

UNIVERSITY OF PADOVA



FACULTY OF ENGINEERING

Department of Information Engineering
Ph.D. School on Information Engineering

Information Science and Technologies
XXIII Cycle

**Analysis of performance and
interference effects in Radio Frequency
IDentification systems**

Ph.D. Thesis

School Head: Ch.mo Prof. Matteo Bertocco

Supervisor: Ch.mo Prof. Alessandro Sona

Ph.D. candidate: Ing. Andrea Dalla Chiara

*to my beloved wife
the days before and those after, Moira.*

Contents

Contents	v
List of Figures	ix
Acronyms	xiii
Abstract	xvii
Sommario	xix
Introduction	xxi
0.1 Field of interest	xxi
0.2 Motivation	xxii
0.3 Contributions	xxiii
0.3.1 Main contributions	xxiii
0.3.2 Other Contributions	xxiii
0.3.3 Minor contributions	xxiv
0.4 Structure	xxiv
1 Introduction to RFID Systems	1
1.1 Radio Frequency Identification	1
1.2 History of RFID	2
1.2.1 The military contribution	2
1.2.2 Development in civil context	3
1.2.3 Today	7
1.3 System components	8
1.3.1 Transponders	9
1.3.2 The Reader	10
1.3.3 Middleware	11
1.4 Operative frequencies	11
1.4.1 Low Frequency: 120 – 145 kHz	12
1.4.2 High Frequency: 13.56 MHz	13
1.4.3 Ultra High Frequency: 860 – 950 MHz	13
1.4.4 Microwave: above 2.0 GHz	14

1.5	RFID: a meta-technology	14
2	Basic Operating Principles	17
2.1	Electromagnetic Field	17
2.1.1	Near and Far Field	19
2.2	Radiated EM waves	20
2.2.1	Electric field strength	20
2.2.2	Polarization	21
2.2.3	Backscattering technique	22
2.3	UHF: Coupling between reader and tag	23
2.3.1	The channel model	24
2.3.2	UHF in near-field condition	25
3	UHF RFID EPCglobal Gen-2 Class-1	27
3.1	Protocol Overview	28
3.2	Data encoding	29
3.2.1	PIE Encoding	30
3.2.2	FM0 and Miller Encoding	30
3.3	Modulation Techniques	32
3.3.1	SSB-ASK and DSB-ASK	33
3.3.2	PR-ASK	35
3.4	Multiple and Dense Interrogator Mode	35
4	Critical Issues and Test Setup	39
4.1	Critical Issues and opportunities	39
4.1.1	Key parameters	41
4.2	Experimental Analysis	42
4.2.1	Testbed	43
4.2.2	Box and tags disposition	44
4.2.3	Transmitting antenna	45
4.2.4	RFID Reader	46
4.2.5	Boundary conditions	48
4.3	Performance metrics	49
5	Performance Evaluation	51
5.1	Preliminary evaluation	51
5.2	Experimental Results	54
5.2.1	Tilt impairment	55
5.2.2	Aggregated and Separated System Efficiency	56
5.2.3	Environment influence estimation	59
6	Susceptibility to in-channel radio interference	63
6.1	Sources of Interference	63
6.2	Experimental Results	65
6.2.1	Pure sine-wave	65
6.2.2	Wide-band Noise	66

6.2.3	In-channel Noise (SIR)	68
6.2.4	In-channel Noise (BW)	70
6.3	Remarks	71
7	Performance optimization	75
7.1	Operative Deductions	75
7.2	Performance optimization in non disturbed conditions	78
7.2.1	Redundancy	78
7.2.2	Reflective surfaces	78
7.3	Performance optimization in disturbed conditions – Immunity issues	83
7.4	Considerations	84
A	MINERVA Project	89
A.1	Main Components	89
A.1.1	Tmote Sky	89
A.1.2	SkyeModule M9	91
A.1.3	Linksys NSLU2	92
A.2	The MINERVA module	93
A.3	The MINERVA gateway	95
	Conclusions	88
	Bibliography	103

List of Figures

1.1	Active tag for the highways toll/access automatic system (Europe).	4
1.2	RFID examples.	5
1.3	Basic architecture of a RFID system.	8
1.4	Examples of tags shape.	9
1.5	Examples of tag enclosures: (a): LF and HF tags with coil shaped antennas; (b): tags are inserted inside a key; passive (c) and active (d) wristband for local monitoring applications (<i>i.e.</i> for children).	10
1.6	Examples of readers: (a), (b) fixed readers; (c), (d) handheld readers.	11
1.7	The simplest model for an RFID system: the device marked as “interrogator” (or “reader”) emits a signal to communicate with a second device, the “transponder” (or “tag”). The question mark identifies the interrogating device because its fundamental function is basically to broadcast a request for identification. On the other side, the basic function of a tag is to answer the interrogation, identifying itself. The communication protocol is based on radio frequency electromagnetic signals.	12
2.1	Example of the generation of an EM wave from a dipole antenna. Figures shows the evolution of the electric field E during half a period.	18
2.2	Configuration of the electric and magnetic vectors for a plane wave.	20
2.3	Polarization of electromagnetic waves. The linear polarization (a) is obtained with a simple dipole: the direction of the electric field E remains the same through propagation, and so do the magnetic field H (omitted here), which keeps orthogonal to E . The circular polarization (b) is obtaining combining the emissions of two dipoles, in quadrature. The resulting electric field E rotates its direction, and so do H (here omitted), maintaining its own direction orthogonal to the one of E .	21
3.1	PIE symbols referred to the time interval defined TARI.	30
3.2	FM0 encoding.	31

3.3	Miller encoding: baseband signals.	31
3.4	Miller sequence with sub-carrier contribution. The effect of the multiplication with a square wave with higher frequency has the direct effect of increasing the number of transition in the same interval of time. Considering Miller baseband signal (black traces), the number of phase reversal increase with M . As a consequence, at the operative frequency, the spectrum of tag's response is split into two contribution equally separated from the zero frequency, and spectral distance rises linearly with M	32
3.5	"Reader-to-tag" modulation. In (a), the the 010 baseband signal is shown, respecting TARI requirements of Fig. 3.1. (b) represents the modulating waveform which will be upconverted at the operative frequency, becoming (c) ($Mod_depth = \frac{A-B}{A}$). It's worth nothing that interval in which the modulated signal is attenuated is shorter in PR-ASK than DSB and SSB. In (d) the demodulated signals are shown: envelope is extracted, and phase is not used.	34
3.6	Examples of Dense-Interrogator-mode operation. (a): frequency hopping with 500 kHz maximum channel width; channel-boundary backscatter is admitted because there's no fixed adjacent channel. The communication shown implements PR-ASK, with 250 kHz of backscatter link frequency (BLF): a portion of the backscatter exits channel boundaries. (b): 200 kHz channel width, with 600 kHz spacing from each other: SSB-ASK is used to keep bandwidth narrow and maintain sufficient guard-band. In this configuration the backscatter spectrum is located in the spacing region between channels (300 kHz of BLF). (c): 500 kHz adjacent channels: communication spectrum must be all limited within boundaries.	36
4.1	Picture of the testbed adopted. The image shows the target of identification process, and a measurement antenna used to detect power levels.	42
4.2	Schematic view of the adopted testbed: measurement instrumentation is not shown (spectrum analyser, power meter and Radio Frequency (RF) measurement antennas).	43
4.3	(a) Container-box, (b) tagged boxes and (c) disposition.	44
4.4	Shape of tags used in the experiments.	45
4.5	Intermec IA39B antenna.	45
4.6	Radiation diagram of Intermec IA39B antenna.	46
4.7	Intermec IF5.	47
5.1	Alignment between reader and tag: (a) circularly polarized reader antenna, (b) parallel orientations of a linearly polarized tag antenna, (c) orthogonal orientation of a linearly polarized tag antenna.	52

5.2	Degradation of System Efficiency (SE) with a weakly tilted vertical antenna (5°), with respect the reference vertical one.	55
5.3	System Efficiency (SE) versus box-to-antenna distance d_s , measured for different $P_{r,dBm}$. The antenna is vertically oriented with respect to the ground floor.	57
5.4	SE versus d_s , at $P_{r,dBm} = 30$ dBm, for different orientations of the tags along x, y, z directions.	58
5.5	SE versus d_s , with tags all oriented along y and for different power levels $P_{r,dBm}$	59
5.6	Maximum distances d_{90}^* and d_{80}^* , above which a 90% and 80%, respectively, of tags are identified. The dashed lines represent the theoretical values of d_s^* estimated inverting eq. (5.1) with $k_f = 0$ and -2 dB.	60
6.1	Internal interference due to systems proximity. Interference contributions indicated as (c) and (d) are represented from one system to the other only, for reasons of order; however the symmetrical contribution is present as for (a) and (b).	64
6.2	Single tone interference, superimposed to reader's continuous wave.	65
6.3	Wide-band White Gaussian Noise, interfering on the whole channel.	67
6.4	SE versus d_s , at three different interference signal power levels (1 MHz bandwidth AWGN centered at 869.538MHz).	68
6.5	White Gaussian Noise with increasing bandwidth.	69
6.6	SE versus SIR measured at the container-box side. The full functionality is obtained only at very high values of SIR.	70
6.7	Signal To Interference Ratio (SIR) as a function of noise bandwidth.	71
6.8	SE versus interference bandwidth, with $P_i = -15$ dBm constant.	72
7.1	Comparison between SE measured using: (i) single dipole tags and one reader antenna Reader Antenna (RA); (ii) double orthogonal dipole tags, and one reader antenna RA; (iii) single dipole tags and two reader antennas RA, placed at the same distance d_s from the target boxes, along orthogonal directions.	77
7.2	Illustration of the direct path from reader to a tag, and reflected path coming back from a reflective surface.	79
7.3	Disposition of metallic surfaces. Considering the standard $\{x, y, z\}$ reference systems, in (a) the metallic plane is disposed under the tagged target, on xy directions; in (b), behind target, on yz directions.	80
7.4	SE_y (a) and SE_x (b) measured using metallic reflection surfaces, as illustrated in Fig. 7.3.	82
A.1	Front and Back of the Tmote Sky module.	90
A.2	Front and lateral of the SkyModule M9.	91

A.3	Linksys NSLU2.	93
A.4	The MINERVA Module, obtained combining a Radio Frequency Identification (RFID) reader module with a wireless sensor node.	94
A.5	Schematic view of the complete system: the module is used to set a wireless network of independent RFID readers, and through the wireless link data and other messages are transmitted to and from the gateway/base-station. The gateway forwards data in any IP network.	96

Acronyms

ASK	Amplitude Shift Keying
AWGN	Additive White Gaussian Noise
BAP	Battery Assisted Passive
BLF	Backscatter Link Frequency
BPSK	Binary Phase Shift-Keying
CDMA	Code Division Multiple Access
DoD	Department of Defence
DSB	Double Side Band
EAS	Electronic Article Surveillance
EM	Electromagnetic
EMC	Electromagnetic Compatibility
EMI	Electromagnetic interference
EOF	End of Frame
EPC	Electronic Product Code
FDM	Frequency Division Multiplexing
GNSS	Global Navigation Satellite System
HF	High Frequency
I²C	Inter Integrated Circuit
IA	Interference Antenna
IC	Integrated Circuit

IEEE	Institute of Electrical & Electronics Engineers
IFF	Identification Friend or Foe
ISM	Industrial, Scientific and Medical
ITF	Interrogator Talk First
LF	Low Frequency
MINERVA	Modular Instrumentation and Network Equipment for RFID Versatile Approach
NAS	Network Attached Storage
NFC	Near Field Communication
NSA	Normalized Site Attenuation
NSLU2	Network Storage Link for USB 2.0 Disk Drives
OOK	On-Off Keying
PIE	Pulse Interval Encoding
PR	Phase Reversal
RA	Reader Antenna
RF	Radio Frequency
RFID	Radio Frequency IDentification
SE	System Efficiency
SIR	Signal to Interference Ratio
SIR	Signal To Interference Ratio
SMA	SubMiniature version A
SNR	Signal to Noise Ratio
SNR	Signal to Noise Ratio
SOF	Start of Frame
SPI	Serial Peripheral Interface
SSB	Single Side Band

TTL	Transistor-Transistor Logic
UHF	Ultra High Frequency
USB	Universal Serial Bus
UWB	Ultra Wide Band
WSN	Wireless Sensor Network

Abstract

During the last years, the definition of “communication” has been rewritten by the viral diffusion of a class of devices which has been thought and created to open new and fast channels of interaction. The contraction they create on the space of communications is linked to a virtually instantaneous availability, so we all have access to anything, and in any place. Today, in this way, unimaginable amounts of information are transferred through wireless systems. With an image, we could say that the concept of voice has been amplified or even re-created: who could speak, now may go further, without even moving; moreover, inanimate objects have received the gift of speech. A virtual contracture of the world, in which anyone can talk and be listened to, by any other actor. In such a dimension, there must be a specific structured order, to make efficient this unique opportunity, and in this sense rules and strategies are necessary.

The whole work describe in these pages is inserted in the context of non wired communications.

On the whole and wide field of interest, recalling the image suggested, attention will be mainly focused on devices that give voice to otherwise inanimate things. We will talk about RFID systems, which are diffusing in many practical situations.

A RFID system is a very complex system that compresses and synthesizes many fields of study, including signal processing, the design of radio frequency circuits and antennas, networks and information systems, etc.. Down more specifically, attention will be primarily focused on systems developed for large-scale applications, such as the management of inventories, or the supply chain. In this context, the most promising technology utilizes electromagnetic waves in the Ultra High Frequency (UHF) spectrum, and passive devices with no internal power supply.

RFID is not a new technology, but it represents the maturity of a technology known since about seventy years. Despite of such an age, until the first of the nineties, the potential of technology in civil applications has not actually been experienced, and it came with the revolution in the supply chain and the per-

spective of continuous monitoring, tracking and localization.

In recent years, **RFID** technology continues to evolve and change, in the direction of improving reliability and minimize risk of error. Along these pages, **RFID UHF** technology will be carefully analysed, paying particular attention to reliability issues still open, and all aspects and strategies that can help to improve performance.

The effects of electromagnetic interference represent an innovative aspect of the work proposed. Because of the peculiar nature of **RFID** systems, disturbances on the communication channel can be interpreted from two points of view: as a random loss of function, still important and dangerous, and as voluntary noise. Knowledge of system behaviour in the presence of interfering agents is very important to assess risk situations and minimize consequences. The ultimate goal is to provide useful metrics to improve performance and increase the robustness of the **RFID** systems against interference, to designers of both hardware and protocols.

Sommario

Nel corso degli ultimi anni, la definizione di comunicazione è stata riscritta con metódica cura dalla diffusione virale di una classe di dispositivi pensati e creati per aprire nuovi rapidissimi canali di interazione. La contrattura dello spazio delle comunicazioni che essi generano è legata a una disponibilità praticamente istantanea, per cui ne abbiamo accesso tutti, e in qualsiasi luogo. Oggi, in questo modo, impensabili quantità di informazioni vengono trasferite attraverso sistemi senza fili. Con una immagine, potremmo dire che è stato amplificato o addirittura ricreato il concetto di voce: chi poteva parlare, ora può spingersi più in là, senza neppure muoversi; oggetti inanimati hanno ricevuto il dono della parola. Una contrattura virtuale del mondo, nel quale chiunque può parlare e farsi ascoltare, da qualsiasi altro attore. È naturale che deve esistere un ordine preciso e strutturato, per rendere fattiva questa straordinaria opportunità, e in questo senso si rendono necessarie regole e strategie.

Il contesto nel quale si innesta il lavoro descritto in queste pagine, è proprio quello delle comunicazioni non cablate.

Di tutto il vasto campo di interesse, l'attenzione sarà concentrata principalmente sui dispositivi che, nel paragone proposto, danno voce a "cose" altrimenti inanimate. Si tratta dei sistemi di identificazione a radio frequenza (RFID), che, seppur lentamente, si stanno diffondendo a macchia d'olio in un gran numero di situazioni pratiche.

Un sistema RFID è un sistema molto complesso che comprime e sintetizza numerosi campi di studio, tra i quali il processamento di segnali, la progettazione di circuiti a radio frequenza e di antenne, le reti e i sistemi informativi, ecc. Scendendo più nello specifico, l'attenzione sarà concentrata principalmente sui sistemi sviluppati per le applicazioni di larga scala, come ad esempio la gestione delle scorte di magazzino, o della catena di distribuzione, tra loro facilmente correlate. In questo contesto, i sistemi più promettenti sfruttano onde elettromagnetiche nello spettro UHF, e impiegano dispositivi passivi privi di circuiti interni di alimentazione.

I sistemi RFID di oggi non costituiscono una tecnologia nuova, ma la vicina

maturità di una tecnologia nota da almeno settanta anni. Nonostante questo, prima degli anni novanta non si è potuto sperimentare concretamente la potenzialità della tecnologia in ambiti civili, che è giunta con la rivoluzione della catena di distribuzione e la prospettiva del monitoraggio continuo, del tracciamento e della localizzazione.

In questi anni, la tecnologia dei sistemi **RFID** continua a evolversi e cambiare, nella direzione di migliorare l'affidabilità e ridurre al minimo i rischi di errore. In queste pagine verrà analizzata con cura la tecnologia dei sistemi **UHF**, ponendo particolare attenzione ai problemi di affidabilità ancora aperti, e a tutti gli aspetti e le strategie che possono aiutare a migliorare le prestazioni.

Un aspetto particolarmente innovativo del lavoro proposto riguarda lo studio sul campo degli effetti di interferenza elettromagnetica. Per la particolare natura dei sistemi **RFID** studiati, i disturbi del canale di comunicazione possono essere interpretati da due punti vista: sia in un'ottica di perdita di funzionalità casuale ma comunque importante e dannosa, sia in un'ottica di disturbo volontario. La conoscenza del comportamento del sistema in presenza di agenti di interferenza è molto importante al fine di valutare le situazioni di rischio e limitarne il più possibile le conseguenze.

L'obiettivo finale è fornire ai progettisti dell'hardware e dei protocolli un insieme di metriche e indicazioni utili a migliorare le prestazioni e aumentare la robustezza dei sistemi **RFID** contro l'interferenza.

Introduction

In the context of wireless devices, one of the most discussed vision is the “Internet of Things”. The basic idea of the “Internet of Things” is that any object or person or place can be part of a virtual system, in which any other has access. In this way, virtually anything became a living actor: the stage is of course the Internet, and from here the name.

Nowadays, good candidates for the “Internet of Things” are the [RFID](#) systems, which are diffusing everywhere for automatic identification applications. In [RFID](#) systems, in fact, each object is equipped with a smart label that allows the wireless communication and identification.

During the last ten years, [UHF](#) technology proved to be the most promising solution especially in large scale [RFID](#) application, for a wide set of reasons, and it is now diffused worldwide, mainly along the supply chain. This means that a very large number of objects are tagged with smart labels, and are ready for any application in which the automatic identification can be used to achieve some results: one for all, the substitution of bar-code.

In the present work, the performance of [UHF RFID](#) systems in real-world conditions are experimentally assessed. To this aim, suitable testbeds are used and experiments are performed in a set of real-life boundary conditions. The goal is twofold: from one side, the experimental investigation of the reliability in typical environmental conditions; from the other side, the deduction of helpful and practical hints for designers and technicians, with the aim of the efficient assessment and enhancement of performance.

0.1 Field of interest

Is now an established fact that the process of study and development of new technologies and new devices requires great interaction between a growing number of disciplines. A good example of this proliferation is given by the differentiation within the Institute of Electrical & Electronics Engineers ([IEEE](#)), and it’s interesting to notice that any technological improvement is based on

the contribution of several IEEE's societies, or even inspired them.

Considering a RFID system together with all its practical applications (both the ones foreseen for the future, and the actual ones), there are a great number of fields of interests involved, with either correlations coming from non technical disciplines. Using, for example, a bottom-up approach, from the design stage to real-life implementations, it is possible to recognized research areas such as:

- Circuits and solid-state circuits development;
- Microwave theory and techniques, signal processing, and communications;
- Antennas and propagation;
- Electromagnetic Compatibility (EMC);
- Instrumentation, measurement and reliability;
- Computer and computational intelligence;
- Automation and control systems;
- Industrial electronics and industry applications;
- Consumer electronics theory, and social implications;
- Systems and man cohabitation;
- Large scale economy.

Within these areas, the present work is set in the contexts of instrumentation and measurement, and electromagnetic compatibility.

Attention will be primarily focused on systems developed for large-scale applications, such as supply chain or management of inventories.

The most promising technology employs electromagnetic waves in the UHF spectrum, and passive devices with no internal power supply, so great effort has been done to measure performance and verify reliability when RFID systems implement real-life applications.

0.2 Motivation

Within the modern RFID scenario, UHF systems are playing an important role, with great expectations for the future, but *reliability* is still a critical issue. There exists several reasons, such as distances, in-channel interference, obstacles, wave reflections, the use of passive devices, an so on: all these aspects may

cause a significant degradation of the radio link, with predictable consequences on the overall performance.

To the aim of performance and reliability improvement, the design and setup of modern UHF systems is a topic widely studied and discussed worldwide in the scientific community, as documented in [1, 2, 3, 4, 5, 6]. Some helpful contributions to enhance the reliability are available in the scientific literature: *i.e.* interesting results have been obtained in terms of antenna design, tag power consumption and communication algorithms and protocols [7, 8, 9, 10]. Simulations and experimental tests have also been proposed in order to highlight RFID systems performance in some typical scenarios [5, 11, 12, 13], and efforts have been done to analyse band efficiency and to develop suitable informative structures [14].

However, these contributions lack of experimental results showing the actual performances that can be achieved by UHF RFID systems, the problems that can be encountered in practice and the corresponding solutions.

0.3 Contributions

0.3.1 Main contributions

With respect to the available literature, the analysis is conducted from an experimental point of view and original results are provided, showing the performance of UHF RFID systems in a variety of representative configurations. With respect the motivations given, the main contributions are related to the context of reliability, with particular interest in two areas:

- i. performance evaluation in real-life applications,
- ii. immunity issues due to electromagnetic interference.

In both analysis, critical aspects of UHF RFID systems are pointed out and helpful solutions are provided.

0.3.2 Other Contributions

As a corollary of the main research areas and other multidisciplinary interests involving wireless communications and Wireless Sensor Network (WSN), the possibility of fusion between them has been explored. In this sense, an application that embeds a RFID reader and WSN devices has been developed, to demonstrate that a small size and modular approach can help to reduce costs, and achieve grater versatility.

The development of this application has been named MINERVA¹ Project, and it is described in Appendix A.

0.3.3 Minor contributions

As highlighted in the previous sections, the main work focused on performance issues of RFID systems. However, the study of electromagnetic signals and communication protocols allowed the development of further relevant results in topics far from the RFID context, as here briefly mentioned.

One important result is documented in [15] where an approach has been proposed to evaluate the adequacy of anechoic enclosures that do not fulfil the requirements regarding the Normalized Site Attenuation (NSA) factor. In particular, important considerations are drawn from experimental measures, and simulation data.

The second contribution is related to the Global Navigation Satellite System (GNSS) context. As documented in [16], a detailed analysis of correlation properties of GPS and GALILEO modulated signals have been done, with the aim of proving that the authentication of the open signal can be achieved from short sequences of the encrypted ones. An algorithm has also been developed to evaluate the parameters needed for the correct authentication.

0.4 Structure

Chapter 1 A general introduction on RFID systems is here given. It describes the main elements and scenarios, useful to understand the wide variety of applications implemented with RFID systems.

Chapter 2 In this chapter some theory about the electromagnetic wave generation and transmission is given. The aim is to highlight the main physical principles, necessary to discuss the experimental results.

Chapter 3 The most diffused standard for UHF RFID systems is the EPC Global Gen-2 Class-1. In this chapter, particular attention is given to the protocol and to the communication issues related to both “reader-to-tag” and “tag-to-reader” wireless links.

Chapter 4 In this chapter, critical issues of a RFID system are discussed, mainly focusing on UHF implementations. Starting from the mentioned ineffi-

¹The name is the acronym of Modular Instrumentation and Network Equipment for RFID Versatile Approach (MINERVA).

ciencies, a testbed has been realized to verify and characterize them: the experimental setup is here described.

Chapter 5 Relations between the Electromagnetic (EM) field levels at the tag antenna and the overall performance of a UHF RFID system are investigated experimentally. The main purpose is to analyse phenomena involved, highlighting the importance of preliminary measurements in the setup and optimization of real-life systems.

Chapter 6 RFID wireless link is based on RF signals, hence potentially susceptible to Electromagnetic interference (EMI) phenomena. In this chapter, the susceptibility to in-channel interference is experimentally investigated.

Chapter 7 The knowledge of limits and their mechanism is important, because it gives the chance to obtain the desired performance through the proper tuning of system parameters and resources. Suitable rules are here described and verified.

Appendix In modern wireless communication context, WSNs are becoming quite popular. Starting from considerations on costs and versatility, a modular approach for RFID readers has been developed, interfacing and embedding a WSN node and a reader module. The possibility of mesh networks of readers has been demonstrated; furthermore a real-time data collection and a network interface system have been implemented to control the mesh of readers from the network.

Chapter 1

Introduction to RFID Systems

1.1 Radio Frequency Identification

In a great variety of contexts the automatic identification is used to improve process performance, *i.e.* from the access control to the traceability of items. There are several reasons, such as the reduction of both time required to complete a task, and number of mistakes, the precision and repeatability and so on: it's worth noting that all of them allow to reduce costs and improve service. Radio Frequency IDentification (**RFID**) represents a wireless communication technology used for automatic identification purposes, which is becoming so effective that the main application fields interested in the use of **RFID** systems include [11, 12, 17]:

- Aerospace,
- Apparel,
- Automotive,
- Chemical,
- Defence,
- Health care,
- Labelling,
- Logistics,
- Manufacturing,
- Packaging

- Pharmaceuticals,
- Retail.

The reasons of this growth can be found in the increasing reliability, together with the need of automation not requiring any manual interaction, and the decreasing costs of infrastructures and devices.

In such contexts, **RFID** is used to collect information from the identified objects, and/or track their position in a given monitored spatial volume [12]. This is typically accomplished through the use of one base station called *reader* a *transponder* or *tag*, to be placed close to the objects to be identified and/or tracked.

1.2 History of RFID

Nowadays, the **RFID** technology is demonstrating to be ready for a wide spread and employment in a great variety of application fields. However, **RFID** did not share the same process of development and evolution common among the most diffused and known wireless technologies, such as Bluetooth, WIFI, GSM, UMTS and so on.

1.2.1 The military contribution

The very first applications usually categorized as **RFID** are to be found before and during the Second World War, precisely in the context of the development of Identification Friend or Foe (**IFF**) systems.

In Britain, an **IFF** system using a device called *transponder* and mounted on vehicles was operative before the conflict: such device was employed to transmit a signal to the Chain Home Radar (the first RADAR system, in operation since 1939), to indicate that the aircraft under surveillance was friendly.

Starting with the MK-I system during the Second World War, **IFFs** were initially developed with separate equipment and antennas: they were successively incorporated to work with the main RADAR antenna. When **IFF** is active, the searching RADAR automatically sends interrogating pulses: the **IFF** unit in a friendly target will automatically respond with the correct reply and the same reply is made visible on operator's screen.

The MK-III **IFF** is considered the precursor of modern **IFF** systems, and it implements the co-location of **IFF** interrogator on the RADAR antenna, rotating with it to give directional indications. The same device also receives the response, so it was known as an "interrogator-responder" system. MK-III has a great historical importance, because it represents the first implementation

of the complete architecture of a RFID system. Furthermore, the technology of IFF transponder is still very important in a great number of applications in both military and civil contexts, one for all Satellite communications, and navigation systems: this is the reason why great effort is still dedicated to development and improvement, especially for what concerns new cryptographic and non-cryptographic protocols. The aim is to allow proper operation even in highly perturbed environments such as most war zones.

1.2.2 Development in civil context

The historical development of IFF systems shows that the basic principles of the RFID technology came from the military context, and they are strictly related to the identification applications implemented with RADARs and transponders. After the War, in the late 1948, the principles of modern RFID systems [18] were known and discussed, but the electronic technology suitable for a low cost realization was not mature enough. This is the main reason why the subsequent two decades there were no progress towards the modern architectures: all the effort has been spent to improve components in separate contexts.

'60s years

The first civil application appears at the end of '60s years, with the commercialization of the Electronic Article Surveillance (EAS) systems: they are commonly considered the first civil RFID applications. EAS systems use 1-bit transponders, which may be ON (1) or OFF (2). Items placed on the shelves carry transponders with bit set to ON: the status is changed to OFF only after payment, so the readers at the exit door do not react. Otherwise, any ON-transponder is detected and the alarm consequently activated.

EASs have been largely adopted as anti-theft systems, so they also have the primate for the first pervasive RFID application.

'70s years

The RFID architecture, as we know nowadays, has been essentially developed during the '70s, when the electronic circuits became integrated, more reliable, and cheaper. During these years, many laboratories, academies, and industries started to develop and produce circuits implementing identification through Radio Frequencies.

The first patents on RFID are documented at the beginning of 1973, and during the same year another patent has been assigned for the access control application: a reader hidden behind a door was set to control the unlocking system,



Figure 1.1: Active tag for the highways toll/access automatic system (Europe).

and the door was open only if a transponder with a correct identification number was detected by the reader.

Moving from a strict military context, the U.S. Government assigned resources to develop a system capable of tracking nuclear materials, which has been realized by Los Alamos Scientific Laboratory. Furthermore, many U.S. industries involved in military projects started to produce devices for civil applications: as an example, General Electric, Philips and others competed the first realization for the tracking of moving items and vehicles. The concept of putting a transponder in a civil vehicle came out during these years: the idea was to equip gates with a reader capable of recognizing vehicles and drivers to allow access to authorized personal only. The direct evolution of this system came during the '80s, coupling the access control with an automated payment system: it is still widely used worldwide to manage the toll for highways, tunnels and bridges.

It is interesting to note that, despite of such a ferment, the most important actors kept working independently: it was largely shared the conviction that technology was not mature enough to define official standards. The freedom for all the actors was considered essential to keep open the research and encourage the development of new ideas and the improvement of the technology. In this context, the RFID technology left laboratories and research in strict sense, to become the subject of a new interests with commercial targets.

'80s years

The '80s are commonly considered the period of the final implementation of the RFID technology, with a worldwide diffusion, even if limited within different contexts in each part of the world. In the U.S. the greatest interests were concentrated on the control and tracking of moving goods and vehicles, and on the access control of personal and people. On the other hand, in Europe, the fields of major efforts have been the identification of animals with short range

systems, and the toll/access management of the highways.

Other applications have been developed for the control of automated production lines, with important improvements in terms of robustness and reading range, but they kept to be too much expensive, so the employment was limited to particular high value applications and products.

'90s years

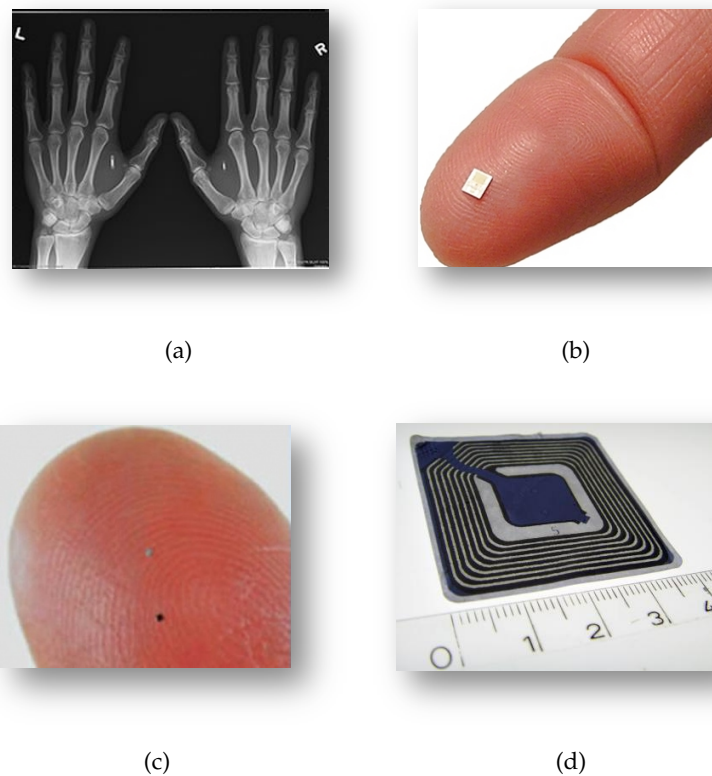


Figure 1.2: RFID examples.

Finally, during the '90s years the right conditions for the development of the modern technology were met. From one side, the shrinkage of integrated circuits allowed the miniaturization of RFID chips, together with a drastic reduction of power consumption, making the passive backscatter possible, as theorized in the late '40 [18]. Furthermore, with the shrinkage of the circuit size the target of drastic decrease of cost was finally met. On the other hand, the improvements of the process of the Integrated Circuit (IC) permitted to produce circuits carrying a small amount of non volatile memory, which can store the identification number and other information or data related to the carrying object.

Table 1.1: The Decades of RFID

Decade	Events
1940 – 1950	Development of IFF systems implementing the basic elements of a RFID system (World War II). Concepts of RFID discussed in the scientific community [18].
1950 – 1960	Research and laboratory experiments.
1960 – 1970	Development of the theory of RFID. Very first civil applications (EAS systems).
1970 – 1980	Explosion of RFID development. Early implementations.
1980 – 1990	Diffusion of commercial applications.
1990 – 2000	Codification of widely adopted standards. World wide diffusion.
2000 – ...	Development of new concept RFIDs and diffusion continues.

One of the most promising RFID technology, UHF, has been developed and patented during the early '90s, by IBM. The employment of ultra high frequencies offered wider read-range (a few meters under good conditions) and faster data transfer. IBM did some early pilots with Wal-Mart, and finally sold its patents to Intermec, a bar code systems provider: Intermec RFID systems have been installed in several different applications, from warehouse tracking to farming.

Despite of undeniable improvements, the technology was still expensive due to the low volume of sales and the lack of open, international standards.

The turning point has to be found in 1999, when the Uniform Code Council, EAN International, Procter & Gamble and Gillette funded the Auto-ID Center at the Massachusetts Institute of Technology. In this context, great effort has been done to investigate the possibility of putting low-cost RFID transponders on *any* product, to track them through the supply chain. The new idea was to avoid great amount of intelligence on transponder's chip, in order to keep it as cheap as possible: only an identification number should be stored. The complete information associated to the assigned item was not inside the transponder, any more, but in a database accessible over the Internet.

This assumption changed completely the point of view: previously, tags were a mobile database. With the new premise, RFID become a networking technology, linking objects to the Internet through the tag.

Between 1999 and 2003, the Auto-ID Center gained the support of a great number of companies, together with the U.S. Department of Defence (DoD) and many key RFID vendors. It developed two air interface protocols (Class 1 and Class 0), the Electronic Product Code (EPC) numbering scheme, and a network

architecture for looking up data associated on an RFID tag on the Internet. The technology was licensed to the Uniform Code Council in 2003, and the Uniform Code Council created EPCglobal, as a joint venture with EAN International, to commercialize EPC technology. EPCglobal ratified a second generation standard in December 2004, paving the way for broad adoption.

In the same years, with the aim of enabling pallet-level tracking of inventory, Wal-Mart issued a RFID mandate requiring its top suppliers to tag pallets with EPC labels. The DoD did soon the same with its top 100 suppliers. All this effort was motivated by the increased shipping, receiving and stocking efficiency and the decreased costs of labour, storage, and product loss that pallet-level visibility of inventory can offer.

1.2.3 Today

The lack of a shared standard largely penalized the diffusion and interoperability, mainly during '80s and '90s; the second generation of EPCglobal standard solved this situation, and made them possible. As a consequence, some of the biggest retailers in the world, such as Wal-Mart, and the U.S. Department of Defense decided to implement EPC technology to track goods in their supply chain. The pharmaceutical, tire, defence and other industries are also moving to adopt the technology.

Despite of a very long time spent in a sort of incubation state, RFID is nowadays moving to a mature stage and seems to be ready for a wide spread and employment for a variety of applications, across any industry and field in the *new economy*. These years, in particular, are very important because of the recent improvements of the integration technology of radio frequency circuits with traditional CMOS. New devices are being sold worldwide such as smart-labels, smart-phones, contactless payment systems, and they are changing the way of trading goods and money, integrating telecommunications, wireless networks, Internet, virtual money and so on.

From a strictly economical point of view, the most important achievement is the reduction of transponder's cost down to 0.05 Euro¹ or even less: this is the revolutionary turning point because it make sustainable the possibility of assigning an identification number to anything, and so the physical distribution of the information. In other words, these are the theorized basis for the *Internet of Things*: a worldwide connection in which any thing can interact and be digitally recognized, categorized and described through informations stored in its transponder or over the Internet.

¹UHF systems with passive tags.

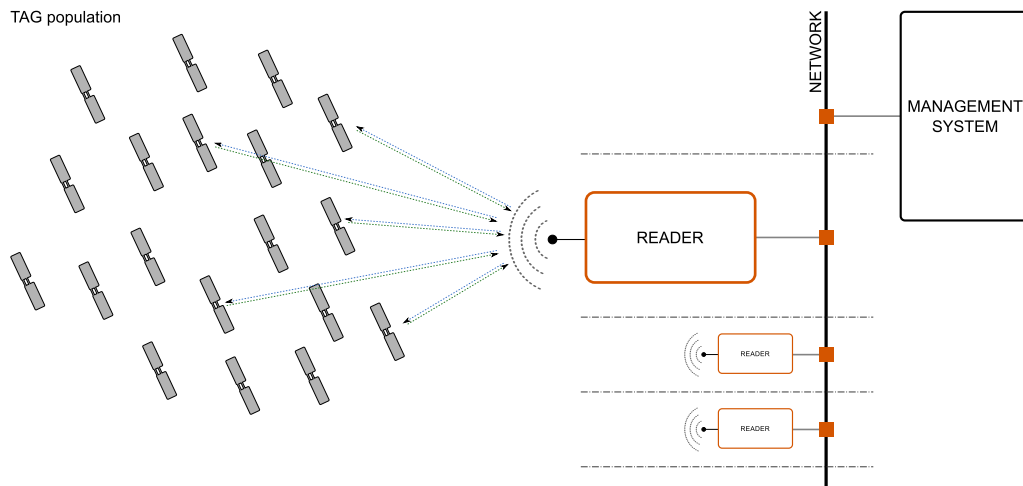


Figure 1.3: Basic architecture of a RFID system.

1.3 System components

Despite of a great variety of different technologies, any **RFID** system comprise three fundamental elements:

Transponder: the transponder is the radio-frequency responding device, usually placed on the item that has to be identified; it is also called *TAG*. The tag comprises an integrated circuit with logic and control functions (Fig. 1.2(b) and 1.2(c)), equipped with a small amount of memory. The circuit is connected to an antenna (Fig. 1.2), and everything is build in a plastic case which can have several shapes, depending on its function (label, Smart Card, key, etc.).

The memory is used to store an identification code, and some additional information: the circuitry allow to transmit data without physical contact, employing radio-frequency signals.

Reader: the reader is the interrogation device.

Management system: tags usually contain and transmit their identification code and some data. The management system, networked with readers, receives tags' ID and get the corresponding informations from its own databases (or from other databases over network or over Internet): data is than managed according to the purposes of the applications.

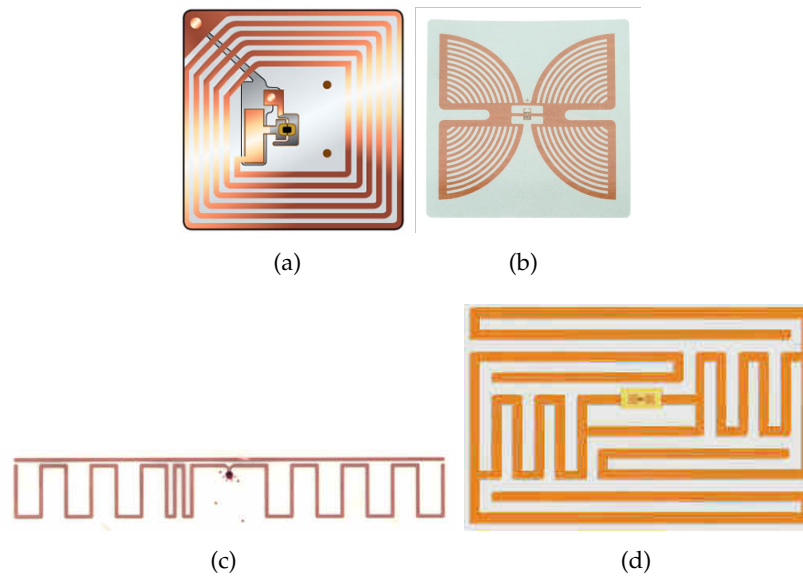


Figure 1.4: Examples of tags shape.

1.3.1 Transponders

Transponders or tags are commonly distinguished in three categories, based on their power supply.

Passive Tag: Transponders are usually defined as *passive*, if they have no internal source of energy, such as a battery. As a consequence they require an external electromagnetic field to obtain energy necessary to active internal circuitry and initiate a signal transmission; furthermore, they have no internal RF transmitter, but they use their antenna to backscatter the signal received from reader. The modulation of antenna's backscatter parameter allow the transmission of stored data. Reading range is limited from a few centimetres, to a few meters, depending on the operating frequency.

Battery Assisted Passive Tag: Battery Assisted Passive (BAP) tags are equipped with a battery, which is employed to feed the internal circuits, or other devices, *i.e.* sensors. Battery is not used to feed an internal active RF transmitter: they reflect reader's RF energy for communication, so the tag is said RF quiet (as passive). They require an external source to wake up but they have wider range, up to tens of meters.

Active Tags: circuitry of active devices are powered by an internal battery, that is also used to feed an active transceiver, so they do not need a reader to be activated. They are much more complex than the others, and they can be equipped with large *read* and *write* memories, and sensors. For the



Figure 1.5: Examples of tag enclosures: (a): LF and HF tags with coil shaped antennas; (b): tags are inserted inside a key; passive (c) and active (d) wristband for local monitoring applications (*i.e.* for children).

same reason, they are also more expensive. Active tags can operate with ranges of hundred of meters, depending on battery and transmitter.

1.3.2 The Reader

In a RFID system, the reader is the device that collect the information data contained in the tags. It is basically a fixed or mobile transceiver (Fig. 1.6), with a control circuitry usually connected to a network to communicate with the management system and transmit data.

Readers for passive and BAP tags, which are the most diffused, use electromagnetic waves to communicate with the target transponder, and they also transmit the signal that will be passively reflected as a response to the interrogation.

A great number of communication techniques is used for the tag-reader link, depending on application requirements such as reading range, data rate, number of tagged item, material penetration and so on, and all these features influence the operative frequency.



Figure 1.6: Examples of readers: (a), (b) fixed readers; (c), (d) handheld readers.

1.3.3 Middleware

Any RFID system is a complex machine made of many elements that must work together with order and coherence. The whole software system that connects local software components (*i.e.* reader's interfaces, users' client, web services, databases, etc.) and applications is usually addressed as *middleware*. Middleware consists of a set of services that allows multiple processes running on one or more machines to interact, and in this sense it allows the management system to communicate with readers and any other networked component, to the aim of the main application.

1.4 Operative frequencies

Radio frequency identification (RFID) is a wireless communication technology used for identification purposes. The identification process relies on a wireless communication link basically between two devices: the interrogator (reader) and one or more transponders (tags) (as represented in Fig. 1.7). The former is used to interrogate tags, which reply sending to the reader the stored data, that is typically the identification code (ID) of the tagged item.



Figure 1.7: The simplest model for an RFID system: the device marked as “interrogator” (or “reader”) emits a signal to communicate with a second device, the “transponder” (or “tag”). The question mark identifies the interrogating device because its fundamental function is basically to broadcast a request for identification. On the other side, the basic function of a tag is to answer the interrogation, identifying itself. The communication protocol is based on radio frequency electromagnetic signals.

Nowadays, several variants of RFID systems are known and employed. Their main differences are in terms of the following issues: the final application purpose, the range of frequency, the spatial range of the reader, the need of cryptography, the capability to operate in the proximity of reflective and dielectric materials, etc.

In general, RFID systems are classified considering the operative frequency of the wireless link. Such a classification is due to two main reasons: from one side most performance features are strictly related to the transmission characteristics of the electromagnetic signal. On the other side, the operative functionality is influenced by wavelength, and so are the coupling techniques used to allow the communication between reader and tag.

In this sense four main classes are identifiable.

1.4.1 Low Frequency: 120 – 145 kHz

Low Frequency (LF) sub-band in the range 120 – 145 kHz is the first that has been used for automatic identification. There are mainly two operative frequencies:

- 125.5 kHz, mainly used in automotive;
- 134.2 kHz, largely used for animals because the presence of water do not impede the transmission of the electromagnetic wave with this frequency.

Because of the electromagnetic properties of conductors in this frequency range, the reader-tag link is based on inductive coupling between their antennas, with the same principle of two coils in a transformer.

Read range for passive LF tags is in general limited to the diameter of reader's antenna, because further the intensity of magnetic field decreases inversely with the third power of distance, and so power coming back from the tag is inversely proportional to the sixth power of distance. For this reason, read and write tags have different ranges for the two operations, and in general, the maximum write distance is about a half of the read range, because of the higher energy needed to complete the operation.

The data rate of LF systems are limited to a range from 200 bit/s to a few thousands of bit per second: with such a low data rate, the identification of more than one single tag within the read range is not possible.

1.4.2 High Frequency: 13.56 MHz

High Frequency (HF) frequency band is allowed worldwide for RFID applications, so it has been for long the most employed.

The reader-tag link is obtained by inductive coupling, as in LF systems, so one tag is in general made of a coil shaped antenna, typically obtained cutting a single foil of copper or aluminium. The number of coils influence tag sensitivity, and so the read range.

HF technology is much more advanced with respect LF, even if they have much in common: HF tags for example implements anti collision algorithm that allow the access of multiple tags within the operative range of the reader.

Electromagnetic field in the HF band is not influenced by the presence of liquids, so it has been used for long for tracking in logistics, even if the possible read range is limited to about one meter.

Another diffused application for HF RFID is the "Contactless Smart Card". Short read range, together with the possibility of implementing larger memories and cryptographic algorithms made Smart Card the ideal candidate for secure payments, and the basis for the development of Near Field Communication (NFC) devices at 13.56 MHz.

1.4.3 Ultra High Frequency: 860 – 950 MHz

In UHF RFID systems, reader-tag coupling is based on electromagnetic transmission, as in traditional radio systems, feature that allow operating ranges wider with respect the ones obtained for LF and HF: in passive systems, three meters are quite common. This is the reason why this particular technology is

the perfect candidate for logistic applications, and management of the objects. With respect HF and LF, UHF signal has two limits that need the employment of specific devices, that is the high attenuation due to liquids, and the influence of metals on transmission. On the other hand, the communication link can reach high data rate (in the range of hundreds kilobit per second) and anti-collision algorithms have been implemented, allowing the identification of hundreds of tags per second.

1.4.4 Microwave: above 2.0 GHz

In this frequency band, devices working in the Industrial, Scientific and Medical (ISM) microwave band are included, that means, for example wireless networks, WLAN, Bluetooth, ZigBee, mainly for what concerns the 2.4 GHz interval. They have the same advantage of HF, that is, bands are recognized worldwide and so reserved also for RFID systems. The signals employed are quite similar to that used in UHF systems with the advantage that the higher frequency allow a further reduction of antenna size, but this correspond to a reduced capability of energy harvesting. However, the EM field can be easily concentrated on specific regions, and directive antenna can be use.

In the last years, devices traditionally used for wireless sensor network (*i.e.*: Bluetooth, Zigbee, etc.) are being absorbed, and used as very smart transponders in particular RFID applications. Furthermore, new applications changed the RFID paradigm of narrow band signalling, making use of Ultra Wide Band (UWB) signals. In this context, tags are complete transceivers which transmit short pulses: they are mainly used in precise localization applications.

1.5 RFID: a meta-technology

The previous paragraphs demonstrates that the evolution of RFID did not behave as a progressive enhancement and improvement of a well defined technology. Through the years, RFID maintained the essence of the acronym, that is Radio Frequency Identification, but this aim has been accomplished by means of many different devices and technologies. For this reason, the historical meaning of the acronym now represents a wide set of devices which implement the identification, and many other functions, operating through different physical principles.

Systems become even more intelligent and independent: the classical transponder as alternative for the bar-code is only the tip of the iceberg. In this sense, RFID should be considered a *meta-technology*, rather than one technology. A sort

of container in which it is possible to categorize all technologies implementing the automatic identification process, through radio frequency electromagnetic waves.

Chapter 2

Basic Operating Principles

In this chapter some theory about the electromagnetic wave generation and transmission is given. A more detailed analysis of all the phenomena involved, and the precise demonstrations of the assertions can be found in the bibliography, as suggested. In this context, the aim of the present chapter is to highlight the main principles behind a UHF RFID system, necessary to explain the experimental results.

2.1 Electromagnetic Field

The efficiency of a UHF RFID system strongly depends on the wireless link characteristics. In LF and HF RFID systems, the wireless link is obtained through the magnetic coupling between reader's and tag's antennas (generally coil-shaped antennas) [19]. The induced voltage in the tag's coil is rectified and used to power the internal circuitry: data is transferred generating another modulated magnetic field to be sensed by the reader, or modulating the impedance of the tag antenna, according to the data stream to be sent. Inductive coupling transfers impedance variation to the reader, together with the modulated information.

The main difference that distinguishes UHF RFID systems from the other architectures is related to the wavelength of the signal. It is very important because it influences reader's and tag's antennas coupling. In particular, in free space, when a signal is emitted from a conductor, the wavelength of the resulting electromagnetic wave (in Fig. 2.1 a representation of the behaviour of electric field in a dipole antenna) is calculated as the ratio of the speed of light and the frequency of the signal:

$$\lambda = \frac{c}{f} \quad (2.1)$$

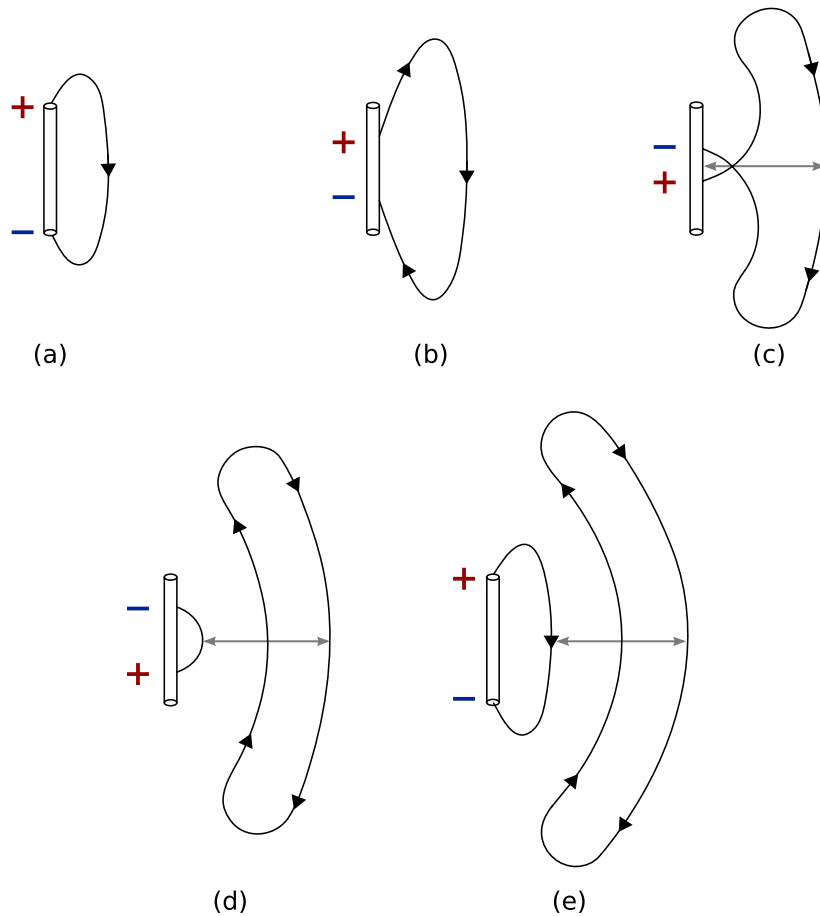


Figure 2.1: Example of the generation of an EM wave from a dipole antenna. Figures shows the evolution of the electric field E during half a period.

The operation of a **UHF RFID** system is essentially based on backscatter modulation, according to the following procedure:

1. the reader radiates an RF signal within its read range,
2. the tags receive and use this signal for energy supply,
3. once sufficiently supplied, tags modulate the scattering parameters of their embedded antennas according to the data stream to be delivered,
4. the reader measures the intensity of the reflected signals coming from the tags,
5. the reader deduces from these measures the data stream.

Table 2.1: Wavelength corresponding to the EM frequency commonly used for RFID applications.

Frequency	Wavelength [cm]
125 kHz	$2.4 \cdot 10^5$
13.56 MHz	$2.2 \cdot 10^3$
433 MHz	62.3
868 MHz	34.6
915 MHz	32.8
2.40 GHz	12.5
5.80 GHz	5.2

2.1.1 Near and Far Field

The effectiveness of the described mechanism strictly depends on the spatial region in which the tags operate with respect to the reader antenna position. Such regions are typically denoted as “near-field” and “far-field” regions: they are separated by a boundary that depends on the main dimension of the generating antenna.

Considering antennas whose largest dimension is smaller than wavelength λ (this may be the condition of a conductor loop, or a folded dipole), at a distance:

$$r_0 = \frac{\lambda}{2\pi} \quad (2.2)$$

the electromagnetic field begins to separate from the antenna into space in the form of an electromagnetic wave. The volume from the antenna to the point where the electromagnetic field forms is called the “near-field” of the antenna. The region after the point at which the electromagnetic wave has fully formed and separated from the antenna is called the “far-field”.

Eq. (2.2) holds for antennas smaller than the wavelength; considering larger dimensions, that is, greater than λ , the approximations given for the boundary is:

$$r_0 = \frac{2D^2}{\lambda} \quad (2.3)$$

where r_0 is the distance between the boundary and reader’s antenna, and D is the antenna maximum dimension.

The values collected in Table 2.1 show that before UHF systems, there was no emission from reader’s antennas: the distance of emission (r_0 , the boundary of the far-field region) is too large, and the decay of the magnetic field goes with the third power of the distance [19], so at r_0 the EM field is too weak to emit. Inductive coupling was the only the mechanism available, so the system reader/tag was similar to a transformer.

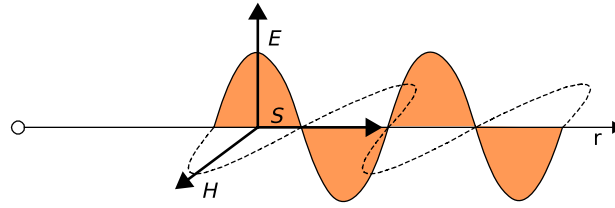


Figure 2.2: Configuration of the electric and magnetic vectors for a plane wave.

On the other hand, the employment of higher frequencies reduces the boundary distance, and electromagnetic emission can take place. This is fundamental because the free space attenuation only is relevant for the electromagnetic waves.

2.2 Radiated EM waves

2.2.1 Electric field strength

Once that the electromagnetic wave separates from the emitting antenna, it propagates through the space, transporting energy. In condition of spherical or isotropic emitter, energy radiates uniformly in all directions, so the radiation density S (defined as the radiation power per unit area) can be easily calculated as:

$$S = \frac{P_{EIRP}}{4\pi r^2} \quad (2.4)$$

where P_{EIRP} (Effective/Equivalent Isotropically Radiated Power) is the amount of power emitted by a theoretical isotropic antenna, equally distributed in all directions.

From the theoretical analysis of the electromagnetic propagation, an EM wave is described by the evolutions of its vectors \mathbf{E} and \mathbf{H} , in time and in space (see Fig. 2.2). Precise relations hold between the two vectors and radiation density [19, 20]:

$$\mathbf{S} = \mathbf{E} \times \mathbf{H} \quad (2.5)$$

and in vacuum condition, with an isotropic emitter, the electric field strength can be obtained by the following:

$$E = \sqrt{\frac{P_{EIRP} \cdot Z_F}{4\pi r^2}} \quad (2.6)$$

where r indicates the distance from the emitting source, and Z_F the characteristic wave impedance.

This equation is very important, because it demonstrates that the attenua-

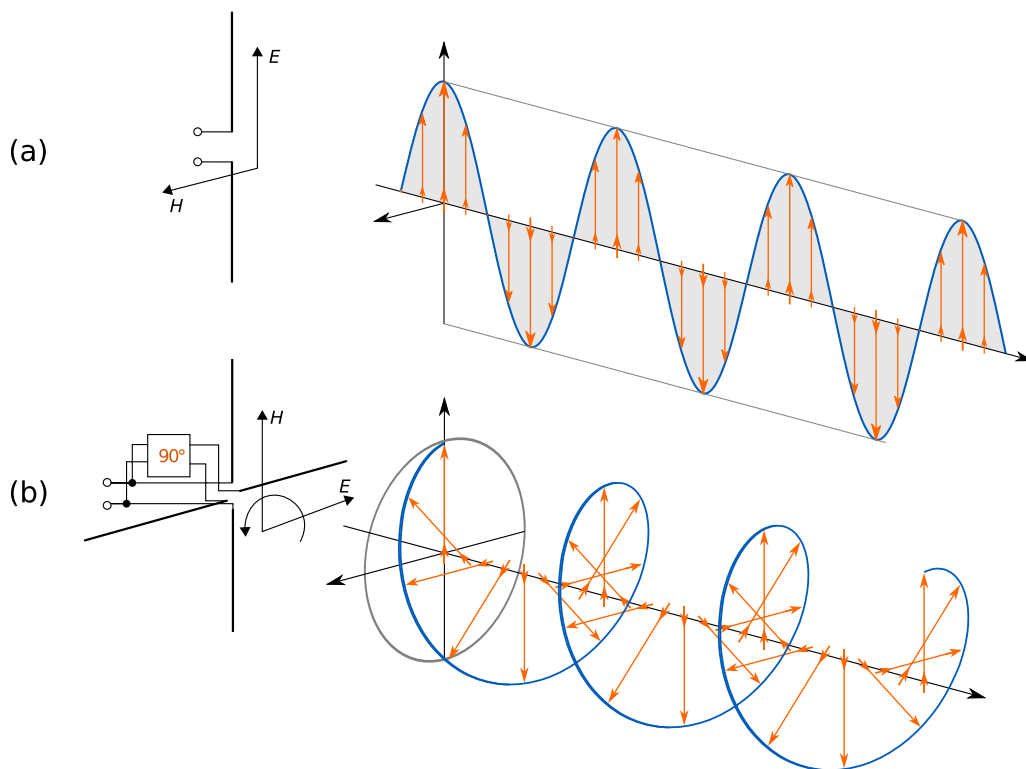


Figure 2.3: Polarization of electromagnetic waves. The linear polarization (a) is obtained with a simple dipole: the direction of the electric field \mathbf{E} remains the same through propagation, and so do the magnetic field \mathbf{H} (omitted here), which keeps orthogonal to \mathbf{E} . The circular polarization (b) is obtained combining the emissions of two dipoles, in quadrature. The resulting electric field \mathbf{E} rotates its direction, and so do \mathbf{H} (here omitted), maintaining its own direction orthogonal to the one of \mathbf{E} .

tion of an electromagnetic wave is inversely proportional with the distance. The magnetic field strength in inductive coupled devices, instead, decays with the third power of distance, so UHF devices ensure wider reading ranges.

2.2.2 Polarization

The polarisation of an electromagnetic wave is the property that describes the direction of the oscillation, in particular the oscillation of the electric field. The polarization of electromagnetic waves commonly has two distinctions: the *linear* and the *circular* polarization. These alternatives are two special cases of the most general elliptical polarization.

In linear polarisation the direction of the field lines of the electric field \mathbf{E} remain the same during propagation, and it is usually distinguished in *vertical* and *horizontal*, in relation to the surface of the earth. The dipole antenna is a linear polarised antenna in which the electric field lines run parallel to the

dipole axis.

The circular polarization is obtained coupling two orthogonal dipoles, each one emitting the same electric field, but in quadrature. In other words, one dipole is fed via a $\lambda/4$ delay line (Fig. 2.3). In this configuration, direction of the electromagnetic field generated completely rotates (2π) each progression of one wavelength in space. The rotation direction of the field can be determined by the arrangement of the delay line: there are two alternatives, left-handed and right-handed circular polarisation.

Modulating the amplitude of the electric field at the collector of the two dipoles, the resulting polarization is elliptical: the delay line set the direction of rotation and the slope of the ellipse main axis.

2.2.3 Backscattering technique

In real life conditions, an electromagnetic wave propagating in the space interacts with the environment: it hits objects and surfaces, that react to the incident energy. In general, a portion of the incident energy is absorbed (or transmitted in certain condition), and the remaining portion is reflected, or scattered in any direction, with varying intensity. A small fraction of the scattered energy can come back to the emitting antenna.

In UHF RFID systems the reflected signal carries data stored inside tags. In other words, the principle is the one of RADAR, in which the backscattering properties of the target must be optimized to improve detectability and so the efficiency of the communication scheme. In this sense, any tag is characterized by its own *radar cross-section*, σ , that indicates the power backscattered by its antenna, given a certain incident power density.

Using again the hypothesis of isotropic emitter, the power transmitted from reader's antenna can be indicated as P_{EIRP} . Such power propagates equally in all direction of space. The radiation density S that reaches transponder's antenna can easily be calculated using eq. (2.4), and the power backscattered by tag antenna is given by:

$$P_S = \sigma \cdot S \quad (2.7)$$

where σ is the radar cross-section, or *scattering area*, and it has the dimension of a surface.

Considering the tag as another isotropic emitter, eq. (2.4) holds and the power density that reaches the reader's antenna is:

$$P_{Sback} = \frac{P_S}{4\pi r^2} = S \cdot \frac{\sigma}{4\pi r^2} = \frac{P_{EIRP}}{4\pi r^2} \cdot \frac{\sigma}{4\pi r^2} = \frac{P_{EIRP}}{(4\pi)^2} \cdot \frac{\sigma}{r^4} \quad (2.8)$$

Eq. (2.8) demonstrates that, given the reader's output power, the most significant parameter is the radar cross section of the tag. The radar cross-section depends upon a wide set of parameters, such as the physical size, the shape, material, surface structure, and so on.

Taking into account the features of the electromagnetic wave itself, the cross section is also influenced by polarization and wavelength. The dependence on wavelength plays such an important role, so objects are divided into three categories:

Rayleigh: the wavelength of the incident wave is large compared to the dimensions. As an example of expected behaviour, the cross-section exhibits a λ^{-4} dependency for objects whose main dimension is about half the wavelength. For larger dimensions, σ can be considered negligible.

Resonant: the main dimension is comparable with the wavelength. In this condition, small variations in the wavelength, or in the geometry, may cause significant positive fluctuations on σ . This is the reason why the best performance are achievable if the antenna of the transponder is tuned to the operative frequency (that is its own resonance frequency).

Optical: object dimensions are smaller than the wavelength. In this condition, cross-section is influenced by geometry of incidence, only, that is position and angle of incidence.

2.3 UHF: Coupling between reader and tag

In the context of UHF RFID systems, there are mainly three categories of tags: passive tag, BAP tags, and active tags. In both passive and BAP tags, the communication with the reader is managed modulating the incident electromagnetic wave; passive tags differ because they also feed their internal circuits using part of the incident energy. As said, the greatest interest is concentrated on passive tags, because, despite of a simpler architecture, their cost allows the massive employment. Nevertheless, the efficiency of the mechanism of transmission and retransmission is vital to ensure the proper functionality of the whole system. In particular, the power that reaches tags' antenna is a fundamental parameter, because it influences both the activation of the circuits, and the power level of the backscattered signal.

2.3.1 The channel model

Considering a typical UHF RFID application, the operating frequency may be set to 868 MHz, that corresponds to $\lambda = 34.6$ cm (refer to Table 2.1). This configuration gives two alternatives to the boundary distance, which distinguishes the near-field and far-field regions.

For any reader antenna with main dimension D smaller than the wavelength, that is $D < 34.6$ cm, r_0 is independent of D :

$$r_0 = \frac{\lambda}{2\pi} \cong 5.5 \text{ cm} \quad (2.9)$$

On the other hand, for any reader antennas with $D > 34.6$ cm, r_0 depends on the main dimension and:

$$r_0 = \frac{2D^2}{\lambda} \cong 1.43 \text{ m} \quad (2.10)$$

As a consequence, for a typical antenna of 0.5 m maximum dimension, all tags positioned at a distance $d < 1.43$ m from the reader's antenna operate in the near-field region.

In general, the power P_t received and available at the tag antenna output connector can be determined as follows:

$$P_t = P_r \cdot \rho \cdot C, \quad (2.11)$$

where P_r is the power at the input connector of the reader antenna, ρ is the impedance matching coefficient between the reader and its antenna, and C is the coupling coefficient between the reader's and tag's antennas [21].

In UHF RFID systems, critical conditions are met far from reader's antenna, where it is important to maintain high power levels to activate passive tags and to ensure an observable backscattered signal. Such configuration allows UHF systems to operate in far-field conditions both at the reader and tags side. In these conditions, the radiated electric and magnetic fields propagate as a plane wave, perpendicular one with another and to the wave propagation direction and C can be expressed as follows:

$$C = G_t \cdot L_p \cdot G_r \cdot p, \quad (2.12)$$

where G_r and G_t are reader's and tag's antenna gains, respectively; p is the polarization mismatch coefficient between them, and L_p is the path loss, that is the attenuation due to propagation in space.

According to the Friis Transmission Equation [22], path loss in free space can

be determined as:

$$L_p = \left(\frac{\lambda}{4\pi d} \right)^2, \quad (2.13)$$

where d is the distance between reader's antenna and tag.

Considering an ideal matching between the reader and its antenna ($\rho = 1$), P_t in (2.11) and in dBm units changes into¹:

$$P_{t,dBm} = P_{r,dBm} + G_{t,dB} + G_{r,dB} + p_{dB} + 20 \cdot \log_{10} \left(\frac{\lambda}{4\pi d} \right), \quad (2.14)$$

Eq. (2.14) can be used only in the far-field region and in free space conditions, that is, quite rarely in many practical RFID applications. Systems, in fact, often operate in the proximity, or inside, dielectric and metallic materials, such as plastic, liquids, conductive enclosures, in which phenomena like shielding, attenuation and multipath fading may easily occur. In these circumstances, (2.14) can still be used in the following modified version:

$$P_{t,dBm} = P_{r,dBm} + G_{t,dB} + G_{r,dB} + p_{dB} + k_{f,dB} + 20 \cdot \log_{10} \left(\frac{\lambda}{4\pi d} \right), \quad (2.15)$$

where k_f (or $k_{f,dB} = 10 \log_{10} k_f$) is a correction factor to be suitably determined, for instance through measurements.

2.3.2 UHF in near-field condition

The behaviour of the EM field in the near-field region is not uniform, so two sub-regions are usually identified. The first is very close to the antenna, and it is called *reactive region*, because the electromagnetic energy is not radiated yet (see Fig. 2.1(a)). The second region is farther, and here the EM energy is radiated but the angular relationship between the magnetic and electric field is dependent on the distance from the antenna. The approximation of plane wave is still not valid. In these sub-regions, the magnetic component of the electromagnetic field is still substantial, so the behaviour is similar to that of inductive coupled system, such as HFs. In particular, UHF tags operate as HF tags, with interesting advantages such as an increased detectability in the proximity of dielectric and conductive materials, e.g. liquids, carton/plastic boxes, shields, etc.[21].

¹ $P_{t,dBm} = 10 \cdot \log_{10} P_t / 1mW$, $P_{r,dBm} = 10 \cdot \log_{10} P_r / 1mW$,
 $G_{t,dB} = 10 \cdot \log_{10} G_t$, $G_{r,dB} = 10 \cdot \log_{10} G_r$, $p_{dB} = 10 \cdot \log_{10} p$.

Chapter 3

UHF RFID EPCglobal Gen-2 Class-1

Today, the EPC Global is the reference standard for UHF RFID applications most widely accepted worldwide. From 2005, the Second Generation (Gen-2) has significantly enhanced the conditions for a wide implementation of UHF RFID technology, guaranteeing global interoperability and royalty freedom, together with performance improvements.

The standard defines the physical and logical requirements for RFID systems operating in the 860 – 960 MHz frequency range. In such systems, the interrogator, or reader, modulates a radio frequency (RF) carrier in the range 860 – 960 MHz, sending information to the passive tag.

The tag is said passive (Class-1) because it receives the needed supply energy from the RF signal transmitted by the reader. With the collected energy, the tag is subsequently enabled to send back to the reader information like its own ID, further storage data and possible readings from connected sensors. This second transmission is performed by the tag through the modulation of its antenna reflection coefficient, according to a backscattering technique [23]. An informative structure connected to the reader is finally used to collect and process data.

The standard can be considered an extension of the previous EPC UHF protocol Generation-1 and of the ISO 18000-6 protocol [23]. It also adds new features in order to improve the system performance. In particular, the document provides specifications for:

- physical interaction between reader and tag;
- reader and tag operating procedures and commands;
- collision arbitration scheme used to address a specific tag in a multiple-tag environment;

- EPC identifier;
- tag ID;
- “kill” function for permanently disabling a tag;
- optional password-protected access control;
- optional user memory.

Moreover, further documentation is provided in order to define the needed signalling in the case of coexistence of many readers within the same area. The standard also identifies three possible combinations: single, multiple, and dense interrogator modes, suggesting strategies (time-division and frequency-division multiplexing) to prevent mutual interference among different interrogators, and avoid collisions among tag responses.

3.1 Protocol Overview

The standard defines the physical and logical requirements for RFID systems working in the 860 – 960 MHz frequency range, coherently with a Interrogator Talk First (ITF) scheme implementing a random-slotted collision arbitration. As defined in the protocol, the main action comes from the interrogator or reader: it communicates with tags modulating a RF carrier wave, employing mainly three different modulation schemes:

- Double Side Band (DSB) Amplitude Shift Keying (ASK);
- Single Side Band (SSB) Amplitude Shift Keying;
- Phase Reversal (PR) Amplitude Shift Keying;

Tags must be able to demodulate each modulation scheme. The standard sets stringent requirements on the data format and codification. Systems with passive tags cannot rely on precise timing and synchronization circuits on board, bandwidth is limited and power transmission must be optimized to activate tags: all these factors make the coding schemes vital to ensure proper functionality. In the “reader-to-tag” communication, it’s important to maximize energy transfer to target tag, for this reason the standard specifies an encoding scheme based on the length of impulses: Pulse Interval Encoding (PIE).

Passive tags (Class-1) do not have an internal power supply: they are powered by the modulated carrier. Once powered, the tag is ready to answer to the interrogator. The power supplied by the modulated RF signal is not sufficient

for the transmission, so once that the interrogation message ends, the reader continues to emit the RF carrier unmodulated, sensing for a backscatter reply. Powered and addressed tag does not spend energy to transmit a signal, it modulates amplitude or the phase of the continuous wave emitted by the reader, changing the scattering parameter (or reflection parameter) of its own antenna. Again, in the “tag-to-reader” communication, the data stream format is not arbitrary, it is selected by the interrogator, and set to FM0 or Miller-modulated subcarrier. It’s worth noting that all these encoding schemes are based on transitions, so any sequence is self-temporized.

The second generation of the standard defines three main operations, available at the reader side to address the tags:

SELECT: this operation allows to set conditions before a inventory, in order to address only a subset of the population of tags: in this sense, it is possible to target only the tags whose memory contains a precise code or EPC field, making more efficient and rapid the operation of inventory. Furthermore, the *select* condition can be set by the operator employing typical logical condition, such as in a database (negation, union, intersection, etc.).

INVENTORY: the *inventory* operation is used to identify tags within reader’s field. The standard defines the procedure in order to identify each tag, one by one, resolving conflicts and superimpositions, and setting suitable flags: this is mandatory because an inventory round operates in one only session per time.

ACCESS: once terminated the inventory operation, the reader can address a single precise tag and communicate exclusively with it. *Access* allow the reader to operate on the memory of the tag, to read and write it, and to modify the tag future state, *i.e.* killing it.

3.2 Data encoding

As said, data encoding is well defined inside the standard. In any passive system, in fact, there are a lot key parameters that may affect the communication, so the proper encoding scheme must be chosen.

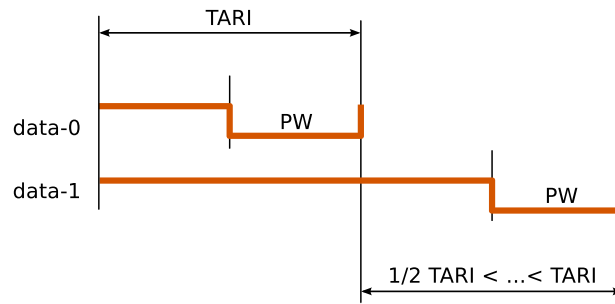


Figure 3.1: PIE symbols referred to the time interval defined TARI.

3.2.1 PIE Encoding

The “reader-to-tag” link employs PIE, as shown in Fig. 3.1. The scheme is based on a reference time interval called TARI, which corresponds to the duration of “data-0”. As shown in Fig. 3.1, PIE maximizes the high level of the symbol which corresponds to the continuous RF wave. On the other hand, low values correspond to the attenuated continuous RF wave, so the energy transfer is optimized.

It’s worth noting that bits “0”, “1”, and all the special symbols such as Start of Frame (SOF) or End of Frame (EOF) are a compositions of multiple TARI periods: as a consequence, bit sequences with the same number of bit may have different length once encoded. This aspect is convenient in terms of energy transfer, and does not represent a limit because the sequence is self-timed.

The width of TARI impulse is also important because it defines the minimum width of the modulated signal. In other words TARI is responsible of the bandwidth of the resulting RF signal: the lower TARI is, the larger is the spectral distribution. This is the reason why many values of TARI are admissible (6.25, 12.5, 25.0 μ s), in order to respect regulations on spectral emissions which vary depending on regional policies.

3.2.2 FM0 and Miller Encoding

In the “tag-to-reader” communication, the interrogator decide the encoding scheme for the backscattered signal, which can be FM0 or Miller. The most important feature of both encoding techniques is the absence of spectral component at the central frequency (or zero frequency, in baseband). This characteristic is essential for the correct detection of the backscattered signal, at the reader side: tags, in fact, do not generate an independent signal, but they reflect a RF carrier. At the reader side, it is sufficient to filter the main signal (the continuous wave), to reveal the backscattered signal, which is much weaker (as

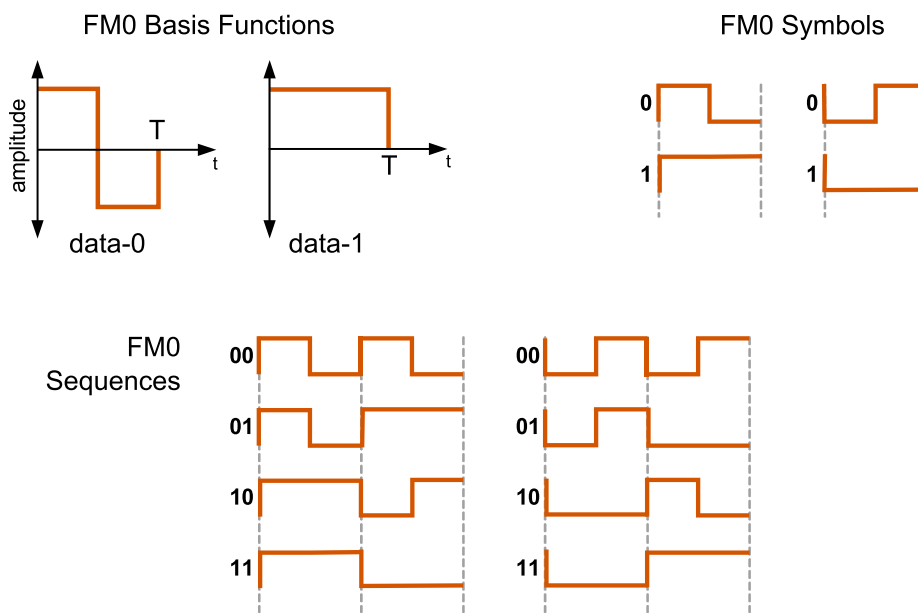


Figure 3.2: FM0 encoding.

described in eq. (2.8).

As shown in Fig. 3.2, each bit occupies a well defined time slot, which is two half-bits. In FM0 encoding, the basis signal takes one time slot, with a base-band phase inversion at the beginning, and an additional mid-symbol phase inversion for “data-0”.

Miller encoding has a few similarities with FM0: each time slot is split in two, and signals are the same, with symbols inverted, as shown in Fig. 3.3. The transition scheme is instead quite different: the mid-symbol inversion occurs with “data-1”, and phase reversal occurs between a sequence of two equal symbols (“data-0” or “data-1”), otherwise it is maintained. Furthermore, the waveform to be transmitted is obtained multiplying the baseband signal by a square wave, with a higher frequency compared with the symbol rate. The ratio between the square frequency and symbol rate is indicated as M . The increment

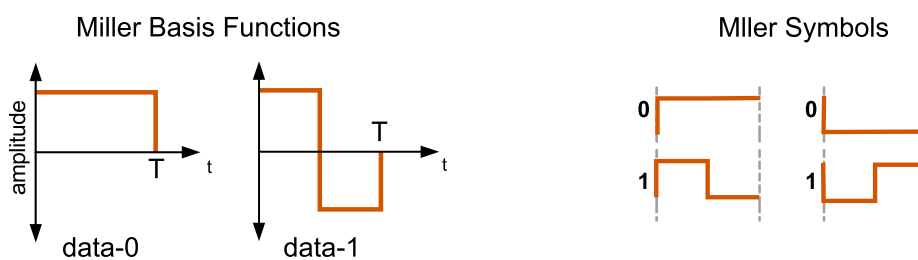


Figure 3.3: Miller encoding: baseband signals.

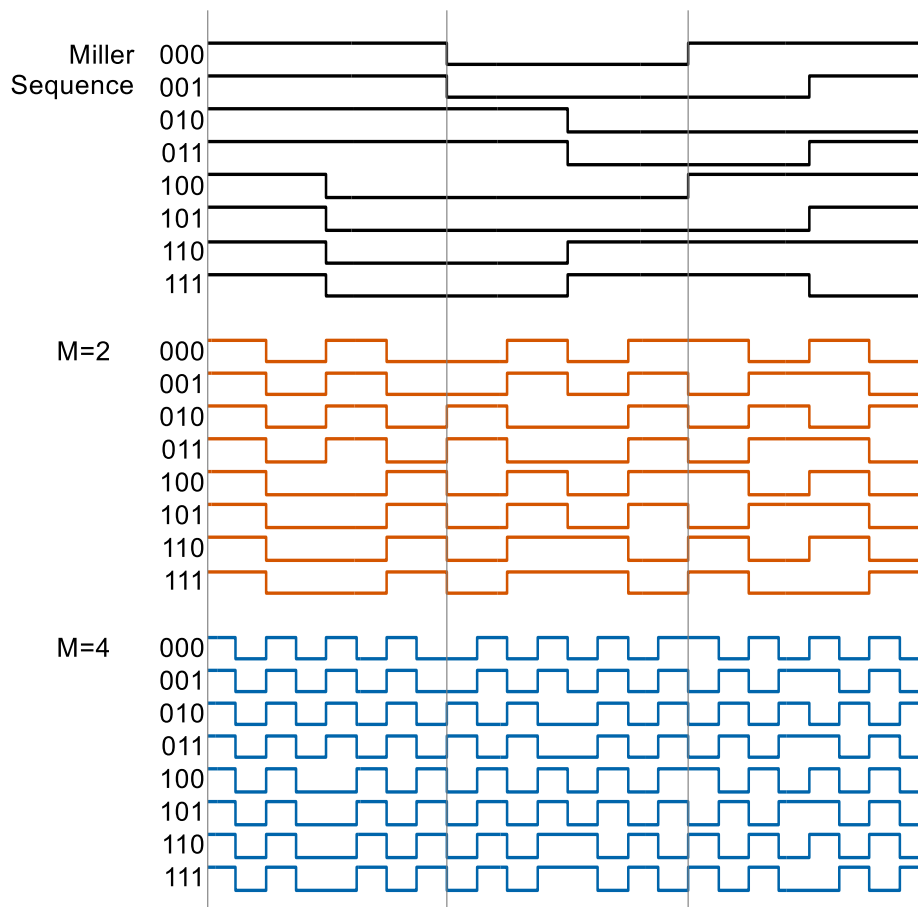


Figure 3.4: Miller sequence with sub-carrier contribution. The effect of the multiplication with a square wave with higher frequency has the direct effect of increasing the number of transition in the same interval of time. Considering Miller baseband signal (black traces), the number of phase reversal increase with M . As a consequence, at the operative frequency, the spectrum of tag's response is split into two contribution equally separated from the zero frequency, and spectral distance rises linearly with M .

by a factor M of the number of transitions in the same time interval (see Fig. 3.4) has an important consequence in frequency domain. The tag signal has no component at the central frequency, because it is divided in two sub-carriers, located farther as M increases. Fig. 3.6 can help: the higher M , the farther the lateral lobes are placed, and the reader can better filter the central frequency component and discriminate the backscattered signal.

3.3 Modulation Techniques

In the communication between reader and tag, modulation techniques must guarantee low complexity in order to avoid the implementation of dedicated

circuitry which may have bad consequences. First of all, demodulation circuits are area consuming on tag chip, which increases linearly the cost of a single tag. Greater chips equipped with advanced demodulation units have necessarily higher power consumption. In passive tags the energy is too much precious because it discriminates between an active tag with a non responding one.

For all these reasons, the most common modulation techniques are the one listed in the previous sections. The simplest modulation scheme is the Amplitude Shift Keying (ASK), in which the amplitude of the carrier wave is modulated by the binary stream. The *high* and *low* levels of amplitude corresponding to binary values "1" and "0" may vary. In passive RFID context, energy transfer is optimized to maintain constant the amplitude, so modulation depth¹ should be maintained low, as a trade-off with the efficiency of the communication.

The compliance with regional regulation may need narrow spectral contents, so ASK can be implemented in two ways: Single and Double Side Band (SSB and DSB), which mainly differ in bandwidth.

An alternative to SSB and DSB is Phase-Reversal (PR) ASK that implements a phase reversal when the modulation signal is low. Such an approach is quite similar to Binary Phase Shift-Keying (BPSK) used in digital communications, but in this context demodulation scheme detects and processes RF carrier envelope, so the baseband signal is not obtained from phase, rather from amplitude.

3.3.1 SSB-ASK and DSB-ASK

ASK modulation techniques provide very poor performance in terms of spectral width for a given bit-rate. In particular, DSB-ASK is the less efficient technique, but with OOK it shows the simplest implementation. SSB-ASK has been developed to enhance the spectral efficiency, in particular for those regions in which regulations fix strict limits. SSB-ASK and DSB-ASK share the same modulation signals, as shown in Fig. 3.5, but the first has half the spectral content than the second. In SSB, in fact, the up-conversion stage moves to the operative frequency the real portion only of the symmetric baseband spectrum (it contains the complete information, being the baseband signal real, Fig. 3.6(b)).

Signal to Noise performance of both ASK techniques is strictly dependant on the *modulation depth* (as defined in Fig. 3.5). The best performance is obtained for a 100% modulation depth, that corresponds to the ON-OFF Keying (OOK) modulation. OOK modulation ensures higher values of Signal to Noise

¹The modulation depth is generally calculated as the ratio of the difference between the highest and lowest amplitude levels, over the greater one (in Fig. 3.5: $Mod_depth = \frac{A-B}{A}$). When the lower level is 0, the modulation is defined On-Off Keying (OOK).

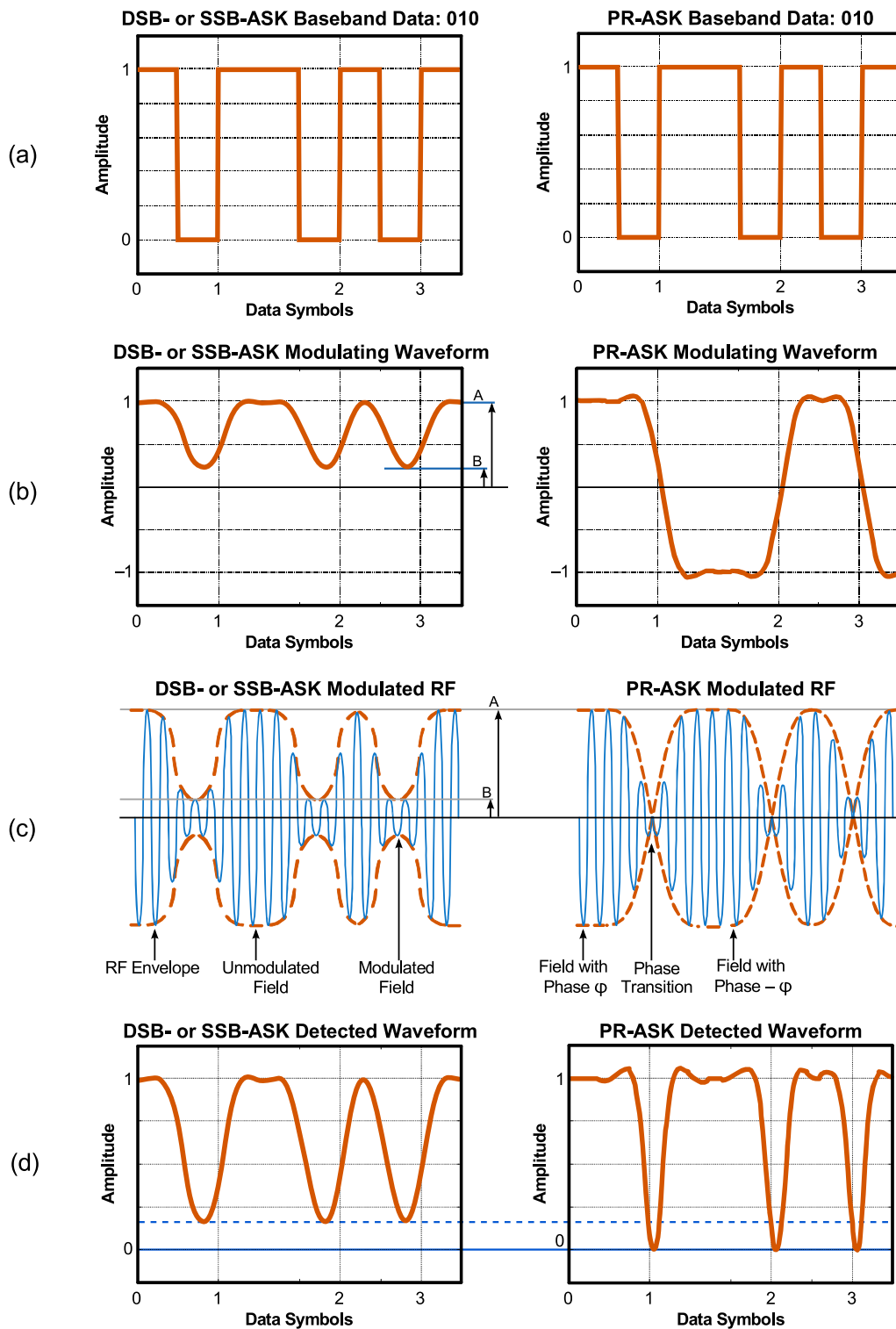


Figure 3.5: "Reader-to-tag" modulation. In (a), the the 010 baseband signal is shown, respecting TARI requirements of Fig. 3.1. (b) represents the modulating waveform which will be upconverted at the operative frequency, becoming (c) ($Mod_depth = \frac{A-B}{A}$). It's worth nothing that interval in which the modulated signal is attenuated is shorter in PR-ASK than DSB and SSB. In (d) the demodulated signals are shown: envelope is extracted, and phase is not used.

Ratio (SNR), so reader's signal can be detected even at wider distance from the source. However, there's no real advantage from a wider "reader-to-tag" link, if energy transmitted is not sufficient to activate the target transponder. OOK-ASK demonstrates the higher robustness against noise, but 100% of modulation depth corresponds to the minimum transmitted power.

3.3.2 PR-ASK

PR-ASK has several advantages, if compared to SSB and DSB. The modulation scheme requires a phase inversion per each transition, that corresponds to a symbol change in PIE encoding. The signal generated has the same characteristic of a digital BPSK, but the modulating signal allows data stream to be extracted from amplitude, rather than phase. In practice, PR-ASK is a BPSK phase modulation at the transmitter side, and an amplitude modulation at the receiver side. In addition to low complexity circuitry, amplitude demodulation gives another advantage: as a result of PIE encoding, each symbol has a zero-crossing, so the resulting signal has a inner temporization (see Fig. 3.5.(c) for PR-ASK).

Modulation depth of PR-ASK is 100% because each transition correspond to a phase reversal, with maximum amplitude, so it maintains the same properties of OOK, with respect to signal to noise levels. On the other hand, amplitude is 0 only in the transition interval, which has precise duration, specified in the standard. This feature is very important because it guarantees the minimization of RF wave switch off, that means a more efficient transmission of energy to the tag.

3.4 Multiple and Dense Interrogator Mode

A *multiple* (or *dense*) reader environment is a region where two or more readers are operating close to each other. Without any control, readers may transmit at the same time, causing a performance degradation. For this reason EPCglobal standard provides a number of methods that readers should use to maximize spectral efficiency and system performance, avoiding reciprocal interference and disturb to other systems.

There are several methods that prevents interference between the interrogators, such as "Listen-before-Talk" polices, or hardware synchronization with a dedicated communication protocol between readers, or through a networked activation manager. As a consequence, each time one interrogator transmits, the other must be idle, so such methods implement a time division multiplex-

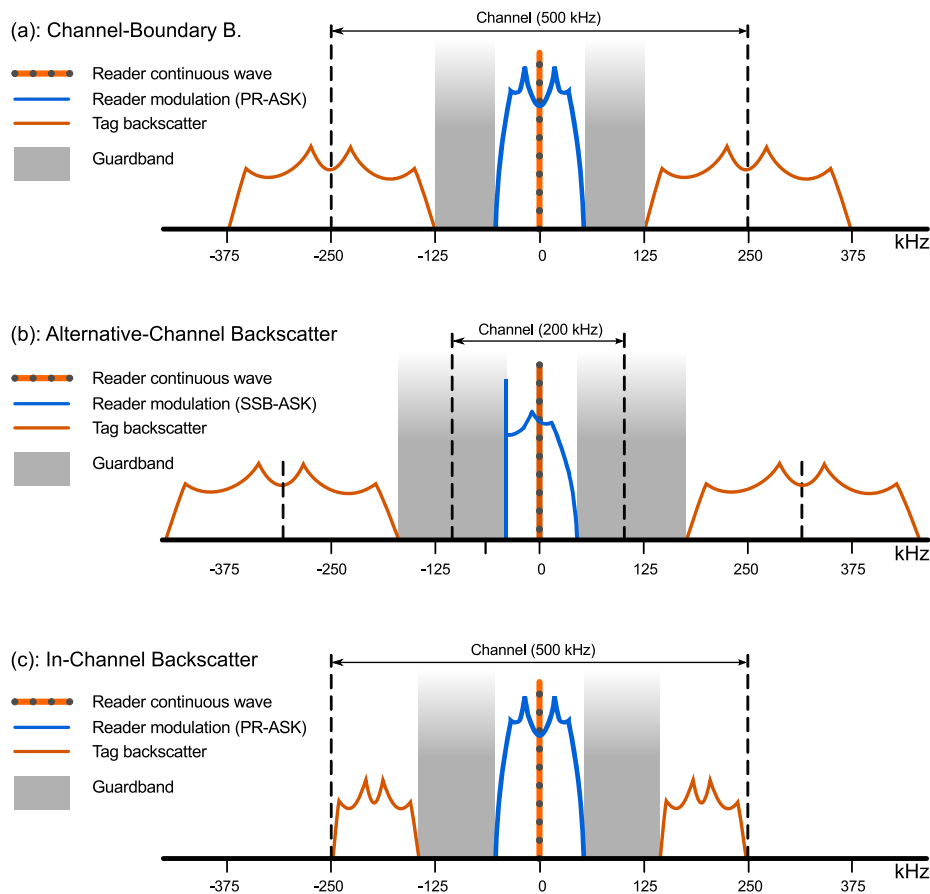


Figure 3.6: Examples of Dense-Interrogator-mode operation. (a): frequency hopping with 500 kHz maximum channel width; channel-boundary backscatter is admitted because there's no fixed adjacent channel. The communication shown implements PR-ASK, with 250 kHz of backscatter link frequency (BLF): a portion of the backscatter exits channel boundaries. (b): 200 kHz channel width, with 600 kHz spacing from each other: SSB-ASK is used to keep bandwidth narrow and maintain sufficient guard-band. In this configuration the backscatter spectrum is located in the spacing region between channels (300 kHz of BLF). (c): 500 kHz adjacent channels: communication spectrum must be all limited within boundaries.

ing, which do not solve the problem of simultaneous operation.

Because of the great number of regional regulations and spectral managements, the standard does not give precise specifications on interrogators requirements: it only defines the goal of channelized signalling aimed at simultaneous transmission. In particular, Frequency Division Multiplexing (FDM) technique is suggested as useful to minimize "reader-to-tag" collisions, and three possible FDM methods are described (refer to Fig. 3.6), to give example of co-operation policies. FDM examples reported are not binding, because local regulations may vary the specific parameters, and prohibit or even encourage these or other

methods:

Channel-boundary backscatter: Interrogator's transmission is shrunk to occupy a small frequency interval at the center of each channel. Backscatter signal, instead, is centred at channel boundaries: this solution gives the opportunity to separate them from the interrogator signal, exploiting intervals external with respect channel boundaries (Fig. 3.6(a)).

Alternative-boundary backscatter: channel is split in many subsets: interrogator's signals are assigned to a subset, and tag's backscatter falls in other subsets (Fig. 3.6(b)).

In-Channel backscatter: Interrogator's transmission occupies a small frequency interval at the center of each channel and backscatter signals are separated from the central frequency, but still maintained within channel boundaries (Fig. 3.6(c)).

Methods described allow multiple readers to operate in the same place, in the same moment: they do not interfere each other, because information are transmitted in different frequency channels, so "reader-to-tag" link is maintained undisturbed.

The same problem affecting readers may impede tag's backscatter to be discriminated. For this reason, Backscatter Link Frequency (BLF) and the multiplying factor M (see Fig. 3.4) must be properly chosen, in order to respect channel regulations, and maintain backscatter spectral content far enough from the reader's signal, for better filtering and discrimination.

Chapter 4

Critical Issues and Test Setup

This chapter gives a general overview of the critical issues that still limit the performance of UHF RFID systems. In the next chapters all issues highlighted will be tested and characterized on the experimental setup here described.

4.1 Critical Issues and opportunities

UHF is nowadays the most promising technology for large scale applications. With respect to HF and the first generation of UHF systems, EPCglobal has significantly contributed to improve the overall system performance. This means, for example, that a greater number of tags can be interrogated and more information per tag can be transferred to the reader, in a wider spatial range, in the same time interval.

Despite of the rapid success of these years and the promising advantages, UHF technology has a number of critical issues, that still represent an obstacle to the massive diffusion and adoption. It's worth noting that mentioned obstacles are not only technology issues, on the contrary, they involve many aspects such as:

- Low compatibility across the world: EPCglobal standard is giving a great contribution, but operative frequencies and power levels are still non uniform. As a consequence, technological solutions may be optimized for a few regions, but unsuitable in other ones; alternatively, lower performance are achieved using devices designed for interoperability, but not optimized.
- Poor performance of specific devices, due for example to short ranges, low detection and identification efficiency, low data rate and access rate, and so on.

- Tag flexibility: in presence of materials and obstacles, electromagnetic transmission undergoes to specific rules, so there is not one only tag or antenna type (*i.e.*: liquids and metallic surfaces heavily influence tag's detectability). Sometimes, the optimum technical solution cannot be used, because of constrains given by object shape. All this issues has important consequences on performance and costs, limiting adoption.
- From a systemic point of view, overall performance are often quite different from expected or documented data. This means, for example, that that there is no real "on-the-shelf" solution, and on the field, tests demonstrate worse results if compared to documentation, sometimes insufficient or even unacceptable to meet application targets.
- RFID tagging give the best advantages if the implementation is shared along the whole supply chain, from producer to costumer. At present day, a great number of realizations represents the solution for one only precise problem.
- Data security is still an open issue.

Issues listed above give a representative overview of the most discussed aspects and each one represent a real opportunity to the development of RFID technology, towards massive adoption.

As said, there are great expectations on UHF as promoted by the EPCglobal standard, however from a technological point of view UHF RFID is not an easy to implement technology. Several perturbing phenomena arise, *e.g.* in-channel background noise and/or interference, effects of absorbing, reflecting and/or diffracting obstacles in the nearness of tags, and so on [1]. Performance loss also arises because of the reduced levels of the power transmitted by the reader, or as consequence of the bad orientation of tags' antennas with respect to the reader one. The influence of such issues are of primary importance in a design and setup stage of a UHF RFID system, and should be properly taken into account. To this purpose, designers should always know in which physical conditions both reader and tags can operate, to guarantee a 100 % percentage of correctly identified tags.

As largely documented in the previous chapters, the most crucial issue is the proper communication between the reader and the tag, because it affects the correct identification of the objects. UHF RFID systems are commonly used for applications in which many tagged items in a given volume have to be identified and discriminated quickly and correctly. The logistic context is a good example: here RFID systems are suitable for identification of products contained

in boxes, pallets, or containers. Again, in avionics tags allow verifying the status of the assembled parts, and so on. For such applications, the efficiency of the system is defined as its capability to quickly and correctly discriminate all tags contained in a given volume, so the communication between reader and tag must be affordable.

4.1.1 Key parameters

Performance of a UHF RFID system depends on several parameters, each strongly related to design or setup choices:

- features of reader's antennas;
- features of tags' antennas;
- power level at the reader antenna's input connector;
- position and orientation of reader's antennas;
- position and orientation of the tags inside the reading volume;
- position of the box containing the tagged items in the reading volume;
- dimensions of the box containing the tagged items in the reading volume;
- dimensions of the reading volume;
- length of the time interval between two subsequent readings;
- speed of the tags during the interrogation;
- number of tags;
- number of reader antennas;
- number of independent readers in the same area;
- tags proximity;
- setup of reader's parameters such as: antenna read sequence, tries per antenna, reading session duration, etc.;
- effects of absorbing and reflective materials within a tagged item;
- effects of absorbing and reflective materials within a box containing tagged items;
- effects of absorbing and reflective materials around the reading volume;



Figure 4.1: Picture of the testbed adopted. The image shows the target of identification process, and a measurement antenna used to detect power levels.

- in-channel interference;
- electromagnetic environment and noise;
- drift effects due to variable environmental conditions.

All parameters listed above may have significant impact on the system efficiency, leading to reading failures, and so missing recognition of one or more tagged items. This possibility is to be avoided especially in those applications in which a 100 % of successful reading is always required.

The latter consideration implies the necessity for a deep knowledge of the effects that each of the listed issues can cause on the final system performance and hence the best conditions under which bad effects are heavily mitigated.

4.2 Experimental Analysis

One of the critical issues listed in the previous paragraph concerns the frequent mismatch between the nominal performance and the results obtained once completed the implementation. All key parameters highlighted influence the overall functionality, so they must be properly tuned in order to maintain and make operative the performance of each single component, once on the field. Real life applications, in fact, are not set in aseptic environment, such as an anechoic chamber, and the boundary conditions have great influence. This is the reason why an experimental approach, representative of real in-field applications, can lead to the comprehension of how the multiple aspects interact, and

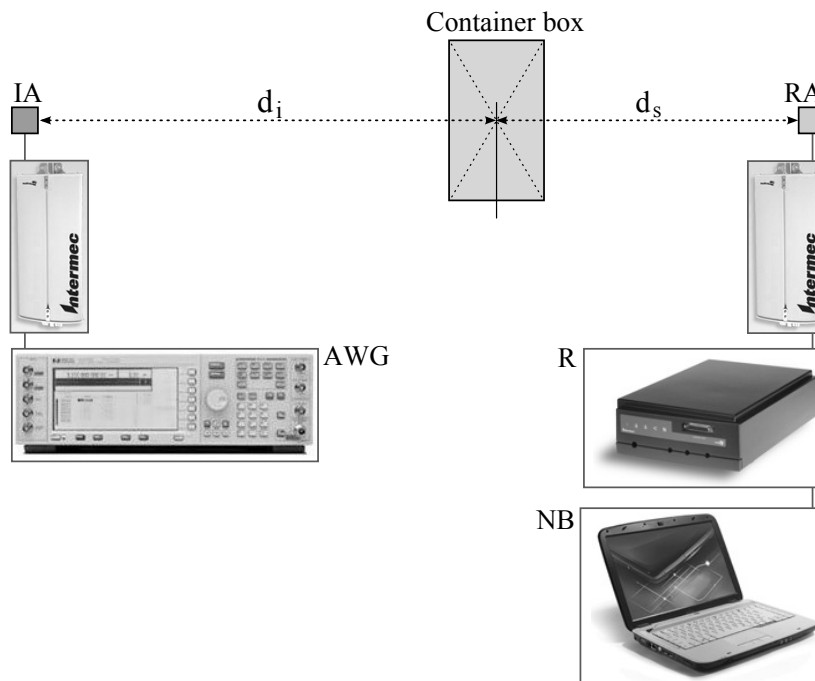


Figure 4.2: Schematic view of the adopted testbed: measurement instrumentation is not shown (spectrum analyser, power meter and RF measurement antennas).

which countermeasures should be taken to avoid performance degradation. In this sense, a number of experiments have been carried out in order to analyse the behaviour in real life applications and deduce rules to improve the reliability of a generic UHF RFID system.

4.2.1 Testbed

All the experiments have been conducted by using a testbed emulating a typical identification task of tagged items, contained in a box. The testbed, sketched in Fig. 4.2, includes all the components involved in the experimental analysis, but only a subset of them has been used in each test, the one necessary to highlight particular issues.

As a general overview, the testbed includes the following components:

1. one $36 \times 41 \times 80$ cm paperboard box, denoted as *container-box*;
2. $N = 36$ empty paperboard $11 \times 12 \times 26.5$ cm small boxes, denoted as *tagged-boxes*;
3. $N = 60$ planar linearly polarized Gen-2 passive UHF tags of size 10×2.5 cm (Fig.4.3);
4. IF5 UHF RFID reader device (R) available from Intermecc;

5. two circularly polarized $55.3 \times 26.1 \times 5.8$ cm Intermec IA39B antennas (Interference Antenna (IA) and Reader Antenna (RA));
6. Notebook (NB) equipped with a 1.6 GHz Intel Centrino processor and a 1 GB RAM;
7. Arbitrary waveform generator (“AWG”) Agilent Technologies E4420B ESG (250 kHz - 6 GHz frequency range);
8. Precision conical dipole: PCD 8250 (80 MHz to 3 GHz);
9. Spectrum Analyzer Agilent ESA E4407B (100 Hz to 26.5 GHz);
10. Real-Time Spectrum Analyzers Tektronix RSA 3408B (DC to 8 GHz, capture bandwidth 36 MHz).

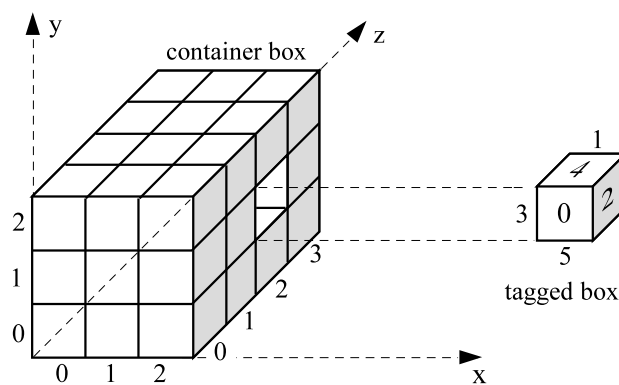
4.2.2 Box and tags disposition



(a)



(b)



(c)

Figure 4.3: (a) Container-box, (b) tagged boxes and (c) disposition.

The empty boxes have been used to allow an easy positioning of the tags in the “container-box”. Specifically, each tag is positioned at the center of one of the



Figure 4.4: Shape of tags used in the experiments.

surfaces of an empty box.

The tagged boxes are placed into the “container-box” according to the desired order and orientation of tags antennas: they are equally distributed along x , y and z directions.

According to Fig. 4.3(c), the position of a tag is identified by a string of four numbers:

$$(x, y, z, o) \quad (4.1)$$

where x , y , z , with $\{x, y, z : 0, 1, 2, \dots\}$, are the coordinates of the tagged box, and o , with $\{o : 0, \dots, 5\}$, identifies the surface on which the tag is attached.

The container-box is placed with the bottom side at 20 cm height from the ground floor.

4.2.3 Transmitting antenna

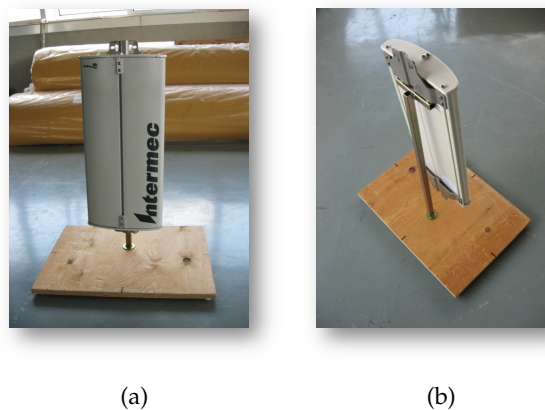


Figure 4.5: Intermec IA39B antenna.

The testbed scheme shows two antennas: the first, *RA* is used to transmit the interrogation signal from the reader; the second, *IA*, is used to transmit electromagnetic interferences to emulate a disturbed environment.

The center of each antenna is positioned at 40 cm from the ground floor and

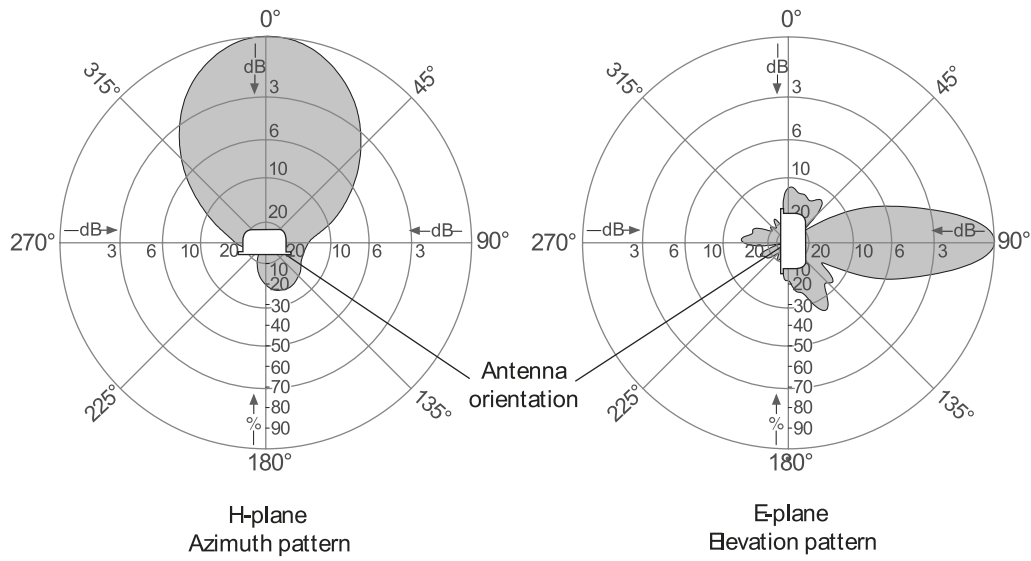


Figure 4.6: Radiation diagram of Intermec IA39B antenna.

at distance d : in detail, d_i indicates the distance of the interferer antenna IA from the container-box, and d_s indicates the distance at which RA transmits the interrogation signal.

Both antennas are vertically oriented, with respect to the ground floor: this configuration guarantees the widest azimuth pattern [24], as shown in Fig. 4.6. Here follow the main features:

Material	Fiberglass
Frequency Range	865-870 MHz
Gain	10.5 dBic
Impedance	50 Ω
Polarization	Circular, left-hand
Maximum Input Power	100 W (@ 50° C)
H-Plane Beamwidth	70° (half power)
E-Plane Beamwidth	30° (half power)
Dimensions	55.3 x 26.1 x 5.8 cm, 3.6 kg

4.2.4 RFID Reader

Intermec IF5 is a fixed UHF RFID Reader, with both *read* and *write* capabilities. The device includes powered general purpose input/output circuitry, which allows direct access to other peripherals. It implements IPv4 and IPv6 with



Figure 4.7: Intermecc IF5.

optional 802.11b/g radio, enabling the integration into networked structures, both wired and wireless.

It is important to report that this device is equipped with four ports for interrogation antennas: the sequence of activation of the four antennas is completely customizable, but is not possible to make simultaneous interrogation transmissions on two or more antennas.

Here follow the main characteristics:

Communication Interfaces	Ethernet 10/100BaseT Wireless 802.11g
Connection to Network	Ethernet 802.3 wired 802.11g (optional)
Input-Output	4x 0-40 V Input 4x 0-48 Vdc 0.5 A Output 500 mA 12 Vdc power
Antenna Connections	4x Reverse SMA, -20dB software controlled
RFID Frequency Ranges	ETSI 865-868 MHz, FCC 902-928 MHz
Tag Air Interfaces	Intellitag G1 (Fairchild G1) ISO 18000-6b (Philips i-code HSL) Philips Version 1.19 EPCglobal UHF Gen-2
Protocols	ANSI INCITS 256:2001 Intermecc Basic Reader Interface

Standards	AIAG B-11 ANS INCITS 256:1999 (R2001) - Parts 2, 3.1, 4.2 ANSI MH10.8.4 ISO-IEC CD18000 Part 4 ISO-IEC WD18000 Part 6
Software	IP v6, SAMBA Client, NFS Client, Telnet Server, Syslog Client, FTP Server, PCMCIA Card Services, OpenSSL, J2ME/CDC. Service Management Framework, SAP-Auto ID Infrastructure (AII). Intermec Network Apps, HTTP-HTTPS Web Server (TFTP Client, DHCP Client, DNS Client, SNMP Client, 802.1x Supplicant). Intermec Developer Library, Intermec Data Collection Engine. Optional WebSphere Everyplace Device Manager (IBM), Optional J2SE (SUN), Java Virtual Machine, Java Script Interpreter
Development	Built in Java and Java Script, Intermec Development Libraries for Java and .Net
Dimensions	35.6 x 23.1 x 9.53 cm

4.2.5 Boundary conditions

All tests have been conducted in a site free of reflective obstacles (in an area of approx 6.0 m radius), with the exception of the concrete ground floor. Surfaces and conditions emulating environment have been added intentionally, as specified afterwards.

The operative frequency has been set to 869.538 MHz, and power levels varied according to experiment target.

If not differently stated, measurements have been performed under the assumption of static setup, *i.e.* with a time duration ΔT_{ic} of each interrogation cycle, long enough to guarantee the correct identification of each tag in the read range of the reader. After a set of preliminary measurements, ΔT_{ic} has been set equal to 1 s. This value is the minimum ΔT_{ic} above which no significant worsening of the number of correctly identified tags has been observed, and below which a few missing tags have been measured.

4.3 Performance metrics

In literature, several methods have been proposed and exploited to evaluate the performance of UHF RFID systems [1, 4, 11, 12, 17, 21]. Since the received power at the tag antenna is one of the most critical issues in the behavior of a UHF RFID system, the measure of the electromagnetic field strength is considered a good metric to predict the expected reading region. However, such an approach only evaluates the theoretical behavior of the electromagnetic field.

Better results are obtainable considering the rate at which the reader can identify tags (reading-rate), generally given by the ratio of successful cycles over the total number of reading cycles. This is a method largely adopted, but actually, there is some ambiguity on the definition of reading-rate and literature shows many different contributions (for further information see [4]).

For the purposes of the present work, mentioned quantities are not effective enough to describe the RFID system.

The RFID system performance have been evaluated in terms of SE, defined as the ratio of the number of correctly identified tags in the reading cycle ΔT_{ic} over the total number contained in the analysed volume:

$$SE = \frac{1}{N} \sum_{ID=1}^N \mathcal{I}(ID) \quad (4.2)$$

where $\mathcal{I}(ID)$ is the identification indicator: its value is 1 if tag corresponding to ID has been identified, 0 otherwise.

SE contains the effects of the reading-rate, but allows a more systematic evaluation of the overall identification task. The best performance is associated to $SE = 100\%$ in all actual conditions; unfortunately, it cannot always be ensured.

Chapter 5

Performance Evaluation

In this chapter, relationships between the EM field levels at the tag antenna and the overall performance of a UHF RFID system are investigated experimentally. The main purpose is to analyse phenomena involved in the operation of a UHF RFID system underlying the importance of preliminary measurements in the setup and optimization of a real-life application.

Experiments have been carried out on a testbed equipped with a real-life UHF RFID system, as described in Chapter 4.

5.1 Preliminary evaluation

Focusing on UHF RFID systems employing passive tags (EPCglobal Gen-2 Class-1 [23]), preliminary informations about performance are derivable from eq. (5.1):

$$P_{t,dBm} = P_{r,dBm} + G_{t,dB} + G_{r,dB} + p_{dB} + k_{f,dB} + 20 \cdot \log_{10} \left(\frac{\lambda}{4\pi d} \right). \quad (5.1)$$

Without any information or model for the environment, k_f must be set to 0 because unknown.

Eq. (5.1) allows to calculate from devices features, the power intensity P_t that reaches transponder's chip and supplies its circuits¹, so it is one of the most effective tool to derive a preliminary performance evaluation.

In the design of UHF RFID systems, a meaningful (even if often underrated) parameter is $P_{t,min}$, which is the minimum power needed to activate the tag. It represents a physical limit under which the tag cannot be correctly identified.

¹The sentence is true with perfect match between the antenna and tag chip. Otherwise, internal circuits are supplied by a portion of the sensed power, proportional to the matching parameter (refer to Sec. 2.3.1).

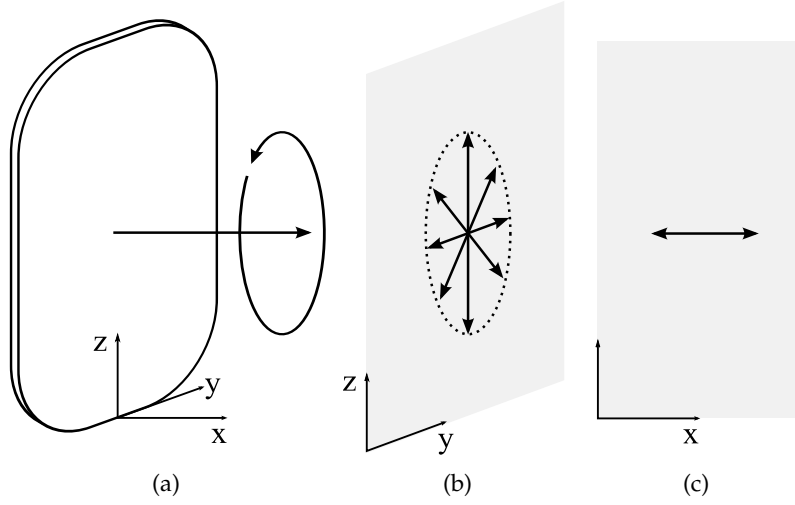


Figure 5.1: Alignment between reader and tag: (a) circularly polarized reader antenna, (b) parallel orientations of a linearly polarized tag antenna, (c) orthogonal orientation of a linearly polarized tag antenna.

The knowledge of $P_{t,min}$ allows to deduce the maximum distance d_{max} from the reader's antenna beyond which tags are no longer detectable by the reader. $P_{t,min}$ is a technological parameter, given for a certain transponder; d_{max} instead can be calculated inverting eq. (5.1).

Here follows a summary of the main parameters, with their values, associated to the testbed adopted:

- $P_{t,min,dBm}^{(2)}$ from -10 to -7 dBm (typ.);
- $G_{t,dB} = 2.15$ dB (dipole antenna);
- $G_{r,dB} = 10$ dB;
- $P_{r,dBm} = 30$ dBm;
- p_{dB} from 0 (perfect alignment) to -20 dB (orthogonal alignment);
- $k_{f,dB}$ is unknown and set to 0 dB.

Electromagnetic transmission of energy between two antennas is maximized if the two antennas are aligned and share the same polarisation direction. On the other hand, whenever polarization directions are orthogonal a damping of 20 dB has to be taken into account in the power transmission due to polarisation losses [25].

² $P_{t,min,dBm} = 10 \cdot \log_{10} P_{t,min} / 1mW.$

Table 5.1: $\hat{P}_{t,dBm}$ for different values of d_s and tag orientations.

d_s [m]	Parallel [dBm]	Orthogonal [dBm]
0.5	13.9	-3.1
1.0	7.9	-9.1
3.0	-1.6	-18.6
5.0	-6.1	-23.1

$P_{r,dBm} = 30$ dBm
 $\lambda|_{f=869.538 \text{ MHz}} = 0.345$ m

Energy transmission in UHF RFID does not constitute an exception to these rules, so the reciprocal orientation of reader's and tag's antenna may heavily affect the communication link. In particular, this is true in any application in which there is no fixed or predictable disposition of transponders.

In order to minimize the effects of the polarization mismatch, the reader's antenna is usually realized with a circular polarization, as represented in Fig. 5.1; tags' antennas are instead typically linearly polarized. This allows to obtain a constant and known mismatch coefficient p_{dB} equal to -3 dB [19, 25] for any orientation of the tag antenna within the reader antenna polarization plane (yz plane). A reduced level equal to $p_{dB} = -20$ dB is instead achieved in the case of a tag antenna orthogonal to the reader surface.

In Table 5.1, some estimates (\hat{P}_t) of P_t are summarized, obtained by applying (5.1) to the parameters above listed. The values of \hat{P}_t are derived for different values of d_s and tag orientations. Such results can be considered general for any UHF RFID for which the following conditions hold:

- operative frequency: 869.538 MHz,
- far-field hypothesis,
- $k_{f,dB} = 0$ dB.

In the case of a UHF reader antenna with 55 cm largest dimension (Intermec IA39B), applying eq. (2.3) the boundary between near-field and far-field regions is at $2D^2/\lambda \cong 1.75$ m. In this situation, far-field conditions are met only for the two larger distances d_s of Table 5.1. As a consequence, accurate estimates of $\hat{P}_{t,dBm}$ can be achieved only at the latter distances.

At 0.5 and 1.0 m, instead, tags operate in near-field conditions with radiated electric and magnetic fields no longer orthogonal with each other. In this case, the values given according to (5.1) are not exact, so they can only be considered a rough estimation of $P_{t,dBm}$. The correction factor $k_{f,dB}$ (which is typically unknown *a priori*) may help tuning the estimations, but it should be determined

from in-field measurements in each point of the space, because, up to the limit of far-field, $k_{f,dB}$ should count all non linear difference between the real electromagnetic distribution (which is a function of position) and the model (valid only in far-field region). Otherwise, calculations should be done on the exact electromagnetic distribution.

In practice, the values in Table 5.1 are meaningful when compared to $P_{t,min,dBm}$, so, even if the model is not precise – considering parallel tags – margin is so wide that tags can be considered active (as demonstrated by experimental evidence). Orthogonal tags, on the other hand, are already in a boundary situation, so they should be analysed separately.

Considering the values obtained, and $P_{t,min,dBm} = -7$ dBm, a 100 % tag identification is expected for $d = 0.5$ m, with evident worsening at $d = 1.0$ m, due to x -oriented tag fed by insufficient power (Fig. 5.1). Conversely, tags coherently oriented with reader's antenna polarization (yz plane in Fig. 5.1) are expected to be identified above $d = 3.0$ m, with some penalization at $d = 5.0$ m, because of power intensity very close to the boundary level.

It is worth noting that equations and considerations above are exact in *free space*: Path-loss defined in (2.13) does not count attenuation effects due to dielectric materials, reciprocal shielding, multi-path fading and other parasitic contributions. For this reason, the power levels listed in Table 5.1 are rounded up estimations, and in real-life applications performance may decay closer to the reader antenna: this will be verified by experimental results. In general, worse performance is expected, with respect to the values listed in Table 5.1, because parasitic effects really influence system behaviour, that is $k_f \neq 0$.

5.2 Experimental Results

As largely discussed and theoretically proved in the previous chapters, UHF technology can implement long range applications, but one of its critical issues is the poor correspondence with the performance documented from in-field tests.

Experimental analysis has been conducted keeping in mind this characteristic, so the results collection and measurement approaches have been implemented maintaining under control how the system and its interrogation region behave moving away the transmission source. In this way, any time a parameter change, there's a direct check of its influence on read-range.

In practice, SE is always measured as a function of the distance d_s between the

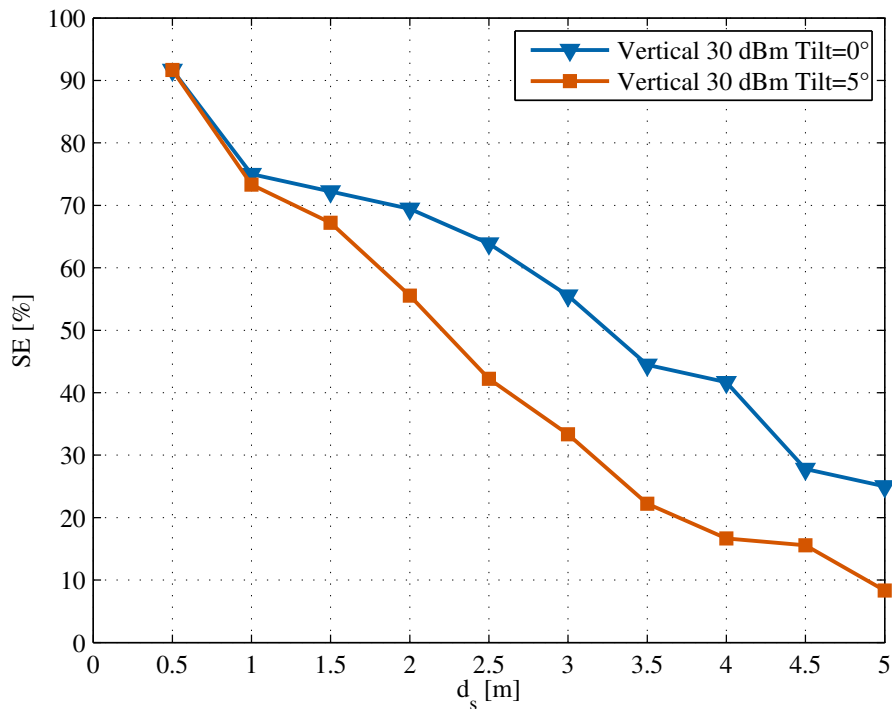


Figure 5.2: Degradation of SE with a weakly tilted vertical antenna (5°), with respect the reference vertical one.

reader's antenna and the target (tagged boxes).

Experiments carried out in this section are focused on the evaluation of the actual performance, beyond the theoretical values.

Considering the testbed described in Fig. 4.2, only a subset of the instrumentation has been employed: in particular, devices dedicated to transmission and measurement of interference signals has not been used. Furthermore, the system has been set with one only antenna, because any other more complex configuration can be seen as a combination of the basic one. In fact, even if equipped with multiple antenna inputs, RFID readers do not activate the transmission on more than one, as a consequence, deductions aimed at performance improvement are equally valid.

5.2.1 Tilt impairment

This simple experiment has been reported to demonstrate how much important is the correct alignment between the tag set under test, and the interrogator's antenna. In particular, results highlight the influence of the antenna's radiation lobe (reported in Fig. 4.6). Intermec IA39B (vertically oriented) has a radiation

lobe focused in its middle plane, wide there and shrunk with respect the vertical direction.

Fig. 5.2 sketches SE as a function of distance from the reader's antenna, distinguishing two similar situations:

- (i) RA exactly vertical and placed in front of the containing-box
- (ii) RA 5° tilted.

Despite of the small tilt, such an impairment causes an evident degradation in performances, mainly far from antenna. This happens because the volume where antenna focuses radiated power is not aligned with the box. In other words, whenever the power radiated power is wasted in empty space – when radiation lobe is oriented away from the volume containing tags – the overall system may show performance degradation.

5.2.2 Aggregated and Separated System Efficiency

In a great number of applications, the distribution and orientation of tags may not be known or well defined, so a good metric for the overall efficiency is SE as calculated in Section 5.2.1, because it makes no distinction on tags disposition. Being all tags equally distributed along the three directions $\{x, y, z\}$, once set the correct alignment, SE has been measured with the same approach, upon the varying of d_s in the range 0.5 – 5 m and for different values of P_r . As shown in Fig. 5.3, results demonstrate a strong correlation between SE and d_s : in particular, SE rapidly decreases upon the growing of d_s according to a quite linear trend. This performance degradation can be attributed to the weaker values of EM field picked-up by each tag upon the growing of d_s , but there is no coherence with eq. (5.1), which suggests a threshold behaviour.

Furthermore, the highest SE value is around 90%, and all the others are below: below 1.0 m, none of the configurations can ensure an efficiency better than 80%, decreasing at a rate around 10 to 20% each time the reader's output power is reduced of 3 dB. This is quite unacceptable for any UHF RFID system, said to be "long-range".

The problem highlighted is due to the fact that SE is calculated on the whole population of tags, but they do not operate in the same conditions. Polarization mismatch between reader's and tag's antennas heavily penalizes all tags orthogonal to the surface of reader's antenna. In coherence with Fig. 5.1, the specified direction corresponds to the propagation direction of the interrogation EM wave, x , and for aligned tags power transmission suffers an

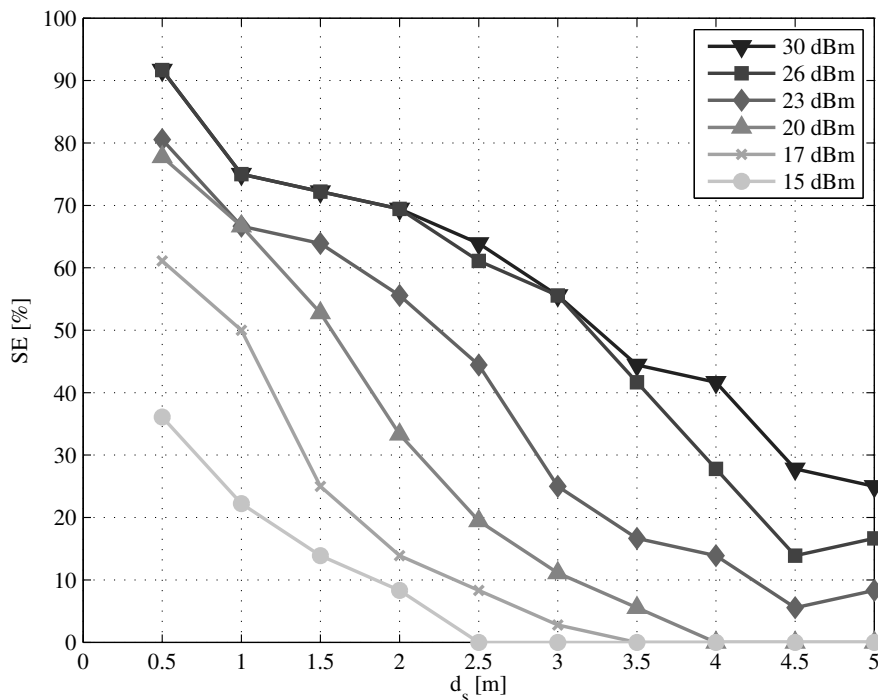


Figure 5.3: System Efficiency (SE) versus box-to-antenna distance d_s , measured for different $P_{r,dBm}$. The antenna is vertically oriented with respect to the ground floor.

attenuation of 20 dB. For this reason, even if more systemic, undifferentiated calculation of SE is misleading.

More precise information about the degradation effect can be deduced from Fig. 5.4, in which SE is analysed for one only value of reader output power ($P_{r,dBm} = 30$ dBm), and calculated considering the tags oriented along x , y or z separately. In the diagram, the curve denoted as “All” represents the mean value of SE obtained by averaging the three sets of values for x , y and z directions (SE_x , SE_y , and SE_z , respectively). This curve coincides with the one shown in Fig. 5.3 for $P_{r,dBm} = 30$ dBm.

Fig. 5.4 is important for several reasons. First of all it highlights that the random disposition of linear tags is detrimental for the overall performance, even in non critical conditions such as proximity to reader’s antenna.

The second contribution is related to the model: the three curves SE_x , SE_y , and SE_z highlight the existence of a threshold behaviour of SE versus d_s , proving the validity of eq. (5.1). In particular, a threshold distance d^* can easily be determined, below which all the tags are identified ($SE = 100\%$) and above which the performance of the system starts to degrade ($SE < 100\%$).

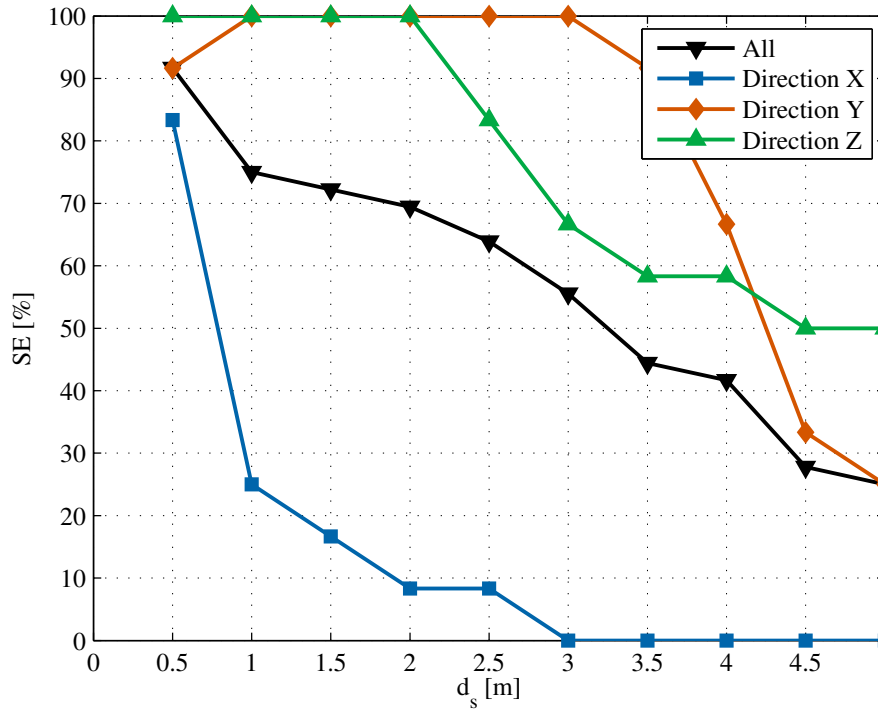


Figure 5.4: SE versus d_s , at $P_{r,dbm} = 30$ dBm, for different orientations of the tags along x , y , z directions.

A detrimental behaviour of the system is instead observed when tags are oriented along x , which means orthogonal to the reader antenna. In this case, full reliability (100 %) of the system can never be guaranteed, even at very small distances.

Fig. 5.4 also highlights a 9 % loss of SE at very small distances (*e.g.* $d = 0.5$ m) and for directions y and z . This fact can be attributed to the the reader antenna's radiation pattern, which, being limited to a nearly 70 degrees beam-width, does not allow a sufficient energy radiation to the outer tags placed at the boundary of the container box. These tags are hence not adequately supplied and thus not correctly identified.

With respect to the theoretical estimations in Table 5.1, the experimental results plotted in Fig. 5.4 show that a degradation of SE may occur also in the case of parallel orientation of tags and for $d > 2$ m, and in particular along z . This disagreement with the theoretical values of Table 5.1 is related to the non symmetrical shape of the radiation pattern [24].

Fig. 5.5 is equivalent to Fig. 5.3, with the exception that tags are not equally

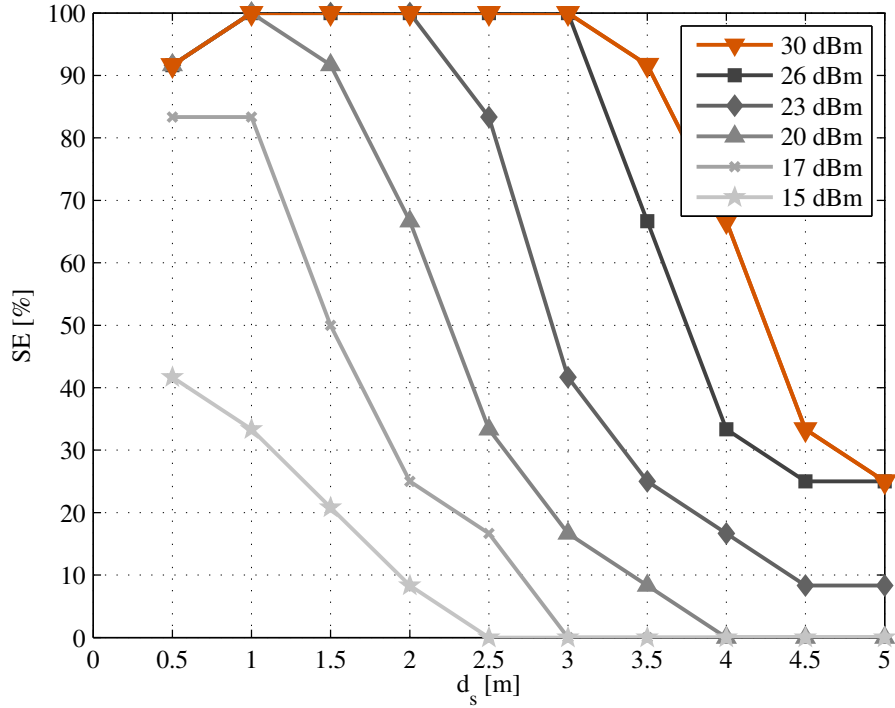


Figure 5.5: SE versus d_s , with tags all oriented along y and for different power levels $P_{r,dBm}$.

distributed, but aligned with y direction (the result of measurement is SE_y , only). From the reported curves, one can note:

1. below a threshold limit of $P_{r,dBm}$ in the range 17-20 dBm, SE is always lower than 100 % regardless of the distance d_s between the tags and the reader;
2. for values of $P_{r,dBm}$ in the range 20-26 dBm, the above defined threshold limit d_s^* increases upon the growing of $P_{r,dBm}$ at a rate of nearly one meter each 3 dB of $P_{r,dBm}$ improvement;
3. further increase of $P_{r,dBm}$ beyond 26 dB improves SE, for $d_s > 3$ m, but does not change d_s^* ;

5.2.3 Environment influence estimation

Data collected in previous section allows to define an *experimental read-range*, that is, the distance above which SE falls below a fixed percentage. In particular, d_{90}^* and d_{80}^* are defined as the distances above which the efficiency of the interrogation systems is lower than 90% and 80% respectively.

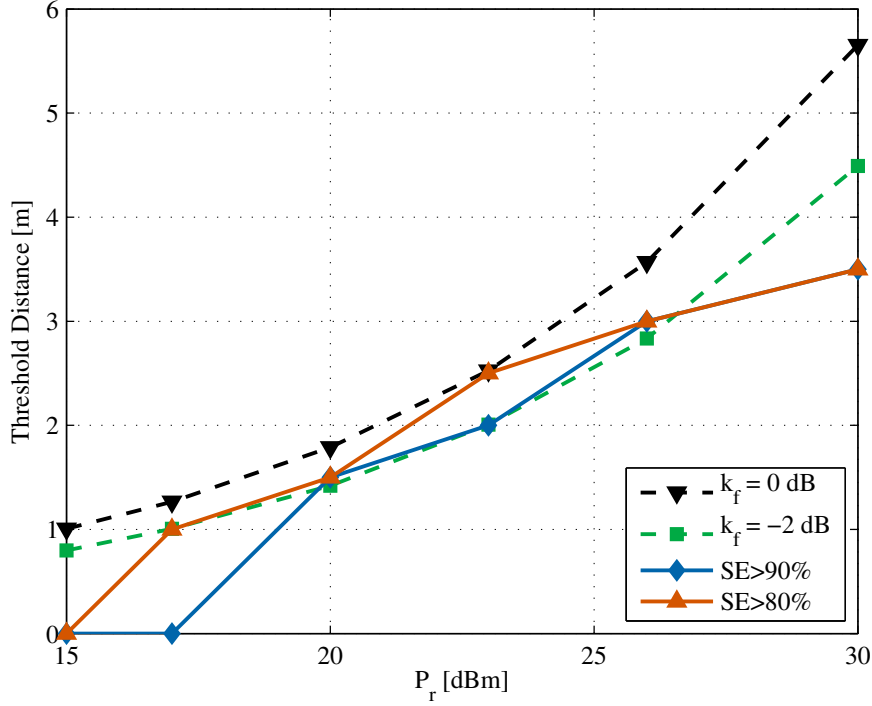


Figure 5.6: Maximum distances d_{90}^* and d_{80}^* , above which a 90% and 80%, respectively, of tags are identified. The dashed lines represent the theoretical values of d_s^* estimated inverting eq. (5.1) with $k_f = 0$ and -2 dB.

d_{90}^* and d_{80}^* are sketched in Fig.5.6: they represent an estimation of the threshold distances d_s^* , for different values of $P_{r,dBm}$ in the range 15 – 30 dBm.

Two dashed curves are also reported representing the values d_s^* obtained theoretically³ inverting eq. (5.1) and setting:

- (i) $k_{f,dB} = 0$ dB
- (ii) $k_{f,dB} = -2$ dB.

In other words, they represent the maximum distance above which a tag correctly operates according to (5.1).

From the diagram, one can note that in the range $17 \leq P_{r,dBm} \leq 26$ dBm, the theoretical curve having $k_{f,dB} = 0$ dB has the same trend of the corresponding one obtained experimentally; moreover, in the range $17 \leq P_{r,dBm} \leq 26$ dBm, the theoretical curve having $k_{f,dB} = -2$ dB is very close to the corresponding one obtained experimentally. As a consequence:

1. eq. (5.1) accurately models the relationship between the power levels radiated by the reader, the overall system efficiency SE and the above defined

³ $P_{t,min,dBm}$ is set equal to -7 dBm.

threshold distances. Therefore it can be efficiently used for accurate predictions of SE in practical applications of UHF RFID systems;

2. the efficient use of eq. (5.1) requires the accurate knowledge of the correction factor $k_{f,dB}$, which can be estimated by measurements on real-life testbeds, as shown in this chapter.

This fact underlines the importance of measurements in the optimization of any UHF RFID system.

Chapter 6

Susceptibility to in-channel radio interference

RFID technology is based on the use of RF signals, hence potentially susceptible to Electromagnetic interference (EMI) phenomena. In this chapter, the susceptibility to in-channel interference is experimentally investigated. In particular, the ability of a real-life system to correctly identify items is assessed in the presence of narrow and wide band radio disturbances.

6.1 Sources of Interference

One of the most underrated reason causing failure in the operation of UHF RFID systems is in-channel interference.

In-channel interference can have different origins: as an example, it can be due to the presence of two or more tags simultaneously transmitting to the same reader, or to the cross-interaction between two independent UHF RFID systems operating within the same environment.

Denoting two independent systems as A and B , several options might take place (Fig. 6.1):

- (a) collisions might arise between signals radiated by A and B readers;
- (b) collisions might arise between signals radiated by A and B tags;
- (c) a reader's communication from A might be interpreted as coming from B and *vice versa*;
- (d) tags of A might be interpreted as belonging to B and *vice versa*.

Clearly, all such issues become even more critical upon the growing of the number of RFID systems simultaneously operating in the same area.

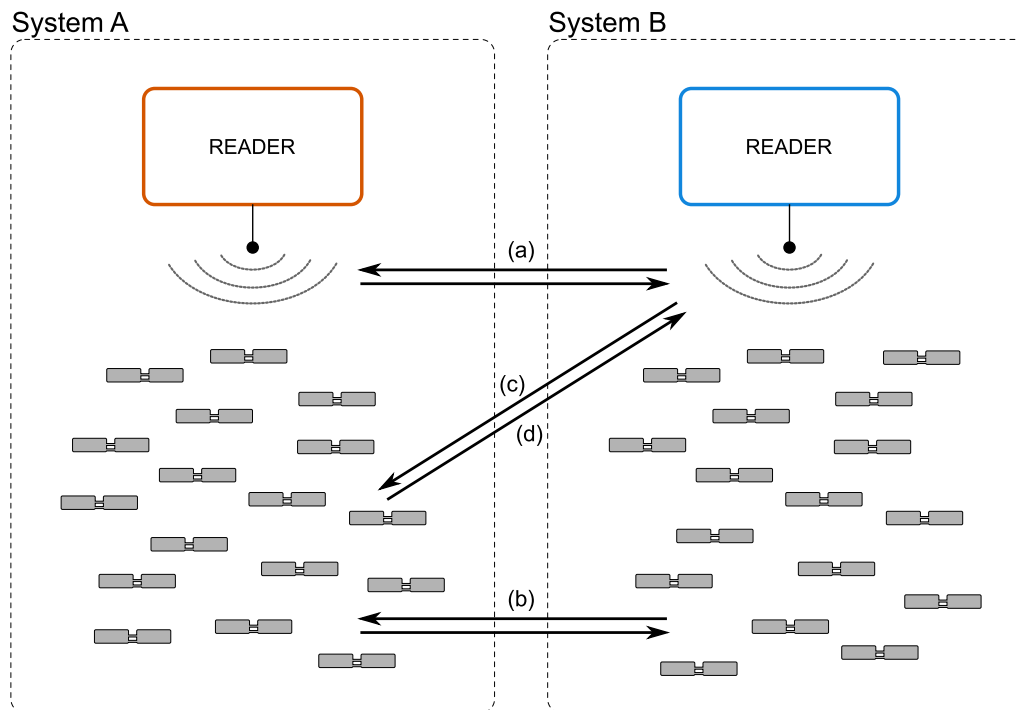


Figure 6.1: Internal interference due to systems proximity. Interference contributions indicated as (c) and (d) are represented from one system to the other only, for reasons of order; however the symmetrical contribution is present as for (a) and (b).

The introduction of the EPCglobal Gen-2 Class-1 standard has significantly contributed to highlight such weaknesses, and in many cases to mitigate their effects.

Improper detections have been filtered and avoided by assigning to each tag a personal code, so that to allow the reader to singularly discriminate them.

Simultaneous tags' response has been solved by means of efficient anti-collision policy algorithms, able to operate also in the presence of multiple sets of tags. For example, the ALOHA algorithm is considered, along with some of its variations (e.g. "Slotted ALOHA"), one of the most effective tool for avoiding collisions [26, 27].

Particular attention has finally been dedicated to the "reader-on-reader" interference; this problem is handled by the standard through the suitable "Multiple and Dense- Interrogator Operating Modes" (refer to Section 3.4), which defines signaling and methods for maximizing spectral efficiency and multiple systems coexistence.

All such techniques can be summarized in the following sentence: immunity against interferences in UHF RFID systems can be improved increasing the distance between tags and between different readers or separating in the time

and/or frequency domain their radiated signals.

It is finally observed that the effort to keep tags costs and power consumption as low as possible does not agree with the aim of increasing the immunity to interference; this is particularly true for passive tags of EPCglobal Gen-2 Class-1. It is also underlined that the above quoted strategies are specifically designed only for in-channel interference arising *internally*, by the system tags or by other similar RFID systems closely operating. The effect of other external sources radiating EM fields in the RFID bandwidth is instead an issue still not clearly known and that should be more deeply investigated.

6.2 Experimental Results

The analysis of robustness against in-channel interference needed the whole equipment described in Section 4.2.1, in order to generate the disturbing signals and measure the power levels.

Test has been designed to verify how the system reacts in presence of representative interference signals, and as done in the previous chapter, particular attention has been paid to how long-range performance changes.

6.2.1 Pure sine-wave

A set of preliminary measurements have been performed to obtain a first evaluation of system immunity capabilities.

The first experiment has been performed in the presence of a single tone interference of -10 dBm power level, at AWG's output connector (Fig. 4.2), and centred at the RFID system operating frequency, 869.538 MHz (Fig. 6.2).

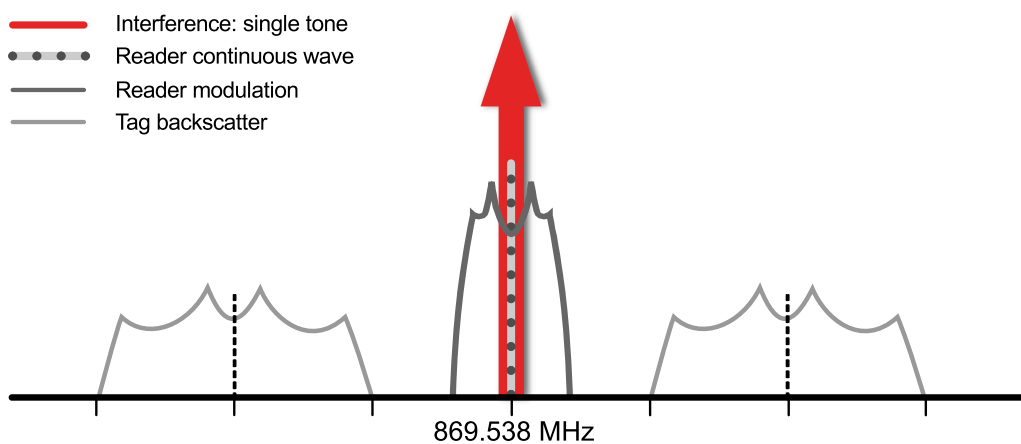


Figure 6.2: Single tone interference, superimposed to reader's continuous wave.

The reader has been set with radiated power level $P_r = 30$ dBm, at its antenna input connector, and antennas have been placed at distances $d_s = 1$ m and $d_i = 2$ m.

In this configuration, despite of an interrogation power level 40 dB higher than that emitted as interference, a strong degradation of SE has been noted, in the order of 50%.

In contrast to previsions, the presence of a single external tone exactly superimposed to reader's continuous wave is not an advantage at all. The condition of identical frequency, in fact, is not sufficient to guarantee the constructive cooperation: on the contrary, there is high probability of phase dis-alignment. The exact and constructive superimposition, in fact, requires three simultaneous conditions: (i) the precise synchronization of both sources, (ii) the exact alignment of the two antennas (alignment of propagation directions), and (iii) the centre of emission of both antennas must be placed at a multiple of the wavelength. These conditions ensures synchronization along axial direction, only; in any other point in space, (iii) is not verified, in general.

As a consequence:

- at tag side ("reader-to-tag" link), amplitude modulation coming from the interrogator combines with the same unmodulated signal: this leads to a reduction of modulation depth together with SNR worsening, or it simply overrides the signal nullifying the data stream.
- at reader side ("tag-to-reader" link), if the interrogation ended correctly, the backscatter signal contains two components multiplexed in phase: one coming from reader's continuous wave, one from the interference. Even if weaker¹, the second component cannot be discriminated with amplitude demodulation, so the reader cannot properly detect tag's response.

The same performance loss occurs even if the two antennas do not face each other. The discrimination between a detrimental and non detrimental effect is to be found in the direction of the disturbing beam: if tags are hit the degradation occurs. The effect on "tag-to-reader" link is attenuated only if the interference backscattered is penalized along that direction (*i.e.* because of dipole orientation, or polarization), so the proper signal is stronger than interferer.

6.2.2 Wide-band Noise

A second set of experiments has been performed in the presence of a wide band interference (Fig.6.3). The waveform generator has been set in Additive White

¹Being the two antennas IA and RA facing each other, the interference has a direct path, so it is even more dangerous.

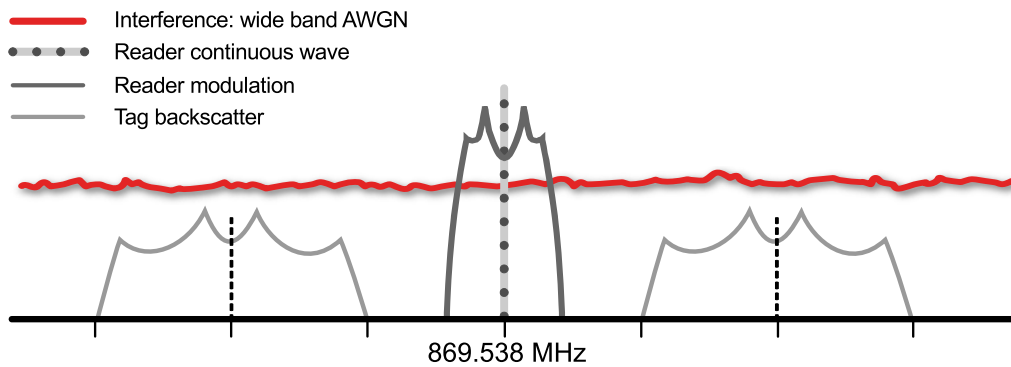


Figure 6.3: Wide-band White Gaussian Noise, interfering on the whole channel.

Gaussian Noise (AWGN) mode, with 1 MHz limited bandwidth and centered at 869.538 MHz.

The interference power level at the generator's antenna collector has been set according to the following values:

1. negligible P_i ,
2. $P_i = -20$ dBm,
3. $P_i = -15$ dBm.

Such a signal allows to emulate all those situations in which the interference spectrum is wide enough to occupy the whole communication frequency interval, regardless of the center frequency.

The main results are summarized in Fig. 6.4: SE, calculated on the whole tags population, is displayed as function of d_s , from 0.75 to 6.0 m, and considering the listed power levels.

Beyond the worsening of identification capabilities as distance d_s increases, effect due to system inner characteristics as described in Section 5.2.2, SE suffers of a visible degradation upon the growing of interference intensity. SE calculated at the closest position, $d_s = 0.75$ m, is representative of the drastic degradation:

P_i	SE
Negligible	> 90%
-20 dBm	72%
-15 dBm	44%

Tabbed values are unacceptable for most RFID applications.

The measures demonstrate that the effect of the interference has not a preferential direction. In fact, tags are linearly polarized, and equally distributed along

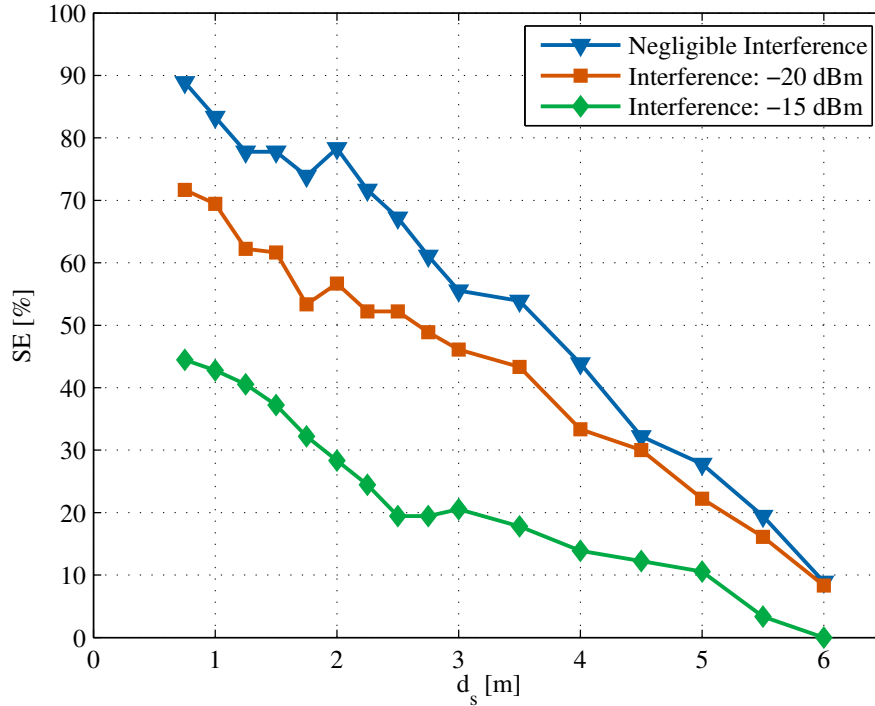


Figure 6.4: SE versus d_s , at three different interference signal power levels (1 MHz bandwidth AWGN centered at 869.538MHz).

the three directions of space: despite of the mixed disposition, the three curves reported clearly maintain their shape and trend, regardless of P_i ; this means that the interfering signal indistinctly affects the whole set of tags.

6.2.3 In-channel Noise (SIR)

Results given highlight that in-channel interference has a detrimental effect on the overall efficiency; however they do not allow to quantify the minimum level of admitted interference, beyond which the full functionality of the RFID system is guaranteed.

In order to identify thresholds, SE has been represented as function of Signal to Interference Ratio (SIR), which has been measured exactly where tagged boxes are placed; in particular, the following configuration has been set:

- $d_i = 2$ m,
- $d_s = 1$ m,
- $P_s = 30$ dBm,
- variable interference power intensity at AWG output from -30 to 0 dBm,

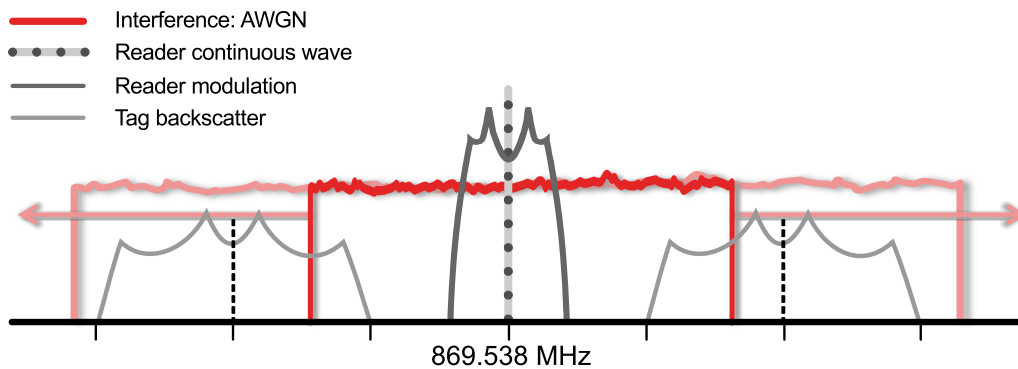


Figure 6.5: White Gaussian Noise with increasing bandwidth.

- bandwidth from 0.001 to 10 MHz.

The obtained outcomes are summarized in Fig. 6.6.

Measures show that *SE* has an upper limit at about 91%, despite of the interference level. As explained in Section 5.2.2, the effect is not due to the presence of the interfering signal: this is also demonstrated by upper bound which does not change, regardless of the presence or not of an interfering signal. In this case, a 9% *SE* loss can be considered and viewed as a systematic error (offset), due to the topology of the testbed setup.

Excluding offset as a consequence of interfering signals, the results in Fig. 6.6 highlight a strong susceptibility of UHF RFID system performance to AWGN interference, deducible from the evident *SE* decrease correlated both with noise bandwidth and power level.

The diagram suggests that *SIR* must be kept above proper thresholds, e.g. in the case of a 10 kHz bandwidth interference, the condition $SIR \geq 53$ dB must always be respected to maintain system functionality.

Table 6.1: Thresholds deduced from *SIR* analysis.

Bandwidth	<i>SIR</i> threshold
10 kHz	53 dB
30 kHz	65 dB
> 100 kHz	71 dB

From another point of view, the measures in Fig. 6.6 also suggest a relation holding between the threshold level of *SIR* and noise bandwidth.

The analysis, as sketched in Fig. 6.7, is quite interesting because it describes the admitted interference levels, for a given noise bandwidth, to ensure the desired reliability level. First of all, as highlighted above, the threshold shows

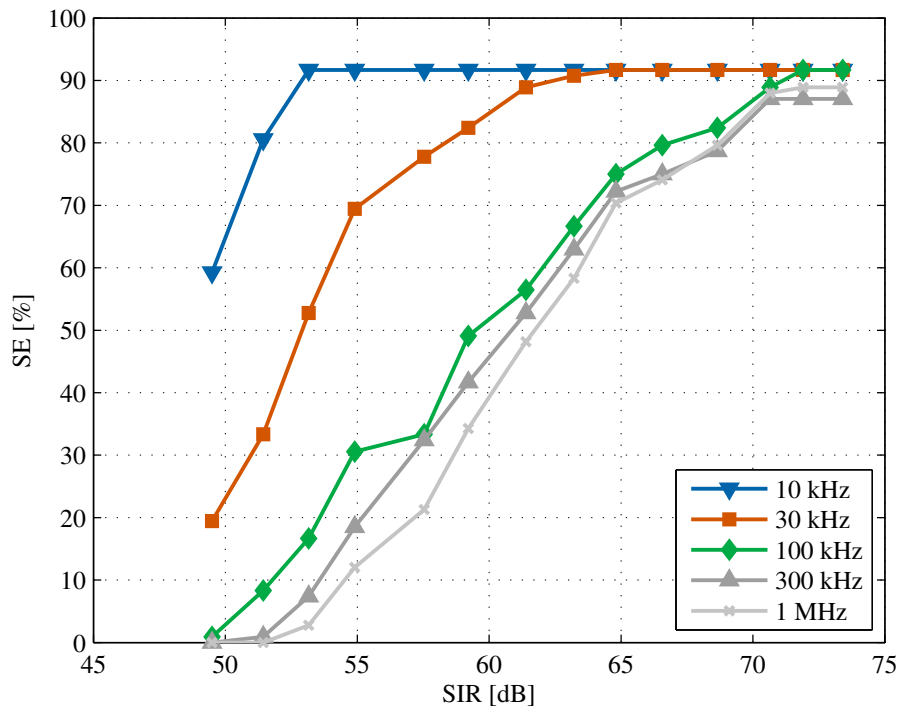


Figure 6.6: SE versus SIR measured at the container-box side. The full functionality is obtained only at very high values of SIR.

a clear saturation above 100 kHz. Furthermore, it's worth noting that before saturation, SIR threshold increases at a rate of about 18 dB/dec: this is an important experimental result, suitable to evaluate the admitted interference level with respect a certain noise bandwidth, within the tested frequency interval 1 kHz – 100 kHz.

6.2.4 In-channel Noise (BW)

In Fig. 6.8, SE is represented as a function of the interference bandwidth. In these measurements, reader's output power level and interferer's one are kept constant, equal to $P_s = 30$ and $P_i = -15$ dBm respectively. The following distances have been then considered: $d_s = d_i = 2$ m.

It is important to note that the displayed curve shows a sharp SE drop when the interference spectrum intersects the backscattered signal bandwidth (roughly near 100 kHz). For narrow (i.e. < 50 kHz) and wide (i.e. > 1 MHz) bandwidths, SE remains high: in the first case, a small amount of interference energy superimposes to the RFID system useful signal and, in particular, tags' backscattered signals are not disturbed. In the second case, SE returns high because the interference power intensity is spread on a large frequency inter-

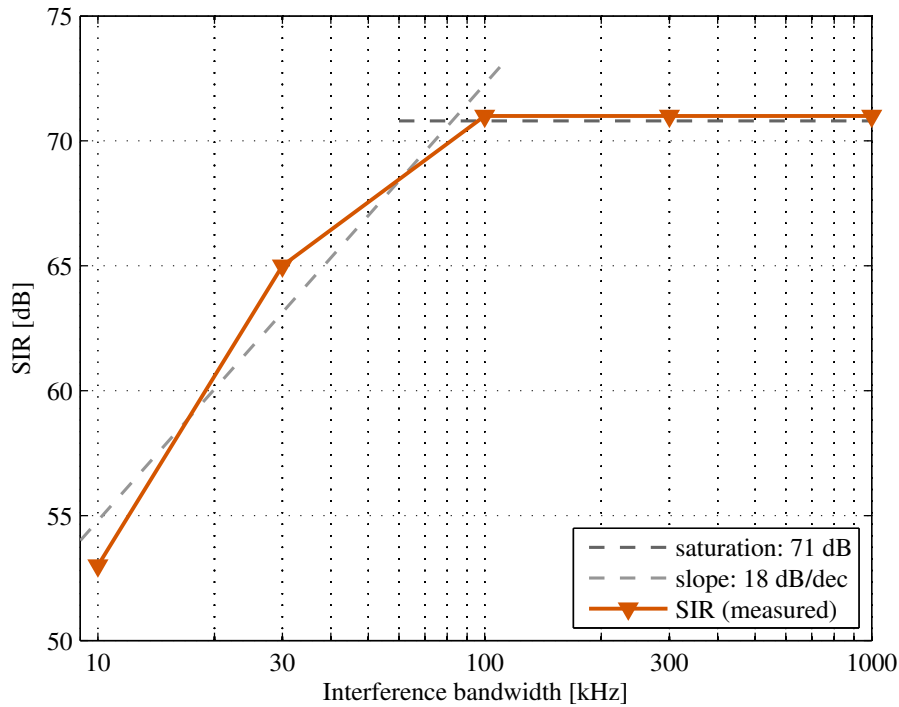


Figure 6.7: SIR as a function of noise bandwidth.

val. In fact, this condition corresponds to a higher SIR, therefore the reader can discriminate tags' responses above a lower noise floor.

6.3 Remarks

The experimental results clearly show that adequate SE levels can be guaranteed only with high SIRs. In particular, Fig. 6.6 highlights three thresholds, SIR_{tr} :

1. For 10 kHz interference bandwidth, $SIR > SIR_{tr1} = 53$ dB;
2. For 30 kHz interference bandwidth, $SIR > SIR_{tr2} = 63$ dB;
3. Above 100 kHz interference bandwidth, $SIR > SIR_{tr3} = 70$ dB.

The first two conditions are difficult to satisfy, because the interference must be exactly centered at the operation frequency of the reader; furthermore thresholds appear to be significantly correlated to the bandwidth, changing in the range [50 – 70] dB up to 100 kHz.

On the other hand, the setup with 100 kHz bandwidth or higher is much more

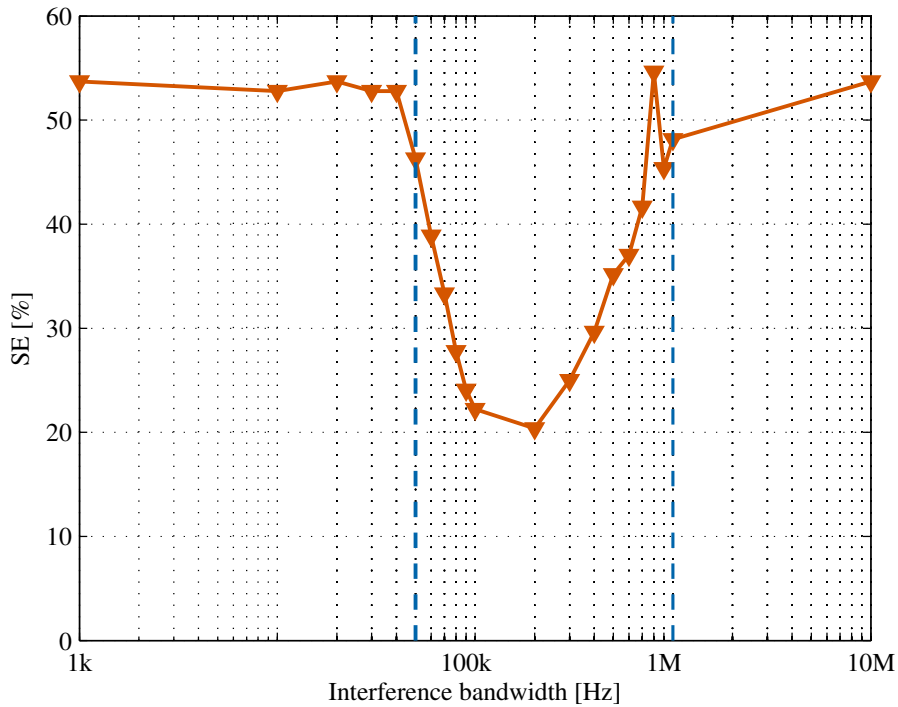


Figure 6.8: SE versus interference bandwidth, with $P_i = -15\text{dBm}$ constant.

meaningful, because it emulates the general condition in which the backscattered signal is disturbed (i.e. 100 kHz bandwidth is sufficient to intersect backscattered signal). For this reason, the results obtained with these configurations can be extended for any random signal interfering with the proper one in the frequency domain.

As a consequence, SIR_{tr3} can be considered a significant and representative parameter for the following two reasons: from one side, it is more restrictive, therefore it includes the former thresholds, SIR_{tr1} and SIR_{tr2} . From the other side, above 100 kHz, SE maintains its trend and the threshold remains constant, hence SIR_{tr3} may be taken as a lower bound: it represents the minimum admitted SIR for UHF RFID systems working at 869.538 MHz, in the general condition of disturbed RF channel.

The last consideration is also verified in Fig. 6.8: if the interference spectrum is wide enough, i.e. above 100 kHz, the backscattered signal is disturbed and the curve clearly shows a sharp worsening of system performance, confirming the threshold behaviour.

As said, SIR_{tr3} quantifies the weakness of the UHF RFID system in terms of the rejection to the interference signals: it is worth noting that $SIR_{tr3} = 70\text{ dB}$

is a quite high value if compared to the thresholds that should be respected in other wireless communication systems (*i.e.* nearly 10 and 20 dB respectively for 802.11b and 802.15.1 receivers [28]). In other words, UHF RFID systems should be maintained in a noiseless electromagnetic environment, at least in the UHF portion of the spectrum, to ensure the correct functionality.

It is important to state that worldwide, different portions of the frequency spectrum are assigned to UHF RFID, together with local limits to the admitted power emitted by the reader. For these reasons, the behaviour of the system should be slightly different, but the trend keeps the same, particularly for what concerns SIR thresholds.

Chapter 7

Performance optimization

Analysis of in-field applications highlighted how technological critical issues actually influence system performance, beyond the theoretic values which are always measured in non realistic conditions.

Results obtained disclose limits that UHF RFID system cannot overcome. However, the knowledge of such limits and their mechanism is important, because it gives the chance to obtain the desired performance through the proper tuning of system parameters and resources.

In this sense, theoretical discussion and measurement based verifications reported are useful means to obtain suitable rules for the setup of UHF RFID systems.

7.1 Operative Deductions

Basing on the outcome of the previous chapter, the starting issue is the definition of the portion of space in which the identification process has to take place. There are mainly (not only) three choices¹:

1. short range applications, below 1.0 m,
2. long range applications (a few meters),
3. very long range applications (ten meters and further).

As largely described in [21], for short range applications UHF RFID systems can work as reliably as HF RFID, especially for what concerns the capability of penetrating materials, one of the most discussed limit. [21] enlists several approaches to implements short range applications, making use of both standard

¹Proposed classification should not be considered general, but only useful for the purposes of the present work.

and “ad-hoc” devices, even exploiting the near-field properties of the reactive region. In this sense, the most effective solution for very short range applications (from centimetres to tens of centimetres) employs magnetic loop antennas for tags, or for both reader and tags. In the first case, tags are detectable only in proximity of the standard reader antenna, but standard tags may disturb, even if placed a few meters from the system. With the second solution, obtainable at cost of substituting both reader’s and tags’ antennas, only tags very close to the antenna can be identified, rejecting both the ones far placed and in some measure the closer ones equipped with a standard far-field dipole antenna, ineffective to backscatter a weak magnetic field.

Other short range applications (up to about one meter) can be implemented with standard devices, paying attention that antenna radiating region occupies the region to be scanned only. Again, far place tags may lead to improper detection.

For what concerns long range applications (i.e. logistics) passive tags are largely adopted. As largely discussed in Section 5.2.2, up to about 3 meters, passive tags constitute the most affordable solution, but particular attention should be paid to tag positioning and alignment. Tags placed orthogonally with respect the reader’s antenna surface have to be avoided: otherwise above one meter most of them will become mute.

As demonstrated, tags must be radiated by power levels higher than -10 dBm (at least), so they must be placed properly to guarantee activation. Otherwise, strategies such as *redundancy* have to be adopted (Sec. 7.2.1), because maximum interrogator’s power is limited by local regulations.

The simplest approach requires readers equipped with two or more antennas, properly placed to create a wider volume with EM intensity above -10 dBm. The reader used in the experiments has four interrogation outputs, and it implements the possibility of setting custom activation sequences of the antennas. As a consequence, it is possible to enlarge the reading region, or even improve the efficiency in the same one. As an example, antennas should be oriented with orthogonal surfaces, not sharing the propagation direction of radiated EM field: in this way, there is not a penalized direction², so the same tags, mismatched with one antenna, are matched for another, and vice versa.

There is an alternative to the problem of mismatched tags, especially in any applications that do not allow precise tag positioning: double dipole antenna tags. There exist transponder’s chips with two RF ports: two dipole antennas, perpendicular each other, get rid of the problem of one penalized direction.

²Penalization comes from polarization loss (refer to Section 5.1).

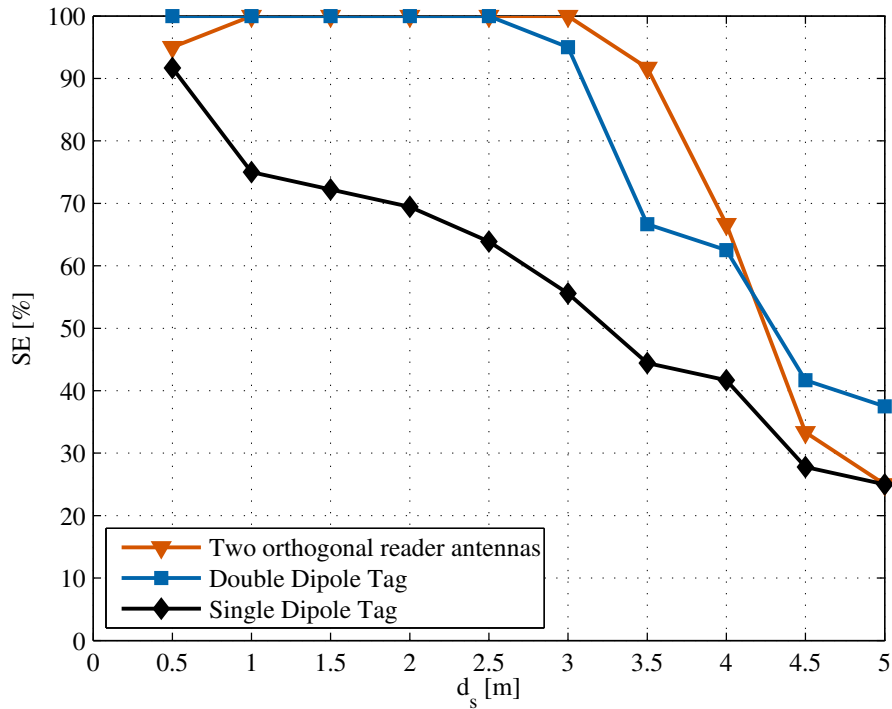


Figure 7.1: Comparison between SE measured using: (i) single dipole tags and one reader antenna RA; (ii) double orthogonal dipole tags, and one reader antenna RA; (iii) single dipole tags and two reader antennas RA, placed at the same distance d_s from the target boxes, along orthogonal directions.

Each mismatched antenna is associated with a matched one, so the tag is reachable no matter its orientation, compatibly with power level.

For very long range applications, with typical distances between reader's antenna and tags in the order of 10 meters or more, passive tags are not suitable any more: *battery-assisted passive* (BAP) tags and *active* tags are needed. Both tag typologies are powered by an internal battery, that is used to supply the internal circuitry.

In BAP tags, the RF output stage is not internally supplied, so the wireless communication remains based on backscatter, but limit of minimum P_t is removed. In active device, all circuitry is internally powered, so maximum distance can be increased with the output power, coherently with the inversion of eq. (2.4), now referred to the tag as independent transmitter.

With active tags, the physical limit is no more related to the minimum EM field intensity necessary to power a microelectronic circuit, but to the minimum RF signal detectable by the reader.

7.2 Performance optimization in non disturbed conditions

7.2.1 Redundancy

The *redundancy* approach introduced in the previous paragraphs shows interesting improvement, with no radical modification of the system. In Fig. 7.1 SE has been sketched, as measured from three different experiments:

- i. Single dipole antenna tags, and one interrogation antenna RA available at the reader side. These are the same conditions of experiments described in Section 5.2.2. $P_r = 30$ dBm.
- ii. Tags equipped with two dipole antennas: dipole antennas are linearly polarized, so the two are disposed orthogonal to each other. As said, this topology ensures that at least one dipole is correctly aligned with the reader's antenna. Reader's configuration is the same as point (i): one interrogation antenna RA active. $P_r = 30$ dBm.
- iii. Single dipole antenna tags. Reader's configuration is different: two identical antennas are available, and they are activated in series, not simultaneously. The two are placed at the same distance d_s , but along orthogonal directions. $P_r = 30$ dBm.

Measures clearly show a radical performance improvement of system efficiency. It's important to note that, with configurations (ii) and (iii) all tags are in the same conditions, no one of them suffer of penalizations due to polarization mismatch. As a consequence, the model of eq. (5.1) become valid for the whole population of tags, and the overall efficiency shows the expected threshold behaviour.

7.2.2 Reflective surfaces

One of the results of the analysis on interference effects (Chapter 6) demonstrates that the composition of reader's continuous wave with a replica has high probability to disturb the wireless communication.

One useful model that describes this phenomenon approximates the solution of Maxwell's equations by *ray tracing method*.

Considering the basic configuration sketched in Fig. 7.2, reader's antenna can be considered a fixed source emitting the RF wave:

$$s(t) = \cos 2\pi f_0 t \quad (7.1)$$

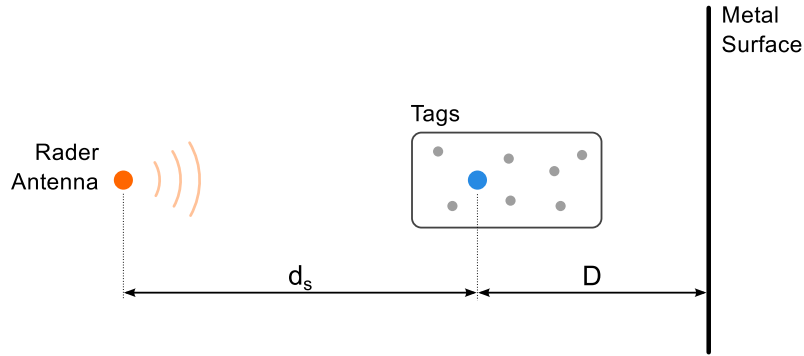


Figure 7.2: Illustration of the direct path from reader to a tag, and reflected path coming back from a reflective surface.

where $f_0 = 869.538$ MHz, in this particular case.

One from tags population in the target box is a fixed receiver placed at distance d_s from the source, and at a distance D ⁽³⁾ from a perfectly reflecting surface. The basic assumption is that, without the target tag, the EM field where should be located the receiving antenna is the sum of free space field coming from reader's antenna, and a reflected signal from the surface. Furthermore, the effects⁴ due to the presence of the receiving antenna are considered negligible. In the presence of ideal (infinite) reflecting surface, the reflected wave at a given point is the same as the free space wave that would exist on the opposite side of the wall if the wall were not present. In other word, with notation of Fig. 7.2, the reflected wave has the intensity of a free space wave at a distance $d_s + 2D$. In response to a transmitted sinusoid, it is possible to express the electric far field [20], at time t and in position $\mathbf{u} = (r, \theta, \psi)$:

$$E_r(f, t, \mathbf{u}) = \frac{\alpha(\theta, \psi, f) \cos 2\pi f_0(t - \frac{r}{c})}{r} \quad (7.2)$$

where r is the distance from the transmitting antenna, and (θ, ψ) the vertical and horizontal angles from the antenna to position \mathbf{u} , respectively. The function $\alpha(\theta, \psi, f)$ is the radiation pattern of the transmitting antenna, and $f_0 \cdot \frac{r}{c}$ is the delay due to travelling at the speed of light (c).

Using (7.2) for both the direct and the reflected wave, considering $r = d_s$ and assuming the same antenna gain α :

$$E_{ds}(f, t) = \frac{\alpha \cos 2\pi f_0(t - \frac{d_s}{c})}{d_s} - \frac{\alpha \cos 2\pi f_0(t - \frac{d_s + 2D}{c})}{d_s + 2D}. \quad (7.3)$$

³It is not D of eq. (2.3), that instead indicated the major physical dimension of an antenna.

⁴Perturbation of local EM field, and interference of the reflected component.

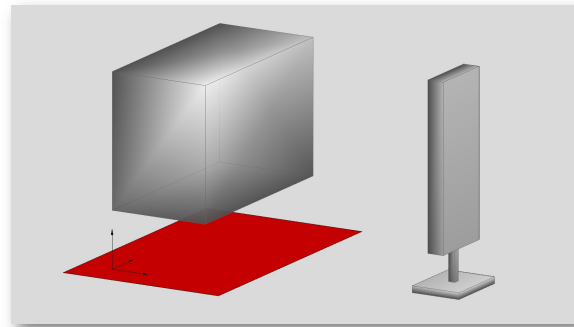
As said, the received signal is the superimposition of two waves of frequency f_0 and the phase difference is:

$$\Delta\theta = \left(\frac{2\pi f_0(d_s + 2D)}{c} + \pi \right) - \left(\frac{2\pi f_0 d_s}{c} \right) = \frac{4\pi f_0}{c} \cdot D + \pi. \quad (7.4)$$

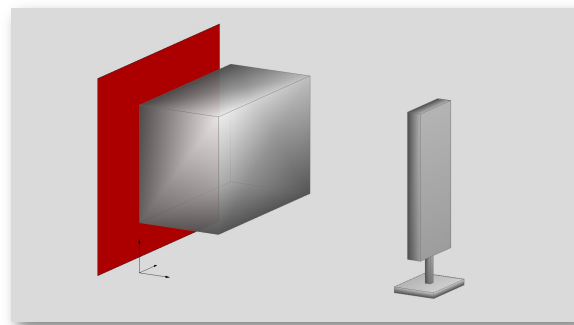
Where $\Delta\theta$ is an integer multiple of 2π , the two waves add *constructively*. On the contrary, where $\Delta\theta$ is an odd integer multiple of π , the two waves add *destructively*: the resulting signal is weaker. As a function of d_s , eq. (7.3) represents a spatial pattern of constructive and destructive interference. In such a pattern, the distance from a peak to a valley is $\lambda/4$ and it is defined the *coherence distance*:

$$\Delta d_s := \frac{\lambda}{4}. \quad (7.5)$$

The same consideration are valid for the **UHF RFID** system: in presence of reflecting surfaces, in the target volume a pattern of constructive and destructive



(a)



(b)

Figure 7.3: Disposition of metallic surfaces. Considering the standard $\{x, y, z\}$ reference systems, in (a) the metallic plane is disposed under the tagged target, on xy directions; in (b), behind target, on yz directions.

interference is created. This effect is not easy to be modelled in real-life application, especially in presence of multiple and different metallic surfaces, which have good reflection properties.

In this sense, if the metal surface is wide enough, that is larger than wavelength, it acts as a good approximation of the reflective surface described above, and its contribution in terms of reflective components may be non negligible. The use of metal plates can become an advantage, for two main reasons:

1. it can help to make the electromagnetic environment regular, that is, the reflection patter can be approximated with eq. (7.3), rather than a complex model of surroundings. This is an information useful to properly set the system.
2. The constructive pattern can be used to enhance power levels in certain regions of space, coherently with eq. (7.5), according to which $\Delta d_s := \frac{\lambda}{4} = 8.6 \text{ cm}$ at $f_0 = 869.538 \text{ MHz}$.

A set of experiments has been carried out to verify the previous sentences: the testbed has been modified and a square iron plate has been used as reflective surface (1.7 meters per side).

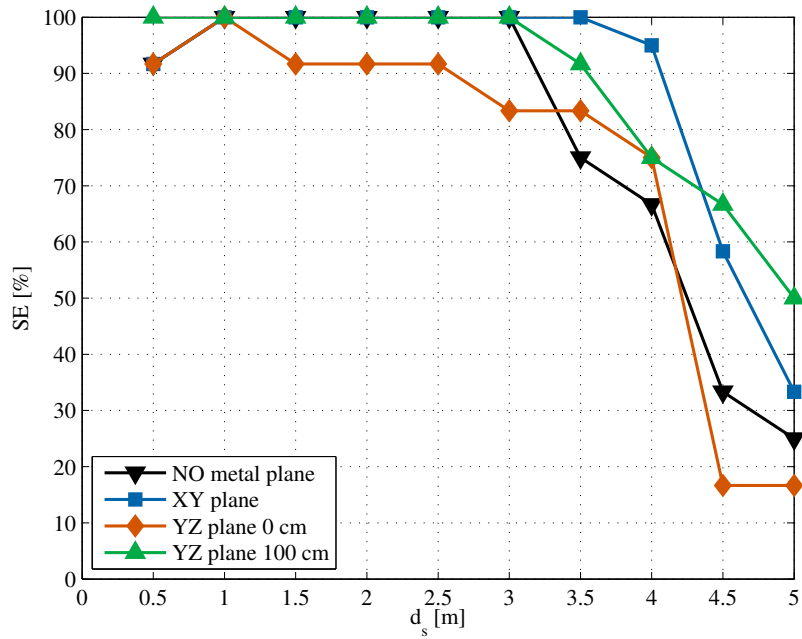
As expected, phenomena described are not simple to be tuned, so several different configurations have been tested, and in Fig. 7.3 the most representative are illustrated. In (a) the metal plate is disposed under the target box, 20 cm below the bottom side, on the ground floor; in (b), it is placed behind, facing reader's antenna.

The outcome related to the proposed configurations are sketched in Fig. 7.4. In general terms, it is possible to isolate improving conditions, but there are aspect to be discussed.

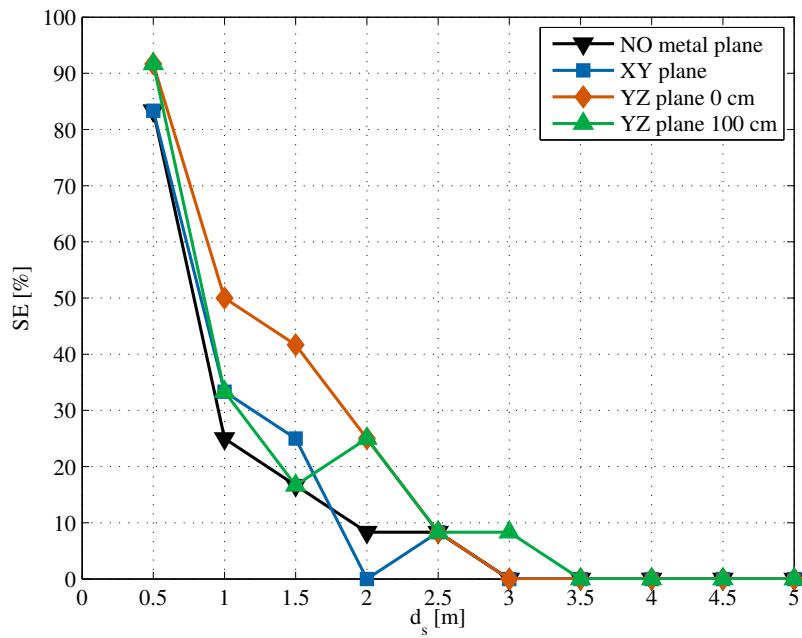
- (a) In Fig. 7.4(a), SE is measured considering only tags aligned with the direction y^5 (see scheme in Fig. 5.1): compared to the setup without obstacles, SE_y shows trends quite different, depending on the position of the metal plate. It is interesting to give evidence that performance improvements are observed with metallic surface placed on the ground floor (Fig. 7.3(a)), in a configuration that is completely different with respect the one modelled by eq. (7.3), with noticeable gain in terms of identified percentage, far from reader's antenna. In particular, full functionality is guaranteed half a meter beyond, with 95 % of correct identifications at 4.0 m.

On the other hand, the configuration with vertical surface placed behind

⁵For reasons of conciseness, the analysis on the y and z direction together has been omitted, because it leads to the same consideration given for SE_y .



(a)



(b)

Figure 7.4: SE_y (a) and SE_x (b) measured using metallic reflection surfaces, as illustrated in Fig. 7.3.

the target box and *adherent* to the rear side (Fig. 7.3(a)) has a general performance degradation: as discussed, the pattern of constructive and destructive interference modulates with distance, and it has higher strength if the surface is closer to the target. This is the reason why the disposition on plane yz has a general detrimental effect: at odd multiples of the pattern is destructive, and tags are non sufficiently fed. As a consequence, in-field measures are necessary to obtain better performance, as demonstrated by the outcome of the experiment with metal plate at 1.0 m from the rear side. This result demonstrate that such a short coherence distance (8.6 cm) does not allow to avoid regions of attenuated field, within the volume occupied by target box.

- (b) In Fig. 7.4(b), SE is measured considering only tags aligned with the direction x (see scheme in Fig. 5.1), that is SE_x : in this case, the outcome is symmetrical, with respect the one found for SE_y . The best performance is obtained with the metal plate adherent to the rear side of the target box, as a result of a constructive interference in a region of space where tags were not sufficiently fed.

In general, SE_x benefits from the presence of a reflective surface, in a proportion similar to that noticed for SE_y , but -20 dBm due to polarization mismatch remains a heavy penalization. Again the correct setup must be found with proper in-field measures.

It's worth noting that the effectiveness of the employment of a reflective surface must be properly evaluated, because improvements for a subset of tags population, may be detrimental for another.

7.3 Performance optimization in disturbed conditions – Immunity issues

Experiments clearly demonstrate that immunity techniques employed to allow complex RFID environments do not ensure rejection to in-channel interference. Experiments heavily stressed the radio channel and demonstrated that UHF RFID system can be totally muted by trivial jamming signals – this represent a very important issue of data integrity –, and moreover noisy environment may cause frequent fault conditions. This is mainly due to the fact that the wireless communication is based on amplitude modulation, which do not allow good performance in terms of interference rejection.

Experiments pointed out that unwanted signals become even more detrimental when interfering with tags' response signal. This behaviour suggests that the

reader cannot discriminate the the proper signal if mixed with spurious spectral components. This is the reason why shielding is mandatory in disturbed environment, or in any application which does not tolerate fault conditions. It's worth noting that experiments outcome also suggests that very sensible front-end circuitry at the reader input ⁶, may be completely useless if unknown interfering signals corrupt tag's response. Furthermore, precise circuitry is often fragile, so the interference may become even more dangerous because it should damage the RF front-end.

The stringent requirements of UHF RFID system, especially in terms of tag power consumption, forced the choice of amplitude modulation, but the future must be the employment of other modulation schemes, *i.e.* frequency modulation [29] or phase modulation, which demonstrates much less sensitivity with respect the variations of the environmental electromagnetic field. Further improvements may be achieved employing Code Division Multiple Access (CDMA) modulation schemes, which can ensure the discrimination of signals even if below the noise floor: usually readers do not have stringent power consumption limits, so they can carry out complex signal processing and calculations.

7.4 Considerations

The instructions given above have been deduced from the theoretical discussion, and from in-field measures: this should suggest that the most suitable setup is the result of both the knowledge of the actual limits of a physical system, and the experience gained with reliable measurements. In this particular field, the distribution of the EM field is very important, together with the spatial range of application: the setup must not leave aside the clear notion of these parameters, because they impose heavy limitations, that must be respected.

It is worth noting that where regulations allows higher power levels, *i.e.* 33 dBm at the reader output, the same consideration holds, with the exception that the boundary distance stretches coherently with equations (2.14) and (2.15).

At last, it is important to remember that the basic assumption for the present work is "stationary hypothesis": the same considerations remain valid for dynamic systems, but they also have to respect maximum speed restrictions. However, better results are expected because, the scanning capability improves if the containing box slides through the reading region. This fact is known and

⁶High gain and low noise input circuitry is more sensible to weak signals, so efficiency in terms of reading range is improved.

intentionally exploited to take both the advantages of near and far field regions. To this purpose, a careful design of the reader antenna dimension and shape antenna is always required.

Conclusions

In these years, the EPCglobal standard has greatly contributed to a significant enhancement of RFID applications based on passive tags and UHF technology, together with a worldwide diffusion.

Nevertheless, non trivial and unsolved problems are still delaying the wide spread of these systems in many practical applications. Starting from an experimental approach, the described results underlined the importance of preliminary measurements in the setup of the system, in order to estimate the achievable efficiency and reliability. As a result, several guidelines have been deduced considering singular features, and their composition allow to significantly enhance the overall functionality.

The proper optimization of system parameters, however, may be not enough, because modern RFID systems still suffer of low immunity to in-channel interference. Further experiments has been set up to intentionally disturb a typical inventory application, and estimate how vulnerable UHF RFID passive systems are.

The outcome highlighted that the most significant weakness is due to the amplitude modulation based communication: this aspect must not be underestimated because it exposes UHF RFID to functionality loss in presence of disturbed environment, and moreover reveals an important problem of integrity whenever interferences are intentional.

As widely said in literature, UHF RFID can be considered a powerful enabling technology, but unfortunately, it is not bug free. Desired performance is achievable, but much work has still to be done to obtain the necessary reliability, and maybe the next generation should implement the needed improvements.

Appendix A

MINERVA Project



In this chapter, the *MINERVA* project is described in broad terms. The overall project counted three main phases that correspond to: (i) the implementation of the wireless module with *RFID* functionality; (ii) the development of the software to drive the outcome of *RFID* interrogations to a base station; (iii) the implementation of a real-time data collection systems with remote access, and data retrieval.

The aim of this project is to demonstrate that *RFID* applications are also achievable with low cost and modular devices, which can be combined to create complex but still versatile systems.

A.1 Main Components

A.1.1 Tmote Sky

The Tmote Sky (Fig. A.1), and its equivalent implementations, is a wireless node widely used in *WSN*, and largely adopted for research purposes [30]. In detail, the Tmote Sky module is a low power “mote” with integrated sensors, radio, antenna, microcontroller, and programming capabilities. Here follows the most significant features:

- 250 kbps 2.4 GHz IEEE 802.15.4 Chipcon Wireless Transceiver;
- Interoperability with other IEEE 802.15.4 devices;

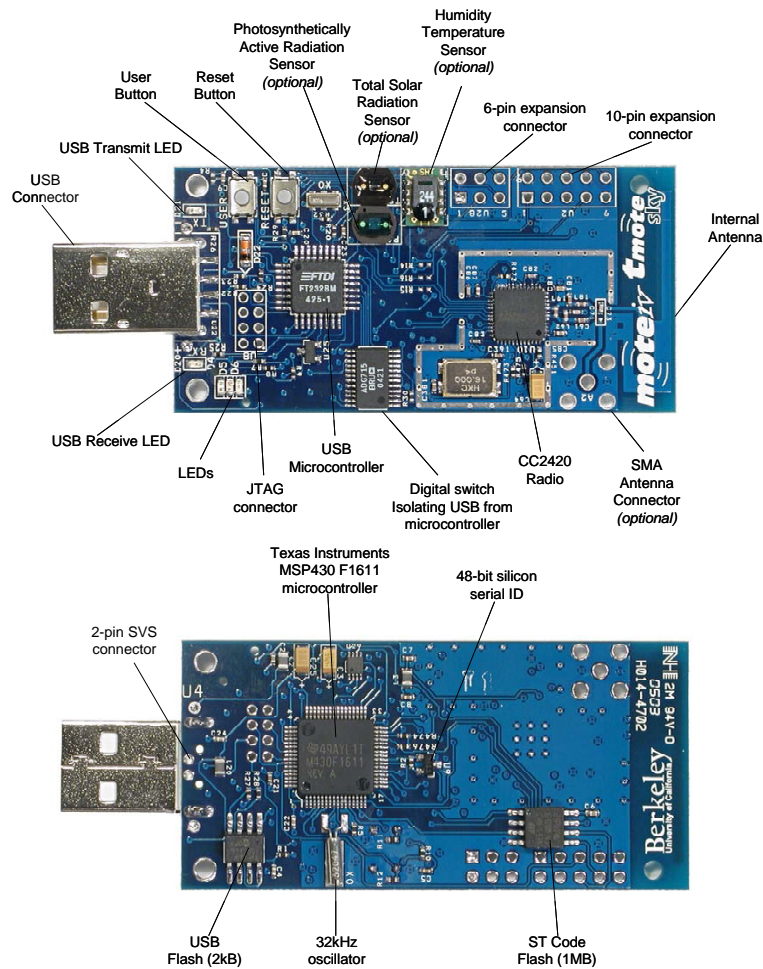


Figure A.1: Front and Back of the Tmote Sky module.

- 8 MHz Texas Instruments MSP430 microcontroller (10 kB RAM, 48 kB Flash);
- Integrated ADC, DAC, Supply Voltage Supervisor, and DMA Controller;
- Integrated onboard antenna with 50 m range indoors / 125 m range outdoors;
- Integrated Humidity, Temperature, and Light sensors;
- Ultra low current consumption;
- Fast wakeup from sleep ($< 6\mu\text{s}$);
- Hardware link-layer encryption and authentication;
- Programming and data collection via Universal Serial Bus (USB);

- 16-pin expansion support and optional SubMiniature version A (SMA) antenna connector;
- TinyOS support: mesh networking and communication implementation.

A.1.2 SkyeModule M9

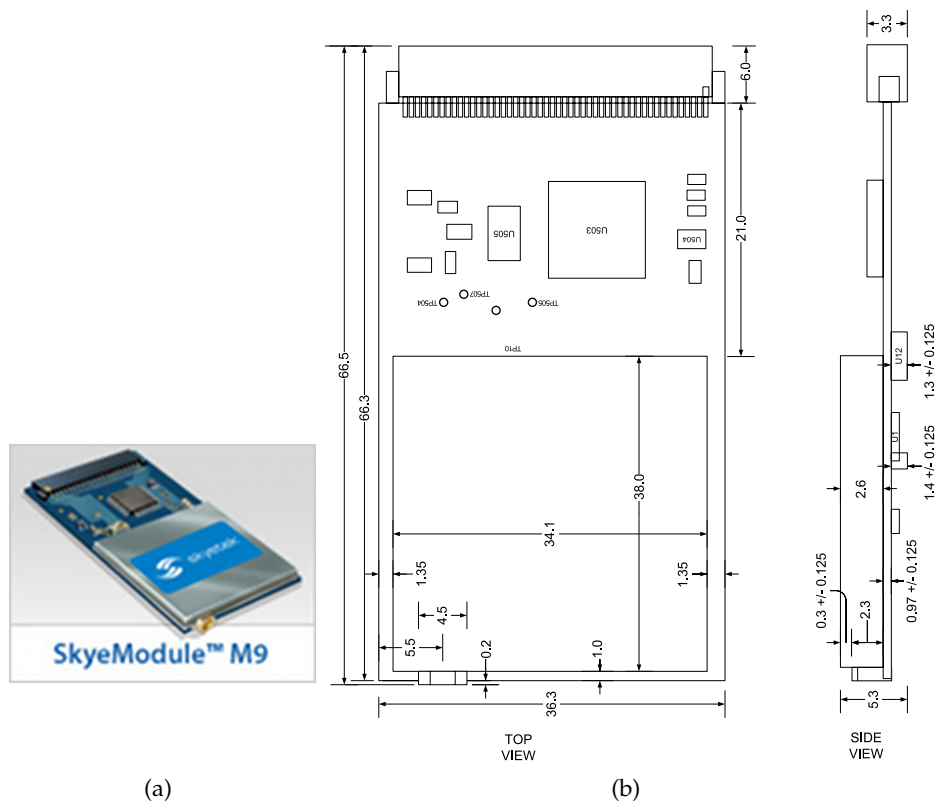


Figure A.2: Front and lateral of the SkyeModule M9.

The Skyetek SkyeModule M9 is a read/write low power RFID module, globally compliant with UHF EPC Class-1 Gen 1/2 and ISO 18000-6B tags; here the main features:

Protocols	EPC Class-1 Gen1 EPC Class-1 Gen2/ISO 18000-6C ISO 18000-6B
Protocol Features	Anti-collision Dense Reader Mode
Frequency range	862 – 955 MHz
Read performance	25 tags per second

Read range	8 dBi antenna: 2.5 m
Output power	Adjustable 10-27 dBm @ 0.1-0.5 dB steps based on power level Power Accuracy: ± 1 dBm
Transponder Communication Rate	EPC Class-1 Gen1: slow/fast modes EPC Class-1 Gen2/ISO 18000-6C: 40, 80 kbps ISO 18000-6B: 40 kbps
Communication interfaces	RS232 (Serial UART): 9.6 – 115.2 kbps SPI: Mode 1 up to 4Mb/s USB: 2.0 Full Speed 12 Mb/s
Dimensions	70 x 53 x 9 mm
Supply voltage	3.5 – 5.5 V
Consumption	Sleep mode: 5mA Idle mode: 170 mA Scan mode: 850 mA @ 27 dBm

A.1.3 Linksys NSLU2

Linksys Network Storage Link for USB 2.0 Disk Drives (NSLU2) is a network interface for attached storage devices: it shares USB hard disks or flash memories available over a network using the SMB protocol. The core of the device is the Intel XScale IP420 CPU (ARM-compatible): it runs a modified version of Linux which controls the two USB 2.0 ports where storage devices are connected. Here a selection of the main features:

Type	Network Attached Storage (NAS)
Operating System	Linux based
CPU	266 MHz Intel XScale IXP420 (ARM compatible)
Memory	32 MB SDRAM 8MB Flash
Connectivity	1x 10/100 RJ-45 Ethernet 2x USB 2.0
Standards	USB 1.0/1.1/2.0, IEEE 802.3, IEEE 802.3u
Dimensions	21 x 91 x 130 mm
Power Supply	5 V, 600 mA



Figure A.3: Linksys NSLU2.

By default, the NSLU2 runs a modified version of Linux, whose source codes have been released because of the terms of the GNU General Public License (GPL). With the availability of the source code, several communities started working on projects around the NSLU2, modifying both hardware and firmware, up to alternative operating systems.

In this context, the possibility of changing the operating system allows to transform the device in a general purpose low cost and low power computer. There are mainly two main firmware replacements: the one known as “Unslug” is based on the original firmware, and maintains whole compatibility and functionality, with some improvement. The alternative is th SlugOS/BE based on the OpenEmbedded Framework: the installation require an hard drive, but it allows the installation of a great number of expansion packages.

For the purposes of the project, the NSLU2 has been updated to a SlugOS/BE version.

A.2 The MINERVA module

The basic element of the modular approach is obtained combining two devices, that is the RFID reader module and the WSN node (Fig. A.4).

The M9 module implements different communication protocols, that is:

- Transistor-Transistor Logic (TTL) (or RS-232 but some additional circuit is needed),

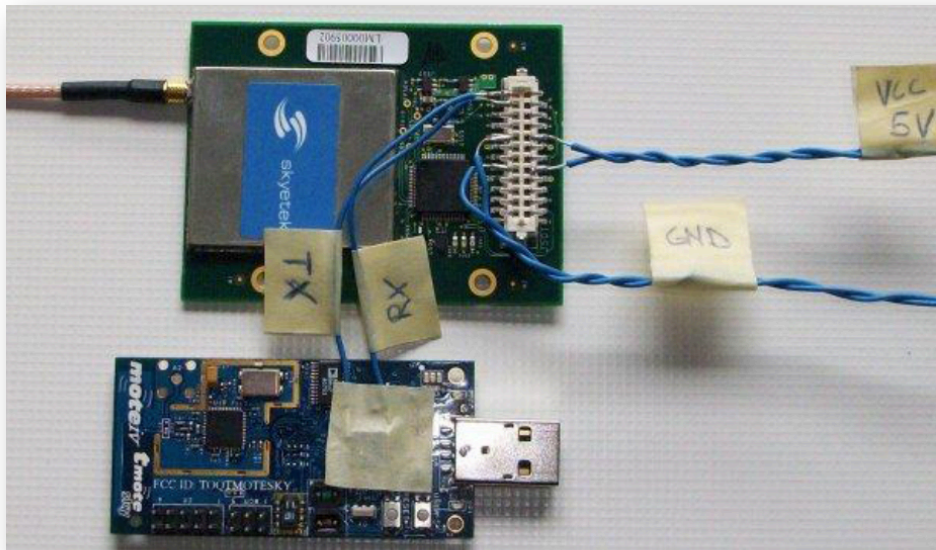


Figure A.4: The MINERVA Module, obtained combining a RFID reader module with a wireless sensor node.

- Serial Peripheral Interface (SPI),
- Inter Integrated Circuit (I²C),
- USB.

TTL has been chosen for the cabled communication link between the two modules, to satisfy and meet the connectivity limitations of the mote. TTL interface make use of two serial lines only, one for the signal transmission, TX, and one for reception, RX.

The Mote runs a particular operating system suitable for low power devices, the *TinyOS*, and programs are written in high level programming language (NesC): in this way the communication between the two modules has been implemented to run on the mote as master, which activates the functions of the M9 module, as slave. The communication employs the native protocol of the Skyetek module.

The main target of this implementation is to receive from the reader all data collected from the population of tags: because of the limitation of the SkyeModule M9, it is not possible to set how data is transmitted, so further computation on the TTL stream is needed, to extract the tags' IDs (and eventually additional data).

In a first stage, the task of data extraction was assigned to the mote, in order to

simplify the implementation of data transfer across a wireless network, towards a base station. However, the communication with the reader module requires high computation for the microcontroller, so it impedes the execution of a parallel task of stream interpretation. For this reason, the whole TTL stream, converted in a bit stream, must be forwarded to the base station, as it is, and the extraction of tags' data is done remotely.

The necessity of stream forward is an important limit because the continuous transmission is quite onerous, and, moreover it occupy the radio link for long. If tags' IDs can be extracted and stored in the mote, and transmitted only once that a certain amount of data has been collected, the transmission through the wireless network is optimized: first of all, additional bits used in TTL communication and useless in the RFID application, can be suppressed; second, RFID detection would not occupy the radio link until the task is completed. In this sense, the Tmote Sky is not appropriate for the assigned tasks, because higher computation capabilities are required. However, this implementation demonstrates that it is possible to create a RFID application using modular devices, and moreover it shows how the reader may become a "mesh" reader (Fig. A.5). A network of MINERVA modules creates a structure of distributed readers, each with limited performance if compared to industrial readers, but lower costs and higher versatility: considering, for example, items stored in a warehouse, the mesh allows the monitoring at shelf level.

A.3 The MINERVA gateway

The transmission over *ad-hoc* wireless networks, as well as the mesh architecture (Sec. A.2), requires an interface that implements the link with the computer network, mandatory in RFID applications with middleware and distributed databases. In this sense, a networked base-station is necessary: NSLU2 has this role.

In the proposed architecture, the NSLU2 is equipped with an external hard drive which is used to implement a local database¹, and with a USB plugged wireless node that connects the device with the wireless network.

Because of the limited computational capabilities of the mote, the TTL stream (transmitted across the wireless network) is interpreted by the NSLU2, and a general RFID interrogation is in practice a serial interrogation done by one wireless module at a time. However, once solved computation bottleneck, pa-

¹The hard drive is partitioned: one portion contains the operating system, the other is used to store in a database all the data obtained from the wireless nodes.

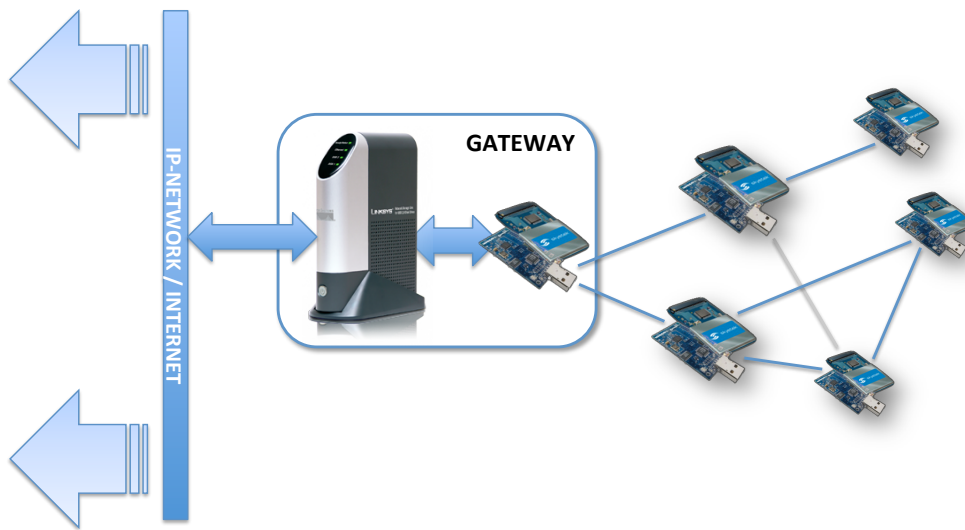


Figure A.5: Schematic view of the complete system: the module is used to set a wireless network of independent RFID readers, and through the wireless link data and other messages are transmitted to and from the gateway/base-station. The gateway forwards data in any IP network.

parallel functionality can be achieved, and so the NSLU2 become only the master of the mesh-reader, and its job is to collect tags' IDs and make them available over the IP network. In this sense, NSLU2 is the gateway.

In addition, all data collected from the network is stored in a local database, so applications have access to both real-time forward of tags' IDs, and also retrieval of data related to other interrogations (*i.e.*: useful in monitoring or tracking applications).

From the point of view of a generic RFID application, the gateway has the same role of a networked reader, so the typical operations (inventory, read/write, identification, etc.) are activated through proper methods and software requests, and resulting data is then forwarded. However, the gateway is not a reader: it translates application requests in messages to be send to the proper node over the wireless network, with several advantages:

- it is possible to gain spatial selectivity, addressing different nodes;
- the system is equivalent to a reader with virtually infinite antennas (in practice limited to the maximum number of wireless nodes);
- the RFID identification task may be executed far from the gateway, and data transferred node by node: long and expensive RF cables are avoided;
- system expansion is a simple upgrade of the wireless network;

- if the node can discriminate tags, it can send a message to the base station, and so a particular object can be localized: if one only module reports its presence, it is localized within the read range of the module, otherwise within the intersection of the read ranges.

Precise localization is possible, without the employment of UWB expensive transponders.

Bibliography

- [1] M. Bertocco, A. Dalla Chiara, G. Gamba, and A. Sona, "Experimental analysis of uhf rfid impairments and performance," in *Instrumentation and Measurement Technology Conference, 2009. I2MTC '09. IEEE*, pp. 759–764, May 2009.
- [2] S.-L. Chen and K.-H. Lin, "Characterization of rfid strap using single-ended probe," *Instrumentation and Measurement, IEEE Transactions on*, vol. 58, pp. 3619–3626, Oct. 2009.
- [3] K. Rao, P. Nikitin, and S. Lam, "Antenna design for uhf rfid tags: a review and a practical application," *Antennas and Propagation, IEEE Transactions on*, vol. 53, pp. 3870–3876, Dec. 2005.
- [4] S. Hodges, A. Thorne, H. Mallinson, and C. Floerkemeier, "Assessing and optimizing the range of uhf rfid to enable real-world pervasive computing applications," *Pervasive Computing*, vol. 4480, pp. 280–297, Aug. 2007.
- [5] V. Deolalikar, M. Mesarina, J. Recker, and S. Pradhan, "Perturbative time and frequency allocations for rfid reader networks," *Emerging Directions in Embedded and Ubiquitous Computing*, vol. 4097, pp. 392–402, Aug. 2006.
- [6] H.-P. Huang and Y.-T. Chang, "Robust design for rfid system testing and applications," in *Robotics and Automation, 2007 IEEE International Conference on*, pp. 4594–4599, april 2007.
- [7] J. Siden, P. Jonsson, T. Olsson, and G. Wang, "Performance degradation of rfid system due to the distortion in rfid tag antenna," *Microwave and Telecommunication Technology, 2001. CriMiCo 2001. 11th International Conference on*, pp. 371–373, 2001.
- [8] N. Tran, B. Lee, and J.-W. Lee, "Development of long-range uhf-band rfid tag chip using schottky diodes in standard cmos technology," in *Radio Frequency Integrated Circuits (RFIC) Symposium, 2007 IEEE*, pp. 281–284, june 2007.
- [9] S. Jain and S. R. Das, "Collision avoidance in a dense RFID network," *WiN-TECH '06: Proceedings of the 1st international workshop on Wireless network testbeds, experimental evaluation and characterization*, pp. 49–56, 2006.

- [10] D.-F. Tseng and Z.-C. Lin, "An anti-collision algorithm in rfid systems based on interference cancellation and tag set partitioning," in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pp. 1609–1614, May 2008.
- [11] M. Jo, S.-H. Cha, H. Choo, and H.-H. Chen, "Prediction of rfid tag detection for a stationary carton box," in *Sensing Technology, 2008. ICST 2008. 3rd International Conference on*, pp. 248–253, 30 2008-Dec. 3 2008.
- [12] M. Jo, H. Y. Youn, S.-H. Cha, and H. Choo, "Mobile rfid tag detection influence factors and prediction of tag detectability," *Sensors Journal, IEEE*, vol. 9, pp. 112–119, Feb. 2009.
- [13] R. H. Clarke, D. Twede, J. R. Tazelaar, and K. K. Boyer, "Radio frequency identification (RFID) performance: the effect of tag orientation and package contents," *Packaging Technology and Science*, vol. 19, no. 1, pp. 45–54, 2006.
- [14] Z. Min, L. Wenfeng, W. Zhongyun, L. Bin, and R. Xia, "A rfid-based material tracking information system," in *Automation and Logistics, 2007 IEEE International Conference on*, pp. 2922–2926, aug. 2007.
- [15] M. Borsero, A. Dalla Chiara, C. Pravato, A. Sona, M. Stellini, and Z. A., "Considerations about radiated emissions tests in anechoic chambers that do not fulfil the nsa requirements," in *16th IMEKO TC4 Symposium*, (Florence, Italy), pp. 825–830, Sept. 2008.
- [16] O. Pozzobon, L. Canzian, A. Dalla Chiara, and D. M., "Anti-spoofing and open gnss signal authentication with signal authentication sequences," in *NAVITEC 2010: 5th Esa Workshop on Satellite Navigation Technologies (Navitec 2010) & European Workshop on GNSS Signals and Signal Processing*, Dec. 2010.
- [17] C.-T. Huang, L.-W. Lo, W. ling Wang, and H.-L. Chen, "A study for optimizing the reading rate of rfid tagged cartons in palletizing process," in *Industrial Engineering and Engineering Management, 2008. IEEM 2008. IEEE International Conference on*, pp. 1138–1142, Dec. 2008.
- [18] H. Stockman, "Communication by means of reflected power," *Proceedings of the IRE*, vol. 36, pp. 1196 – 1204, oct. 1948.
- [19] K. Finkenzerler, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*. John Wiley & Sons, 2nd ed., May 2003.
- [20] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. New York, NY, USA: Cambridge University Press, 2005.
- [21] P. Nikitin, K. Rao, and S. Lazar, "An overview of near field uhf rfid," in *RFID, 2007. IEEE International Conference on*, pp. 167–174, March 2007.
- [22] H. Friis, "Noise figures of radio receivers," *Proceedings of the IRE*, vol. 32, pp. 419–422, July 1944.

- [23] EPCglobal Inc., "EPCTMRadio-Frequency identification protocols Class-1 Generation-2 UHF RFID. protocol for communications at 860 MHz – 960 MHz," *EPCglobal Standards*, 2005.
- [24] "Intermec Home Page." Intermec:
<http://www.intermec.com>.
- [25] K. Rothammel, *Antennenbuch*. Berlin: Deutscher Militärverlag, 1968.
- [26] J. G. Lee, S. J. Hwang, and S. W. Kim, "Performance study of anti-collision algorithms for epc-c1 gen2 rfid protocol," *Information Networking. Towards Ubiquitous Networking and Services: International Conference, ICOIN 2007, Estoril, Portugal, January 23-25, 2007. Revised Selected Papers*, pp. 523–532, 2008.
- [27] L.-C. Wang and H.-C. Liu, "A novel anti-collision algorithm for epc gen2 rfid systems," in *Wireless Communication Systems, 2006. ISWCS '06. 3rd International Symposium on*, pp. 761–765, Sept. 2006.
- [28] IEEE, "Ieee recommended practice for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements part 15.2: coexistence of wireless personal area networks with other wireless devices operating in unlicensed frequency bands," *IEEE Std 802.15.2-2003*, pp. 1–115, 2003.
- [29] S. Zheng, F. Yu, and Y. Zhu, "A novel rfid transceiver architecture with enhanced readability," in *Wireless Communications, Networking and Mobile Computing, 2007. WiCom 2007. International Conference on*, pp. 2074–2077, Sept. 2007.
- [30] "Tmote Sky Datasheet." Moteiv. <http://www.moteiv.com>.
- [31] V. D. Hunt, A. Puglia, and M. Puglia, *RFID: A Guide to Radio Frequency Identification*. Wiley-Interscience, John Wiley & Sons Inc., 2007.
- [32] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions*. New York: Dover, 1965.
- [33] J. Proakis, *Digital Communications*. McGraw-Hill Science Engineering Math, August 2000.
- [34] "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999)*, pp. C1–1184, June 12 2007.
- [35] "Wireless medium access control (mac) and physical layer (phy) specifications for wireless personal area networks (wpans)," *IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002)*, pp. 1–580, 2005.
- [36] "Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)," *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, pp. 1–305, 2006.

- [37] S. Y. Shin, H. S. Park, and W. H. Kwon, "Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b," *Comput. Networks*, vol. 51, no. 12, pp. 3338–3353, 2007.
- [38] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, "Assessing coexistence problems of IEEE 802.11b and IEEE 802.15.4 wireless networks through cross-layer measurements," in *Instrumentation and Measurement Technology Conference Proceedings, 2007 IEEE*, (Warsaw, Poland), pp. 1–6, May 2007.
- [39] I. Howitt, "Bluetooth performance in the presence of 802.11b WLAN," *IEEE-TOVT*, vol. 51, pp. 1640–1651, Nov. 2002.
- [40] J. Howitt, I.; Gutierrez, "IEEE 802.15.4 low rate - wireless personal area network coexistence issues," *Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE*, vol. 3, pp. 1481–1486 vol.3, 16-20 March 2003.
- [41] I. Howitt, "WLAN and WPAN coexistence in UL band," *Vehicular Technology, IEEE Transactions on*, vol. 50, no. 4, pp. 1114–1124, Jul 2001.
- [42] M. Petrova, J. Riihijarvi, P. Mahonen, and S. LaBell, "Performance study of IEEE 802.15.4 using measurements and simulations," in *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, vol. 1, (Las Vegas, NV, USA), pp. 487–492.
- [43] A. Koubaa, M. Alves, and E. Tovar, "A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks," *Factory Communication Systems, 2006 IEEE International Workshop on*, pp. 183–192, June 27, 2006.
- [44] J. Polastre, R. Szewczyk, and D. Culler, "Telos: enabling ultra-low power wireless research," in *Information Processing in Sensor Networks, 2005. IPSN 2005. Fourth International Symposium on*, pp. 364–369, Apr. 2005.
- [45] J. Polastre, J. Hill, and D. Culler, "Versatile low power media access for wireless sensor networks," in *SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*, (New York, NY, USA), pp. 95–107, ACM, 2004.
- [46] L. Angrisani, M. Bertocco, G. Gamba, and A. Sona, "Effects of RSSI impairments on IEEE 802.15.4 wireless devices performance susceptibility to interference," *Proc. of IEEE International Symposium on Electromagnetic Compatibility, EMC Europe 2008*, Sept. 8-12, 2008.
- [47] M. Zuniga and B. Krishnamachari, "An analysis of unreliability and asymmetry in low-power wireless links," *ACM Trans. Sen. Netw.*, vol. 3, no. 2, p. 7, 2007.
- [48] W. Kluge, F. Poegel, H. Roller, M. Lange, T. Ferchland, L. Dathe, and D. Eggert, "A fully integrated 2.4-gHz IEEE 802.15.4-compliant transceiver for ZigBee applications," *Solid-State Circuits, IEEE Journal of*, vol. 41, no. 12, pp. 2767–2775, Dec. 2006.

- [49] J. Crols and M. Steyaert, "Low-if topologies for high-performance analog front ends of fully integrated receivers," *Circuits and Systems II: Analog and Digital Signal Processing, IEEE Transactions on [see also Circuits and Systems II: Express Briefs, IEEE Transactions on]*, vol. 45, no. 3, pp. 269–282, Mar 1998.
- [50] S. Mirabbasi and K. Martin, "Classical and modern receiver architectures," *Communications Magazine, IEEE*, vol. 38, no. 11, pp. 132–139, Nov 2000.
- [51] P.-I. Mak, S.-P. U, and R. P. Martins, "Transceiver architecture selection: Review, state-of-the-art survey and case study," *Circuits and Systems Magazine, IEEE*, vol. 7, no. 2, pp. 6–25, 2007.
- [52] N. Wu, M. Nystrom, T. Lin, and H. Yu, "Challenges to global rfid adoption," in *Technology Management for the Global Future, 2006. PICMET 2006*, vol. 2, pp. 618 –623, july 2006.
- [53] "CC2420 2.4 GHz IEEE 802.15.4 Zigbee RF Transceiver." TI Product data sheet. <http://focus.ti.com/docs/prod/folders/print/cc2420.html>.
- [54] "EPCglobal Inc. Home Page." EPCglobal Inc.: <http://www.epcglobalinc.org>.
- [55] M. Bertocco, A. Dalla Chiara, G. Gamba, and A. Sona, "Experimental comparison of spectrum analyzer architectures in the diagnosis of rf interference phenomena," in *Instrumentation and Measurement Technology Conference, 2009. I2MTC '09. IEEE*, pp. 765 –770, May 2009.
- [56] L. Benetazzo, M. Bertocco, A. Dalla Chiara, G. Gamba, A. Sona, and M. Ponzin, "Enhanced use of rssi-based wireless network nodes for power measurement purposes," in *Instrumentation and Measurement Technology Conference, 2009. I2MTC '09. IEEE*, pp. 1037 –1042, May 2009.
- [57] M. Bertocco, A. Dalla Chiara, and A. Sona, "Performance evaluation and optimization of UHF RFID systems," in *Instrumentation and Measurement Technology Conference (I2MTC), 2010 IEEE*, pp. 1175 –1180, May 2010.
- [58] M. Bertocco, A. Dalla Chiara, and A. Sona, "Experimental analysis of uhf rfid system susceptibility to in-channel radio interference," in *Electromagnetic Compatibility Conference (EMC) Europe, IEEE 2010*, Sept. 2010.