on ElectroMagnetic Compatibility (CEM2020) OUT-OF-BAND 60 GHz VULNERABILITY OF FRONT-ENDS AND FPGA USING NEAR-FIELD INJECTION

Jérémy Raoult, Mathieu Guery, Vincent Pouget, Sylvie Jarrix, Laurent Chusseau

20th International Symposium on ElectroMagnetic Compatibility (CEM2020)

OUT-OF-BAND 60 GHz VULNERABILITY OF FRONT-ENDS AND FPGA USING NEAR-FIELD INJECTION

Jérémy Raoult[1,*], Mathieu Guery[1], Vincent Pouget[1], Sylvie Jarrix[1], Laurent Chusseau[1]
[1]IES, Université de Montpellier, CNRS, Montpellier, France
[*]jeremy.raoult@ies.univ-montp2.fr

Abstract. Integrated circuits can be sensitive to out-of-band electromagnetic disturbances or even intentional attacks. We have already shown this concept at 60 GHz for front-end receivers thanks to a radiation in the near-field. A more detailed study is proposed here thanks to an increased power of the source, which makes it possible to exceed an excitation level of 10 kV/m, and also to the study of a digital FPGA circuit on which two test circuits have been implemented. Initial results show that this digital circuit is more robust and will require more advanced attack strategies in the future.

I. Introduction

In a very close future, the electromagnetic environment will be enriched by new communications at a few tens of GHz and even more up to mm-wave. This is already the case of the ongoing 5G standard, which involves a carrier frequency of 60 GHz for the communication between base stations. Moreover, high power electromagnetic weapons also tends to operate up to 100 GHz [1], leading to a better compactness. As a result, the current RF circuits will have to coexist with signals having carriers at mm-wave. They have obviously not been designed nor tested in such conditions.

A huge amount of information is sent and received in a digital form. This information is sensitive and may thus require to be protected against unauthorized access. Attacks targeting directly the implementation are a very serious threat to the security of a system. Among the possible threats, the physical weaknesses of the integrated circuits (ICs) are among the most important. EM fault-injection combined with side-channel attack is the most recent physical technique that is used to break a cryptosystem [2] because EM fields are able to influence encapsulated chips while bypassing existing countermeasures. EM fault-injection tests used probes which are frequency limited to a few GHz [3]. Immunity tests at higher frequencies (mm-wave) have never been conducted. However it is now easier to find mm-wave sources, with high output power, and at affordable prices. Injecting an EM signal at such high frequencies could become a new threat to the security of ICs.

We developed recently an experimental setup to test the mm-wave immunity of analog RF front-ends [4]. A 60 GHz signal in pulsed or CW mode is injected in the near-field above chips. Complete extinctions of nominal RF functions of some circuits were demonstrated, although the injected frequency is ten to twenty times that of normal RF operation of the ICs. A better understanding of the effects of mm-wave power injection on ICs requires an increased power of the source, which makes it possible to exceed an excitation level of 10 kV/m that is of the same order of magnitude than a High Power EM weapon used in a far-field. With this new experimental setup, we also just started to test the mm-wave sensitivity of a very common digital IC, namely a FPGA on which two test circuits have been implemented. After the description of the experimental setup, we explain the methods involved for the test of mm-wave immunity and presents the main results on RF and digital ICs.

II. Experiments

II.1. Experimental Setup

The experimental setup is sketched in Fig. 1. It involves mostly a mm-wave source, namely a Gunn diode from Quinstar (model QTM-602001SV) achieving 20 dBm output power and a slight tunability around 60 GHz. Its output is amplified owing to a MI-wave 955 Series Amplifier delivering at least 32 dBm over the desired 59-61 GHz bandwidth. Because of the strong mismatch during injection experiments the amplifier is protected by two isolators in series and then feed a rectangular WR15 waveguide whose open-end radiates over the IC to test.

The output of the circuit is routinely monitored by a high-speed oscilloscope. Alternatively a spectrum analyzer and a monitoring of the power supply could be added. The relative position of the $3.76 \times 1.88\,\mathrm{mm}^2$ WR15 open waveguide and the DUT is controlled by stepper motors on all three axes with a resolution of $1\,\mu$m. A rotating stage allows to control the polarization interacting with the circuit. A very important feature of the Gunn source is its ability to be switched on and off using the simple TTL signal at low frequency. The latter must not exceed 20 kHz but short rise and fall times are welcome with aim of producing transient excitation.

Considering the 1 W available power at WR15 output after isolator attenuations, we estimate analytically, using the model developed by Baudrand *et al.* [5], a the

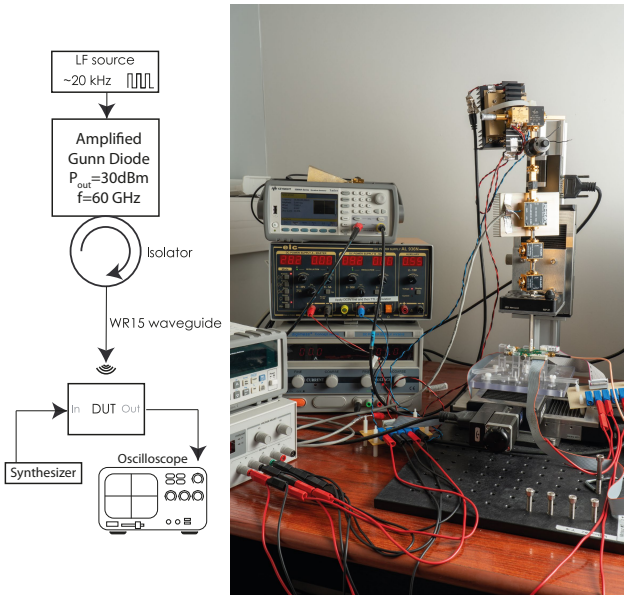

Fig. 1. Experimental setup. Left: principle. Right: photograph of the true bench.

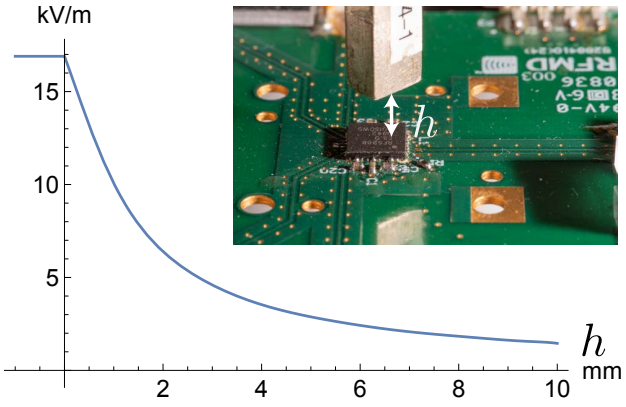

Fig. 2. Calculated maximum filed intensity versus h the distance between the open-ended WR15 waveguide and the target. The inset shows a close view of the experiment in action with h labeled. In practice the IC is often closer to the waveguide.

maximum field intensity of ≈ 17 kV/m at WR15 contact, and more than 10 kV/m at a distance of 1 mm (that is, a typical IC package thickness). Calculation results are plotted in Fig. 2 together with a close view of the WR15 waveguide overflying the IC to illustrate the interaction distance h. With such a power level the contactless near-field interaction thus allows to reach field intensities of the same order of magnitude than HPEM [1] only using a moderate mm-wave power. Moreover one can modulate easily both the injection power simply by changing the guide-to-sample distance or the amplifier feed and it is possible to combine measurements with stepper motor displacements to acquire a full 2D raster-scanning of the target. It has already been used to show mm-wave injection effects with a spatial resolution better than the IC size [4].

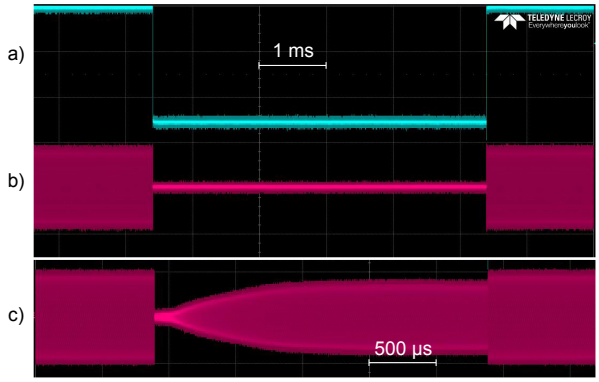

Fig. 3. Oscilloscope traces of the chopped reference signal at 20 kHz (a), the RF6535 front-end operating in PA mode @ 2.4 GHz at two different injection powers (b) and (c). When the chopped signal is in up state, the 60 GHz source is inhibited. In (c), the final value of the attenuated output, measured just before the mm-wave source is switched off, defines the CW sensitivity to injection by its ratio to the non perturbed amplitude.

II.2. First Results

Let us first recall the effect of the 60 GHz out-of-band injection on a RF front-end as measured with an oscilloscope. This is best illustrate with a RF6535 front-end from Qorvo operating in PA mode at a frequency of 2.4 GHz. As seen the PA switches from its normal operation to a complete extinction when the 60 GHz is applied (Fig. 3b). At time scales of these oscilloscope traces, this operation is quasi instantaneous and follows exactly the mm-wave, either for its ignition or its extinguishment [6], [7].

When the impinging power is reduced, for instance when the waveguide to DUT distance h is increased, one observes the same sudden extinction of the DUT operation but a further recovery begins just after the transient. It appears with a long time constant (see Fig. 3c), and eventually the peak-to-peak amplitude of the DUT signal remains reduced indefinitely as compared to the non-illuminated operation. This reduced steady-sate value, expressed in % when referring to nominal operation, is the sole marker of the electromagnetic susceptibility of the circuit in CW regime. It acts as a reduction of gain under illumination that we attribute to a rectification phenomenon in the active non-linearities of the circuit following the electromagnetic coupling with one or more lines. This coupling is more or less reinforced by the sensitivity to polarization of this effect [6].

This hypothesis was validated in [4] using high-frequency models because actual modern IC designs always integrate transistors with a very high transition frequency, f_T, which is at least in the order of 100 GHz, even to operate much lower in frequency. Enumerating the possible channels of the perturbation, it is believed that rectifier mechanisms yielding large variations in power supply current, especially if applied to current-mirrors, are responsible of the observed behavior. A circuit model

using a capacitance coupling was able to explain qualitatively with success the CW effect, but the lack of the detailed IC design prevent a more quantitative analysis including the electromagnetic coupling. Nonetheless our interpretation of the perturbation on current-mirror through the feeder tracks is physically sound and suggests an increased sensitivity with ICs built with even faster component technologies. Note that this sensitivity may also depend on the architecture.

II.3. Influence of excitation power

The great improvement proposed here is the rising of the excitation power now reaching 1 W at WR15 end. Unfortunately only a few of the front-ends already tested [4], [6] is still available in the lab and it was impossible to test them all again for comparison. However, this was done with the Qorvo RF5288 and RF6535 ICs, qualifying 6 references out of the 13 functions previously tested (see [6]). Results are summarized in Table 1. with the CW impact as factor of merit of the perturbation compared between the two excitation levels.

Table 1. Impact of the out-of-band perturbation on the CW gain. A 100% value stands for complete extinction. PA: Power Amplifier, LNA: Low-Noise Amplifier.

Ref.	Function	f (GHz)	Impact @20dBm	Impact @30dBm
5288	LNA	2.45	85	**85**
5288	LNA	5	0	**0**
5288	PA	2.45	5	**20**
5288	PA	5	30	**30**
6535	LNA	2.4	80	**80**
6535	PA	2.4	100	**100**

A careful examination of the new factor of merit @ 30 dBm shows fewer changes than initially expected, but most of the subtleties are hidden. On the one hand, it is necessary to highlight the increase in the disturbance of the LNA 5288 operating at 2.45 GHz, which is now strongly affected by out-of-band injection. On the other hand, the other references remain unchanged despite the sharp increase in the incident electromagnetic field. For example, the LNA 5288 and 6535 operating around 2.5 GHz have a similar factor of merit $\approx 80\,\%$ but their response to polarization is very different for the two input powers. By moving to 30 dBm, the gain changes significantly over a much wider range of angles between the guide and the circuit as compared to the case of 20 dBm. This is probably due to the fact that the threshold power required to modify the function is reached more easily even if the projection of the linearly polarized injection field is not perfectly aligned with the targeted microstrip line. Therefore, all transients are steeper when the field strength increases, even if the stable steady-state disturbance appears unchanged. The underlying physics of this threshold effect can probably be found in the architecture of these functions, which is unknown for commercial devices.

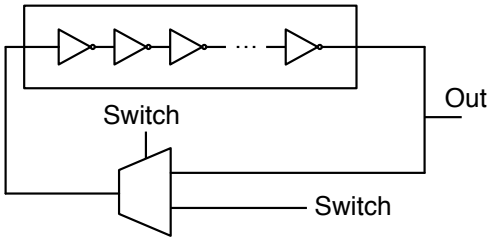

Fig. 4. Scheme of the ring oscillator test circuit.

II.4. FPGA

Previous work was extended to a numerical card from the manufacturer OHO-Electronik from its GODIL series and based on a Xilinx Spartan 3E FPGA. To our knowledge, we report here the first mm-wave immunity tests on such an IC. We chose this widely used device because of its top-mounted chip and relatively thin housing that both maximize interactions with the radiated electromagnetic wave at waveguide end. Two test circuits were implanted in the FPGA to evaluate its vulnerability to mm-wave: a ring oscillator and a shift register, respectively based on asynchronous and synchronous operations.

a - Ring oscillator

A ring oscillator (RO) consists of a loop chain of inverters (see Fig. 4). The correct implementation in VHDL language requires a multiplexer to close the loop. With an odd number of inverters in the RO, an oscillation is generated whose frequency depends on both the number of gates and their propagation delay. ROs are used by manufacturers as a reference structure to qualify a new technology. In some secure ICs, they are the basis of internal clocks used for random number generators [8]. Millimetre-wave EM injection is expected to slightly change the oscillation frequency, as already seen at lower frequencies [9]. Physics knowledge based on our previous interaction model predict current (or voltage) fluctuations after coupling with the FPGA. If these fluctuations are large enough, they act back on the internal current source after non-linear conversions, and cause a change in the propagation delay and therefore in the oscillation frequency of the RO.

We used typically 1001 logic gates to occupy the largest layout surface and thus increase the coupling possibilities with our WR15 output. As a result, a frequency of $\approx$ 10 MHz was synthesized. Once the VHDL program has been compiled and implemented in the FPGA, the experiment consists, as with analog circuits, to fly over the chip at small guide-chip distance, while injecting the

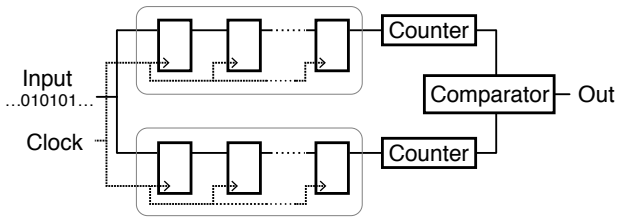

Fig. 5. Scheme of the shift register test circuit.

60 GHz signal in CW or pulsed mode. In the latter case and since the circuit is asynchronous, the pulse signal modulating the 60 GHz signal is not correlated with the intrinsic frequency of the RO.

Even if a fast oscilloscope was used to monitor the FPGA output, no variation of the RO frequency was obtained, even at very close distance. However, the measured oscillation frequency was very difficult to stabilize, and exhibits a large jitter, thus embedding any susceptibility within the corresponding frequency noise. New protocols are being presently studied to improve the signal-to-noise ratio and extract the influence of EM injection on ROs if it exists.

b - Shift register

The shift register (SR) is a synchronous logic circuit composed of D flip-flop connected in series (see Fig. 5). To evaluate the sensitivity of SR to mm-wave injection, we have implemented 2 similar shift registers followed by a counter which adds the received values. The data at the entry of each register are the same. Counter outputs are compared with aim to detect a logical fault. The effective surface and position used by each SR in the FPGA can be easily directed by the choice of the number of flip-flops and by the use of special VHDL directives. Provided that the clock frequency is faster than the input signal, no data bit can be lost.

A logical fault would be produced if the EM injection is able to invert a logical level [10]. The fault then spreads to the rest of the register until the counter is shifted at the end of the register, setting the comparator output to 0. The experimental protocol for EM injection is the same as the one used previously but has not yet been conducted at the moment of this proposal writing. Extended tests are ongoing.

III. Conclusion

We have shown that injection experiments can remotely shut down RF front-ends using mm-wave radiated in the near field. In this communication, we have reinforced our previous results [4] with an improved power capable of radiating a field greater than 10 kV/m in the vicinity of the CIs. It proved easier to affect RF front-ends, some of which were disrupted for the first time.

One logic circuit based on a FPGA was then studied using two test programs implemented in the layout. Initial attempts have not shown any disruption yet. As a result, digital ICs seem more robust to such large out-of-band attacks, but improvements are expected using new protocols and synchronous strategies that would require a major redesign of our test bench.

REFERENCES

[1] W. A. Radasky, C. E. Baum, and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 314–321, 2004.

[2] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic transient faults injection on a hardware and a software implementations of aes," in *Fault Diagnosis and Tolerance in Cryptography (FDTC)*. IEEE, 2012, pp. 7–15.

[3] L. Chusseau, R. Omarouayache, J. Raoult, S. Jarrix, P. Maurine, K. Tobich, A. Boyer, B. Vrignon, J. Shepherd, T.-H. Le, M. Berthier, L. Rivière, B. Robisson, and A.-L. Ribotta, "Electromagnetic analysis, deciphering and reverse engineering of integrated circuits (E-MATA HARI)," in *22nd International Conference on Very Large Scale Integration (VLSI-SoC)*, Playa del Carmen, MX, 2014, pp. 189–194.

[4] J. Raoult, P. Payet, and L. Chusseau, "Identification of vulnerability within front-ends chips using 60 GHz near-field injection," in *49th European Microwave Conference*, Paris, 2019.

[5] H. Baudrand, J.-W. Tao, and J. Atechian, "Study of radiating properties of open-ended rectangular waveguides," *IEEE Trans. Antennas Propag.*, vol. 36, no. 8, pp. 1071–1077, 1988.

[6] P. Payet, M. Guery, J. Raoult, and L. Chusseau, "Out-of-band disturbance of mm-wave EMI on RF front-ends," *Microelectronics Reliability*, vol. 76–77, pp. 670–673, 2017.

[7] P. Payet, J. Raoult, and L. Chusseau, "Remote extinction of a 2.4 GHz RF front-end using millimeter-wave EMI in the near-field," *PIER Lett.*, vol. 68, pp. 99–104, 2017. [Online]. Available: http://www.jpier.org/PIERL/pier.php?paper=17032102

[8] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, "Contactless electromagnetic active attack on ring oscillator based true random number generator," in *Constructive Side-Channel Analysis and Secure Design*. Springer, 2012, pp. 151–166.

[9] P. Maistri, R. Leveugle, L. Bossuet, A. Aubert, V. Fischer, B. Robisson, N. Moro, P. Maurine, J.-M. Dutertre, and M. Lisart, "Electromagnetic analysis and fault injection onto secure circuits," in *22nd International Conference on Very Large Scale Integration (VLSI-SoC)*. IEEE, 2014, pp. 1–6.

[10] K. Kim and A. A. Iliadis, "Critical upsets of CMOS inverters in static operation due to high-power microwave interference," *IEEE Transactions on Electromagnetic Compatibility*, vol. 49, no. 4, pp. 876–885, 2007.