World Academy of Science, Engineering and Technology
International Journal of Electrical and Information Engineering
Vol:15, No:03, 2021

Identification of Failures Occurring on a System on Chip Exposed to a Neutron Beam for Safety Applications

Authors : S. Thomet, S. De-Paoli, F. Ghaffari, J. M. Daveau, P. Roche, O. Romain

Abstract : In this paper, we present a hardware module dedicated to understanding the fail reason of a System on Chip (SoC) exposed to a particle beam. Impact of Single-Event Effects (SEE) on processor-based SoCs is a concern that has increased in the past decade, particularly for terrestrial applications with automotive safety increasing requirements, as well as consumer and industrial domains. The SEE created by the impact of a particle on an SoC may have consequences that can end to instability or crashes. Specific hardening techniques for hardware and software have been developed to make such systems more reliable. SoC is then qualified using cosmic ray Accelerated Soft-Error Rate (ASER) to ensure the Soft-Error Rate (SER) remains in mission profiles. Understanding where errors are occurring is another challenge because of the complexity of operations performed in an SoC. Common techniques to monitor an SoC running under a beam are based on non-intrusive debug, consisting of recording the program counter and doing some consistency checking on the fly. To detect and understand SEE, we have developed a module embedded within the SoC that provide support for recording probes, hardware watchpoints, and a memory mapped register bank dedicated to software usage. To identify CPU failure modes and the most important resources to probe, we have carried out a fault injection campaign on the RTL model of the SoC. Probes are placed on generic CPU registers and bus accesses. They highlight the propagation of errors and allow identifying the failure modes. Typical resulting errors are bit-flips in resources creating bad addresses, illegal instructions, longer than expected loops, or incorrect bus accesses. Although our module is processor agnostic, it has been interfaced to a RISC-V by probing some of the processor registers. Probes are then recorded in a ring buffer. Associated hardware watchpoints are allowing to do some control, such as start or stop event recording or halt the processor. Finally, the module is also providing a bank of registers where the firmware running on the SoC can log information. Typical usage is for operating system context switch recording. The module is connected to a dedicated debug bus and is interfaced to a remote controller via a debugger link. Thus, a remote controller can interact with the monitoring module without any intrusiveness on the SoC. Moreover, in case of CPU unresponsiveness, or system-bus stall, the recorded information can still be recovered, providing the fail reason. A preliminary version of the module has been integrated into a test chip currently being manufactured at ST in 28-nm FDSOI technology. The module has been triplicated to provide reliable information on the SoC behavior. As the primary application domain is automotive and safety, the efficiency of the module will be evaluated by exposing the test chip under a fast-neutron beam by the end of the year. In the meantime, it will be tested with alpha particles and electromagnetic fault injection (EMFI). We will report in the paper on fault-injection results as well as irradiation results.

Keywords : fault injection, SoC fail reason, SoC soft error rate, terrestrial application
Conference Title : ICREED 2021 : International Conference on Radiation Effects on Electronic Devices
Conference Location : Paris, France
Conference Dates : March 29-30, 2021