# Disruption of a RF Front-End Subject to an Out-of-Band Signal

Pierre Payet, Jérémy Raoult, Laurent Chusseau

# Disruption of a RF Front-End Subject to an Out-of-Band Signal

Pierre Payet, Jérémy Raoult and Laurent Chusseau *Member, IEEE,*

IES, Université de Montpellier, 860 rue de Saint Priest, 34095 Montpellier, France
Email: payet@ies.univ-montp2.fr

***Abstract*—This paper deals with the effects of an electromagnetic interference (EMI) from an out-of-band signal impinging on a 2.4 GHz RF receiver operating in the linear regime. The injection signal is radiated in the near-field above the circuit package at a frequency of 60 GHz. Due to the nonlinear behavior of active devices, we observed a gain quenching leading to a complete inhibition of the receiver that occurs together with a current overconsumption. Disruptions are experimentally studied depending on the position above the package, the distance between the EMI source and the circuit, as well as the frequency used to switch on and off the millimeter source.**

## I. Introduction

ELECTRONIC circuits are sensitive to perturbative signals with frequencies close to their operating frequency [1], this perturbation being either conducted or radiated. Because of the intrinsic performance of individual devices within the modern Si-roadmap, most of the components of a circuit are also sensitive outside the designed operating bandwidth (out-of-band signals) and especially at much more higher frequency than that designed for this purpose [2]. Although high frequencies do not contribute to the output signal, they may induce DC offsets and low frequency amplitude variations at the output [3], mainly because of the non-linear behavior of the active devices within the amplifier. The resulting effect on the expected function that should deliver the electronics are diverse and can range from a low malfunction up to a permanent damage [4], [5], including in-between a logic restart or a reduction of the lifetime of the system [6].

In practice, interferences may be either unwanted or targeted by an attacker. On the one side, unwanted disruptions may result from the multiplication of communicating devices that fill the electromagnetic environment with growing operating frequencies. As an example, a laptop can disrupts a medical device or even tools onboard of an aircraft [7]. This arises because operating frequencies of such unintentional interferers are constantly increasing to reach now the millimeter-wave bands for example with the emergence of the future 5G standard or last Wifi generation 802.11ad [8]. On the other side, a lot of intentional sources exist such as jammers but also military sources dedicated to intentional EMI attack. These sources are usually classified according to their power and/or frequency band, for example in narrow band high power microwave (HPM) sources or high-intensity radiated fields (HIRF) sources produced by electron beam [9] and operating in the 1–100 GHz band. High-power broadband sources use the ultra-wide band (UWB) or radar technologies with pulsed high-voltage generators [10]–[13]. The effects of intentional EMI by such sources have been examined in [14]. They are mainly used on front door targets where the coupling path uses available ports for the propagation of electromagnetic energy and communication with the external environment, for example antennas or sockets [1], [15], [16].

To the best of our knowledge, no EMI study have been conducted yet involving a millimeter-wave source and a usual RF front-end operating in the 2.4 GHz band. In this communication, we focus experimentally on the susceptibility of such a radio receiver subjected to an external 60 GHz signal. Furthermore the receiver is placed in the near-field of the interferer, so as to locally evaluate its susceptibility to EMI and enhance the 60 GHz energy transferred to the target. Such a receiver is expected as a vulnerable target because its goal is to handle signals of very small amplitudes [1]. We will present several results related to this out-of-band disruption signal, namely the distance between the EMI source and the circuit, as well as the modulation frequency used to switch on and off the millimeter source.

## II. Experimental setup

The experimental details are represented in the diagram of Fig. 1. The source used as an interferer is a Gunn oscillator (Quinstar, QTM-602001SV) delivering an output power of $\approx$ 20 dBm. Although the oscillation frequency can be mechanically tuned in a range of $\pm 2$ GHz, it was always set to 60 GHz in the sequel. This source can be switched on and off using a TTL signal whose frequency $f_m$ is limited to 20 kHz. A 35 dB isolator is inserted just after the Gunn source to ensure a stable operation whatever its load. The 60 GHz signal feeds a rectangular WR15 waveguide whose open end radiates the signal onto the device under test (DUT). The 3D positioning of the open end of the waveguide above the circuit package is achieved via motorized stages. To overcome the relatively low power of the source, the DUT is placed as close as possible to the waveguide end of size $3.76 \times 1.88\,\mathrm{mm}^2$. As a major consequence, the DUT is in the near-field of the electromagnetic interferer at typical distances above the circuit package ranging from 0 to 400 $\mu$m. Such distances are well in the near-field zone since the wavelength is $\lambda = 5$ mm. We can thus guarantee that the maximum energy is transferred locally in a small region of the circuit.

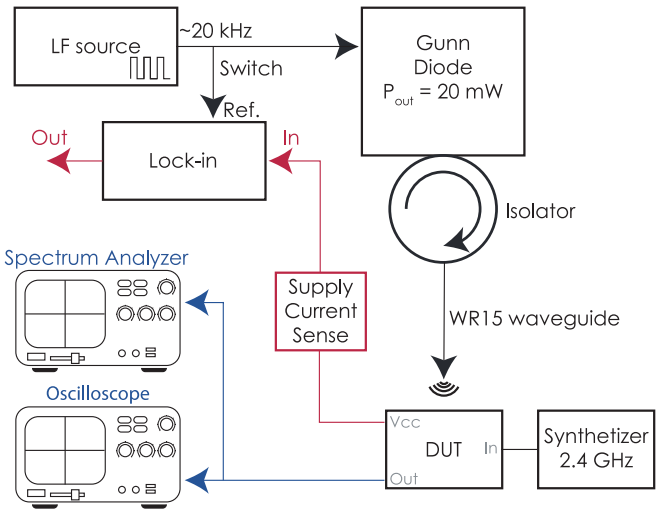


Fig. 1. Scheme of the experimental setup.

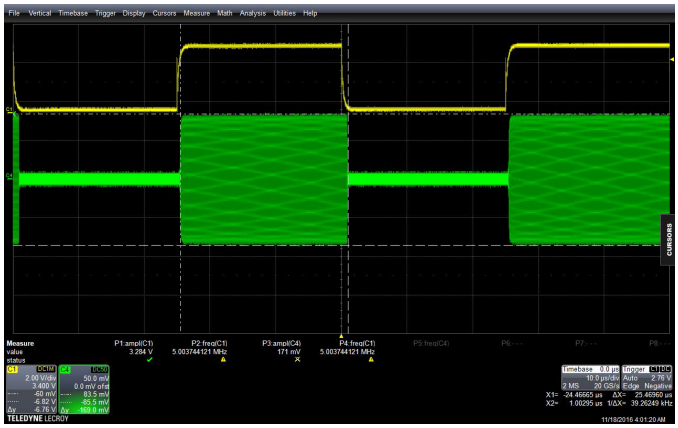

Fig. 2. Screenshot of the time signal at the receiver output (lower trace) and the switching signal applied to the 60 GHz source (upper trace).

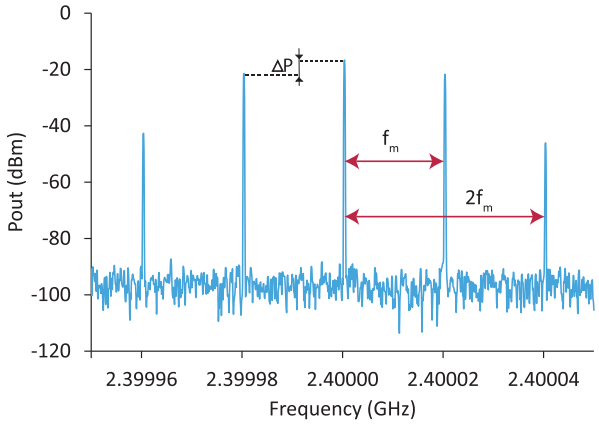


Fig. 3. Frequency measurement of the output signal with an input power of -20 dBm, $f_0 = 2.4$ GHz, $f_m = 20$ kHz.

The DUT (Qorvo, RF6535) is a commercial front-end module that enables Wifi and Zigbee applications in the 2.4 GHz band. A switch is included to select the transmit or receive path, the latter configuration being always active is subsequent experiments. In this receiver mode, the RF6535 exhibits a typical 8.6 dB gain and an average supply current of 10.7 mA. To test the susceptibility, the DUT operates in the linear regime with a -20 dBm, $f_0 = 2.4$ GHz input signal obtained from a Keysight synthesizer N5171B. The output signal is monitored both in time and frequency domains using an Lecroy oscilloscope ZI610 and a Keysight spectrum analyzer (CXA series). Simultaneously we record the supply current with a 1 A/V Hall current probe connected to a lock-in amplifier (Signal Recovery, Model 7265). The output of the lock-in thus provides the amplitude of the first Fourier component of the current at $f_m$.

## III. Results and Discussion

The open waveguide was first positioned as close as possible to the circuit package and we proceed to a 2D scanning while observing the 2.4 GHz output simultaneously in the time and frequency domains. The most sensitive region of the chip was first sought. The Fig. 2 shows both the switching TTL control at $f_m = 20$ kHz and the time signal at DUT output at that particular point.

When the switching signal is high, the Gunn source is turned off and the LNA output exhibits a 2.4 GHz sinusoid figured as a shaded area in Fig. 2 because of the timebase matched to the TTL control and not to the 2.4 GHz signal. When the switching signal is low, the Gunn source is turned on and injects the 60 GHz disruption signal. The major effect noticed here is the complete quenching of the function. Although we expected some disruption in the functional operation of the RF front-end, such a dramatic shut down was unexpected. Notice that it occurs with an out-of-band injection frequency 25 times greater than that of the LNA nominal frequency. The corresponding spectrum is given in Fig. 3. It exhibits numerous sidebands at $f_0 \pm nf_m$ around the signal frequency $f_0 = 2.4$ GHz. Only those close to $f_0$ are pictured in Fig. 3. It is observed that the first sideband amplitudes are only $\Delta P = 5$ dB below that of the fundamental. Such a low power difference is consistent with the strong time distortion observed in Fig. 2.

In a second step, $f_m$ has been varied in the range 200 Hz–20 kHz and the fundamental and first sideband powers were monitored. Results are plotted in Fig. 4. The power at fundamental decreases slowly when $f_m$ increases. In the same time, the power at first sideband increases with a steeper slope. At 10 kHz both power values are frozen and any subsequent evolutions pursue steadily from 10 kHz to 20 kHz. To go further we have represented some time evolutions at 600 Hz, 10 kHz and 20 kHz in the insets of Fig. 4. At both highest frequencies the same time behavior is obtained, *i.e.* the amplification is quenched as soon as the 60 GHz is set, the nominal function being immediately recovered when the

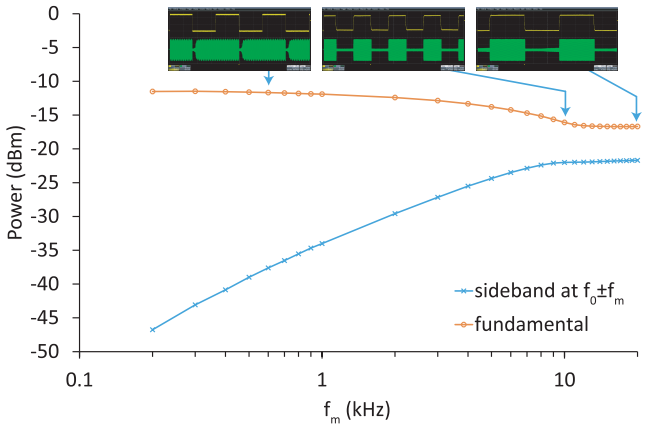


Fig. 4. Evolution of fundamental ($f_0$, circle) and first sideband ($f_0 \pm f_m$, cross) powers versus the switching frequency. Inserts are screenshots at three given switching frequencies.

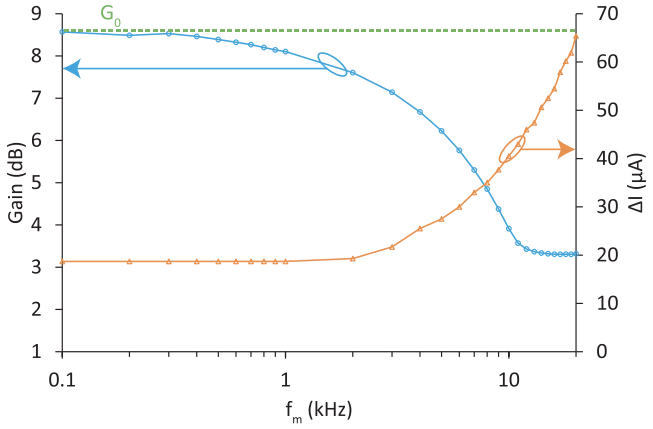


Fig. 5. Evolution of the gain and variation of the supply current as a function of the switching frequency from 0.1 to 20 kHz.

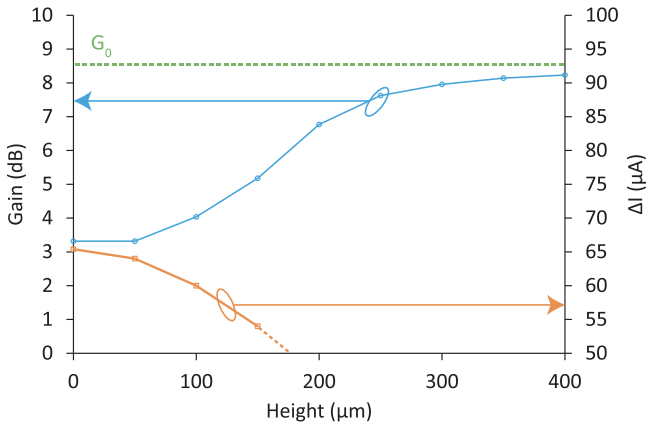


Fig. 6. Evolution of gain and variation of supply current as a function of the height from 0 to 400 μm.

60 GHz is released. At lower frequency, *e.g.* $f_m = 600$ Hz, the amplification recovers before the 60 GHz is turned off. It is worth to point out that this occurs at any frequency $f_m \leq 10$ kHz and that the amplification is quenched during a fixed time $t_q = 100$ $\mu$s. To the contrary, at $f_m > 10$ kHz the effective time of application of the 60 GHz becomes lower than $t_q$ and the front-end quenching exactly mimics the 60 GHz turn-on. This behavior confirms the evolution of fundamental and first sideband powers. On the physical side, applying a CW 60 GHz source seems not sufficient to create an important disruption in the circuit and the switching of source plays a role still unveiled.

For convenience, we now compute a so-called gain $G$ as the ratio of the power at the fundamental, already plotted in Fig. 4, to the power at LNA input. In fact it reproduces a usual datasheet characteristic of the front-end and can be compared to the known nominal gain $G_0 = 8.6$ dB even if it averages both the switch-on and switch-off times of the LNA and must not be confused with the usual gain. $G$ is plotted versus $f_m$ in Fig. 5, it starts from $G_0 = 8.6$ dB at the lowest $f_m$-values and loses 5 dB when $f_m \geq 10$ kHz, reaching at that point its minimum value. From a system point of view, the RF front-end seems unperturbed at low $f_m$, although we saw previously that any switching edge of the 60 GHz source induces a transient shut down of duration $t_q$.

The Fig. 5 also plots the variation of the supply current $\Delta I$ as a function of $f_m$. As seen, $\Delta I \approx 20\,\mu$A up to 2 kHz but it is never null, thus being a kind of witness of the disruption of the circuit albeit the gain remains at its nominal value. At $f_m > 2$ kHz, $\Delta I$ increases strongly with the switching frequency. We can infer that such growth may continue above our experimental limit of $f_m > 20$ kHz. This phenomenon seems uncorrelated to $G$, which tends asymptotically to a constant value above $f_m = 10$ kHz.

To complement the experimental characterization, the influence of the stand-off distance $h$ between the open waveguide and the package has been evaluated. Starting from the conditions of Fig. 1 where a contact with the package was established, $h$ is increased up to 400 $\mu$m. Increasing $h$ will lower the mm-wave power seen by the DUT, and by the way the induced disruption. The Fig. 6 thus plots the gain $G$ and $\Delta I$ as a function of $h$. As we guess the LNA gain recovers with the increase of $h$, according to the expected lowering of mm-wave power coupled to the circuit. Experiments then evidence the expected disruption dependence with the power excitation. Intuitively, the current decrease observed simultaneously with the $G$ increase proceeds of the same dependence of the coupling with mm-wave power. To get more insights into the effect of incident power, we observed the time traces while moving the waveguide probe. We found that the quenching time $t_q$ regularly decreases from its value at contact $t_q = 100$ $\mu$s to about $t_q = 25$ $\mu$s at a height $h = 300$ $\mu$m. As a consequence a return to a quasi nominal state is obtained at $h = 400$ $\mu$m.

## IV. Conclusion

A 60 GHz injection experiment has been presented and applied to a RF receiver front-end operating in the 2.4 GHz band. The radiative disruption we submit the circuit to is therefore largely out-of-band, leading to the amazing total inhibition of the RF function when the EMI is applied. Such a quenching of the amplification was shown fully reproducible and non-permanent. In relationship with the disruption we observed some current overconsumption by the circuit that is some kind of witness of the attack as seen from the circuit side.

We have highlighted the influence of two parameters on this disruption, namely the switching frequency of the mm-wave source and the stand-off distance between the illuminating waveguide and circuit package. Changes in the switching frequency have demonstrated the importance of source transients. Increasing the stand-off distance have resulted in a decrease of the effective mm-wave power seen by the circuit and therefore has lowered the disruption both on the receiver gain and current overconsumption.

In the future this injection method will be tested on other receiving modules with other operating frequencies and with other pulse shapes.

## References


[1] D. Mansson, R. Thottappillil, M. Backstrom, and O. Lundén, "Vulnerability of european rail traffic management system to radiated intentional EMI," *IEEE Transactions on Electromagnetic Compatibility*, vol. 50, no. 1, pp. 101–109, 2008.

[2] C. Pouant, J. Raoult, and P. Hoffmann, "Large domain validity of MOSFET Microwave- Rectification Response," *International Workshop on the Electromagnetic Compatibility of Integrated Circuits (EMC Compo)*, pp. 232–237, 2015.

[3] M. J. Van der Horst and A. Linnenbank, "Amplitude-Modulation Detection in Single-Stage Negative-Feedback Amplifiers Due to Interfering Out-of-Band Signals," *IEEE Transactions on Electromagnetic Compatibility*, vol. 47, no. 1, pp. 34–44, 2005.

[4] R. Hoad, N. J. Carter, D. Herke, and S. P. Watkins, "Trends in EM Susceptibility of IT Equipment," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 390–395, 2004.

[5] R. Thottappillil, D. Månsson, and M. Bäckström, "Response of Electrified Railway Facilities to Intentional Electromagnetic Interference : Review of Research at Uppsala University," *Asia-Pacific Sympsoium on Electromagnetic Compatibility & 19th International Zurich Symposium on Electromagnetic Compatibility*, pp. 291–294, 2008.

[6] W. Radasky and E. Savage, "Intentional Electromagnetic Interference ( IEMI ) and Its Impact on the U . S . Power Grid," *Metatech Corporation*, 2010.

[7] S. Bandopadhyay and J. Varkey, "Emi susceptibility characteristics of electromedical equipment in a typical hospital electromagnetic environment with particular reference to electrocardiography," in *International Conference on Electromagnetic Interference and Compatibility*. IEEE, 1995, pp. 266–272.

[8] E. Perahia, C. Cordeiro, M. Park, and L. L. Yang, "Ieee 802.11 ad: Defining the next generation multi-gbps wi-fi," in *2010 7th IEEE Consumer Communications and Networking Conference*. IEEE, 2010, pp. 1–5.

[9] E. Schamiloglu, "High Power Microwave Sources and Applications," *Microwave Symposium Digest, 2004 IEEE MTT-S International*, vol. 2, pp. 1001–1004, 2004.

[10] V. G. Baryshevsky, A. E. Borisevich, A. A. Gurinovich, G. Y. Drobyshev, P. V. Molchanov, and A. V. Senko, "A compact high power microwave (HPM) source," *Pulsed Power Conference, 2009 IET European*, 2009.

[11] W. Carey, A. Wiebe, D. Schwindt, L. Altgilbers, M. Giesselmann, B. McHale, and K. Heinemann, "Autonomous RF Radiation Package for Various Applications," *IEEE Pulsed Power Conference*, pp. 218–221, 2005.

[12] C. E. Baum, W. L. Baker, W. D. Prather, J. M. Lehr, J. P. O'Loughlin, D. V. Giri, I. D. Smith, R. Altes, J. Fockler, D. McLemore, M. D. Abdalla, and M. C. Skipper, "JOLT : A Highly Directive , Very Intensive , Impulse-Like Radiator," *Proceedings of the IEEE*, vol. 92, no. 7, pp. 1096 – 1109, 2004.

[13] R. Pecquois, "Etude et réalisation d'une source de rayonnement large bande de forte puissance basée sur un concept innovant de transformateur résonant impulsionnel," *Ph.D. dissertation, Université de Pau*, 2012.

[14] 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.

[15] M. G. Bäckström and K. G. Lövstrand, "Susceptibility of Electronic Systems to High-Power Microwaves : Summary of Test Experience," *IEEE Transactions on Electromagnetic Compatibility*, vol. 46, no. 3, pp. 396–403, 2004.

[16] F. Fiori, S. Benelli, G. Gaidano, and V. Pozzolo, "Investigation on VLSIs' Input Ports Susceptibility," *IEEE International Symposium on Electromagnetic Compatibility*, pp. 326–329, 1997.