On the impact of ionizing and non-ionizing irradiation damage on security microcontrollers in CMOS technology

Theresa Krüger
Telekom Security
Bonn, Germany
https://orcid.org/0009-0004-6217-453X

***Abstract*—The possible effects of irradiation on security controllers implemented in CMOS technology are studied. First, the decrease of the effectiveness of a light sensor/detector as countermeasure against laser fault injection is analysed. Second, the use of irradiation as fault injection method is proposed.**

***Index Terms*—irradition, sensor damage, fault injection, attack potential**

I. Introduction

Light sensors are frequently used as a countermeasure against laser fault injection (LFI) attacks on secure implementations of algorithms in integrated circuits (ICs). They are typically implemented together with the other CMOS transistors on the same silicon substrate. The functionality of light sensors is based on the same concepts as that of pixel detectors. A pixel detector is similar to a CMOS image sensor. The difference between them is that the pixel detector is not optimized for detecting photons in the optical range but is optimized for detecting charged particles generated in high energy physics experiments. One outstanding characteristic of the pixel detector is the high timing precision of the detection process which is in the order of few tens of nanoseconds. It is a known effect in the field of particle physics detectors [1] that transistors in ICs and light sensors in ICs are subject to a performance degradation due to the exposure to ionizing radiation[1] and non-ionizing radiation[2], the resulting effects called total ionising dose damage (TID damage) and non-ionizing energy loss damage (NIEL damage) respectively. If the transistors of the security controller stop to function before the light sensors stop to function, this is not considered a security concern but rather a denial of service situation. If the transistors of the security controller continue to function, but the efficiency of the light sensors degrades significantly, this may be used by an attacker to "switch off" the light sensor by irradiation.

With ionizing radiation faults can also be induced by two mechanisms which differ in their timing behaviour. First, the electrical characteristics of the CMOS transistors changes after exposure to ionizing irradiation and these changes may cause faults in the computation of the security controller. This method is called Irradiation Fault Injection (IFI). Second, charged particles passing through the security controller cause faults similar to LFI. This method is called Charged Particle Fault Injection (CPFI). It is possible to inject faults by exposing the security controller to a charged particle beam where the particles traverse the whole chip and further. CPFI has small practical limitations as to the position where the faults can be induced and is particularly interesting where LFI becomes difficult due to photon absorbing packaging. This is due to the fact that the charged particles pass through the whole security controller and further dependent solely on their range in the given material path.

II. Results of studies of irradiation effects on pixel detectors by RD50

The efficiency of pixel detectors is known to be a function of the geometrical layout of the charge collection node, ionizing and non-ionizing doses, depletion voltage (if applicable) and the doping concentration of the sensitive volume. Extensive experimental research in this field has been performed by the CERN RD50 collaboration[3]. The performance characteristics of different pixel detector layouts have been simulated and their efficiency characterized in laboratory and in beam experiments. The RD50 collaboration investigated the irradiation effects on both the transistors and sensors to provide a solid basis for the decision about which technology shall be used by the detectors used in collider experiments [1]. The amount of the radiation dose that a detector is exposed to in its lifetime was simulated and concrete upper levels of total doses determined. To test detector layouts, samples were produced and irradiated at different reactors to achieve the same doses as are expected after roughly 10 years of operation in the inner part of the hadron collider experiments[4]. The technology mostly tested in the course of these studies is a 65 nm CMOS

[1]Ionizing radiation means the particles that carry a charge that is not zero and photons which are the exchange particles of the eletromagnetic interaction.

[2]Non-Ionizing radiation means the particles that do not carry a charge, like the neutron or neutral pion.

[3]International research and development cooperation with the focus of "Radiation hard semiconductor devices for very high luminosity colliders" organised by CERN, a fundamental physics research organization in Europe founded in 1952 located at the Swiss/France border and partially in Geneva. The results are summarised on their webpage: http://rd50.web.cern.ch/

[4]It is assumed that the damage effects depend on the total dose and not on the actual dose rate.

process.
NIEL damage has the following impacts on pixel detectors:

- Increase of the leakage current
- Trapping of the mobile charge carriers.

TID damage has the following impacts on pixel detectors:

- Shift of the threshold voltage,
- Degradation of the transconductance and
- Increase of the OFF state current for nmos transistors.

For pixel detectors the NIEL damage results in charge collection efficiency degradation which in turn leads to tracking performance degradation in the collider experiments. The leakage current increase leads to higher cooling requirements and has no impact on the detector readout for AC-coupled detector designs. Dependent on the design the leakage current increase may impact the readout electronics. For pixel detectors the TID damage results in the denial of service of the readout electronics.

III. Review of Light Sensor implementations in Security Controllers

The radiation tolerance of light sensors of security controllers is usually not a primary design goal as well as the radiation tolerance of the used transistor technology. Light sensors, such as BBICS [2], [3], use as charge collection node the shallowly depleted region between the deep n-well and the low resistive p-substrate. The p-bulk contact is on ground potential and the n-contact inside the deep nwell is on the digital supply voltage (VDD) potential. Thus this junction is a reversly biased diode as is the default setting in such CMOS transistors. Similarly, the settings are just the opposite for deep p-wells.
NIEL damage leads to an increase of the leakage current. If the leakage current increases, the expected behaviour of the BBICS sensors is that they are just always on. Therefore NIEL damage does not appear to be the exploitable attack path. TID damage leads to a change of the following transistors characteristics: Threshold voltage shift, transconductance degradation and increase of off state current for nmos transistors. The first two lead to slower switching times and can cause device failure. The latter affects mostly analog functions such as PLLs, Bias generators or BBICS. By applying different TID doses it might be possible to "switch off" the BBICS permanently or induce faults.
Other implementation are also based on the creation of mobile charge carriers in a semiconductor, see the patents [4] and [5].

IV. Applicability of RD50 results to light sensors in security ICs

The light sensors of security controllers and pixel detectors based on semiconductors are based on the collection of mobile charge carriers potentially created within a depletion region. The difference between them is really just the name. Light or photons and particles interact differently with matter and therefore have different energy loss mechanisms, see [6]. Photons loose energy in a medium by photo-effect, compton radiation and pair-creation. Particles mostly loose energy in a medium by ionisation. Even though the energy loss mechanisms are different for photons and particles, this distinction is not relevant because in both cases mobile charge carriers are created and then read out by a dedicated circuitry. Thus a light sensor is a particle detector where the sensitivity is optimized for photons in the visible frequency spectrum. Therefore the effects of NIEL damage and TID damage studied with pixel detectors apply to light sensors in security controllers, the extent to which may be determined experimentally.

V. Impact on the attack potential

The vulnerability analysis is one class of the Common Criteria evaluations where the attack potential is being rated taking into account the following factors: Elapsed time, Expertise, Knowloedge of the TOE (target of evaluation), Equipment and Window of opportunity. For the here described attack scenario rating the irradiation with X-rays impacts the factors time and equipment. The irradiation of samples with xrays can be bought as a service at various facilities. A collection of facilities who provide irradiation services for scientific purposes is provided at the link: https://irradiation-facilities.web.cern.ch/publicDB.php. Exemplary, at the KIT irradiation facility[5] a time period of 6 weeks is expected between sample arrival and return shipment. The dose rate is 40 kGy/h = 4 MRad / h. A typical effective dose of 10 MRad [7] leads to an irradiation duration of 2.5 hours. Thus, the elapsed time is less than 2 months. An X-ray tube for the irradiation purpose need not be purchased, but the irradiation can be bought as a service. The X-ray tubes are not freely available. The equipment is rated as specialised. A successful attack would result in smart cards not being resistant against high attack potential.

VI. Further work

The conclusions in this paper are preliminary in the sense that they depend on the detector layout and readout electronics which are mostly confidential information. The future work is to perform irradiation campaigns with exisiting technologies and characterise the effects.

References

[1] M. Moll, *Development of radiation hard sensors for very high luminosity colliders - CERN-RD50 project*, NIMA, 511, 97-105, 2003.

[2] R. P. Bastos, J. M. Dutertre and F. S. Torres, *Comparison of bulk built-in current sensors in terms of transient-fault detection sensitivity*, 2014 5th European Workshop on CMOS Variability (VARI) pp. 1-6, doi: 10.1109/VARI.2014.6957089, 2014.

[3] R. P. Bastos and F. S. Torres, *On-Chip Current Sensors for Reliable, Secure, and Low-Power Integrated Circuits*, (1st. ed.). Springer Publishing Company, Incorporated., 2019.

[4] T. Kautzsch, *PHOTO CELL DEVICES FOR PHASE-SENSITIVE DETECTION OF LIGHT SIGNALS*, Infineon, Patent no. US 9,190,540 B2, 17.11.2015.

[5] R. Daamen et. al., *INTEGRATED CIRCUIT INCLUDING A DIRECTIONAL LIGHT SENSOR*, NXP B.V., Patent no. US 2014/0203391 A1, 24.07.2014.

[5]The irradiation facility of the Karlsruhe Institut of Technology, 76344 Egg.-Leopoldshafen, Germany provides information at the link http://www.etp.kit.edu/english/irradiation_center.php

[6] W. R. Leo, Techniques for nuclear and particle physics experiments: a how-to approach; 2nd ed., Springer, Berlin, 1994, url = https://cds.cern.ch/record/302344, doi = 10.1007/978-3-642-57920-2

[7] F. Faccio et al., *Radiation-Induced Short Channel (RISCE) and Narrow Channel (RINCE) Effects in 65 and 130 nm MOSFETs*, IEEE Trans. on Nucl. Sci. 62.6 (2015): 2933-2940

[8] CEM, Australia, Canada, France, Germany, Japan, Netherlands, New Zealand, Republic of Korea, Spain, Sweden, United Kingdom, United States, *Common Methodology for Information Technology Security Evaluation Evaluation methodology*, Version 3.1 Revision 5, CCMB-2017-04-004, April 2017.