Towards Trusted Devices in FPGA by Modeling Radiation Induced Errors

Jan Pospíšil, Tomáš Vaňát, Jan Schmidt
Department of Digital Design
Czech Technical University in Prague, Faculty of Information Technology
Prague, Czech Republic
Email: jan.pospisil@fit.cvut.cz, tomas.vanat@fit.cvut.cz, jan.schmidt@fit.cvut.cz

***Abstract*—Field Programmable Gate Arrays (FPGAs) offer great opportunity for wide range of applications. FPGA chips are also used in secure applications, where they can represent critical parts of such systems when implementing some of key functions. On one hand, FPGAs offer universal usage through their programmability, but on the other hand their complex structure is prone to several types of disturbances, one of which can be a radiation, either natural, or induced by an attacker. The response of basic CMOS structures to radiation (e.g. laser or ionizing radiation) is well documented in terms of Single Event Effects (SEE) and Single Event Upsets (SEU), but the impact of these interferences on a particular design implemented in an actual FPGA can be predicted with difficulty. This weakness can be exploited to fault-attack the target design. Although radiation attack is less probable than other types, a security device properly eliminated from service by radiation can impose a significant risk to the whole system.**

There are two main possibilities of testing the impact of radiation on the design dependability parameters. The first one is the Accelerated Life Test (ALT), which is based on increasing the amount of the radiation in the environment, where the device is tested. Using this method (in simple terms), the device receives the same amount of radiation as it would receive during years of operation, in few minutes. If appropriate energy spectrum of particles is used, this method gives very accurate results. The problem is that it is very expensive and not easily accessible. The alternative is to use a simulation model. To create the model, it is necessary to have a detailed description of the physical structure of the tested hardware, which is not always available for commercial FPGAs, thus we can use only approximate models. Methods allowing to classify faults in nearly all models have been published.

In the presentation we will introduce our method of modeling the behavior of FPGA described by a custom architecture with emphasis to resistance to radiation induced soft-errors. Because of detailed descriptions of architectures used in commercial FPGAs are not available, we have to propose an artificial architecture based on all knowledge we have about the commercial ones. This proposed architecture is consecutively processed through modified open-source VTR toolchain and testing designs are placed and routed to this architecture by the same tool. Beside this, ALT fault injections on real FPGAs are conducted to obtain data characterizing a behavior of the same testing designs under radiation. Data obtained by these experiments helps to calibrate the results obtained by simulation of the proposed architecture. The result of this work will provide a calibrated model to this method to perform more realistic SEU testing and prediction of the impact of natural radiation and radiation-based attacks on a design implemented in FPGA. As a result, the obtained models will help us to design radiation and attack resilient FPGA architectures, and/or attack-resistant designs based on existing FPGAs.