Hochschule Ostwestfalen-Lippe
University of Applied Sciences

Institut Industrial IT
www.init-owl.de

Research Project

Systematic Investigation of Interference Immunity, Transmission, and Data Security of Industrial Wireless Technologies

Systematische Untersuchung der Störfestigkeit, Übertragungs- und Datensicherheit industrieller Wireless-Technologien (SUDIWI)

Hochschule Ostwestfalen-Lippe
Project Number: 1769X05
Project time: 01.07.2006 - 31.12.2007

Final Report

(Sachbericht des Zwischennachweises nach Nr. 6 ANBest-P)

Prof. Dr.-Ing. Uwe Meier
Prof. Dr. rer. nat. Stefan Heiss
M.Sc. Kaleem Ahmad, Dipl.-Ing. Kai Helmig

Lemgo, 27.06.2008

Prof. Dr.-Ing. Uwe Meier
Hochschule Ostwestfalen-Lippe
Department of Electrical Engineering and Computer Science
Fachbereich Elektrotechnik und Technische Informatik
Institut *Industrial IT*
Liebigstrasse 87
D-32657 Lemgo

uwe.meier@hs-owl.de
www.hs-owl.de/fb5 or www.init-owl.de

Content

Summary

Systematic Investigation of Interference Immunity, Transmission, and Data Security of Industrial Wireless Technologies (SUDIWI)

Project Partner
Weidmüller Interface GmbH Co. KG, Detmold
OWITA GmbH, Lemgo
RS-Schwarze GmbH, Schloss Holte-Stukenbrock
Fachhochschule Solothurn Nordwestschweiz, Olten, Schweiz

Funded by BMBF, programme "Angewandte Forschung an Fachhochschulen im Verbund mit der Wirtschaft (FH^3)"; project number: 1769X05; project time: 01.07.2006 - 31.12.2007

Abstract
Wireless technologies are increasingly desired in numerous innovative applications of industrial automation. Meanwhile, a great variety of commercial wireless technologies (Bluetooth, WLAN, ZigBee, nanoNET) is available which are offered as a large selection of OEM products. To avoid later disappointments technological limits should be considered early in the initial planning stage. Passive impairments, like multipath propagation and time varying channel responses due to movements, as well as active sources of disturbances have to be considered. The latter are caused by parasitic machine emissions and unintentional or even intentional other wireless systems. For the same reason decisions concerning the usage of security features and/or enhancements have to be made in the initial planning phase of an industrial wireless application, to choose solutions from a suitable set of protocols, technologies and products that support the identified security aims.
The goal of this research project was the investigation of the transmission reliability of wireless systems for industrial applications. Additionally, an assistance guide (User Manual, see Appendix) should be developed with two major issues:

- Firstly, enterprises of the industrial automation area, especially companies of small and medium size, should be given help for the development of interference resistant wireless products.
- Secondly, prospective customers shall be offered guidance for installation, and constraints for planning a wireless automation system shall be outlined.

Thus, an effort should be made in order to place the continuing industrial usage of wireless technologies on a reliable ground. Resulting from the investigations of this project we can conclude that available wireless automation systems are reliable supplements - but no substitutes - for wire based fieldbus systems.
Packet loss rates PLR < 1e–5 can be achieved with respect to passive environmental effects like multipath or channel movements. However, it is necessary, that line-of-sight communication is possible. Maximal distances of 10...30 m are possible, depending on the maximal allowed path loss. As a rule of thumb we suggest, that the theoretical path loss limit of transmitter power over receiver sensitivity shall be at least 30 dB above the intended operational path loss.
A crucial parameter is the coexistence behavior of any wireless system. We were able to show, that interference from other wireless systems is the most important source of system degradation. We suggest system guidelines to improve and optimize the coexistence behavior.

Anyway, it remains the main source of impairment and needs to be investigated very carefully.
As existing wireless systems lack information about their coexistence behavior, we further suggest the development of *standardized measurement guidelines*. They will provide important quantitative features of wireless systems in order to improve the process of *frequency management* in manufacturing companies. All wireless products should be certified according to the proposed new measurement standard.
This study reports the possibilities and limitations of state-of-the-art and widely used existing technologies. As a conclusion, it recommends further necessary research: Only collaborative systems should be used in future high density coexistence environments. Technological enhancements like ultra-wide-band systems (UWB) and multiple-input-multiple-output features (MIMO) will further improve the performance of next generation wireless PAN systems.

1 Goal

Wireless technologies are increasingly desired in numerous innovative applications of industrial automation. Meanwhile, a great variety of commercial wireless technologies (Bluetooth, WLAN, ZigBee, nanoNET) is available which are offered as a large selection of OEM products. To avoid later disappointments technological limits should be considered early in the initial planning stage. Passive impairments, like multipath propagation and time varying channel responses due to movements, as well as active sources of disturbances have to be considered (Fig. 1). The latter are caused by parasitic machine emissions and unintentional or even intentional other wireless systems. The presence of other wireless systems creates a coexistence environment.

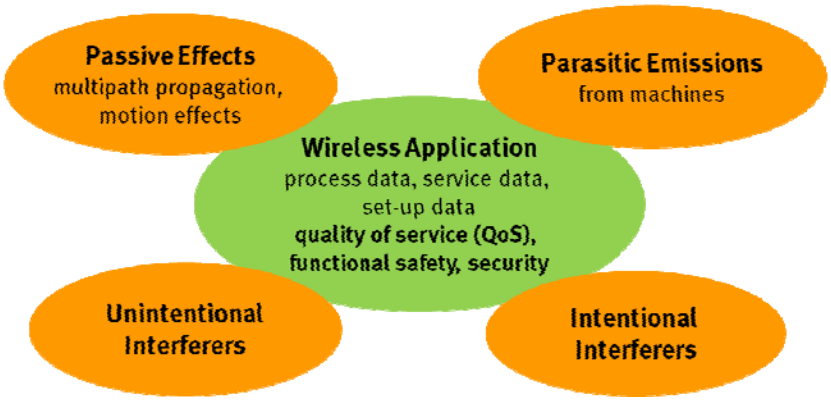


Figure 1: In contrast to wire based transmission systems wireless applications can be impaired by several environmental effects

The goal of this research project was the investigation of the transmission reliability of wireless systems for industrial applications. Additionally, an assistance guide (User Manual, see Appendix) should be developed with two major issues:

- Firstly, enterprises of the industrial automation area, especially companies of small and medium size, should be given help for the development of interference resistant wireless product.
- Secondly, prospective customers shall be offered guidance for installation, and constraints for planning a wireless automation system shall be outlined.

Thus, an effort should be made in order to place the continuing industrial usage of wireless technologies on a reliable ground.

2 Prerequisites

The project was carried out in the institute Industrial IT *(inIT)* of the Ostwestfalen-Lippe University of Applied Sciences. *inIT* is part of the department of *electrical engineering and computer science*. Contributing persons were

- Prof. Dr.-Ing. Uwe Meier; head of project; part time
- Prof. Dr. rer. nat. Stefan Heiss; part time

- Prof. Dr.-Ing. Stefan Witte; part time
- Dipl.-Ing. Kai Helmig; scientific member; 01.07.2006 - 30.09.2007
- M. Sc. Kaleem Ahmad; scientific member; 01.10.2007 - 31.12.2007
- Dipl.-Ing. Rainer Günther; scientific member; part time
- Ajay Bhardwaj; student work contract; part time
- Sureshkumar Ponnampalam; student work contract; part time
- Min Jing Nigel Goh; student work contract; part time
- Curtis Cretton; student work contract; part time

3 Project Organization

To answer the relevant questions of the project proposal five main work packages were defined:

- Investigation of interference immunity for relevant wireless technologies with a focus on Bluetooth, WLAN, ZigBee, nanoNET.
- Investigation of the quality and reliability of industrial data transmission for selected wireless technologies.
- Security investigation with respect to industrial applications and vulnerability.
- Definition of parameter for an optimal system design.
- Recommendations for standard measurement procedures should be worked out and should be submitted to appropriate organizations.

4 State of the Art

Important publications by other research groups which have been considered in this project:

[1] M. B. Shoemake: Wi-Fi (IEEE 802.11b) and Bluetooth, Coexistence Issues and Solutions for the 2.4 GHz ISM Band, Texas Instruments February 2001, White Paper

[2] A. Batra, J.-M. Ho, and K. Anim-Appiah, Proposal for Intelligent BT Frequency Hopping for Enhanced Coexistence, IEEE 802.15-01/082, January 2001

[3] J. Liang, Proposal for Collaborative BT and 802.11b MAC Mechanisms for Enhanced Coexistence, IEEE 802.15-01/080, January 2001

[4] M. B. Shoemake, Proposal for Power Control for Enhanced Coexistence, IEEE 802.15-01/081, January 2001

[5] M. B. Shoemake and Paul Lowry, IEEE 802.11b and Bluetooth Coexistence Testing Results, IEEE 802.15-01/084, January 2001

[6] U. Meier: Funkübertragung in Feldbussystemen, Schlussbericht BMBF 1708599; Berichtszeitraum 01.09.1999 - 30.04.2001; Lemgo: Fachhochschule Lippe, Fachbereich Elektrotechnik und Informationstechnik; Hannover: Universitätsbibliothek und

Technische Informationsbibliothek; 2001

[7] S. Witte, M. Schnückel: Drahtlose Kommunikation von Automatisierungskomponenten mit mobilen, kommerziellen Endgeräten, BMBF-Projekt 01.09.2003 - 28.02.2005, Förderkennzeichen 1705003, Abschlussbericht

[8] A. Willig, K. Matheus, A. Wolisz, Wireless Technology in Industrial Networks, Proc. of the IEEE, vol. 93, no. 6, June 2005

[9] L. Rauchhaupt, "Funkgestützte Kommunikation in der Automatisierungstechnik" In: at–Automatisierungstechnik 53 (2005) Nr. 4-5, S. 197ff

[10] Verein Deutscher Ingenieure, Verband der Elektrotechnik, Elektronik, Informationstechnik: Funkgestützte Kommunikation in der Automatisierungstechnik (Radio based communication in industrial automation), VDI/VDE Richtlinie 2185, September 2007

[11] Körber, H.-J.; Wattar, H.; Scholl, G.: Modular wireless Real-Time Sensor/Aktor Network for Factory Automation Applications; IEEE Transaction on Industrial Informatics, Volume 3, Nr. 2, May 2007

[12] L. Rauchhaupt, E. Hintze, A. Gnad: Über die Bewertung der Zuverlässigkeit industrieller Funklösungen, Automatisierungstechnische Praxis, atp 49, 2007, Heft 3 (38 - 47), Heft 4 (50 - 57)

[13] K. M. J. Haataja: Evaluation of the current state of Bluetooth security, Department of Computer Science, University of Kuopio, 2007

[14] N. K. Dennis, P. A. Porras, E. Jonsson: How to secure Bluetooth-based piconetworks, in Proc. of the 26th International Conference on Computer Safety, Reliability, and Security (SAFECOMP), September 2007

[15] K. Scarfone, D, Dicoi: Wireless Network Security for IEEE 802.11a/b/g and Bluetooth (DRAFT), NIST SP 800-48r1, August 2007

5 Co-operation with Partners

Cooperating industrial partners were Weidmüller Interface GmbH Co. KG (www.weidmueller.de) from Detmold and OWITA GmbH (www.owita.de) from Lemgo. Both companies have very much experience in developing industrial wireless systems. They further offer broad experience in the field of wireless industrial applications. This experience could be utilized during the research work of this projects.
The company RS-Schwarze GmbH (www.rs-schwarze.de) from Schloss Holte-Stukenbrock was a very helpful partner in developing the coexistence based measurement test sites. They provided numerous contacts to further supporting companies.
We further appreciate a lot of helpful and stimulating discussions with our partners from Fachhochschule Solothurn Nordwestschweiz (www.fhnw.ch), Olten, Switzerland.

6 Results

6.1 Measurement Devices

Bluetooth, ZigBee IEEE 802.15.4, nanoNET CSS (chirp spectrum spreading), and narrowband FSK were selected as WPAN systems for the investigations in this research project. WLAN was considered only as an additional interferer. The following subsections provide a short overview of these technologies.

Bluetooth: Bluetooth based on IEEE 802.15.1 was originally designed as a cable replacement technology. In order to allow for worldwide deployment, it is placed in the ISM band at 2.4 GHz. It uses GFSK for signal modulation, FHSS for spreading, TDMA for channel access and TDD for duplexing. For Bluetooth transmission 79 radio frequency channels with 1 MHz spacing are defined over a total bandwidth of 79 MHz. Three classes are defined with respect to the transmitting power level: class 1 transmits with 20 dBm for a maximum range of approximately 100 m, class 2 transmits with 4 dBm for approx. 30 m, and class 3 with 0 dBm covering a maximum range of 10 m. The requirement for a Bluetooth receiver is a minimal sensitivity level of at least –70 dBm. Adaptive frequency hopping, forward error correction (FEC) and automatic repeat request (ARQ) with maximal 5 retransmissions were used.

NanoNET (nanoPAN 5360): It is based on the IEEE 802.15.4a WPAN standard and implements chirp spread spectrum (CSS) modulation. It operates in the 2.4 GHz ISM band. This system achieves a maximum bit rate of 2 Mbps, although 1 Mbps and 500 kbps can also be selected. The targeted range for nanoNET is a maximum outdoor range at LOS of approximately 900 m and an indoor range of approximately 60 m (typical). The transmission power can vary from –42 dBm to +6.9 dBm. The receiver sensitivity is –92 dBm @ 1 Mbps. CSMA/CA is implemented to access the channel. Forward error correction (FEC) with a (7,4) HAMMING code and automatic repeat request (ARQ) with maximal 5 retransmissions were used.

Figure 2: Bluetooth based sensor actor interface (SAI) module with integrated antennas (Weidmueller)

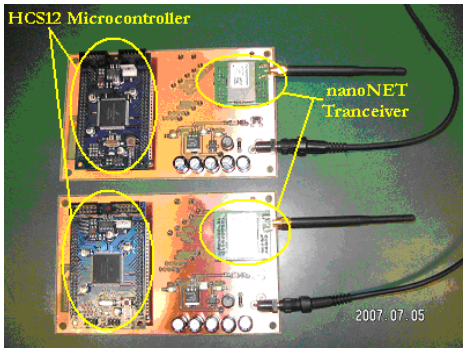


Figure 3: Two NanoNET systems (nanotron) with HCS12 microcontroller

ZigBee IEEE 802.15.4: ZigBee is a low data rate, low power consumption, and low cost wireless networking technology. It is built on the MAC and physical layer of IEEE 802.15.4. The IEEE 802.15.4 standard specifies a low data rate solution with multi-month to multi-year battery life and very low complexity. It implements CSMA/CA to access the channel. It specifies three physical layers operating in the 868/915/2400 MHz band and provides a maximum bitrate of 250 kbps. It implements O-QPSK/DSSS to modulate signals in the 2.4 GHz band. Two additional optional physical layers are also specified working in the 868/915 MHz band. A total of 27 channels numbered 0-26 are available,

16 of which are in the 2.4 GHz band, 10 in the 915 MHz band and 1 in the 868 MHz band. As IEEE 802.15.4 specifies only the lower two layers of the protocol, the ZigBee alliance aims to provide the upper layers of the protocol stack, from the network to the application layer. CRC for error detection without any retransmission was used. Packets were discarded in case of detected errors.

WLAN: IEEE 802.11 often called Wi-Fi/WLAN, is composed of a number of specifications that primarily define the physical and MAC layers of WLAN systems. IEEE 802.2 LLC is used as a standard interface between MAC and higher layers. It has many extensions but only IEEE 802.11g is studied in this project. It offers up to 54 Mbps bitrate and operates in the 2.4 GHz ISM band. It supports four different physical layers of which two are mandatory: ERP-DSSS/CCK and ERP-OFDM. Although principally 13 different channels each with a 20 MHz bandwidth can be used (Europe except France and Spain), only three non-overlapping channels can be selected to operate in parallel. CSMA/CA is used to access the channel.

Figure 4: 802.15.4 system with MG2400-F48 transceiver (Radiopulse)

Figure 5: WLAN access point (Linksys)

Narrowband FSK: The ATR 2406 transceiver developed by Atmel Corporation is used to study narrowband FSK. It operates in the 2.4 GHz ISM band. With a maximum power level of 4 dBm it can range up to 30 m. It offers 95 channels each with 864 kHz bandwidth. The maximal bitrate is 1.1 Mbps but smaller values can also be selected. No channel access method nor any error correction is implemented for it.

6.2 Measurement Environments

Several different environments were investigated in order to achieve results which enable generic conclusions:

- *Anechoic shielded measurement chamber* (AC): This room serves as a reference environment. It is the best radio environment without multipath, time-varying or interference effects.
- *University labs* (LAB): Measurements in this environment provide results in the area between office and industrial environments.
- *Industrial environments* (IND) cover the main area of investigation.

  IND 1 Mechanical production hall, 12 m distance, line of sight (LOS), moving persons.

  IND 2 Mechanical production hall, 12 m distance, obstructed line of sight (OLOS), moving persons.

  IND 3 Mechanical production hall, 3 m distance, OLOS, slow machine movements.

IND 4 Connector assembling machine, 4 m distance, LOS, fast cyclic machine movements.

IND 5 Mechanical production hall, 3 m distance, LOS, sparc erosion machines were operating.

IND 6 Warehouse with high shelf cantilever system, NLOS, distance range 1...50 m, cantilever speed up to 0.6 km/h, SAI was located in a plastic box.

IND 7 Warehouse with high shelf cantilever system, NLOS, distance range 1...50 m, cantilever speed up to 6 km/h, SAI was located in a plastic box.

IND 8 Robot based production cell, LOS, moving SAI with 13 km/h, distance range 1...4 m

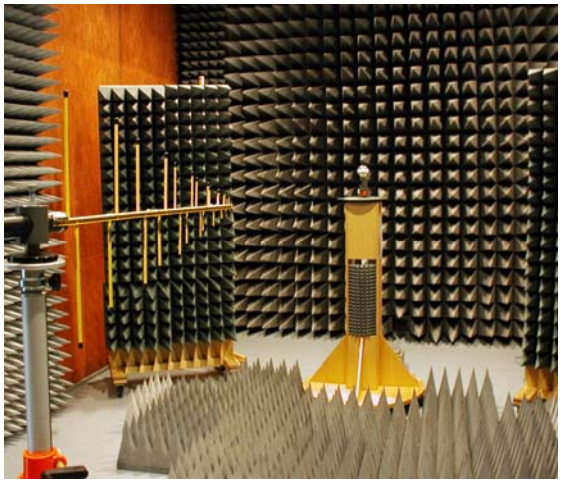


Figure 6: Environment AC

Figure 7: Environment IND 1, 2

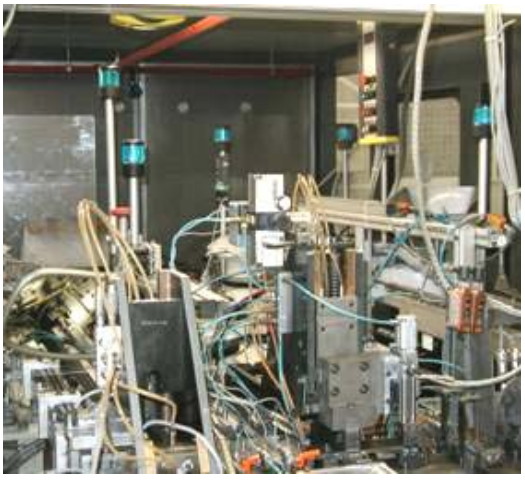


Figure 8: Environment IND 4

Figure 9: Environment IND 5

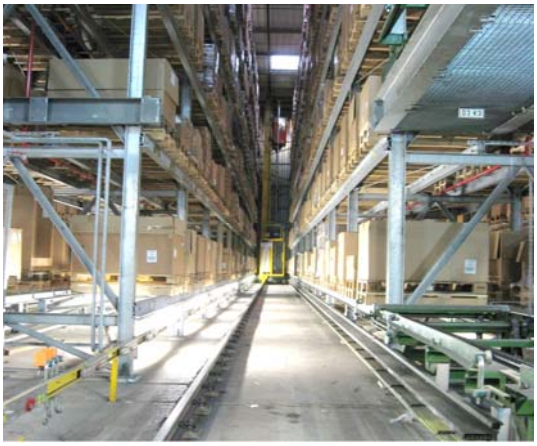


Figure 10: Environment IND 6, 7

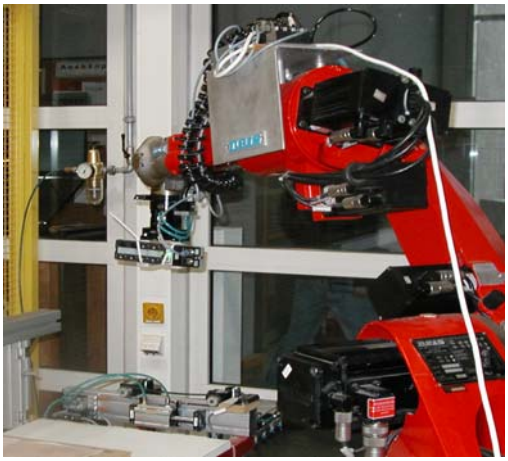


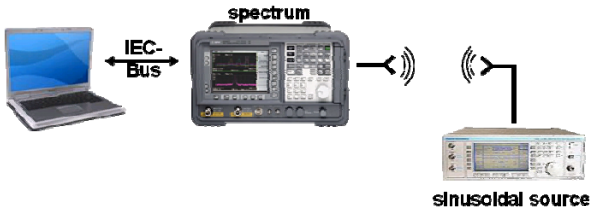
Figure 11: Environment IND 8

6.3 Test Sites

Different test sites were developed during this project. They can be classified with respect to the transmission layers of the wireless system.

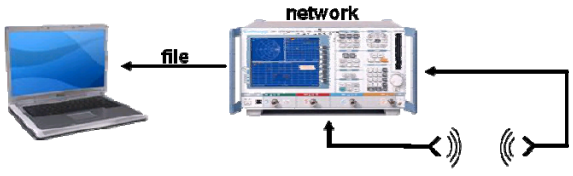
- *High frequency layer (RF layer)*: channel loss, delay spread, coherence bandwidth, DOPPLER spread, coherence time. Measurement devices: vector network analyzer, spectrum analyzer
- *Base band layer*: packet repetitions; signal-to-noise ratio (SNR); received signal strength (RSSI); packet loss rate (PLR); bit error rate (BER)
- *Application layer*: packet loss rate (PLR); bit error rate (BER); delay or latency; jitter

Each of the test sites provides the measurement of specific parameters. All test sites are plotted and briefly described in the following Figures. Fig. 12 and Fig. 13 show the test sites of the RF layer.



Detection of interferers
Investigation of time-varying channels
Channel attenuation for moving DUTs
DOPPLER spread, coherence time

Figure 12: Spectrum analyzer



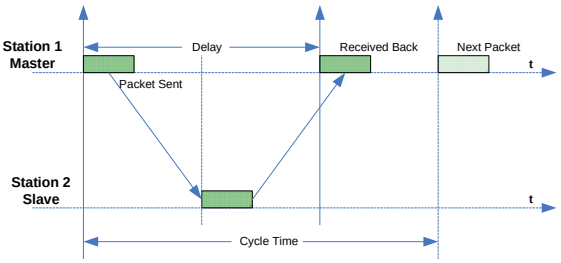
Investigation of multipath propagation
Channel attenuation for stationary DUTs
Impulse response
Delay spread, coherence bandwidth

Figure 13: Vector network analyzer

The DUTs were operated in a cyclic master-slave configuration. The master generates cyclic requests of the slave which answer with a pre-known telegram. This enables the master to calculate packet loss rate, residual bit error rate, delay or latency and jitter (Fig. 14 and Fig. 15).

Delay and jitter measurements on different protocol layers
Packet loss / packet errors / bit errors

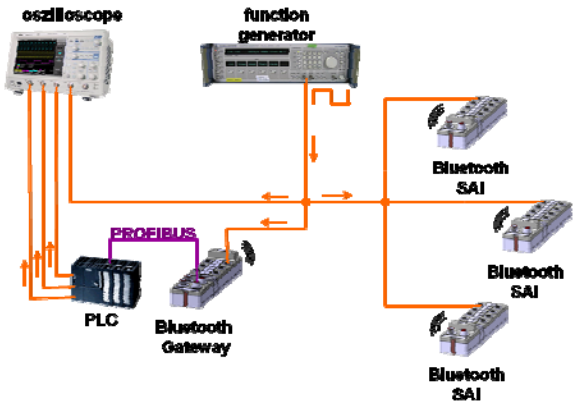
Figure 14: PC based protocol analyzer with master-slave configuration. Slaves are operated in loop-back mode.



Delay and jitter measurements on application layer
Packet loss / packet errors / bit errors

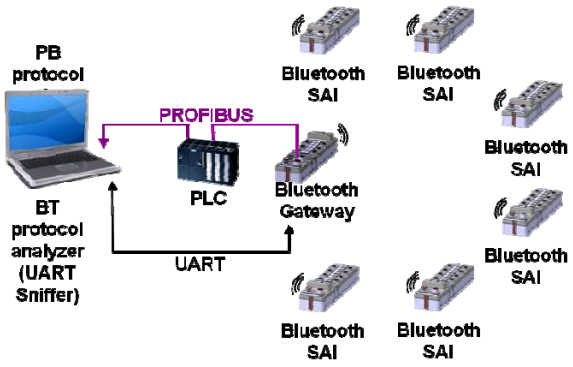
Figure 15: Timing diagram in a master-slave configuration with loop-back mode of the slaves

The Bluetooth system was only operated in a star network topology with up to 6 slaves (Fig. 16 and Fig. 17).



Delay and jitter measurements on the sensor and actuator level
Analyzing the overall performance

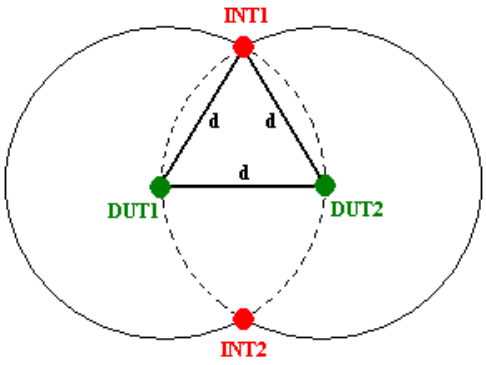
Figure 16: Oscilloscope



Analyzing the overall performance on the sensor and actuator level

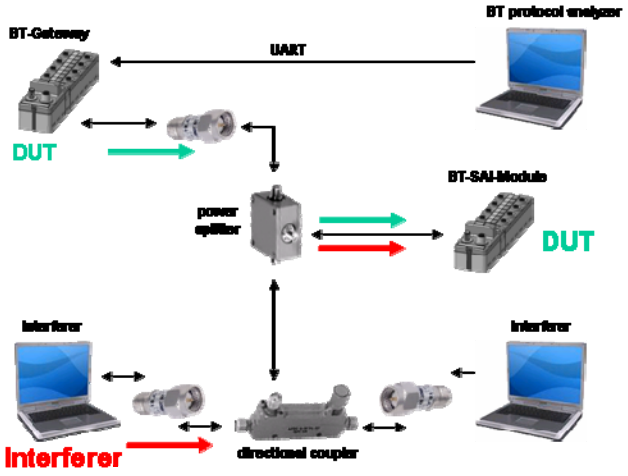
Figure 17: PLC based protocol analyzer

A coexistence test setup was used to investigate the coexistence behavior of different systems (Fig. 18). The distance between the DUT (device under test) transceivers and between DUT and interferer is identical. This distance *d* should be selected as a typical distance with respect to the intended application. We selected $d = 3\,\mathrm{m}$ for all measurements. Measurements according to Fig. 18 were carried out in the environments given in section 6.2.
Additional measurements were carried out with the cable based test site of Fig. 19. This test site enables reproducible measurements of the interfering behavior without any multipath or time-varying contributions.



A distance of 3 m was selected as a representative WPAN distance

Figure 18: Recommended equal-distance coexistence test site



Reproducible measurement environment
Investigation of interfering behavior without multipath or time-varying environmental contributions

Figure 19: Cable based test site

Resulting from the equal-distance definition in Fig. 18 the *signal-to-interference ratio* (SIR) as the ratio of signal power over interference power at the input of the DUT receiver can be calculated very easily: It is the ratio of the transmitter power levels given in the data sheets, because the DUT signal level and the interferer signal level decay in the same way (Table 1). The following parameter sets were used for the measurements:

- *DUT* = {Bluetooth, ZigBee, nanoNET, narrowband FSK}
- *Interferer* = {Bluetooth, ZigBee, nanoNET, narrowband FSK, WLAN}
- *Coexistence Parameters* = {Frequency, Transmission Power, Retransmission Mechanism, Error Correction Mechanism, Bitrate, Cycle Time, Packet Size, Bandwidth, No. of Interferers, SIR}

Table 1: Technologies investigated vs. interference;
SIR values are given in respective cells for the equal-distance model of Fig. 18

	Bluetooth	ZigBee	nanoNET	FSK
Bluetooth	-	-20dB	-36dB	-16dB
WLAN	0dB	-20dB	-36dB	-16dB
ZigBee	20dB	-	-16dB	4dB
nanoNET	36dB	16dB	-	20dB
FSK	16dB	-4dB	-20dB	-

Investigated technology = ■ *Technology used as interferer* = ■

6.4 Transmission Reliability without Interferers

Fig. 20 and Fig. 21 show typical results of RF channel measurements. Strong time dispersion (Fig. 20) is caused by multipath propagation, while time selective fading is the dominant

channel feature in a moving robot application. Both effects cause either frequency or time varying fading effects.

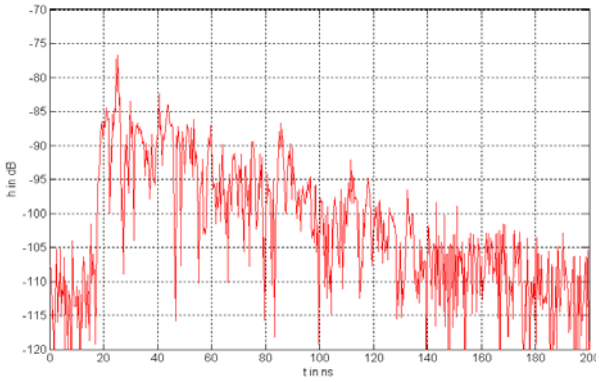


Figure 20: Impulse response in an industrial multipath environment.

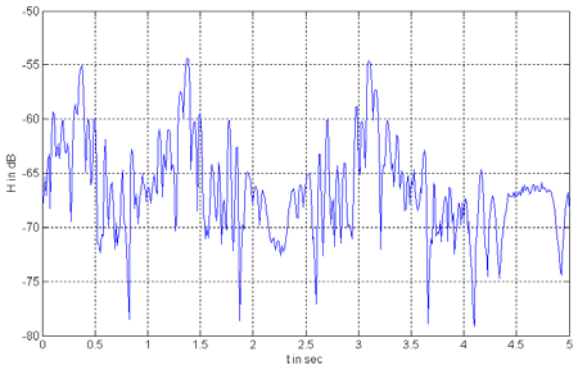


Figure 21: Time varying channel response of a robot application.

To let a wireless system operate successful in such a hostile passive environment, a careful design is necessary with respect to channel loss and fading margin. Pathloss L is the most important parameter for optimal system operation. Fig. 22 shows two linear increasing prediction curves for ideal free space (blue line) and a laboratory environment (green line). They are based on the equation

$$L/\mathrm{dB} = 40.15 + 10 \cdot n \cdot \log_{10}(d/\mathrm{m})$$

with path loss exponents $n = 2$ for ideal free space and $n = 3$ for lab environment. All measured path loss values were found between these two prediction curves.

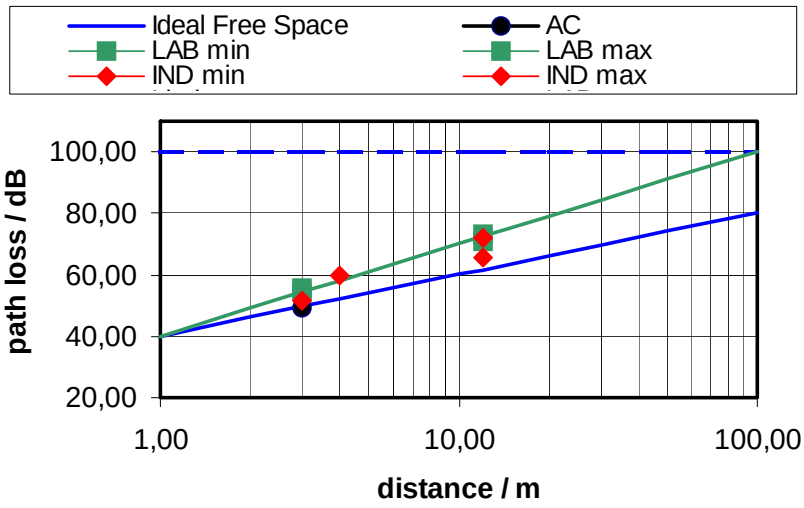


Figure 22: Average pathloss of different environments in the 2.4 GHz band with 0 dBi antennas.

Given a maximal transmitter power of 20 dBm (100mW) and a receiver sensitivity of –80 dBm (10 pW) we can derive a maximal theoretical pathloss of 100 dB. Taking into account fading with pathloss variations of ±15 dB, the maximal average pathloss should not exceed 85 dB. From Fig. 22 we can derive a maximal distance of 30...40 m for a reliable system performance.

Some industrial environments show even more signal fading up to 30 dB. In this case a distance of 10 m should not be exceeded.

Fig. 23 shows results of PLR and BER measurements taken in an anechoic shielded chamber and lab without any interferers are considered as reference values. For the Bluetooth system no bit errors were detected while the PLR was 0 % in the anechoic shielded chamber (AC) and 8e–5 in the lab. The BER for ZigBee also remains zero in both environments while the PLR was almost 0.28 % in the AC and 0.32 % in the lab. For the nanoNET system the BER is in the order of 1e–4 in both environments and the PLR is 0 % in the AC and 0.3 % in the lab. For the narrowband FSK system the BER is 0.2 %, and 0.38 %, respectively and the PLR is 0.76 % and 0.9 %, in the AC and lab environments respectively.
As the FSK system doesn't use any error correcting mechanisms nor frequency hopping, it can be concluded, that such a system cannot meet the requirements of industrial applications.

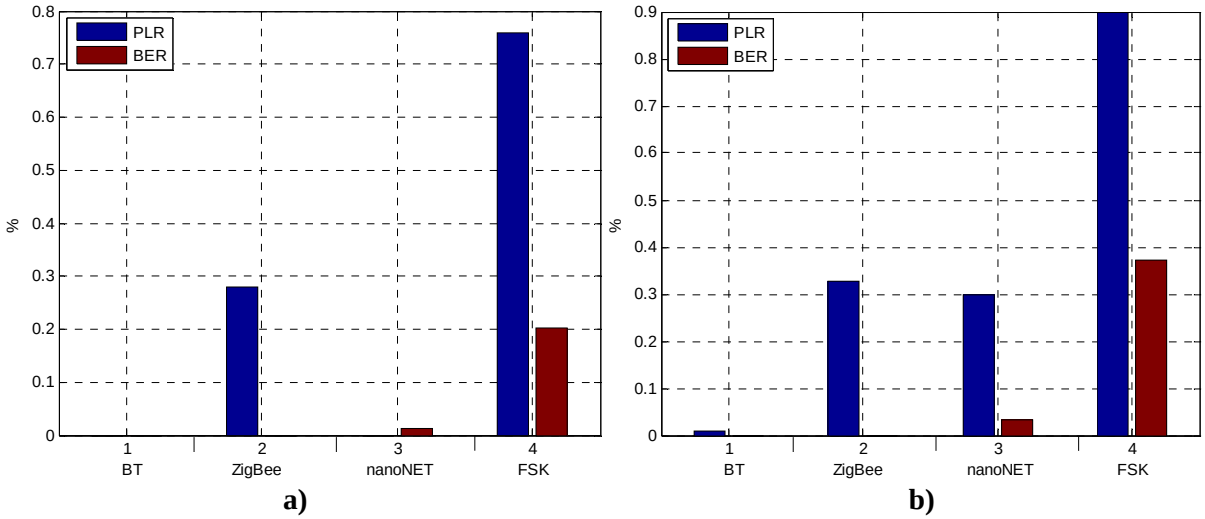


Figure 23: a) Reference measurement: PLR and BER in an anechoic shielded chamber **b)** Reference measurement: PLR and BER in lab without any interference

As the Bluetooth systems is the best of all systems with respect to transmiison reliability, additional measurements were carried out in all environments given in section 4.2. Table 2 lists the results. The reason for the errors in IND 6 and IND 7 was the exceeded coverage range.

Table 2: Packet losses of the Bluetooth system in industrial environments. Packet losses were detected only in these environments.

environment	measurement cycles	erroneous cycles	relative errors
IND 4	9,747	1	$1.0 \cdot 10^{-4}$
IND 6	1,690	5	$3.0 \cdot 10^{-3}$
IND 7	2,986	4	$1.3 \cdot 10^{-3}$

Fig. 24 shows results of delay and jitter measurements on a PROFIBUS network with wireless and wire based sensor actuator interface modules acc. to test site in Fig. 16. The

measured overall jitter depends on Bluetooth jitter, Bluetooth polling time, Profibus polling time and number of SAIs.

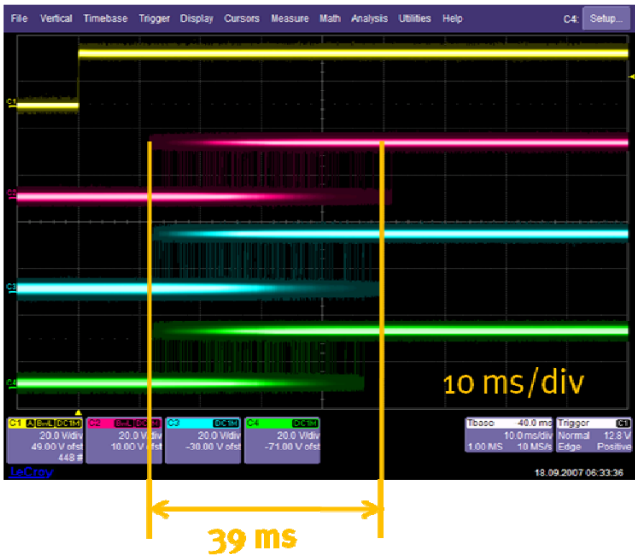


Figure 24: Delay and jitter measurements on a PROFIBUS network acc. to Fig. 16

6.5 Transmission Reliability with Interferers - Coexistence

Section 4.4 showed how a reliable transmission system can be realized with respect to passive effects of the environment. However, interfering effects need to be considered as well. Furthermore it could be derived, that these effects are the worst effects in industrial environments. Table 3 lists the results of Table 2 extended by interfering measurements.

Table 3: Packet losses of the Bluetooth system in industrial environments. Packet losses were detected only in these environments. WLAN interferer with SIR = 0 dB.

environment	measurement cycles	erroneous cycles	relative errors
LAB, 3m, 2 interferers	21,705	3	$1.4 \cdot 10^{-4}$
LAB, 12m, 1 interferer	15,293	5	$3.3 \cdot 10^{-4}$
LAB, 12m, 2 interferers	9,451	4	$4.2 \cdot 10^{-4}$
IND 4	9,747	1	$1.0 \cdot 10^{-4}$
IND 6	1,690	5	$3.0 \cdot 10^{-3}$
IND 7	2,986	4	$1.3 \cdot 10^{-3}$

Additional results of coexistence measurements for other DUTs are shown in Fig. 25. The following parameters were selected only for the measurements in the lab environment presented in this subsection:

- Bluetooth packet type DM3 with 120 bytes payload size.
- NanoNET transmission power 6.90 dBm. ARQ and FEC turned off.

- Narrowband FSK bit rate 72 kbps.

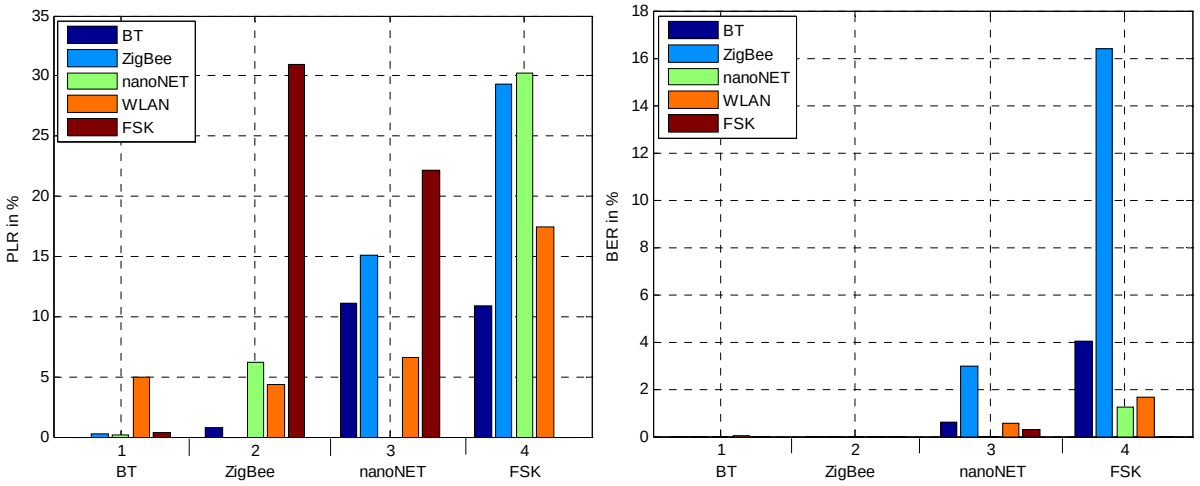


Figure 25: a) PLR without optimization for tested systems in the presence of selected interferers **b)** BER without optimization for tested systems in the presence of selected interferers (legend shows interferers)

Results of Fig. 25 (Coexistence without optimization):

- **Bluetooth:** The maximum PLR is in the order of 5.0 % when two WLAN systems are used for interference. For all other interferers the PLR remains less than 0.4 %. The BER for the Bluetooth system is in the order 1e-5 when two WLAN interfering systems are used. Otherwise it remains zero.
- **ZigBee:** The PLR is 0.74 % for Bluetooth interference, 6.24 % for nanoNET interference, 4.4 % for WLAN interference, and 30.9 % for narrowband FSK interference. The BER remains zero for all interferers.
- **NanoNET:** The PLR is 11.1 % with Bluetooth interference, 15.1 % with ZigBee interference, 6.61 % with WLAN interference, and 22.2 % with narrowband FSK interference. The BER remains in the order of 1e-3 except for ZigBee interference. In the presence of ZigBee interference the BER is almost 3 %.
- **Narrowband FSK:** The PLR is 10.9 % for Bluetooth, 29.3 % for ZigBee, 30.3 % for nanoNET, and 17.5 % for WLAN interference. The maximum value of BER is in the order of 16 % with ZigBee interference, for all other interferers it remains in the order of 1...4 %.

In order to improve the results of Fig. x, optimization was done by changing either some parameters of the DUT itself (whenever possible) or of the interfering system. For example in case of ZigBee only the parameters of the coexisting systems were changed while in case of Bluetooth the packet types of the DUT were also changed along with some parameters of the interfering systems. The following parameters were selected for the measurements presented in this subsection:

- Bluetooth packet type DM1 with 10 bytes payload size.
- NanoNET transmission power –16 dBm. ARQ and FEC turned on.
- Narrowband FSK bit rate 500kbps.

The optimized coexistence results are shown in Fig. 26.

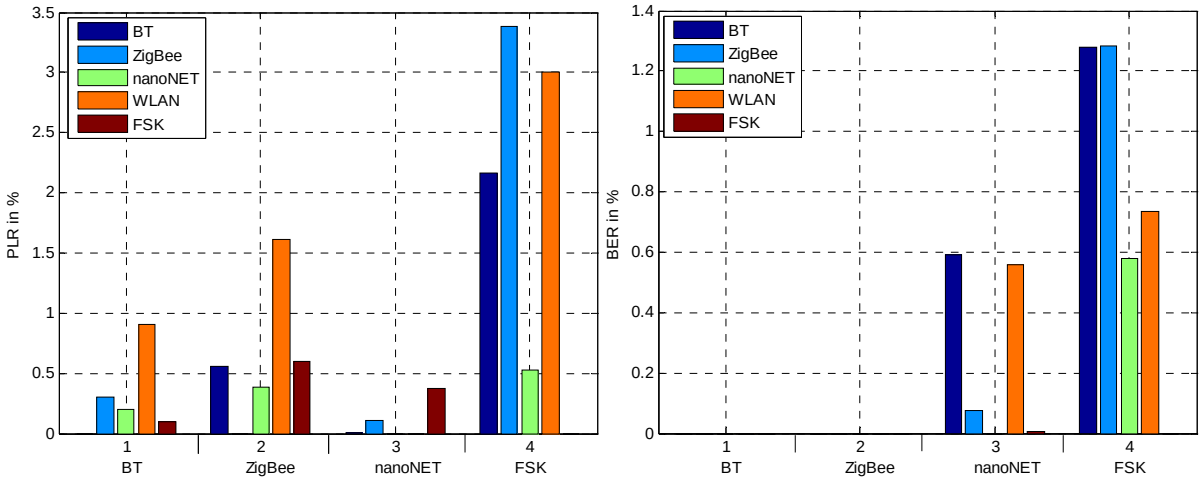


Figure 26: a) Optimized PLR for tested systems in the presence of selected interferers **b)** Optimized BER for tested systems in the presence of selected interferers (legend shows interferers)

Results of Fig. 26 (Coexistence with optimization):

- **Bluetooth:** The PLR is between 0.1 % … 0.3 % for all interferers except WLAN. The maximum PLR value of 0.91 % is observed when WLAN is used as an interferer. The BER remains zero with all interferers.
- **ZigBee:** The BER remains zero in all coexisting environments while the maximum value of PLR was 1.6 % for WLAN interference. The PLR remains between 0.3 % … 0.6 % for all other interferers.
- **NanoNET:** The PLR remains less than 0.4 % for all coexisting systems. The BER is in the order 1e–4 … 1e–5 for narrowband FSK and ZigBee systems and almost 0.6 % for Bluetooth and WLAN coexisting systems.
- **Narrowband FSK:** The PLR is 0.5 % for nanoNET interference and between 2 % … 3.5 % for all other coexistence environments. The BER remains in the order 0.6 % ... 1.3 % with different interfering systems.

On the basis of these results the following conclusions can be drawn:

- A low bit rate increases the collision probability and degrades the coexistance behavior.
- The nanoNET system is a very convenient interferer because of its very low power transmission. Except from the FSK system all other systems exhibit very good results in the presence of a nanoNET interferer. This holds even when the nanoNET system transmits with its maximal power level of 6.90 dBm.
- WLAN is the worst interferer for the FHSS based Bluetooth system as it offers 0 dB SIR and covers 20 MHz of the frequency band. I.e. 20 Bluetooth channels will be skipped by the adaptive frequency hopping algorithm. Though nanoNET effects even 64 Bluetooth channels, there is less interference due to the high SIR value of 36 dB.
- The Bluetooth system is an excellent DUT choice in coexistence environments.

6.6 Security of Industrial Wireless Applications

Principal decisions concerning the usage of security features and/or enhancements have to be made in the initial planning phase of an industrial wireless application, in order to choose solutions from a suitable set of protocols, technologies and products that support the identified security aims.

As such decisions may have far-reaching consequences for the complete lifecycle of an application, a detailed threat analysis has to be conducted. In the course of such an analysis, the following categories of threats have to be considered:

- loss of confidentiality,
- loss of integrity/authenticity and
- denial of service (DoS).

It should be noted, that in many office applications confidentiality and integrity/authenticity are considered more important than protection against DoS. At least DoS for some moderate time intervals may be tolerable for such applications. To the contrary, in industrial applications the situation is totally different. While data confidentiality might be unimportant (e.g. for sensor data), service availability in real time might be of prime concern in process control or automation applications.

A well-defined closed network that is not accessible by non-authorized personnel, might be operated without risk, even if no specific security mechanisms are deployed. On the other hand, in a wireless environment no physical controls over the boundaries of transmissions exist. As a result, data may be captured far beyond the physical location that the wireless network was intended to serve, in particular if high-gain antennas are used.
Furthermore, DoS attacks at the lowest protocol layers have to be considered as realistic threads. Either jamming the medium or intentionally violating media access control mechanisms may substantially degrade or even block the channel.

Eavesdropping on wireless IEEE 802.11a/b/g networks is easily possible with freely available software tools running on standard notebooks under the Linux OS. Eavesdropping on a Bluetooth piconet is not that simple. In fact, it is often claimed, that FHSS provides some protection from eavesdropping and malicious access. In order to quantify this claim, a detailed investigation on the effort to eavesdrop a Bluetooth connection was carried out.

To eavesdrop on a Bluetooth connection, special purpose protocol analyzers can be used. However, to synchronize with a Bluetooth communication, the information necessary to derive the frequency hopping sequence (FHS) must be known. This information is taken from the piconet master's 24-bit lower address part (LAP), 4-bit from the upper address part (UAP) and the master's clock value. This information is contained in so called FHS packets that are exchanged in inquiry or paging procedures (see Fig. 27). For security reasons it is therefore recommended to turn discoverable mode off (disabling inquiry scans). But, the information necessary for the FHS determination can also be derived from listening to one fixed physical RF channel of an ongoing Bluetooth communication for a short time interval only. Actually each single packet contains the LAP and from the distribution of the time slots used for the

fixed physical RF channel, the master's clock value and the remaining 4-bit from the UAP can be deduced. A practical realization of this synchronization method could be implemented on the basis of a freely available SDR (software defined radio) solution running on appropriate hardware (USRP (universal software radio peripheral) motherboard with RFX2400 daughterboard), that is available for less than 1000 $.

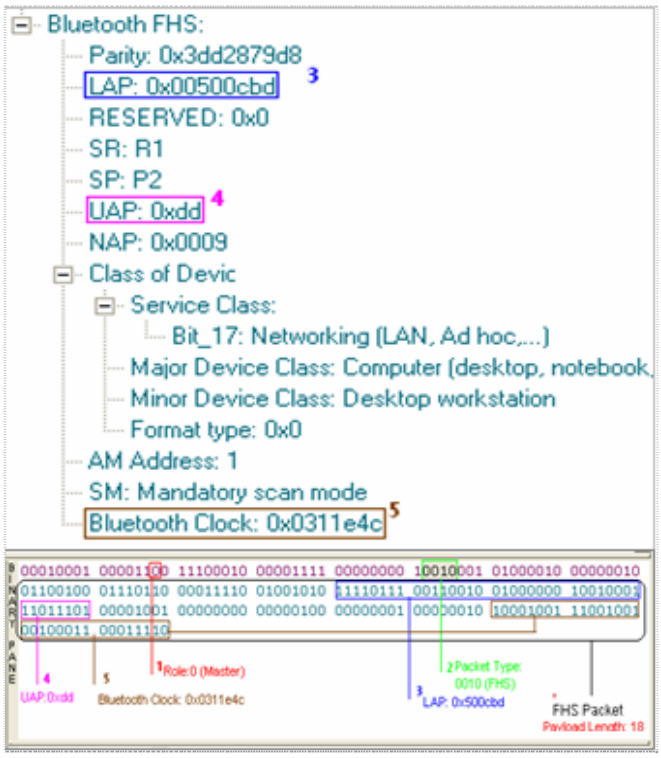


Figure 27: FHS Packet Sniffed by FTS4BT Bluetooth Protocol Analyzer & Packet Sniffer, Frontline Test System

While no general solution can be offered for protection against intentional DoS attacks on the PHY and MAC layers, data confidentiality can be provided by encryption and data integrity/authenticity by the calculation and verification of message authentication codes (MAC) or digital signatures. Furthermore, logical network access control can be enforced on the basis of authentication mechanisms.
All these measures require the usage of cryptographic keys. Hence, procedures for key distribution and configuration of wireless devices and network infrastructure components have to be considered, if such protective measures are identified to be necessary.
Most wireless technologies specify (optional) security mechanisms at the ISO/OSI layer 2. As all these different mechanisms offer multiple choices for their configuration and integration into some security infrastructure (e.g. RSN architecture in 802.11i), a thorough application specific analysis is necessary in order to find an appropriate solution. It might even be the case, that the usage of some security protocol at a higher protocol layer, like IPsec or TLS, provides a better solution for a particular application.

6.7 Guidelines for Optimal System Performance

The following parameters are found essential for the performance of radio systems working in coexistence environments.

1. *Frequency:* If possible, the operating frequency of the DUT system should be selected with respect to existing frequency allocations. As for example most WLAN systems choose the channels 1 (center 2412 MHz), 6 (center 2437 MHz) or 11 (center 2462 MHz), ZigBee systems should use the channels 15 (center 2425 MHz), 20 (center 2450 MHz), 25 (center 2475 MHz), or 26 (center 2480 MHz) and narrowband FSK systems should use the channels 25 ... 29 (2422.6 … 2426.92 MHz), 54 … 58 (2447.65 … 2451.97 MHz), or 83 … 94 (2472.71 … 2482 MHz) as shown in Fig. 28.

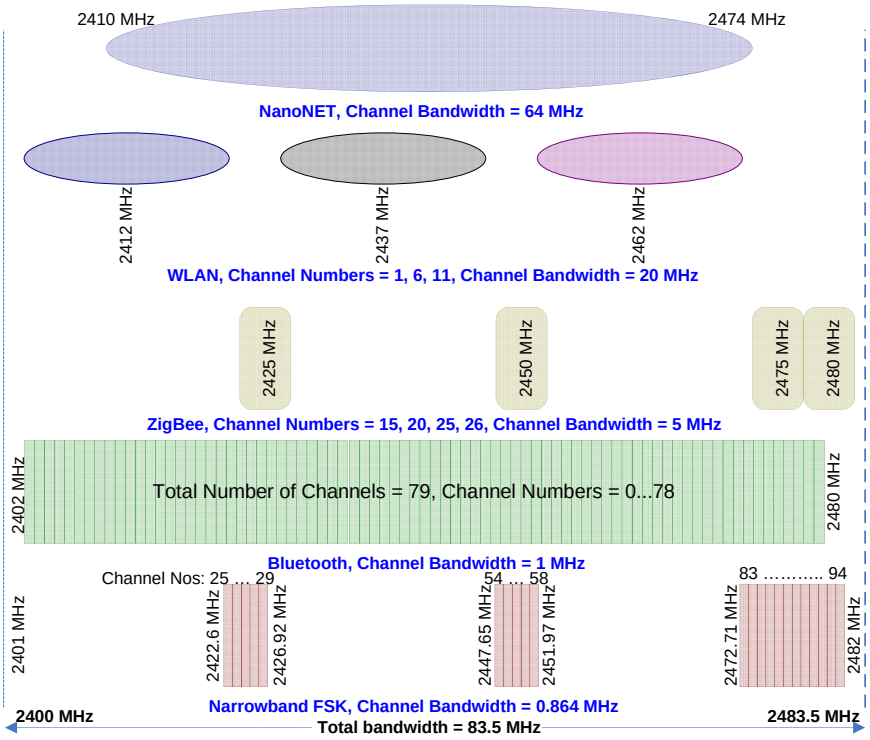


Figure 28: Recommended channels

2. *Cycle time:* It is defined as the time interval between successive packet transmissions of the master for cyclic data exchange. A careful selection of the cycle time can help to minimize packet collisions of coexisting systems. NanoNET and narrowband FSK were tested in the presence of each other with several cycle times for both systems. The PLR can be up to 8 % for the FSK system and up to 22 % for the nanoNET system when both of these were using different cycle times of 30 ms and 50 ms, respectively. While the PLR for both systems was less than 0.5 % when using the same cycle time of 50 ms and synchronizing the systems properly. This synchronization was achieved experimentally. But future systems should use appropriate synchronization methods.

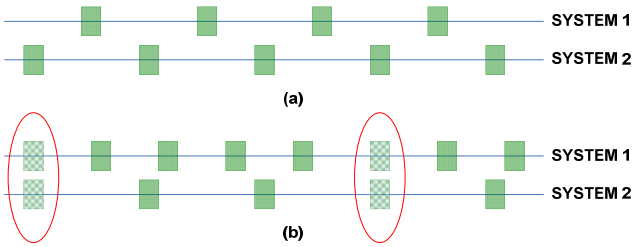


Figure 29: Adjusting cycle time to minimize collisions. a) Synchronized systems, b) non-synchronized systems

3. *Transmission power and SIR:* The transmission power of the devices is another important factor to determine the transmission quality. Higher transmission power usually ensures better transmission for a standalone radio system as the SIR should be as high as possible. But it should be selected carefully in a coexistence environment as it reduces the SIR of the coexisting systems. When the nanoNET interferer was set to a power level of –16 dBm, a PLR of less than 0.5 % was observed for all radio systems. But the PLR for narrowband FSK and ZigBee were increased to more than 6 % when the nanoNET interferer transmitted with its maximum power level of 6.90 dBm.

4. *Retransmission mechanism (ARQ):* The maximum number of retransmissions can be configured with respect to the desired application as it effects the transmission performance in two different ways. A high number improves the performance in terms of BER and PLR but impairs the real-time behavior with increased delay and jitter. As packet delay and jitter might be critical parameters for industrial systems, a compromise needs to be achieved between packet delay and PLR. In any case, the number of allowed retransmissions should be limited. The nanoNET and the Bluetooth systems use ARQ with maximal 5 retransmissions and achieve a PLR in the range 0 % … 1.6 %. Whereas without using ARQ the nanoNET system shows a PLR in the order of 6 % … 22 % for different coexisting systems.

5. *Forward error correction (FEC):* It can decrease BER and PLR for good channels but unfortunately increase these parameters when dealing with insufficient channel quality. The Bluetooth and the nanoNET systems use these error correction mechanisms. The BER was zero for the Bluetooth system and in the order 1e–4 … 1e–3 for the nanoNET system. On the other hand the BER was always in the order 1e–3 or worse for the narrowband FSK system which didn't use any error correction mechanism. The jitter of the nanoNET system was almost 8.35 ms when using FEC, and only 1.35 ms without FEC, respectively.

6. *Bitrate:* The higher the bitrate the smaller is the symbol duration and vice versa. Using low bitrates means transmitting with long symbol durations and hence high collision probability between coexisting systems. The narrowband FSK system was tested with bitrates of 500 kbps and 72 kbps. An FSK system with 72 kbps bitrate suffers from very high interference and the PLR with different interfering systems was between 20 % and 32 %. On the other hand the PLR of the FSK system in the presence of interferers could be reduced to only 0.1 % … 3.5 % when transmitting with 500 kbps bitrate. The bitrate also effects the jitter: 20.25 ms jitter was observed for the FSK system with 72 kbps and 62.26 ms with 500 kbps when it was working in the coexistence of the nanoNET system.

7. *Packet Size:* The Bluetooth system was investigated for different packet sizes and it revealed that the larger packet sizes imposed not only more interference to coexisting systems

but also degraded the performance of the system itself. Thus, small packet sizes reduce the collision probability and should be preferred in coexistence environments.

8. *Number of Interferers:* Increasing the number of interferers (homogeneous or heterogeneous) will increase the level of interference. The Bluetooth system was investigated in the presence of one and two WLAN systems, both operating in separate channels. The PLR was 0.91 % in the presence of one WLAN system, and 5.0 % PLR in the presence of two WLAN systems, respectively. The packet delay and jitter were also increased with the number of interferers. The packet delay was 5.4 ms for one interferer and 10.4 ms for two interferers, while the jitter was 30 ms for one WLAN interferer and 35 ms for two WLAN interferers.

9. *Bandwidth:* Systems using high bandwidth offer more interference to coexisting systems. It is important to use low transmission power if a system uses high bandwidth. The nanoNET and WLAN systems are two examples with 64 MHz and 20 MHz bandwidths, respectively. The nanoNET system was found to be the best system with respect to interfering other coexisting systems because it transmits with only –16 dBm while WLAN and Bluetooth are strong interfering systems, transmitting with 20 dBm transmission power.

10. *Antenna patterns:* Although not studied within the course of this investigation, we like to mention that directional antennas of the DUT systems can reduce interfering radiation. Unfortunately, fixed spatial pattern allocations require stationary applications. As wireless PAN systems are mainly used in portable or mobile sensor actuator networks, this item is not usable.

11. *The coexisting systems:* Each system is not suitable to coexist with each other system even after optimization. For example the nanoNET system was found to be very good in the coexistence of a WLAN system with 0 % PLR and worse in the presence of a narrowband FSK system with almost 0.4 % PLR. On the other hand the Bluetooth system works well in the presence of a narrowband FSK system with almost 0.1 % PLR and worse in the presence of a WLAN system with almost 0.9 % PLR.

Table 4 grades the results of different systems in different coexisting environments after optimization.

TABLE 4: Technology grading with respect to coexistence after optimization. x not measured, ++ very good, + good, o medium, - bad, -- very poor

	Bluetooth	**ZigBee**	**nanoNET**	**FSK**
Bluetooth	x	o	+	--
WLAN	+	+	+	--
ZigBee	++	x	++	--
nanoNET	++	+	x	o
FSK	++	+	+	x

Investigated technology = ■ *Technology used as interferer =* ■

6.8 Recommendations for Standards and User Organizations

The available industrial wireless systems are able to meet their intended application requirements. To further increase the market acceptance of prospective users it is important to establish *standardized measurement guidelines*. This measurements should primarily focus on coexistence assessments.
During the course of this project several discussions with prospective users and system producers had been carried out. All agreed, that these today missing standardized measurement guidelines are really needed. They will enable and provide further important quantitative features of wireless systems in order to improve the process of *frequency management* in companies.
It is further desirable that all wireless products should be certified according to the proposed measurement standard. The adaption of wireless systems will be placed on a reliable ground and as a consequence, further wireless applications might arise.
As an appropriate way to establish these measurement guidelines, working groups like GMA working group 5.21 "Radio based communication in industrial automation" or ZVEI working group "Wireless in Automation" shall be involved.
The institute Industrial IT will further contribute to the development of *standard measurement guidelines*.

6.9 Conclusions

Available wireless automation systems are reliable supplements - but no substitutes - for wire based fieldbus systems.
In general we can conclude, that packet loss rates PLR < 1e–5 can be achieved with respect to passive environmental effects like multipath or channel movements. However, it is necessary, that line-of-sight communication is possible. Maximal distances of 10...30 m are possible, depending on the maximal allowed path loss.
As a rule of thumb we suggest, that the theoretical path loss limit of transmitter power over receiver sensitivity shall be at least 30 dB above the intended operational path loss.
In order to achieve these results, several technological items need to be carefully selected and utilized: frequency hopping, diversity schemes, channel coding, packetizing, modulation, symbol rate selection, antenna design. E.g. wireless automation systems based on Bluetooth technology are extremely reliable due to their inherent system features like adaptive frequency hopping at high operating frequencies, error detection and correction.
A crucial parameter is the coexistence behavior of any wireless system. We were able to show, that interference from other wireless systems is the most important source of system degradation. We suggest system guidelines to improve and optimize the coexistence behavior. Anyway, it remains the main source of impairment and needs to be investigated very carefully.
As existing wireless systems lack information about their coexistence behavior, we suggest the development of *standardized measurement guidelines*. They will provide important quantitative features of wireless systems in order to improve the process of *frequency management* in manufacturing companies. All wireless products should be certified according to the proposed new measurement standard.

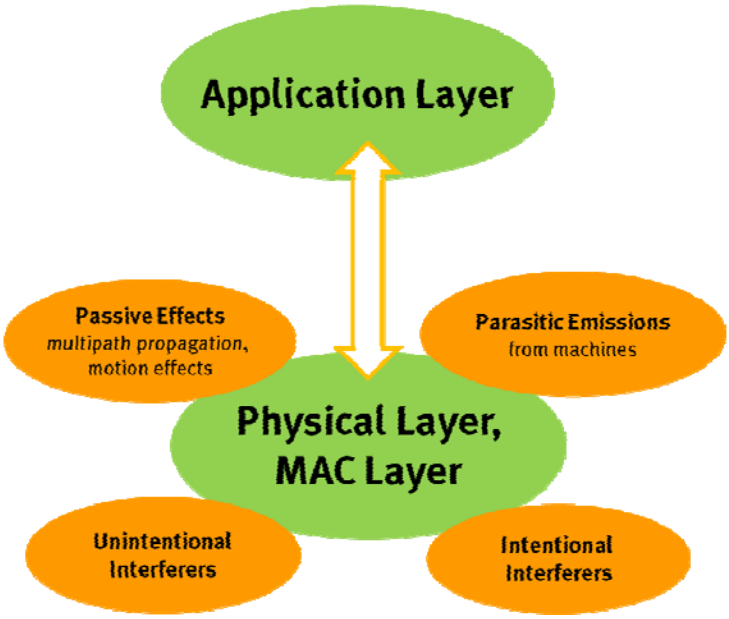


Figure 30: Although wireless applications might be impaired by several environmental effects, a careful design can avoid these effects with respect to the application layer

This study reports the possibilities and limitations of state-of-the-art and widely used existing technologies. As a conclusion, it recommends further necessary research: Only collaborative systems should be used in future high density coexistence environments. Technological enhancements like ultra-wide-band systems (UWB) and multiple-input-multiple-output features (MIMO) will further improve the performance of next generation wireless PAN systems.
As Fig. 30 illustrates, in an optimized system all environmental effects attack the physical and MAC layer only and will eventually be invisible to the application layer. As far as security aims are concerned, this goal can be achieved with already established cryptographic algorithms and protocols. Nevertheless, the optimal choice of adequate security measures including the design of a sound security infrastructure will always be a challenging task, depending on a detailed thread analysis.

7 Usage of Results

All relevant results have been published on conferences and in regular journals. This *final report* and the *users' guide* will be further published via the homepage of the institute Industrial IT (www.init-owl.de). The URL of the SUDIWI project is: http://www.hs-owl.de/init/research/projects/b/filteroff/14/single.html
Any questions addressed to the authors of this report are very much appreciated and will be answered immediately.

8 Technical Progress During Project Duration

Several other working groups in universities and companies worked also on the investigation of industrial wireless systems. If possible and available published results were included in this project.
An important ZVEI initiated and funded project (05/2006 - 11/2006) was carried out at the institute IFAK e.V. (www.ifak-md.de) in Magdeburg: *Durchführung von Tests zur Bewertung der Koexistenz verschiedener Funksysteme im industriellen Umfeld (KoTest)*. Measurements of different industrial systems in a coexistence environment in the *experimentelle Fabrik Magdeburg* and an anechoic measurement chamber were carried out.
The results of this project were carefully studied and provided a valuable contribution to the SUDIWI project. In addition to only one industrial environment in the KoTest project we investigated several industrial environments in the SUDIWI project. Furthermore, the development and usage of a cable based test site proved to be extremely valuable for coexistence investigations.
Worth mentioning are also the working groups GMA 5.21 "Radio based communication in industrial automation" and ZVEI "Wireless in Automation". The SUDIWI working group discussed essential items with these working groups [U. Meier: Messverfahren zur Verbesserung des Interferenz- und Koexistenzverhaltens von Funksystemen, ZVEI - Wireless in der Automation, Arbeitskreis Koexistenz, Frankfurt, November 2007].

9 Publication of Results

9.1 Conferences and Journals

- M. Höing, K. Helmig, U. Meier: *Untersuchungen zur Störfestigkeit und Übertragungssicherheit der Bluetooth-Technologie am Beispiel eines industriellen Sensor-Aktor-Systems*; 8. Wireless Kongress, 27. - 28. September 2006, Dortmund
- U. Meier: *Störfestigkeit und Übertragungssicherheit industrieller Wireless-Technologien*, CONNECTIVITY 2006 Innovation for Power, Data and Signal Connectivity, Detmold, Sept. 2006
- M. Höing, K. Helmig, U. Meier: *Erprobungstests von drahtlosen Sensor-Aktor-Systemen in rauen Industrieumgebungen*; SPS/IPC/DRIVES, 28. - 30. November 2006, Nürnberg
- K. Helmig, U. Meier, M. Höing: *Völlig ungestört - Untersuchungen zur Störfestigkeit und Übertragungssicherheit der Bluetooth-Technologie*; MessTec & Automation, 11/2006, 64 - 65
- M. Höing, K. Helmig, U. Meier: *Bluetooth ungestört - Erprobungstests der Bluetooth-Technologie am Beispiel eines industriellen Sensor-Aktor-Systems*; Wireless Automation 2007, 28.02. - 01.03.2007, Magdeburg
- U. Meier, S. Witte, K. Helmig, M. Höing, M. Schnückel, H. Krause: *Performance Evaluation and Prediction of a Bluetooth Based Real-Time Sensor Actuator System in Harsh Industrial Environments*; 12th IEEE Conference on Emerging Technologies and Factory Automation, Patras, Greece, Sep 2007

- K. Helmig, J. S. Michels, U. Meier: *Untersuchung der funktionalen Sicherheit eines Bluetooth-basierten Sensor-Aktor-Systems unter Echtzeitbedingungen*; SPS/IPC/DRIVES, 27. - 29. November 2007, Nürnberg
- M. Höing, K. Helmig, U. Meier: *Funken mit Bluetooth - Untersuchungen zur Störfestigkeit und Übertragungssicherheit der Bluetooth-Technologie am Beispiel eines Weidmüller SAI-Moduls*; Automatisierungstechnische Praxis, atp 49, 8/2007, 15 – 16
- U. Meier: *Messverfahren zur Verbesserung des Interferenz- und Koexistenzverhaltens von Funksystemen*, ZVEI - Wireless in der Automation, Arbeitskreis Koexistenz, Frankfurt, November 2007
- Tabassam, Ahmad Ali; Heiss, Stefan: Bluetooth Device Discovery and Hop Synchronization by the Eavesdropper . in: 3rd IEEE International Conference on Emerging Technology (ICET07) Islamabad, Pakistan, Nov 2007
- K. Ahmad, U. Meier: *Performance Investigation and Optimization of Chirp Spread Spectrum Systems for Wireless Sensor Actuator Networks*; Third International IEEE Conference on Wireless Communications and Sensor Networks Allahabad, India, Dec 2007
- M. Höing, K. Ahmad, U. Meier: *Koexistenzmessungen – von der Theorie zu Standardisierungsbetrachtungen, dargestellt anhand von Messungen an einem industriellen Bluetooth-System*; Wireless Automation 2008 Berlin, Germany, Feb 2008
- U. Meier: *Wireless for Mobile and Flexible Manufacturing*; Hanover Fair, April 2008, Wireless Automation, Speaker's Corner, keynote speech
- Tabassam, Ahmad Ali; Heiss, Stefan: Bluetooth Clock Recovery and Hop Sequence Synchronization Using Software Defined Radios . in: Proc. of 2008 IEEE Region 5 PBASICS2 Conf Kansas KS, USA, Apr 2008
- K. Ahmad, U. Meier: *Coexistence Optimization of Wireless PAN Automation Systems*; 7th IEEE International Workshop on Factory Communication Systems (WFCS 2008), Dresden, Germany, May 2008

9.2 Final Thesis of Students

- Ajay Bhardwaj: *Investigation of Wireless Channel Models for Industrial Applications*, Master, 2006
- Muhammad Rizwan Mustafa: *Transmission Modelling and Performance Prediction for an Industrial Wireless Application*, Master, 2006
- Manuel Bastert: *Entwicklung und Erprobung einer Testbox zur Vermessung von WLAN-Systemen*, Diplom, 2006
- Benjamin Pape: *Entwicklung eines Messplatzes für Emissionsmessungen*, Diplom, 2007
- Min Jing Nigel Goh, Curtis Cretton: *Measurement Set-Up for Three Dimensional Radiation Patterns*, Industrial Placement, 2007
- Kaleem Ahmad: *Performance Investigation of Chirp Spread Spectrum Systems for Industrial Applications*, Master, 2007

- Sureshkumar Ponnampalam: *Development and Performance Investigation of a Measurement Set-Up for Spread Spectrum Data Transmission*, Master, 2007
- Ehsan Ullah Warriach: *Performance Investigation of different Bluetooth modules and Communication Modes*, Master, 2007
- Fabian Taubitz: *Validation of Bluetooth synchronous communication in respect of industrial environments*, Master, 2007
- Ahmed Mahmoud Khalil: *Measurements tool for Bluetooth-based Sensor-Actor-Interface (SAI) modules*, Bachelor, 2007
- Ahmad Ali Tabassam: Bluetooth Security in Industrial Applications, Master, 2007

10 Abbreviations

AC	*Anechoic Shielded Chamber*
ARQ	*Automatic Repeat Request*
BER	*Bit Error Rate*
DUT	*Device Under Test*
FEC	*Forward Error Correction*
FSK	*Frequency Shift Keying*
LOS	*Line Of Sight*
NLOS	*Non Line Of Sight*
OLOS	*Obstructed Line Of Sight*
PAN	*Personal Area Network*
PLR	*Packet Loss Rate*
SAI	*Sensor Actuator Interface*
SIR	*Signal-to-Interference Ratio*
WLAN	*Wireless Local Area Network*

Appendix: Users' Guide