Battery powered tags for ISO/IEC 14443, actively emulating load modulation

Klaus Finkenzeller, Giesecke & Devrient GmbH, Prinzregentenstraße 159, 81607 München,
Klaus.finkenzeller@gi-de.com

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. It becomes a real problem, when the contactless data carriers are miniaturized even further, to be operated inside a mobile phone as a micro-SD or SIM card. With a passive transponder, a reliable communication with the reader can not be guaranteed any more. A proposal for a new work item in the standardization of contactless smartcards (ISO/IEC 14443), which describes the use of battery-assisted transponders, will be a helpful new approach to overcome such limitations. The following article describes the basic principle behind this new type of transponder.
April 2011

1 Introduction

Inductive 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). Inductive coupled RFID systems 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 ID1 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.

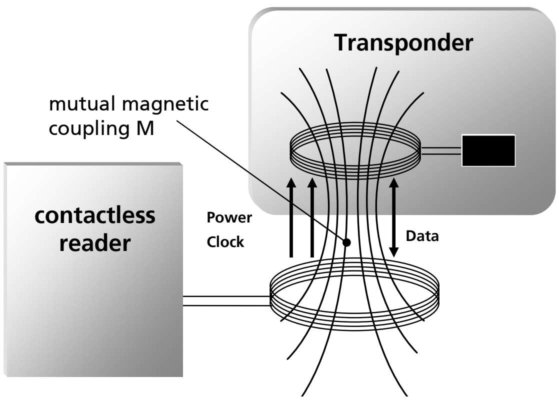

Figure 1: An inductive coupled RFID system uses mutual magnetic coupling to transfer power and data.

The operating range is limited by the coupling factor between the reader/interrogator antenna and the transponder antenna. If the size of the transponder antenna gets very small, the operating distance drops until there is no more communication possible.
To enable mobile phones with contactless functionality, NFC (near field communication) has been developed. Specified in ISO/IEC 18092, NFC allows a mobile phone to act as an ISO/IEC 14443 compatible transponder, as well as a reader. Additionally a peer to peer communication mode is supported.
In this paper, we discuss the possibility to use very small, battery powered, active transmitting transponders, to enhance mobile phones with contactless functionality, by just plugging the transponder in a mobile phone. This is done by bringing contactless card functionality into a micro SD memory card.

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 with 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.

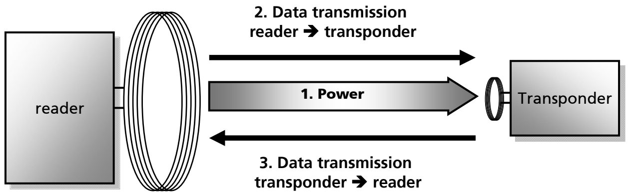

Figure 2: The limiting factors of a contactless communication. (1) Power transfer: the small antenna cannot extract enough power from the field and therefore (2) not receive any data. (3) Load modulation: the return signal from the small antenna to the reader is too small with load modulation

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 back from the smart card 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 antennas are used (SIM cards, micro SD cards). If a small contactless card of this type is used in a mobile telephone or a PDA, the already small reader range, additional shielding caused by the battery and metal layers in the phone, quickly leads to problems, so that the transponder can no longer be accessed by an external reader.

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. In a mobile phone, power is already available for devices such as a micro SD card.
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 an 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 this modulation sidebands.

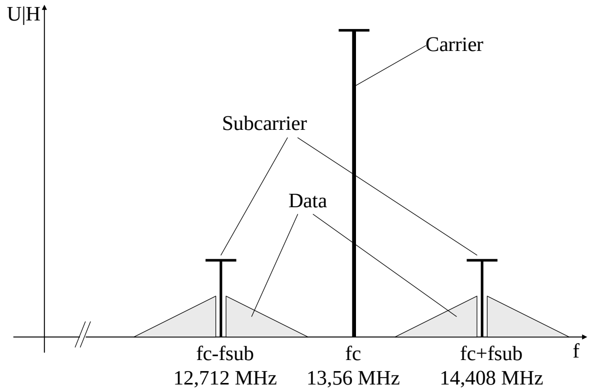

Figure 3 shows the frequency spectrum at the reader antenna resulting from a common passive load modulation with a subcarrier, according to ISO/IEC 14443-2.

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. Containing no information, a constant 13.56 MHz carrier signal does not need to be transmitted by the transponder, and it is anyway transmitted constantly by the reader. A signal with these properties is known as dual sideband (DSB) modulation.

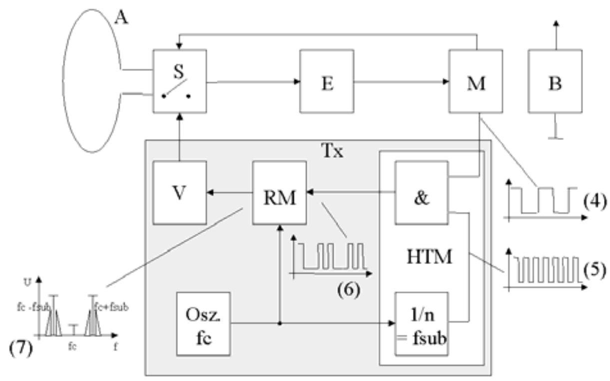

Figure 4: Basic circuit of a transponder, generating active load modulation.

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:

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

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

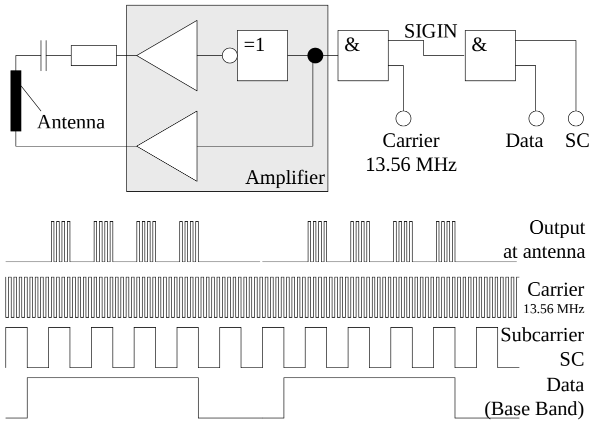

Figure 5 shows an ASK modulator to generate an ASK type active load modulation.

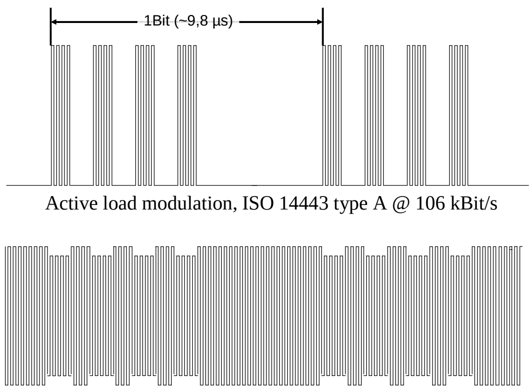

Figure 6 shows the RF Signal at 13.56 MHz of an active and a passive transponder, while transmitting the same data signal.

3.1 Influence of the antenna size

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 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, the resulting reader range was full 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.

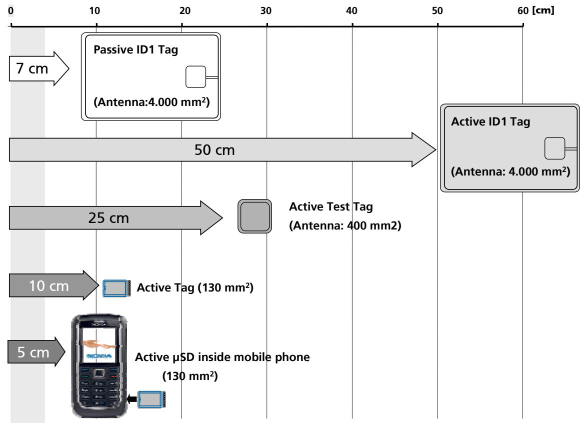

Figure 7 shows the difference in the ranges of active and passive systems with different antenna sizes.

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 micro SD card, it is easily possible to achieve a range of nearly 10 cm. So even if the card is installed in a mobile phone, suffering from additional shielding, an acceptable communication range of a few centimetres can be achieved.

3.2 A micro SD card using active load modulation

A closer examination of the mobile phone market shows that the proportion of NFC-enabled devices in comparison to the total number of phones sold by producers will increase only very slowly. In order to make NFC applications breakthrough, a much larger market share of NFC-enabled mobile phones is required.

Figure 8: Size comparison –micro-SD sized transponder antenna

Due to their small dimensions of 11 mm × 15 mm × 0.7 mm (slightly larger than a fingernail), micro SD Cards are used in mobile devices such as mobile phones. as memory card for pictures, MP3 files and applications. Micro SD is the world's smallest memory card format and is supported by many mobile-phone manufacturers, such as Kyocera, Motorola, Samsung, Nokia and Sagem and GPS device makers like Garmin, as well. This opens up the possibility to provide a contactless micro-SD card in order to enhance phones with a contactless interface. As there is power supply for the micro-SD provided by the phone, the described active load modulation can be used.

A micro SD card with an active RFID interface has a few additional components compared to a conventional micro SD card. Besides the usual flash memory and flash controller, a contactless micro SD card normally has a security chip (usually a smart card chip) with its own operating system (SCOS). This security chip controls the active RFID interface needed for the enhanced contactless data transmission and reception. Another important component is the antenna, which may have the form of a loop antenna, as this type of antenna can be realised very simple just on the cards PCB.

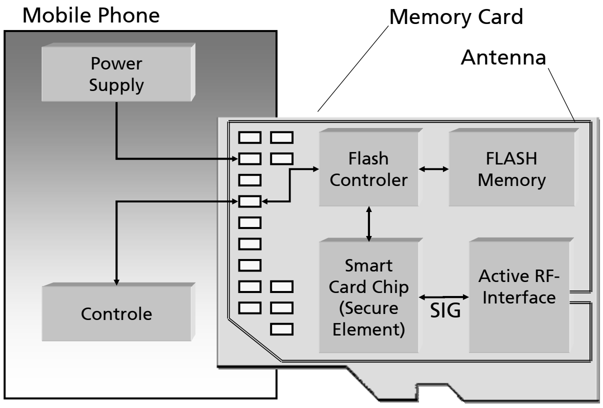

Figure 9 Components of a secure micro SD card with an active RFID interface.

Figure 10: Contactless payment terminal (left) and mobile phone with micro-SD card (front)

3.3 Active RFID interface ASIC

To generate the modulation signal required to increase the reading range and to deal with the very weak reader signals received by the antenna while inside a mobile phone, 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 11. 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.

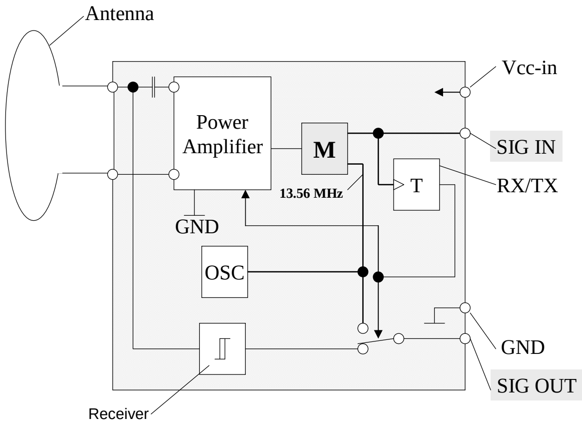

Figure 11 shows a simplified block diagram of the required active RFID interface module.

SIGOUT corresponds to the RF signal received by the reader and is a 13.56-MHz clock signal, which is suppressed during the modulation pulses of the reader:

SIGIN corresponds to the control signal used to drive a common load modulator in a passive transponder and consists of the modulated subcarrier signal. This interface is known as NFC-wired interface (NFC-WI) [2] and normally used to connect a secure element with a NFC front end in a mobile phone.

When the interface module is in transmit mode, which means that data is being sent from the connected smart card chip to an external contactless reader, the modulated subcarrier signal is fed to the signal input SIGIN by the smart card chip. The SIGIN signal is provided together with a 13.56-MHz carrier signal to the modulator whose output then feeds the power amplifier.

The antenna and the series capacitor form a series-resonant circuit connected to outputs of the power amplifier, with the result that under resonant conditions the RF current flowing in the antenna resonant circuit is limited only by the DC resistance of the conductors and the amplifier, which means that the maximum possible transmit power is obtained (see [1] with regard to current matching).

In receive mode, the receive signal picked up by the antenna is amplified and fed to the smart card chip from the SIGOUT output. The signal conditioner acts as an amplifier to enable reception of very weak signals (in order to achieve maximum operation range) and as a threshold comparator (Schmitt trigger) to provide a digital signal at the output of the signal conditioner.

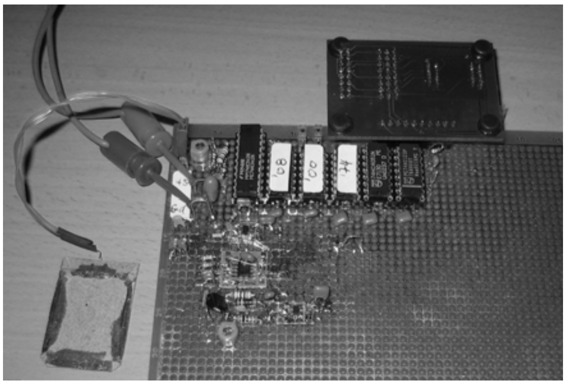

Figure 12: A first setup to generate active load modulation for ISO/IEC 14443. The smart card chip is placed on the small board connected on the top.

A 13.56-MHz clock signal and the signals from the NFC-WI are needed to process the modulation signals. As it is not possible to receive the reader signal while transmitting the active load modulation signal, the oscillator (OSC) generates the 13.56-MHz carrier signal required for transmission on board.

3.3.1 Switching between RX and TX

To switch between receive mode and transmit mode, the signals on SIGIN have to be observed, as this is the only information available from the smart card controller. However this switching signal can very easily be derived from the SIGIN signal because the latter signal is only active when data is actually being transmitted.

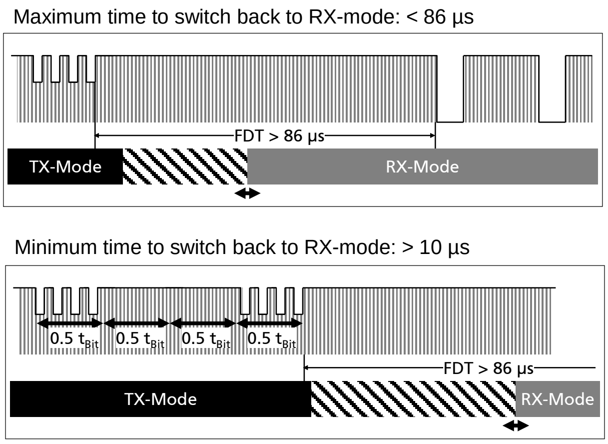

Figure 13 shows the minimum and maximum hold times of the timing element defined by the FDT (top) and the bit interval at 106 kbit/s (bottom).

To do so, a timing element is triggered on the leading edge of the signal on the SIGIN line. The hold time of the timing element is largely uncritical and can be chosen as desired between T_{BIT} (bit length, 9,8 µs) and FDT (the frame delay time, ~86 µs).

3.3.2 Comparison between different modulator circuits

For the data transfer from the tag to a reader according to ISO/IEC 14443 type A, at the default bitrate of 106 kBit/s an ASK modulated subcarrier (OOK, on off keying) will be used to feed the load modulator. To simulate that signal with active load modulation, the required modulation side bands can be generated most effectively by using a ring modulator. It is expected that the generated dual side band modulation (DSB) should provide the best results, regarding the communication distance. This results from the total suppression of the 13,56 MHz carrier signal, so that the available power can be transmitted within the side bands. To verify this assumption, we have investigated the following modulator circuits in respect of their performance and energy consumption:

- Simple digital ring modulator
- Optimized digital ring modulator
- ASK-modulator

3.3.2.1 Digital ring modulator

The simple digital ring modulator disappointed by its poor carrier suppression in the analyzed signal according to ISO / IEC 14443 - Type A. This is mainly due to the fact that the carrier signal is sent all the time, without any relation to the logic state of the base band signal, leading to unnecessary high power consumption as well. A suppression of the carrier signal is, other then expected, not recognizable in the spectrum.

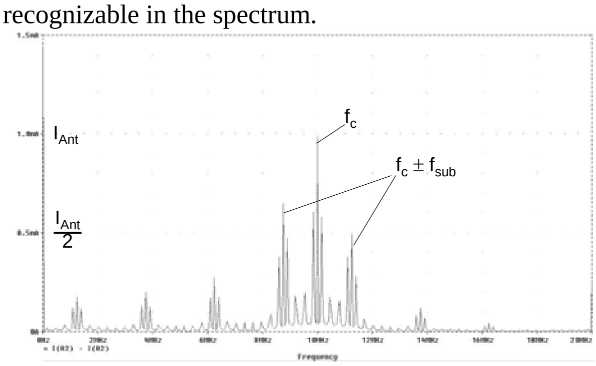

Figure 14 shows the frequency spectrum of the output signal of the simple ring modulator in an endless sequence of 1-bits

3.3.2.2 Optimized ring modulator

Looking at the load modulation signal according to ISO/IEC 14443 type A, it stands out that the subcarrier pulses are transmitted only half the period of each bit. To optimise the simple ring modulator in that sense, we have decided to clock the output signal with the base band Manchester code of ISO/IEC 14443 type A. This results in a reduction of the energy consumption per bit of 50% compared to the simple ring modulator. The RF signal then is sent only at the times when the 848 kHz subcarrier signal is on.
The communication range of this circuit corresponds exactly to the range of the simple digital ring modulator.

The carrier frequency in the output spectrum now is significantly suppressed, as we would expect from a ring modulator.

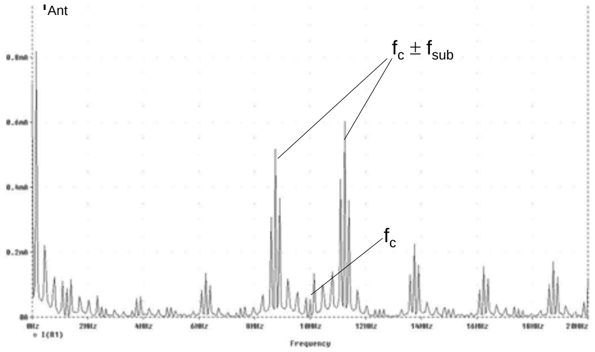

Figure 15 shows the frequency spectrum of the output signal of an optimized ring modulator with an endless sequence of 1-bits. The carrier frequency f_c (13.56 MHz) is clearly suppressed.

3.3.2.3 ASK modulator

The ASK modulator is implemented by an AND operation of all input signals. The output signal only consists of carrier frequency bursts clocked by the modulated subcarrier.

The spectrum clearly shows about half the power transmitted with the remaining carrier signal. Additionally to the lower power consumption, this is also contributing to the drop in distance, compared with the ring modulator. A possible interference of this remaining carrier with the reader's carrier however is of no harm. An ISO/IEC 14443 reader only listens at the subcarrier sidebands generated by the transponder, but not at its own carrier frequency.

Regarding the operating distance, losses have to be taken. The operating distance drops to 83% compared with the ring modulator. The energy consumption per bit however is only 25% compared to the simple ring modulator. This circuit thus appears to be ideal for battery operated devices.

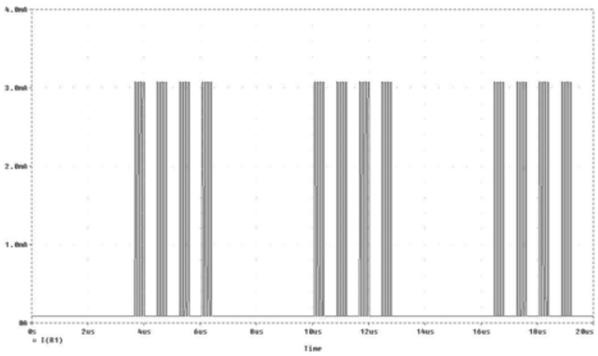

Figure 16 shows the output of the ASK modulator with an endless sequence of 1-bits in the time domain.

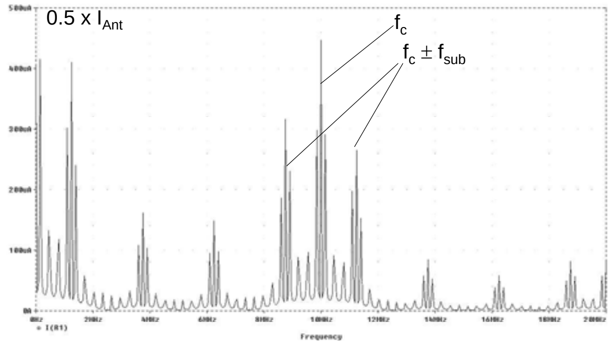

Figure 17 shows the frequency spectrum of the output signal of the ASK modulator with an endless sequence of 1-bits.

3.3.2.4 Review

The examined circuits have shown different performance in terms of the achieved reading range and power consumption (at constant transmission power)

MODULATOR	ENERGY PER BIT, REL.	OPERATING RANGE REL.
Digital ring modulator	100 %	100 %
Optimised digital ring modulator	50 %	100 %
ASK-Modulator	25 %	83 %

Regarding the energy consumption per bit, the ASK modulator will be the best choice, with a energy consumption of only 25% compared to the simple digital ring modulator. Additionally, implementation becomes quite easy when interfacing the smart card chip with NFC-WI. The signal on SIGIN needs no more conversion and can directly feed the modulator.

Regarding however the performance, the ring modulator shows 6 dB more signal strength at the 848 kHz sidebands. This results in around 20% more reading range. Here the optimised ring modulator should be the choice, as it shows good performance together with acceptable energy consumption.

3.3.3 Digital modulation circuits for ISO/IEC 14443-type B and higher bitrates.

For ISO/IEC 14443-3 type B as well as for higher bitrates from 212 kBit/s up to 848 kBit/s, a different coding and modulation is used for the load modulation subcarrier: BPSK, binary phase shift keying. Actively emulating that signal we expect that also the digital ring modulator will show the best results, regarding the reading range.

We investigated the simple digital ring modulator, and the ASK modulator.

3.3.3.1 Digital ring modulator

The digital ring modulator shows good performance regarding the reading distance and clear-carrier suppression, as expected from a ring modulator. The relative energy consumption is 100%, as a signal is transmitted during the whole bit duration.

3.3.3.2 ASK Modulator

The ASK modulator shows no carrier suppression at all, as we expected. The reading range is about 83% compared with he ring modulator, the energy consumption however drops to 50%.

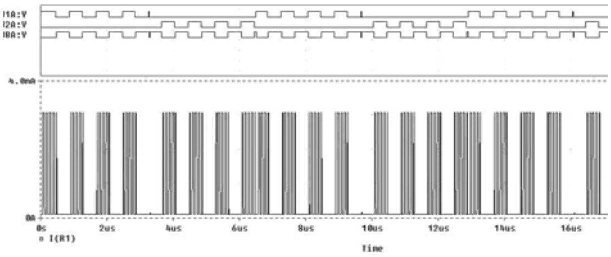

Figure 18: Output signal of an ASK modulator, using a BPSK modulated load modulation subcarrier.

3.3.3.3 Review

Using BPSK, the two modulator types again showed clearly differences.

MODULATOR	ENERGY PER BIT, REL.	OPERATING RANGE REL.
Digital ring modulator	100 %	100 %
ASK-modulator	50 %	83 %

If reading range is the bottle neck, the ring modulator should be used. For battery operated devices however we recommend to use an ASK modulator, as it requires only half the energy per bit, but still reaches 83% of the maximum reading distance.

4 Standardisation

A transponder using active load modulation generates a signal which can not be distinguished from a classical load modulation by any reader. Nevertheless, there is a strong need to standardise this technology. 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 that 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 necessary to improve the specification of the physical device, which is defined in part 2 of ISO/IEC 14443, as well as the associated compliance tests defined in ISO/IEC 10373-6 have to be adopted. Beside 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]

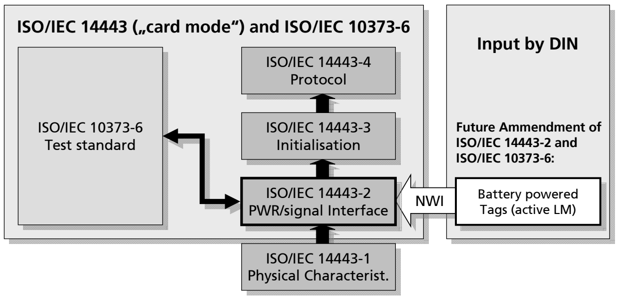

Figure 19: Our approach of standardising active load modulation in ISO/IEC 14443

"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 standardisation of this interesting and future-oriented matter, in September 2010 we made a corresponding DIN contribution to WG8[1] [5] which has been presented to WG8 [8] at the following meeting in Takamatsu (Japan). As a result, a NP ballot has been launched in December 2010 by SC17/WG8 with the following description [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:

Currently more and more small PICC form factors are penetrating the market. Very often these PICCs are attached on metal surfaces (mobile phones) or they are even operated inside a mobile phone (memory cards). These metal environments often cause additional drops in performance (reading distance).

WG8 has reacted with different antenna classes, which results in different ranges for the field strength for each

[1] WG8, standing for Working Group 8, is one of the Working Groups within the subcommittee ISO/IEC JTC1/SC17 "Identification Cards" and was established in 1988 to develop standards for contactless chipcards.

class, thus resulting in reduced operating range for classes with increased minimum field strength.
Actively powering the PICC will allow the PICC to handle field strength down to 1,5 A/m even in metal environment, while transmitting an enhanced modulation signal will allow the PCD to pick up the PICC signal even with very bad mutual coupling between PICC and PCDs antenna, e. g. with metal environment. So PICCs with external power supply will be an innovative approach to operate very small PICC antennas with PCDs already in the field."
In February 2011 the NP was accepted by the standardisation committees. The standardisation of battery powered tags within ISO/IEC 14443 therefore is on its way now.

5 Conclusion

For the first time, the use of active load modulation allows to operate ISO/IEC 14443 compliant transponder with a very small form factor, even in a system that was originally designed for contactless smart cards in ID1 format. First applications in a micro-SD form factor, designed for usage in a mobile phone, show the huge potential behind this new technology, especially regarding the fact that the installed reader base does not need to be changed at all. This is due the fact that the active transponders described in this article are fully interoperable with common passive transponders.
So in the future, we can expect a wide impact of this new approach to many contactless applications based on ISO/IEC 14443, especially in a mobile phone environment or in totally new applications we can not yet imagine.

6 Literature

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

[2] ECMA-373, Near Field Communication Wired Interface (NFC-WI), 1st Edition / June 2006

[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/ http://rfid-handbook.de/downloads/

[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] ISO/IEC JTC1/SC17/WG8, "Contactless Integrated Circuit Cards" http://wg8.de/

About the author

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.