

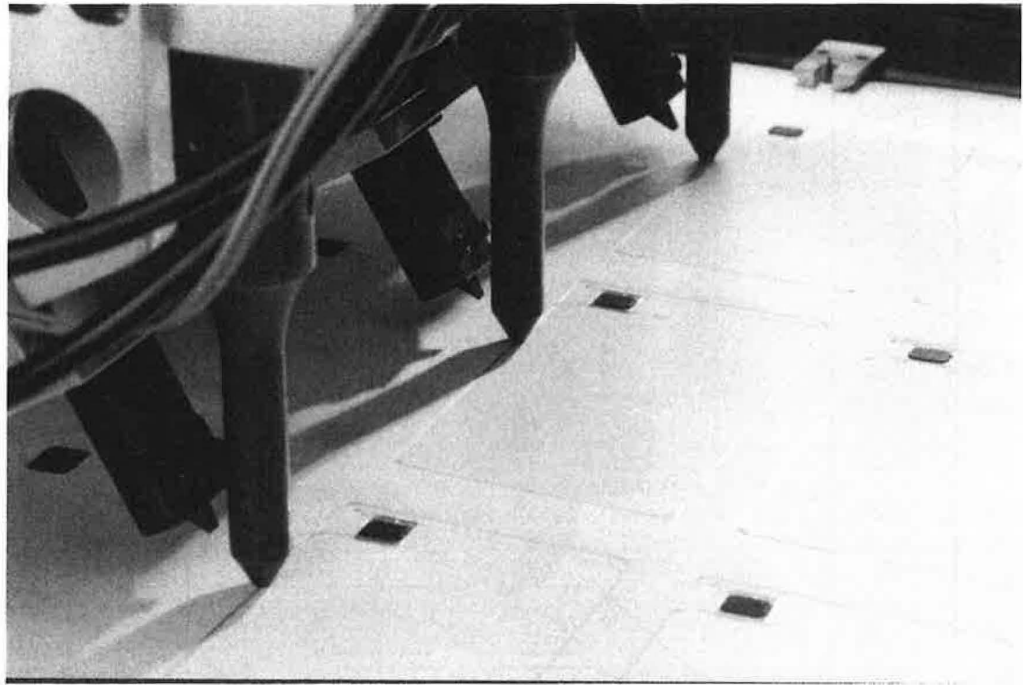


Figure 12.7 Manufacture of a smart card coil using the embedding technique on an inlet foil. The sonotrodes, the welding electrodes (to the left of the sonotrodes) for contacting the coils, and some finished transponder coils are visible (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)

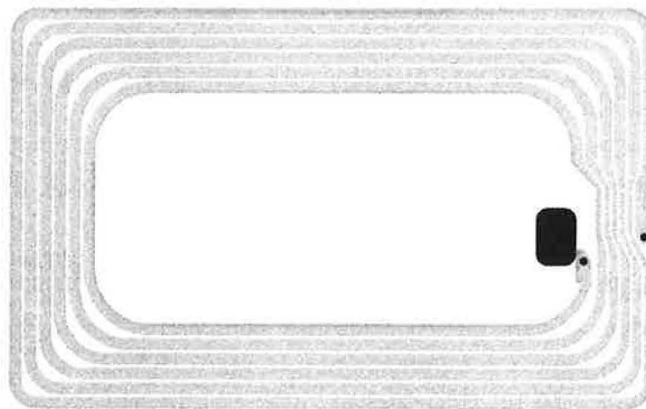


Figure 12.8 Example of a 13.56 MHz smart card coil using screen printing technology

coil resistance of an etched coil can easily be calculated from the surface resistance R_A (Cu: $500 \mu\Omega/\square$ where $d = 35 \mu\text{m}$).

12.2.2 Connection technique

The different types of antenna also require a different connection technique between the antenna coil and the transponder chip.

Table 12.1 Surface resistance of polymer thick film pastes with different admixtures given a layer thickness of 25 μm (Anderson, 1998)

Conductor	Surface resistance
Silver (Ag)	5–20 $\text{m}\Omega/\square$
Copper (Cu)	30–120 $\text{m}\Omega/\square$
Graphite (carbon)	20 000–100 000 $\text{m}\Omega/\square$

Table 12.2 Typical properties of some polymer thick film pastes (Anderson, 1998)

Paste	Dupont 5028	Dupont 5029
Surface resistance after drying	27–33 $\text{m}\Omega/\square$	14–20 $\text{m}\Omega/\square$
Surface resistance after lamination	8–10 $\text{m}\Omega/\square$	4–5 $\text{m}\Omega/\square$
Layer thickness after drying (200 μm screen)	16–20 $\text{m}\Omega/\square$	28–32 μm
Viscosity (RVT UC&S 14 10 rpm)	15–30 $\text{m}\Omega/\square$	35–50 Pa.s

Antenna coils made of wire, i.e. wound or embedded coils, are connected to the chip module using microwelding techniques. The lacquer enamelled antenna coil is bared in the connection area of the chip module using a special tool and then welded to the terminals (lead frames) of the chip module using ultrasound (Haghiri and Tarantino, 1999).

Contacting a printed coil to the chip or a module is problematic as conventional soldering and welding techniques do not work for polymer pastes. The use of flip chip technology,² in which fixing and contacting of the chip can take place using a conductive adhesive, offers a solution. A second solution is the use of cut clamp technology (CCT). In this approach the metal terminals (lead frame) of the chip module are punched through with a pointed tool, so that pointed crowns are formed (Figure 12.9). The chip module is then pressed onto the carrier foil from below, so that the peaks of the crown penetrate the foil and make contact with the antenna terminals. The crown peaks are bent over using a flat stamp, making a permanent mechanical and electrical connection between the chip module and the antenna coils.

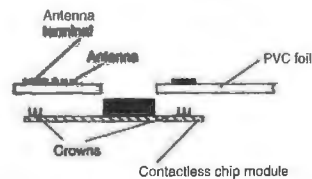


Figure 12.9 Contacting of a chip module to a printed or etched antenna by means of cut clamp technology

²The contactless chip is placed directly upon the terminals of the coil with the contact areas (bond pads) downwards.



Finally, a reflow soldering procedure, like the procedure used for fitting components to SMD printed circuit boards, is available for the connection of an etched coil to a chip module. In order to prevent short circuits (between the coil windings) in the vicinity of the chip module as a result of the soldering process, the coil is first printed with a solder resist (typically light green), keeping the antenna terminals free. A defined quantity of soldering paste is deposited onto these connection areas by a dispenser. After the chip module has been inserted into a stamped hole on the carrier foil provided for this purpose and is thus fixed into position, heat is supplied to the terminals of the chip module by a suitable soldering tool (soldering stamp). This causes the soldering paste to melt, creating a permanent electrical and mechanical connection between the chip module and the antenna coil (Figure 12.10).

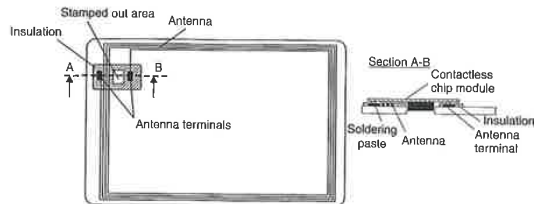


Figure 12.10 Soldered connection between the chip module and an etched antenna

12.2.3 Lamination

In the next step, the overlay and inlet foils are assembled and joined together with precision. Finally, the foils are placed in a laminating machine. By the conduction

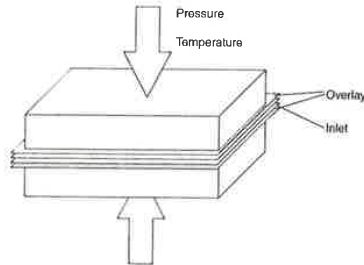


Figure 12.11 During the lamination procedure the PVC sheets are melted at high pressure and temperatures up to 150°C

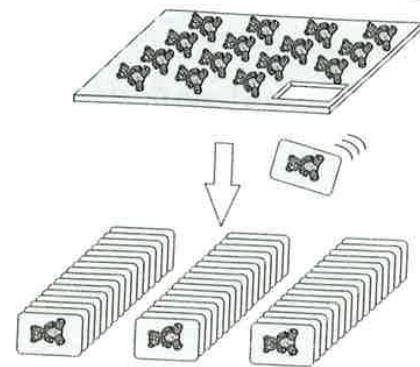


Figure 12.12 After the cooling of the PVC sheets the individual cards are stamped out of the multi-purpose sheets

of heat, the foils are brought into a soft elastic state at high pressure (approximately 100–150°C). This 'bakes' the four sheets to create a permanent bond (Figure 12.11). After the lamination and cooling of the laminated PVC foils, the individual smart cards are stamped out of the multi-purpose sheet (Figure 12.12). A subsequent functional test ensures the quality of the cards before these can be sent to the customer.

13

Example Applications

13.1 Contactless Smart Cards

The first plastic cards appeared in the USA as early as the beginning of the 1950s, when cheap PVC replaced cardboard. In the years that followed, plastic credit cards became widespread. Incidentally, the first credit card was issued by Diners Club in 1950.

The rapid development of semiconductor technology made it possible to integrate data memory and protective logic onto a single silicon chip in the 1970s. The idea of incorporating such an integrated memory chip into an identification card was patented in 1968 by Jürgen Dethloff and Helmut Grötrupp in Germany. However, it was not until almost 15 years later that the great breakthrough was achieved with the introduction of the telephone smart card by the French company PTT. Several million telephone smart cards were in circulation in France by 1986 (Rankl and Effing, 1996). These first generation smart cards were memory cards with contacts. A significant improvement was achieved when entire microprocessors were successfully integrated into a silicon chip, and these chips incorporated into an identification card. This made it possible to run software in a smart card, thus opening up the possibility of realising high-security applications. Thus, smart cards for mobile telephones and the new bank cards (EC with chip) were realised exclusively using microprocessor cards.

Since the mid-1980s, repeated attempts have been made to launch contactless smart cards onto the market. The operating frequency of 135 kHz that was normal at the time and the high power consumption of the silicon chips on the market necessitated transponder coils with several hundred windings. The resulting large coil cross-section, and the additional capacitors that were often required, impeded manufacture in the form of ID-1 format plastic cards, and transponders were usually cast into inconvenient plastic shells. Due to this limitation, contactless smart cards played a minor role in the smart card market for a long time.

In the first half of the 1990s, transponder systems were developed with an operating frequency of 13.56 MHz. The transponders required for these systems required just five windings. For the first time it was possible to produce transponder systems in the 0.76 mm thick ID-1 format. The great breakthrough in Germany occurred in 1995, with the introduction of the 'Frequent Traveller' contactless customer loyalty card in ID-1 format by the German company Lufthansa AG. It was noteworthy that these cards, manufactured by the Munich company Giesecke & Devrient, still had a magnetic strip,

RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, Klaus Finkenzeller
© 2003 John Wiley & Sons, Ltd ISBN: 0-470-84402-7

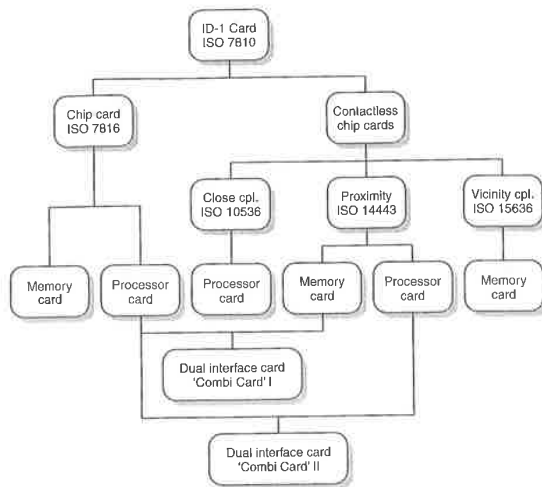


Figure 13.1 The large 'family' of smart cards, including the relevant ISO standard

a hologram and were embossed with the customer number and name. A more in-depth description of this project is included in Section 13.3.

Today, contactless smart cards are divided into three groups based upon the applicable standards (Figure 13.1): close coupling, remote coupling (inductively coupled) and vicinity coupled (inductively coupled) smart cards. While vicinity coupling cards are only available in the form of memory cards, microprocessor cards have been available in the form of inductively coupled cards in small pilot projects since 1997.

Currently, the main fields of application for contactless smart cards are payment systems (public transport, ticketing) or passes (ID cards, company pass) (Figure 13.2). In the long term we can expect that contactless smart cards will largely replace cards with contacts in their classical fields of application (telephone cards, EC cards). In addition, contactless technology will allow smart cards to be used in completely new fields — fields we may not yet have even thought of.

13.2 Public Transport

Public transport is one of the applications where the greatest potential exists for the use of RFID systems, particularly contactless smart cards. In Europe and the USA

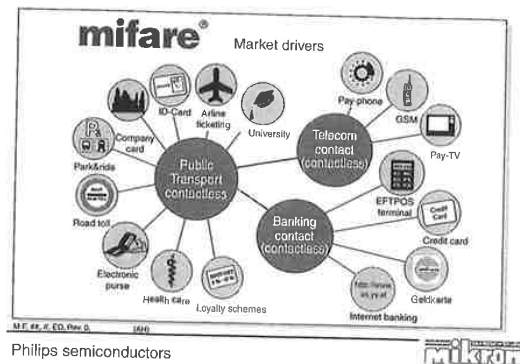


Figure 13.2 The main fields of application for contactless smart cards are public transport and change systems for telephone boxes or consumer goods (groceries, cigarettes) (reproduced by permission of Philips Electronics N.V.).

traffic associations are still operating at a huge loss, sometimes as much as 40% of turnover (Czako, 1997), which must be made up by subsidies from the community and country in question. Due to the increasing shortage of resources, long-term solutions must be sought that will cut these losses by reducing costs and increasing income. The use of contactless smart cards as electronic travel passes could make an important contribution to improving the situation (AFC = automatic fare collection). In the field of fare management in particular there is a great deal of room for improvement.

13.2.1 The starting point

The unhealthy financial situation of transport companies naturally has many different causes. However, the following factors are worth mentioning in connection with electronic travel passes:

- Transport companies incur high costs through the sale of travel passes by automatic dispensers. For example, the sale of a travel pass through an automatic dispenser in Zürich costs Sfr 0.45, where the average sales price is Sfr. 2.80 (Czako, 1997). Thus, 16% of the sales price is lost from the outset by the provision of the dispenser, maintenance and repairs alone (filling with notes and coins, repairs, damage by vandalism).
- In vehicles, too, expensive electronic ticket printers or mobile devices are required. Sometimes the tickets are even sold by the driver, which causes long waiting times

while passengers board, plus the additional security risk presented by the continuous distraction of the driver.

- Paper tickets are thrown away after use, although the manufacture of fraud-proof tickets for transport companies is becoming more and more expensive.
- In German cities in particular, losses of up to 25% must be taken into account due to fare-dodgers (Czako, 1997). This is because German transport companies have very liberal travelling conditions and permit entry to the underground system and buses without travel passes first being checked.
- Association discounts can only be calculated on the basis of costly random counts, which leads to imprecision in the calculation.

13.2.2 Requirements

Electronic fare management systems have to fulfil very high expectations and requirements, particularly with regard to resistance to degradation and wear, write and read speed and ease of use. These expectations can only be satisfactorily fulfilled by RFID systems. The most common format for contactless smart cards is the ID-1 format and, recently, wrist watches.

13.2.2.1 Transaction time

The time taken for the purchase or verification of a travel pass is particularly critical in transport systems in which the pass can only be checked inside the vehicle. This is a particular problem in buses and trams. In the underground railway, passes can be checked at a turnstile, or by conductors. A comparison of different methods shows the clear superiority of RFID systems in terms of transaction times (Table 13.1).

13.2.2.2 Resistance to degradation, lifetime, convenience

Contactless smart cards are designed for a lifetime of 10 years. Rain, cold, dirt and dust are a problem for neither the smart card nor the reader.

Table 13.1 Passenger processing times for different technologies. Source: transport companies in Helsinki, taken from Czako (1997)

Technology	Passenger processing time (s)
RFID I (remote coupling)	1.7
Visual verification by driver	2.0
RFID II (close coupling)	2.5
Smart card with contacts	3.5
Cash	>6

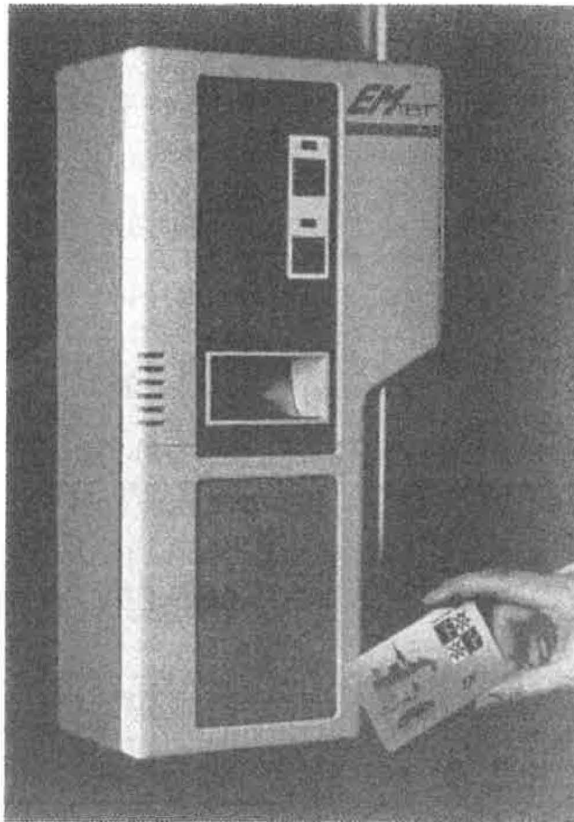


Figure 13.3 Contactless reader in a public transport system (photo: Frydek-Mistek project, Czechoslovakia, source: reproduced by permission of EM Test)

Contactless smart cards can be kept in a briefcase or handbag and are therefore extremely convenient to use (Figure 13.3). Transponders can also be fitted into wrist-watches.

13.2.3 Benefits of RFID systems

The replacement of conventional paper tickets by a modern electronic fare management system based on contactless smart cards provides a multitude of benefits to all those involved. Although the purchase costs of a contactless smart card system are still higher than those of a conventional system, the investment should repay itself within a short period. The superiority of contactless systems is demonstrated by the following benefits for users and operators of public transport companies.

Benefits for passengers

- Cash is no longer necessary, contactless smart cards can be loaded with large amounts of money, passengers no longer need to carry the correct change.
- Prepaid contactless smart cards remain valid even if fares are changed.
- The passenger no longer needs to know the precise fare; the system automatically deducts the correct fare from the card.

- Monthly tickets can begin on any day of the month. The period of validity begins after the first deduction from the contactless card.

Benefits for the driver

- Passes are no longer sold, resulting in less distraction of driving staff.
- No cash in vehicle.
- Elimination of the daily income calculation.

Benefits for the transport company

- Reduction in operating and maintenance costs of sales dispensers and ticket devaluers.
- Very secure against vandalism (chewing gum effect).
- It is easy to change fares; no new tickets need to be printed.
- The introduction of a closed (electronic) system, in which all passengers must produce a valid travel pass, can significantly reduce the number of fare dodgers.

Benefits for the transport association

- It is possible to calculate the performance of individual partners in the association. Because precise data is obtained automatically in electronic fare management systems, the discount for the association can be calculated using precise figures.
- Expressive statistical data is obtained.

Benefits for the treasury

- Reduction of the need for subsidies due to cost reductions.
- Better use of public transport due to the improved service has a positive effect on takings and on the environment.

13.2.4 Fare systems using electronic payment

Transport association regions are often divided into different fare zones and payment zones. There are also different types of travel pass, time zones and numerous possible combinations. The calculation of the fare can therefore be extremely complicated in conventional payment systems and can even be a source of bewilderment to local customers.

Electronic fare management systems, on the other hand, facilitate the use of completely new procedures for the calculation and payment of fares. There are four basic models for electronic fare calculation, as shown in Table 13.2.

13.2.5 Market potential

It is estimated that around 50% of all contactless cards sold are used in the public transport sector (Hamann, 1997). The biggest areas of use are the large population

Table 13.2 Different fare systems for payment with contactless smart card

Fare system 1	Payment takes place at the beginning of the journey. A fixed amount is deducted from the contactless smart card, regardless of the distance travelled.
Fare system 2	At the beginning of the journey the entry point (check-in) is recorded on the contactless card. Upon disembarking at the final station (check-out), the fare for the distance travelled is automatically calculated and deducted from the card. In addition, the card can be checked at each change-over point for the existence of a valid 'check-in' entry. To foil attempts at manipulation, the lack of a 'check-out' record can be penalised by the deduction of the maximum fare at the beginning of the next journey.
Fare system 3	This model is best suited for interlinked networks, in which the same route can be travelled using different transport systems at different fares. Every time the passenger changes vehicles a predetermined amount is deducted from the card, bonus fares for long distance travellers and people who change several times can be automatically taken into account (see Figure 13.4).
Best price calculation	In this system all journeys made are recorded on the contactless card for a month. If a certain number of journeys was exceeded on one day or in the month as a whole, then the contactless card can automatically be converted into a cheaper 24 hour or monthly card. This gives the customer maximum flexibility and the best possible fares. Best price calculation improves customer relations and makes a big contribution to customer satisfaction.

centres in Asia (Seoul, Hong Kong, Singapore, Shanghai), and European cities (Paris, London, Berlin).

In 1994 and 1995 around 1 million contactless smart cards were produced per year worldwide for public transport applications. In the period 1996 to 1997 the volume rose to over 40 million cards per year (Droschl, 1997). The expected volume for 1998 alone is around 100 million contactless smart cards worldwide for public transport applications (Hamann, 1997). Given annual growth rates of 60% or more, we can expect the annual demand for contactless smart cards to have risen to 250 million by the turn of the century.

The highest growth rates for contactless smart cards in public transport applications will be in the Asiatic-Pacific area, because of the new infrastructures being created here using the latest technologies (Droschl, 1997).

13.2.6 Example projects

13.2.6.1 Korea - Seoul

The largest electronic travel pass system (AFC) yet to use contactless cards was commissioned at the start of 1996 in the metropolis of Seoul, South Korea (see Figures 13.5-13.7). The Korean 'Bus Card' is a prepaid card, issued with a basic value of 20 000 W (~17 euro). Fares are calculated according to fare system 1. A bus journey costs an average of 400 W (~0.35 euro), but every time the passenger changes vehicles they must pay again.

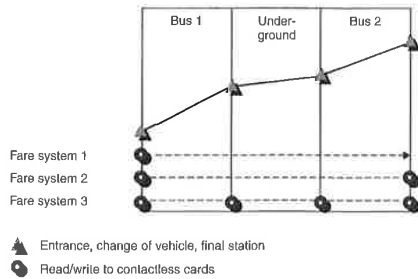


Figure 13.4 Use of the different tariff systems in a journey by public transport. The journey shown involves two changes between the underground and bus network. The number of times the smart card is read depends upon the fare system used



Figure 13.5 Use of a contactless smart card in Seoul. A contactless terminal is shown in communication with a contactless smart card in the centre of the picture (reproduced by permission of Intec)

The card can be used on all 453 lines and recharged at identified kiosks as required. The transport association, Seoul Bus Union, is made up of 89 individual operator companies with a total of over 8700 buses, which were all equipped with contactless terminals by the middle of 1996. When the Kyung-Ki province that surrounds the capital city was included in the scheme, a further 4000 buses and a total of 3500 charging points were fitted with terminals by 1997 (Droschl, 1997). The RFID technology used in this project is the MIFARE® system (inductively coupled, 10 cm, 13.56 MHz), which is very popular in public transport applications.

It is predicted that four million Bus Cards will be in circulation by the end of 1997. The huge success of this system has convinced the government of Seoul to introduce a compatible system for the underground railway system.



Figure 13.6 Contactless smart card for paying for journeys in a scheduled bus in Seoul (reproduced by permission of Klaus Finkenzeller, Munich)



Figure 13.7 Reader for contactless smart cards at the entrance of a scheduled bus in Seoul (reproduced by permission of Klaus Finkenzeller, Munich)

13.2.6.2 Germany – Lüneburg, Oldenburg

One of the first smart card projects in Germany's public transport system is the *Fahrsmart* project in the KVG Lüneburg — VWG Oldenburg transport association. The subsidised *Fahrsmart* pilot project was launched by the Ministry for Education and Research in this area as early as 1990/91. Around 20 000 smart cards with contacts

were issued to customers for this project. However, significant flaws in the installed systems became evident during this pilot project; the biggest problem was that the registration time of over three seconds per passenger was considered to be excessive.

At the beginning of 1996 a new field test was launched, the Fahrsmart II system based upon contactless smart cards. The RFID technology used was the MIFARE® system by Philips/Mikron. System integration, i.e. the commissioning of the entire system, was performed by Siemens VT (Berlin).

The Fahrsmart system automatically calculates the cheapest price for the customer (best price guarantee). The passenger must check in at the start of the journey using their personal smart card and check out at the end of the journey. The journey data obtained are collected in the on-board computer and stored on the smart card for verification.

When the vehicle returns to the depot at the end of the day the current day's data is sent from the vehicle computer to the station server via an infrared interface (Figure 13.8). The processed data is then transferred to the central Fahrsmart server via an internal network. To calculate the monthly invoice, the Fahrsmart server analyses the usage profile of each individual passenger and calculates the cheapest ticket for the distance travelled (individual journey, weekly pass, monthly pass etc.). Figure 13.9 shows a Fahrsmart II smart card.

13.2.6.3 EU Projects – ICARE and CALYPSO

Some of the above-mentioned local transport projects using contactless smart cards, like almost all projects realised to date, are so-called closed exchange systems. In practice this means that the smart cards are 'charged up' with money, but can only be used within the public transport system in question as a ticket or means of payment for small amounts — for example in the operating company's drinks machines. They cannot be used in other shops or even as an electronic travel pass in other towns.

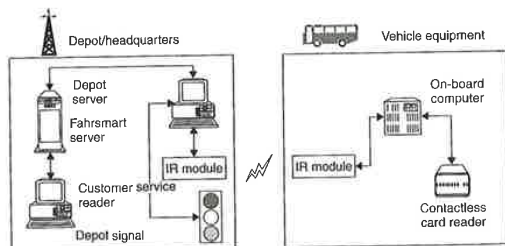


Figure 13.8 System components of the Fahrsmart system. The vehicle equipment consists of a reader for contactless smart cards, which is linked to the on-board computer. Upon entry into the station, the record data is transferred from the on-board computer to a depot server via an infrared link



Figure 13.9 Fahrsmart II contactless smart card, partially cut away. The transponder coil is clearly visible at the lower right-hand edge of the picture (reproduced by permission of Giesecke & Devrient, Munich)

This means that the card holder has to store money for a specific application in the electronic purse of each closed system and no longer has direct access to this for a different application (e.g. telephone smart card, contactless travel pass, prepaid card for the company restaurant) (Lorenz, 1998b).

This is the result of the card technology used, since the cards that have predominated up until now have only a memory chip and thus do not satisfy the strict security requirements of the credit institutes for open automated financial exchange systems.

Open financial exchange systems based upon a microprocessor chip have already been successfully introduced in the field of contact smart cards. In Germany these systems are the Paycard from Telekom, the VISA-Cash-Karte, and the 'ec-Karte mit Chip', the latter having the greatest customer base with approximately 50–55 million cards in use. These cards were designed for payments of small sums and can be used everywhere that suitable readers are available. From the point of view of the user, it would be ideal if the cash card could be used as a ticket for local public transport. Due to the high transaction times of contact smart cards (see Section 13.2.2.1) electronic cash cards have also not yet been able to establish themselves as an electronic travel pass in local public transport applications.

Various solutions have been proposed that aim to combine the user-friendliness of contactless tickets with the security of contact exchange systems, and thus improve the acceptance of such systems by customers (Lorenz, 1998b).

The hybrid card is the combination of a contactless smart card with an additional contact chip on one card. There is, however, no electrical connection between the two chips. This means that it must be possible to transfer sums of money from one chip to the other — for example in special machines. Due to this limitation, the hybrid card too can only be considered as a provisional solution.

The dual interface card (or Combicard, see Section 10.2.1) resulted from the combination of a contact and a contactless interface on a single card chip. This is actually the

ideal solution for the combination of an electronic travel pass with an open financial exchange system. However, the question of when the electronic purse of the German ZKA (ec-card) will be available as a dual interface card, and what quantities will exist, must remain unanswered for the present. However, VISA has already announced that it will integrate its VISA cash chip, previously based upon contact technology, into a combichip in Madrid.

The envelope solution, in which a contactless 'adapter' turns the contact smart card into a contactless pass, offers the advantage over the above-mentioned variants that the microprocessor smart cards already in circulation can be made usable as contactless cards without changing the cards themselves (Figure 13.10).

The envelope solution is central to ICARE ('Integration of contactless technologies into public transport environment'). This EU-supported project is oriented towards the use of open electronic exchange systems in local public transport systems (Lorenz, 1998a). The field trials for this project, which was started as early as 1996, will be performed in various European regions.

In Paris, the largest European conurbation, 40 000 RATP staff and 4000 passengers have already been equipped with an envelope. As an additional feature, an emergency call feature has been developed that is currently being tested in the metro. This feature can be triggered by means of the envelope. In addition to the envelope concept, the development of a disposable ticket was also given some priority in Paris.

In Venice, a town with a high proportion of day trippers, several landing stages have been fitted with contactless readers. In addition to the contactless ticket function, a central feature in Venice is the multifunctionality of the concept. The card can be used in museums, hotels, or as a car park ticket. In the district of Constance on Lake Constance, after an initial field trial in Autumn 1996, a second field trial was initiated

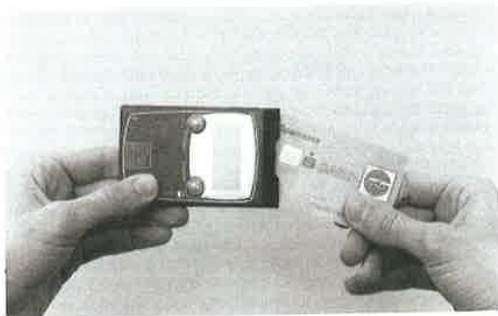


Figure 13.10 The contactless FlexPass of the district of Constance showing the GeldKarte and envelope (reproduced by permission of TCAC GmbH, Dresden)

in January 1998. In this second trial the cashcard of the local savings bank is used in conjunction with an envelope to form the 'FlexPass' (Lorenz, 1998b), which can be used in local transport (Figure 13.11).

A hands-free antenna with a range of 1 m allows statistical data on card use to be recorded without the customer having to hold the envelope near to the reader.

In Lisbon, a medium-sized European capital city with a complex local public transport system and numerous public and private operating companies, the development of a handsfree antenna was also central to the project.

Since 1998, research activities have been continued under the EU CALYPSO project ('Contact And contactLess environments Yielding a citizen Pass integrating urban Services and financial Operations'). Transport companies have increased their efforts to build up a partnership with the operators of automated exchange systems. Among other companies from the German credit industry, the Deutsche Sparkassen- und Giroverband (DSGV) has been recruited as a partner (Ampélas, 1998; Lorenz, 1998c).

The objective of the CALYPSO project is the 'FlexPass'. The intention is that this will replace both the paper ticket and the cash used by the customer for payment. A new aspect of the project is the introduction of further services on the envelope, for example a dynamic passenger information service, i.e. departure times and connections



Figure 13.11 Contactless transaction using the FlexPass at a reader (reproduced by permission of TCAC GmbH, Dresden)

in January 1998. In this second trial the cashcard of the local savings bank is used in conjunction with an envelope to form the 'FlexPass' (Lorenz, 1998b), which can be used in local transport (Figure 13.11).

A hands-free antenna with a range of 1 m allows statistical data on card use to be recorded without the customer having to hold the envelope near to the reader.

In Lisbon, a medium-sized European capital city with a complex local public transport system and numerous public and private operating companies, the development of a handsfree antenna was also central to the project.

Since 1998, research activities have been continued under the EU **CALYPSO** project ('Contact And contactLess environments Yielding a citizen Pass integrating urban Services and financial Operations'). Transport companies have increased their efforts to build up a partnership with the operators of automated exchange systems. Among other companies from the German credit industry, the Deutsche Sparkassen- und Giroverband (DSGV) has been recruited as a partner (Ampélas, 1998; Lorenz, 1998c).

The objective of the CALYPSO project is the 'FlexPass'. The intention is that this will replace both the paper ticket and the cash used by the customer for payment. A new aspect of the project is the introduction of further services on the envelope, for example a dynamic passenger information service, i.e. departure times and connections



Figure 13.11 Contactless transaction using the FlexPass at a reader (reproduced by permission of TCAC GmbH, Dresden)

are shown on the display. Use in car parks or the integration of (emergency) call services is also being considered.

In the long term, the inclusion of further applications in the fields of parking, tourism, public administration, or even car-sharing on the FlexPass is planned (Lorenz, 1998c).

13.3 Ticketing

13.3.1 Lufthansa miles & more card

The Lufthansa 'Ticketless flying' project is the German showcase project for contactless smart card systems. The pilot test involving 600 regular fliers from May to December 1995 ran so smoothly that by March 1996 the 'Miles & More' programme was extended to all *Lufthansa* cards ('HON Club', 'SENATOR' and 'Frequent Traveller'), and the Lufthansa owned service company AirPlus was established. Since Autumn 1996, all of the approximately 250 000 regular fliers possess the new contactless 'ChipCard'. This new contactless smart card — in conjunction with the Lufthansa central computer in Munich-Erding — replaces both the old paper ticket and the conventional boarding pass.

The RFID system selected for this project was the MIFARE® system by Philips/Mikron. The terminals were developed by Siemens-Nixdorf, while the contactless smart cards were manufactured by the Munich company Giesecke & Devrient. In addition to a contactless transponder module, the cards also incorporate a magnetic strip, raised lettering, signature strip, hologram and an optional (contact based) telephone chip (Figure 13.12).

From the point of view of the passenger, the system operates as follows: the card holder books a flight by telephone via a travel agent, quoting his individual card

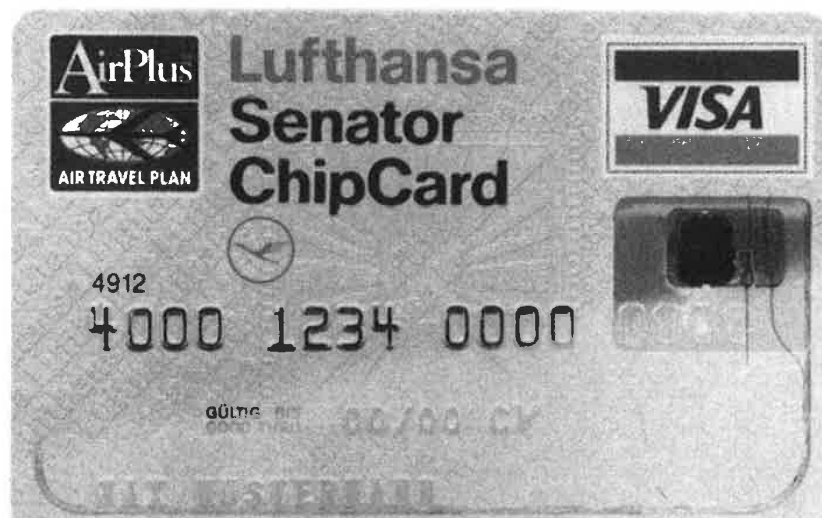


Figure 13.12 Miles & More — Senator ChipCard, partially cut away. The transponder module and antenna are clearly visible at the right-hand edge of the picture underneath the hologram (reproduced by permission of Giesecke & Devrient, Munich)



Figure 13.13 Passenger checking in using the contactless Miles & More Frequent Flyer Card (reproduced by permission of Lufthansa)

number. With the new cards, the booking may be performed up to one hour before departure. An electronic ticket is created that combines personal data and the flight data, and this is saved in the Lufthansa computer. To check in at the airport (at the last minute) the smart card owner only has to present his contactless smart card briefly at the Chip-In-Terminal (Figure 13.13). Normally, he can do this without even removing the card from his briefcase. The system verifies the booking, and the flight data appear on the screen. At this point the passenger is given the option of either confirming the suggested flight including seat reservation or selecting an alternative flight on the touch screen monitor. The passenger receives a printed receipt specifying his seat number and boarding gate, plus other details. This procedure allows the passenger to check in with his hand luggage in less than 10 seconds, which helps to prevent queues at the terminal. When he arrives at the boarding gate he merely presents his ChipCard once again and can then board.

The new ChipCard solution benefits both passengers and Lufthansa and AirPlus. The passengers are overjoyed about the time saving on the ground, the ability to book at short notice and the convenient and simple operation. Clear rationalisation

successes can be seen at Lufthansa and AirPlus, above all due to the self service of customers, which significantly reduces labour intensive handling and verification tasks. Furthermore, the ability to accept short notice bookings is increased by the time saving on the ground, thus increasing competitiveness compared to alternative travelling options (according to Giesecke & Devrient, 1997).

13.3.2 Ski tickets

Anyone entering a *ski lift* has to be in possession of a valid daily or weekly pass. These tickets were originally made of cardboard and validated by a date stamp. Checking paper tickets is very labour intensive because each ticket must be checked visually for validity. Furthermore, it is inconvenient for individual skiers to have to fish around in their anoraks for a sodden paper ticket with cold fingers before every journey on the lift.

RFID technology offers an ideal alternative by replacing paper tickets with contactless smart cards or disk transponders (Figure 13.14). When the transponder is sold a deposit of 5–10 euros is usually retained. After use, the transponder can be returned and the deposit refunded. The lift operator can revalue the transponder using special readers and it can thus be reused.

The read range of the system is designed to be great enough that the transponder tickets no longer need to be held in the hand, but can remain in an anorak pocket.

All ski lift entrances are protected by a turnstile, which is released by the read electronics upon detection of a valid transponder. In order to read the skier's transponder, however it is carried, every entrance is monitored by two antenna opposite each other.

The size of the magnetic antenna is a problem, because it must be very large due to the desired read range. The resulting magnetic coupling between the two reader antennas is so great at a distance of several metres that the resulting mutual interference makes it impossible to read a transponder. To circumvent this problem, ski ticket

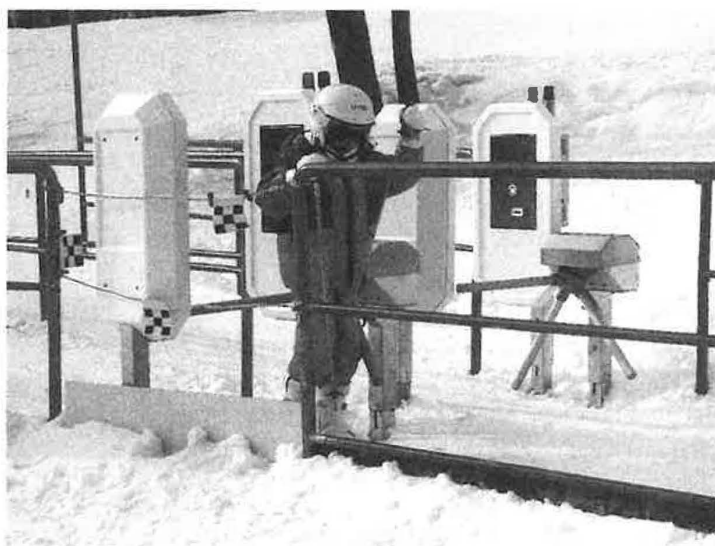


Figure 13.14 Contactless reader as access control and till device at a ski lift (reproduced by permission of Legic Identsystems, CH-Wetzikon)

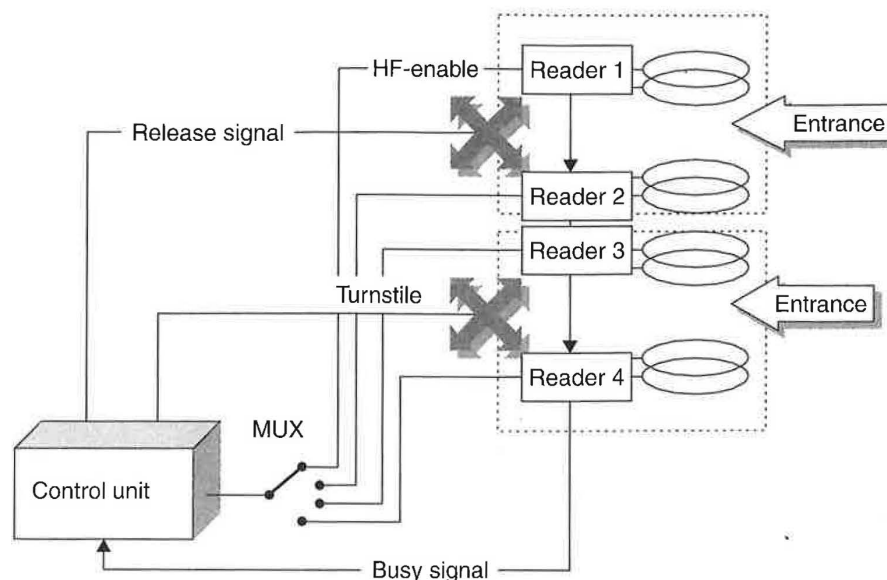


Figure 13.15 To achieve mutual decoupling the readers are switched alternately in time-division multiplex operation

systems activate only one reader at a time, while the HF field of all other readers is switched off altogether. To achieve this, a multiplexer sends a start signal to one reader after the other in a cyclical sequence, which causes the addressed reader to switch on its HF field and check for the presence of a transponder (Figure 13.15). If the reader discovers a transponder, then it activates a *busy signal*. The busy signal tells the control unit to suppress the cyclical start signal for the duration of the busy signal. The active reader is now free to perform the data exchange it has begun with the transponder. After the end of this transaction, the active reader stops transmitting the busy signal, whereupon the multiplexer can continue its cyclical interrogation.

13.4 Access Control

Electronic access control systems using data carriers are used to automatically check the *access authorisation* of individuals to buildings, (commercial or event) premises, or individual rooms. When designing such systems we must first differentiate between two fundamentally different systems with corresponding properties: online and offline systems.

13.4.1 Online systems

Online systems tend to be used where the access authorization of a large number of people has to be checked at just a few entrances. This is the case, for example, at the main entrances to office buildings and commercial premises. In this type of system, all terminals are connected to a central computer by means of a network.

The central computer runs a database in which each terminal is assigned all the data carriers authorised for access to that terminal. The authorisation data generated from the database is loaded into the terminals (or into an intermediate door control unit) via the network and saved there in a table.

Changes to an individual's access authorisation can be made by a single entry on the central computer of the access control system. The data carrier itself does not need to be present, since only an entry in the central database has to be edited. This is advantageous, because it means that sensitive security areas can be protected against unauthorised access even in the event of a data carrier being lost.

The data carriers of an online system only have to be able to store a small amount of data, for example a unique pass number. The use of read-only transponders is also possible. See Figure 13.16.

13.4.2 Offline systems

Offline systems have become prevalent primarily in situations where many individual rooms, to which only a few people have access, are to be equipped with an electronic access control system. Each terminal saves a list of key identifiers (e.g. general-key-3, floor-waiter-7, guest-room-517), for which access to this terminal is to be authorised. There is no network to other terminals or a central computer.

Information regarding the rooms to which the data carrier can provide access is stored on the data carrier itself in the form of a table of key identifiers (e.g. 'guest-room-517', 'sauna', 'fitness-room'). The terminal compares all the key identifiers stored on a data carrier with those stored in its own list and permits access as soon as a match is found. The transponder is programmed at a central *programming station*, for example at the reception of a hotel upon the arrival of the guest. In addition to the authorised rooms, the transponder can also be programmed with the duration of validity, so that hotel keys, for example, are automatically invalidated on the departure date of the guest.



Figure 13.16 Access control and time keeping are combined in a single terminal. The watch with an integral transponder performs the function of a contactless data carrier (reproduced by permission of Legic® -Installation, Kaba Security Locking Systems AG, CH-Wetzikon)

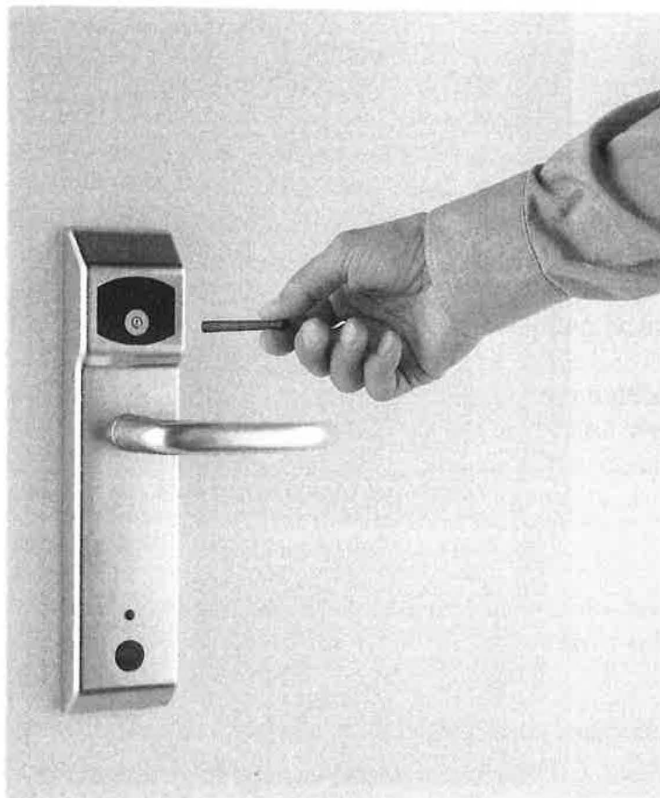


Figure 13.17 Offline terminal integrated into a doorplate. The lock is released by holding the authorized transponder in front of it. The door can then be opened by operating the handle. The door terminal can be operated for a year with four 1.5 V Mignon batteries and even has a real time clock that allows it to check the period of validity of the programmed data carrier. The terminals themselves are programmed by an infrared data transmission using a portable infrared reader (reproduced by permission of Häfele GmbH, D-Nagold)

Only in the event of a data carrier being lost do key identifiers need to be deleted from the terminal in question using a suitable programming device.

Offline systems offer the following advantages over conventional lock systems with key and cylinder (Koch and Gaur, 1998) (see Figures 13.17 and 13.18):

- Early specification on a lock plan in the normal sense is not necessary. The system is initially coded for use as a building-site. When the site is handed over, the door terminals are recoded for commercial use by means of an infrared interface. Subsequent changes and expansions do not pose any problems.
- The option of programming time windows opens up further options: Temporary employees can receive a 'three-month key', the data carriers of cleaning staff can be given precise time specifications (for example Mondays and Fridays from 17.30 to 20.00).
- The loss of a key causes no problems. The data of the lost key is deleted from the read stations, a new key is programmed, and this key's data is entered on the terminals in question.



Figure 13.18 The hotel safe with integral offline terminal can only be opened by an authorised data carrier (reproduced by permission of (hotel-safe is shown by the picture) Häfele GmbH, D-Nagold)

13.4.3 Transponders

Access control using PVC cards has been around for a long time. Hole punched cards were used initially, which were superseded by infrared passes (IR barcode), magnetic strip passes, Wiegand passes (magnetic metal strips), and finally smart cards incorporating a microchip (Schmidhäusler, 1995; Vírnic and Posten, 1992). The main disadvantage of these procedures is the inconvenience of the operating procedure due to the fact that the cards must always be inserted into a reader the right way round. Access control using contactless systems permits much greater flexibility because the transponder only needs to pass a short distance from the reader antenna. Passes can be made in the form of contactless smart cards, key rings, and even wristwatches.

A great advantage of contactless access control systems is that the reader is maintenance-free and is not influenced by dust, dirt or moisture. The antenna can be mounted 'under plaster', where it is completely invisible and protected against vandalism. Hands-free readers are also available for mounting in turnstiles or to increase convenience. In these designs, the transponders do not even need to be removed from the pocket or jacket clip.

Cat flaps operated by a transponder in the cat's collar represent another application in the field of access control, as does the use of read-only transponders as anti-theft sensors for opening or closing doors and windows (Miehling, 1996).

13.5 Transport Systems

13.5.1 Eurobalise S21

Although Europe is moving closer together cross-border transport still presents an obstacle to Europe's railways. Different signals and train security systems force trains to incur the cost of carrying multiple sets of equipment on locomotives and tractive units. It is often necessary to expend precious time changing tractive vehicles at the border, burdening trains with a competitive disadvantage compared to flying or travelling by road (Lehmann, 1996).

For this reason, the European Union is backing the purchase of a unified European train security and control system, the *ETCS* (European Train Control System). The ETCS will facilitate interoperable cross-border traffic and improve the competitiveness of railways by implementing the latest train control technology.

The ETCS comprises four main systems:

- **EURO-Cab** A vehicle device, in which all connected elements are linked to the secure vehicle computer EVC (European Vital Computer) by a special ETCS bus system.
- **EURO-Radio** A GSM radio link between the vehicles and a radio centre by the track, the RBC (Radio Block Center).
- **EURO-Loop** A system for linear data transfer over distances up to several hundred metres. The system is based upon so-called leakage cable, i.e. coaxial cables for which the sheathing is designed to be partially permeable to the electromagnetic field. The frequency ranges of this application lie between around 80 MHz and 1 GHz (Ernst, 1996). EURO-Loop is primarily used to transfer information for the evaluation of discretely transmitted data.
- **EURO-Balise** A system for the discrete transmission of data. Depending upon design, local data (location marking, gradient profiles, speed limits) or signal-related data for the route are transmitted to the vehicle (Lehmann, 1996).

The *Eurobalise* subsystem is particularly important, because it is a crucial prerequisite for the full introduction of the ETCS. In January 1995, after lengthy experiments, the technical framework data for the EURO-Balise were determined. It is an inductively coupled RFID system with anharmonic feedback frequency.

The power supply to the system is taken from a passing tractive unit by inductive coupling at the ISM frequency 27.115 MHz. Data is transferred to the tractive unit at 4.24 MHz, and the system is designed to reliably read the data telegram at train speeds of up to 500 km/h. See Figures 13.19 and 13.20, and Table 13.3.

Four different balise types have been developed by Siemens:

- Type 1 transmits a permanently programmed telegram.
- Type 2 transmits a telegram that can be programmed by the user via the contactless interface. For example, this may be line data such as gradient and speed profiles.



Figure 13.19 Euro balise in practical operation (reproduced by permission of Siemens Verkehrstechnik, Braunschweig)

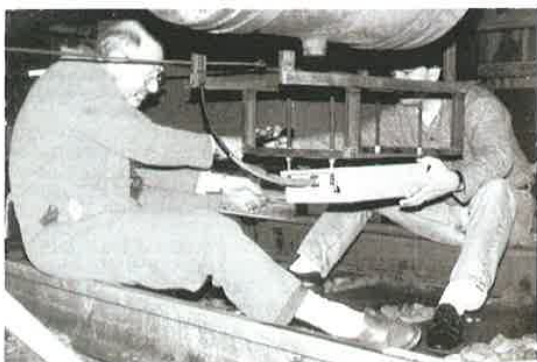


Figure 13.20 Fitting a read antenna for the Euro balise onto a tractive unit (reproduced by permission of Siemens Verkehrstechnik, Braunschweig)

Table 13.3 Basic data for the Eurobalise

Coupling	Inductive
Power transmission frequency, vehicle → balise	27.115 MHz
Data transmission frequency, balise → vehicle	4.24 MHz
Modulation type	FSK
Modulation index	1
Data rate	565 Kbit/s
Telegram length	1023 or 341-bit
Useful data size	863 or 216-bit
Read distance	230 to 450 mm
Maximum sideways offset	180 mm
Coverage with snow, water, ore	Non-critical

- Type 3 transmits a telegram generated by a line device (transparent balise). Type 3 is primarily used in connection with signals.
- Type 4 makes it possible to download data as vehicles drive past.

13.5.2 International container transport

International freight transport containers have been identified using the alphanumeric identification procedure specified in the international standard ISO 6346 since the end of the 1960s. This identification mark consists of four letters, the owner's code, a six-digit numeric serial number and a test digit, and is painted onto the outside of the container at a specified position (Figure 13.21).

Almost all of the 7 million containers in use worldwide employ the identification procedures specified in this standard and thus have their own, unmistakable identification number. The process of manually recording the container identification number and entering it into the computer of a transshipment plant is extremely susceptible to errors. Up to 30% of identifications have been falsely recorded at some point. Automatic data transmission can help to solve this problem by the reading of a transponder attached to the container. In 1991 the international standard ISO 10374 was drawn up to provide a basis for the worldwide use of this technology.

The bands 888 to 889 MHz and 902 to 928 MHz (North America) and 2.4 to 2.5 GHz (Europe) are used as the operating frequencies for the transponders. The transponders must respond on all three of the frequency ranges used. Backscatter modulation (modulated reflection cross-section) with an FSK modulated subcarrier is the procedure used for the data transfer from the container to the reader. The subcarrier frequencies are 20 kHz and 40 kHz. A total of 128 bits (16 bytes) are transmitted within just 2 ms.

ABZU 001234 3

Figure 13.21 Container identification mark, consisting of owner's code, serial number and a test digit

The reader's signal is not modulated (read-only transponder). The specified maximum reader distance is 13 m.

ISO 10374 specifies the following information that can be stored in the transponder:

- owner's code, serial number and test digit;
- container length, height and width;
- container type, i.e. suitcase container, tank container, open top container and others;
- laden and tare weight.

A battery provides the power supply to the electronic data carrier in the transponder (active transponder). The lifetime of the battery corresponds with the lifetime of the container itself, i.e. around 10 to 15 years.

The same technology is used in the identification of goods wagons in North American and European railway transport. A European standard is in preparation for the automatic identification of European interchangeable containers (Siedelmann, 1997).

13.6 Animal Identification

13.6.1 Stock keeping

Electronic identification systems have been used in stock keeping for almost 20 years (Kern and Wendl, 1997) and are now state of the art in Europe. In addition to internal applications for automatic feeding and calculating productivity, these systems can also be used in inter-company identification, for the control of epidemics and quality assurance and for tracing the origin of animals. The required unified data transmission and coding procedures are provided by the 1996 ISO standards 11784 and 11785 (see Section 9.1). The specified frequency is 134.2 kHz, and FDX and SEQ transponders can both be used. A size comparison of the various transponders is given in Figure 13.22.

There are four basic procedures for attaching the transponder to the animal: collar transponders, ear tag transponders, injectible transponders and the so-called bolus (Figure 13.23). Cross-sections of different types of transponders are shown in Figure 13.24.

Collar transponders can be easily transferred from one animal to another. This permits the use of this system within a company. Possible applications are automatic feeding in a feeding stall and measuring milk output.

Ear tags incorporating an RFID transponder compete with the much cheaper barcode ear tags. However, the latter are not suitable for total automation, because barcode ear tags must be passed a few centimetres from a hand reader to identify the animal. RFID ear tags, on the other hand, can be read at a distance of up to 1 m.

Injectible transponders were first used around 10 years ago. In this system, the transponder is placed under the animal's skin using a special tool. A fixed connection is thereby made between the animal's body and the transponder, which can only be removed by an operation. This allows the use of implants in inter-company applications, such as the verification of origin and the control of epidemics.

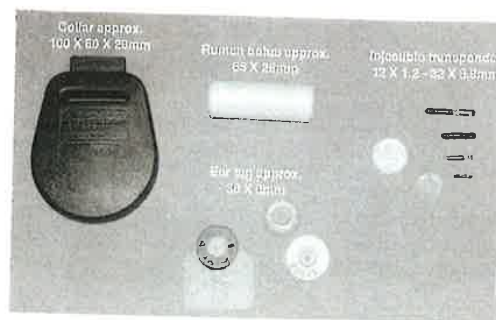


Figure 13.22 Size comparison of different variants of electronic animal identification transponders: collar transponder, rumen bolus, ear tags with transponder, injectible transponder (reproduced by permission of Dr Michael Klindworth, Bayerische Landesanstalt für Landtechnik, Freising)

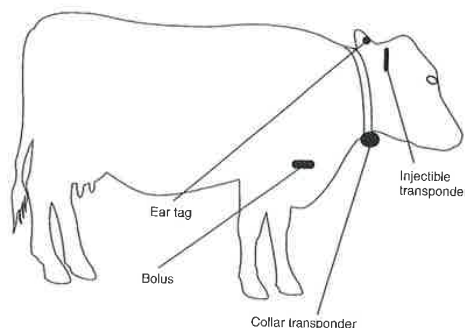


Figure 13.23 The options for attaching the transponder to a cow

The implant is in the form of a glass transponder of 10, 20 or 30 mm in length (Figure 13.25). The transponder is supplied in a sterile package or with a dose of disinfectant. The dimensions of the glass transponder are amazingly small, considering that they contain the chip and a coil wound around a ferrite rod. A typical format is 23.1 mm × 3.85 mm (Texas Instruments, 1996).

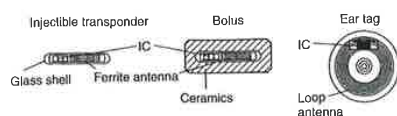


Figure 13.24 Cross-sections of various transponder designs for animal identification (reproduced by permission of Dr Georg Wendt, Landtechnischer Verein in Bayern e.V., Freising)



Figure 13.25 Enlargement of different types of glass transponder (reproduced by permission of Texas Instruments)

Various instruments and *injection needles* are available for performing the injection:

- 'Single-shot' devices use closed hollow needles ('O' shape), which are loaded individually. Single use needles containing transponders in a sterile package are also available. The hollow needles are sharpened at the tip, so that the skin of the animal is ripped open when the needle is inserted. The blunt upper part of the needle tip presses the cut flap of skin to one side so that the insertion point is covered up again when the needle has been removed, allowing the wound to heal quickly (Kern, 1994).
- The 'Multi-shot' device has a magazine for several transponders, thus dispensing with the need to load the device. Open-ended hollow needles ('U' shaped) are used, as these are easier to clean, disinfect and check than closed hollow needles and can therefore be used several times.

The injection does not hurt the animal and can be carried out by practised laymen. However, attention should be given to hygiene to ensure that the wound heals safely.

An injected transponder represents a foreign body in the animal's tissues. This can lead to problems in the locational stability of the transponder within the animal's body, and may therefore cause problems when reading the transponder. From our experience of war injuries we know that shrapnel can often wander several decimetres through the body during a person's lifetime. An injected transponder can also 'wander' around. To solve this problem, the Bayerischen Landesanstalt für Landtechnik in Weihenstephan, a



Figure 13.26 Injection of a transponder under the scutulum of a cow (reproduced by permission of Dr Georg Wendt, Landtechnischer Verein in Bayern e.V., Freising)

branch of the Technical University in Munich, has been investigating various injection sites since 1989 (Kern, 1994). As a result of these studies, injection under the *scutulum* is currently favoured over the use of the right ear, with the injection being directed towards the occipital bone (Figure 13.26). According to findings of the Landanstalt, this position is also suitable for measuring the animal's body temperature.

The so-called *bolus* is a very useful method of fitting the transponder. The bolus is a transponder mounted in an acid resistant, cylindrical housing, which may be made of a ceramic material. The bolus is deposited in the rumen, the omasum that is present in all ruminants, via the gullet using a sensor. Under normal circumstances the bolus remains in the stomach for the animal's entire lifetime. A particular advantage of this method is the simple introduction of the transponder into the animal's body, and in particular the fact that it does not cause any injury to the animal. The removal of the bolus in the slaughter house is also simpler than the location and removal of an injected transponder (Kern and Wendt, 1997). See Figures 13.27–13.30.

It is clear that the injected transponder and the bolus are the only foolproof identification systems available to stock keepers. A more detailed comparison of the two systems (Kern and Wendt, 1997) shows that the bolus is particularly suited for use in the extensive type of stock keeping that is prevalent in Australia or South America. In intensive stock keeping methods, commonly used in central Europe, both systems appear to be suitable. The degree to which bolus, injection or even RFID ear tags will become the industry standard means of identification remains to be seen. See Geers *et al.* (1997), Kern (1997) and Klindtworth (1998) for further information on the material in this section.

13.6.2 Carrier pigeon races

Participating in races is a significant part of carrier pigeon breeding. In these races, hundreds of pigeons are released at the same place and time, at a location a long

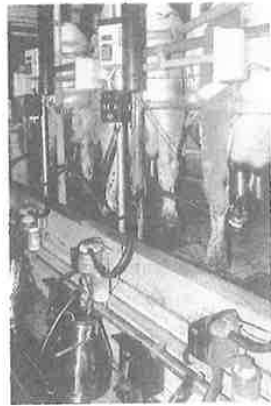


Figure 13.27 Automatic identification and calculation of milk production in the milking booth (reproduced by permission of Dr Georg Wendl, Landtechnischer Verein in Bayern e.V., Freising)



Figure 13.28 Output related dosing of concentrated feed at an automatic feed booth for milk cows. In the illustration the cow is identified by the transponder at its neck (reproduced by permission of Dr Georg Wendl, Landtechnischer Verein in Bayern e.V., Freising)

distance from their home. Pigeons are judged by the time they take to return home from the point where they were released. One problem is the reliable recording (confirmation) of arrival times, because in the past the breeders themselves recorded the times using a mechanical confirmation clock.



Figure 13.29 Oral application of a bolus transponder (reproduced by permission of Dr Michael Klindtworth, Bayerische Landesanstalt für Landtechnik, Freising)

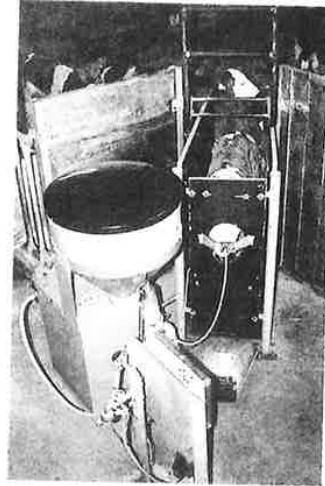


Figure 13.30 Example of automated animal recognition in practice: grouping calves properly for feeding often requires much time and effort. Here a machine takes on this task: the animals can receive an individually adjustable amount of milk in several small portions (reproduced by permission of Dr Michael Klindtworth, Bayerische Landesanstalt für Landtechnik, Freising)



Figure 13.31 Pigeon upon arrival at its own pigeonry. Upon the pigeon's entry, the transponder in the ring is read (reproduced by permission of Legic IdentSystems, CH-Wetzikon)

To solve the problem of timing, the pigeons are fitted with rings that incorporate a read-only transponder based upon a glass transponder. As the pigeons are loaded onto the transporter for transport to the release site, the serial numbers of the transponders are read to register the animals for participation in the race. Upon the pigeon's arrival at its home pigeonry a reader installed in the pigeonhole records the serial number and stores it, together with the precise arrival time, in a portable control unit. Judging takes place by the reading of the devices at the operating point (Figure 13.31).

However, the ingenuity of some of the breeders was greatly underestimated when this system was first introduced. It was not long before some breeders were not only able to read the transponder codes from the pigeon ring, but could also fool the reader using a simulation device in the home pigeonry. The technology involved was fairly simple — all that was required was an extremely simple read-only transponder, whose 'serial number' could be altered using external DIP switches. Thus, some breeders were able to significantly accelerate the 'flight speeds' of their champions.

An effective measure to protect against such attempts at fraud is the incorporation of an additional writable EEPROM memory into the transponder. The memory size is just 1 byte to keep the chip size and cost of circuitry low (Figure 13.32). Before the start, a previously determined random number, for which there are $2^8 = 256$ possibilities, is written to this byte in the transponder at the headquarters. It is crucial that the breeder does not have access to his bird while it is being transported to the release site after the transponder has been programmed. This prevents the random number from being read. When the pigeon reaches its home pigeonry, its arrival is confirmed electronically. The time, together with the transponder code and the secret random number are stored. When the records are evaluated at the headquarters, the random number read upon arrival is compared with the number programmed at the start. The measured times are only validated if the two figures are identical, otherwise it is assumed that an attempted fraud has taken place.

The procedure described is clearly adequate to successfully prevent attempted fraud. With 256 possibilities for the random number the probability that this will be guessed correctly in a single attempt is only 0.4%.

In order to keep the weight and dimensions of the pigeon transponder low, glass transponders are used in this application, which are cast into a plastic ring. These plastic

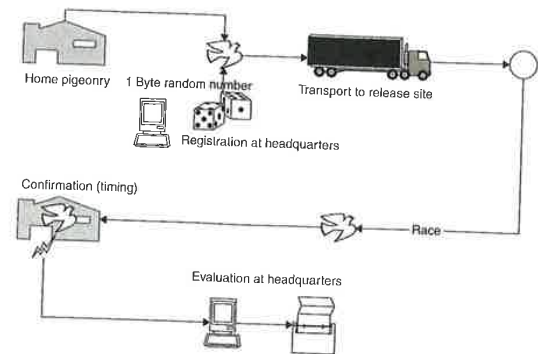


Figure 13.32 The generation of a random number which is written to the transponder before the start protects against attempted fraud



Figure 13.33 Typical antenna of an electronic confirmation system. The transponder on the pigeon's left leg is also clearly visible (reproduced by permission of Deister Elektronik, Barsinghausen)

rings can be fastened to the pigeon's leg without hindering the animal or causing it any discomfort (Figure 13.33).

13.7 Electronic Immobilisation

The sharp rise in *vehicle theft* at the beginning of the 1990s — particularly in Germany — boosted the demand for effective anti-theft systems. Battery-operated

remote control devices with a range of 5–20 m had already been available on the market for years. These are small infrared or RF transmitters operating on the UHF frequency 433.92 MHz, which are primarily used to control the central locking system and an integral alarm. An (electronic) immobiliser may also be coupled to the remote control function. In this type of anti-theft device, however, the mechanical lock can still be used to gain access to the vehicle — in case the remote control device fails to work due to the failure of the battery in the transmitter. This is the greatest weakness of this type of system, as the system cannot check whether the mechanical key is genuine. Vehicles secured in this manner can therefore be opened with a suitable tool (e.g. picklock) and started up by an unauthorised person.

Since the middle of the 1990s, transponder technology has provided a solution that can be used to check the authenticity, i.e. the genuineness, of the key. This solution has proved ideal for the realisation of the electronic immobilisation function via the ignition lock. Today, transponder technology is usually combined with the above-mentioned remote control system: the remote control operates the vehicle's central locking and alarm system, while transponder technology performs the immobilisation function.

13.7.1 The functionality of an immobilisation system

In an *electronic immobilisation* system a mechanical ignition key is combined with a transponder. The miniature transponder with a ferrite antenna is incorporated directly into the top of the key (see Figure 13.34). The antenna is integrated into the ignition lock (Figure 13.35).

The reader antenna is integrated into the *ignition lock* in such a manner that when the ignition key is inserted, the (inductive) coupling between reader antenna and transponder coil is optimised. The transponder is supplied with energy via the inductive coupling and is therefore totally maintenance free. Electronic immobilisers typically operate at a transmission frequency in the LF range 100–135 kHz. ASK modulation is the preferred modulation procedure for the data transfer to the transponder, because it allows reader and transponder to be manufactured very cheaply (Doerfler, 1994). Load modulation is the only procedure used for data transmission from the transponder to the reader.

When the ignition key is turned in the ignition lock to start the vehicle, the reader is activated and data is exchanged with the transponder in the ignition key. Three procedures are employed to check the authenticity of the key:

- Checking of an individual serial number. In almost all transponder systems the transponder has a simple individual *serial number* (unique number). If the normal number of binary positions is used, significantly more different codes are available than worldwide car production ($2^{32} = 4.3$ billion, $2^{48} = 2.8 \times 10^{14}$). Very simple systems (first generation immobilisation) read the transponder's serial number and compare this with a reference number stored in the reader. If the two numbers are identical the motor electronics are released. The problem here is the fact that the transponder serial number is not protected against unauthorised reading and, in theory, this serial number could be read by an attacker and copied to a special transponder with a writable serial number.
- Rolling code procedure. Every time the key is operated a new number is written to the key transponder's memory. This number is generated by a pseudo-random



Figure 13.34 Ignition key with integral transponder (reproduced by permission of Philips Electronics N.V.)

generator in the vehicle reader. It is therefore impossible to duplicate the transponder if this system is used. If several keys are used with one vehicle then each key runs through its own pseudo-random sequence.

- Cryptographic procedures (authentication) with fixed keys. The use of cryptographic procedures offers much greater security (second generation immobilisation). In the *authentication* sequence (challenge response) knowledge of a secret (binary) key is checked, without this key being transmitted (see Chapter 8). In vehicle applications, however, unilateral authentication of the key transponder by the reader in the ignition lock is sufficient.

The RFID reader now communicates with the vehicle's *motor electronics*, although this communication is protected by cryptographic procedures. The motor electronics control all important vehicle functions, in particular the ignition system and fuel system. Simply short circuiting or disconnecting certain cables and wires is no longer sufficient to circumvent an electronic immobilisation system (Figure 13.36). Even attempting to fool the motor electronics by inserting another ignition key of the same type into the ignition lock is bound to fail because of the authentication procedure between reader and motor electronics. Only the vehicle's own key has the correct (binary) key to successfully complete the authentication sequence with the motor electronics.

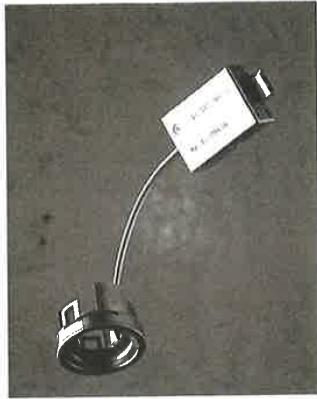


Figure 13.35 The antenna of the electronic immobilisation system is integrated directly into the ignition lock (reproduced by permission of Deister Elektronik, Barsinghausen)

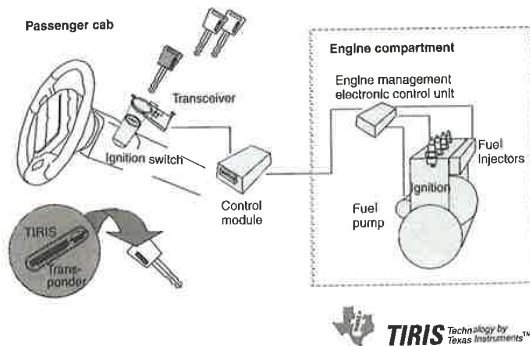


Figure 13.36 Functional group of an electronic immobilisation system. The RFID reader authenticates itself with regard to the motor electronics to prevent the manipulation of the reader. The motor electronics control the ignition, fuel and starter and thus can block all the crucial functions of the vehicle (reproduced by permission of Texas Instruments)

The installation of such an electronic immobiliser to the engine management system can only be performed at the factory by the vehicle manufacturer, thus guaranteeing optimal interaction between engine control system and security device. The individual key data is programmed in the factory by laser programmable fuses on the chip or by writing to an OTP-EEPROM. The vehicle manufacturer is also responsible for implementing appropriate security measures to prevent criminals from unlawfully procuring replacement parts (Wolff, 1994). With few exceptions, electronic immobilisation systems have been fitted to all new cars as standard since the beginning of 1995 (Anselm, 1996). See Figure 13.37.

13.7.2 Brief success story

In 1989 the Berlin wall and the border to Eastern Europe were opened, and the years following 1989 were characterised by dramatic increases in vehicle thefts in Germany. From 48 514 thefts in 1988, the figure had risen to 144 057 thefts just five years later in 1993 — almost a threefold increase. This prompted the German Federal Supervisory Office for Insurance to declare a change to the General Insurance Conditions for Motor Vehicle Insurance (AKB) at the beginning of 1993.

According to the old conditions, vehicle owners with fully comprehensive insurance could, under certain conditions, claim the full price for a new car if their vehicle was stolen, although the resale value of the stolen vehicle and thus the damage suffered was significantly less than this (Wolff, 1994). The value of a vehicle after just a few months falls a long way short of the price of a new car.

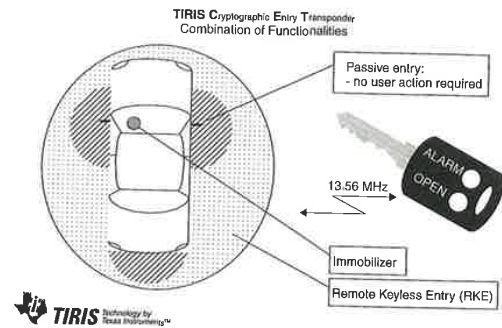


Figure 13.37 Electronic immobiliser and door locking system are integrated into a transponder in the ignition key. In the ignition lock and in the vicinity of the doors (passive entry) the transponder is supplied with power by inductive coupling. At greater distances (remote keyless entry) the transponder is supplied with power from a battery (round cell in the top of the key) at the push of a button ('OPEN') (reproduced by permission of Texas Instruments)

Under the new conditions, only the cost of replacing the vehicle, i.e. its actual market value, is refunded in the case of loss (accident, theft, ...). Furthermore, if the loss is due to theft an excess is deducted from the payment, which may be waived if the vehicle is fitted with an approved anti-theft device (Wolff, 1994). The vehicle owner's own interest in having an effective anti-theft device was significantly increased by the new insurance conditions.

The effectiveness of electronic immobilisation has been clearly demonstrated by the decreasing trend in vehicle thefts in Germany. In 1994 there had already been a slight fall of about 2000 to 142 113, compared to the record figure from 1993. Two years later — 1996 — 110 764 thefts were reported. This represents a fall of 22% in just 2 years.

Another factor is that since 1995 electronic immobilisers have been fitted to all new cars — with a few exceptions — in the factory as standard. If we consider vehicles secured in this manner alone, then we can expect a reduction in the theft rate by a factor of 40(!).

In this connection it is interesting to examine investigations by insurance companies into vehicle thefts where electronic immobilisers were fitted (Anselm, 1995, 1996; Caspers, 1997).

Of 147 stolen vehicles in 1996, 70% of thefts were performed using the original key, which the thief had obtained by breaking into homes, garages and workshops, or by stealing from offices, bags and changing rooms or by the fraudulent renting and misappropriation of rental or demonstration cars. In the remaining 30% of cases, the vehicles either disappeared under circumstances that indicated the cooperation of the owner (without this being proved in individual cases), or vehicles were loaded onto lorries and transported away by professionals.

There has not been one case since 1995 where the electronic immobiliser has been 'cracked' or beaten by a thief.

13.7.3 Predictions

The next generation of immobilisers will also incorporate a passive, cryptologically secured access system. In this system, a reader will be fitted in each of the vehicle's doors. Sequential systems (TIRIS®) will be able to achieve a remote range, in which the transponder is supplied by a battery, so that the vehicle's central locking system can be operated from a greater distance away. This is similar in its function to the combination of an immobiliser and central locking remote control on a single transponder.

13.8 Container Identification

13.8.1 Gas bottles and chemical containers

Gas and chemicals are transported in high quality rented containers. Selecting the wrong bottle during refilling or use could have fatal consequences. In addition to product specific sealing systems, a clear identification system can help to prevent such errors. A machine readable identification system gives additional protection (Braunkohle, 1997).

A large proportion of containers supplied today are identified by barcodes. However, in industrial use the popular barcode system is not reliable enough, and its short lifetime means that maintenance is expensive.

Transponders also have a much higher storage capacity than conventional barcodes. Therefore additional information can be attached to the containers such as owner details, contents, volumes, maximum filling pressure and analysis data. The transponder data can also be changed at will, and security mechanisms (authentication) can be used to prevent unauthorised writing or reading of the stored data.

Inductively coupled transponders operating in the frequency range <135 kHz are used. The transponder coil is housed in a ferrite shell to shield it from the metal surface (see also Section 4.1.12.3).

The manufacturing process for the transponders is subject to exacting standards: the transponders are designed for an extended temperature range from -40 °C to +120 °C; their height is just 3 mm. These transponders must also be resistant to damp, impact, vibrations, dirt, radiation and acids (Bührlen, 1995).

Because the transmission procedure for transponders used in container identification has not been standardised, various systems are available. Because a device has been developed that can process all the transponder types used, the user can choose between the different transponder systems — or may even use a combination of different systems.

Mobile and stationary readers are available (Figures 13.38 and 13.39). Stationary readers can be incorporated into a production system which automatically recognises and rejects wrong containers. After filling, the current product data is automatically stored on the transponder. When this system is used in combination with database management, the number of containers used by a customer for a given gas consumption can be drastically reduced, because excessive standing times or storage periods can be easily recognised and corrected. In addition, all the stations that the container passes through on its way to the customer and back can be automatically recorded by the use of additional readers. So, for example, it is possible to trace customers who return the



Figure 13.38 Identification of gas bottles using a portable reader. The reader (scemtec SIH3) is designed to function with transponders from different manufacturers (reproduced by permission of Messer Griesheim)



Figure 13.39 Portable antenna for reading inductively coupled transponders mounted on gas bottles or other containers (reproduced by permission of SCEMTEC Transponder Technology GmbH, Reichshof-Wehrath)

containers dirty (Braunkohle, 1997). For gas, where there is not much potential for product differentiation between manufacturers, the associated cost savings can convey an important competitive advantage (Bühlren, 1995).

In total, over eight million gas bottles in Germany alone are waiting to be fitted with transponders. For Europe, this figure is approximately 30 million. In addition to gas bottles, transponders are also used for rental containers, beer kegs and boxes and transportation containers for the delivery industry.

13.8.2 Waste disposal

Because of increasingly rigorous environmental legislation, the cost of waste disposal is increasing all the time. Costs associated with creating new waste disposal sites and maintaining existing sites are being passed on to individual households and industrial companies. Automatic measurement of the amount of waste produced helps to distribute the costs fairly. For this reason, more and more cities are using RFID systems to optimise communal waste disposal, and are thus putting the conditions in place for replacing the flat rate charge for waste disposal with a charge based upon the quantity

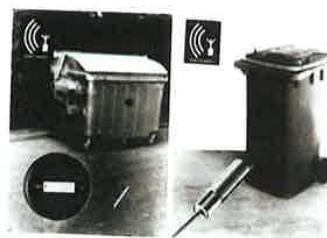


Figure 13.40 Left, dustbin transponder for fitting onto metal surfaces; right, reader antenna for installation in the dustcart. A plastic dustbin fitted with a transponder is shown in the background (reproduced by permission of Deister Electronic, Barsinghausen)

of waste produced. The waste disposal companies will only charge for the amount that has actually been removed.

To achieve this goal, a transponder is fitted to the dustbin and automatic reader systems are installed in rubbish collection vehicles (Figure 13.40). As soon as the dustbin is placed on the vehicle's emptying device its transponder is read. In addition, either the weight or the volume of rubbish is calculated, depending upon the preference of the community. A counter, to show how often the bin has been emptied in the year, is also feasible (EURO-ID, n.d.).

The identifier read by the transponder is stored in a smart card in the vehicle's on-board computer together with the data collected. At the end of a round the driver passes the card to the operations centre so that the collected data can be processed. Individual households no longer pay a monthly flat rate, but each receive an individual bill (Prawitz, 1996) (Figure 13.41).

In Germany RFID systems are already in use in various cities, including Bremen, Cologne and Dresden, and in numerous communities.

13.9 Sporting Events

In large-scale sporting events such as major marathons, the runners who start at the back of the field are always at a disadvantage, because their times are calculated from the moment the race is started. For many runners it takes several minutes before they actually cross the starting line. In very large events with 10 000 participants or more, it might be 5 minutes before the last runners have crossed the starting line. Without individual timing, the runners in the back rows are therefore at a severe disadvantage.

To rectify this injustice, all runners carry a transponder with them. The system is based upon the idea that each runner places his feet repeatedly on the ground and thus comes very close to a ground antenna. In experimental events it was found that using a ingenious arrangement of multiple antennas in an array and a chip in the shoe over 1000 runners can be registered up to eight times in a minute with a start width of just 4 m (ChampionChip, n.d.).

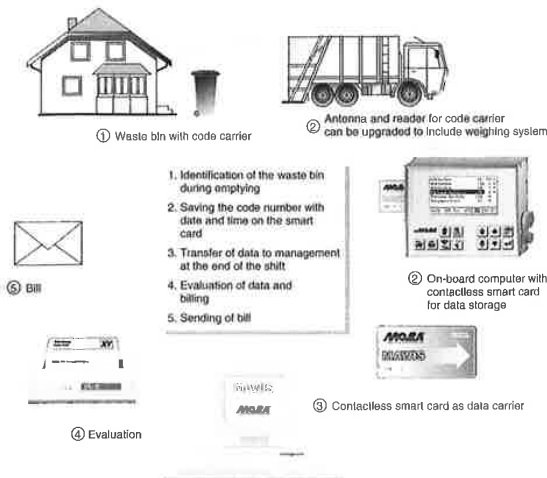


Figure 13.41 Waste generation cycle including billing (reproduced by permission of MOBA Mobile Automation GmbH, Elz)

The transponder is based upon a glass transponder operating in the frequency range 135 kHz, embedded into a specially shaped (ABS) injection moulded housing (Figure 13.42). To get the transponder as close as possible to the ground — and thus to the antenna of the time measurement device — this is attached to the runner's shoe using the shoelaces (Figure 13.43).

The reader antennas are cast into thin *mats* and can thus be placed on the ground and still be protected from all environmental influences (Figure 13.44). The dimensions of a single mat are 2.10 m × 1.00 m. At a normal running speed a net time resolution of ± 1 s is possible, derived from the time the runner remains within the read range of a mat. The accuracy for cyclists improves to ± 0.2 seconds. The measured time is immediately displayed on a screen, so that the reader can read his current intermediate time or final time as he passes a control station.

The runner can make a one-off purchase of the transponder for 38 DM and then use it wherever compatible timing systems are used.

The performance of a transponder based timing system has been demonstrated at the following events: Rotterdam Marathon (10 000 participants), Shell Hanseatic Marathon, Hamburg (11 500 participants) and the Berlin Marathon (13 500 participants) (Champion-chip). See Figure 13.45.

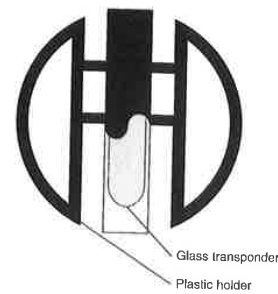


Figure 13.42 The transponder consists of a glass transponder, which is injected into a plastic housing that is shaped according to its function. The diagram shows the partially cut away plastic housing



Figure 13.43 The ChampionChip transponder is fastened to the runner's shoe with the shoelace (reproduced by permission of ChampionChip BV, NL-Nijmegen)

13.10 Industrial Automation

13.10.1 Tool identification

As well as its metal cutting tool industry, Germany's woodworking industry also plays a dominant role in the world market. The modern woodworking and furniture manufacturing industry is dominated by *CNC technology* because this enables manufacturers to manufacture at a low cost and remain competitive.

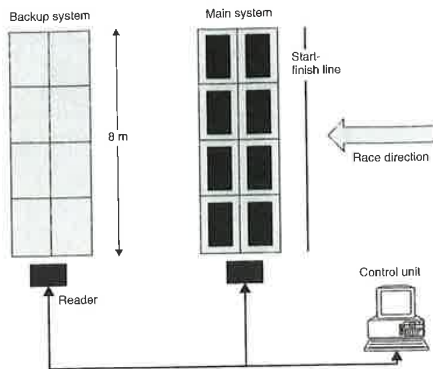


Figure 13.44 A control station consists of a main system and a reserve system. The systems are made up of arrays of antennas in mats



Figure 13.45 Runners passing the control station at the end of the 101st Boston Marathon. In the foreground we can see the mats containing the readers. The times can be displayed on a screen immediately (reproduced by permission of ChampionChip, NL-Nijmegen)

CNC machines equipped with tool holders and automatic tool changers fulfil tasks that are increasingly associated with small batch production. This increases the proportion of manufacturing costs incurred by retooling and tool-change times.

Another consideration is the fact that a CNC woodworking machine differs from a metalworking machine because of its higher rotation and path speeds. Rotation speeds

from 1000 min^{-1} to more than $20\,000 \text{ min}^{-1}$ (!) are attained in wood and plastic processing. The risk of accidents for man and machine is therefore very high during the tool-change operation; for example, hazards may be caused by the wrong fitting of the CNC machine's chain magazine (Leitz, n.d.; Töppel, 1996).

This potential hazard can be eliminated by fitting a transponder in the *taper shaft* or in the *retention bolts* of the toolholder (Figures 13.46 and 13.47). All relevant tool data are preprogrammed into the transponder by the tool manufacturer. The machine operator fits the transponder tools into the CNC machine's toolholder in any order. Then the CNC machine initiates an automatic read sequence of all tools in the toolholder, during which the tools are first ordered into toolholder positions and then all geometric and technical data for the tools is transmitted correctly to the tool management system of the CNC control unit (Figure 13.48). There is no manual data entry, which eliminates the possibility of human error (Leitz, n.d.). The danger of accidents due to excessive speeds, the selection of the wrong rotation direction or the incorrect positioning of the tool in relation to the workpiece is thus eliminated.

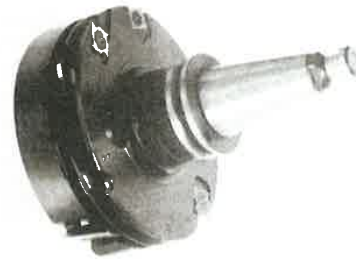


Figure 13.46 CNC milling tool with transponder in the retention bolts (reproduced by permission of Leitz GmbH & Co., Oberkochen)

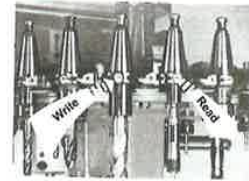


Figure 13.47 Various woodworking tools with transponder data carrier in the taper shaft (reproduced by permission of EUCHNER & Co., Leinfelden-Echterdingen)

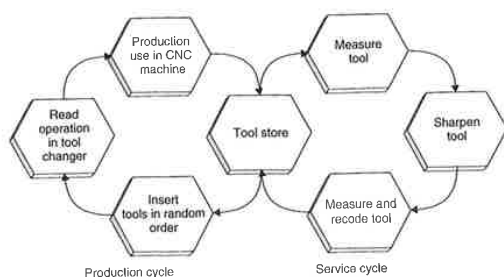


Figure 13.48 Representation of the tool cycle when using transponder coded CNC tools

Table 13.4 Example of a data record for a tool transponder

Customer	Furniture Production Plant XY
LEITZ ID no.	I30004711 D25x60
Manufacturing ref.	Y21
Place of manufacture	UHE
Rotation direction	3
Max. rotation speed	24 000
Min. rotation speed	18 000
Ideal rotation speed	20 000
Radius correction	25 011
Longitudinal correction	145 893
Greatest radius	25 500
Greatest length	145 893
Maximum travel	3000
Current travel	875
Tool number	14
Tool type	1
Number of sharpenings	2
Angle of clearance	20
Cutting rake	15
Free text	Finishing cutter HM Z = 3

Inductively coupled transponders operating in the frequency range <135 kHz are used. The transponder coil is mounted on a ferrite core to shield it from the metal surface (see also Sections 4.1.12.3 and 2.2). The transponder must have a minimum of 256 bytes of memory, which is written with an ASCII string containing the required tool data. An example of a data record is illustrated in Table 13.4 (from Leitz, n.d.).

Modern transponder coded CNC tools can be incorporated into a cost saving production and service cycle. The service cycle is incorporated, smoothly and simply, into the production cycle as follows.

The worn tool is first examined and measured in detail to determine its condition. The tool is then serviced, sharpened and balanced on the basis of this data. After every maintenance sequence the tool length and radius is updated and written to the transponder, so that correctly dimensioned workpieces are produced by both new and sharpened tools without intervention by the operator.

13.10.2 Industrial production

Production processes underwent a process of continuous rationalisation during the development of industrial mass production. This soon led to production line assembly ('conveyor belt production'), with the same stage of production being performed at a certain position on the assembly line time after time. For the present, a production process of this type is only able to produce objects that are identical in function and appearance. However, the days are numbered for machines that produce large quantities of a single product with no variants.

If different variants of a product are to be produced at the same time on an assembly line in an automated procedure, the object must be identified and its status clearly recognised at every work station, so that the correct processes can be performed. Originally, this was achieved by objects being accompanied by process cards, which gave the operating personnel all the information required at a particular work station — the desired paint colour, for example. This was first achieved in electronic form using coding pegs affixed to the revolving palettes so that palette numbers could be read by the electronic control system. The position of these coding pegs could be sensed by inductive proximity switches (Weisshaupt and Gubler, 1992). This procedure has recently been improved by the use of barcode labels, which can simply be stuck onto the individual objects.

RFID technology now provides an additional option — data carriers that can not only be read, but also written. Now, in addition to recording the identity of an object, it is also possible to document its current status (e.g. processing level, quality data) and the past and future (desired end state) of the object.

Using modern identification techniques, production systems can now be realised which can produce variants of a product, or even different products, down to a batch size of one (Weisshaupt and Gubler, 1992). The automotive industry is a good example: since vehicles are predominantly produced to order and it is rare for two identical vehicles to be ordered, automatic material flow tracking is crucial to smooth operation. A vehicle must be clearly identified at the individual manufacturing stages to avoid, for example, an unwanted air conditioning system from being fitted, or the wrong paint colour being applied during painting (Homburg, 1996).

There are two possible methods of controlling a system based upon object data: centralised and decentralised control.

Centralised control In this approach, material flow and object status are continuously monitored during the process and are stored in a database on a central computer (Figure 13.49). This builds up an image of the current process data and system status in the process control system of the central computer. It makes no difference whether the status of objects in the process is determined using barcodes, radio, optical character recognition, RFID or any other type of information coding and transmission.

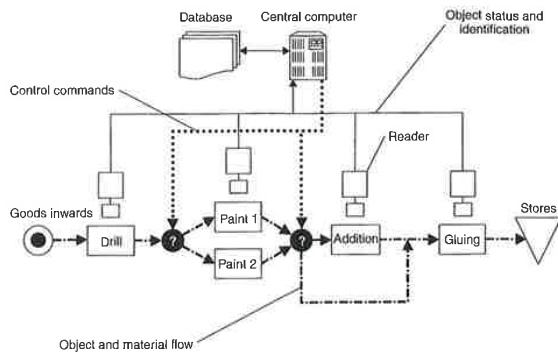


Figure 13.49 The object and data flow in a central control system is performed using completely separate routes. The central computer has a powerful database in which all process data is stored

The monitoring of the process must be completely infallible, otherwise there is a danger that an object will become out of control. The restarting of the system after a fault or the crashing of the control software can be a particularly critical moment.

Centralised control systems based upon a powerful central database are particularly common when it is necessary to access the information from different locations simultaneously, when a transparent image of process data must be available continuously for other purposes, or if important data needs to be stored permanently (Homburg, 1996). Apart from production, typical applications include stores technology, logistics or the collection of operating data.

Decentralised control The use of readable and writable data carriers opens up the possibility of controlling a system locally, i.e. completely independently of the central process computer. Each object carries a complete data record with it that contains information about its identity, its current status, its history and its future — material and data flow are thus interlinked (Figure 13.50). For this to be successful, it must be possible not only to read the relevant data from the object at each processing station, but also to change and update this information. Of all known identification technologies, this can only be achieved with the necessary reliability using writable RFID transponders.

The option of changing the object data in the transponder at each processing station means that it is possible to create an information flow between the individual processing stations, which takes the pressure off the control system. Production and processing operations are becoming faster all the time, so the fact that information can be carried with the object and is available in the right place can become a decisive factor in speeding processes up. Due to possible overheads associated with accessing a remote

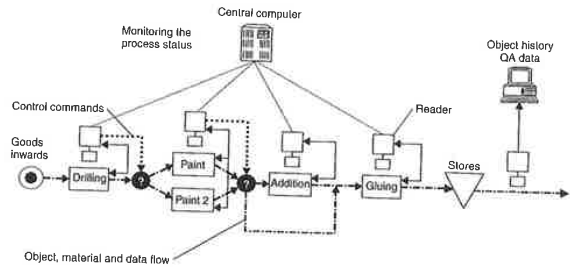


Figure 13.50 In a decentralised system the data is carried along with the objects

database, readers in systems that operate at a rate of seconds are becoming increasingly unable to keep pace with the process, for example in the setting of points or the initiation of the correct processing operation (Homburg, 1996).

13.10.2.1 Benefits from the use of RFID systems

- **Quality control:** In modern production lines the quality of products is tested at test points located at a number of stations. When the product is inspected at the end of the production process, it must be possible to unambiguously attribute the quality data gathered earlier to the correct object. With writable transponders that travel with the product this is easy to achieve because all the quality data obtained during the production process is carried with the object.
- **System security:** Shifting object data from the central computer to the object significantly increases system security. Even after software crashes or failures of the central computer, the relationship between an object and its current data can be established anywhere and at any time. If necessary, objects can also be withdrawn from the production process without losing the data. If the object is subsequently put back into the process, work can continue without problems or faults occurring (Weisshaupt and Gubler, 1992).
- **Data security:** Protecting the data stored in the transponder using a checksum procedure (e.g. CRC, see Section 7.1) ensures the complete security of the data that has been read. Read errors are recognised as such and the data ignored.
- **Flexibility:** The use of writable transponders facilitates much more flexible control of the manufacturing process. For example, the setup data for universally programmable robots and production machines can be written to the transponder carried with the object during the preparatory stage and is available immediately where it is needed. Using this technique, products can be manufactured right down

to a batch size of one, without having to set up a complex communication with the central computer for each object.

- **Harsh environmental conditions:** RFID systems are completely insensitive to dust, moisture, oils, coolants, cuttings, gases, high temperatures and similar problems that can occur in a manufacturing environment. Glass and plastic transponders usually comply with protection type IP67; that is, they are totally dustproof and waterproof. Even particularly dusty or dirty environmental conditions, which would make the use of barcode readers impossible due to the rapid blocking of scanner optics, pose no problems for RFID systems.

13.10.2.2 The selection of a suitable RFID system

When selecting a suitable RFID system for use in the production process, the characteristics of the different memory technologies should be considered (see Table 13.5; see also Section 10.3).

EEPROM Data stored in an EEPROM is retained for several years without a power supply. The energy required for writing to or reading from a transponder using EEPROM technology is transmitted by inductive coupling. Since the transponders do not require a battery they may be very small. The guaranteed number of write access operations to a memory address is typically around 100 000 cycles, which is greater than the lifetime of the transponder. However, an innovative type of EEPROM technology is now available on the market which can be reprogrammed more than 10^6 times. This

Table 13.5 Comparison between the two memory technologies for transponders

	EEPROM/FRAM	SRAM
Memory size	16 byte–32 Kbyte	1–512 Kbytes
Data transmission	Inductive coupling	Inductive coupling, backscatter
Power supply	Inductive coupling	Battery
Typical number of write cycles	EEPROM: 100 000–1 000 000 FRAM: 10^{10}	Unlimited
Typical temperature range	–20 °C–120 °C	0 °C–60 °C
Applications	Applications with a limited number of reprogramming operations (EEPROM)	Applications with any number of reprogramming operations, e.g. in assembly systems
	Applications with expanded temperature range	Use in the 'normal' industrial temperature range
	—	Need for higher memory size with short transaction time
	—	Large transponder range required (or low positional accuracy)

can be increased still further by the use of FRAM memory technology. Over 10^{10} write cycles are already being achieved using this technology.

SRAM In contrast to EEPROMS, SRAM memory cells require a constant power supply to retain stored data. Therefore, transponders using this memory technology always have their own battery. Data transmission between reader and transponder employs either inductive coupling or the backscatter procedure (microwave). SRAM memory can be reprogrammed any number of times with high write speeds. However, the integral battery limits the temperature range of this transponder to 0–60 °C.

13.10.2.3 Example projects

Let us now consider a few examples of the use of RFID systems in manufacturing. It is no coincidence that most of the examples described here are taken from the *automotive industry*. In this industry in particular companies are continuously striving to optimise the production process.

In BMW's Dingolfing factory (Southern Germany), the car bodies of the 7 and 5 series were originally identified manually at the identification points using barcode readers. To cut costs, a microwave identification system was installed (2.45 GHz, transmission power of reader: 10 mW) at the end of 1996. A transponder is now fitted to the bonnet of each painted body as it enters the production process and data for the model (e.g. chassis number) is written to this transponder (Figure 13.51). A total of around 3000 transponders are in circulation. Around 70 readers are installed in the assembly area at individual identification points in the various assembly stages. As



Figure 13.51 After successful identification of the vehicle, its specific data is interrogated and displayed (reproduced by permission of Peppert & Fuchs GmbH, Mannheim)

soon as the body enters the interrogation zone of a reader the read process is initiated by an inductive proximity switch. The required data is read from, or if necessary written to, the transponder. The transponders are equipped with a battery designed for a lifetime of 8 years. They have a memory size of 32 Kbytes, and the range of up to 4 m is sufficient in all stages of assembly (Pepperl & Fuchs, 1998, n.d.a).

In Mercedes Benz's Tuscaloosa factory in the USA, inductively coupled transponders (125 kHz, read-only system) are used for the identification of skids for vehicle bodies. After the skid has travelled through the painting line several times it must be cleaned. This selection process can be performed without incurring additional costs by data capture using transponders (Schenk, 1997).

In the production of its 1E generation, vehicle manufacturer General Motors produces 26 different engine models under one roof at its Flint factory (Michigan, USA). The product range incorporates a multitude of engine types, which includes 1997 to 1998 models, 5.0 to 5.7 litre engines, engines for automatic or shift transmission, engines for export, engines designed to run on environmental fuel and petrol, and engines for cars and lorries. Fitting the product carriers with transponders (13.56 MHz, 8 Kbyte memory) makes it possible to track and identify all engine models throughout the production process. Using RFID it is possible to trace any engine in the factory within seconds. Around 50 readers are installed in the production area for this purpose (Escort, 1998a).

The John Deere Company in Waterloo (Iowa, USA), the worldwide market leader in the production of agricultural machinery, employs an inductively coupled RFID system in the manufacture of tractors. The tractor bodies are equipped with special transponders that can withstand temperatures of up to 225 °C, and can even communicate with a reader at these temperatures, which means that they can be used in the painting ovens (Escort, 1998b). The data carriers (13.56 MHz, 8 Kbyte memory) can be easily fitted to the rear axle of the tractor chassis. Because most tractors are manufactured to order, the use of modern identification technology allows tractors to be adapted to individual customer requirements.

The use of RFID systems in the meat processing industry is another interesting example. Barcode systems cannot be used due to the high temperatures of above 100 °C during canning and the long cooling periods. The company J. M. Schneider Meats, one of the largest meat processing companies in Canada with 15 factories, therefore uses an inductively coupled RFID system in the processing sequence for product identification and tracking. At the beginning of the process the meat is stacked onto mobile shelves. The meat is conveyed into the chill room via the smoking chambers on these shelves and in the last stage of processing it is heated to above 100 °C for conservation. It is vital that the company always knows precisely where the individual shelves are and which process they are currently undergoing. Transponders are therefore attached to the individual shelves (13.56 MHz) and significant data, such as the location of the shelves, meat type and weight data, is written to the transponder. The delivery time of the meat, which depends upon its use-by date, can also be consistently tracked by means of the RFID system (Escort, 1998c).

A further application that should clarify how RFID systems can help to increase the quality of a product by tolerance selection (Pepperl & Fuchs, n.d.b) is illustrated in Figure 13.52. This application involves the assembly of a precision clutch release stop. The system consists of a pallet rotary system, two robots and a manual work

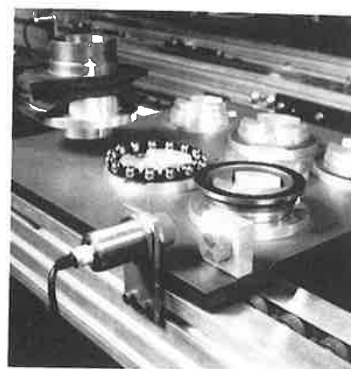


Figure 13.52 Individual components of a clutch release stop on a revolving pallet. Transponder and reader antenna are visible in the lower part of the photo (reproduced by permission of Pepperl & Fuchs, Mannheim)

station. All the pallets are equipped with transponders. The individual components that make up the stop are measured by one of the robots and these measurements are used to assemble components so that the play in the finished stop is minimised. This allocation of individual components to each other is written as data to the transponder and thus carried along with the individual components. The second robot is an assembly robot which assembles the individual components into a stop. At this point the data is read from the transponder, so that the robot can always assemble the correct individual components.

The use of RFID systems can also bring benefits in *storekeeping* and *order processing*. One of the leading pharmaceutical companies, Sanacorp in Munich, has an electronically controlled stock keeping and order processing system, which allows products to be automatically collected in accordance with the delivery note. More than 6000 consignment containers (plastic containers) pass through the stores every day and need to be identified at individual loading points. In the old system using barcode labels or reflective code labels up to 100 errors occurred daily, meaning that the falsely identified consignment containers passed through all of the loading points on the way to the goods outwards, thus delaying the entire consignment. To guarantee the infallible recognition of the consignment containers these were fitted with transponders (134 kHz, SEQ), which were welded to the base of the plastic trough. The reader antennas are located under the conveyor belts at the relevant stations. As soon as a consignment container rolls into the interrogation zone of a reader the transponder is read and the stored data is transferred to the stock-control computer. The central computer is informed of where each consignment container is located, whether delays

are occurring during loading, and how busy the individual loading points are. The rapid collection of goods from the stores is important because customers, who are mainly pharmacists, expect the consignment to arrive on time and be complete. This can only be guaranteed by a technically infallible order picking procedure (Sander and Mollik, 1997).

13.11 Medical Applications

The ability of passive transponders to operate reliably for years without their own power supply — which may be susceptible to failure — predestined this technology for applications in *human medicine*.

Glaucoma is a condition in which increased interocular pressure (IOP) at first causes a narrowing of the field of vision, and ultimately results in complete blindness. The latest research has shown that interocular pressure is subject to sharp diurnal fluctuations and that not only the absolute pressure, but also the pressure fluctuations, significantly influence the risk of blindness (Ullerich, 2001). Therefore, the continuous measurement of the interocular pressure under normal conditions and in the patient's normal environment is necessary to improve understanding of the progression of the condition and facilitate an individual programme of treatment (Bögel and Niederholz, 2001). This is in contrast to the normal practice of measuring IOP exclusively during surgery hours with the aid of a tonometer.

In patients with a cataract, the natural lens is removed from the eye and replaced by an *artificial interocular lens*. This prompted the idea of integrating a full transponder, i.e. a *microcoil* and a transponder chip with an integral capacitive pressure sensor, into the haptic of such an artificial intraocular lens. Figure 13.53 shows such a transponder unit after casting in PDMS (polydimethylsiloxane), a soft silicon normally used for the manufacture of artificial lenses.

The external diameter of the microcoil is around 10.3 mm and the internal diameter 7.7 mm. For the optical part of the lens 5 mm is specified. The microcoil is manufactured on a flexible polyimide foil (Ullerich, 2001; Ullerich *et al.*, 2000, 2001a,b)



Figure 13.53 Transponder unit after casting into an artificial intraocular lens made of silicon. (reproduced by permission of IWEI, RWTH Aachen, D-52074 Aachen)



Figure 13.54 Cast transponder unit deformed by a pair of tweezers (reproduced by permission of IWEI, RWTH Aachen, D-52074 Aachen)

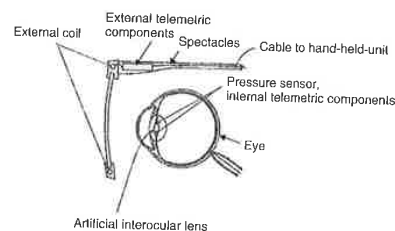


Figure 13.55 An implanted transponder with a pressure sensor, and an antenna coil integrated into the frame of a pair of glasses make up the system for the continuous measurement of interocular pressure (reproduced by permission of IWEI, RWTH Aachen, D-52074 Aachen)

and is thus foldable, which makes the implanting of the transponder much easier (see Figure 13.54). The pressure sensor is micromechanically integrated into the transponder chip and has a sensitivity of 1.3 mbar, which roughly corresponds with the precision of current tonometer measurements (Ullerich 2001).

So that the transponder can be read continuously, the reader's antenna is integrated into the frame of a pair of glasses. The control of the coil and the storage of the measured data takes place with the aid of the reader, which is connected to the glasses via a cable (Figure 13.55).

- TagMaster (1997) Datasheet: *Mark Tag™ S1255, multiple access read-only-card*, TagMaster AB, S-Kista
- Tanneberger, Volkmar (1995) *Informationsübertragung im Strassenverkehr mit passiven, batterielosen Mikrowellen-Transpondern*, Verlag Shaker, Braunschweig, ISBN 3-8265-0788-6
- TEMIC (1977) Telefunken microelektronik GmbH, *Remote Control and Identification Systems*, Design Guide, D-Heilbronn, August
- Texas Instruments Deutschland GmbH (1996) *Standard Transponder Specifications*, 06/1996
- Tietze, U. and Schenk, Ch. (1985), *Halbleiter Schaltungstechnik*, 7th edn, Springer-Verlag, Berlin, ISBN 3-540-12488-6
- Töppel, Matthias (1996) Zehn Milliarden Zugriffszyklen — Prozeßgesteuerte Identifikationssysteme, *elektro AUTOMATION*, 4, Konradin Verlag, Leinfelden-Echterdingen
- Ullerich, Stella (2001) *Herstellung und Charakterisierung ein- und mehrlagiger flexibler Mikropulen für medizinische Telemetrie-anwendungen*, Rheinisch-Westfälische Technische Hochschule (RWTH) Aachen, December, <http://opac.bib.rwth-aachen.de/>
- Ullerich, S., Mokwa, G., Bögle, G. vom and Schnakenberg, U. (2000) Mico coils for an advanced system for measuring intraocular pressure, *Technical Digest 1st annual International IEEE-EMBS Special Topic Conference on Microelectronics in Medicine and Biology*, Lyon, France, 12–14 October, pp. 470–4
- Ullerich, S., Mokwa, G., Bögle, G. vom and Schnakenberg, U. (2001a) A foldable artificial lens with an integrated transponder system for measuring intraocular pressure, *Technical Digest 11th International Congress on solid-state sensors and actuators Transducers '01 and Eurosensors XV*, Munich, Germany, 10–14 June, pp. 1224–7
- Ullerich, S., Mokwa, G., Bögle, G. vom and Schnakenberg, U. (2001b) Foldable micro coils for a transponder system measuring intraocular pressure, *Proceedings of Sensors 2001*, 8–10 May, Nuremberg, Germany, vol. 1, pp. 319–342
- Vcd, Krebs D., Unpublished manuscripts, Venture Development Corp., <http://www.vdc-corp.com>
- Virnich, M. and Posten, K. (1992) *Handbuch der codierten Datenträger*, Verlag TÜV Rheinland GmbH, Cologne, ISBN 3-8249-0044-0
- Vogt (1990) *Vogt Elektronik, Components Handbook — 1990*, Passau
- Weisshaupt, Bruno and Gubler, Gerda (1992) *Identifikations- und Kommunikationssysteme, Datenträger verändern die Automation*, Die Bibliothek der Technik, Band 61, verlag moderne industrie AG & Co., Landsberg/ Lech, ISBN 3-478-93071-5
- Wolff, Hartmuth (1994) Optimaler Kfz-Diebstahlschutz durch elektronische Wegfahrsperrern, *GME Technical Report*, No. 13, *Identifikations-systeme und kontaktlose Chipkarten*, vde-Verlag, Berlin
- Zechbauer, Ulrike (1999) Mit amorphen Metallen auf der Jagd nach Ladendieben, *Forschung und Innovation*, 1, Siemens AG, Munich, <http://www.forschung-innovation.de>
- Zorzi, Michele (1995) Mobile radio slotted ALOHA with capture and diversity, *Wireless Networks*, 1

14.4 Printed Circuit Board Layouts

14.4.1 Test card in accordance with ISO 14443

This section contains the layout, component mounting diagram, and jumper settings for the circuit introduced in Section 10.1.1.2. This is a contactless test card used to generate a load modulation signal in accordance with ISO 14443 at a reader.¹

¹ Reader: 13.56 MHz. Contactless smart card: load modulation with subcarrier 847 kHz. Subcarrier ASK modulated with Manchester coding or BPSK (2-FSK) modulated with NRZ coding.

The layout of the test card is available to download from the author's homepage (<http://rfid-handbook.de/downloads>) as a Postscript or Gerber file.

14.4.2 Field generator coil

The layout depicted shows the *field generator coil* described in Section 9.2.4. This coil is however also excellently suited for use as an antenna in the frequency range of 13.56 MHz.

Table 14.1 Jumper position for setting the supported modulation procedures

Jumper setting*	Jp1	Jp2	Jp3	Jp4	Jp5	Jp6	Jp7	Jp8	Jp9
Don't transmit	—	—	3.3	—	—	—	—	—	—
Manchester 1111	1.3	2.2	3.3	Down	—	—	—	—	—
Manchester 1010	1.3	2.1	3.3	Down	—	—	—	—	—
BPSK 1111**	1.3	2.3	3.3	—	—	—	—	—	—
BPSK 1010, Phase 0°	1.2	2.3	3.3	—	Right	—	—	—	—
BPSK 1010, Phase + $\pi/2$	1.2	2.3	3.3	—	Left	—	—	—	—
BPSK external data, phase 0°	1.1	2.3	3.1	Down	Right	—	—	—	—
BPSK external data, phase + $\pi/2$	1.1	2.3	3.1	Up	Left	—	—	—	—
R-modulation	—	—	—	—	—	Off	Off	Right	Down
C-modulation	—	—	—	—	—	On	On	Left	Up

*The card is held such that the antenna is to the right.

**Subcarrier unmodulated.

Table 14.2 Parts list for test chip card

Component	Value/type	Comment
C1	22 pF	—
CV1	6–60 pF	Adjusting of the transponder resonant frequency
C2	100 pF	—
7C3	10 nF	—
C4	10 pF	Modulation capacitor
C5	10 pF	Modulation capacitor
R1	4.7 Ω	—
R2	4.7 k Ω	—
R3, R4, R5, R6	1 M Ω	—
R7	10 Ω	Shunt resistor during C-modulation
R8	470 Ω	Shunt resistor during R-modulation
R9	1–1.8 k Ω	Modulation resistor
D1, D2, D3, D4	BAR42	—
D5	3V8	Zenor diode
L1	~3.5 μ H	Conductor loop in the layout
U1	74HC4040	Asynchronous 12-bit binary counter
U2	74HC74	Dual D flip-flop
U3	74HC00	4 $\times$ NAND
U4	74HC03	4 $\times$ NAND, Open Collector

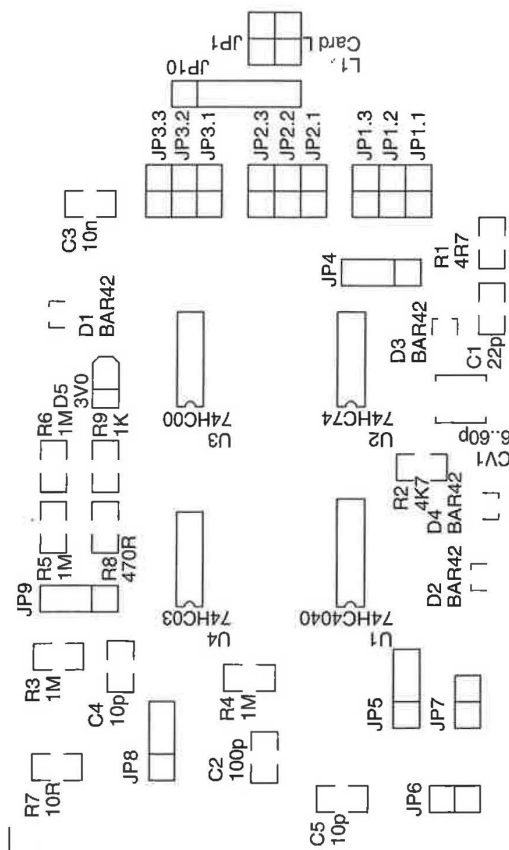


Figure 14.1 Component mounting diagram of the ISO 14443 test card. The transponder's antenna is in the upper half of the printed circuit board

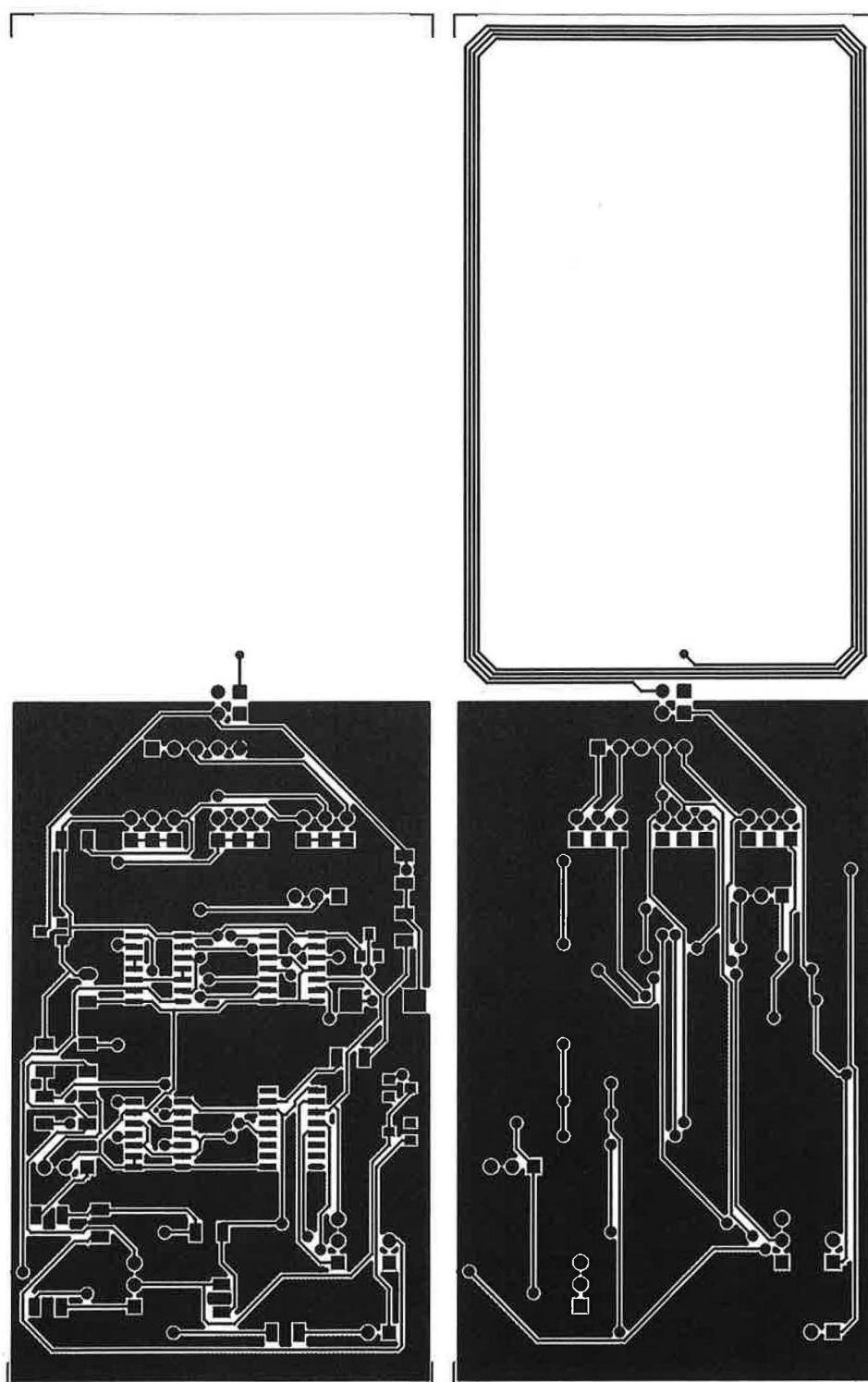


Figure 14.2 Printed circuit board layout of the test card, front and back

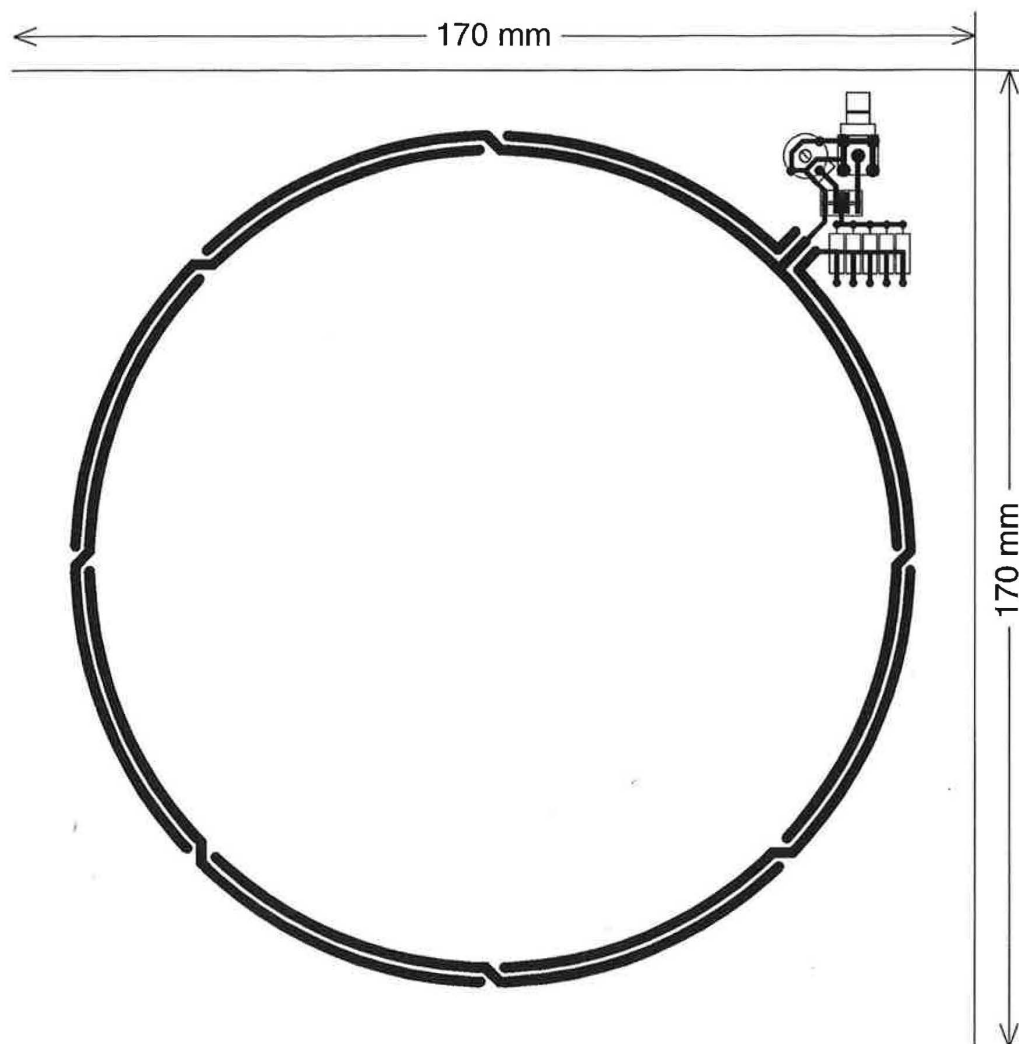


Figure 14.3 Layout of the field generator coil — front (reproduced by permission of Philips Semiconductors, Hamburg)

Table 14.3 Parts list of the interface circuit

Component	Value	Comment
C1	47 pF	—
C2	180 pF, 33 pF	Parallel
C3	2–27 pF	Trimming capacitor
R1	$5 \times 4.7 \Omega$	Parallel

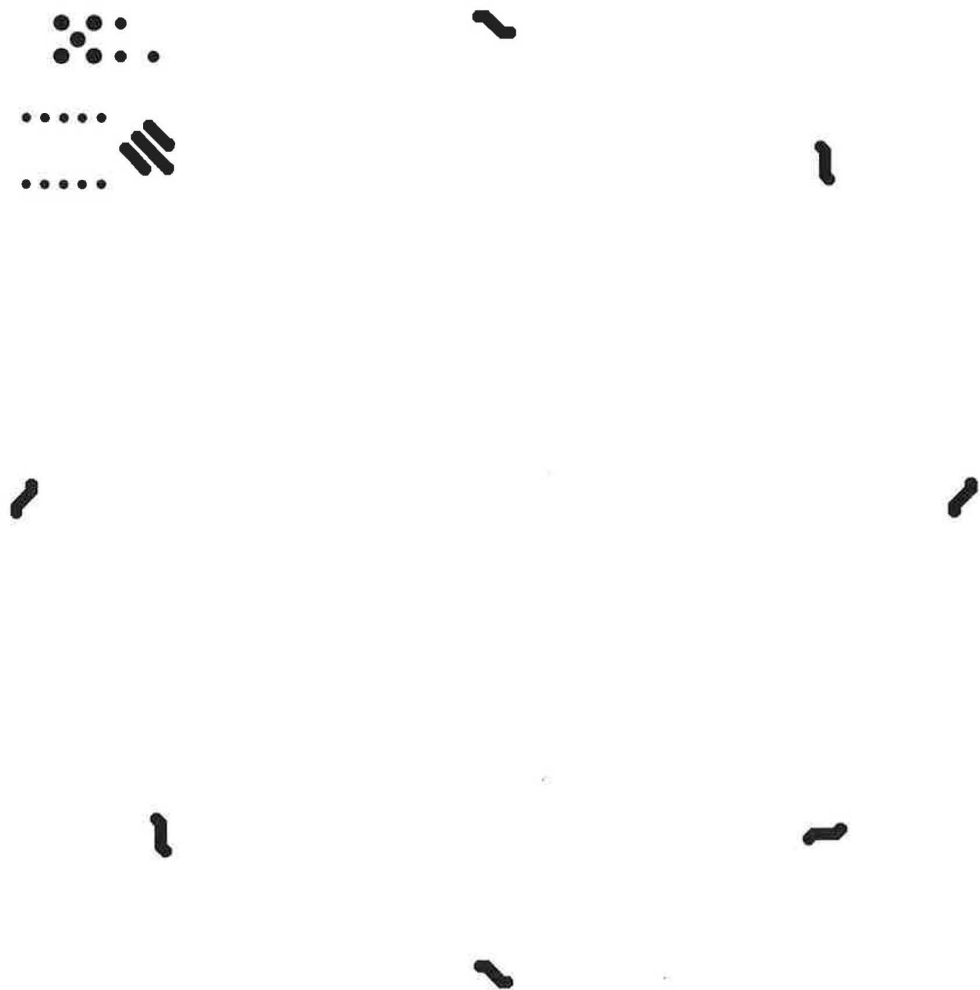


Figure 14.4 Layout of the field generator coil — back (reproduced by permission of Philips Semiconductors, Hamburg)

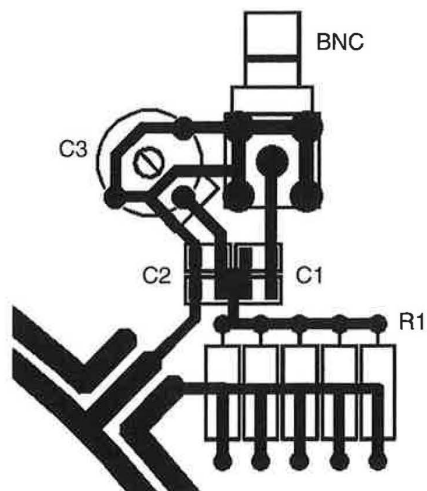


Figure 14.5 Interface circuit of the field generator coil — component mounting diagram

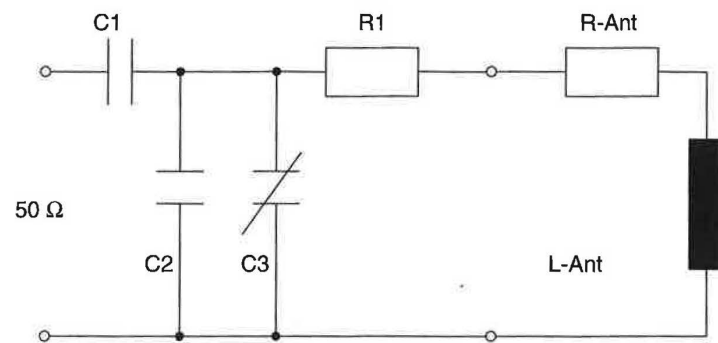


Figure 14.6 Interface circuit of the field generator coil — circuit