Hindawi Publishing Corporation
International Journal of Antennas and Propagation
Volume 2016, Article ID 4715898, 6 pages
http://dx.doi.org/10.1155/2016/4715898

Research Article

Far-Field Testing Method of Spurious Emission Produced by HF RFID

Nikola Gvozdenovic,[1] Ralph Prestros,[2] and Christoph F. Mecklenbräuker[1]

[1]*Christian Doppler Lab for Sustainable Mobility, Institute of Telecommunications, Vienna University of Technology, Gusshausstrasse 25/E389, 1040 Vienna, Austria*
[2]*NXP Semiconductors Austria GmbH, Mikronweg 1, 8101 Gratkorn, Austria*

Correspondence should be addressed to Nikola Gvozdenovic; ngvozden@nt.tuwien.ac.at

Received 22 December 2015; Revised 4 March 2016; Accepted 24 April 2016

Academic Editor: Ji-Woong Choi

We present measurements of spurious emission produced by high-frequency radio frequency identification (HF RFID) using carrier frequency of 13.56 MHz. HF RFID tags produce unwanted emission due to rectification and more generally due to nonlinearity of analog front end. Depending on the conducting material of an HF RFID coil and surrounding dielectric material, the coil behaves as more or less good antenna on some harmonic frequencies. Exact characterization and analysis of unwanted emission is important from the security perspective as well as from the perspective of interference with other systems. Consequently we measured the harmonics produced in the integrated circuitry and characterized radiation properties of the antenna. Finally we present the measurements of the spurious emission performed in a Gigahertz Transverse Electromagnetic (GTEM) cell.

1. Introduction

The investigation of spurious emissions produced by contactless chip-cards is of interest due to potential interference with other systems and due to security and privacy concerns. Many RF power and data transfer systems employ strong encryption like 3DES or AES thus greatly decreasing possibility for loss of confidential information. However, some systems (building access and inventory systems) use uncoded data on the tags which are vulnerable to reply style attacks.

In these systems the information is transmitted at the fundamental frequency through magnetic field which is proportional to the inverse cube of the distance [1]; thus the distance at which the unwanted emission is detectable is quite small, couple of meters.

On the harmonic frequency the spurious emission is carried by the electromagnetic field which decays slowly, proportional to the inverse square of the distance [1]. As we will present in this paper the field strength of this emission is also very low compared to the spectral mask and therefore practically undetectable.

In [2] the authors measured spurious emission distance for exemplary ISO/IEC 14443 type A transponder and reader configurations in different environments using higher-order harmonics. In [3, 4] electromagnetic emission of HF RFID system is measured and its susceptibility to jamming and eavesdropping is evaluated.

Harmonics and intermodulation products are produced by the nonlinear RF front end of the integrated circuitry. They are more or less efficiently radiated by the antenna depending on which frequencies they are and what is the radiation characteristic of the antenna on that frequency. When we have the radiation properties of the antenna and the value of the nonlinearity produced by the electronic circuitry of the device that is powered by RF we can think of various methods to decrease the spurious emissions or even to completely block it.

Harmonic analysis in RFID systems currently is well studied in UHF RFID, like in [5]. Here also a redundant harmonic link is proposed [6, 7].

Antennas for near-field power and data systems are optimized to efficiently transfer power and information on the carrier frequency by magnetic coupling. We analyzed the behavior of these antennas on other frequencies by simulating them with one of the EM simulators and by measuring their

Figure 1: Signal received on the tower.

radiation properties in an anechoic chamber. We observe that on some frequencies the radiation properties of these antennas deteriorate significantly but on some they radiate well.

A method for accurate measurement of harmonics produced by an HF RFID chip is explained in Section 4. The strength of the harmonics produced by the circuitry strongly depends on the power induced in it so spurious emission produced by a tag is higher if the reader uses higher power. Thus this can be a reason for an attack of malware on a reader.

This paper is organized as follows: in Section 2 we give an overview of communication properties of the HF RFID. In Section 3 we investigate radiation properties of HF RFID antenna. In Section 4 we show a model of the circuitry for spurious emission and measurement of the harmonics produced. Measurement of the spurious emission of the whole system is shown in Section 5.

2. HF RFID Overview

Contactless chip cards are defined in the standard [8]. Communication system consists of a tag called proximity identity chip card (PICC) and a reader called proximity coupling device (PCD). PICC and PCD are magnetically coupled on 13.56 MHz carrier frequency. Consequently as an antenna for both PICC and PCD planar spiral coil is used. PCD is a source of magnetic field and powers the PICC. There are two communication interfaces:

> Type A: downlink, ASK with Modified Miller code, uplink, load modulation with ASK Manchester code
>
> Type B: downlink, ASK with NRZ code, uplink, load modulation with BPSK NRZ code.

PICC is powered through magnetic field on the carrier frequency and uses highly power-efficient load modulation on the uplink where it changes its input impedance by switching a transistor at the RF front end and thus modulates the carrier produced by the PCD.

According to standard PICCs are tested in "PCD test assembly" at a distance of 10 cm from the PCD coil. In Figure 1 we show reader's request A (REQA) package and tags anticollission A (ATQA) response. There is 86.43 μs long pause between two packages.

In our experiment, we look for this signal shape on harmonic frequencies.

3. Radiation Properties of HF RFID Antenna

Typical coil used in a PICC as specified in the standard [8] is shown in Figure 2.

PICC antenna geometry is defined by the outer dimensions a and b, number of turns N, pitch p (distance between centers of conductors), and conductor width w. By varying these basic geometrical parameters we can manipulate the radiation properties of the antenna on the harmonic frequencies on which we want to prevent the spurious emission. PEEC (partial element equivalent circuit) model of PICC antenna is presented in [9, 10] and evaluated by measurement which can be used for simulation and modeling of radiation properties of the antenna. In those publications we showed that measurement results and HFSS simulation match well. Consequently in this section we will use HFSS to simulate the properties of the antenna.

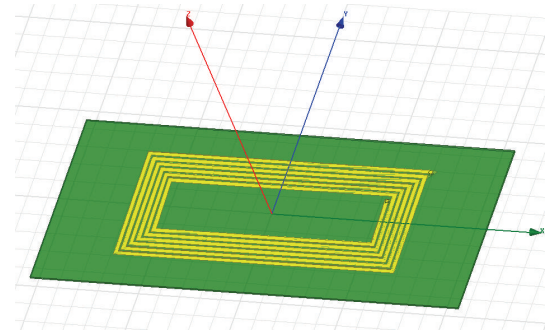


Figure 2: Typical PICC antenna geometry: 70 × 30 mm size, N = 6 turns, conductor width w = 1 mm, and pitch p = 2 mm. Card substrate is Rogers RO4350 and the thickness is 51 mm.

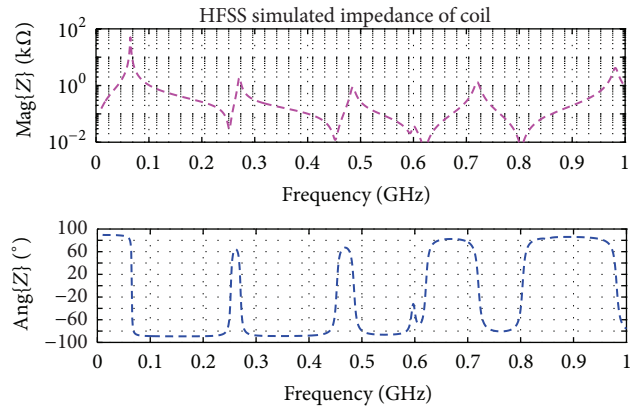


Figure 3: Coil impedance versus frequency.

Integrated circuitry of the PICC produces harmonics due to nonlinear analog front end. Especially dangerous are odd harmonics on the UHF frequencies since the antenna of the potential eavesdropper is small enough (e.g., to be placed in a backpack). These harmonics are then radiated by the coil which on the harmonic frequency behaves as an antenna.

Impedance of the antenna geometry from Figure 2 versus frequency is shown in Figure 3. The antenna is dominantly inductive up to the first antiresonance. Due to parasitic capacitive effects on the antenna there are resonances on the higher frequencies on which spurious emission can occur.

Figure 4 shows radiation pattern of PICC antenna on 266 MHz. Antenna behaves as a small magnetic loop antenna. Maximum gain is in the plane of the antenna.

This is important to know in which direction we should fight the spurious emission.

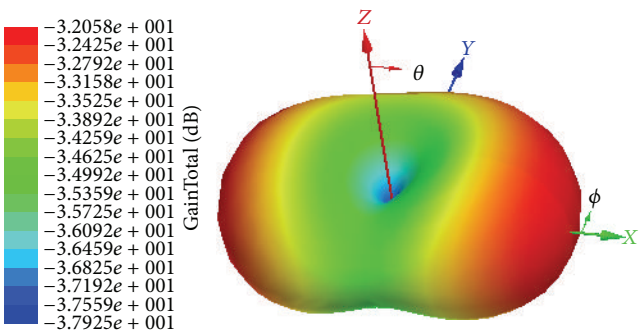


FIGURE 4: Radiation pattern of PICC antenna on 266 MHz. Antenna behaves as a small magnetic loop antenna. Maximum gain is in the plane of the antenna.

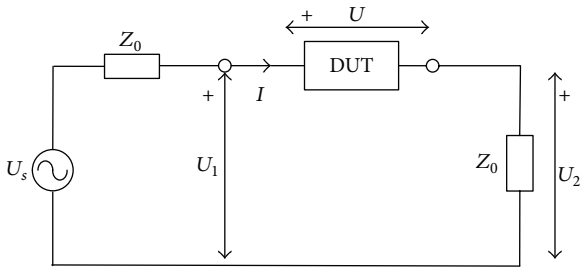


FIGURE 5: Measurement circuit reference model.

4. Harmonic Model of HF RFID Integrated Circuitry

In this section we discuss measurement and modeling of nonlinearity of HF RFID chips. More details on the measurement are given in [11].

Since it is expected that chip has high input impedance reflection method is prone to error. Consequently we used series measurement setup proposed in [12] to measure chip's impedance as well as amplitude of harmonics produced by the chip. The chip is placed in a test fixture, and the inner conductors are connected through the chip while outer conductors are short-circuited through the test fixture as shown in Figure 5.

For the measurements we use a ZVA8 VNA by Rohde & Schwarz which is controlled by Matlab through VISA interface. VNA generates signal at port 1 on the fundamental frequency on the specific power level. This signal is amplified to increase the range of the signal. Since the amplifier and VNA itself induce harmonics, a custom designed low-pass filter (LPF) is used that also provides an impedance of 50 Ω for all harmonics produced by DUT.

We measured S_{21} parameter and b_2/a_1 ratio with VNA using series method as in [11]. From that we can find chip impedance and currents and voltages on the chip on both fundamental and harmonic frequencies as

$$Z_t = 2Z_0 \frac{1 - S_{21}}{S_{21}},$$

$$I_f = \frac{U_s}{Z_t + 2Z_0} = \frac{U_s}{2Z_0} S_{21},$$

$$I_h = \frac{U_s}{2Z_0} \frac{b_2}{a_1},$$

$$U_f = U_s \left(1 - S_{21}\right),$$

$$U_h = U_s \left(1 - \frac{b_2}{a_1}\right), \tag{1}$$

where Z_t is the impedance of the chip, I_f and U_f are current and voltage on the chip on the fundamental frequency, and I_h and U_h are current and voltage on the chip on the harmonics.

We recalculate the power produced on port 1 of the VNA to source voltage as

$$P = \frac{U_s^2}{Z_0},$$

$$n\,[\text{dBm}] = 10 \log \frac{P\,[\text{W}]}{1\,\text{mW}}, \tag{2}$$

$$U_s = \sqrt{10^{n[\text{dBm}]/10} \cdot Z_0}.$$

We analyze the chip's response at the fundamental and odd numbered harmonic frequencies ($3f_0$, $5f_0$, etc.) as a function of the available power at the fundamental frequency of $f_0 = 13.56$ MHz. Impedance is calculated from the S_{21} measurement at the fundamental. The generated harmonics are related to the incoming wave at port 2 of the VNA (b_2).

An equivalent circuit model commonly used for HF RFID chip [13, 14] is shown in Figure 6(a). Elements of this model are

(i) input capacitor C_{in} for tuning the antenna,

(ii) full-wave rectifier (consisting of diodes like in Figure 6(a) or of transistors),

(iii) shunt voltage regulator for stabilizing the internal DC voltage,

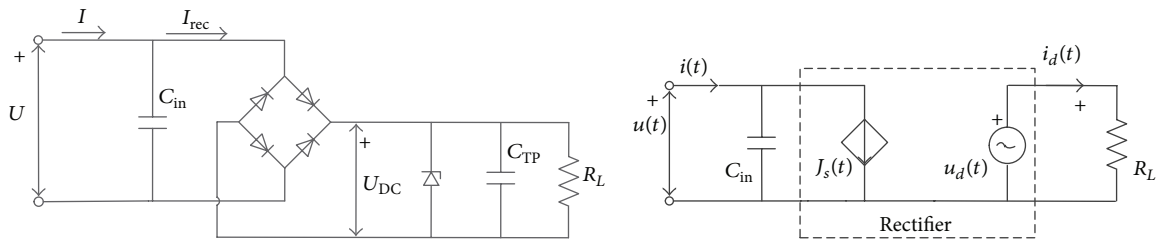
(iv) capacitor C_{TP} for storing the DC charge,

(v) resistor R_L as the load of the digital circuitry.

Commonly used harmonic model for full wave rectifier circuit is shown in Figure 6(b). Due to rectification chip behaves as current controlled current source. It produces harmonic currents on the AC sides which are controlled by DC current inside the chip:

$$i_s(t) = \sum_{n=1,3,5,\ldots}^{\infty} \frac{4}{n\pi} I_d \sin\left(n2\pi f_0 t\right) = i_{sf}(t) + i_{sh}(t). \tag{3}$$

Current and voltage shapes on the rectifier are shown in Figure 7. AC current in the rectifier starts flowing in the point when AC and DC voltages are equal. We can see that the harmonics produced on AC side are mostly due to AC current shape [15]. If we do Fourier analysis of the currents we will see that ideally it consists only of the odd harmonics. AC voltage harmonics exist but are less pronounced. DC voltage has sawtooth shape and consists mostly of the even harmonics. We can find DC current as $I_{\text{DC}} = U_{\text{DC}}/R_L$.



(a) Proposed reference chip model (b) Simplified harmonic model of a chip

Figure 6: Proposed reference model and simplified harmonic model of a chip.

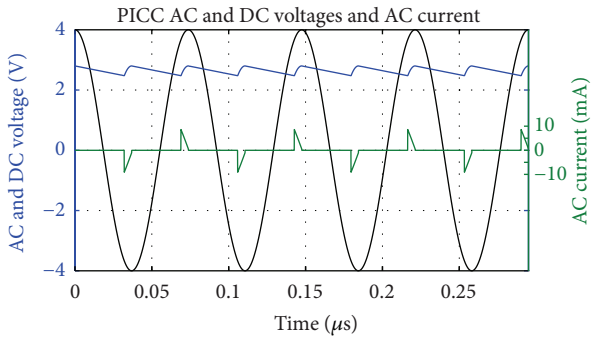


Figure 7: Rectifier AC current and voltage and DC voltage.

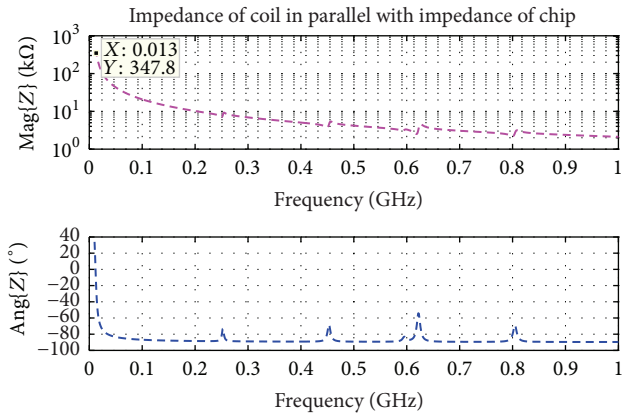


Figure 8: Equivalent PICC impedance (chip in parallel with antenna).

This model is strongly simplified but helps us in understanding our measurement results. Usually the rectifier consists of transistors, and the limiter as well as the internal circuitry has more complicated structure, but the final chip should be in compliance with this reference PICC circuit.

Now we investigate the behavior of the whole card. RF frontend of an HF RFID chip is capacitive and it is connected in parallel to an inductive coil, thus forming a resonance circuit. The resonance frequency of the tag is predefined and should be in a certain range (14–16 MHz).

In Figure 8 we show the equivalent PICC impedance (chip in parallel with the antenna) versus frequency. We see that there is first resonance on 13 MHz but also there are resonances on higher frequencies.

5. Spurious Emissions Measurement in GTEM Cell

To accurately measure far-field radiation of harmonic and to avoid interference from other systems we used Gigahertz Transverse Electromagnetic (GTEM) cell shown in Figure 9(a). GTEM cell has pyramidal shape and its outer structure is metallic and conductive. Inner conductor called septum is shifted from the center of the structure and is the upper border of usable test volume. The port A at the tip of the GTEM cell has a 50 Ω coaxial connector and the septum is terminated with a 50 Ω resistor box. The basis of the pyramidal structure is covered with high-frequency absorbers.

Equipment under test (EUT) is placed in the GTEM cell as shown in Figure 9(b). The placing as well as positioning of the structure depends on the size of the GTEM cell and it is defined in the standard [16].

The block diagram of the measurement setup is shown in Figure 10. Reader antenna called Poller0 (matching is included) and a PICC are placed inside the cell. The KeoLab reader is outside of the cell; it is connected through the cell to its antenna and sends reader signal. LPF is used to filter out harmonics produced by the reader. Additionally, the reader is connected to the signal analyzer for triggering. Signal analyzer is connected to GTEM cell coaxial connector and receives both reader signal and PICC response. For the far-field measurements the EUT should be placed in three orthogonal orientations. Using these three measurement results the GTEM software based on the standard [16] calculates electrical field that would be radiated at 10 m distance.

First we wanted to see what is the power produced by the reader. That is why we have connected the reader directly to the signal analyzer. The power of the signal produced by the reader is less than but close to 1 W.

Next we connected the setup and measured harmonics in the GTEM cell. In Figure 11 we show power at port A of the signal on the third harmonic: PCD command REQA and PICC response ATQA. REQA has fixed value of 26 hex and ATQA is variable and in this case 0400 hex. There is an 86.43 μs break in between commands, so called frame

(a) GTEM cell (b) EUT

Figure 9: GTEM cell and EUT.

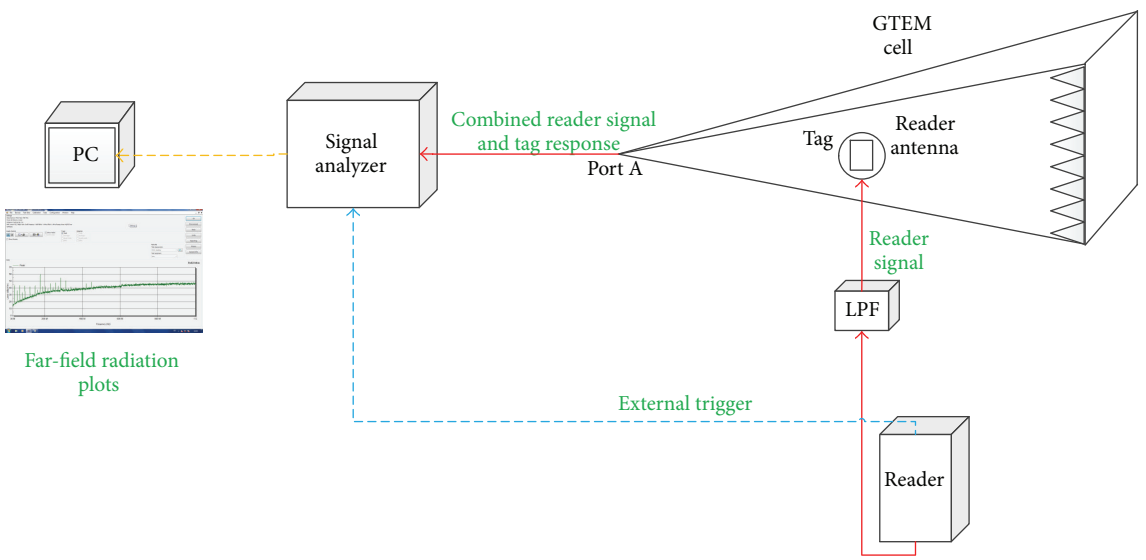


Figure 10: The block diagram of the measurement setup.

delay time (FDT). The signal analyzer settings for these measurements are as follows:

FREQ: $n \times f_0 + f_0/16$,

$f_0 = 13.56$ MHz, $n = 1, 2, 3, 4, \ldots$,

SPAN: ZeroSpan,

BW: 1 MHz,

AMP: Unit: dBm,

BW: FilterTypeChannel,

TRACE: DetectorManualSelect: RMS.

In Figure 12 we show far-field emission of harmonics up to 1 GHz measured in GTEM cell. This is the electrical field radiated by the EUT at 10 m distance. We observe that the odd harmonics are significantly stronger than the even ones. The harmonics produced by the reader dominate over the weak response from the card. The spurious emission is below the radiation emissions limit for incidental radiators defined in [17].

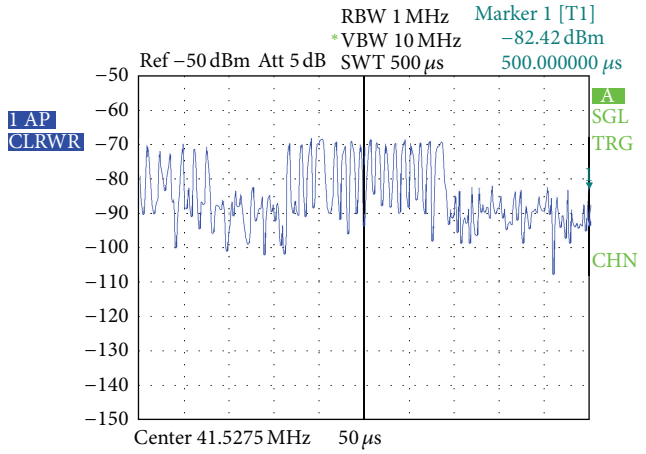


Figure 11: REQA and ATQA on the third harmonic.

This setup can be used as a reference for different methods of spurious emission suppression.

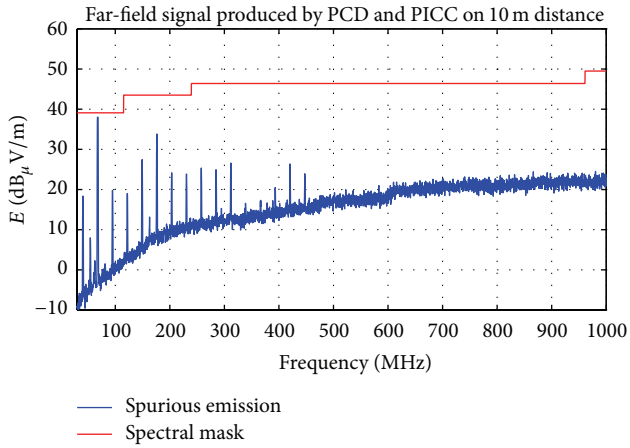


Figure 12: Emission measurement in GTEM cell (PCD and PICC).

6. Conclusions

In this paper, we have investigated spurious emission from the HF RFID tags. First we have investigated radiation properties of an HF RFID antenna. We see that the antenna radiates well on certain frequencies. Afterwards we characterize harmonic behavior of an analog front end of the integrated circuit. Due to rectification, most dangerous are odd harmonics. Finally we measured in a GTEM cell electric field radiated by an HF RFID tag on frequencies up to 1 GHz. As shown above both the PCD and PICC signals are very low compared to the spectral mask and therefore practically undetectable.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This work has been funded by the Christian Doppler Laboratory for Wireless Technologies for Sustainable Mobility, the Federal Ministry of Economy, Family and Youth, and the National Foundation for Research, Technology and Development of Austria and by the authors' industrial partner NXP Semiconductors Austria GmbH.

References

[1] J. Kraus and D. Fleisch, *Electromagnetics: With Applications*, Mcgraw-Hill International Editions, Electrical Engineering Series, WCB/McGraw-Hill, Boston, Mass, USA, 1999.

[2] M. Engelhardt, F. Pfeiffer, K. Finkenzeller, and E. Biebl, "Extending ISO/IEC 14443 type a eavesdropping range using higher harmonics," in *Proceedings of the European Conference on Smart Objects, Systems and Technologies (SmartSysTech)*, pp. 1–8, Erlangen/Nuremberg, Germany, June 2013.

[3] D. R. Novotny, J. R. Guerrieri, M. Francis, and K. Remley, "HF RFID electromagnetic emissions and performance," in *Proceedings of the IEEE International Symposium on Electromagnetic Compatibility (EMC '08)*, pp. 1–7, IEEE, Detroit, Mich, USA, August 2008.

[4] J. R. Guerrieri, D. R. Novotny, M. H. Francis, and K. Remley, "Electromagnetic emissions and performance for proximity RFID," in *Proceedings of the 3rd European Conference on Antennas and Propagation (EuCAP '09)*, pp. 1997–2001, Berlin, Germany, March 2009.

[5] G. Andía Vera, Y. Duroc, and S. Tedjini, "Analysis of harmonics in UHF RFID signals," *IEEE Transactions on Microwave Theory and Techniques*, vol. 61, no. 6, pp. 2481–2490, 2013.

[6] G. A. Vera, Y. Duroc, and S. Tedjini, "Redundant backscattering modulation of passive UHF RFID tags," in *Proceedings of the IEEE MTT-S International Microwave Symposium Digest (MTT '13)*, pp. 1–3, Seattle, Wash, USA, June 2013.

[7] G. A. Vera, Y. Duroc, and S. Tedjini, "Tag-to-reader harmonic link in passive UHF RFID," in *Proceedings of the IEEE MTT-S International Microwave Symposium (IMS '14)*, pp. 1–4, June 2014.

[8] Identification cards—Contactless integrated circuit cards—Proximity cards, ISO/IEC Std. 14 443, 2008.

[9] N. Gvozdenovic, L. Mayer, R. Prestros, C. Mecklenbruker, and A. Scholtz, "PEEC modeling of circular spiral coils," in *Proceedings of the European Microwave Conference*, pp. 1103–1106, Nuremberg, Germany, October 2013.

[10] N. Gvozdenovic, R. Prestros, and C. F. Mecklenbräuker, "HF RFID spiral inductor synthesis and optimization," in *Proceedings of the International Symposium on Wireless Personal Multimedia Communications (WPMC '14)*, pp. 53–59, Sydney, Australia, September 2014.

[11] N. Gvozdenovic, L. W. Mayer, and C. F. Mecklenbrauker, "Measurement of harmonic distortions and impedance of HF RFID chips," in *Proceedings of the 8th European Conference on Antennas and Propagation (EuCAP '14)*, pp. 2940–2944, April 2014.

[12] *Impedance Measurements—Evaluating EMC Components with DC Bias Superimposed*, Agilent Technologies, Santa Clara, Calif, USA, 2009, http://cp.literature.agilent.com/litweb/pdf/5989-9887EN.pdf.

[13] W. Lin, B. Geck, and H. Eul, "Optimization of NFC compatible transponder with respect to the nonlinear IC impedance," in *PRoceedings of the IEEE MTT-S International Microwave Workshop Series on Wireless Sensing, Local Positioning and RFID (IMWS '09)*, pp. 1–4, IEEE, Cavtat, Croatia, September 2009.

[14] K. Finkenzeller, *RFID-Handbuch: Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC*, Hanser, 2008, http://books.google.at/books?id=49HTBDrfqFUC.

[15] D. I. O. A. R. Djordjevic, *Ispitivanje Elektromagnetne Kompatibilnosti/Examination of Electromagnetic Compatibility*, Edited by D. I. O. A. R. Djordjevic, Akademska Misao/Academic Mind, 2012.

[16] ISO/IEC Std, "Electromagnetic compatibility (EMC) Part 4–20: testing and measurement techniques Emission and immunity testing in transverse electromagnetic (TEM) waveguides," IEC 61000-4-20, 2010.

[17] FCC Title 47 CFR Part 15 Rules: Unlicensed RF Devices, FCC Std., https://en.wikipedia.org/wiki/Title_47_CFR_Part_15.