices, Technologies, and Software and Their Impact on Critical System Reliability

# A NEW METHODOLOGY FOR THE SIMULATION OF SOFT ERRORS ON MICROPROCESSORS : A CASE STUDY

S. REZGUI, R. VELAZCO,  
TIMA Laboratory  
46, Av. Félix Viallet  
38031 Grenoble (France)

R. ECOFFET  
CNES  
18, av. Edouard Belin  
31055 Toulouse (France)

S. RODRÍGUEZ  
INTA  
Torrejón de Ardoz  
28850 (Spain)

## ABSTRACT

Radiation effects on processors is a major concern with reduction of transistors features. Among these effects, bitflips resulting from the ionization from the charged particles hitting the circuit are considered critical owing to their random occurrence. These effects, called Single Event Effect (SEU), constitute a serious threat to the reliability of digital equipment built on advanced circuits. The increasing demand of high reliable embedded-systems (spacecraft, satellites, avionics, automotive control...) requires more studies of the behavior of microprocessors-based boards under radiations. The observability of this behavior involves the description of the operating of the microprocessor facing faults. Since the mean time between faults in radiation environment is long and ground tests expensive, several techniques of fault injection have been investigated to evaluate the error rate of different applications.

This work presents a strategy allowing to characterize and to quantify the effects of upsets on the operation of microprocessor-based digital architectures. The approach relies on the injection of transient bitflips, randomly in time and location, concurrently with the execution of a program. This can be achieved with minimal "intrusiveness" by software/hardware means, using the interruption mechanism. In fact, implementing this method, suppose that the tested application is a processor-based electronic board, organized around a device capable to execute instruction sequences and take into account asynchronous signals (interruptions). The key idea is the generation and storage at an appropriate memory address, of a piece of code, called here *CEU (Code Emulating an Upset)*, whose execution will provoke the content inversion of the selected bit, called *CEU target*. If the processor is properly configured the CEU code execution can be triggered by the assertion of an interrupt-like signal. The interruption activation instant and the CEU target can be pseudo-randomly chosen by an ad-hoc external mechanism. In this way, bitflips may be injected in all accessible processor's CEU targets (internal registers and SRAM memory area) as well as in the external SRAM where program data and code is stored. A particular effort was done to extend the approach to critical registers (program counter, stack pointer, status registers...). It is important to note that the CEU code may include instruction sequences to read, modify and overwrite, values stored in the stack. This makes it possible to inject CEUs on PC and other context registers, sometimes not directly accessible by the instruction set.

Advantages of the proposal fault injection strategy are the reduced intrusiveness in the system, the low-cost, the possibilities of automatization and the flexibility of the model in terms that several modules can be migrated on other tests of different processors. Nevertheless, must be mentioned two limitations of the CEU injection approach: (a) as interruptions are always taken into account at predetermined fixed instants, the effects of SEUs occurring during instruction execution are not possible to be simulated, (b) not all possible upset sensitive targets can be upset. In spite of these limitations, we assume that the performances of modern processors and their huge internal memory space, make the accessible area represent a significant percent of the total sensitive area, giving some representativity to the results of the proposed fault injection approach.

Implementing the proposed fault injection approach needs an extra hardware to load the memory with data corresponding to the desired CEU code, to trigger the interrupt signal, and to compare the program execution time and outputs to expected values. The architecture of a dedicated test system, called THESIC (Testbed for Harsh Environment Studies on Integrated Circuits) that we developed as a platform for SEU ground testing purposes [1], offered a suitable platform for the CEU injection. Indeed THESIC is organized in two boards, a motherboard for control of testing operation and user interface, and a daughterboard for the adaptation of the device under test (DUT) to the motherboard bus protocol. The communication between the two boards is achieved in asynchronous way through a common memory, called MMI (Memory Mapped Interface). Typically, during a test the DUT indicates by an interruption when the MMI area has data to be transferred to motherboard. When this happens, the motherboard interrupts the DUT board to read the results and thus detect errors. To cope with critical errors (*black out* situations resulting of upsets affecting the program sequencing) a programmable software watchdog was implemented in the motherboard.

The THESIC motherboard was thus enhanced with pseudo random interruption generation capabilities. A new operation mode, was also included in the THESIC interface, providing different options for CEU injection.

With these options the selection of the two parameters of simulated upsets - the location to be corrupted and the occurrence instant - can be chosen either pseudo-randomly or deterministically. This flexibility appears to be very useful for the investigation of the effects of upsets on complex applications. For instance, repeated experiments with *pseudo-random* choice for both the CEU target and occurrence instant, allow to get objective figures about the fraction of upsets which have no effects for a given program. Moreover, it may also put in evidence the configuration (occurrence instant ; location) of critical upsets. A *deterministic choice* of the CEU parameters becomes useful to reproduce such events and study their consequences in detail. Finally, an *exhaustive mode* was also included: at each clock cycle a CEU is injected on a particular target. This mode allows to identify, for the studied CEU target, which are its upset sensitive periods for a given program. As stated in [2], the computation of such periods could lead to the evaluation of duty factors, and thus to an accurate estimation of the program cross-section.

Previous work, validated on the 80c51 from Intel and the Digital Signal Processor TMS320C50 from Texas Instruments [3], proved the functionality of the CEU injection method. In this work we describe another application of CEU injection method on the microprocessor 68332 of Motorola in order to evaluate the potentialities of this new technique on different processors executing different applications. Fault injection sessions were performed on two different programs, a 10x10 matrix multiplication with both the operand and result matrixes resident within the internal memory of the microprocessor, and program modules of a final application implemented on digital architecture built around this processor for ground testing purposes, included in a satellite called CESAR. This project is an earth observation satellite mission developed in cooperation between INTA (Instituto Nacional de Técnica Aeroespacial, *National Institute for the Aerospace Techniques*) from Spain and CONAE (Comisión Nacional de Actividades Espaciales, *National Commission for Space Activities*) from Argentina. The primary objectives of this project will be cartography, thermal studies and geophysics. The application running on the microprocessor 68332, captures those solar spectra that contain information on gases present in the atmosphere. In order to do that, the microprocessor controls the exposition time of a PDA (sensor array of 1024 photodiodes) image detector of 1024 pixels and reads it by means of the converter AD677 connected to a synchronous channel (QSPI port of the 68332). For the purpose of ground testing and fault injection on the microprocessor 68332, a new daughterboard was designed and developed, including also the converter AD677, needed for the adaptation of programs developed for CESAR instrument. During CEU injection sessions, appropriate signal stimuli will exercise the A/D converter, simulating in some way the measures performed in flight.

## EXPERIMENTAL RESULTS

To validate this new method, we have ran experimental tests on the matrix multiplication program where 10% of the internal memory, 50% of the CPU registers, the status register SR and the program counter PC are used. We have ran 10 experimental sessions where an average of 12600 CEUs are injected each time, on the sensitive zones of this circuit. Referring to the experimental results, we have concluded that more than 95% of the total number of injected faults do not cause errors on the results of this program, while only 4% of them provoked errors and 0,8% caused system crashes. An exhaustive experiment was particularly investigated on the program counter PC shows that 14,7% of the CEU injected are tolerant, 37,7% caused errors on the matrix result and 47,7% provoked system crashes.

The final paper will provide the details, results and conclusions of CEU injection experiments performed on the Motorola 68332, when running the two programs, the matrix multiplication and the final software application which will run on the instrument on board the satellite. The CEU injection method makes possible the quantification of the rate of "effective" upsets for the tested programs, and thus to derive realistic figures for the expected error rate in flight. Such experiments could lead to a well sound methodology for actual application error-rate estimation, based on limited radiation testing (to evaluate the SEU cross-section per register type) and hardware/software fault injection to statistically evaluate the amount of upsets having consequences for the program execution.

## REFERENCES

- [1] R. Velazco, Ph. Cheynet, A. Bofill, R. Ecoffet, THESIC: A testbed suitable for the qualification of integrated circuits devoted to operate in harsh environment, *IEEE European Test Workshop (ETW' 98)*, Sitges, (Espagne), pp. 89-90, may 1998.
- [2] R. Koga, W. A. Kolasanski, M. T. Marra and W.A. Hanna, Techniques of microprocessor testing and SEU-rate prediction, *IEEE Trans on Nuclear Science* Vol. NS-32, N° 6, pp. 4219-4224, december 1985.
- [3] R. Velazco, S. Rezgui, R. Ecoffet, Transient bitflip injection on microprocessor-based digital architectures, *accepted for presentation at NSREC 2000 Conference* (Reno, USA, 24-29 July 2000).