Range Extension of an ISO/IEC 14443 type A RFID System with Actively Emulating Load Modulation

Klaus Finkenzeller, Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81607 München, Klaus.finkenzeller@gi-de.com
Florian Pfeiffer, perisens GmbH, Arcistr. 21, 80333 München, pfeiffer@perisens.de
Erwin Biebl, Fachgebiet Höchstfrequenztechnik der Technischen Universität München, Arcistr. 21, 80333 München, biebl@tum.de

Summary / Abstract

Originally designed for contactless smart cards in the form factor ID1, today ISO/IEC 14443 finds new applications in an increasing number of different form factors. Most famous among the new form factors are applications such as the electronic passport (e-passport) or contactless credit cards in a form factor that is only half or one third as large ("key fob") as ID1. The need of increasingly smaller form factors, however, more often leads to problems in the field, because the small transponder cannot always be read out reliably. This has led to a new type of a battery powered transponder, actively emulating load modulation, to enhance the operating distance. Whereas ISO/IEC 14443 focuses on very small antennas and small transmission power to allow reliable communication distances of a few centimetres, we were looking in the opposite direction. Using quite large antennas and huge transmission power we achieved communication distances in the range of a few meters. We also learned, however, that the effort spent to enhance the reading range increases drastically with each additional meter, quickly ending up with equipment like a "broadcast radio station". The issue presented in this paper is not linked to a future application, but describes the practical limits of a potential attack scenario.

February 24, 2011

1 Introduction

Inductively coupled RFID systems are being used in a huge number of applications such as payment (credit cards), ticketing (public transport and events), access control (company card) and identity verification (ePass, eID). Inductively coupled RFID systems are operated in the 13.56 MHz band and are primarily covered by the ISO/IEC standards 14443, 15693, 18000-3 and 18092.

The majority of applications mentioned above operate according to ISO/IEC 14443. This standard is designed for high security communication with ID-sized (smart card) transponders at proximity distances of 10 cm or less [4]. Transponders are field powered and use load modulation to transmit data back to a reader.

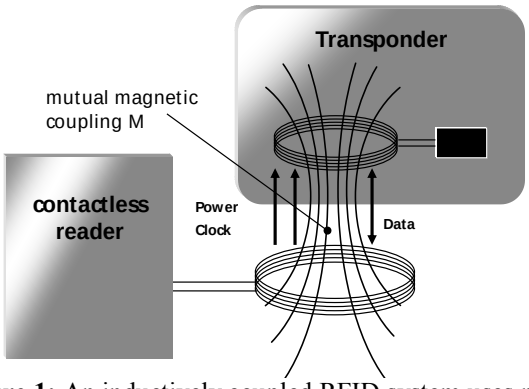

Figure 1: An inductively coupled RFID system uses mutual magnetic coupling to transfer power and data.

The operating range is limited by the coupling factor between the reader/interrogator antenna and the transponder antenna. The coupling factor itself depends on the geometry between the reader and transponder antenna, namely the diameter of the antennas and the distance between the antennas.

In this paper, we discuss the possibility to overcome these limitations by using battery powered, active transmitting transponders, emulating load modulation, with a focus on the physical limits when using any power and any antenna size of the transponder antenna.

2 Limiting factors

Contactless transponders according to ISO/IEC 14443 are powered from the high frequency field generated by the reader. The field strength of the magnetic field in zero distance is defined between 1.5 and 7.5 A/m. If a transponder comes into proximity of a reader, this strong magnetic field induces a voltage which can be used to supply the transponder with energy. To transfer data from the reader to the transponder, simple amplitude shift keying (ASK) is used.

To transfer data from a transponder back to a reader, load modulation is used. To do so, a modulation resistance connected in parallel to the antenna of the transponder is switched on and off at the clock rate of the signal to be

transmitted. ISO/IEC 14443 specifies that the load resistor is keyed by a modulated subcarrier (fc = 848 kHz). The subcarrier itself is ASK modulated with the Manchester coded data signal at a bitrate of 106 kBit/s.

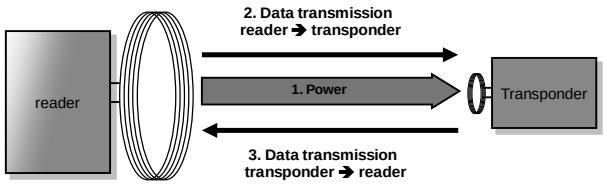

Figure 2: The limiting factors of a contactless communication. (1) Power transfer: the small antenna cannot extract enough power from the field and therefore (2) not receive any data. (3) Load modulation: the return signal from the small antenna to the reader is too small with load modulation

The limiting factors of such a system with regard to the communication range are
(1) the ability to supply a contactless smart card with adequate power for operation in the power range of the reader and in parallel
(2) the reception of data transmitted by the reader, and
(3) the ability to transmit data from the smart card back to the reader, which requires sufficient magnetic coupling between the reader antenna and the smart card antenna (coupling factor k and mutual magnetic inductance M).
A range of approximately 5 to 10 cm can be reached in contactless systems compliant with ISO/IEC 14443 using smart cards in the typical ID1 format. However, the achievable range drops dramatically when very small (SIM cards, micro SD cards) or very large (> ID1) transponder antennas are used, as the coupling factor between the reader and transponder antenna gets quite small. In the worst case, a transponder can no longer be accessed by any reader in proximity to the transponder.

3 Principles of active load modulation

To solve this problem, the limiting factors must be eliminated. In the case of the power range (1), this problem can be solved very simply. To do this, it is only necessary to supply the contactless smart card with power by means of an electrical contact.
The problem of data transmission (3) from the card to a reader is somewhat more complex. Even with a card having a supplementary source of power (an active card), conventional load modulation is not a satisfactory solution because it provides only marginal improvement over a passive card unless the magnetic coupling is improved. A possible solution is to use some other method to generate a signal with the same spectral characteristics as a load modulation signal and to actively transmit this signal to the reader. This is precisely the method to be used in small battery supplied tags.

If we observe the frequency spectrum at the reader antenna resulting from load modulation, in the case of ISO/IEC 14443 we see two additional spectral lines (at 12.712 MHz and 14.408 MHz) along with the carrier signal (at 13.56 MHz). These additional signals are separated from the carrier signal by the subcarrier frequency (848 kHz), with modulation sidebands on each side of these signals. The transmitted data is contained exclusively in these modulation sidebands.

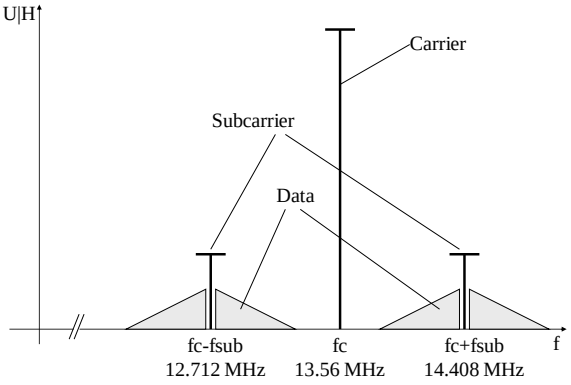

Figure 3 shows the frequency spectrum at the reader antenna resulting from load modulation with a subcarrier.

To transmit data from an active transponder to a reader, it is only necessary to generate the two subcarrier spectral lines along with the sidebands containing the data and transmit them to the reader. The carrier signal does not have to be transmitted since it is transmitted constantly by the reader anyway. A signal with these properties is known as dual sideband (DSB) modulation.

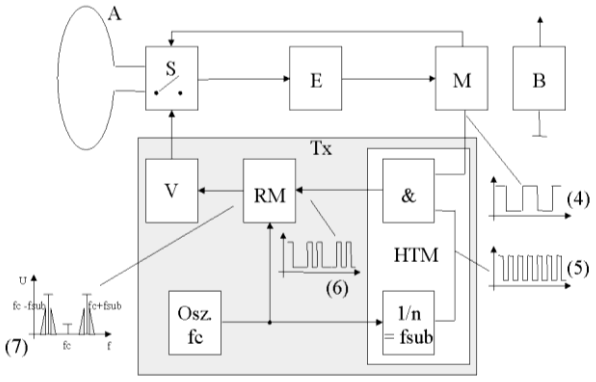

Figure 4: Basic circuit of a transponder, generating active load modulation.

A basic telecommunication circuit that can be used to generate such a DSB modulation is the ring modulator (RM). Figure 4 illustrates the use of such a circuit as a RF interface in an active RFID transponder. The inputs to the ring modulator are a 13.56-MHz carrier signal (fc) and the modulated subcarrier (6). The output signal (7) of the ring modulator is the required DSB signal. The amplitude of

this signal is increased by an amplifier (V), and the amplified signal is radiated by the antenna (A).
As the required signals are binary signals (high/low states) instead of analogue signals, the required modulation can also be generated in a much simpler manner. As is well known, an amplitude modulated analogue signal can be generated by multiplying two sinusoidal signals with different frequencies:

$$U_{\mathrm{mod}} = U_1 \sin(\omega_1 t) \cdot U_2 \sin(\omega_2 t). \quad (3.1)$$

Multiplication of binary signals, which is equivalent to (binary) ASK modulation, can be implemented with a simple AND operation.

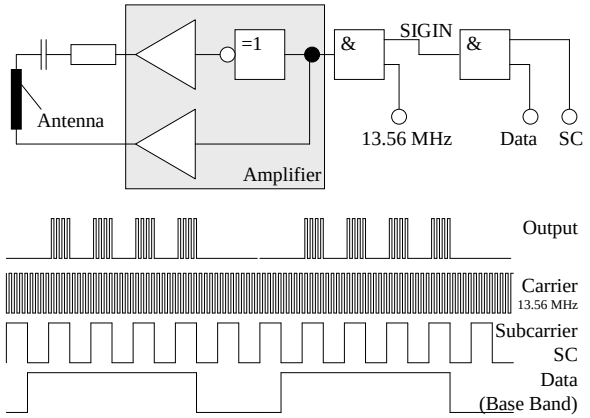

Figure 5 shows an ASK modulator to generate an ASK type active load modulation.

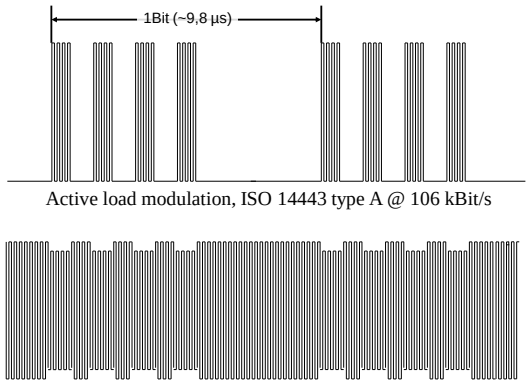

Figure 6 shows the RF Signal at 13.56 MHz of an active and a passive transponder, while transmitting the same data signal.

3.1 Upcoming standards

A transponder using active load modulation generates a signal which cannot be distinguished from a classical load modulation by any reader. Nevertheless, there is a strong need to standardise this technology [3]. So for ISO/IEC 14443-2, it is mandatory to use a passive load-modulator. A transponder using active load modulation can never be compliant with the current version of ISO/IEC 14443 for the following reason:

„Clause 8.2.2 – The PICC shall be capable of communication to the PCD via an inductive coupling area where the carrier frequency is loaded to generate a subcarrier with frequency fs. **The subcarrier shall be generated by switching a load in the PICC**".
In the standard it is therefore necessary to improve the specification of the physical device, which is defined in part 2 of ISO/IEC 14443; and the associated compliance tests defined in ISO/IEC 10373-6 have to be adopted as well. Besides defining a new wording within some sections of the standard, with the aim to explicitly allow active load modulation, there are still needs to clarify some further issues [6]
"*In order to be able to test these (active) PICCs independently from the numerous devices in which they can be inserted and also to test these devices independently from the PICCs which can be inserted in them, it was proposed to define a "Reference Active PICC". The same reasoning also applies for any other PICC which usually or always operates within a device.*
The main objectives of the New Work Item Proposal were then clarified:
Not to preclude the use of a battery (i.e. allow "active PICC modulation"), because present ISO/IEC 14443-2 explicitly defines "load modulation" for PICC;
Define the RF limits for "Active PICCs" (independently from any device), so that these limits include margins to take typical device attenuation into account;
Define the RF limits for devices, measured with a "Reference Active PICC."
In order to initiate the standardization of this interesting and future-oriented matter, in September 2010 we made a corresponding DIN contribution to SC17/WG8 [5] which has been presented to WG8 at the following meeting in Takamatsu (Japan). As a result, an NP ballot has been launched in December 2010 by SC17/WG8 with the following title [7]:
„*PICCs with external power supply – Use power supply other than the PCD-field so that PICCs with very small antenna and/or metallic environment can be compliant with ISO/IEC 14443-2*"

4 Implementation

4.1 First results and target of this paper

In a very first approach, the influence of the antenna size on the data transmission range of a tag using active load modulation was determined experimentally. The measurements were made using an ISO 14443 type A compliant reader such as the well known NXP Pegoda reader.
This reader can read typical contactless smart cards (ID1) over a range of typically about 7 cm. Using the same antenna size together with a circuit generating active load modulation, by contrast, the resulting read range was 50 cm.
As can be seen, even with an antenna having only 10% of the area of a contactless smart card (approximately the

Multi Media Card form factor) it was possible to achieve a communication range of 25 cm. In principle, reducing the antenna area by 10 reduces the reading range by approximately two, which equals approximately the 3rd root of the area ratio between two antennas.

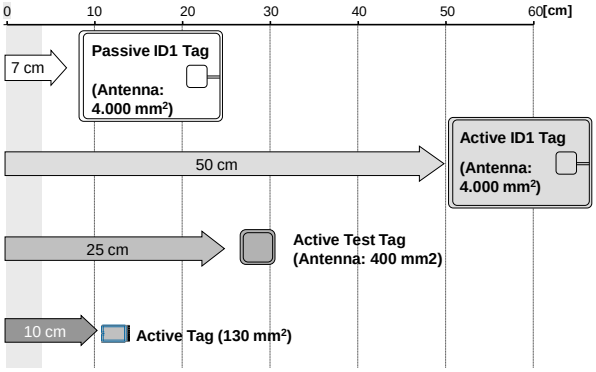

Figure 7 shows the difference in the ranges of active and passive systems with different antenna sizes.

This technology is thus especially suitable for achieving an acceptable operating range, even with a very small antenna for example in a data storage device. With an antenna having the same size as a common micro SD card (130 mm^2), it is easily possible to achieve a range of nearly 10 cm.

In contrast to the first results shown above, we tried to find out the limits in communication distance when using very large transponder antennas and huge (theoretically unlimited) transmission power. This paper will show the measurements we have carried out, and discuss the theoretical approach. As we are interested in absolute range limits, we do not restrict our measurements to legal limitations for field emissions. It is self-evident that an attacker would not follow these limitations as well.

4.2 Prototype implementation

The prototype implementation is based on an active ISO/IEC 14443 tag system as described in [2]. To generate the modulation signal required to increase the reading range we have developed a special RF interface which is connected with the secure element.

A simplified block diagram of the active RFID interface module is shown in Figure 8. The interface module consists of an amplifier, a modulator (M), an oscillator (OSC) with a frequency divider, and a signal conditioner. At the RF side, the interface module is connected with an antenna coil. On the digital side, the interface module has one signal output, SIGOUT, and one signal input, SIGIN, both of which are connected with the secure element.

SIGIN and SIGOUT are used to link the smart card microcontroller with the active RFID interface module.

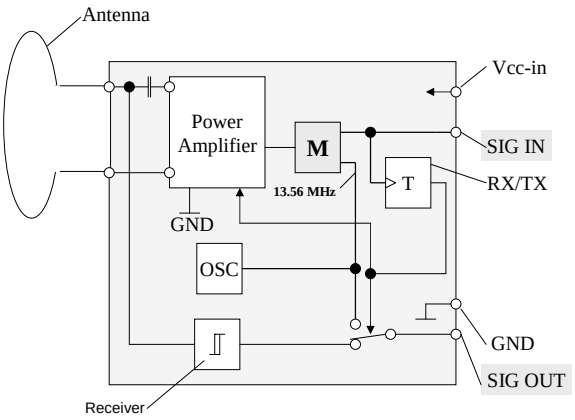

Figure 8 shows a simplified block diagram of the required active RFID interface module

To extend the range of this system, we optimized the HF front end architecture by using a high-sensitive receiver and a high power transmitter with a large antenna. In a typical RFID architecture, the receiving (RX) and transmitting (TX) paths share the same antenna. In principle, a single antenna configuration has two main disadvantages when applied in a range optimized system combining high sensitivity and high power:

- An antenna with low quality factor has to be used to provide the required RX and TX signal bandwidth. This results in a reduced induced voltage for RX and respectively in a reduced field strength for TX.
- The RX stage can be damaged due to the high TX power.

To overcome these disadvantages we implemented a system with two separated RX and TX loop antennas, as shown in Figure 9.

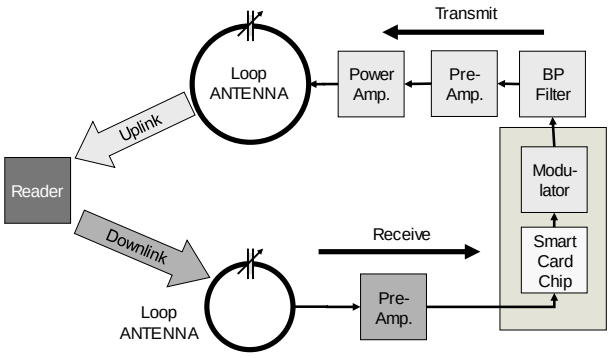

Figure 9: Prototype implementation

4.3 Theoretical approach

Our experiments have shown, as described later, that the dominant limiting factor is the ability to transmit data back from the smart card to the reader (3).

To allow this direction of communication, it is especially necessary to provide a certain level of magnetic field strength in the location of the reader antenna. In a 13.56 MHz system, loop antennas are used to generate the magnetic field. These antennas can usually be considered as

small loops (compared to the wavelength λ) with constant current along their length. This simplification can be made up to a circumference of 0.1 λ and accordingly a diameter of 0.032 λ [8]. Even for a diameter of 0.1 λ the error in the radial magnetic field is smaller than 5 % [9]. With a free space wavelength of 22.1 m for 13.56 MHz, this approximation can be used for loop antennas with a diameter of up to 2.2 m.
For a small loop antenna and an observation distance greater than the radius of the loop ($r > a$) the magnetic fields are

$$H_r = j\frac{ka^2 I_L \cos\theta}{2r^2}\left(1+\frac{1}{jkr}\right)e^{-jkr} \quad (3.2)$$

$$H_\theta = -\frac{(ka)^2 I_L \sin\theta}{4r}\left(1+\frac{1}{jkr}-\frac{1}{(kr)^2}\right)e^{-jkr} \quad (3.3)$$

$$H_\varphi = 0. \quad (3.4)$$

Figure 7 depicts the coordinate system applied to the formulas of the small loop antenna.

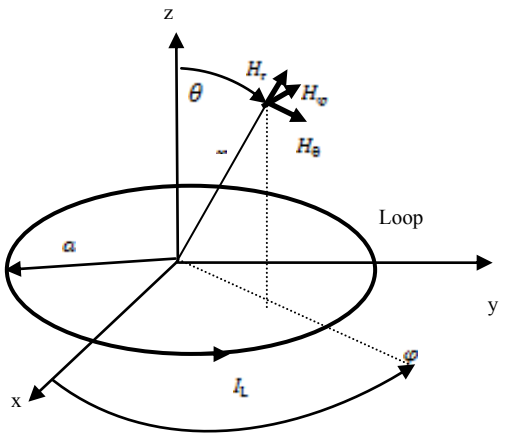

Figure 10: Coordinate system

According to (3.2) and (3.3) the magnitude of the magnetic field at a fixed distance r depends on the loop current I_L and the surface area ($\sim a^2$) enclosed by the loop. To raise the magnetic field and thus the reading range, the current and/or the antenna size has to be increased.
In a transmitting mode of an active tag system, the loop antenna is connected with a power source (= power amplifier with matching circuit), as shown in Figure 11.

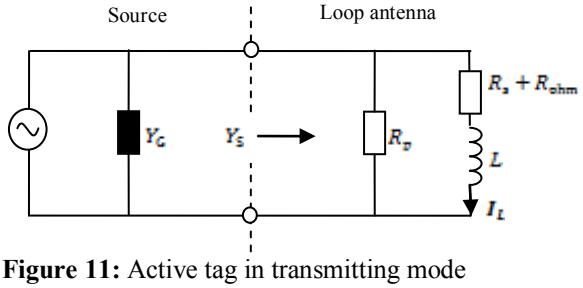

Figure 11: Active tag in transmitting mode

The loop antenna can be represented by an ideal inductance L with loss and radiation resistance $R_s + R_{ohm}$. To provide the required bandwidth, an additional resistance R_p is placed in parallel to the loop. The source impedance has to be matched to the conjugate-complex of the loop antenna.

$$Y_G = Y_S^* = \left(\frac{1}{R_p || (R_S + R_{ohm} + j\omega L)}\right)^* \quad (3.5)$$

$R_s + R_{ohm}$ can usually be neglected, as the radiation and the ohmic loss of the loop is rather small compared to that of R_p. Therefore the circuit diagram in Figure 11 can be reduced to the one shown in Figure 12.

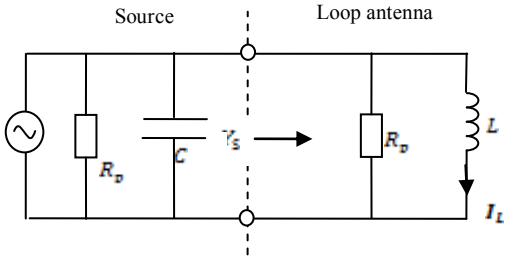

Figure 12: Active tag in transmitting mode (simplified configuration)

The loop current I_L depends on the quality factor Q of the resonant LC circuit. The quality factor is defined as the ratio of the average reactive power Q_r (stored in the capacitor and inductor) to the average active power P (dissipated in the resistor) at the resonant frequency.

$$Q = \frac{Q_r(\omega_r)}{P(\omega_r)} \quad (3.6)$$

The average reactive Power Q_r is

$$Q_r(\omega_r) = \frac{1}{2} {I_L}^2 \omega_r L. \quad (3.7)$$

Inserting (3.7) in (3.6), we can calculate the loop current as follows:

$$I_L(\omega = \omega_r) = \sqrt{\frac{2P\,Q}{L\,\omega_r}} \quad (3.8)$$

The loop current is directly proportional to the square root of the power and the square root of the quality factor as well as inversely proportional to the square root of the loop inductance. Especially the last-mentioned relation is interesting: As stated previously, a large antenna size is required to get a high magnetic field. But a bigger antenna size produces also a higher inductance and thus decreases the loop current. The inductance of a circular loop antenna is:

$$L = \mu\, a\left(ln\left(\frac{8a}{b}\right) - 2\right) \quad (3.9)$$

Where a is the radius of the loop and b the radius of the wire. For $a \gg b$ the inductance is approximately directly proportional to the radius a of the loop and thus the loop current inversely proportional to the square root of the radius. The influence of the radius on the loop current is thus by far weaker than the influence on the magnetic field.

Considering this approximation and the above stated equations, a relationship between magnetic field and the relevant hardware parameters (power, quality factor and antenna size) can be specified.

$H \sim A^{3/4}$	A… Area enclosed by the loop
$H \sim \sqrt{P}$	P… Transmit power
$H \sim \sqrt{Q}$	Q…Quality factor

Table 1: Factors influencing the magnetic field

In the near field **($r < 2\pi/\lambda = 3.5\text{m}$),** the maximum transmit range r_{max} is directly proportional to the third root of the magnetic field. Thus the relation between r_{max} and the hardware parameters are:

$r_{max} \sim \sqrt[4]{A}$	A… Area enclosed by the loop
$r_{max} \sim \sqrt[6]{P}$	P… Transmit power
$r_{max} \sim \sqrt[6]{Q}$	Q…Quality factor

Table 2: Factors influencing the transmit range (in the near field)

These proportionalities are demonstrated with an example: A doubling of the transmit range requires an increase in antenna area by 16, an increase of power or quality factor by even 64. A higher quality factor is usually not possible, as the quality factor is limited by the required signal bandwidth.

To generate a maximum induced coil voltage at the reader, the orientation of the tag antenna in respect to the reader antenna has to be considered. To take a closer look at this, the maximum tangential magnetic field (for $\theta = 0°$) and the maximum radial magnetic field (for $\theta = 90°$) is plotted in dependence of the distance.

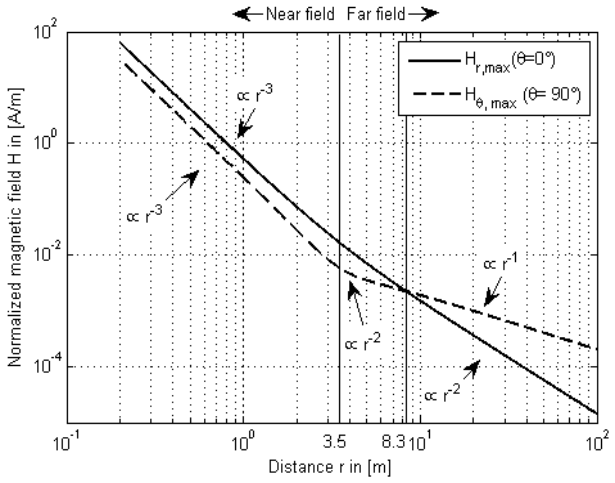

Figure 13: Normalized magnetic field of a small loop antenna in dependence of the distance (with a=1m and I_L=1A)

In the near field ($r < 2\pi/\lambda = 3.5\text{m}$), the maximum radial field is twice the maximum tangential field. However, for $r > 2\pi/\lambda$, the radial field decreases faster than the tangential and at a distance of 8.3 m, the maximum tangential field is larger than the maximum radial field. This point of interception depends only on the wavelength and not on the size of the antenna – provided that the aforementioned assumptions are satisfied. This should be considered for the orientation of receiving and transmitting antenna, as represented in Figure 14.

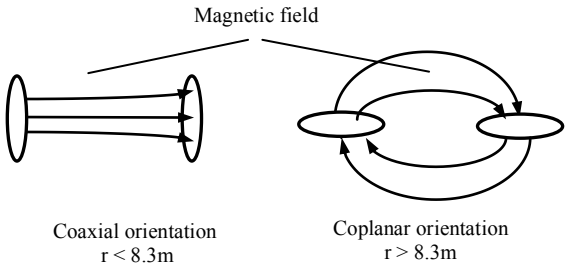

Figure 14: Optimum antenna orientation

4.4 Receiver front-end

We used a 19 x 12.5 cm² rectangular loop as receiving antenna. Since the receiving range is limited due to noise, no antenna with larger size is required. For ISO/IEC 14443 type A, the downlink uses modified Miller bit coding with 100 percent amplitude modulation. The pulse duration of the Miller glitches goes from 2 to 3 microseconds, which corresponds to a radio frequency bandwidth of 333 to 500 kHz (= 1 / glitch duration). To maximize the designated signal amplitude and minimize the noise, the loop is made resonant with a capacitor. The quality factor of the resonant circuit has to be less than 27 (= 13.56 MHz / 0.5 MHz) to cover the required bandwidth. We added an additional resistor to limit the quality factor to 27. The received signal level is increased using an op-amp based non inverting amplifier. The amplifier is protected against over-voltages with an anti-parallel Schottky diode pair between input and ground. The amplifier output is connected with the interface module of the active tag.

4.5 Transmitter front-end

The active ISO/IEC 14443 type A load modulation signal is generated with an active tag. A subsequent band pass filter selects the 14.41 MHz upper side band of the 848 kHz subcarrier signal. A typical ISO/IEC 14443 compliant reader only evaluates the upper side band signal (USB). The other signal parts do not contribute to the transfer of data from a tag to a reader. Each side band of a 100 percent amplitude modulated signal using rectangular pulses contains only about one fourth of the overall signal

power. Figure 15 shows the power distribution of an ISO/IEC 14443 type A uplink signal.

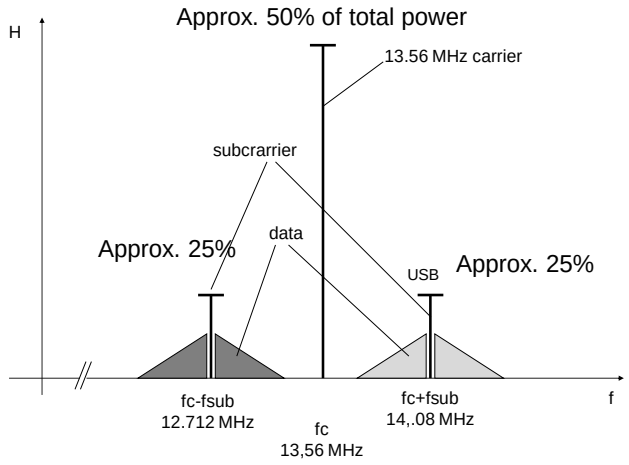

Figure 15: Power distribution of an ISO/IEC 14443 type A uplink signal

Using a single side band transmitter, the upper side band power can be enhanced by a factor of approximately four (+6 dB) compared to a conventional double side band system. The band pass filter was implemented as a coupled resonator filter consisting of two LC resonators, with the following parameters:

Center frequency	14.41 MHz
3-dB Bandwidth	800 kHz
Suppression at 13.56 MHz	18 dB

Table 3: Parameters of the coupled resonator band pass filter

A measured TX-spectrum of an ISO/IEC 14443 type A signal, generated by an active tag system is depicted in Figure 16 and Figure 17 before and after band pass filtering. The upper side band (USB) is within the pass band region. The lower side band (LSB) and carrier signal are in the stop band region.

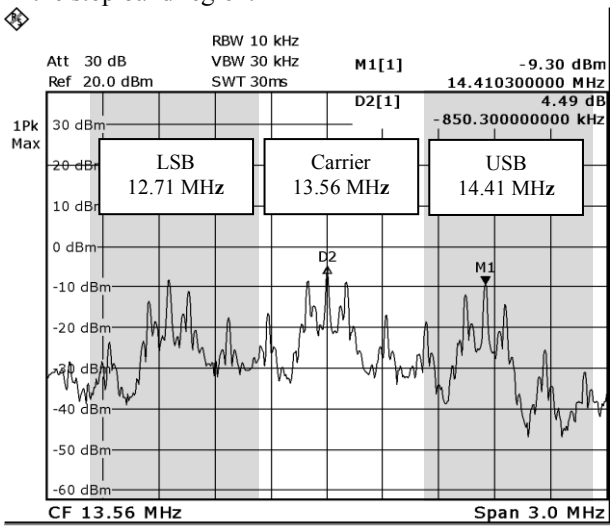

Figure 16: Measured ISO/IEC 14443 type A Manchester coded downlink spectrum of the active tag system

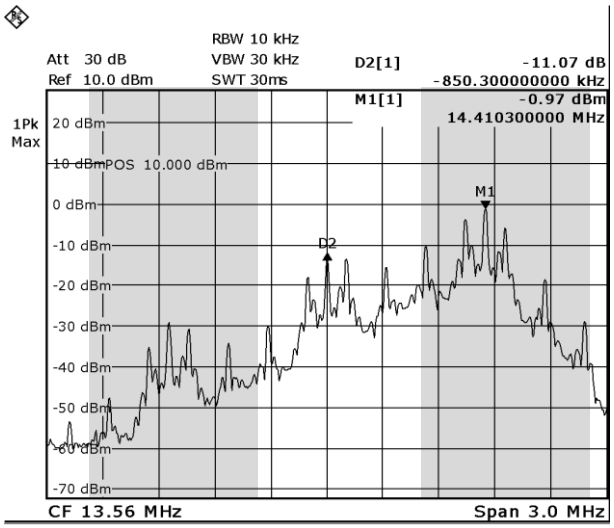

Figure 17: Measured ISO/IEC 14443 type A Manchester coded downlink spectrum of the active tag system after band pass filtering

The subsequent preamplifier adjusts the signal input level of the power amplifier. The employed power amplifier has a nominal output power of 50 Watt.
In addition to a high output power, another necessary condition for an increased range is a large antenna with a high quality factor. For our prototype implementation, we constructed a 1 · 1 m² copper tube loop antenna as described in [10]. The antenna is matched at 14.41 MHz - the centre frequency of the upper side band signal. The 3dB bandwidth is 650 kHz, corresponding to a Q factor of 22. For a Manchester coded ISO/IEC 14443 type A signal, the bandwidth should be greater than 424 kHz (2 · 212 kHz) to prevent pulse broadening.
The prototype implementation without TX antenna is shown in Figure 18.

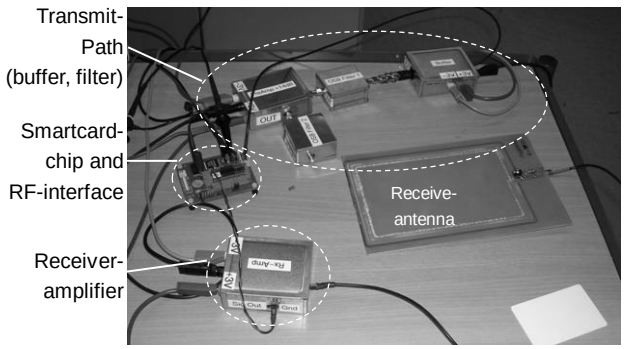

Figure 18: Discrete prototype implementation without TX-antenna

5 Results

5.1 Measurement results

In our experiments we used a CLRD701 NXP Pegoda reader compliant with ISO/IEC 14443. First we determined the maximum range allowing a valid reception of

the reader signal. As stated before this downlink range is noise limited and thus limited due to the man made noise as predominant noise source in the high frequency domain. Hence the maximum range is strongly environment dependent. The experiments were performed at the lab corridor of the Technische Universität München. In this environment we could achieve a maximum receiving range of up to 9 meters. This demonstrates that the receiving range is not the limiting factor regarding the maximum communication range.
Then we measured the maximum range of a full duplex communication between reader and tag. The experiments were again performed in the lab corridor with no other 13.56 MHz readers in proximity so that the active tag system does not answer to another reader with a stronger signal. To provide a high isolation between receiver and transmitter, we placed the RX and TX loop antennas at two different sides of the corridor. Figure 19 shows a picture of the arrangement.

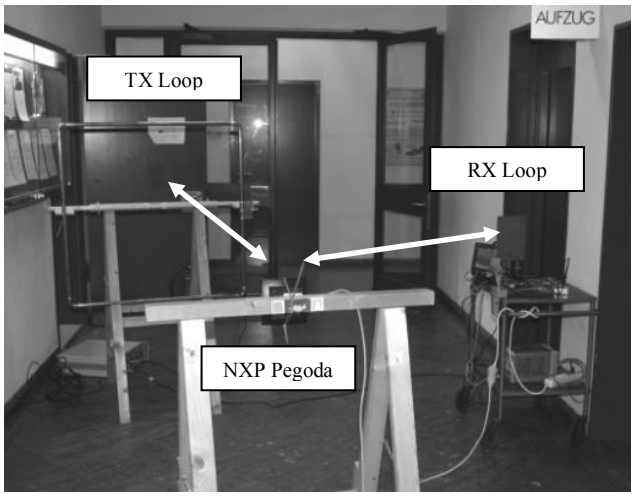

Figure 19: Measurement configuration in the lab corridor

The NXP Pegoda was connected to a battery-driven laptop to avoid cable coupling effects between tag and reader. The maximum communication range measured was 2.8 meters using the 50 Watt amplifier.

5.2 Extrapolation of results

It is often important to estimate how much energy and respectively what antenna size is necessary to achieve a further increase in range. Equations (3.2) and (3.3) give us the dependence between magnetic field and distance. Together with the proportional relationships established in table 1, an estimated communication range can be calculated in dependence of power and antenna size. As reference point we used the measured maximum range of 2.8 m based on a 1 m^2 TX loop size and an amplifier with a 50 Watt nominal power. The extrapolated graphs are shown in Figure 20 and Figure 21.

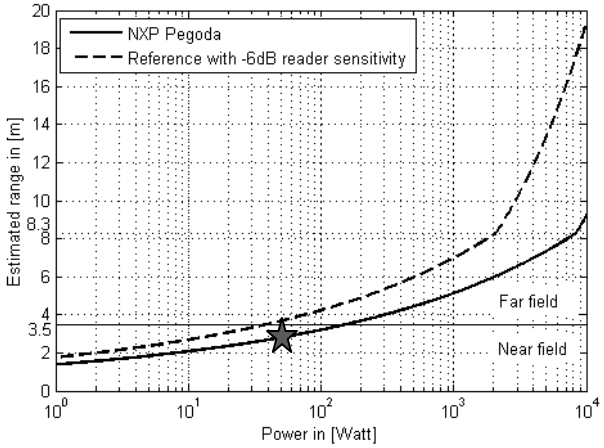

Figure 20: Power extrapolation (star: measured range using a TX loop size of 1 m^2 and a 50 Watt amplifier)

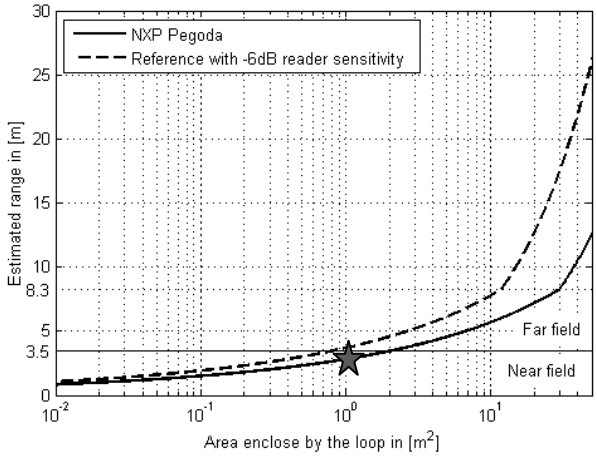

Figure 21: TX Antenna size extrapolation (star: measured range using a TX loop size of 1 m^2 and a 50 Watt amplifier)

The dashed line represents a reader, which has a sensitivity that is by 6 dB better (= half of the amplitude) than the used NXP Pegoda reader. The horizontal continuous line represents the near-field–far-field transition and even there, the slope of the power-range-graph remains relatively gentle. A gentle slope stands for little range extension with increasing power. For example, a range extension from 2.8 to 5 meters requires a power increase from 50 to 1000 Watt when assuming equal antenna size - or an increase of the antenna size from 1 to 6 m^2 when assuming equal power. Initially at 8.3 m, where the tangential magnetic field becomes larger than the radial one, there is a sudden increase in the graph's slope. But even with a reader sensitivity increased by 6 dB, a 2000 Watt amplifier is necessary to achieve this point - and respectively a TX antenna size of 12 m^2.

6 Conclusion

An ISO/IEC 14443 type A RFID tag with active load modulation and optimized front end design allows a communication range of up to a few meters. With a prototype implementation using a 50 Watt amplifier and a transmit antenna 1 m^2 sized, a range of 2.8 m could be experimentally achieved. The limiting factor of the

system was the ability to send data back from the active tag to the reader. A theoretical model was derived to describe the relationship between power and range and respectively antenna size and range. The model shows that a further range increase is practically limited as the necessary power and respectively antenna size become very large.

6.1 Extended range attack

As the short communication range of a smart card is an important security feature, the presented method could also be subject of an active attack scenario. Typical ISO/IEC 14443 compliant passive tags are designed to operate over a distance of about 10 cm or less, hence the typical contactless applications do expect the card holder to be in proximity of the reader as well. In contrast, an extended range attack would allow to "remote control" an ISO/IEC 14443 compliant reader from a distance of a few meters. However, the effort to carry out such an attack, the large antennas as well as the huge power supply needed, does not allow operating such an attack from a handy briefcase. An attack similar to the one described would be difficult to install and is therefore limited to very few selected places where the large equipment could be installed and power-supplied without drawing attention and risking discovery.

6.2 Future work

In our investigations we used a non frequency synchronized active tag system. As a passive tag system is in principle frequency coherent, such a non-coherent characteristic could be due to a reduced communication range. We plan to implement a frequency synchronized active tag to investigate this issue in the future.

7 Literature

[1] Finkenzeller, K., RFID-Handbook, http://rfid-handbook.com

[2] Finkenzeller, K.: Battery Powered Tags for ISO/IEC 144, Actively Emulating Load Modulation. RFID Systec 2011, To be published: May 2011.

[3] Finkenzeller, K., Batteriegestützte Transponder in ISO/IEC 14443, eine neue Transponder-Klasse, presented at the smartcard workshop 2011, Darmstadt, February 2011 http://www.smartcard-workshop.de/

[4] SC17/WG8N0165, Terms of reference for SC17/WG8/TF2 „Remote coupling communication cards" (RCCC), http://wg8.de/WG8DocList.html, 1993

[5] SC17/WG8N1722, Finkenzeller, Klaus, Enhanced Modulation PICC to PCD, DIN Contribution, http://wg8.de/WG8DocList.html, -September 2010

[6] SC17/WG8N1745, Roux, Pascal, Minutes of the 33rd meeting of WG8 Task Force 2, S. 7, http://wg8.de/WG8DocList.html, September 2010

[7] SC17/WG8N1755, New Work Item Proposal, Revision 1, PICCs with external power supply, http://wg8.de/WG8DocList.html, October 2010

[8] Balanis, C., A.: Antenna Theory. Third edition, Hoboken, New Jersey: John Wiley & Sons, Inc., 2005

[9] Werner, D., H.: An Exact Integration Procedure for Vector Potentials of Thin Circular Loop Antennas. Antennas and Propagation, IEEE Transaction on, vol.44, no.2, pp.157-165: February 1996.

[10] Texas Instruments: HF Antenna Cookbook. No. 11-0826-001: January 2004.

About the authors

Klaus Finkenzeller was born in Ingolstadt, Germany in 1962. He received his Dipl.-Ing. (FH) degree in electrical engineering from the Munich University of Applied Sciences (FH), Munich Germany. In 1989 he joined Gisecke & Devrient. Since 1994 he has been involved in the development of contactless smart cards and RIFD systems. He is currently working as a technology consultant for RFID/security, where he is involved in basic development and innovation projects.
Since 1994 he has been engaged in the standardisation of contactless smartcards and RFID Systems (DIN NI 17.8, NI 31.4, SC17/WG8), where he has been vice chair of the German DIN NI17.8 (ISO/IEC 14443) for more than 10 years now.
Up to now he has published about 130 individual patent applications, mainly in the RFID field of technology.
In 1998 he published the RFID handbook, which now is available in its 5th edition and in 7 different languages. In 2008 Klaus Finkenzeller received the Fraunhofer SIT smartcard price for his work on RFID, especially the RFID handbook.

Florian Pfeiffer was born in Starnberg, Germany, in 1976. He received the Dipl.-Wirtsch.-Ing. (FH) degree in industrial engineering from the Fachhochschule München, Munich, Germany, in 2001, the Dipl.-Ing. and Dr.-Ing. degrees in electrical engineering from the Technische Universität München, Munich, Germany, in 2005 and 2010, respectively. In 2009, together with Erwin M. Biebl, he founded an engi-

neering company for high frequency electronics (perisens GmbH), where he is chief executive.

Erwin M. Biebl was born in Munich, Germany, in 1959. He received the Dipl.-Ing., Dr.-Ing., and Habilitation degrees from the Technische Universität München, Munich, Germany, in 1986, 1990, and 1993, respectively. In 1986, he joined Rohde & Schwarz, Munich,Germany, where he was involved in the development of mobile radio communication test sets. In 1988, he was with the Lehrstuhl für Hochfrequenztechnik, Technische Universität München. In 1998, he became a Professor and Head of the Optical and Quasi-Optical Systems Group. Since 1999, he has been Head of the Fachgebiet Höchstfrequenztechnik, Technische Universität München. He has been engaged in research on optical communications, integrated optics, and computational electromagnetics. His current interests include quasi-optical measurement techniques, design and characterization of microwave and millimeter-wave devices and components, sensor and communication systems, and cooperative approaches to sensor and communication systems and networks. Dr. Biebl is a member of the Informationstechnische Gesellschaft (ITG) in the Verband Deutscher Elektrotechniker (VDE), Germany, a senior member of the IEEE and an appointed member of the commission B of URSI, Germany.