On the Proposition of an EMI-Based Fault Injection Approach [1]

F. Vargas, D. L. Cavalcante, E. Gatti*, D. Prestes, D. Lupi*

Electrical Engineering Dept.
Catholic University – PUCRS
Av. Ipiranga, 6681.
90619-900 Porto Alegre – Brazil
vargas@computer.org

**Instituto Nacional de Tecnologia Industrial - INTI*
CITEI, INTI
Av. Gral. Paz 5445 - San Martín.
(1650) Buenos Aires - Argentina
lupi@inti.gov.ar

1. Introduction

The prevention of system failure in critical applications is decisively important, owing to the costly and hazardous consequences. Transient faults are the major source of system failures in such applications [1]. Having such a goal in mind, a study of error effects to characterize system susceptibility to faults is mandatory. An effective way to reach this goal is by using *fault-injection techniques*.

The following paper describes a new approach to perform physical fault injection in electronic systems. The approach is settled around a *GigaHertz Transverse Electromagnetic* (GTEM) cell, which is employed in a controlled process to inject faults in the system under test (SUT). The assumed fault models are *delay faults* (provoked by signal propagation delay increase in SUT critical paths, thus resulting in de-synchronization between the computed data to be latched and the clock signal) and *bit-flips* (i.e., corruption of static data stored in memory elements).

Aiming at detecting and classifying the occurrence of such faults during test, we implemented two test setups. The first one (say "HW-based approach") is represented by a watch-dog which is tightly connected to the SUT. The watch-dog is implemented by a remote personal computer. The second test setup is based on application code modifications to add consistency checks and signatures into specific parts of the code to detect faults (say "SW-based approach"). The detected faults are further classified into "control-flow" [2] or "data-flow" [3] faults [4].

2. The Test Setup

Fig. 1 summarizes the test setup used to perform fault injection. The *RF Signal Generator* Module is used to select the signal carrier, and the frequency and amplitude of the modulator signal. In the next step, the signal is properly amplified (*Power Amplifier* Module) before feeding the GTEM Cell.

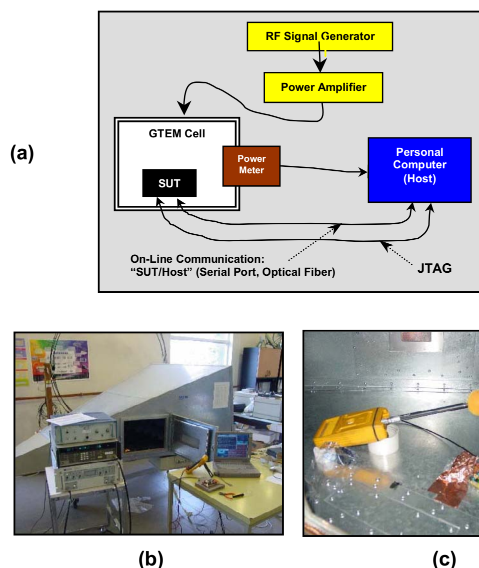

Fig. 1. Test setup for EMI-based fault injection. (**a**) and (**b**): General scheme and equipments at INTI. (**c**): SUT (MSP430F149 Texas Microcontroller) and Power Meter inside the GTEM Cell.

The desired EM field surrounding the SUT inside the GTEM Cell is precisely controlled by combining by one side the *signal carrier frequency*, with the *modulation signal frequency, amplitude and power*, by the other side. In order to monitor the resulting EM field inside the GTEM cell, it is commonly used a field sensor (*Power Meter*) near the SUT (Fig. 1c), which provides real-time measurements through the serial connection (optical fiber) to the Personal Computer (*Host*). The innovative fault injection approach resides on the following aspects: this test setup, which is used to certificate consumer electronics to electromagnetic compatibility – EMC (emission and susceptibility levels), is generally taken into account by assuming international standards such as those dictated by the

[1] *This work is partially supported by CNPq and Red PUCARA-CYTED.*

IEEE COMPUTER SOCIETY

International Electromagnetic Commission (IEC) [5]. Typically, these standards rule characterization procedures that aim at verifying the SUT behavior under EM fields ranging from 3 to 10 V/m (except for automotive industry embedded electronics, that requires EM fields one order of magnitude higher). In our case, we are proposing the utilization of such a GTEM cell not to measure the EM emission and EM susceptibility of the SUT, but to operate as a *powerful controlled process to inject faults in the SUT*. To do so, we apply much higher EM fields, ranging from 70 to 200 V/m in order to push the SUT towards failure states.

2.1. Practical Experiments

This section summarizes the preliminary results that we have obtained up to the moment concerning the use of GTEM cell as a tool for fault injection.

Fig. 2 shows the normalized number of the processor failures as a function of the electromagnetic field, given in volts per meter. In the sequence, Fig. 3 shows that the number of injected faults is not only a function of the instant EM field incident over the SUT, but it is also affected by the EM field modulation: even though the EM field is increased from 70 to 100V/m (Columns A to C, for the Bubble Sort) which could make one thinks that, as consequence, the number of erroneous outputs would increase, it was reduced. Note that for this interval, the RF modulation was reduced from 1GHz to 0.1GHz and 0.15GHz, respectively. This can probably be explained due to the fact that by reducing the RF modulation, there is an increase of the coupling effect between the modulated RF wavelength and the processor die tracks, processor input pins and board tracks. This effect induces large transient noisy currents, which reach internal processor latches and increase the probability of system malfunction.

3. Final Considerations

The work's main objective was to present a new *EMI-based fault injection technique*. This technique intends to be an alternative to other commonly used fault injection approaches, such as *heavy-ion radiation*, *power-supply disturbances* (also known as *pin-level fault injection*), *mutation analysis* or *saboteurs*.

The approach is based on a *GigaHertz Transverse Electromagnetic (GTEM)* cell that is employed in a controlled process to inject faults in the SUT. The number of faults injected in the SUT is a function of *RF signal modulation* and the *EM field value* to which the SUT is exposed inside the GTEM cell. By combining these two parameters, it is possible to expose the SUT to a more (or less) harmful environment.

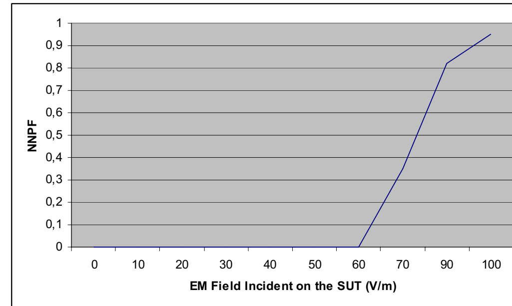

Fig. 2. **N**ormalized **N**umber of **P**rocessor **F**ailures [NNPF = (# of runs yielding erroneous outputs)/(# of runs)] as a function of the EM incident field applied on the SUT (V/m). Workload: *Bubble Sort*.

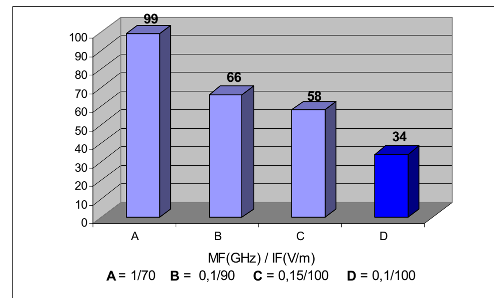

Fig. 3. Number of erroneous memory words as a function of *Modulation Frequency* (**MF**) and *EM Incident Field* (**IF**). Results for workloads *Bubble Sort* (Columns A, B, C) and *Matrix Multiplication* (D).

References

[1] Miremadi, G.; Torin, J. *Evaluating Processor-Behavior and Three Error-Detection Mechanisms Using Physical Fault-Injection*. IEEE Transactions on Reliability. Vol. 44, No. 3, September 1995. pp. 441-454.

[2] Oh, N.; Shirvani, P. P.; McCluskey, E. J. *Control-Flow Checking by Software Signatures*. IEEE Transactions on Reliability. Vol. 51, No. 2, March 2002. pp. 111-122.

[3] Rebaudengo, M.; Sonza Reorda, M.; Torchiano, M.; Violante, M. *Soft-Error Detection Through Software Fault-Tolerance Techniques*. IEEE Design for Testability Workshop (DFT'99), 1999.

[4] Vargas, F.; Cavalcante Lopes, D.; Chaves da Silva, J.; Barros Jr., D. *EMI-Induced Soft-Error Rate Estimates for COTS Microprocessor*. 5th IEEE Latin American Test Workshop – LATW'04. Cartagena, Colômbia, March 2004, pp. 169-172.

[5] *International Electrotechnical Commission - International Standard IEC 61000-4-29 Normative*. (www.iec.ch)

1530-1591/05 $20.00 © 2005 **IEEE**

IEEE COMPUTER SOCIETY