Technical State of Art of "Radio Frequency Identification – RFID" and implications regarding standardization, regulations, human exposure, privacy

Dominique Paret

PHILIPS Semiconductors
51, rue Carnot - BP 317 - 92156 Suresnes, France
dominique.paret@philips.com

Abstract

Starting from near and far electromagnetic field theory, the conference introduces the main principles used in Radio Frequency Identification - RFID i.e. inductive coupling or propagation using backscattering principle (batteryless / battery assisted) from LF 125 kHz up to SHF 5,8 GHz.

We will continue by introducing the main problems for reception of the small signals coming back from tag load modulations and demodulation mechanics and possible simulations. We will introduce also some new technological points such as Very High Baud Rate possibilities and relations between wafer processing / mounting and global tag cost.

We will conclude describing important inter relations between technical ideas, technologies, standardizations, regulations, human exposure, privacy, etc. .

1. Scientific basis

Scientific basis are quite simple, electromagnetic waves, close and far fields versus relations between wave lengths and working distances, Maxwell equations, propagation phenomena (including of course external environments, reflex ions, etc.) on one hand in UHF/SHF, Biot & Savart equations, inductive coupling on the other hand in LF & HF. Nothing new, all theses nice things are well known!

In addition to that, some functional, economical, RF regulatory issues, etc. considerations as "easy to use", "low cost", "worldwide application", as to be under consideration… and their direct interactions with new scientific basis as respectively Friis, radar equations, back scattering principle for UHF/SHF and detailed theories around magnetic coupling for LF/HF and for both, digital background and RF techniques (modulation, spread spectrum, etc.).

The purpose of this paper is to introduce in short words a global view of the technical dark side of RFID.

2. Technical background

RFID is used for contactless identification. In itself, the term contactless doesn't indicate any working distance (range).

RFID is globally classified in, "close distance", "proximity", "vicinity", "long distance" and "very long distance" which are related to techniques and local RF regulations. Let's have a look on technical issues first. We will come back to regulation later.

2.1. Basic technical background

The RFID system is built around two elements. The "base station" / "interrogator" (what people/press is calling with a wrong name of "reader") and the "tag".

a) Base station contains a transmitter part able to deliver some radiated power on a carrier frequency and a receiver part able to receive the (small) signal coming back from the tag.
b) Tag includes an antenna, a device including identifier element and/or memory- "chipless" (for example, SAW) or "with a chip"(integrated circuit) - and in some case a battery (see bellow). 99% of the market is using tags with chips.

Many technical problems have to be solved in RFID in order to establish the communication between base station and tag.

a) The first one is to succeed to supply the chip. Two possibilities exist.
   - The electromagnetic radiated energy supplies by the base station (via Poynting vector in UHF/SHF or induced e.m.f due to magnetic coupling in LF/HF) is able to deliver sufficient power to supply the electronic of the tag. In this case the tag is "batteryless".
   - the collected radiated energy is not sufficient to supply the chip and a local battery has to be on board of the tag to supply its local electronic. In this case the tag is "battery assisted"
b) The second one is that the input (receiver) sensitivity of the tag has to be sufficient to demodulate the incoming commands from the base station
c) For the third one, the answer from the tag (signals coming back from the tag) has to be higher than the minimum sensitivity of the base station receiver. Here also several possibilities are existing.
   - the tag is only designed to respond to the commands coming from the base station. In this case, base station – tag is a TRANSmitter – resPONDER couple, i.e. a TRANSPONDER.
   - the tag can emit on its own a carrier and the global system is a pure bi-directional TRANSmitter reCEIVER i.e. TRANSCEIVER

2.2. Remarks

If the return link, from tag to base station is based on a re-radiated signal from the tag (using for example an tag antenna "load modulation" and back scattering techniques), the tag is called "passive". If the return link, from tag to base station is based on a radiated signal from the tag (using for example a reel RF emitter on board) the tag is called "active".

The "passive" and "active" adjectives are not related to the presence of a battery on board of the tag but only to the process used for the return communication link !!!

2.3. Some additional techniques

RFID life is not easy. Signals coming back from tag to the base station are very weak, environmental noise is high, S/N is low, absorption and reflections are existing, multiples tags can be present simultaneously in the electromagnetic field, other tags can already speak, etc. etc.

To solve this large number of problems additional techniques must be used. Giving some indications

a) The spread spectrum or similar techniques can be used when permitted by local regulations. Very often (mainly in US due to FCC facilities), Frequency Hopping Spread Spectrum – FHSS- is used to solve disturbances due to reflection problems. Direct Sequence Spread Spectrum – DSSS is used to improve detection level in case of very low S/N ratio. With some minor performances, due to local regulations (ETSI), in most European countries, it is possible to use Frequency Agility techniques as Listen Before Talk – LBT
b) The process to solve collisions problems between tag communications (what people/press is calling with a wrong name of "anti collision") has to be implemented. In order to solve different issues, two different branches of solutions exist. Deterministic (at the bit level) and Probabilistic (Aloha times slotted)
c) The base stations RF input stage and demodulators have to be carefully designed using sometimes mono-static or bi-static antennas structures, circulators or bi-directional couplers, I/Q digital demodulators for Manchester Sub-carrier, FM0, (D)BPSK, QPSK, x-QAM, digital filtering and other DSP techniques in order to avoid "zero lines" demodulations.

3. Technological background

Improve communication/working range! Reduce the cost! Always the same (crazy) story! … and technology is behind that. Now to be serious.

In order to improve the communication range, the chip consumption must be reduced at a minimum. With actual technologies chip manufacturers reach some tenths µW … but the other very significant parameter to improve communication ranges is the value of EIRP powers delivered by base station … which are limited by local regulations!

What is possible to reduce the cost at the technological level? Reduce the size of the gates, reduce the die size, and increase the number of part per wafer. Well. Today standard production is based on 8" wafer and 0,18 mm transistors. To-morrow production will be 12" and 30 nm. With new silicon technologies, the surface of the die will decrease (example from 1 mm² to 0,5 mm² even less) and, at the end, sawing lanes silicon to separate dies each other on the wafer will consume more silicon that the dies themselves!

The right answer is not to reduce the cost of the die but to implement more functionalities on the chip in order to offer more applicative possibilities for the same price, i.e reducing the global price!

4. International Standardization

Looking to RFID applications, all RFID frequencies have physical advantages and drawbacks in terms of attenuation, field shaping, absorption, reflection, etc. There is not only one frequency able to do everything! Due to these conventional physical considerations, the JTC1 SC31 (Automatic Identification) from ISO decided to standardize the "Air Interface" (Physical Layer and Data Link Layer of the OSI model) for all possible RFID frequencies inside the JTC1 SC31 SG3 WG4 committee.

ISO 18 000 – 2	for frequencies below 135 kHz
ISO 18 000 – 3	for 13,56 MHz
ISO 18 000 – 4	for 2,45 GHz
ISO 18 000 – 6	for 860 – 960 MHz
ISO 18 000 – 7	for 433 MHz

Complete set of standards was released in September 2004. In addition to that, an additional set of "conformance tests" is in preparation – ISO 18 047 –x ("x" is related to the frequency value in accordance to ISO 18 000 – x) and also a "performance test" ISO 18 046 – x is also in preparation.

5. RF Regulations

Technique is technique but must be in accordance with regulations and mainly with local regulations.

In accordance to ITU, World is divided into 3 regions + space. FCC 47 part 15 gives guidance's in USA/Canada, CEPT & ETSI (ETSI 300 330 & 220) and ERC (ERC 70 03) in Europe (en France AnFR et ARCEP ex ARP), ARIB (ARIB STD T81) in Japan, and so on. Of course, due to a lot of historical reasons, there is not a full WorldWide regulation harmonization and big differences still exist between national states in terms of RF pollutions (in dBµV/m or dBµA/m in LF & HF bands), radiated power (ERP and EIRP in UHF & SHF), dwell ratio (occupation duty cycle), spread spectrum facilities, etc.

Due to these numerous differences, RFID operational ranges are strongly dependant on local regulations and global commercial advertisements have to be studied very carefully to avoid large misunderstandings and nice dreams.

6. Human exposure aspects

As other RF techniques RFID is submitted to "human exposure" aspect, mainly for long range applications where radiated powers are more important. In accordance with "World Health Organisation"- (WHO) and - International Commission on Non-Ionizing Radiation Protection (ICNIRP) standard and recommendations, SAR - Specific Absorption Rate - measurements are realized on are "robot". Long range RFID systems designed in accordance to existing RF regulations (at max. EIRP) are many dB below the maximum values.

7. Privacy issues

Radiation is radiation! When you radiate some information via RF, you always can receive them somewhere. Now, to reach the intrinsic content of the information it could be an other story.

Regarding privacy, some distinctions must be done between protected and secured data.

- "protected data" means that the air interface communication is/could be not secured … but the physical access to the data (address, etc.) into the tag memory is protected and can be reached only via secured password, rolling code, etc.
- "secured data" or "secured communications" means that the communication into the communication medium (the air) is ciphered (with crypto algorithm like DES, 3xDES, AES, RSA, ECC, etc.) and communication privacy is assumed.

For consumer applications (for example : electronic labels), if tags have not these facilities on board, a simple “kill bit” can also be implemented in order to “kill” the access to the tag to preserve privacy of the content of the memory

8. conclusions

RFID is a mixture of many accurate analog and digital techniques, which cover all kind of modulations and demodulations principles and digital processing in order to recover original data.

Three kinds of borders around RFID techniques are installed. The first one is directly related to technology possibilities, the second are existing ISO international standardizations for interoperability purpose, the last one are local regulations compliances.

For further reading…

[1] Paret D. (2002) *RFID et Cartes à puce sans contact - Fundamental*. DUNOD, Paris, 250 pp.
[2] Paret D. (2003) *RFID et Cartes à puce sans contact - Application*. DUNOD, Paris, 350 pp.
[3] Paret D. (2005) *RFID and Contactless Smart Cards - Applications,* John Wiley, London NY, 410 pp.
[4] Paret D. (2006) RFID in UHF & SHF, DUNOD, Paris, John Wiley London, NY, 650 pp.