# Impact of GSM Interference on passive UHF RFIDs

Benjamin Brunner was and Florian Pfeiffer is at perisens GmbH, Lichtenbergstr. 8,
85748 Garching near München, pfeiffer@perisens.de
Klaus Finkenzeller, Giesecke & Devrient GmbH, Prinzregentenstr. 159, 81677 München,
klaus.finkenzeller@gi-de.com
Erwin Biebl, Fachgebiet Höchstfrequenztechnik, Technische Universität München,
Arcisstr. 21, 80333 München, biebl@tum.de

***Abstract*—This paper presents an interference analysis considering the impact of GSM uplink signals on passive UHF transponders in accordance of the ISO/IEC 18000-6 standard, both operating in a similar frequency band. The GSM uplink signal (from the mobile device to the base station) is particularly critical as interferer, as the mobile device can be located close to a transponder system e.g. several persons having a phone call close to a subway ticketing system. The measurements were conducted with GSM interferer signals generated by an RF signal generator and a programmable GSM mobile phone.**

**February 17, 2015**

## I. Introduction

Backscatter-coupled RFID systems are currently used in a large number of applications such as logistics, supply chain, warehouse management, retail stores, and similar applications. Furthermore UHF RFID applications are more and more prevalent in public environments such as ticketing or access systems, and thus increasingly exposed to GSM interference.

Backscatter-coupled RFID systems mainly operate in the UHF frequency ranges $868\,\mathrm{MHz}$ (Europe) and $915\,\mathrm{MHz}$ (USA, Asia). These UHF-RFID Systems are primarily covered by the standard (ISO/IEC 18000-6, 2010).

The majority of the applications mentioned above operate according to ISO/IEC 18000-63, which describes the physical characteristics and protocol behavior of the so called Electronic Product Code, the EPC. This standard is designed for fast detection of huge numbers of transponders in the field at the same time, and for transferral of a small amount of data between an interrogator and a tag.

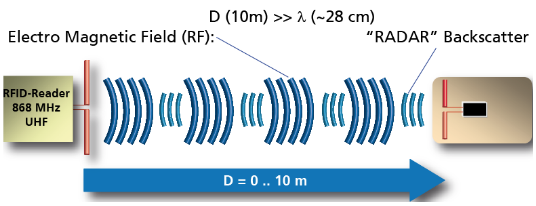


Fig. 1: Principle of UHF RFID

A typical transponder is field-powered and uses modulated backscatter signals to transmit data back to the interrogator. The operating range of these passive (or field-powered) transponders is mainly limited by the ability to get sufficient power from the field into the transponder in order to operate the silicon chip. Typical maximum operating distances of such passive transponders are between $3$ and $10\,\mathrm{m}$. The power radiated from the interrogators to provide operation power for the tags, typically is in the range of $2\,\mathrm{W}$ ERP (Europe) or $4\,\mathrm{W}$ EIRP (USA, Asia).

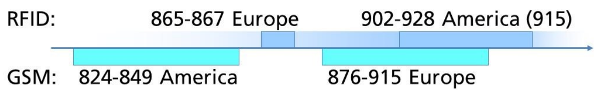


Fig. 2: Worldwide frequency ranges of RFID and GSM mobile phones

GSM mobile phones also transmit signals in the $850/900\,\mathrm{MHz}$ frequency range. The transmission power in the handset is limited to a maximum of $2\,\mathrm{W}$ ERP in GSM 850/900 and therefore in the range of the RFID reader transmit power. Typically, an RFID transponder works as a broadband power detector without having any signal selectivity. The frequency range seen by a RFID transponder is only limited by the bandwidth of its antenna, which typically is derived from a dipole. To allow worldwide exchange of goods where a transponder is attached, most of the RFID transponder antennas are designed to cover the full frequency range from $850\,\mathrm{MHz}$ to $930\,\mathrm{MHz}$. Due to these boundary conditions, it is obvious that a GSM signal transmitted in proximity of a RFID transponder most likely will power up this transponder and probably interfere its communication with the interrogator.

## II. GSM Interference

The GSM standard uses a combination of FDMA and TDMA (Frequency and Time Division Multiple Access). Up- and Downlink bands are divided into channels of $200\,\mathrm{kHz}$ bandwidth and TDMA frames contain eight time slots (so called 'bursts') with each $\approx 577\,\mu\mathrm{s}$ long. Depending on the usage of the mobile device (SMS, GPRS, phone call) and the current network situation different number of slots are used. This is outlined in Fig. 3. As GSM uses GMSK (Gaussian Minimum Shift Keying) modulation, the transmitted power for a single burst was assumed to be constant in our investigations. Furthermore, only the upload band is of interest for this study, because the mobile device is located rather near the RFID tag.

### A. *Far-Field Measurement*

In the first measurement the interference behavior shall be analyzed via a far-field scenario. The far-field measurement

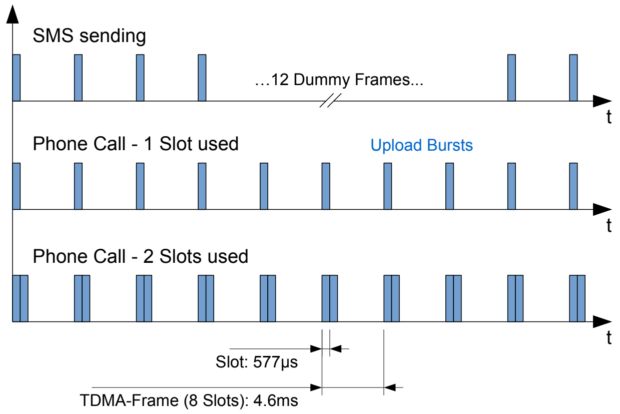


Fig. 3: Illustration of GSM TDMA timings

Fig. 4: Measuring setup for which the SIR can be calculated. Reference dipole was replaced by different RFID transponders.

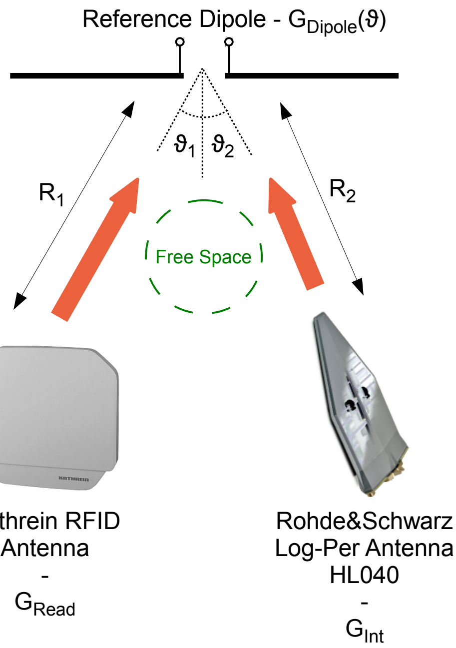


Fig. 5: Measuring setup for calculating the SIR

represents the case that a cellular phone call is conducted in the proximity of an UHR RFID communication. Here, the interfering mobile phone is simulated by a signal generator (continuous wave mode), which is located in the far-field of the UHF RFID transponder to exclude near-field coupling. The far-field is usually defined with $R_{far} \geq {}^{2D^2}/_{\lambda}$, where D is the aperture size of the antenna and lambda the free space wavelength. Assuming an aperture size of $10\,\mathrm{cm}$ this would result in a distance $R_{far}$ of at least $6\,\mathrm{cm}$ at $868\,\mathrm{MHz}$. In this experiment we used the Kathrein UHF RFID Reader System RRU4-ETL-E6 with an appropriate wide range antenna and analyzed several UHF RFID transponders. Exemplary results are shown with an example NXP UCODE G2iL UHF RFID transponder. The Rohde & Schwarz Log-Per antenna HL040 served as interferer antenna, whose nearly constant gain over the bandwidth is important for later calculations. Since we were interested in the tag's receiver behavior (for the time being) we wanted only to see the effects of different passive tags. The measurements were carried out in a shield EMC chamber to exclude any external influence. This setup is shown in Fig. 4.

To be able to evaluate the behavior/quality of the receiver independent of the influences of the measuring setup, the ratio between the powers of RFID reader and interferer at the RFID chip input, is a mandatory quantity. This signal to interferer ratio is called 'SIR'. To be more precise, the SIR is less a ratio of powers, but more a ratio of power densities at the transponder's antenna. With a reference measurement such the one depicted in Fig. 5, it is not necessary to approach, for example, distances between the components, antenna gains and cable attenuation theoretically.

As a first step, the RFID transponder is replaced by a dipole antenna for a $50\,\Omega$ system with the gain $G_{Dipole}(\vartheta)$. This antenna has the distance $R_1$ to the RFID reader and $R_2$ to the interferer antenna. The RFID reader is set to transmit a continuous wave with the power $P_{Out\text{-}Read}$. The power that is therefore received and measured at the dipole is called $P_{In\text{-}Read}$. The same measurement is then repeated with the interferer's appropriate powers $P_{Out\text{-}Int}$ and $P_{In\text{-}Int}$. Ideal input powers are calculated with Eq. 1 and Eq. 2.

$$\begin{aligned} P_{In\text{-}Read}[\mathrm{dBm}] &= P_{Out\text{-}Read}[\mathrm{dBm}] + G_{Read}[\mathrm{dB}] + G_{Dipole}(\vartheta_1)[\mathrm{dB}] \\ &\quad - L_{R1}[\mathrm{dB}] \\ &= P_{Out\text{-}Read}[\mathrm{dBm}] + D_1[\mathrm{dB}] \end{aligned} \tag{1}$$

$$\begin{aligned} P_{In\text{-}Int}[\mathrm{dBm}] &= P_{Out\text{-}Int}[\mathrm{dBm}] + G_{Int}[\mathrm{dB}] + G_{Dipole}(\vartheta_2)[\mathrm{dB}] \\ &\quad - L_{R2}[\mathrm{dB}] \\ &= P_{Out\text{-}Int}[\mathrm{dBm}] + D_2[\mathrm{dB}] \end{aligned} \tag{2}$$

The variables $G_{Read}$ and $G_{Int}$ represent the corresponding antenna gains of RFID reader and interferer. Because of the symmetric directional characteristic of the dipole, the gains of $G_{Dipole}(\vartheta)$ are assumed to be equal if the angles are equal. The set output and measured input powers result in $D_1$ and $D_2$. In the variables $L_{R1}$ and $L_{R2}$, all attenuations, mainly of free space and cables, are summarised. The SIR at the reference dipole antenna can then be calculated with Eq. 3.

$$\begin{aligned}\mathrm{SIR[dB]} &= \mathrm{P_{In\text{-}Read}[dBm]} - \mathrm{P_{In\text{-}Int}[dBm]} \\ &= \mathrm{P_{Out\text{-}Read}[dBm]} - \mathrm{P_{Out\text{-}Int}[dBm]} + \mathrm{D_1[dB]} - \mathrm{D_2[dB]} \quad (3)\end{aligned}$$

With the assumptions that an antenna has a symmetric pattern (absolute gain negligible) and that the reader and interferer frequencies in the measurements are equal (matching effects negligible), the calculated SIR also holds for this antenna at the certain frequency (position of reference dipole and antenna assumed to be equal). This conclusion can be made for UHF RFID transponder antennas, because they usually have a common dipole structure. The frequency should be set to the later used reader frequency ($\approx$868 MHz). When sweeping the interference frequency $G_{\mathrm{Int}}$ has to be constant over this very frequency range (and equivalent to $G_{\mathrm{Int}}$ at the frequency in the reference measurement) as demanded before.

Considering this setup and applying an interference in the form of a frequency sweep to an UHF RFID tag we measured the SIR characteristic shown in figure Fig. 6. The detection rate averaged over several read commands is color coded. 1 (red) means the tag could be detected with every read operation and 0 (blue) means the tag could not be detected at all.

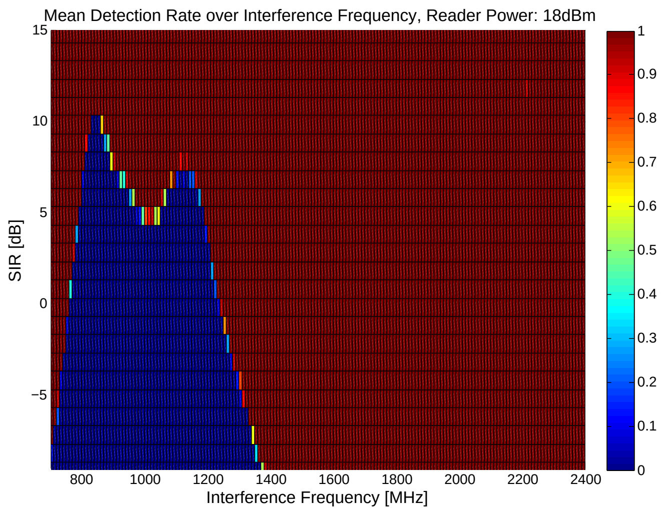


Fig. 6: Mean detection rates for CW interferences with increasing SIR and frequency

The SIR, in our case defined as the ratio of power densities at the transponder's antenna, outlines the antenna's impedance matching. There are two resonant frequencies recognizable, whose coupling most likely serves to expand the bandwidth for world wide usability. This characteristic implies the high sensitivity of the simple detector receivers in the GSM 850/900 frequency bands. It is striking that the transition from full detection to no detection seems to be very abrupt, which could be related to reader internal thresholds.

The SIR threshold indicates the maximum allowed interference power relative to the RFID reader power. Assuming free space path loss with power decreasing proportional to the square of the distance, the SIR at the transponder can be calculated as follows:

$$\mathrm{SIR}_{linear} = \left(\frac{\mathrm{P_{Reader}}}{\mathrm{P_{Mobile}}}\right)\left(\frac{\mathrm{R_{Mobile\text{-}Tag}}}{\mathrm{R_{Reader\text{-}Tag}}}\right)^2, \qquad (4)$$

where $\mathrm{P_{Reader}}$ and $\mathrm{P_{Mobile}}$ stand for the transmitted powers (EIRP) of RFID reader and mobile phone, and $\mathrm{R_{Mobile\text{-}Tag}}$ and $\mathrm{R_{Reader\text{-}Tag}}$ represent the corresponding distance to the RFID transponder. Considering equal distances from RFID reader and mobile phone to the transponder, a SIR of 6 dB means that the communication does not get disturbed when the RFID reader power is at least 6 dB higher than the interference power.

A closer look at a certain (arbitrarily chosen) frequency, for example 880 MHz, over varying reader power leads to the behaviour shown in Fig. 7.

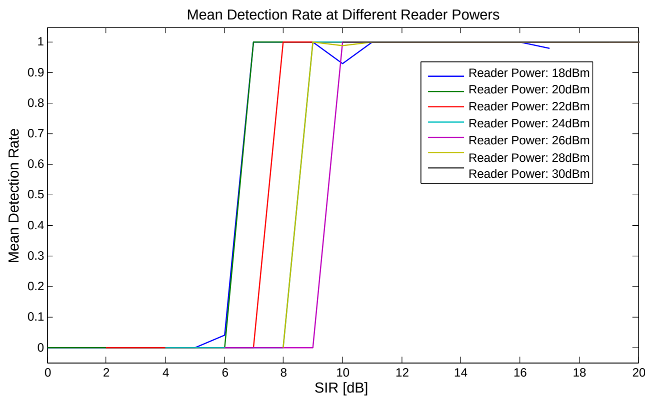


Fig. 7: Mean detection rates for CW interferences at 880 MHz over SIR. The 24 dBm corresponding plot is overlaid by the 28 dBm plot. Interference power was limited, thus a disturbance could not be reached with a high reader power of 30 dBm. The mean detection rate is therefore 1 and above the SIR of 10 dB.

With a reader power of e.g. 26 dBm and therefore a necessary SIR of more than 9 dB, a mobile phone with 2 W (ERP) transmission power would disturb the RFID transponder in a distance of $\approx 6.3 \cdot \mathrm{R_{Reader\text{-}Tag}}$. For example, at a distance of 2 m between RFID reader and tag, a packet collision between an UHF RFID packet (from the reader) and a GSM uplink burst from a mobile phone in a distance of up to 12.6 m would cause a packet error at the RFID transponder.

### *B. Timing*

The GSM system does not use continuous wave form signals, but instead uses short pulses due to TDMA modulation. This behavior makes it necessary to take a closer look at the GSM and RFID communication protocols and their timing characteristics. Assuming that the receiving disturbance of the transponder is the most significant influence, interference from the transponder's reply can be ignored. In simple form, the communication between a RFID reader (Interrogator) and a transponder (Tag) is outlined in Fig. 8.

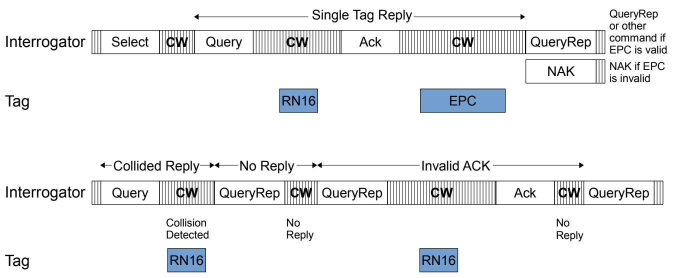


Fig. 8: Communication procedure of an inventory round for a single tag (based on[3])

The 'Select' command addresses a group of tags based on user-defined criteria. If a tag is not activated by that command, meaning it is not addressed or the Select command is disturbed, it will not respond to further commands.

The comparison between the GSM and RFID timings is illustrated in Fig. 9 in a simplified manner. The following assumptions are made for the following investigations:

- GSM: 1 Slot used (representing a phone call)
- RFID: Reader Data Rate: 40kbits; Transponder Data Rate: 80kbits

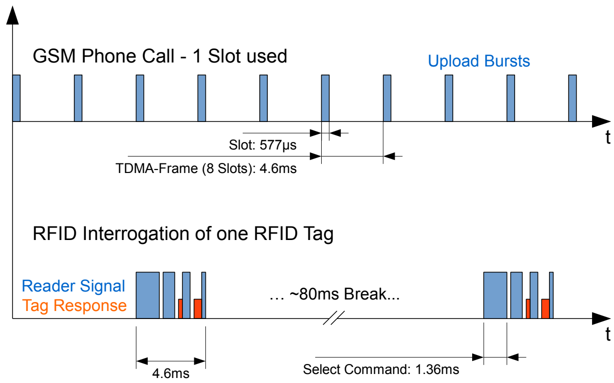


Fig. 9: GSM TDMA timing for one used slot compared to UHF RFID interrogation signal

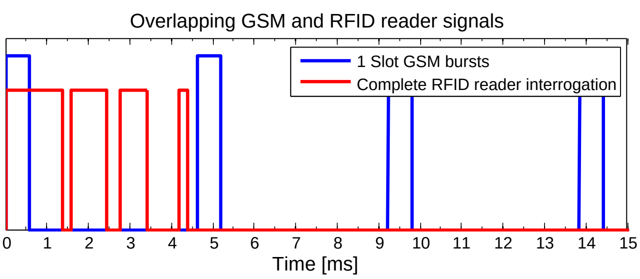


Fig. 10: GSM and RFID signals for detection rate simulation

In Fig. 10 the exemplary GSM and RFID signals are shown. Both are discretized by 1 µs and have a maximum amplitude of 1. A cross-correlation of both signals yields the window of overlap (in microseconds) available at each instant, during which a disturbance can occur in the period of a RFID reader interrogation (also discretized by 1 µs). Normed by the data rate, this signal represents the amount of overlapping bits at each time step (microsecond). Moving forward, this signal will be called 'c' and shall be interpreted as a vector. Averaging the 'probability' of an uncorrupted bit to the power of vector c (element-wise) results in a value that can be interpreted as a mean detection rate 'DR'. The corresponding equation and its application to the previous GSM and RFID signals are given in Eq. 5 and represented in Fig. 11 as dashed lines. 'BER' stands for bit error rate. A BER of 1 means that every bit overlapped by a GSM burst is corrupted. For comparison a constant disturbance (continuous sine wave) was also simulated.

$$\mathrm{DR}(BER) = \mathrm{mean}((1 - BER)^{c}) \tag{5}$$

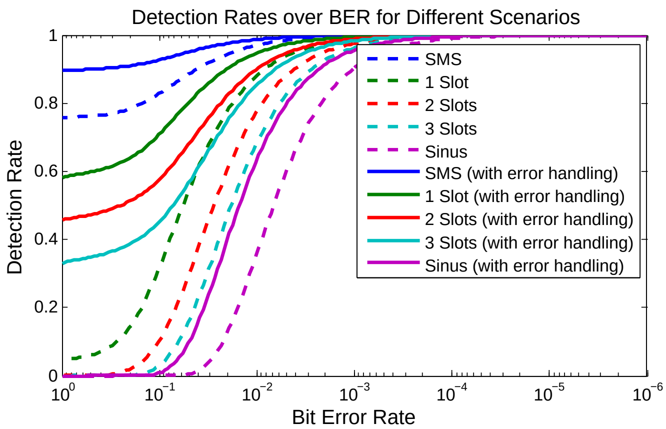


Fig. 11: Simulation of detection rates over BER for different GSM scenarios and with and without error handling techniques

The 'Select' command has the longest duration in comparison to the other commands and because of it functions as transponder activator, it is likely the only command that can not be caught by error handling techniques. This means when only the select command is disturbed the whole interrogation will fail. The protocol specified in the EPC Class-1 Gen-2 Standard[3] is more complicated, but this assumption will suffice for first investigation purposes. Corresponding simulation results (commands except 'Select' are caught by error handling) are shown in Fig. 11 as solid lines.

With BER $= 1$ (with which every overlapping bit is corrupted) Table I summarizes the mean detection rates for different GSM scenarios, with and without error handling techniques, which is equivalent to considering the disturbance of only the 'Select' command and the disturbance of all commands.

For various reader powers and slot configurations, the detection rate was measured twenty times and averaged while increasing the interference power. For one and two slot interferences, this is shown in Fig. 12. The small oscillations are due to insufficient measurement values.

| | Without Error Handling | Error Handling |
|---|---|---|
| SMS | 0.76 | 0.9 |
| 1 Slot | 0.04 | 0.58 |
| 2 Slot | 0 | 0.46 |
| 3 Slot | 0 | 0.33 |
| Sinus | 0 | 0 |

Table I: Simulated detection rates with full disturbance at overlapping signals

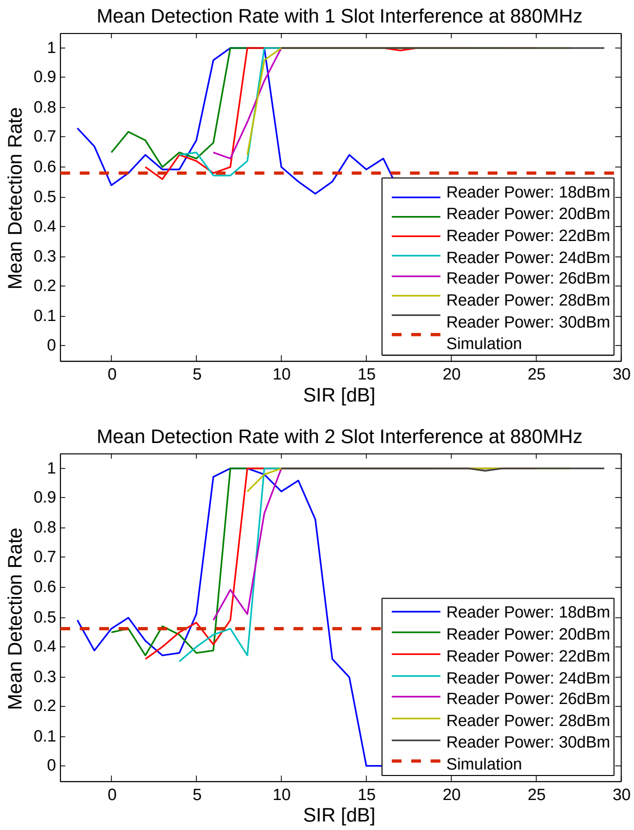


Fig. 12: Measured mean detection rate for one and two slot interferences over SIR

Low interference powers (high SIRs) are not strong enough to cause any communication disturbances. With SIRs between $5\,\mathrm{dB}$ and $10\,\mathrm{dB}$ the mean detection rate decreases abruptly and settles for further increasing interference powers. Notable in both plots are the falling detection rate with a reader power of $18\,\mathrm{dBm}$, and increasing SIR. This can be explained with range extensions, where $18\,\mathrm{dBm}$ is too low to provide the transponder chip with enough power. With the additional power from interference, the transponder powers up until its receiver becomes affected and the detection rate decreases again. The plateau on which the detection rates settle with low SIR nearly matches the simulated values in Table I for a BER $= 1$ and only the select command considered (error handling). Measurements with three slots also matched.

### *C. Near-Field Measurement*

In the near-field scenario the UHF transponder is located in the very close proximity of a transmitting mobile phone. This situation can for example occur when a headset is used to make a telephone call and the phone is carried in the same bag as a transponder (e.g. used for access control). In contrast to the far field case, the field strengths are significantly higher. To evaluate this near-field interference, the transponder under test was located close to a real mobile phone as shown in Fig. 13.

Fig. 13: Measuring setup for near-field investigations

The firmware of the mobile device is modified (OsmocommBB[4]) in that way that most frequently performed actions (phone call, SMS sending, GPRS upload) can be done with adjustable settings (frequency, power, slot allocation). In this setup no reference can be measured for calculating the SIR. Instead, the transmitting power determined in the modified firmware of the phone was logged.

In a frequency sweep measurement (only one slot used) the mean detection rate did not show any significant frequency dependencies as can be seen in Fig. 14. A possible explanation is that the presence of the mobile phone in the near-field detunes the transponder's antenna impedance matching and shifts the sensitive frequency range to the outside of the GSM band. What is striking is that the presence of the mobile device alone requires a $5\,\mathrm{dB}$ to $6\,\mathrm{dB}$ higher reader power to achieve the detection threshold.

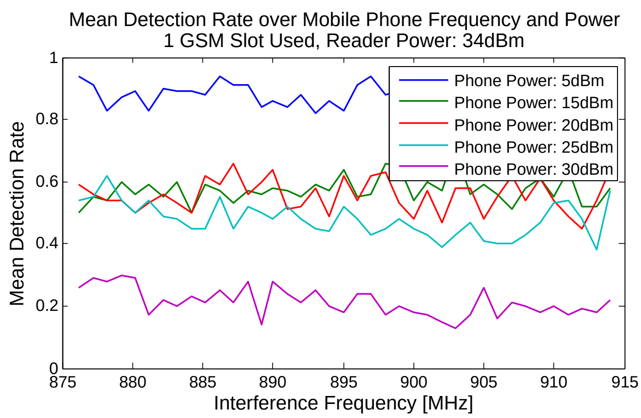


Fig. 14: Mean detection rate in near-field over frequency

Increasing the transmit power of the mobile phone leads to decreasing mean detection rates as depicted in Fig. 15. There is no saturation effect as measured before in the far-field scenario. It is very likely that the interference power in the measurement before was just not high enough. For high powers the mean detection rate easily drops below $10\,\%$ with this particular transponder. Using 2 slots leads to a maximum detection rate of $5\,\%$ and 3 slots to even only $2\,\%$. In the SMS scenario, however, the mean detection rate never dropped below $80\,\%$ independent of power and examined transponder.

In contrast to the far-field measurements, where the interference is most likely based on only the time overlapping GSM pulses and RFID downlink, it seems that a higher interference power makes the receiver temporary numb after each pulse. This transient effect leads to detection rates decreasing down to almost zero percent.

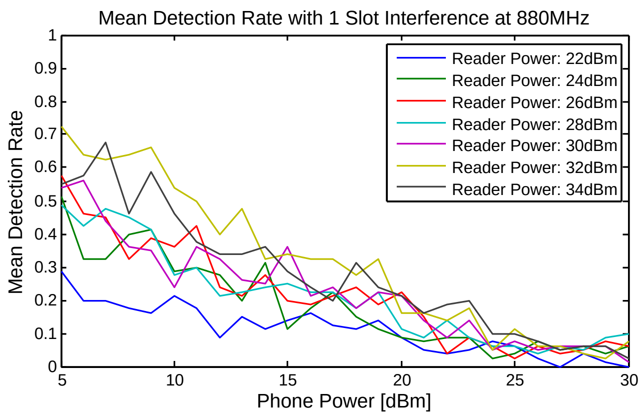


Fig. 15: Mean detection rate for one slot interferences in near-field over phone power

## III. Conclusion

In this paper interferences of GSM uplink signals on passive UHF RFID transponders in accordance of the ISO/IEC 18000-6 standard were analysed. GSM uplink signals are critical as interferer, because the mobile device can be located close to a transponder system and the used frequency ranges of the GSM 850/900 and UHF RFID systems overlap.

Far-field measurements showed that the corresponding RFID transponders are very sensitive over a large frequency bandwidth, most likely to ensure worldwide functionality. With increasing interferer power, detection rates decreased rapidly at a certain ratio of RFID reader power and interference power, called 'SIR'. One of the examined transponders showed this SIR threshold to be $9\,\mathrm{dB}$ with an interference frequency of $880\,\mathrm{MHz}$ and a reader power of $26\,\mathrm{dBm}$. Thereby, a GSM mobile phone with $2\,\mathrm{W}$ (ERP) can disturb the RFID communication even when the mobile phone is located over six times farther from the transponder than is the RFID reader.

The GSM system uses TDMA thus it was important to study the effect of interference pulses on the RFID communication. The 'Select' command in the RFID communication protocol was found to play an important role in the interference behaviour and is probably responsible for low detection rates when the command is disturbed. This could be explained by the purpose of this command itself. Only when the 'Select' command activates the RFID transponders, error handling techniques can take effect. However, the select command is one of the longest commands and therefore particularly vulnerable. If disturbed, the transponders do not know whether they have to react to the interrogation or not.

In conclusion, the results indicate that with the same amount of interrogations, a shorter 'Select' command (and thus a higher reader data rate) led to higher detection rates concerning overlapping GSM and RFID signals. Doubling the transponder data rate had no effect, whereas doubling the reader data rate increased the mean detection rates by over $10\,\%$. With increasing functionality of the RFID systems, e.g. encryption, the vulnerability of longer commands to GSM interferences will probably increase.

Investigations in the near-field of the transponder were carried out by mounting a firmware-modified mobile phone onto the transponder. Just the presence of the mobile phone itself made a $5\,\mathrm{dB}$ to $6\,\mathrm{dB}$ higher reader power necessary to achieve the detection threshold. Moreover, the phones presence in the near-field also detuned the transponder's antenna and shifted the sensitive frequency ranges to the outside of the GSM band. The extremely high interference power of the mobile phone decreased the mean detection rate further to almost zero for configurations using one or more slots. An exception to that is the case of sending SMS. Breaks between the pulses are too long to seriously affect the RFID communication. Even with high interference powers, the mean detection rates never dropped below $80\,\%$.

Last but not least, it should be mentioned that not only GSM but also other mobile communication systems can interfere UHF RFIDs. One of these, for example, is the LTE B20 uplink at $832\,\mathrm{MHz} - 862\,\mathrm{MHz}$, that is used worldwide.

## References

[1] K. Finkenzeller, 2012: *RFID Handbuch (RFID Handbook)*, 6th ed. Munich, Germany: Hanser Verlag, ISBN 978-3446429925, http://rfid-handbook.de

[2] ISO/IEC FDIS 18000-63, 2012: Information technology - Radio frequency identification for item management - Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C. Geneva, Switzerland.

[3] GS1: EPC Radio-Frequency Identity Protocols Generation-2 UHF RFID. http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2, visited: 02.12.2013

[4] Osmocom: OsmocomBB EMI Firmware. http://bb.osmocom.org/trac/wiki/emi-firmware, visited: 09.11.2013

**Benjamin Brunner** was born in Überlingen, Germany, in 1988. He received the M.Sc. degree in electrical engineering from the Technische Universität München, Munich, Germany, in 2014. Following this, he joined the perisens GmbH. In 2015 he changed to the A.D.C. Automotive Distance Control Systems GmbH (Continental).

**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 engineering company for high frequency electronics (perisens GmbH), where he is chief executive. Since 2013, he is visiting lecturer for an automotive radar course at the university of applied science in Ingolstadt (THI). Florian Pfeiffer is a member of the Informationstechnische Gesellschaft (ITG) in the Verband Deutscher Elektrotechniker (VDE).

**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 Giesecke & 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 NI 17.8 (ISO/IEC 14443) for more than 10 years now. Up to now he has published more than 130 individual patent applications, mainly in the RFID field of technology. In 1998 he published the RFID handbook, which now is available in its 6th 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.

**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.