

RFID: Talkative

by Klaus Bäumer

Have Aldous Huxley's "Brave New World" fantasies already become reality? Fiction becomes very real with the replacement e.g. of usual barcode tags used on almost every product by intelligent microchips. The magic word is „RFID“.

“RFID is a radio technology enabling touchless identification of objects and living entities. Present application foci are the areas of logistics and security. But conceivable applications may seem almost unlimited.”

The technological principle behind communication via RFID (Radio Frequency Identification) is really not so new. It has been applied for more than 60 years in aviation, and nowadays is a crucial component of security as a secondary radar principle resp. collision warning system. Airplanes are equipped with a so-called transponder, i.e. a combination transmission/reception device, that automatically sends back information such as identification, flight height, course, speed and rates of change when receiving a radar signal.

RFID technology links this functional principle with the possibilities of modern chip construction. So-called smart tags are the result, which can be classified as another member of the family of identification systems. In contrast to magnetic stripe cards or conventional chip cards, smart tags allow contactless data interchange, and they are able to store more data than the barcode system. Most smart tags do not need energy supply, and some types can be re-written several times.

Technology

There is a great variety of systems. However, they are all similar with regard to the basic functioning of two discrete functional units, the **reading/processing device** and the **transponder**. As soon as a transponder enters the electromagnetic field of the processing device, stored data is sent.

When categorizing transponder types according to their “intelligence”, **1-bit transponders** are the group of the simplest structure and functionality. They have no chip and actively communicate only one status message: “A transponder is within reading range of the processing unit”. 1-bit transponder operation is based on simple physical effects. In one group, tran-

tags

sponders consist of a resonant circuit tuned to the operation frequency of the reader. Their presence in the detection area is then in general recognized by drawing energy from the field of the processing unit. Another group operates in the microwave range. The resonant circuit is constituted by a dipole and a capacitive diode (technical term: varactor). The diode's nonlinear characteristic creates i.e. integer multiples of the operation frequency. They are reflected from the transponder and thereby detected.

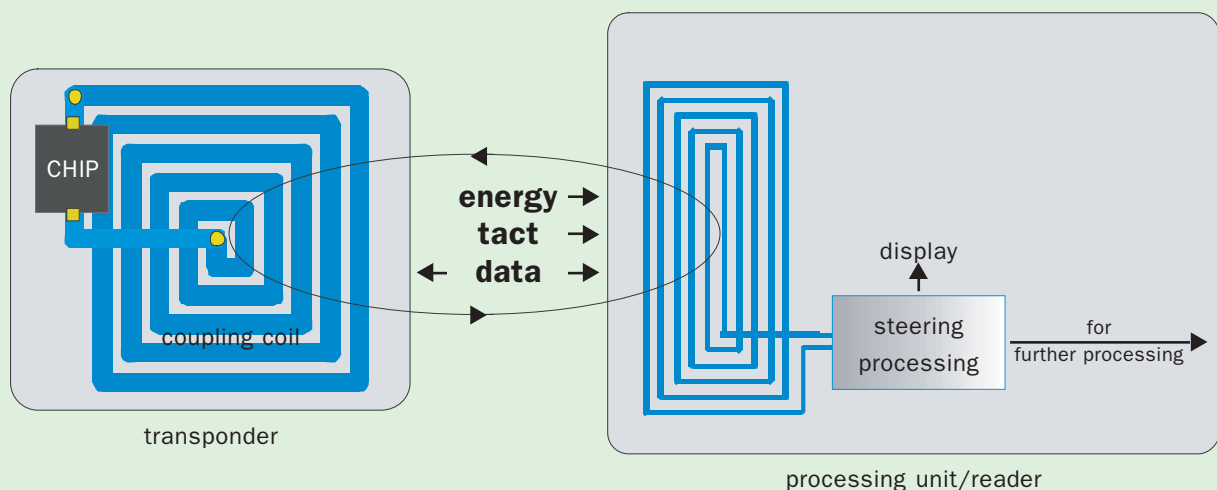
A third group operates in the long-wave range according to the frequency division principle. The presence of a transponder is again detected by the reflected energy of a certain frequency. Other techniques use magnetic hysteresis effects in metal strips or magneto-acoustic effects in certain metals occurring in the low-frequency range. Transmission power may not exceed 0.5 W in the EU. Actual radiation power levels vary widely across systems and manufacturers. This technique is already established in retail business as the **EAS system** for electronic theft protection.

Depending on the type, the security transponder is either removed at the cash register or functionally destroyed by a strong magnetic field.

The second group, **read-only transponders**, are functionally comparable to the barcode. They are integrated in the product, or permanently attached; and they communicate the product's identity over its entire life span. Read-only transponders are not rewritable; data memory capacity amounts to a few hundred bits. The third group, **read-write transponders**, are equipped with computerized functions. Aside from the radio frequency component for data transmission and reception, also a microprocessor and data memory are integrated, in some models even sensors of physical or chemical environmental parameters. The **range** of RFID systems depends on the types of **coupling** and **energy supply** used by the devices.

Passive systems obtain the required energy from the field of the processing unit. The range is approx. 3 m.

Active systems include a feeding battery for energy supply; ranges of 15 m or more are possible.



Data interchange and energy transfer in the **close coupling range** (1 to 20 mm) occur either through capacitive or inductive coupling. In capacitive coupling (via the electric field component), capacitor structures act as an antenna; in inductive coupling (use of the magnetic field components), coils play this role. The close coupling range on the one hand provides increased security and is therefore used especially by access control and payment systems. The second advantage is the possibility to supply transponders requiring higher power levels with energy. Operation frequencies are in the range of a few Hz to some MHz.

The principle of magnetic coupling is applied in **remote coupling-range** with ranges of up to 3 m. Operation frequencies are in part standardized and amount to 100 to 135 kHz, 6.75 MHz, 13.56 MHz, 27.125 MHz. The majority of the systems that are on the market nowadays belong to this category.

Both ranges operate with electric or magnetic coupling in the so-called antenna **nearfield**, i.e. the distance between transmitter and receiver is small compared to the wavelength of the electromagnetic field. The **long coupling range** for its part is based on electromagnetic radio coupling in the farfield. Corresponding systems therefore operate on frequencies of 868 MHz, or in the microwave range at 2,45 GHz, 8 GHz and 24.125 GHz. At bridgeable distances of 1

to 15 m, however, transmission energy has to be provided by an external energy supply. Long-range systems are found especially in transportation, e.g. for the tracking of containers carried by transport vehicles or trains.

The systems make use of the whole technological spectrum for data transfer. Depending on their complexity, analog and digital modulation techniques, simple and error-protective coding, encryption and anti-collision techniques are applied. Anti-collision techniques e.g. allow accurate, simultaneous detection of a greater number of transponders that are in the same area at the same time. This is e.g. made by bulk detection of pallet charges.

Mechanical **construction types** are nowadays easily adjusted to the different areas of application.

Molded from plastic, they come in the shape of hard tags or credit cards. Transponders melted into glass tubes can be applied in human or veterinary medicine. Complete integration into single products is also possible during the manufacturing process. Tags cost a fraction of a cent for simple product security surveillance resp. some euros, for transponders with integrated sensors.

Coding and encrypting of stored information is done depending on the area of application. On the one hand there are insular proprietary solutions enabling the user to protect data so as to adhere to internal company confidentiality standards.

On the other hand, it is seen as important to label goods as uniformly as possible world wide. The barcode with the EAN number already allows discrete labelling of manufacturer and type of article. As for smart tags, it is the EPC, the electronic product code, which is able to identify not only the product type but each individual item.

Applications

RFID systems have been established in many areas in the last few years – in access control systems, as anti-theft devices in department stores, as an immo-



bilization device in car keys, or as a subcutaneously implanted glass rod for animal identification. Even Tsunami victims still not identified were thus labelled. At present, market opportunities of RFID applications are thought to be extremely favorable. Because of the

- integration density that is possible now
- increasing „intelligence“ of transponders and
- pressure for rationalization in the areas of production and

commerce, a dynamic development is expected in the coming years. A crucial aspect is lowering the costs of manufacturing. As always, hopes are high with regard to self-reinforcing effects due to increasing sales figures.

RFID technology will penetrate the whole supply chain of many branches – comprising suppliers, the manufacturing process and, via retail business, even customers. Driving factors are the

- reduction of costs in production, logistics and recycling
- high-standard safety documentation for products with mandatory

surveillance such as nutritional goods, drugs or safety-relevant components e.g. in aviation and motor vehicle technologies.

For **marketing**, information pertaining to product use, users and product life-cycle are naturally of great interest. In principle, RFID tags would be able to pro-

Numbers of new applications are growing. Sensible and less sensible ideas alike are realized ever more quickly. Whoever wants to do so, can get a RFID chip – which is about the size of a grain of rice - injected under the skin in some countries. This chip may e.g. allow access to the beach. Or it makes sure that the left hip joint is operated in hospital, not the right hip – and, of course, that the correct patient is operated.



A buyer who pushes his shopping cart through the aisles of the supermarket without cash register, selects a printer and has his user card at hand to pay for it without making physical contact, will certainly see this as an advantage. And if the printer itself contains a transponder that stores user data during operation for guarantee and service purposes, these data can be called up later on. A corresponding reading device is required anyhow for the separation of materials at recycling facilities. The EPC number of the printer is one of a kind. A utopian vision that may become reality very soon.

vide such information. In the **area of security** provision, RFID technology will improve storage and high reading of speed biometric data. Producers expect higher acceptance of **payment systems**, due to the simplified use of chip cards without physical contact.

Light and shadow

In risk assessment, the emphasis is rather on aspects of data protection and data security than on exposure to electromagnetic fields. Critics increasingly point out gaps, weak points and possibilities for abuse.

With regard to **data safety**, these are:

- tapping or intentional interference with air interface
- unauthorized reading, deactivation or tag removal
- forging of stored data and of identity.

The application of RFID technology appears to make sense and seems acceptable in many areas. Technological options, economic gain as well as responsible use and, as a consequence, acceptance by society will decide whether RFID will be fully successful.

Glossary

- **EAS:** Electronic Article Surveillance, electronic anti-theft protection
- **EAN:** European Article Number
- **EPC:** Electronic Product Code
- **RFID:** Radio Frequency Identification
- **smart label:** intelligent tag
- **transponder:** an electronic device consisting of receiver and transmitter that responds to signals by sending information

Sources and other information

- <http://de.wikipedia.org/wiki/RFID>
- Finkenzeller, Klaus, "RFID-Handbuch"
- Hilty, Lorenz, EMPA, "RFID-alles sicher?"
- Mangelot, Timothee, elektronik industrie 01/2002, "Welche Vorteile bietet die RFID-Technik?"
- Tontrarra, Hans, VDE dialog 01/2005, "Funkende Chips"
- Wölk, Michaela, IZT, "RFID-Anwendungen heute und morgen"

Dipl. Ing. Klaus Bäumer, Deutsche Telekom AG