THE SPECIAL QUESTIONS OF THE WIRELESS INDUSTRIAL COMMUNICATION AND THEIR LOGISTICS APPLICATIONS

István Ajtonyi

University of Miskolc, Hungary

Abstract: The paper gives an introduction and description of industrial communication types. It reviews the newest results of the RFID based identification. It describes the main problems of interaction of RFID systems and different wireless industrial communication systems with measurement results. The paper also deals with the communication problems in RFID systems.

Keywords: wireless networks, interferences, RFID systems

1. Wireless systems

Although the origins of radio frequency based wireless networking can be traced back to the University of Hawaii's ALOHANET research project in the 1970s, the key events that led to wireless networking becoming one of the fastest growing technologies of the early 21st century have been the ratification of the IEEE 802.11 standard in 1997, and the subsequent development of interoperability certification by the Wi-Fi Alliance (formerly WECA).
While the various Wi-Fi variants that have emerged from the original 802.11 standard have grabbed most of the headlines in the last decade, other wireless networking technologies have followed a similar timeline, with the first IrDA specification being published in 1994, the same year that Ericsson started research on connectivity between mobile phones and accessories that led to the adoption of Bluetooth by the IEEE 802.15.1 Working Group in 1999.
During this period of rapid development, the variety of wireless networking technologies has expanded to fill the full range of requirements for data rate (both high and low), operating range (long and short) and power consumption (low and very low).
As regards the transfer speed and the price, significant differences can be observed in the standards, that are illustrated in the fig. 1. and fig. 2.
Wireless networks now operate over four orders of magnitude in data rate (from ZigBee at 20 kbps to wireless USB at over 500 Mbps), and six orders of magnitude in range (from NFC at 5 cm to WiMAX, and also Wi-Fi, at over 50 km).
Wireless communication systems can be classified into three groups depending on the transfer and coverage distance:

- WPAN,
- WLAN,
- WWAN.

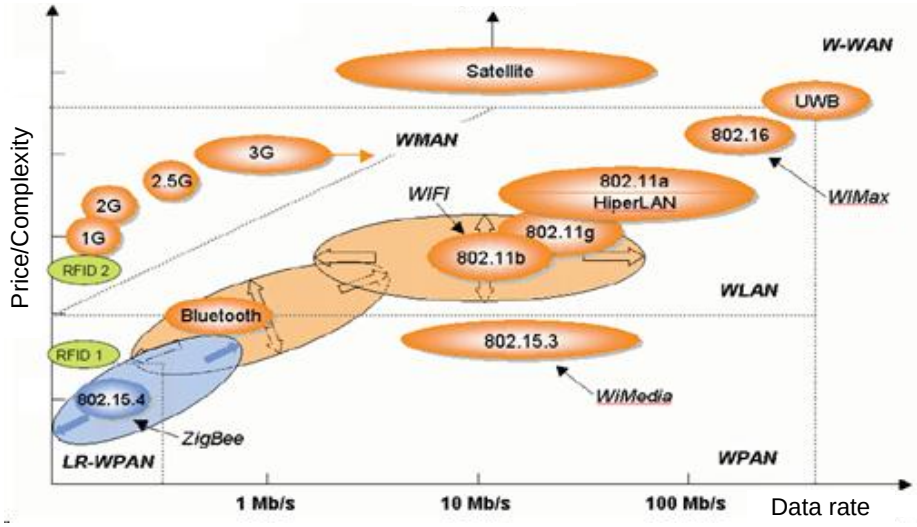

Figure 1. Transfer speed/price comparison for wireless communication techniques [2.]

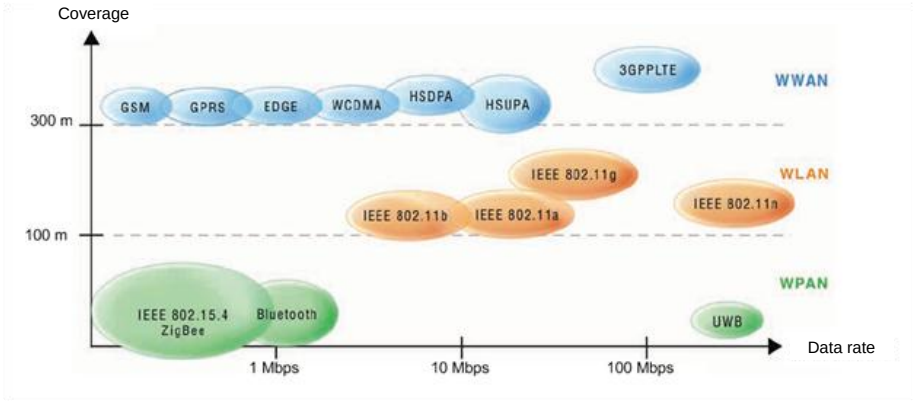

Figure 2. Wireless communication techniques classified by transfer distance [2.]

Types of these groups are shown in the fig. 3.

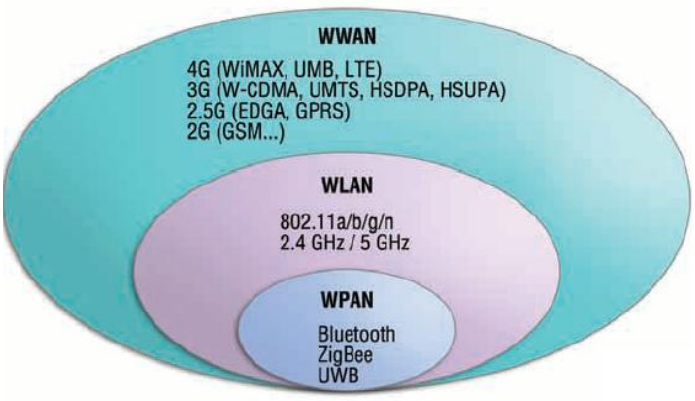

Figure 3. Types of wireless communication

At the present time, the following wireless techniques are used in the industrial applications:

- WPAN,
- WLAN,
- WWAN,
- Industrial Wireless Networks (WIHART, IWLAN, etc.),
- RFID,
- others.

The RF bands which are used for most wireless networking are the unlicensed ISM or Instrument, Scientific and Medical bands, of which the tree most important lie at 915 MHz (868 MHz in Europe) 2.4 GHz and 5.8 GHz (table 1). As well as these narrow band applications, new networking standards such as ZigBee will make use of the FCC spectrum allocation for ultra wideband radio (UWB - "Ultra Wideband Radio") that permits very low power transmission across a broad spectrum from 3.1 to 10.6 GHz.

Table 1. Radio frequency bands in use for wireless networking

RF band	**Wireless networking specification**
915/868 MHz ISM	Zigbee
2.4 GHz ISM	IEEE 802.11b, g, Bluetooth, ZigBee
5.8 GHz	IEEE 802.11a

Compared to traditional twisted-pair cabling, using RF transmission as a physical network medium poses a number of challenges, as outlined in table 2. Security has been a significant concern since RF transmissions are far more open to interception than those confined to a cable. Data link reliability, bit transmission errors resulting from interference and other signal propagation problems, are probably the second most significant challenge in wireless networks.

Table 2. Radio frequency networking challenge

Challenges	**Considerations and solutions**
Link reliability	Signal propagation, interference, equipment setting, link budget
Media access	Sensing other users (hidden station and exposed station problems). Quality of service requirements.
Security	Wired equivalent privacy (WEP), Wi-Fi Protected Access (WPA). 80211i, directional antennas.

The secure network connection and transfer are depending on the following factors:

- signal propagation,
- modulation methods (ASK, FSK, QPSK, DQPSK, 16QAM, 128 QAM, 256QAM, PSM, PAM),
- spreading methods (DSSS-Barker, DSSS-CCK, FHSS, THSS),
- wireless multiplexing and multiple techniques (TDMA, TDD, FDMA, FDD, OFDM, CDMA),
- transmitter power (~ 100 mW),
- antenna characteristics,
- antenna gain,
- receiver sensitivity, interference,

- receiver noise (theoretical thermal noise),
- industrial noises.

The bit error rate is depending strongly on the applied modulation methods. The results of measurements can be seen in the fig. 4.

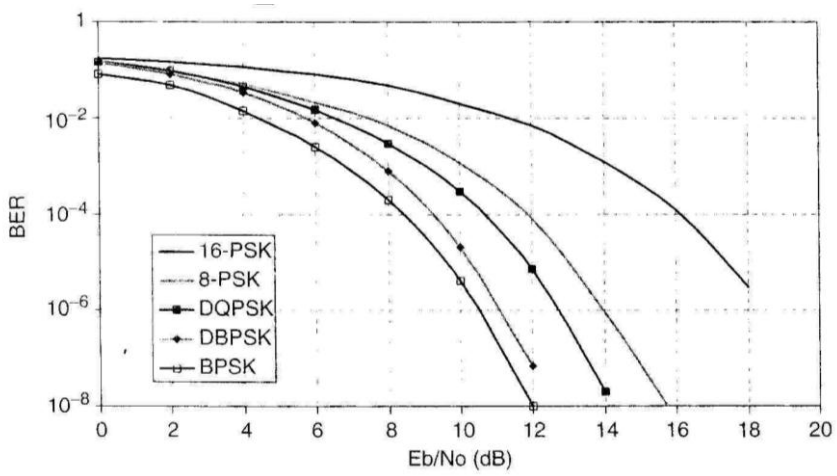

Figure 4. Bit Error Rate (BER) for some common modulation methods

2. RFID systems

An archetypal RFID system consists of an **interrogator**, more often known as a reader, a **transponder** or tag, and **antennas** to mediate between voltages on wires and waves in air (fig. 5.). The reader antenna or antennas may be integrated with the reader or physically separate and connected with a cable; the tag antenna is generally physically integrated with the tag. Most tags have at least one integrated circuit (IC), often known as a silicon chip, containing the tag ID and the logic needed to navigate the protocol that guides discussions between the tag and reader. There are tag technologies that do not use silicon ICs, though we will touch only peripherally on them in this book. The reader may contain a user interface of its own but more often will be connected to a network or a particular host computer, which interacts with the user to control the reader, and stores and displays thee resulting data.

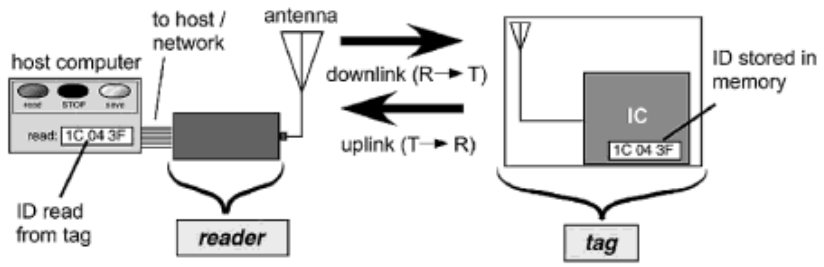

Figure 5. Overview of RFID system

A link in radio parlance is the data-carrying connection that exists between a specific radio transmitter and receiver. Although they occupy the same physical space and generally use the same antennas, engineers often distinguish between the communications channel carrying

information from the reader to the tag - the **downlink** or **forward** link-and that carrying information from the lag 1o the reader - the **uplink** or **reverse link**. In a real application, it is not unlikely that multiple tags will be present in the neighborhood of the reader, and also possible that many readers will be located in close proximity 1o one another.
Readers and tags usually live in a larger world of information storage and handling, from which point of view, an RFID reader is just another sensor, sharing that position with bar code scanners, keyboards touch screens and other data collection apparatus (fig. 6.). In a small organization, this infrastructure might consist of a database running on the local host or even a spreadsheet that just records the list of unique tag reads. In a large organization or company, operating activities are managed by a much bigger database, of ten known as an enterprise resource planning system (ERP), manufacturing resource planning (MRP), or perhaps a warehouse management system (WMS) depending on the context. Because an **RFlD** system is likely to distinguish between specific individual object rather than just between classes of objects, it may generate a lot more data than traditional tracking system. A whole class of software applications, generically known as RFID **middleware**, is arising provide a bridge between the ERP database and business processes and the newfangled RFID equipment. Though this matter is not a topic of the present volume, it is important for the reader to realize that the mere collection of data is not equivalent to the production of useful information, and the implementation of an infrastructure of RFID readers and tags should be regarded as the enabler for improvements in information handling and business process that create improved efficiency, rather than an end in itself.

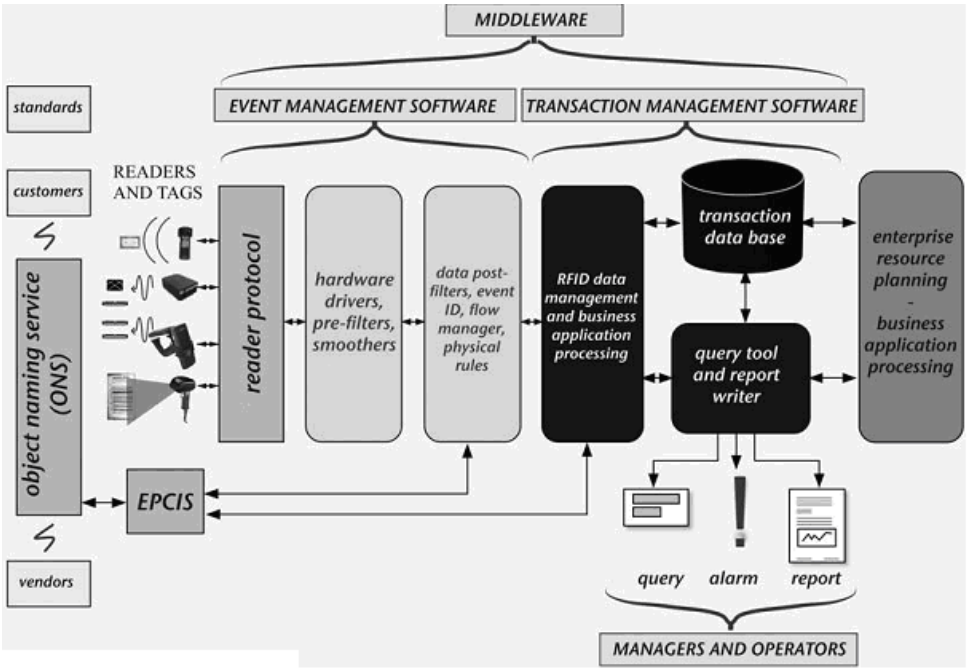

Figure 6. RFID as a sensor within an overall software infrastructure

Frequency Bands for RFID
RFID systems use frequencies varying by a factor of 20 000 or more from around 100 kHz to over 5 GHz (fig. 7.). Systems rarely operate arbitrarily across this vast swath of spectrum, most of the activity is concentrated in fairly narrow bands that have been made available

by regulators for unlicensed industrial activities. The most commonly encountered frequency bands at the 125/134 kHz, 13.56 MHz, 860-960 MHz, and 2.4-2.45 GHz. The 125/134 kHz systems operate within the low-frequency (LF) band and are often referred to as LF tags and readers. Readers at 13.56 MHz operate in the high-frequency band and are thus similarly characterized as HF systems.

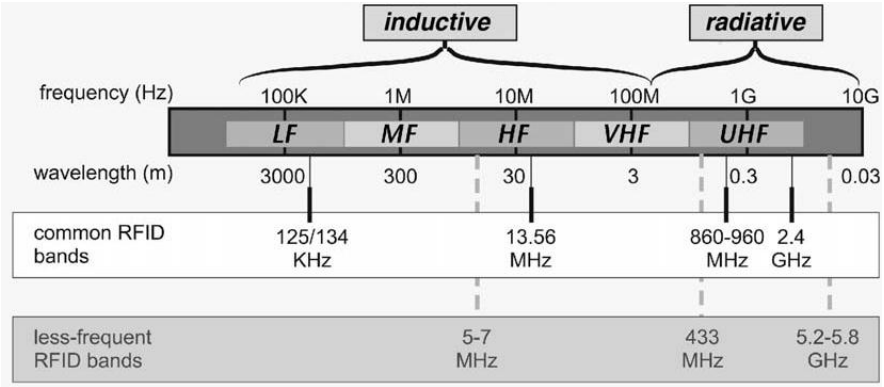

Figure 7. RFID frequency bands

Approximate values for the skin depth in differing materials at the most common RFID frequencies are given in table 3. (The values for water and animal tissue are rough estimates because the frequency dependence of the ionic conductivity has not been accounted for). It is apparent that at 125 kHz water and water-containing materials has essentially no effect on RFID operation and that a thin sheet of metal is readily tolerated.

Table 3. Skin depth for various common materials

Material	Skin Depth At			
	125 kHz	13.56 MHz	900 MHz	2.4 GHz
Tap water	8 m	2 m	4 cm	8 mm
Animal tissue	2 m	60 cm	2 cm	8 mm
Aluminium	0.23 mm	71 µm	2.7 µm	1.6 µm
Copper	0.18 mm	55 µm	2.1 µm	1.3 µm

Conclusions of the interference measurement carried out in at 900 MHz are represented in the fig. 8.

Since passive RFID is a short-range technology, the propagation issues of interest mostly have to do with indoor propagation and obstacle tolerance. Radio waves can get through obstacles in three ways:

- **Direct penetration:** many dielectric materials, like dry paper or cardboard, dry wood, nonconductive plastics, most textiles, and glass, are substantially non absorbing and have modest refractive indices (2-4) for 900 MHz radio waves. Such materials are sometimes known as RF-lucent. Radiation incident on lucent materials suffers modest reflections due to refractive-index mismatch – a refractive index of 3 causes a loss of about 3 dB per interface. Absorption is negligible. So many common materials that are solid obstacles for visible light are of moderate to negligible consequence for 900 MHz radiation. In contrast, metals reflect essentially all the radiation that falls upon them. Water, with a dielectric constant of around 80,

also reflects almost all of an incident wave and absorbs most of the rest. They are RF-opaque.

- **Diffractions:** visible light has wavelengths across. RF-opaque objects still cast shadows, but they are diffuse and not monotonic. A typical object a few wavelengths across casts a shadow about 10- to 15-dB deep, with a relatively shadow.
- **Reflection:** many objects in the indoor environment reflect radio waves. Dielectrics like glass reflect modestly at perpendicular incidence but rather effectively at glancing angles (greater than 70 degrees from the normal). Water and metal are excellent reflectors. Signals can bounce off a reflective object and illuminate a region that is shadowed from direct illumination by the reader antenna. Reflected waves add to or subtract from the direct wave from the reader antenna, causing the received signal strength to vary from place to place in a fashion that is complex and not readily predictable, even in a generally static environment. This variation is known as fading. Because of the limited link budget of RFID tags, RFID tags are usually close to and at least partially illuminated by the direct beam from the reader antenna, so fading is of less importance in RFID than in many other radio systems. However, it is still significant. Reflections particularly from the floor cause read zones to be discontinuous, with tags read at (say) 10 meters and not at 9. People are wonderful reflectors and will cause tags to be read or missed at the edge of the edge of the read zone as they move around, even when they are far from the direct beam from the reader antenna to the tag.

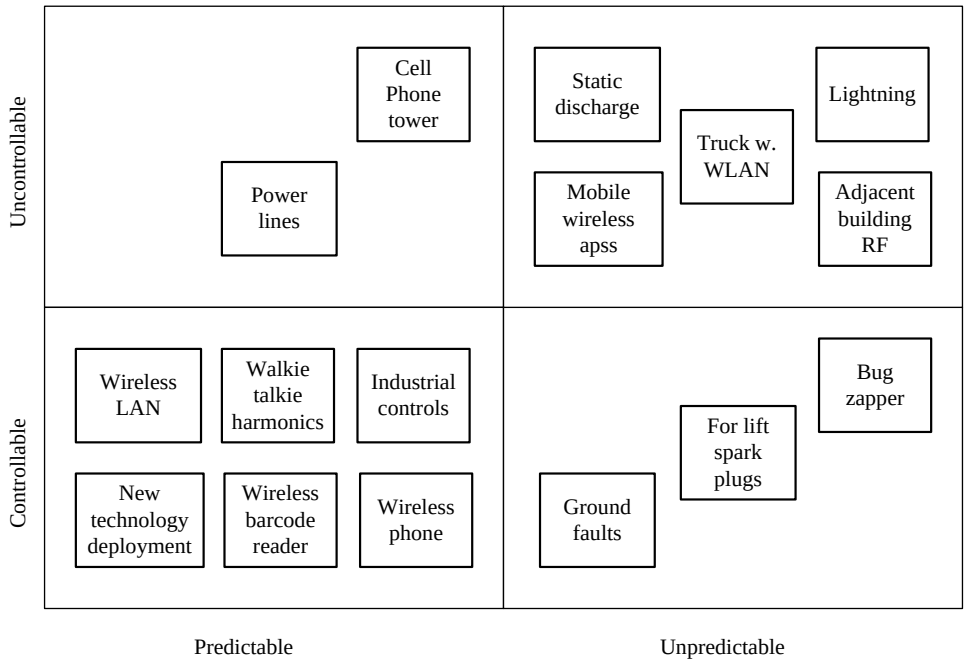

Figure 8. Sources of interference in the 900-MHz band, and their general properties

The recommended fields of application of RFID devices operating at various frequencies are summarized in the table 4.

Table 4. Common RFID frequencies and their usage

Frequency Range	Common Frequency	Common Uses
LF-Low frequency	• 30 kHz • 125 kHz • 134.2 kHz • 300 kHz	• Access control • Animal identification • Lot identification • Chemical process use • Distribution
HF-High frequency	• 3 MHz • 13.56 MHz (ISO 15693) • 30 MHz	• Logistic warehouse management • Automatic manufacturing and tracking • Retail • Hospitals • Baggage check • Library management • Parcel tracking • Security • Smart cards
UHF-Ultrahigh frequency	• 300 MHz • 433 MHz • 866 MHz (Europe) • 915 MHz (United States)	• Retail • Toll roads • Logistics-Inside a factory and through the supply chain • Long-range applications • Item tracking
Microwave frequency	• 2.45 Gigahertz • 3.0 Gigahertz	• Long-range applications • Item tracking • Freight tracking

Summary

Within the framework of TÁMOP (Social Renewal Operative Program) program an accredited laboratory has been established at the Department of Automation and Communication Technology, University of Miskolc, where combined use of wireless communication and RFID devices can be tested. Furthermore, in this laboratory we carry out individual R&D activities as well.

The Department has an own developed ZigBee wireless network. Currently, we have been working on the development of a ZigBee based RFID network the aim of which it to exploit the benefits of both standards. For achieving this goal we have had to develop ZigBee tags.

ZigBee tags communicate over the 802.15.4 protocol. The 802.11 protocol has high data communication rates at up to 54 Mbps while ZigBee transmits at a maximum of 250 kbps. ZigBee is an ideal choice for certain types of applications where data throughput is not an issue. A remote control is an example of a good ZigBee application.

ZigBee tags offer a longer battery life than Wi-Fi tags, and they do not require as much software embedded in the tag to implement the protocol. The protocol software is usually referred to as a "stack".

The ZigBee infrastructure does require ZigBee access points to be installed just like conventional active tag infrastructures. However, once a ZigBee infrastructure is installed it can be used to communicative with any ZigBee enabled device as well as ZigBee tags.

Another research topic of high priority we have been working on is to develop an indoor positioning system and generate a limited vocabulary from the RFID codes of products for assisting the blind or partially sighted people during shopping.

Acknowledgements
This research was carried out as part of the TAMOP-4.2.1.B-10/2/KONV-2010-0001 and TAMOP-4.2.2/B-10/1-2010-0008 projects with support by the European Union, co-financed by the European Social Fund.

References

[1.] AJTONYI, I.: Ip**ari kommunikációs rendszerek IV**. , AUT-INFO Kft., 2011
[2.] MOXA **Wireless Systems**
[3.] Honeywell Wireless Transducers
[4.] Infrared Data Communication
[5.] RACKLEY, S.: **Wireless Networking Technology**, Newnes, 2007
[6.] DOBKIN, D. M.: **The RF in RFID**, Newnes, 2007
[7.] Own research results