



# Risk Analysis

## Report

### ATJ-kehitysohjelma

### ”Ajoneuvon / työkoneen langattomat lähiverkot (ALMA)”

**AUTHORS** Pauli Mikkonen, CWC  
Matti Kettunen, CWC  
Jukka Kämäräinen, VTT  
Niko Niskala, VTT

Version	Date	Author	Status	Notes
0.1	1.7.2009	PM		Document created
0.5	21.8.2009	PM, MK	Draft	Sent to JI
1.0	4.9.2009	PM, MK, JK, NN	Proposal	
1.1	21.12.2009	JI	Draft	Edits
2.0	21.12.2009	JI	Accepted	

## Table of Contents

1	Abbreviations .....	3
2	Introduction .....	6
3	Risk analysis.....	7
3.1	Types of risks.....	7
3.2	Transmission failures.....	8
3.3	Requirements for reliable wireless control bus .....	9
3.4	Candidates for wireless control .....	10
3.4.1	WLAN IEEE 802.11p.....	10
3.4.2	Bluetooth IEEE 802.15.1-2005 .....	14
3.4.3	Low rate WPAN IEEE 802.15.4-2006 .....	17
3.4.4	Low rate WPAN IEEE 802.15.4a-2007 .....	19
3.4.5	High rate WPAN IEEE 802.15.3-2003 .....	23
3.4.6	High rate UWB, ECMA-368 .....	26
3.5	Comparison of candidate standards against basic threats .....	28
3.6	Possible solutions for communication between machines .....	30
3.6.1	WiMAX IEEE 802.16-2009 .....	30
3.6.2	IEEE 802.20-2008 .....	36
3.6.3	Non-Standard radio system .....	37
3.7	Possible solution for very short range communication .....	39
3.7.1	Modulation.....	39
3.7.2	Coding .....	41
3.7.3	Data Security .....	41
3.7.4	Inductive power and data link risk analysis.....	41
3.7.5	Inductive coupled system advantages.....	43
3.7.6	Comparing key RFID parameters to other wireless standards .....	44
	Conclusions .....	46
	References .....	48

# 1 Abbreviations

ACK	acknowledgement
AM	Amplitude Modulation
ARQ	automatic repeat request
ASK	amplitude-shift keying
AWGN	all-white Gaussian noise
BER	bit error rate
BPSK	binary phase shift keying
BS	Base Stations
CCH	control channel
CEPT	European Conference of Postal and Telecommunication
CRC	cyclic redundancy check
CSMA/CA	carrier sense multiple access with carrier avoidance
CSS	Chirp Spread Spectrum
CSS	chirp-spread spectrum
DQPSK	differential quadrature phase-shift keying
DSRC	dedicated Short Range Communications
DSSS	direct sequence spread spectrum
ECMA	European Computer Manufacturer's Association
EDR	enhanced data rate
EIRP	equivalent isotropically radiated power
EM	Electro Magnetic
ERP	effective radiated power
FDD	Frequency Division Duplex
FEC	forward error correction
FHSS	frequency hopping spread spectrum
FM	Frequency Modulation
GFSK	Gaussian frequency-shift keying
GTS	guaranteed time slot
HARQ	Hybrid automatic repeat request
HCS	header check sequence
HEC	header error check
HS	high speed
I2V	infrastructure-To-Vehicle

ISM	industrial, scientific and medical (band)
ITS	intelligent transport system
L2CAP	logical link control and adaptation protocol
LLC	Logical Link Control
MAC	medium access (layer)
MB-OFDM	multiband orthogonal frequency division multiplexing
MBWA	Mobile Broadband Wireless Access
MIMO	multiple in, multiple out
MSS	Mobile Subscriber Stations
NFC	Near Field Communication
NLOS	Non-line-of sight operation
NRZ	Never Return to Zero
OFDM	orthogonal frequency division multiplexing
O-QPSK	offset quadrature phase-shift keying
PAN	personal area network
PER	packet error rate
PHY	physical (layer)
PIN	personal identification number
PM	Phase Modulation
PMP	Point-to-Multipoint
PSDU	physical layer service data unit
PSK	phase-shift keying
QAM	quadrature amplitude modulation
QoS	quality of service
QPSK	Quadrature Phase Shift Keying
RFID	Radio Frequency Identification
RSSI	received signal strength indication
SIG	special interest group
SNR	signal-to-noise ratio
TCM	trellis code modulation
TDD	time-division duplex
UWB	ultra-wide band
V2V	vehicle-to-vehicle
WLAN	Wireless Local Area Network
WPAN	wireless personal area network

16QAM	(4x4 Amplitude, Phase) Quadrature Amplitude Modulation
64QAM	(8x8 Amplitude, Phase) Quadrature Amplitude Modulation
8PSK	Eight Phase Shift Keying

## 2 Introduction

Currently there are no wireless standards for a general control bus in working machines. All the same security and reliability aspects apply to wireless solutions as to wired solutions. Additionally bit error probability is higher, a wireless bus is easier to hack from the outside by an intruder, and other radio sources which utilize the same frequency band interfere with it. In worst case, the connection can even totally be lost for while, which is unlikely to happen with wired solutions. In that case it would require physical damage in the data transfer medium to cause it. Reliability issues with wireless technologies have to be thoroughly considered.

This report is a preliminary review of potentially suitable wireless standards. Three use cases are described. The first one is for reliable, low delay wireless link between cabin and harvester head, or similar in working machine. The reliability of the wireless technology should be comparable to present wired control bus solutions. The second is for a longer range data transmission link between working machines with less strict reliability requirements. The third is the power and data link in a ball-end controller.

### 3 Risk analysis

#### 3.1 Types of risks

A wireless system is characterised by being physically disconnected and depending on radio communication between different parts of the system. In Table 1, the basic threats and their consequences in wireless systems are presented. [1] The possible candidate standards for reliable control bus are compared against these threats in chapter 3.5.

Table 1 Basic threats and consequences in wireless system

Basic threats	Consequences
The transmission fades because the distance between transmitter and receiver increases.	Signal level is low. Bit error rate increases. Data is corrupted or lost.
The signal fades because of obstacles.	Signal level is low. Bit error rate increases. Data is corrupted or lost.
Transmission signal fades because of environment conditions	Signal level is low. Bit error rate increases. Data is corrupted or lost.
Transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances.	Signal level is low. Bit error rate increases. Data is corrupted or lost. Inserted new messages.
Two or more signals interfere with each other and cause proper signal for another receiver.	Bit error rate is high and therefore an acceptable transient signal can be initiated.
Receiver is too sensitive.	Signal is generated out from noise. Short message can appear. A Receiver is easy to desensitize. Link budget is more important.
Poor capability of a relaying station.	The signal can be delayed e.g. due to heavy traffic or extra signal processing in relaying stations.
The nodes understand the network state or configuration differently at the same time.	Consistency and stability problems especially when nodes are moving. Radio B can hear radios C and A, but radio A cannot hear radio C. This may cause confusion.
Nearby wireless network is using similar communication protocol.	One node is substituted intentionally or unintentionally with another node.
Security; intentional penetration to wireless network.	New messages may be inserted.
Systematic failure, characteristics of wireless communication is not considered.	Almost any of the above mentioned consequences may result.
Sleeping nodes in low power networks. Some nodes can be ordered to sleep to lower power consumption i.e. longer battery life.	There is no communication through a sleeping node until the node awakes.

Message correctness is considered as very important in with respect to safety. It includes integrity, authenticity, timelines and sequencing. [1]

### 3.2 Transmission failures

Basic threats in wireless system can be realized as transmission failures. The failures can be divided in seven sections [1]. They are presented in Table 2. The failures can be fought by correct selection of wireless system and protective mechanisms e.g. utilizing security and encryption, error correction, and redundant transmission path.

Table 2 Transmission failures with explanations

Repetition	Same message is sent repeatedly
Deletion	Message cannot be received or is corrupted
Insertion	Message is received unintentionally, maybe interpreted to have correct address
Incorrect sequence	Messages are received in incorrect order
Message corruption	Message is changed in the transmission path
Delay	Data is received too late because of interference or overloaded media
Erroneous addressing	Message is not what it pretends to be because of misrouting or message is malicious

### 3.3 Requirements for reliable wireless control bus

A reliable wireless communication link is capable of detecting errors in received packets and request retransmission until the errors are removed. In real-time control systems there is requirement for low delay. Interference may have great impact on it. Delay must stay within low predetermined bounds. Because wireless link is more easily accessible security issues have to be carefully scrutinized.

Relevant issues that could be conducted from standards:

- modulation
- bandwidth (transmission rate)
- frequencies (frequency band, global use)
- interference (harmonics/adjacent channels), jamming and coexistence
- receiver sensitivity, transmitter power level and control, SNR
- redundancy, MIMO, retransmission
- channel coding, error correction
- real-time demand, delays
- security, safety against hacking
- expandability (number of nodes, bandwidth sufficiency)

Chip and design dependent:

- temperature area
- power feed and backup
- battery life (temperature, recharge/change interval, power consumption)
- availability
- Prize comparable to current wired solution

### 3.4 Candidates for wireless control

#### 3.4.1 WLAN IEEE 802.11p

*This is an excerpt of the document “Risk Analysis – 802.11p” by H. Viittala. [2]*

Vehicular safety communication requires real-time communication with high reliability imposing a set of new requirements on wireless communication systems. To meet real-time requirement, channel access should be timely and predictable. [3] High-speed vehicles on a complex road environment present challenges at the physical (PHY) layer level. Distances up to 1000 m are supported.

The dedicated short range communications (DSRC) spectrum of 75 MHz at 5.9 GHz has been allocated to be used exclusively for V2V and infrastructure-to-vehicle (I2V) communications by the Federal Communication Commission in the USA. The DSRC band is free but licensed spectrum. The DSRC spectrum is divided in seven 10 MHz wide channels. The channel number 178 is control channel (CCH) and it is reserved for safety communications only. Channels 172 and 184 are designed for public safety applications. The channel use is summarized in Table 3. [4] [5]

Table 3 . Channel use in the DSRC spectrum in the USA

<b>Channel No.</b>	<b>Freq. Range [MHz]</b>	<b>Max. EIRP<sup>1</sup> [dBm]</b>	<b>Channel Use</b>
170	5850-5855	-	Reserved
172	5855-5865	33	Service Channel
174	5865-5875	33	Service Channel
175	5865-5885	23	Service Channel
176	5875-5885	33	Service Channel
178	5885-5895	33/44.8	Control Channel
180	5895-5905	23	Service Channel
181	5895-5915	23	Service Channel
182	5905-5915	23	Service Channel
184	5915-5925	33/40	Service Channel

<sup>1</sup>EIRP = Effective Isotropic Radiated Power

The frequency spectrum within the band of 5.875 – 5.925 GHz has been designated for intelligent transport systems (ITS) by European Conference of Postal and Telecommunication (CEPT) in Europe. The maximum EIRP for an ITS station is limited to 23 dBm/MHz. The frequency sub-band 5.875 – 5.905 GHz has been allocated for a non-exclusive basis for ITS road safety applications. [6] The DSRC channel use in the USA and Europe are presented in Figure 1.

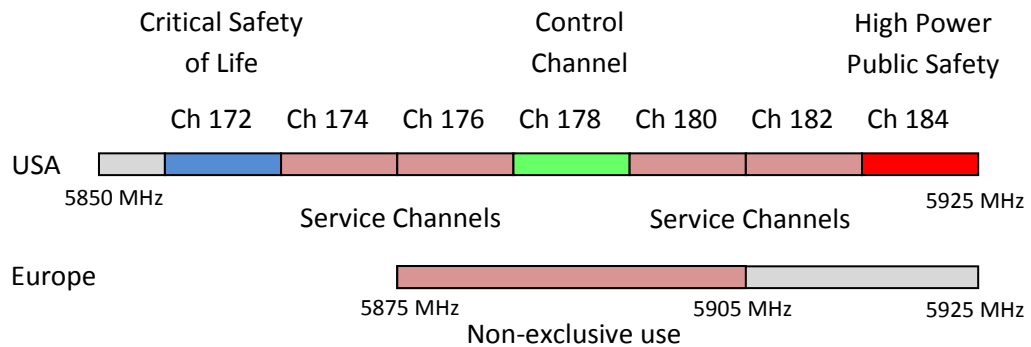



Figure 1 Spectrum allocation in the USA and Europe.

The OFDM PHY of the IEEE 802.11 standard provides communications with data rates of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps having the 20 MHz channel spacing in the 5 GHz ISM band. The support of data rates of 6, 12 and 24 Mbps are mandatory. 802.11 OFDM PHY parameters are described in the Table 4.

Table 4 802.11 OFDM PHY parameters

Mode	Data Rate [Mbps] (20 MHz Channel Spacing)	Data Rate [Mbps] (10 MHz Channel Spacing)	Modulation	Convolutional Coding Rate	Minimum Receiver Sensitivity [dBm]	Adjacent Channel Rejection [dB]	Alternate Channel Rejection [dB]
1	6	3	BPSK	1/2	-82	16	32
2	9	4.5	BPSK	3/4	-81	15	31
3	12	6	QPSK	1/2	-79	13	29
4	18	9	QPSK	3/4	-77	11	27
5	24	12	16-QAM	1/2	-74	8	24
6	36	18	16-QAM	3/4	-70	4	20
7	48	24	64-QAM	2/3	-66	0	16
8	54	27	64-QAM	3/4	-65	-1	15

 = Mandatory

### *Summary of 802.11p*

The DSRC spectrum band at 5.9 GHz is reserved for ITS applications worldwide, e.g., the spectrum within 5.875 – 5.925 GHz and 5.850 – 5.925 GHz in Europe and the USA, respectively. The IEEE 802.11 task group p defines PHY and MAC enhancements to the 802.11 standard required to support ITS applications. The enhancement 802.11p will be based on the ASTM E 2213-03 document. Since 802.11 OFDM PHY is already operating near to the DSRC frequency band, it was justified to choose OFDM PHY as baseline. The 802.11p PHY applies the 10 MHz channel spacing and more stringent receiver requirements than original 802.11. The MAC layer is modified by minimizing the size of the needed overheads to accelerate the establishment time for communication.

Applicability of 802.11p for communications between working machines depends strongly on nature of data and requirements for QoS. 802.11 was originally designed for multimedia purposes where packet sizes are large, PER is in order of 1% and delay may be large and vary, whereas real-time applications require quite short packets, very short and constant delay and error-free transmission. In 802.11, EDCA and HCCA modes were introduced for QoS networks. Nowadays, only EDCA mode is implemented in chipsets. EDCA is contention-based channel access method and may not fulfill stringent real-time requirements. Even though MAC improvements of 802.11p the contention-based channel access may still be insufficient in terms of real-time communications.

802.11 has very strong power behind the scenes due to Wi-Fi Alliance. Since 802.11 is widely adapted across the world and it is expected that an almost one billion chipsets are shipped in 2011 alone [7], continuous development of 802.11 will be ensured. Still, there are not many or any chipsets of 802.11p available at present. Strengths and Weaknesses etc. of the standard 802.11p are described in the Table 5.

Table 5 SWOT analysis of 802.11p

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>• Licensed spectrum</li> <li>• Robust PHY</li> <li>• Strong security (WPA2)</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>• Modified MAC good enough for real-time applications?</li> <li>• QoS requirements of application</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>• Strong Wi-Fi Alliance</li> <li>• Global spectrum for ITS</li> <li>• Widely adapted 802.11 standards</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>• When 802.11p chipsets available?</li> </ul>

### 3.4.2 Bluetooth IEEE 802.15.1-2005

This standard is compatible with Bluetooth specification 1.2. Bluetooth is a low power low cost technology. In a typical topology a master and one slave device is connected. If there are several slave devices they form a Pico-net. Slave devices can associate with multiple masters too thus forming a Scatter-net. Master is in charge of synchronization.

GFSK is used for reducing spectral width per channel (79 channels, 1 MHz each). At the same time FHSS carriers are used for frequency hopping 1600 times per second making it to utilize larger band. As a consequence of its adaptive frequency hopping it spends less time in crowded channels and suffers less from interference. Frequency hopping transceiver also helps combat fading. Data is positioned in time slots and for full duplex transmissions time-division duplex (TDD) scheme is used. [8]

The 2400 – 2483.5 MHz licence free global Industrial, Scientific and Medical (ISM) band is used. Maximum data rate in theory is 1 Mbps. Bluetooth 1.2 is ratified as standard 802.15.1. For higher data rates Bluetooth Special Interest Group (SIG) has specification 2.1 and enhanced data rate (EDR) for 2 Mbps and 3 Mbps transmissions. Two PSK modulation variants are used,  $\pi/4$ -DQPSK and 8DPSK. [9] Specification 2.1 is backward compatible. Specification 3.0 and high speed (HS) main feature is alternate MAC/PHY, a 802.11 protocol adaptation layer. The specification has been published in April 2009.

Four physical channels are defined which of two are used for communication between connected devices (basic and adapted Pico-net channel). One channel is for discovering devices and one for connecting them. Both transmitter and receiver need to be tuned to the same RF at the same time i.e. they must be synchronized to timing, frequency, and also access code, of a physical channel. [8]

The interference performance on co-channel and adjacent 1 MHz and 2 MHz shall be measured with the wanted signal 10 dB over reference sensitivity level. For all the other RF channels wanted signal shall be 3 dB over the reference sensitivity level. The actual raw bit error rate (BER) of  $\leq 0,1$  % is presumed. Receiver sensitivity shall be below or equal to -70 dBm. Interference performance is listed in Table 6. [8]

Table 6 Signal-to-interference ratios of IEEE std 802.15.1

Frequency of interference	Ratio
Co-channel interference, $C/I_{\text{co-channel}}$	11dB
Adjacent (1 MHz) interference, $C/I_{1\text{MHz}}$	0dB
Adjacent (2 MHz) interference, $C/I_{2\text{MHz}}$	-30dB
Adjacent ( $\geq 3$ MHz) interference, $C/I_{\geq 3\text{MHz}}$	-40dB
Image frequency interference <sup>a, b</sup> , $C/I_{\text{Image}}$	-9dB
Adjacent (1 MHz) interference to in-band image frequency, $C/I_{\text{Image} \pm 1\text{MHz}}$	-20dB

Co-channel interference 11 dB describes the ratio between received modulated carrier power and average received co-channel interference power while BER is within limits. Adjacent channel interference can have the same power than received signal without increasing BER, and for further channels the ratio is very low.

Maximum range is about 100 m with highest power class.

Maximum transmit power for the 2000 – 2483.5 MHz band is 100 mW EIRP generally in Europe. For FHSS the maximum spectrum power density is limited to -0 dBW / 100 kHz and for DSSS the maximum spectrum power density is limited to -20 dBW / MHz. [10]

Power class 1 devices reaching 20 dBm (100 mW) shall implement power control. Power control at the level of 4 dBm or lower is optional. Devices check their received signal strength indication (RSSI) and report to peer if the power is above or below desired range. Power class 2 and 3 are limited to 4 dBm (2,5 mW) and 0 dBm (1 mW), respectively. [8]

Forward error correction (FEC), header error check (HEC) and automatic repeat request (ARQ) among other things are provided for better error-control. The reliability gained by ARQ is only dependable of the HEC and cyclic redundancy check (CRC) codes to detect errors. In the longer packet types the probability of an undetected error is too high to support typical applications especially those with a large amount of data being transferred. [8]

Error correction of 1/3 and 2/3 rate FEC are defined [8]. It describes the amount of information that is not redundant.

Connection-oriented Logical link control and adaptation protocol (L2CAP) channels may be created for transport of unicast (point-to-point) data between two devices. L2CAP in

Bluetooth stack provides an additional level of error control that is designed to detect the occasional undetected errors in the baseband protocol and request retransmission of the affected data. This provides the level of reliability required by typical IEEE 802.15.1-2005 applications. For L2CAP channels, the residual error level is comparable to other communication systems, although for logical links the residual error level is somewhat higher. [8]

Security with 128-bit authentication key and up to 128-bit encryption key is provided. Bluetooth is designed for wireless connectivity with fixed, portable, and moving devices within or entering personal operating space. Because of that design principle identical personal identification numbers (PIN) are used for finding out other devices address and pairing them. After users have entered correct PIN codes both devices will generate a link key which can be stored and used to skip future authentication process. For more reliability communication devices should be already authenticated and prevent outside devices to discover them. However, even by using encryption the address is sent unencrypted. If the pseudorandom frequency hopping sequence is analyzed from transmission by third party the addresses can be solved. Another way would be to try out all addresses until device of that specific address replies to the request. Device accepts a basic L2CAP connection request without acceptance of the user. [11]

Finding out frequency hopping sequence gives more efficient way to jam the transmissions by external interference signal. Finding out device address gives chance to flood the device with requests.

Up to 7 slaves can be in one Pico-net. All the devices follow the same frequency hopping and timing rules defined by the master. If device is participating in more than one Pico-net (Scatter-net) it still can send and receive data in one Pico-net at the time. [1]

Off-the-shelf manufacturer packages have nominal supply voltages around 3 V and transmit currents quite typically somewhere around 50 to 60 mA. Receive currents are similar.  $-40^{\circ}\text{C}$  can be reached.

### Summary of 802.15.1

Bluetooth is widely adopted and cheap technology operating at the 2.4 GHz ISM band. Main use is connecting one or several devices over short distances. Frequency hopping rejects interference. However Bluetooth might not fulfil the security and reliability requirements set for reliable control bus. SWOT analysis of the Bluetooth technology is depicted below in the Table 7 .

Table 7 SWOT analysis of Bluetooth

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>Adaptive frequency hopping for better coexistence with static 2.4 GHz channels, full duplex transmission</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>Decreased data rates with FEC, reliability in low delay use</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>Possible to use higher data rates with EDR (non-IEEE standard)</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>Security features</li> </ul>

### 3.4.3 Low rate WPAN IEEE 802.15.4-2006

802.15.4 is designed for ultra low power low data rate sensor networks. It is generally called Zigbee which can be misleading since Zigbee actually refers to higher layer protocol stack.

Offset quadrature phase-shift keying (O-QPSK) is used in static 5 MHz channel with direct-sequence spread spectrum (DSSS) at 2.4 GHz band. DSSS is used to spread signal over larger bandwidth than the modulated information signal. That gives better signal-to-noise ratio increasing resistance to interference and jamming. Maximum of 250 kbps can be reached with the 2.4 GHz main band and there are 16 available channels. Another frequency band is 868 MHz (one channel) e.g. in Europe and 915 MHz (ten channels) in e.g. in North America. Modulation used is BPSK with 20 kbps (in Europe, otherwise 40 kbps). Two other optional modulations are specified for these frequency bands, amplitude shift keying (ASK)

with maximum data rate of 250 kbps. O-QPSK has maximum data rate of 100 kbps in Europe and 250 kbps in North America. [12]

Maximum transmit power at 868.0 – 868.6 MHz band is limited to 25 mW ERP (or effective radiated power, a sum of transmitter power and antenna gain subtracted by attenuation of transmission line) [13]. 2.4 GHz band's maximum transmit power is limited to 100 mW. Devices at the 2.4 GHz band are expected to operate with transmit powers between -3 dBm to 10 dBm, 0 dBm being typical. 868 MHz devices are assumed to transmit at a power between -3 dBm and +10 dBm. These typical values for low cost systems are caused by European regulations of out of band emissions. For higher transmit powers additional expensive filtering would be needed. [12]

Receiver sensitivity at 2.4 GHz band is -85 dBm or better. By the standard's definition that specific receiver sensitivity yields packet error rate (PER) < 1 % with physical layer service data unit (PSDU) size of 20 octets. Receiver jamming limits are 0 dB at the adjacent channel and 30 dB at the alternate channels. [12]

All devices are able to scan specified list of channels. A PAN coordinator can scan channels for energy above threshold, carrier, and carrier sense with energy above threshold. Carrier sense includes detection of same modulation and spreading characteristics. Scan in each channel is to help select a free channel prior to starting a new PAN. [12] Adaptive channel hopping similar to 802.15.1 is not provided.

Transmissions are contention based but PAN coordinator can allocate time slots for devices with time critical data.

Carrier sense multiple access with collision avoidance (CSMA/CA) is used for physical medium access. Network coordinator can also define the format of a super-frame. It is bounded by beacons sent by coordinator. Part of super-frame can be used for contention-free period for low-latency applications. Those portions are called guaranteed time slots (GTSs). [12] Acknowledgement requests and retransmissions can be used with reliable link. Number of retries and acknowledgement wait times can be set. [12] Bit errors are checked with CRC from every frame.

128 bit security is utilized. Data confidentiality, data authenticity and replay protection are provided by the MAC sublayer security services [12].

Large number of devices can be set in a network. Typically in IEEE 802.15.4 sensor networks individual devices send little amount of data and not very often. The demand for bandwidth then is low. Even if point-to-point communication with the requirement for low latency is kept, the data rate is quite limited.

Nominal current is around 30 mA. Receive currents are at the same level or lower. Supply voltages under 2 V are possible. -40°C operating temperature can be reached.

#### *Summary of 802.15.4*

As designed for sensor networks, 802.15.4 has low data rate and very low power. Contention free transmission is possible by using super-frames and beacons to give guaranteed time-slots for devices in the network. 2.4 GHz globally and 868/915 MHz depending on the region are available. Main modulation is O-QPSK with DSSS and optional modulations can be used. Still, data rate is limited to 250 kbps at maximum, which is quite low. Strengths and Weaknesses etc. of the standard 802.15.4 are described in the Table 8.

Table 8 SWOT analysis of 802.15.4

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>Cheap and low powered, DSSS for increasing SNR against carrier wave interference, global 2.4 GHz ISM frequency, multiple manufacturers</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>Inadequate low-latency reliability with sustainable data rate</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>Optional frequency band</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>Potentially crowded band 2.4 GHz</li> </ul>

#### 3.4.4 Low rate WPAN IEEE 802.15.4a-2007

802.15.4a-2007 amendment adds two additional physical layers, Chirp Spread Spectrum (CSS) and Ultra-wide band (UWB). Differences from 802.15.4 are presented here.

## CSS PHY

CSS uses spread spectrum technique that uses chirp pulses. A chirp is sinusoidal signal whose frequency changes over time. It has good resistance for interference and Doppler effect. Differential quadrature phase-shift keying (DQPSK) is used for modulation with 8-ary bi-orthogonal coding for 1 Mbps and 64-ary bi-orthogonal coding for optional 250 kbps data rate. [14] Typically 22 MHz frequency channel is used and for ranging 80 MHz.

Fourteen different channels are defined with four different subchirp sequences form a set of 56 complex channels. Three channels are non-overlapping, at 22 MHz. Maximum transmission rate of the 802.15.4a-2007 CSS PHY is defined 1000 kbps [14]. However Nanotron's NanoLOC chip supports data rates up to 2 Mbps. [15]

Receiver sensitivity is -91 dB (250 kbps) and -85 dBm (1 Mbps). That yields PER < 1% with PSDU size of 20 octets. Minimum receiver jamming resistance is presented in Table 9. Transmitter shall be capable of transmitting at least -3 dBm and a receiver shall have a receiver maximum input level greater than or equal to -20 dBm. [14]

Table 9 Jamming resistance of 802.15.4a CSS

<b>Data rate</b>	<b>Nonoverlapping adjacent channel rejection (25 MHz offset) (dB)</b>	<b>Nonoverlapping alternate channel rejection (50 MHz offset) (dB)</b>
1 Mb/s	34	48
250 kb/s (optional)	38	52

## UWB PHY

The UWB technology has very good interference and jamming tolerance by its wide frequency band. Data is transmitted in very short bursts.

Twelve channels are 500 MHz each and four channels over 1000 MHz each. Channels are distributed below 1 GHz (250 – 750 MHz), low band (3244 – 4742 MHz) and high band (5944 – 10234 MHz). [14]

Data rates of up to 851 kbps are supported. However, UWB PHY offers optional data rates as high as 27 Mbps. Higher data rates are provided to allow devices in close proximity to shorten their transmission duty cycle. UWB PHY uses a UWB direct sequence modulation [14].

Transmitter has no minimum transmit power in the standard but should transmit lower power when possible to reduce amount of interference to other devices. Maximum transmit power is limited by local regulatory authorities. [14] In Europe commission of European Communities has released a decision on maximum mean EIRP densities in different frequency ranges. The result of this decision is shown in Table 10. [16]

Channel scan has UWB PHY specific additions for clear channel access compared to 802.15.4. Energy detection has a series of measurements, each a fraction of the total channel bandwidth. [14]

Table 10 Allowable power in different frequencies of UWB

Frequency range (GHz)	Maximum mean e.i.r.p. density (dBm/MHz)	Maximum peak e.i.r.p. density (dBm/50 MHz)
Below 1,6	- 90,0	- 50,0
1,6 to 3,4	- 85,0	- 45,0
3,4 to 3,8	- 85,0	- 45,0
3,8 to 4,2	- 70,0	- 30,0
4,2 to 4,8	- 41,3 <i>(until 31 December 2010)</i>  - 70,0 <i>(beyond 31 December 2010)</i>	0,0 <i>(until 31 December 2010)</i>  - 30,0 <i>(beyond 31 December 2010)</i>
4,8 to 6,0	- 70,0	- 30,0
6,0 to 8,5	- 41,3	0,0
8,5 to 10,6	- 65,0	- 25,0
Above 10,6	- 85,0	- 45,0

Reed-Solomon code and inner half-rate convolutional code (Viterbi) is used for forward error correction with UWB PHY. Depending on the use of inner convolutional code the overall FEC rate either 0.44 or 0.87. [14]

At least two manufacturers can be found for CSS chips: Nanotron and STMicroelectronics. Nominal voltage for the products is around 2.5 V. Transmit and receive currents is around 30 mA. At least one UWB chip manufacturer can be found, Decawave. Manufacturer's datasheets show that UWB is very low powered, especially transmit, which can be as low as 2 mA. Receive current is around 20 mA at 3 V.

*Summary of 802.15.4a*

Two interesting low-rate WPAN PHY amendments, CSS and UWB, offer better interference tolerance and data rate. CSS has been successfully used in harsh industrial environments operating at 2.4 GHz. UWB offers great coexistence and optionally much higher data rates. SWOT analysis of the 802.15.4a technology is described below in the Table 11.

Table 11 SWOT analysis of 802.15.4a

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>• Low power, transmitter is simple and has very low power (UWB), good interference tolerance, good coexistence and low interference caused to other media (UWB), higher data rates than basic 802.15.4, global ISM frequency (CSS), global use (UWB)</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>• Not too many manufacturers, low transmit power limits range (UWB)</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>• Nanotron's CSS chips can be used with non-IEEE standard data rate up to 2 Mbps, UWB can operate even with faster data rates if manufacturer supports it</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>• Potentially crowded band (CSS)</li> </ul>

### 3.4.5 High rate WPAN IEEE 802.15.3-2003

802.15.3 is designed to be a high data rate wireless architecture for fixed, portable and moving devices in fairly short distances. A goal is to achieve a level of interoperability and coexistence with other 802.15 standards. Consideration has also been done to improve coexistence with 802.11b. In 802.15.3 networks, or Pico-nets, devices communicate in peer-to-peer manner. Pico-net coordinator manages QoS requirements, power save modes and access control to the Pico-net [17].

2.4 GHz band is used with five 15 MHz channels available. Five modulation formats are defined each with different data rates. They are presented in Table 12. Trellis code modulation (TCM) is used for all but one mode. At least DQPSK modulation shall be supported by 802.15.3-compliant device. [17]

Table 12 Modulation, coding and data rates of 802.15.3

Modulation type	Coding	Data rate
QPSK	8-state TCM	11 Mb/s
DQPSK	none	22 Mb/s
16-QAM	8-state TCM	33 Mb/s
32-QAM	8-state TCM	44 Mb/s
64-QAM	8-state TCM	55 Mb/s

The receiver sensitivity is the minimum power level of the incoming signal present at the input of the receiver where error rate criterion is met. It is defined as frame error rate (FER) of less than 8 %, after error correction, with a frame payload length of 1024 octets and pseudo-random data. The receiver sensitivities for different modulations can be seen in Table 13. [17]

The transmitted spectral density shall be no higher than limited in the spectral density mask in Figure 2. It shows relative transmitter limits around central frequency. Maximum transmit power is limited to 100 mW EIRP and 10 mW/MHz peak power density in Europe.

Pico-net coordinator can change the channel dynamically that Pico-net is using without user intervention or the disruption of the services in the Pico-net. Evaluation of channel status can

be done by gathering channel information from other devices, performing a passive scan or requesting other devices to perform a channel scan. [17]

The receiver jamming resistance levels for different modulations are shown in Table 14. [17]

Table 13 Receiver reference sensitivities of the 802.15.3

Modulation	Reference sensitivity
QPSK-TCM	-82 dBm
DQPSK	-75 dBm
16-QAM-TCM	-74 dBm
32-QAM-TCM	-71 dBm
64-QAM-TCM	-68 dBm

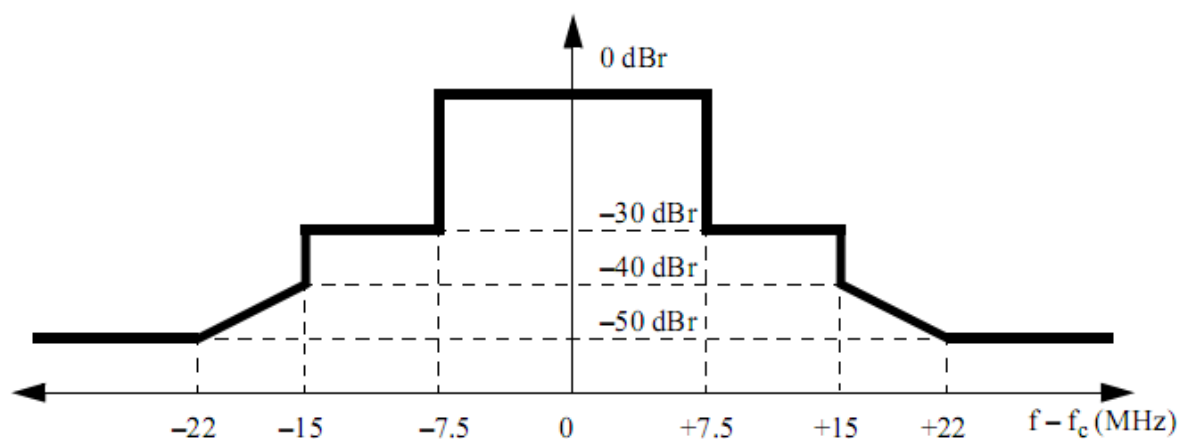


Figure 2 Transmit power spectral density mask of 802.15.3

Table 14 Receiver jamming resistance requirements of 802.15.3

Modulation format	Adjacent channel rejection	Alternate channel rejection
QPSK-TCM	33 dB	48 dB
DQPSK	26 dB	41 dB
16-QAM-TCM	25 dB	40 dB
32-QAM-TCM	22 dB	37 dB
64-QAM-TCM	19 dB	34 dB

Three acknowledgement types are defined. They are no-ACK, immediate-ACK and delayed-ACK. Immediate ACK is sent right after intended recipient has received frame. Delayed acknowledgement is for directed stream data frames. [17]

Frame format for the 11 Mbps mode differs slightly from other modes. Biggest difference is that PHY and MAC header plus header check sequence (HCS) are modulated twice, with 22 Mbps DQPSK and again with 11 Mbps QPSK-TCM. Idea is to ensure that header error rate is lower than frame payload error rate. For the other modes that is only modulated with 22 Mbps DQPSK. Preamble is always modulated with 22 Mbps DQPSK. [17]

Data transport with QoS is supported. Timing in 802.15.3 is based on super-frame. It has a beacon for timing allocations and management information, contention access period for commands and asynchronous data, and channel time allocation period for channel time allocations including commands, isochronous streams and asynchronous data connections. [17]

128-bit AES security is used. Data can be encrypted by a key shared by all Pico-net devices or a key shared only between two devices. Also beacons and commands may be integrity-protected. [17]

Chip manufacturers are hard to find. Technology might not be interesting enough as there are other alternatives for high data rate short range uses, e.g. very popular WLAN, and maybe WiMedia based UWB for very short ranges if it gets more common.

### Summary of 802.15.3

Too little too late. A light infrastructure, short range high data rate solution is too much like WLAN (802.11\_), which of cause has already taken the markets. Strengths and Weaknesses etc. of the standard 802.15.3 are described in the Table 15.

Table 15 SWOT analysis of 802.15.3

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>• Well sufficient data rate</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>• Standard since 2003 – where are the commercial chip manufacturers?</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>• ?</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>• May be obsolete - the standard will not be adopted by markets</li> </ul>

### 3.4.6 High rate UWB, ECMA-368

This is standardized also by ETSI (ETSI TS 102 455) and ISO/IEC (ISO/IEC 26907). It is based on WiMedia UWB radio platform.

This standard utilizes unlicensed frequency band of 3100 – 10600 MHz. The standard defines 14 channels 528 MHz each. Multiband OFDM (MB-OFDM) with total of 110 sub-carriers (100 for data and 10 guard carriers, i.e. not in use) are used per band to transmit the information. Frequency-domain spreading, time-domain spreading and forward error correction coding (FEC) are used to vary data rates. Scalable data rates theoretically up to 480 Mbps are supported with couple meter ranges. Data rate will be decreased as more range is needed. The coded data is spread using time-frequency code. The data can be interleaved over three bands, two bands and over single band, and individual OFDM sub-carriers can be nulled. This provides good control over spectrum allowing PHY to be used in range of regulatory and radio coexistence scenarios. [19]

Channel limitations vary regionally. In Europe channels 4 – 6 and 12 – 14 are unusable and some channels have protection requirements. [18] Dynamic channel selection is also available to change channels in coordinated manner between devices.

For a packet error rate of less than 8 % with PSDU of 1024 octets, the minimum sensitivities in all-white Gaussian noise (AWGN) for different data rates are listed in Table 16 [19].

Table 16 Receiver sensitivities for ECMA-368

Data Rate (Mb/s)	Minimum Receiver Sensitivity (dBm)
53,3	-80,8
80	-78,9
106,7	-77,8
160	-75,9
200	-74,5
320	-72,8
400	-71,5
480	-70,4

Receiver has good tolerance for interference and jamming. Transmitter power should use the lowest possible transmit power with which it can maintain its links [19].

FEC used is a convolutional code with coding rates of 1/3, 1/2, 5/8 and 3/4. Security protection includes data encryption, message integrity and replay attack protection. A 4-way handshake mechanism is specified for two devices to identify each other. A secure relationship is established based on pre-shared (128-bit) master key. A recipient device can suggest optimal data rate to increase throughput or perhaps reduce frame error rate. The ECMA-368 standard, however, does not describe how to determine optimal data rate. [19]

#### *Summary of ECMA-368*

High data rate UWB is still waiting for its breakthrough. Especially multimedia applications were general insight in the design. WiMedia based radio platform has high data rate, although theoretical data rate and true data rate can be quite far apart, good coexistence and interference tolerance. High data rate gives possibilities for forward error correction. WiMedia is ceasing its operation and implementing a technology transfer to Bluetooth SIG, Wireless USB Promoter Group and USB Implementers Forum, and still some uncertainty is

upon this technology. SWOT analysis of the ECMA technology is depicted below in the Table 17.

Table 17 SWOT analysis of ECMA-386.

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>• Coexistence, interference tolerance, minimal interference caused to single band media, high data rate, global use</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>• Limited range, data rate decreases fast as range increases, not designed for time-critical applications</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>• Chips and consumer products are gradually getting to markets, standard is used in Wireless USB which could be next hit</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>• Technology not yet stabilized in the markets</li> </ul>

### 3.5 Comparison of candidate standards against basic threats

In table 1 were described the basic threats in wireless system. Now the strengths of SRC standards are projected against these threats.

*The transmission fades because the distance between sender and receiver increases*

IEEE standard 802.11p has especially good range and UWB has lowest range because of its low transmit power. Still, all candidates have sufficient range for this application.

*The signal fades because of obstacles*

The desired range is quite short. Objects directly between communicating radio nodes could be harmful to signal level and signal to noise ratio. Physically separate redundant radio interface or antennas could be used. Line of sight could be kept more reliably and not be dependent on position of the boom between cabin and the harvester head.

*Transmission signal fades because of environment conditions*

Weather conditions are not substantial factor in such a short range considering fading. In larger context of environmental conditions interference can be fought by using divergent

frequencies (802.11p, 802.15.4a UWB, ECMA-368) or by frequency hopping (Bluetooth). 802.15.4 and 802.15.4a CSS are somewhat vulnerable because they are using popular licence free 2.4 GHz band. CSS uses wide 80 MHz band when 1 Mbps data rate is selected and should not be as sensitive to overlapping narrow band interference.

*Transmission signals are reflected from surfaces resulting in echoes and interference, or signal appears because of reflections from long distances*

ECMA-368 and 802.15.4a UWB technologies offer good resistance to multipath fading. Low transmit power decreases reflections from long distances. OFDM modulation in WLAN (802.11a/g/n/p) is good dealing with multipath. Also 802.15.4a CSS offers also resistance to multipath fading and a robust performance.

*Two or more signals interfere with each other and cause proper signal for another receiver*

Other nodes could use frequencies and modulations that are too close to ours. UWB is insensitive to narrow band interference and vice versa in terms of creating signals out of noise. However it is possible that in some conditions they can interfere each other decreasing signal to noise ratio. 802.11p is using higher frequency than OFDM modulated WLAN at 2.4 and 5.0 GHz but its range is also higher. Bluetooth has an adaptive frequency hopping which helps to avoid crowded channels in the 2.4 GHz band. 802.15.4 and 802.15.4a CSS may be vulnerable for this kind of interference if equivalent nodes are operating close by.

*Receiver is too sensitive*

Short messages could be generated out of noise. 802.15.4 and 802.15.4a CSS have best sensitivities of the non-UWB technologies, -85 dBm, with data rates of 250 kbps and 1 mbps respectively. CSS has very good signal-to-noise ratio though. 802.15.4a UWB has good receiver sensitivity and transmitters should always use low power to decrease interference to other devices. Bad frames are dropped by frame correctness check but faulty frame generation in receiver causes a short time when it's not able to receive correct frames.

*Poor capability of a relaying station*

Data is relayed from the control bus through wireless interface. The requirement for data rate of wireless interface is set to meet data rate of control bus. 802.15.4 has quite low but the rest of the standards have sufficient data rate.

*The nodes understand the network state or configuration differently at the same time*

This is a problem with several nodes when they are moving and a node can remain hidden from some of the other nodes. Not relevant in this context.

*Nearby wireless network is using similar communication protocol*

This threat concerns substitution of nodes. Both intentional and unintentional substitution can be fought by using security procedures the standards provide. Substitution would be quite improbable when sufficient and correctly applied security procedures are used.

*Security; intentional penetration to wireless network*

All standards come with at least 128-bit security key which is quite sufficient. Bluetooth has been criticized on security issues mostly because of its wide use and typical use scenario; the devices are not fully authenticated before the communication sequence.

*Systematic failure, characteristics of wireless communication is not considered*

To minimize risks the most suitable communication technology is chosen.

*Sleeping nodes in low power networks. Some nodes can be ordered to sleep to lower power consumption i.e. longer battery life*

Low delays are required. Sleeping is not useful in this context.

### 3.6 Possible solutions for communication between machines

The wireless communication between machines and/or infrastructure does not have any strict reliability requirements. It is not used in control applications so there is no requirement for low delay. Claimed data throughput rate is quite low. The main requirements are long operation range and Non-line-of sight operation (NLOS). Standards like WiMAX (IEEE 802.16), MBWA (IEEE 802.20), foregoing IEEE 802.11p and some Non-standard radio systems are in line with this application.

#### 3.6.1 WiMAX IEEE 802.16-2009

IEEE 802.16 is a series of Wireless Broadbands standard. First mobile Wimax (Worldwide Interoperability for Microwave Access) was defined by the 802.16e-2005. Wimax provides wireless transmission of data using a variety of transmission modes, from point-to-multipoint

links to portable and fully mobile internet access. The technology offers up to 70 Mbps download/upload throughput, and it is primarily meant for Internet applications. The radio access is based on Orthogonal Frequency Division Multiple Access (OFDMA) and Multiple-Input Multiple-Output (MIMO) technologies. Standard 802.16e supports channel bandwidths between 1.25 MHz and 20 MHz. Wimax supports adaptive modulation. Highly efficient 64 QAM coding scheme is used in good signal conditions and for poorer signal BPSK coding is used. PHY specification of 802.16e supports MIMO antennas, which provides good NLOS (Non-line-of sight) characteristics also supported is Hybrid automatic repeat request (HARQ). The MAC layer of mobile Wimax should have support for five different QoS classes, briefly summarized in Table 18. Mobile Wimax Application Classes are represented in Table 19. Minimal latency is less than 25 ms. Temperature range of Wimax is -40 to +65°C.

Table 18 Mobile WiMAX QoS Classes [20]

<b>QoS Class</b>	<b>Supported Service</b>	<b>Example Application</b>
<b>Unsolicited Grant Services (UGS)</b>	Latency- and jitter-sensitive applications with fixed-size data packets at Constant Bitrate (CBR)	Voice over IP (VoIP) without silence suppression
<b>Real-Time Variable Rate (RT-VR)</b>	Real-time applications with variable-size data packet bursts	Video and audio streaming
<b>Non-Real-Time Polling Services (nrtPS)</b>	Delay-tolerant applications with variable-size data packets and guaranteed bitrate demands	File transfers
<b>Extended Real-Time Variable Rate (ERT-VR)</b>	Real-time applications with Variable Bitrate (VBR) data streams and guaranteed bitrate and delay demands	VoIP with silence suppression
<b>Best Effort (BE)</b>	Data streams with no minimum service-level demands	Web browsing, instant messaging, and data transfer

Table 19 Mobile Wimax Application Classes [20]

Class	Application	Bandwidth Guideline		Latency Guideline		Jitter Guideline	
		Low	50 kbps	Low	< 25 msec	N/A	
2	VoIP & Video Conference	Low	32 to 64 kbps	Low	< 160 msec	Low	<50 msec
3	Streaming Media	Low to High	5 kbps to 2 Mbps	N/A		Low	<100 msec
4	Web Browsing & Instant Messaging	Moderate	10 kbps to 2 Mbps	N/A		N/A	
5	Media Content Downloads	High	> 2 Mbps	N/A		N/A	

Figure 3 shows the packet error rate (PER) for urban microcell as a function of signal to noise ratio (SNR). Figure represents simulation results of PER and the experimental data. This data is generated at different link speeds and having different SNR levels [21]

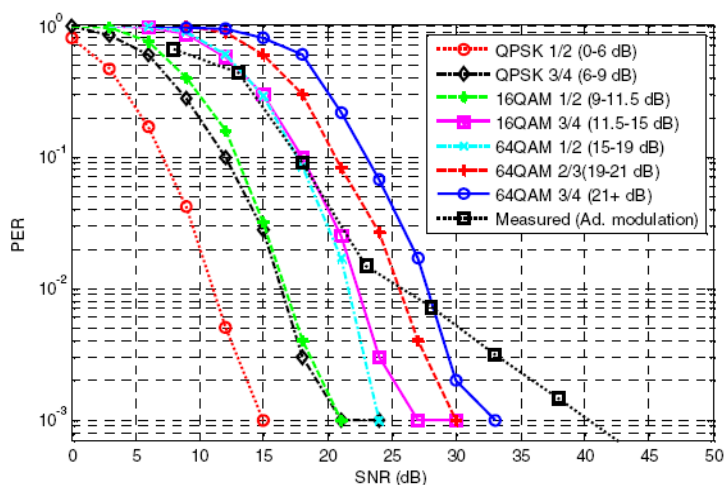


Figure 3 Experimental and simulation PER

The WiMAX Forum has defined certification profiles, which are defined by having three basic characteristics: spectrum band, channel width and duplexing type.

Wimax certification profiles are out-written in Table 20

Table 20 Wimax certification profiles [22][23]

Frequency band	Channel Bandwidth(MHz)	Duplexing
3.5 GHz	3.5	TDD
	3.5	FDD
	7	TDD
	7	FDM
5.8 GHz	10	TDD
<b>Mobile WiMAX</b>		
Frequency band	Channel Bandwidth(MHz)	Duplexing
2.3-2.4 GHz	5	TDD
	8.75	TDD
	10	TDD
2.305-2.320 GHz, 2.345-2.360 GHz	3.5	TDD
	5	TDD
	10	TDD
2.496-2.69 GHz	5	TDD
	10	TDD
3.3-3.4 GHz	5	TDD
	7	TDD
	10	TDD
3.4-3.8 GHz 3.4-3.6 GHz 3.6-3.8 GHz	5	TDD
	7	TDD
	10	TDD

Frequency bands used in different regions can be seen in Table 21.

Frequencies at the 5.8 GHz band are licence free almost in all countries in Europe. Other frequency bands are not licence free.

Table 21 Wimax frequency bands on the region [22][23]

REGION	TYPICAL FREQUENCY BANDS FOR WIMAX
EUROPE	2.5, 3.5 and 5.8 GHz
USA	2.3, 2.5 and 5.8 GHz
CENTRAL AND SOUTH AMERICA	2.3, 2.5 and 5.8 GHz
SOUTH-EAST ASIA	2.3, 2.5, 3.3, 3.5 and 5.8 GHz
MIDDLE EAST AND AFRICA	3.5 and 5.8 GHz

Mobile Wimax network consists of Base Stations (BS) and Mobile Subscriber Stations (MSS). Mobile Stations are registered and controlled by the Base Station i.e. the system doesn't work without the BS. Mobile Wimax defines two operation modes: PMP (Point-to-Multipoint) and Mesh mode. The MSS communicates directly to the BS only in the PMP

mode. In the Mesh mode, the data is sent from a MSS to another MSS and at the end the data may be transferred to another MSS by multiple hops. An example of a Wimax mesh network is depicted in Figure 4 [23].

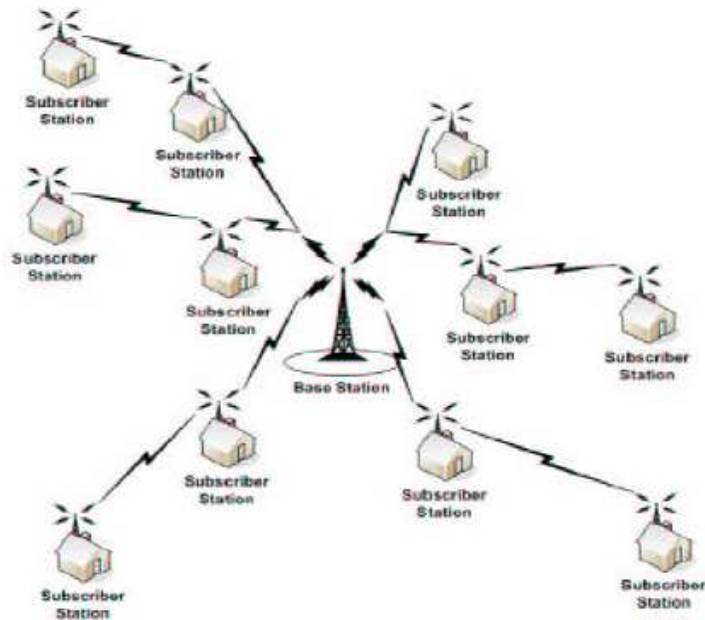


Figure 4 An example of a Wimax mesh network

SWOT analysis of the WiMAX Standard is described in the Table 22

Table 22 SWOT analysis of WiMAX

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>Adaptive modulation, MIMO (Non-line of sight), Free frequency band, Low latency, High throughput data rate, Well knows technique, In general used, several devices manufacturers</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>No Ad-hoc operation, Expensive (Base Station)</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>Devices availability, Non-standard Ad-hoc?</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>Operation range on mobile use</li> </ul>

### 3.6.2 IEEE 802.20-2008

IEEE 802.20 so called Mobile Broadband Wireless Access (MBWA) is approved in June 2008 by IEEE. Layers standardized by this standard IEEE 802.20 are PHY, MAC and Logical Link Control (LLC) layer. Standard 802.20 operates in licensed frequency bands below 3.5 GHz and has high speed data rate (20 Mbps). MBWA supports vehicular mobility up to 250 km/h. The MBWA networks consist of base stations and mobile end users. 802.20 will fill the gap between cellular networks and other IEEE 802 wireless networks currently in use, such as WLANs and WiMAX. [24]

PHY layer of MBWA defines:

- Two duplex modes: Time Division Duplex (TDD) and Frequency Division Duplex (FDD)
- Two forward link hopping modes: Symbol Rate Hopping and Block-Hopping
- Two synchronization modes: Semi Synchronous and Asynchronous
- Two multi-carrier modes: Multi-Carrier On and Multi Carrier Off
- Modulation uses OFDM with QPSK, 8PSK, 16QAM and 64QAM modulation formats
- 

802.20 supports channel bandwidths 1.25 MHz and 5 MHz. Non-line-sight (NLOS) outdoor and indoor systems are provided. MBWA system uses different types of data packets.

Minimal latency of data packet is 10 ms. [25]

The MAC layer consists of functions like session, convergence, security and lower MAC functions. The lower MAC sublayer defines the procedures used during receiving and transmitting over the physical layer. It controls data channel operations: Forward Traffic Channel and Reserve Traffic Channel. Forward- and reserve data link transmissions are divided into units of super-frame, which are further divided into the PHY frame units (FDD and TDD).

SWOT analysis of the MBWA Standard is described in the Table 23

Table 23 SWOT analysis of MBWA.

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>Optimized for fully mobility, High throughput data rate, Low latency</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>No Ad-hoc operation, Devices not availability for the moment</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>Global used in future</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>Operation range on mobile use, No license free frequency band</li> </ul>

### 3.6.3 Non-Standard radio system

There has been a lot of wireless non-standard radio modem manufactures, e.g. XtremeRange series of radio modules by Ubiquiti. These radio system modules are used on the industrial, scientific and medical (ISM) radio band. XtremeRange 9 radios are operating on the frequency band of 900 MHz. Operation range is fairly longer than the range of WLAN. The radio system includes the same MAC than WLAN (802.11a, 802.11b and 802.11g) but PHY is not WLAN compliant. This radio system is FCC compliant, but it is not approved in Europe. The big problem of the non-standard long range equipment is that it has no global frequency approval. The majority of the world would not be able to use the 900MHz band because it has already been allocated. In Europe there is a similar free ISM 433 MHz band.

SWOT analysis of the Non-Standard Radio Systems is described in the Table 24

Table 24 SWOT analysis of Non-Standard radio systems.

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<u><b>Strengths</b></u> <ul style="list-style-type: none"> <li>• Long operation range</li> </ul>	<u><b>Weaknesses</b></u> <ul style="list-style-type: none"> <li>• Non standard, No global frequency band</li> </ul>
<i>External Origin</i>	<u><b>Opportunities</b></u> <ul style="list-style-type: none"> <li>• Technically Simple</li> </ul>	<u><b>Threats</b></u> <ul style="list-style-type: none"> <li>• Devices manufacturer-specific</li> </ul>

### 3.7 Possible solution for very short range communication

Inductively coupled power and data link can be used in very short range communication and powering. In cars and in other heavy vehicle's it can be used e.g. for power controlling and transferring data and power over a small air-gap.

A block diagram of a digital communication system is described in Figure 5. Inductively coupled power and data transfer system requires also three main functional blocks. These blocks are: signal coder and a modulator in the transmitter, the transmission channel and the demodulator and the signal decoder in the transponder (receiver). [26]

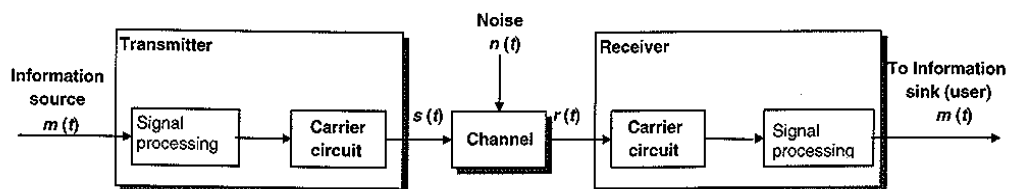


Figure 5 Signal and data flow in a digital communications system.

Figure 6 presents one way to do inductively coupled power and data link.

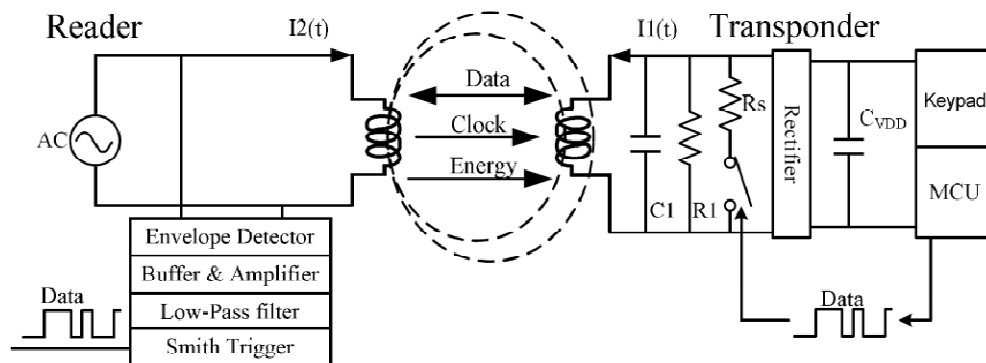


Figure 6 Inductively coupled data and power link.

#### 3.7.1 Modulation

Electromagnetic wave has three main variables: Amplitude, frequency and phase. These variables can be used for three different types of modulation: amplitude modulation (AM),

frequency modulation (FM) and phase modulation (PM). All other modulation procedures are derived from these three basic types. Inductively coupled systems are using digital modulation procedures like ASK (amplitude shift keying) FSK (frequency shift keying) and PSK (phase shift keying) (Figure 7). [26]

In Figure 8 Modulation products using load modulation with a subcarrier are shown.

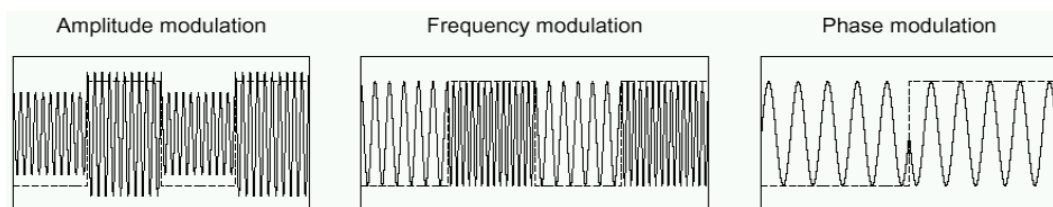


Figure 7 Modulations.

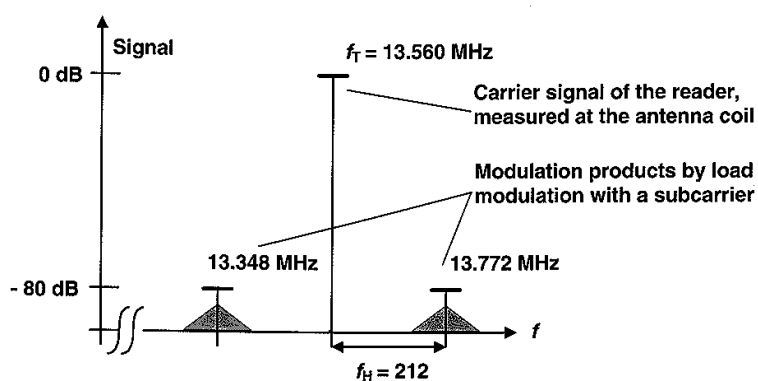


Figure 6.13: Modulation products using load modulation with a subcarrier

Figure 8 Modulation products using load modulation with a subcarrier.

### 3.7.2 Coding

Bits (one and zero) can be represented in various line codes. Inductively coupled systems typically use some of the next methods: NRZ, Manchester, Unipolar RZ, DBP (differential bi-phase), Miller Differential coding and PP coding (Figure 9). [26]

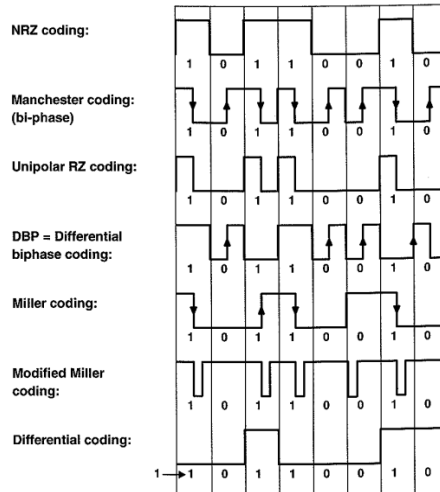


Figure 9 Signal coding by frequently changing line codes in inductively coupled systems.

### 3.7.3 Data Security

Modern authentication protocols can be used. As we know the working range for inductively coupled systems is quite short. Hence it is not easy to access to the system nor generate fault functions. For example RFID payment systems have very high data security level. [26]

### 3.7.4 Inductive power and data link risk analysis

Reliability of inductively coupled power link is better than inductively coupled data link. When power can be delivered, it still isn't sure that the data link is also working.

Risks of the inductive coupled power and data links are as follows:

- External materials
  - Detunes link
  - Coupling coefficient decreases
- Eddy currents (near conductive plates)
  - Magnetic field decreases
- Misalignment decreases efficiency
  - Lateral misalignment

- o Angular misalignment
- External magnetic fields
  - Other RFID & NFC devices
  - Frequency range 13.56 MHz is freely available ISM-band. Nowadays rarely in use, but maybe there will be more use in the future, when RFID/NFC comes more public
- Power supply
  - No power supply
  - Too low power supply
  - Too high power supply
  - Some disturbance
- Temperature, humidity, vibration, ageing etc.
  - o Oscillator creep
  - o Change in operating frequency
- Modulation problems

Risks in inductively coupled links are quite minimal. The biggest problems are caused by external materials which may come too near to the link in use. When building a system the tuning of the link can be done by adjusting the mechanical conditions. If there are changes in the mechanical conditions it is possible that problems will occur, because the link is not at the resonant frequency anymore. If the near put external material is conductive it may also cause eddy currents to occur. Magnetic fields caused by these eddy currents are opposite to the original magnetic field and are decreasing it. If there is some external conductive material between the antenna coils of the link the link will not obviously work at all (usually not possible case).

If the coils are having some misalignment state the efficiency of the link decreases dramatically and finally the link will not work at all. The possibility that antennas can go to a misalignment state is absolutely minimal if the system is designed to work at the worst case situation.

In theory it is possible that near the inductively coupled link some high magnetic fields can occur. These fields may have some affect to the inductive link and cause some problems.

One potential risk might be the frequency range 13.56 MHz because it is in the freely available ISM-band. Nowadays the frequency is not so much in use, but in the future there might be some more use, when RFID/NFC comes more public.

Basic problems concerning to the electronics are temperature, humidity, vibration etc. Alternating temperature might draw e.g. oscillator circuit out of the frequency designed and the efficiency of the link will fall down. Humidity and vibration might break down circuit boards solder joints etc. Vibration affects also to the crystals on board and may cause some changes to their frequencies. [27][28]

### 3.7.5 Inductive coupled system advantages

- Frequency band is available worldwide as the ISM frequency band.
- The air interface is standardized by ISO 15693 and ISO 14443 and HF ePC.
- Robust reader-to-tag communication
- Excellent immunity to environmental noise and electrical interference
- Well defined and localised label interrogation zones
- Minimal shielding effects from adjacent objects and the human body
- Water's damping effects relatively small, field penetrates dense materials
- Freedom from environmental reflections that can plague UHF and microwave systems
- High clock frequency and synchronous subcarrier
- On-chip capacitors for tuning transponder coil can be easily realised
- Cheap IC's, disposable tags
- Cost effective antenna coil manufacturing
- Low RF power transmission so EM regulation compliance cause no problems
- No user licenses for reader systems required (ISM band)
- Possible to use the systems in industrial and in hazardous environments with potential for explosive substances

[27][28]

### 3.7.6 Comparing key RFID parameters to other wireless standards

Table 25 compares inductively coupled links to other wireless standards. [29]

Table 25 Comparing key RFID parameters to other wireless standards.

	Inductive	Zigbee	Bluetooth	802.11b	802.11a	GSM/GPRS	IS2000
Multiple Acces	FHSS/TDMA	CDMA/CA	FHSS/TDMA	FDM/CSMA/CA	FDM/CSMA/CA	FDMA/TDMA	CDMA
Frequency Band	125 kHz – 2.5 GHz	868 MHz, 915 MHz, 2,4 GHz	2402-2484 MHz	2402-2484 MHz	5,2-5,8 GHz	800-2000 MHz	1885-2200 MHz
Data Rate	0,12 kB/s-25 kB/s	20 kB/s – 250 kB/s	122 kB/s	122-1343 kB/s	122-6592 kB/s	1-14 kB/s	12207-244140 kB/s
RF Modulation	ASK, mFKS, mPSK	BPSK, QPSK	FSK	DQPSK	nPSK/QAM-n OFDM	GMSK	QPSK (DL) BPSK (UL)
Transmission Power	1 mW-4W	1 mW	1 mW-100mW	100 mW	2 W	2 W	600 mW
Typical Range	50 cm (passive), 10 m (active)	10 m	1-30 m	120 m	60 m	30 km	20 km

SWOT analysis of the Inductive Link Standard is described in the Table 26

Table 26 SWOT analysis of inductive link.

	<i>Helpful</i>	<i>Harmful</i>
<i>Internal Origin</i>	<p><b><u>Strengths</u></b></p> <ul style="list-style-type: none"> <li>• Free frequency band</li> <li>• Power and data can be delivered</li> <li>• Cheap parts</li> <li>• Excellent immunity to environmental noise and electrical interference</li> </ul>	<p><b><u>Weaknesses</u></b></p> <ul style="list-style-type: none"> <li>• Short working range</li> <li>• Low data rate</li> </ul>
<i>External Origin</i>	<p><b><u>Opportunities</u></b></p> <ul style="list-style-type: none"> <li>• Minimal shielding effects from adjacent objects and the human body</li> <li>• Security applications</li> </ul>	<p><b><u>Threats</u></b></p> <ul style="list-style-type: none"> <li>• Changing environmental conditions</li> <li>• Frequency range use in future?</li> </ul>

## Conclusions

### VSRC

Inductive coupled power and data link could be good selection to very short-range communication. It is cheap, frequency band is free and it has an excellent immunity to environmental noise and electrical interference. One possible risk comes from changing environmental conditions, like in a situation when a conductive material comes near to link. It is also unknown how large the frequency range use is in the future. It is clear that number of devices which use the same frequency range will grow in near future. To get clear vision how inductively coupled power and data link works in heavy vehicles prototype device should be built.

### SRC

Despite the MAC have had some improvements by the 802.11p standard the contention-based channel access may still be insufficient in terms of real-time communications. Because the standard has been just developed there are not very many chipsets available at the moment. But still this is one possible candidate for long range communication between machines which is its original intended use.

Most promising technologies for reliable wireless control bus in this report are defined by the IEEE standard 802.15.4a. This amendment of IEEE Standard 802.15.4-2006 specifies alternate physical layers (CSS, UWB) in addition to the PHYs specified in the base standard. These will give some benefits in form of higher bandwidth and better interference tolerance. There are some examples of higher layer solutions build on the top of the 802.15.4 MAC layer which are used reliably in the industrial environments. This standard has guaranteed time-slots for transmissions. However typical applications are defined as non-critical monitoring, controlling and so on.

The standard 802.15.3 is pretty much obsolete because of the lack of the commercial manufacturers. ECMA-368 is designed for multimedia use but its future is still somewhat unclear. Design points have not been in the safety critical transmissions. The high bandwidth does not fully compensate the other deficiencies.

## MRC

The standard 802.11p is the best solution in functionality. It is a technology, which supports point to point (P2P) or vehicle to vehicle (V2V) architecture. Wimax (802.16) and MBWA (802.20) don't work without a base station. Moreover MBWA are unavailable at this moment. Operation range can be one weakness of the standard 802.11p. Only non-standard radio technologies have sufficient range of few kilometres.

## References

- [1] Malm, T. et al. 2007. Validation of Safety Related Wireless Machine Control Systems. [http://www.nordicinnovation.net/\\_img/tr605.pdf](http://www.nordicinnovation.net/_img/tr605.pdf) [July 10<sup>th</sup> 2009]
- [2] Harri Viittala Risk Analysis – IEEE 802.11p Ajoneuvon / työkoneen langattomat lähiverkot (ALMA) Version 1.0 (21.08.2009).
- [3] IEEE 802.11 Task Group p – Wireless Access in Vehicular Environments, [http://www.ieee802.org/11/Reports/tgp\\_update.htm](http://www.ieee802.org/11/Reports/tgp_update.htm)
- [4] The Federal Communication Commission (FCC), Amendment of the Commission’s Rules Regarding Dedicated Short-Range Communication s Services in the 5.850 – 5.925 GHz band (5.9 GHz band). Report and Order, Doc: FCC 03-324, 78 p, 2004.
- [5] The Federal Communication Commission (FCC), Amendment of the Commission’s Rules Regarding Dedicated Short-Range Communication s Services in the 5.850 – 5.925 GHz band (5.9 GHz band). Memorandum Opinion and Order, Doc: FCC 06-110, 78 p, 2006.
- [6] The Electronic Communications Committee (ECC), Decision on the Harmonized use of the 5875 – 5925 MHz Frequency Band for Intelligent Transport Systems (ITS). Doc: ECC/DEC/(08)01, 5 p., 2008.
- [7] IEEE Standard for Local and Metropolitan Area Networks: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Doc: IEEE Std 802.11-2007, 1232 p., 2007.
- [8] Institute of Electrical and Electronics Engineering, IEEE std. 802.15.1-2005
- [9] Bluetooth SIG, Bluetooth specification v.2.1+EDR [vol 2], available at <http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/>
- [10] European Conference of Post and Telecommunications Administrations / European Radiocommunications Committee (CEPT/ERC) Recommendation 70-03 Annex 1, June 2009, <http://www.eroocdb.dk/Docs/doc98/official/pdf/REC7003E.PDF>
- [11] SecurityFocus, a vendor-neutral site objective, timely and comprehensive security information, <http://www.securityfocus.com/infocus/1830> [July 10<sup>th</sup> 2009]
- [12] Institute of Electrical and Electronics Engineering, IEEE std. 802.15.4-2006
- [13] European Telecommunications Standards Institute, ETSI EN 300 220-1 V2.3.1, 2009-04
- [14] Institute of Electrical and Electronics Engineering, IEEE std. 802.15.4a-2007
- [15] Nanotron Technologies, NanoLOC TRX transceiver key features, [http://www.nanotron.com/EN/PR\\_nl\\_TRX.php](http://www.nanotron.com/EN/PR_nl_TRX.php)
- [16] Official Journal of European Union, Commission Decision of 21 February 2007, on allowing the use of the radio spectrum for equipment using ultra-wideband technology in a harmonised manner in the Community.
- [17] Institute of Electrical and Electronics Engineering, IEEE std. 802.15.3-2003
- [18] WiMedia Alliance, World wide regulatory status (20<sup>th</sup> of January 2009), [http://www.wimedia.org/en/resources/worldwide\\_regulatory.asp?id=res](http://www.wimedia.org/en/resources/worldwide_regulatory.asp?id=res)
- [19] ECMA International, ECMA-368 standard (3<sup>rd</sup> edition, December 2008)

- [20] WiMAX Forum, Mobile Wimax Part 1 Overview and Performance, 2006, [http://www.wimaxforum.org/technology/downloads/Mobile WIMAX Part 1 Overview and \\_Performance.pdf](http://www.wimaxforum.org/technology/downloads/Mobile_WIMAX_Part_1_Overview_and_Performance.pdf)
- [21] Mobile WiMAX: Performance Analysis and Comparison with Experimental Results, Mai Tran, George Zaggoulos, Centre of Communications Research, University of Bristol, IEEE
- [22] WiMAX: IEEE 802.16, Jorge Lopez Vizcaino, Tampere polytechnic, 2008
- [23] Michiyo Ashida and Tapio Frantti, System Architecture for C2C Communications Based on Mobile WiMAX, Springer-Verlag, 2008
- [24] 802.20: Mobile Broadband Wireless Access, Walker Bolton, Yang Xiao, Moshen Guizani,02/2007
- [25] IEEE 802.20 WG, Initial Views on the Desired Characteristics of Mobile Broadband Wireless Access Air Interface, 802m\_ecsg-02-08.
- [26] Klaus Finkenzeller (2003) RFID Handbook: Radio-Frequency Identification Fundamentals and Applications John Wiley & Son, LTD.
- [27] UPM raflatac (2003) Tutorial overview of inductively coupled RFID Systems URL: <http://www.mobiusconsulting.com/papers/rfidsystems.pdf>.
- [28] Rata M., Rata G., Graur A. & Popa V.(2007) The influence of different materials in 13.56 RFID system, RFID EURASIA, s.1-3
- [29] Hande A., Bridgelall R., Bhatia D. (2009) Chapter 18: Energy Harvesting for Active RF Sensors and ID Tags In: Priya S., Inman D.J. (eds.), Energy Harvesting Technologies, Blacksburg.