Emulation-based Fault Injection of Transient Faults in Complex System-on-Chip

Paolo Calao
Politecnico di Torino, Italy
Corso Duca degli Abruzzi, 24 - 10129 Torino (TO)
paolo.calao@gmail.com

Keywords. Fault injection techniques, Sensitivity to transient faults, SoC dependability.

Abstract

Technology scaling systematically increases the sensitivity of electronic systems to radiation, causing a growing interest in the analysis and study of the Single Event Upset (SEU) effects. This is especially true in safety-critical domains, in which devices must ensure high robustness and reliability. Fault injection techniques, both hardware and software, are today widely adopted to analyse and improve the dependability of such devices [1]. Fault injection campaigns allow to observe the response of an application running on a complex System-On-Chip (SoC) to fault conditions and to measure its capability to detect random faults.

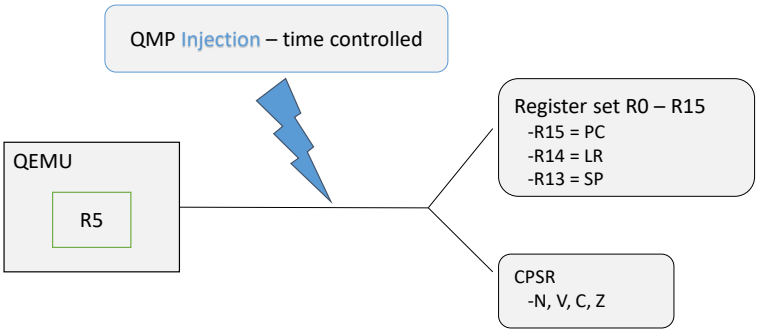

Figure 1. Overview of the injection framework.

```
; validation application ASM code
        MOV R8,  #4
        MOV R9,  #8
        MOV R10, #1
LOOP:   NOP
        CMP R10, #1
        BNE LOOP
CHECK:  ADD R11, R8, R9
        CMP R11, #12
        MOVEQ R10, #100
        MOVNE R10, #200
```

Figure 2. Assembly program used to validate the fault injection framework.

Hardware approaches are needed to accurately validate and measure the dependability of a safety-critical device, but they are really expensive. On the other hand, emulation based approaches are cheaper and faster, also they do not require the physical presence of the device at the expenses of the accuracy (i.e., simplified description of components and reduced time precision) [2]. To benefit from both, these techniques must be used in a complementary way. Emulation-based fault injection is better suited for evaluating the sensitivity of software to soft-errors, which means how good that software is to detect SEU.

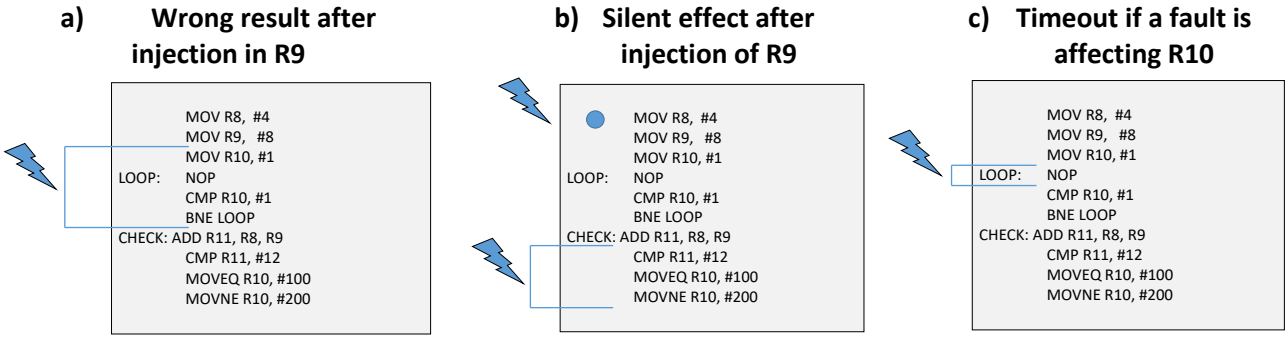

Figure 3. Classification of possible effects of injections.

In this project a QEMU-based fault injector has been realized. It is able to inject bit-flip faults into the register set of ARM CPUs, as depicted in Figure 1. The emulation of an ARM R5 CPU model, executing the assembly program described in Figure 2, has been employed to validate the injection flow. The effects of injections are classified according to the three categories listed in Figure 3. This fault injection framework could be exploited to choose the right self-test software that will be run by a device during a hardware fault injection campaign.

Acknowledgment

This project was developed in the Electronic CAD and Reliability research group laboratory of the Politecnico di Torino University. The supervisors of this work were Paolo Bernardi, which is an Associate Professor of Politecnico di Torino, and Marco Restifo, which is a PhD Student of Politecnico di Torino.

References

[1] Y. Li et al., "A Fault Injection System Based on QEMU Simulator and Designed for BIT Software Testing", Applied Mechanics and Materials, Vols. 347-350, pp. 580-587, 2013.

[2] Ferraretto, Davide & Pravadelli, Graziano. (2015). Efficient fault injection in QEMU. 2015 16th Latin-American Test Symposium, LATS 2015. 10.1109/LATW.2015.7102401.