Abstract

Dependability has so far been used as a required characteristic in order to evaluate complex or critical systems, especially those in which a failure means a risk for human life or high economical losses. Nowadays, the development of embedded systems has increased in all areas, from industrial environments to household uses. Due to the commercial expansion of embedded systems and market competitiveness, many system designers take dependability into account. Dependability evaluation and system validation has to be carried out before the functional-live phase of the product. Since an "in situ" work may require a long time because of the low failure rate of components in modern circuits, it is useful to resort to a experimental validation that generates faulty events forcing the system to deal with them according to design specifications. Fault Injection is an experimental validation method with increasing acceptance based on the realization of controlled experiments where the observation of the system behaviour in present of faults is explicitly induced by the deliberate introduction (injection) of faults into the system.

The effect of physical faults on current semiconductors, with their high operation frequency and integration density, is more aggressive than the effect obtained on devices of less advanced technologies. It can no longer be justified that a single fault only causes a single error. Consequently, it is necessary to deal with multiple errors. It has been also observed with Single Events Upsets on static and dynamic RAM memories. Moreover, thinking on the short distance existing between pads, it would be reasonable to validate the tolerance of the system against multiple faults in physically neighbouring lines.

There are many fault injection techniques and tools, among them, *Physical fault injection at pin level* is applied externally to the system and it can fulfil the requirement of not causing overhead or alteration in the execution of the code. Thus, this technique is suitable to validate complex fault-tolerant real-time distributed embedded systems. The strong temporal requirements of a real-time system, and its own condition of distributed, force us to look for non-overhead solutions that solve both, a runtime integration of the injection tool, where the system under test is never halted or delayed, and a dynamic reading of all the system events that take place at the same time but in different units.

The Time-Triggered Architecture TTA is aimed to the development of safety-critical real-time distributed embedded applications. In the TTA, fail-silence is a main concern in two domains, the time and the value domains. Fail-silence in the time domain should be guarantied by the TTP communication protocol. Fail-silence in value domain guarantees the correctness of the delivered message. This work details an important part of the experiments carried out in the course of the EU-funded IST project “Fault Injection for TTA”. It is focused on analysing the effect of faults at pin level on the TTP^{TM}/C communication controller based on the Time-Triggered Architecture (TTA), revealing weaknesses and encouraging to improve the error detection mechanisms to reach the objective of dependability.

Keywords: Dependability, Experimental Validation, Fault Injection, Time-Triggered Architecture, Physical Faults, Time-Triggered Protocol.