frequency range permit the radio services that occupy this range to reach areas within a radius of over 1000 km continuously at a low technical cost. Typical radio services in this frequency range are aeronautical and marine navigational radio services (LORAN C, OMEGA, DECCA), time signal services, and standard frequency services, plus military radio services. Thus, in central Europe the time signal transmitter DCF 77 in Mainflingen can be found at around the frequency 77.5 kHz. An RFID system operating at this frequency would therefore cause the failure of all radio clocks within a radius of several hundred metres around a reader.

In order to prevent such collisions, the future Licensing Act for Inductive Radio Systems in Europe, 220 ZV 122, will define a protected zone of between 70 and 119 kHz, which will no longer be allocated to RFID systems.

The radio services permitted to operate within this frequency range in Germany (source: BAPT 1997) are shown in Table 5.1.

Wire-bound carrier systems also operate at the frequencies 100 kHz, 115 kHz and 130 kHz. These include, for example, intercom systems that use the 220 V supply main as a transmission medium.

5.1.2 Frequency range 6.78 MHz

The range 6.765–6.795 MHz belongs to the *short wave frequencies*. The propagation conditions in this frequency range only permit short ranges of up to a few 100 km in the daytime. During the night-time hours, transcontinental propagation is possible. This frequency range is used by a wide range of radio services, for example broadcasting, weather and aeronautical radio services and press agencies.

This range has not yet been passed as an ISM range in Germany, but has been designated an ISM band by the international ITU and is being used to an increasing degree by RFID systems (in France, among other countries). CEPT/ERC and ETSI designate this range as a harmonised frequency in the CEPT/ERC 70–03 regulation (see Section 5.2.1).

5.1.3 Frequency range 13.56 MHz

The range 13.553–13.567 MHz is located in the middle of the short wavelength range. The propagation conditions in this frequency range permit transcontinental connections throughout the day. This frequency range is used by a wide variety of radio services (Siebel, 1983), for example press agencies and telecommunications (PTP).

Other ISM applications that operate in this frequency range, in addition to inductive radio systems (RFID), are remote control systems, remote controlled models, demonstration radio equipment and pagers.

5.1.4 Frequency range 27.125 MHz

The frequency range 26.565–27.405 is allocated to CB radio across the entire European continent as well as in the USA and Canada. Unregistered and non-chargeable radio

WAVELYNX EX. 1008, Pg. 51
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Table 5.1 German radio services in the frequency range 9–135 kHz. The actual occupation of frequencies, particularly within the range 119–135 kHz has fallen sharply. For example, the German weather service (DWD) changed the frequency of its weather fax transmissions to 134.2 kHz as early as mid-1996

f (kHz)	Class	Location	Call
16.4	FX	Mainflingen	DMA
18.5	FX	Burlage	DHO35
23.4	FX	Mainflingen	DMB
28.0	FC	Burlage	DHO36
36.0	FC	Burlage	DHO37
46.2	FX	Mainflingen	DCF46
47.4	FC	Cuxhafen	DHJ54
53.0	FX	Mainflingen	DCF53
55.2	FX	Mainflingen	DCF55
69.7	FX	Königswusterhausen	DKQ
71.4	AL	Coburg	—
74.5	FX	Königswusterhausen	DKQ2
77.5	Time	Mainflingen	DCF77
85.7	AL	Brilon	—
87.3	FX	Bonn	DEA
87.6	FX	Mainflingen	DCF87
94.5	FX	Königswusterhausen	DKQ3
97.1	FX	Mainflingen	DCF97
99.7	FX	Königswusterhausen	DIU
100.0	NL	Westerland	—
103.4	FX	Mainflingen	DCF23
105.0	FX	Königswusterhausen	DKQ4
106.2	FX	Mainflingen	DCF26
110.5	FX	Bad Vilbel	DCF30
114.3	AL	Stadtkyll	—
117.4	FX	Mainflingen	DCF37
117.5	FX	Königswusterhausen	DKQ5
122.5	DGPS	Mainflingen	DCF42
125.0	FX	Mainflingen	DCF45
126.7	AL	Portens, LORAN-C, coastal navigation	—
128.6	AL	Zeven, DECCA, coastal navigation	—
129.1	FX	Mainflingen, EVU remote control transmitter	DCF49
131.0	FC	Kiel (military)	DHJ57
131.4	FX	Kiel (military	DHJ57

Abbreviations: AL: Air navigation radio service, FC: Mobile marine radio service, FX: Fixed aeronautical radio service, MS: Mobile marine radio service, NL: Marine navigation radio service, DGPS: Differential Global Positioning System (correction data), Time: Time signal transmitter for 'radio clocks'.

systems with transmit power up to 4 Watts permit radio communication between private participants over distances of up to 30 km.

The ISM range between 26.957 and 27.283 MHz is located approximately in the middle of the CB radio range. In addition to inductive radio systems (RFID), ISM

applications operating in this frequency range include diathermic apparatus (medical application), high frequency welding equipment (industrial application), remote controlled models and pagers.

When installing 27 MHz RFID systems for industrial applications, particular attention should be given to any high frequency welding equipment that may be located in the vicinity. HF welding equipment generates high field strengths, which may interfere with the operation of RFID systems operating at the same frequency in the vicinity. When planning 27 MHz RFID systems for hospitals (e.g. access systems), consideration should be given to any diathermic apparatus that may be present.

5.1.5 Frequency range 40.680 MHz

The range 40.660–40.700 MHz is located at the lower end of the *VHF range*. The propagation of waves is limited to the ground wave, so damping due to buildings and other obstacles is less marked. The frequency ranges adjoining this ISM range are occupied by mobile commercial radio systems (forestry, motorway management) and by television broadcasting (VHF range I).

The main ISM applications that are operated in this range are telemetry (transmission of measuring data) and remote control applications. The author knows of no RFID systems operating in this range, which can be attributed to the unsuitability of this frequency range for this type of system. The ranges that can be achieved with inductive coupling in this range are significantly lower than those that can be achieved at all the lower frequency ranges that are available, whereas the wavelengths of 7.5 m in this range are unsuitable for the construction of small and cheap backscatter transponders.

5.1.6 Frequency range 433.920 MHz

The frequency range 430.000–440.000 MHz is allocated to amateur radio services worldwide. Radio amateurs use this range for voice and data transmission and for communication via relay radio stations or home-built space satellites.

The propagation of waves in this *UHF frequency range* is approximately optical. A strong damping and reflection of incoming electromagnetic waves occurs when buildings and other obstacles are encountered.

Depending upon the operating method and transmission power, systems used by radio amateurs achieve distances between 30 and 300 km. Worldwide connections are also possible using space satellites.

The ISM range 433.050–434.790 MHz is located approximately in the middle of the amateur radio band and is extremely heavily occupied by a wide range of ISM applications. In addition to backscatter (RFID) systems, baby intercoms, telemetry transmitters (including those for domestic applications, e.g. wireless external thermometers), cordless headphones, unregistered LPD walkie-talkies for short range radio, keyless entry systems (handheld transmitters for vehicle central locking) and many other applications are crammed into this frequency range. Unfortunately, mutual interference between the wide range of ISM applications is not uncommon in this frequency range.

WAVELYNX EX. 1008, Pg. 52
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

5.1.7 Frequency range 869.0 MHz

The frequency range 868–870 MHz was passed for Short Range Devices (SRDs) in Europe at the end of 1997 and is thus available for RFID applications in the 43 member states of CEPT.

A few Far Eastern countries are also considering passing this frequency range for SRDs.

5.1.8 Frequency range 915.0 MHz

This frequency range is not available for ISM applications in Europe. Outside Europe (USA and Australia) the frequency ranges 888–889 MHz and 902–928 MHz are available and are used by backscatter (RFID) systems.

Neighbouring frequency ranges are occupied primarily by D-net telephones and cordless telephones as described in the CT1+ and CT2 standards.

5.1.9 Frequency range 2.45 GHz

The ISM range 2.400–2.4835 GHz partially overlaps with the frequency ranges used by amateur radio and radiolocation services. The propagation conditions for this UHF frequency range and the higher frequency SHF range are quasi-optical. Buildings and other obstacles behave as good reflectors and damp an electromagnetic wave very strongly at transmission (passage).

In addition to the *backscatter* (RFID) systems, typical ISM applications that can be found in this frequency range are telemetry transmitters and PC LAN systems for the wireless networking of PCs.

5.1.10 Frequency range 5.8 GHz

The ISM range 5.725–5.875 GHz partially overlaps with the frequency ranges used by amateur radio and radiolocation services.

Typical ISM applications for this frequency range are movement sensors, which can be used as door openers (in shops and department stores), or contactless toilet flushing, plus backscatter (RFID) systems.

5.1.11 Frequency range 24.125 GHz

The ISM range 24.00–24.25 GHz overlaps partially with the frequency ranges used by amateur radio and radiolocation services plus earth resources services via satellite.

This frequency range is used primarily by movement sensors, but also directional radio systems for data transmission. The author knows of no RFID systems operating in this frequency range.

5.1.12 Selection of a suitable frequency for inductively coupled RFID systems

The characteristics of the few available frequency ranges should be taken into account when selecting a frequency for an *inductively coupled* RFID system. The usable field strength in the operating range of the planned system exerts a decisive influence on system parameters. This variable therefore deserves further consideration. In addition, the *bandwidth* (mechanical) dimensions of the antenna coil and the availability of the frequency band should also be considered.

The path of field strength of a magnetic field in the *near* and *far field* was described in detail in Section 4.2.1.1. We learned that the reduction in field strength with increasing distance from the antenna was 60 dB/decade initially, but that this falls to 20 dB/decade after the transition to the far field at a distance of $\lambda/2\pi$. This behaviour exerts a strong influence on the usable field strengths in the system's operating range. Regardless of the operating frequency used, the regulation *EN 300 330* specifies the maximum magnetic field strength at a distance of 10 m from a reader (Figure 5.3).

If we move from this point in the direction of the reader, then, depending upon the wavelength, the field strength increases initially at 20 dB/decade. At an operating frequency of 6.78 MHz the field strength begins to increase by 60 dB/decade at a distance of 7.1 m — the transition into the near field. However, at an operating frequency of 27.125 MHz this steep increase does not begin until a distance of 1.7 m is reached.

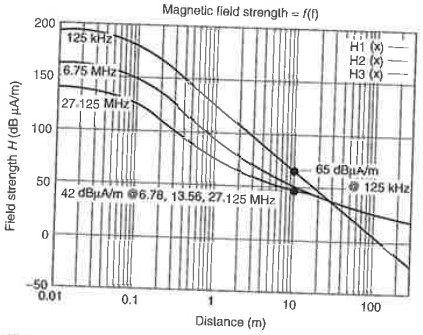


Figure 5.3 Different permissible field strengths for inductively coupled systems measured at a distance of 10 m (the distance specified for licensing procedures) and the difference in the distance at which the reduction occurs at the transition between near and far field lead to marked differences in field strength at a distance of 1 m from the antenna of the reader. For the field strength path at a distance under 10 cm, we have assumed that the antenna radius is the same for all antennas

WAVELYNX EX. 1008, Pg. 53
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

It is not difficult to work out that, given the same field strength at a distance of 10 m, higher usable field strengths can be achieved in the operating range of the reader (e.g. 0–10 cm) in a lower frequency ISM band than would be the case in a higher frequency band. At <135 kHz the relationships are even more favourable, first because the permissible field strength limit is much higher than it is for ISM bands above 1 MHz, and second because the 60 dB increase takes effect immediately, because the near field in this frequency range extends to at least 350 m.

If we measure the range of an inductively coupled system with the same magnetic field strength H at different frequencies we find that the range is maximised in the frequency range around 10 MHz (Figure 5.4). This is because of the proportionality $U_{ind} \sim \omega$. At higher frequencies around 10 MHz the efficiency of power transmission is significantly greater than at frequencies below 135 kHz.

However, this effect is compensated by the higher permissible field strength at 135 kHz, and therefore in practice the range of RFID systems is roughly the same for both frequency ranges. At frequencies above 10 MHz the L/C relationship of the transponder resonant circuit becomes increasingly unfavourable, so the range in this frequency range starts to decrease.

Overall, the following preferences exist for the various frequency ranges:

<135 kHz Preferred for large *ranges* and *low cost transponders*.

- High level of power available to the transponder.
- The transponder has a low power consumption due to its lower clock frequency.

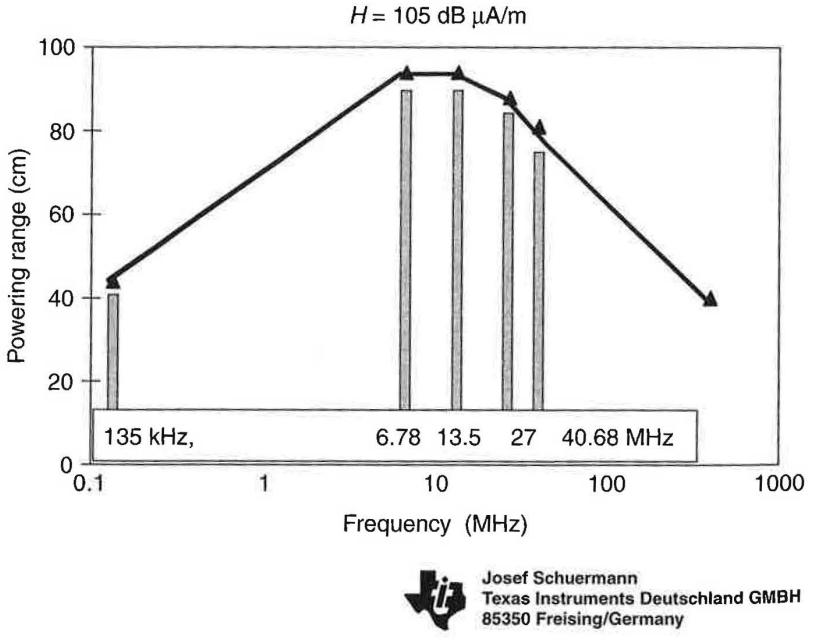


Figure 5.4 Transponder range at the same field strength. The induced voltage at a transponder is measured with the antenna area and magnetic field strength of the reader antenna held constant (reproduced by permission of Texas Instruments)

WAVELYNX EX. 1008, Pg. 54
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

- Miniaturised transponder formats are possible (animal ID) due to the use of ferrite coils in the transponder.
- Low absorption rate or high *penetration depth* in non-metallic materials and water (the high penetration depth is exploited in animal identification by the use of the bolus, a transponder placed in the rumen).

6.78 MHz Can be used for low cost and medium speed transponders.

- Worldwide ISM frequency according to ITU frequency plan; however, this is not used in some countries (i.e. licence may not be used worldwide).
- Available power is a little greater than that for 13.56 MHz.
- Only half the clock frequency of that for 13.56 MHz.

13.56 MHz Can be used for high speed/high end and medium speed/low end applications.

- Available worldwide as an ISM frequency.
- Fast data transmission (typically 106 kbits/s).
- High clock frequency, so cryptological functions or a microprocessor can be realised.
- Parallel capacitors for transponder coil (resonance matching) can be realised on-chip.

27.125 MHz Only for special applications (e.g. Eurobalise)

- Not a worldwide ISM frequency.
- Large bandwidth, thus very fast data transmission (typically 424 kbits/s)
- High clock frequency, thus cryptological functions or a microprocessor can be realised.
- Parallel capacitors for transponder coil (resonance matching) can be realised on-chip.
- Available power somewhat lower than for 13.56 MHz.
- Only suitable for small ranges.

5.2 European Licensing Regulations

5.2.1 CEPT/ERC REC 70-03

This new CEPT harmonisation document entitled *'ERC Recommendation 70–03* relating to the use of *short range devices* (SRD)' (ERC, 2002) that serves as the basis for new national regulations in all 44 member states of CEPT has been available since

WAVELYNX EX. 1008, Pg. 55
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

When CRC algorithms were first developed for disk controllers, priority was given to the realisation of a simple CRC processor in the form of a hardware circuit. This gave rise to a CRC processor made up of backcoupled *shift registers* and XOR gates that is very simple to implement (Figure 7.6).

When calculating CRC 16 using shift registers, the 16-bit shift register is first set to its starting value. The calculation is then initiated by shifting the data bits, starting with the lowest in value, into the backcoupled shift register one after the other. The backcoupling or polynomial division is based upon the XOR logic gating of the CRC bits (Figure 7.7). When all the bits have been shifted through the register, the calculation is complete and the content of the 16-bit CRC register represents the desired CRC (Rankl and Effing, 1996).

7.2 Multi-Access Procedures – Anticollision

The operation of RFID systems often involves a situation in which numerous transponders are present in the interrogation zone of a single reader at the same time. In such a system — consisting of a 'control station', the reader, and a number of 'participants', the transponders — we can differentiate between two main forms of communication.

The first is used to transmit data from a reader to the transponders (Figure 7.8). The transmitted data stream is received by all transponders simultaneously. This is comparable with the simultaneous reception by hundreds of radio receivers of a news programme transmitted by a radio station. This type of communication is therefore known as *broadcast* (abramson, n.d.).

The second form of communication involves the transmission of data from many individual transponders in the reader's interrogation zone to the reader. This form of communication is called *multi-access* (Figure 7.9).

Every communication channel has a defined channel capacity, which is determined by the maximum data rate of this communication channel and the time span of its availability. The available channel capacity must be divided between the individual

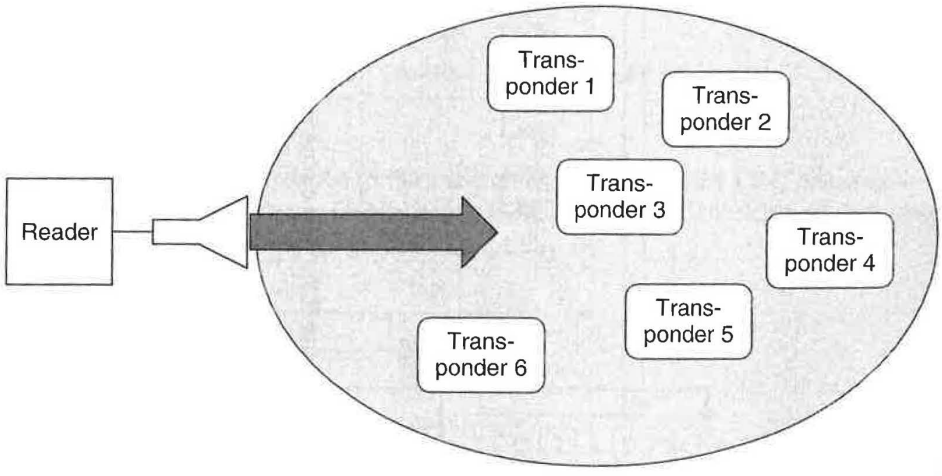


Figure 7.8 Broadcast mode: the data stream transmitted by a reader is received simultaneously by all transponders in the reader's interrogation zone

WAVELYNX EX. 1008, Pg. 56
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

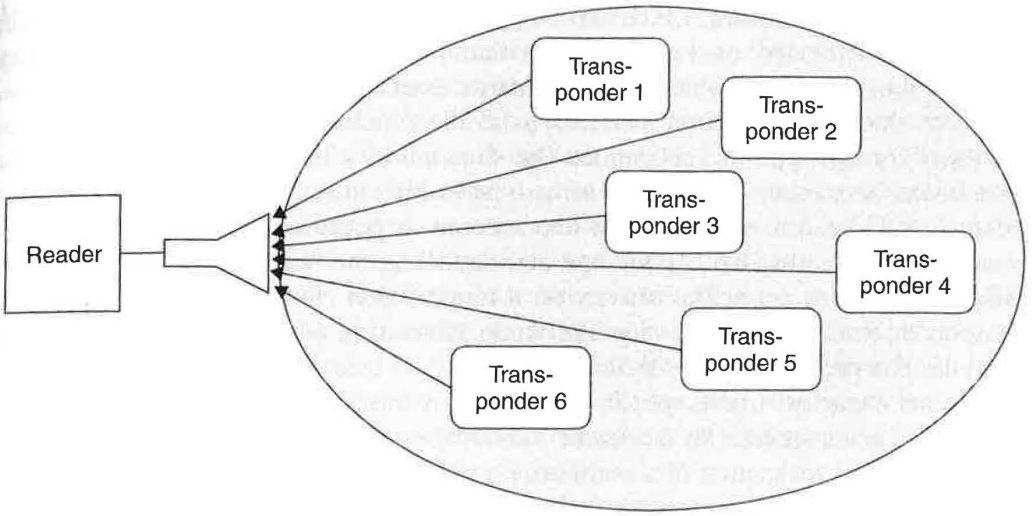


Figure 7.9 Multi-access to a reader: numerous transponders attempt to transfer data to the reader simultaneously

participants (transponders) such that data can be transferred from several transponders to a single reader without mutual interference (collision).

In an inductive RFID system, for example, only the receiver section in the reader is available to all transponders in the interrogation zone as a common channel for data transfer to the reader. The maximum data rate is found from the effective bandwidth of the antennas in the transponder and reader.

The problem of multi-access has been around for a long time in radio technology. Examples include news satellites and mobile telephone networks, where a number of participants try to access a single satellite or base station. For this reason, numerous procedures have been developed with the objective of separating the individual participant signals from one another. Basically, there are four different procedures (Figure 7.10): *space division multiple access (SDMA), frequency domain multiple access (FDMA), time domain multiple access (TDMA)* and *code division multiple access (CDMA)*, otherwise known as *spread-spectrum*. However, these classical procedures are based upon the assumption of an uninterrupted data stream from and to the participants (Fliege, 1996), once a channel capacity has been split it remains split until the communication relationship ends (e.g. for the duration of a telephone conversation).

RFID transponders, on the other hand, are characterised by brief periods of activity interspersed by pauses of unequal length. A contactless smart card in the form of a

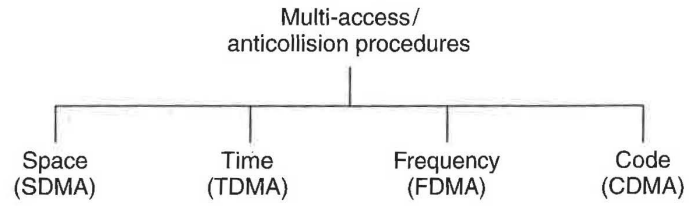


Figure 7.10 Multi-access and anticollision procedures are classified on the basis of four basic procedures

WAVELYNX EX. 1008, Pg. 57
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

public transport travel card, which is brought within the interrogation zone of a reader, has to be authenticated, read and written within a few tens of milliseconds. There may follow a long period in which no smart cards enter the reader's interrogation zone. However, this example should not lead us to the conclusion that multi-access is not necessary for this type of application. The situation in which a passenger has two or three contactless smart cards of the same type in his wallet, which he holds up to the antenna of the reader, must be taken into account. A powerful multi-access procedure is capable of selecting the correct card and deducting the fare without any detectable delay, even in this case. The activity on a transmission channel between reader and transponder thus possesses a very high burst factor (Fliege, 1996) and we therefore also talk of a packet access procedure.

Channel capacity is only split for as long as is actually necessary (e.g. during the selection of a transponder in the reader's interrogation zone).

The technical realisation of a multi-access procedure in RFID systems poses a few challenges for transponder and reader, since it has to reliably prevent the transponders' data (packages) from colliding with each other in the reader's receiver and thus becoming unreadable, without this causing a detectable delay. In the context of RFID systems, a technical procedure (access protocol) that facilitates the handling of multi-access without any interference is called an *anticollision system.*

The fact that a data packet sent to a reader by a single transponder, e.g. by load modulation, cannot be read by all the other transponders in the interrogation zone of this reader poses a particular challenge for almost all RFID systems. Therefore, a transponder cannot in the first instance detect the presence of other transponders in the interrogation zone of the reader.

For reasons of competition, system manufacturers are not generally prepared to publish the anticollision procedures that they use. Therefore, little can be found on this subject in the technical literature, so a comprehensive survey of this subject is, unfortunately, not possible at this point. Some examples at the end of the chapter should serve to clarify the practical realisation of anticollision procedures.

7.2.1 Space division multiple access (SDMA)

The term *space division multiple access* relates to techniques that reuse a certain resource (channel capacity) in spatially separated areas (Fliege, 1996).

One option is to significantly reduce the *range* of a single reader, but to compensate by bringing together a large number of readers and antennas to form an array, thus providing coverage of an area. As a result, the channel capacity of adjoining readers is repeatedly made available. Such procedures have been successfully used in large-scale marathon events to detect the run times of marathon runners fitted with transponders (see also Section 13.9). In this application a number of reader antennas are inserted into a tartan mat. A runner travelling over the mat 'carries' his transponder over the interrogation zone of a few antennas that form part of the entire layout. A large number of transponders can thus be read simultaneously as a result of the spatial distribution of the runners over the entire layout.

A further option is to use an electronically controlled directional antenna on the reader. the directional beam of which can be pointed directly at a transponder (adaptive

WAVELYNX EX. 1008, Pg. 58
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

SDMA). So various transponders can be differentiated by their angular position in the interrogation zone of the reader.[1] Phased array antennas are used as electronically controlled directional antennas. These consist of several dipole antennas, and therefore adaptive SDMA can only be used for RFID applications at frequencies above 850 MHz (typical 2.45 GHz) as a result of the size of the antennas. Each of the dipole elements is driven at a certain, independent phase position. The directional diagram of the antenna is found from the different superposition of the individual waves of the dipole elements in different directions. In certain directions the individual fields of the dipole antenna are superimposed in phase, which leads to the amplification of the field. In other directions the waves wholly or partially obliterate each other. To set the direction, the individual elements are supplied with an HF voltage of adjustable, variable phase by controlled phase modifiers. In order to address a transponder, the space around the reader must be scanned using the directional antenna, until a transponder is detected by the 'search light' of the reader (Figure 7.11).

A disadvantage of the SDMA technique is the relatively high implementation cost of the complicated antenna system. The use of this type of anticollision procedure is therefore restricted to a few specialised applications.

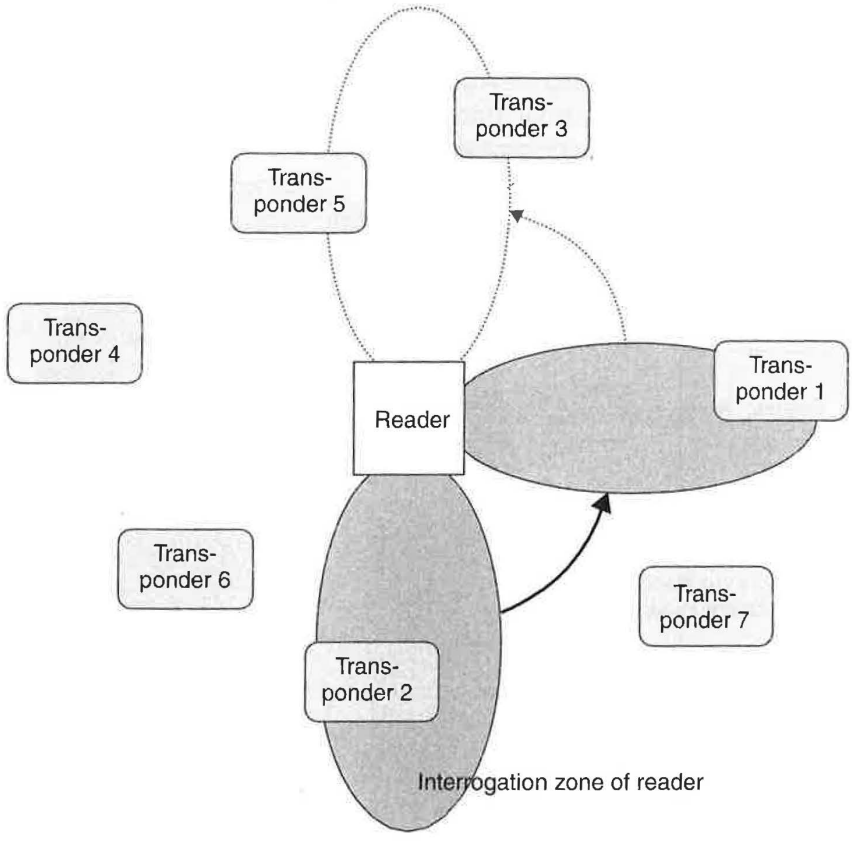


Figure 7.11 Adaptive SDMA with an electronically controlled directional antenna. The directional beam is pointed at the various transponders one after the other

[1] If the angle between two transponders is greater than the beam width of the directional antennas used a transmission channel can be used several times.

WAVELYNX EX. 1008, Pg. 59
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

7.2.2 Frequency domain multiple access (FDMA)

The term *frequency domain multiple access* relates to techniques in which several transmission channels on various carrier frequencies are simultaneously available to the communication participants.

In RFID systems, this can be achieved using transponders with a freely adjustable, anharmonic transmission frequency. The power supply to the transponder and the transmission of control signals (broadcast) takes place at the optimally suited reader frequency f_a. The transponders respond on one of several available response frequencies $f_1 - f_N$ (Figure 7.12). Therefore, completely different frequency ranges can be used for the data transfer from and to the transponders (e.g. reader → transponder (downlink): 135 kHz, transponder → reader (uplink): several channels in the range 433–435 MHz).

One option for load modulated RFID systems or backscatter systems is to use various independent subcarrier frequencies for the data transmission from the transponders to the reader.

One disadvantage of the FDMA procedure is the relatively high cost of the readers, since a dedicated receiver must be provided for every reception channel. This anticollision procedure, too, remains limited to a few specialised applications.

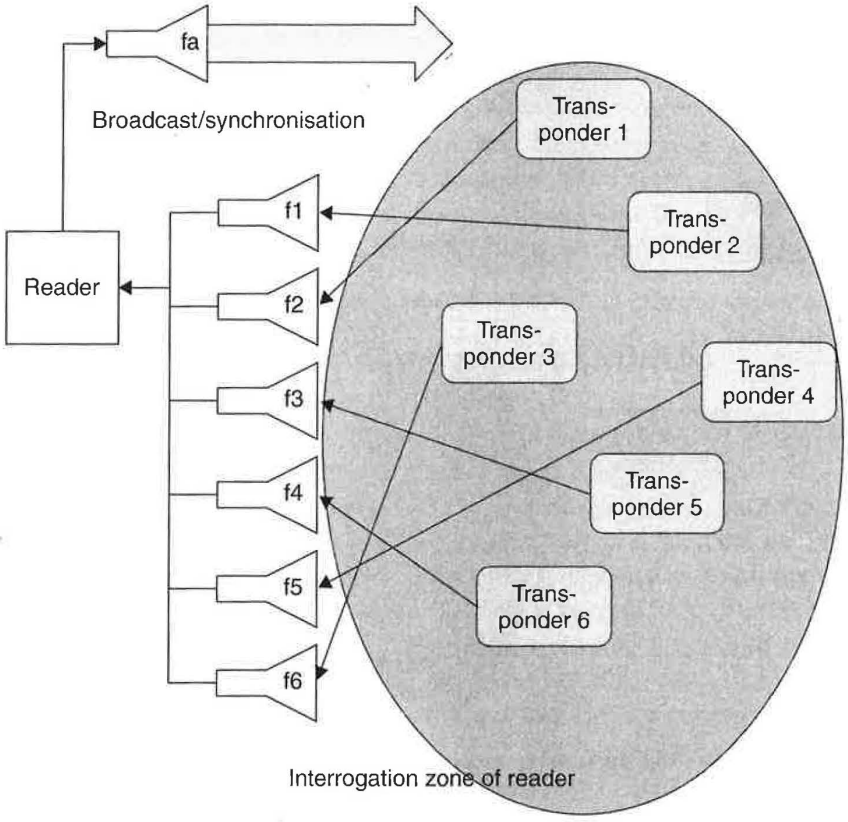


Figure 7.12 In an FDMA procedure several frequency channels are available for the data transfer from the transponders to the reader

WAVELYNX EX. 1008, Pg. 60
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

7.2.3 Time domain multiple access (TDMA)

The term *time domain multiple access* relates to techniques in which the entire available channel capacity is divided between the participants chronologically. TDMA procedures are particularly widespread in the field of digital mobile radio systems. In RFID systems, TDMA procedures are by far the largest group of anticollision procedures. We differentiate between transponder-driven and interrogator-driven procedures (Figure 7.13).

Transponder-driven procedures function asynchronously, since the reader does not control the data transfer. This is the case, for example, in the *ALOHA procedure*, which is described in more detail in Section 7.2.4. We also differentiate between 'switched off' and 'non-switched' procedures depending upon whether a transponder is switched off by a signal from the reader after successful data transfer.

Transponder-driven procedures are naturally very slow and inflexible. Most applications therefore use procedures that are controlled by the reader as the master (interrogator-driven). These procedures can be considered as synchronous, since all transponders are controlled and checked by the reader simultaneously. An individual transponder is first selected from a large group of transponders in the interrogation zone of the reader using a certain algorithm and then the communication takes place between the selected transponder and the reader (e.g. authentication, reading and writing of data). Only then is the communication relationship terminated and a further transponder selected. Since only one communication relationship is initiated at any one time, but the transponders can be operated in rapid succession, interrogator-driven procedures are also known as time duplex procedures.

Interrogator-driven procedures are subdivided into *polling* and *binary search* procedures. All these procedures are based upon transponders that are identified by a unique serial number:

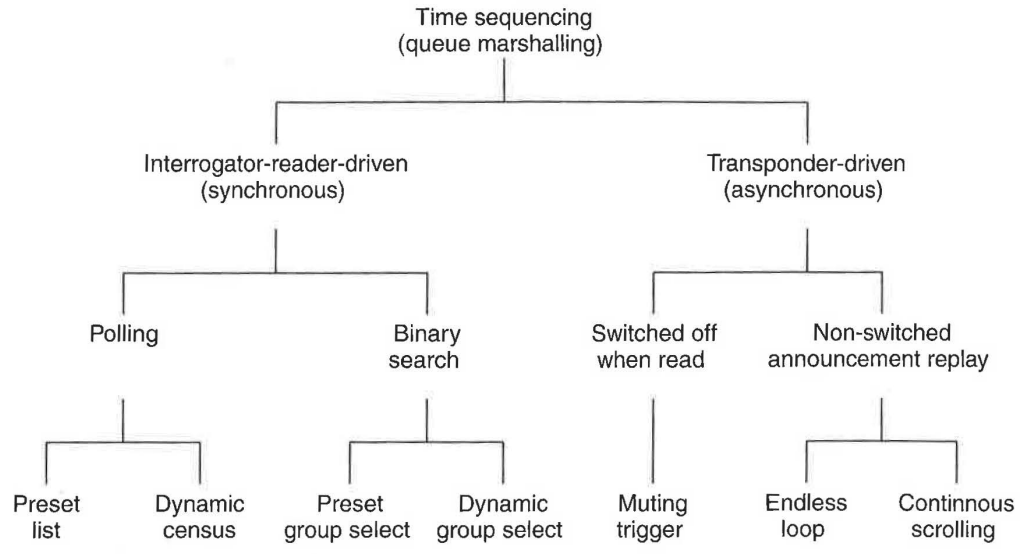


Figure 7.13 Classification of time domain anticollision procedures according to Hawkes (1997)

WAVELYNX EX. 1008, Pg. 61
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

The polling procedure requires a list of all the transponder serial numbers that can possibly occur in an application. All the serial numbers are interrogated by the reader one after the other, until a transponder with an identical serial number responds. This procedure can, however, be very slow, depending upon the number of possible transponders, and is therefore only suitable for applications with few known transponders in the field.

Binary search procedures are the most flexible, and therefore the most common, procedures. In a binary search procedure, a transponder is selected from a group by intentionally causing a data collision in the transponder serial numbers transmitted to the reader following a *request command* from the reader. If this procedure is to succeed it is crucial that the reader is capable of determining the precise bit position of a collision using a suitable signal coding system. A comprehensive description of the binary search procedure is given in Section 7.2.4.

7.2.4 Examples of anticollision procedures

In the following subsections some of the more frequently used examples of anticollision algorithms are discussed. The algorithms in the examples are intentionally simplified such that the functional principle of the algorithm can be understood without unnecessary complication.

7.2.4.1 ALOHA procedure

The simplest of all the multi-access procedures is the *ALOHA* procedure, which got its name from the fact that this multi-access procedure was developed in the 1970s for ALOHANET — a radio network for data transmission on Hawaii. As soon as a data packet is available it is sent from the transponder to the reader. This is a transponder-driven stochastic TDMA procedure.

The procedure is used exclusively with read-only transponders, which generally have to transfer only a small amount of data (serial numbers), this data being sent to the reader in a cyclical sequence. The data transmission time represents only a fraction of the repetition time, so there are relatively long pauses between transmissions. Furthermore, the repetition times for the individual transponders differ slightly. There is therefore a certain probability that two transponders can transmit their data packets at different times and the data packets will not collide with one another.

The time sequence of a data transmission in an ALOHA system is shown in Figure 7.14. The offered load G corresponds with the number of transponders transmitting simultaneously at a certain point in time $t0$ (i.e. 0, 1, 2, 3, ...). The average *offered load* G is the average over an observation period T and is extremely simple to calculate from the transmission duration τ of a data packet:

$$G = \sum_{1}^{n} \frac{\tau_n}{T} \cdot r_n \qquad (7.1)$$

WAVELYNX EX. 1008, Pg. 62
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Table 9.5 Position 1 (state A, unmodulated; state A′, modulated)

A	A′
ΦF	$1\Phi'F1 = \Phi F1 - 90°$
$\Phi F3 = \Phi F1 + 90°$	$\Phi'F3 = \Phi F3 + 90°$

Table 9.6 Position 2 (state A, unmodulated; state A′, modulated)

A	A′
F1	$\Phi'F1 = \Phi'F1 + 90°$
$\Phi F3 = \Phi F1 - 90°$	$\Phi'F3 = \Phi'F3 - 90°$

9.2.2 ISO 14443 – Proximity coupling smart cards

ISO standard 14443 entitled 'Identification cards — Proximity integrated circuit(s) cards' describes the operating method and operating parameters of contactless proximity coupling smart cards. This means contactless smart cards with an approximate range of 7–15 cm, like those used predominantly in the field of ticketing. The data carrier of these smart cards is normally a microprocessor and they often have additional contacts (see also Section 10.2.1).

The standard comprises the following parts:

- Part 1: Physical characteristics.
- Part 2: Radio frequency power and signal interface.
- Part 3: Initialisation and anticollision (still in preparation).
- Part 4: Transmission protocols (in preparation).

9.2.2.1 Part 1 – Physical characteristics

Part 1 of the standard defines the mechanical properties of the smart cards. The dimensions correspond with the values specified in ISO 7810, i.e. 85.72 mm × 54.03 mm × 0.76 mm ± tolerances.

Furthermore, this part of the standard also includes notes on the testing of the dynamic bending stress and dynamic torsion stress, plus irradiation with UV, x-ray and electromagnetic radiation.

9.2.2.2 Part 2 – Radio frequency interference

The power supply of inductively coupled *proximity cards* (*PICC*) is provided by the magnetic alternating field of a reader (PCD) at a transmission frequency of 13.56 MHz.

WAVELYNX EX. 1008, Pg. 63
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

To this end the card incorporates a large area antenna coil typically with 3–6 windings of wire (see Figures 2.11 and 2.12).

The magnetic field generated by the reader must be within the range $1.5\,\text{A/m} \leq H \leq 7.5\,\text{A/m}$. Thus the *interrogation field strength* $H_{\min}$ of a proximity coupling smart card is automatically $H_{\min} \leq 1.5\,\text{A/m}$. This is the only way to ensure that a smart card with an interrogation field strength $H_{\min} = 1.5\,\text{A/m}$ can be read by a reader that generates a field strength of just 1.5 A/m (e.g. a portable, battery operated reader with a correspondingly lower transmission power), at least at distance $x = 0$ from the transmission antenna (smart card in contact) (Berger, 1998).

If the field strength curve of a reader and the interrogation field strength of a proximity coupling smart card are known, then the range of the system can be calculated. The field strength curve of a typical reader in accordance with ISO 14443 is shown in Figure 9.11 (see Section 4.1.1.1). In this case, a smart card interrogation field strength of 1.5 A/m results in a range of 10 cm.

Unfortunately it was not possible to agree to a common communication interface in the development of this standard. For this reason, two completely different procedures for the data transfer between reader and proximity coupling smart card have found a place in ISO 14443 — Type A and Type B. A smart card only has to support one of the two communication procedures. A reader conforming to the standard, on the other hand, must be able to communicate equally well by both procedures, and thus support all smart cards. This means that the reader must switch between the two communication procedures (polling) periodically during 'idle' mode ('wait for smart card').

However, the reader may not switch between the two procedures during an existing communication relationship between reader and card.

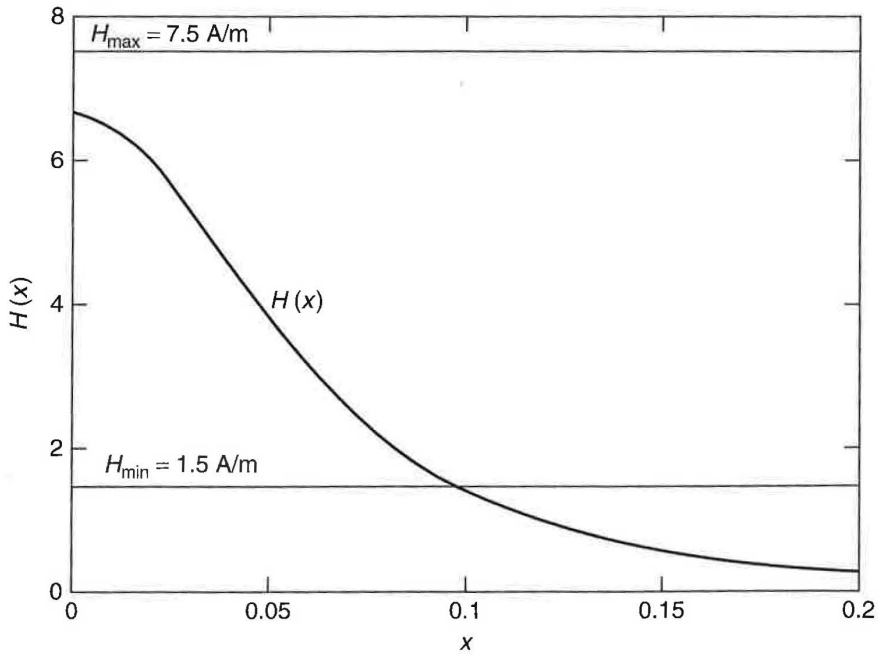


Figure 9.11 Typical field strength curve of a reader for proximity coupling smart cards (antenna current $i_1 = 1\text{A}$, antenna diameter $D = 15\,\text{cm}$, number of windings $N = 1$)

WAVELYNX EX. 1008, Pg. 64
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

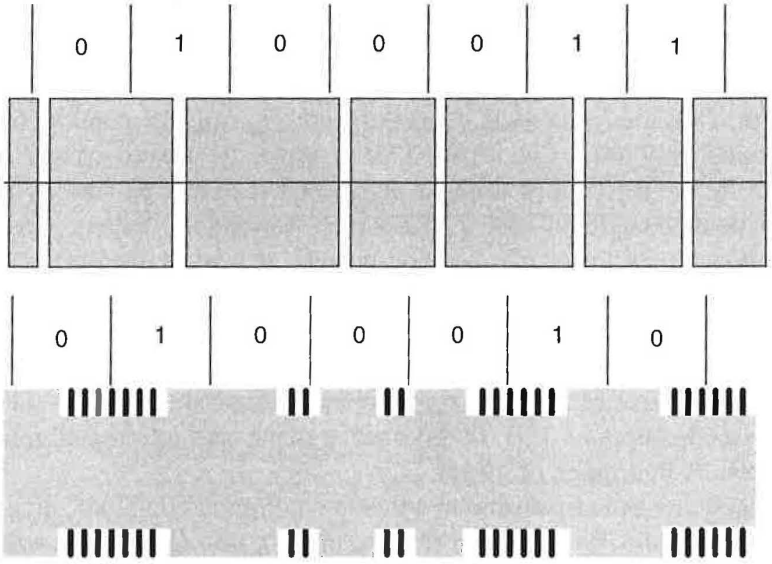


Figure 9.12 Modulation procedure for proximity coupling smart cards in accordance with ISO 14443 — Type A: Top: Downlink — ASK 100% with modified Miller coding (voltage path at the reader antenna). Bottom: Uplink — load modulation with ASK modulated 847 kHz subcarrier in Manchester coding (voltage path at the transponder coil)

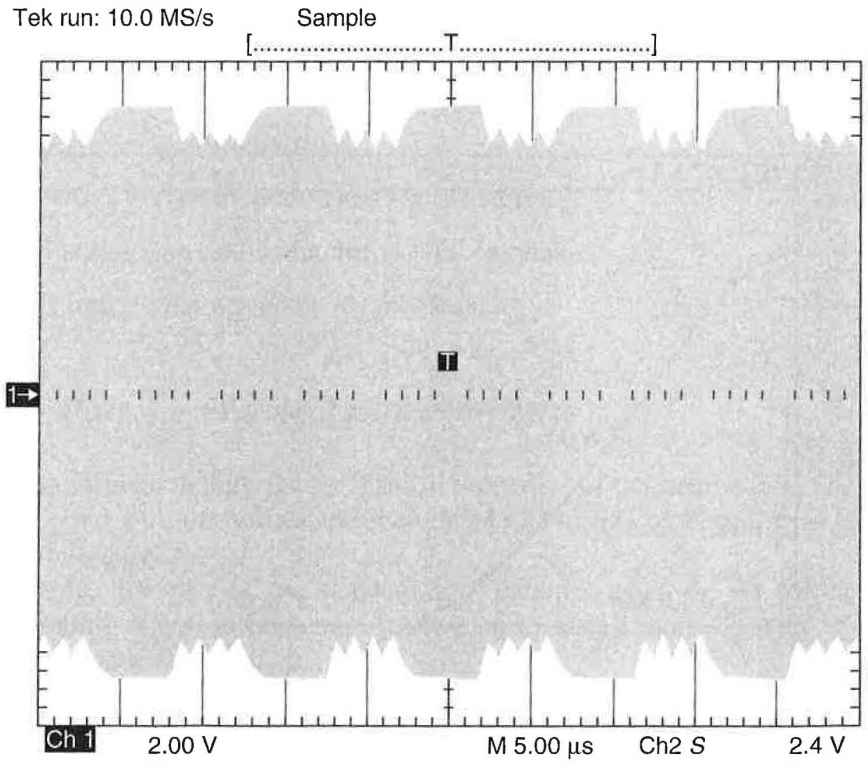


Figure 9.13 The oscillogram of a signal generated at the reader antenna by a Type A card using load modulation with an ASK modulated subcarrier

WAVELYNX EX. 1008, Pg. 65
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Communication interface – Type A In type A cards 100% *ASK modulation* with modified *Miller coding* (Figure 9.12) is defined as the modulation procedure used for the transfer of data from reader to card. In order to guarantee a continuous power supply to the card the length of the blanking intervals is just 2–3 μs. The requirements of the transient response and transient characteristics of the HF signal generated by the reader in the blanking intervals are described in detail in the standard. A load modulation procedure with subcarrier is used for data transfer from the smart card to the reader. The *subcarrier frequency* $f_H = 847\,\text{kHz}$ (13.56 MHz/16). The modulation of the subcarrier is performed by on/off keying of the subcarrier using a Manchester coded data stream. See Figures 9.12 and 9.13.

In both transfer directions the baud rate $f_{Bd} = 106\,\text{kBit/s}$ (13.56 MHz/128).

Communication interface – Type B In Type B cards 10% *ASK modulation* (Figure 9.14) is used as the modulation procedure for the data transfer from reader to card. A simple *NRZ coding* is used for bit coding. The transient response and transient characteristics of the HF signal in the 0/1 transitions are precisely defined in the standard and requirements of the quality of the transmission antenna can be derived from this (see Section 11.4.1.3).

For data transfer from the smart card to the reader load modulation with a subcarrier is also used for the Type B card. The subcarrier frequency $f_H = 847\,\text{kHz}$ (13.56 MHz/16). The subcarrier is modulated by 180° phase shift keying (BPSK) of the subcarrier using the NRZ coded data stream. See Figure 9.15.

In both transmission directions the baud rate $f_{Bd} = 106\,\text{kBit/s}$ (13.56 MHz/128).

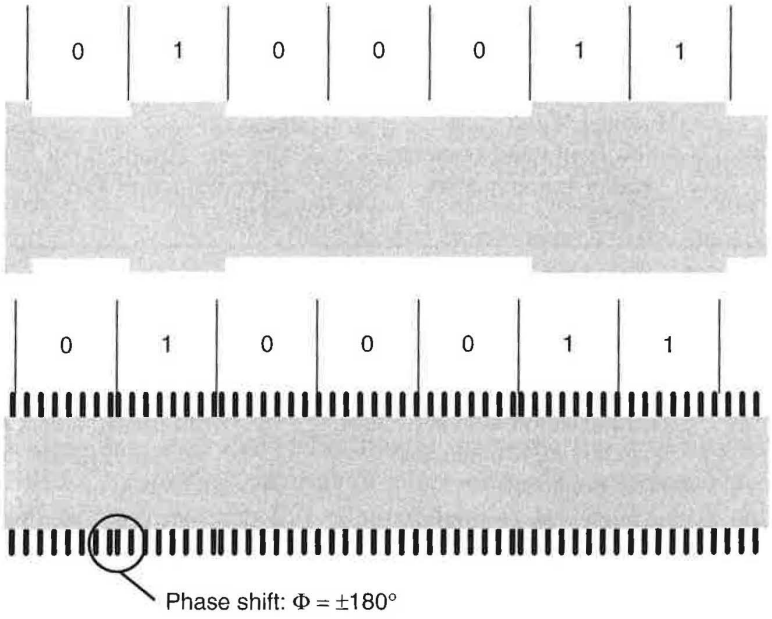


Figure 9.14 Modulation procedure for proximity coupling smart cards in accordance with ISO 14443 — Type B. Top: Downlink — ASK 10% with NRZ coding (voltage path at the reader antenna). Bottom: Uplink — load modulation with BPSK modulated 847 kHz subcarrier in NRZ coding (voltage path at the transponder coil)

WAVELYNX EX. 1008, Pg. 66
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

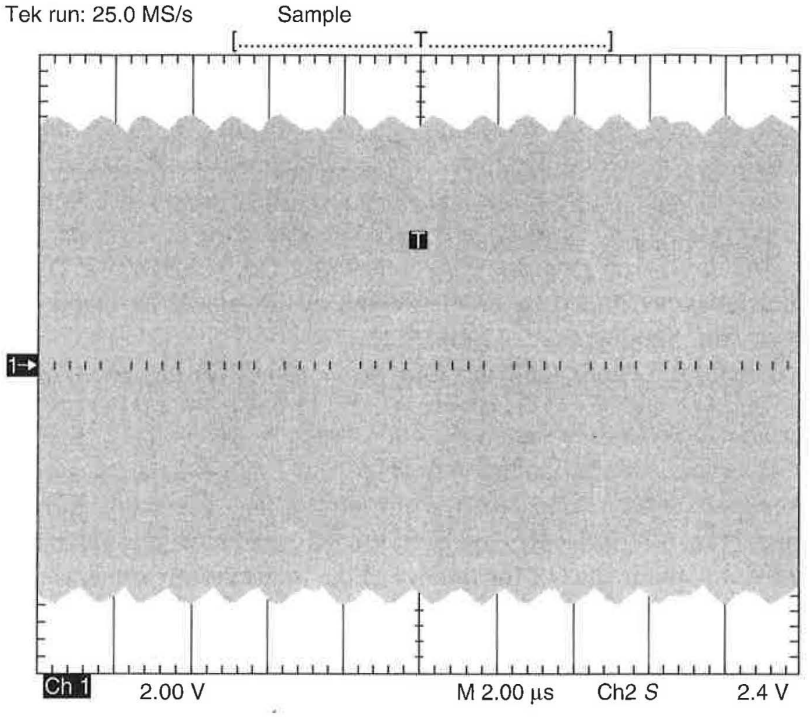


Figure 9.15 The oscillogram of a signal generated at the reader antenna by a Type B card using load modulation with BPSK modulated subcarrier

Table 9.7 Data transfer reader (PCD) → smart card (PICC) (Berger, 1998)

PCD → PICC	Type A	Type B
Modulation	ASK 100%	ASK 10% (modulation index 8%–12%)
Bit coding	Modified Miller code	NRZ code
Synchronisation	At bit level (start-of-frame, end-of-frame marks)	1 start and 1 stop bit per bye (specification in Part 3)
Baud rate	106 kBd	106 kBd

Table 9.8 Data transfer smart card (PICC) → reader (PCD) (Berger, 1998)

PICC → PCD	Type A	Type B
Modulation	Load modulation with subcarrier 847 kHz, ASK modulated	Load modulation with subcarrier 847 kHz, BPSK modulated
Bit coding	Manchester code	NRZ code
Synchronisation	1 bit frame synchronisation (start-of-frame, end-of-frame marks)	1 start and 1 stop bit per byte (specification in Part 3)
Baud rate	106 kBd	106 kBd

Overview To sum up, the parameters shown in Tables 9.7 and 9.8 exist for the physical interface between reader and smart card of an RFID system in accordance with ISO 14443-2.

WAVELYNX EX. 1008, Pg. 67
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

9.2.2.3 Part 3 – Initialisation and anticollision

If a proximity coupling smart card enters the interrogation field of a reader, then a communication relationship must first of all be built up between reader and smart card, taking into consideration the fact that there may be more than one smart card within the interrogation zone of this reader and that the reader may already be in communication with another card. This part of the standard therefore first describes the structure of the protocol frames from the basic elements defined in Part 2 — data bit, start-of-frame and end-of-frame marks — and the anticollision procedure used for the selection of an individual card. Since the different modulation procedure for Type A and Type B also requires a different frame structure and anticollision procedure, the divide between the two types A and B is reflected in Part 3 of the standard.

Type A card As soon as a Type A smart card enters the interrogation zone of a reader and sufficient supply voltage is available, the card's microprocessor begins to operate. After the performance of some initialisation routines — if the card is a dual interface card these include checking whether the card is in contactless or contact mode — the card is put into so-called *IDLE mode*. At this point the reader can exchange data with another smart card in the interrogation zone. However, smart cards in the IDLE state may never react to the reader's data transmission to another smart card ('any command') so that an existing communication is not interrupted.

If, when the card is in IDLE mode, it receives a valid REQA command (Request-A), then an ATQA block (Answer to Request) is sent back to the reader in response (Figure 9.16). In order to ensure that data destined for another card in the interrogation field of the reader is not falsely interpreted as a REQA command, this command is made up of only 7 data bits (Figure 9.17). The ATQA block sent back, on the other hand, consists of 2 bytes and is returned in a standard frame.

After the card has responded to the REQA command it is put into the READY state. The reader has now recognised that at least one card is in the interrogation field and begins the anticollision algorithm by transmitting a SELECT command. The anticollision procedure used here is a dynamic *binary search tree algorithm*.[4] A bit-oriented frame is used for the transfer of the search criterion and the card's response, so that the transmission direction between reader and card can be reversed after a desired number of bits have been sent. The NVB (number of valid bits) parameter of the SELECT command specifies the current length of the search criterion.

The length of a single serial number is 4 bytes. If a serial number is detected by the anticollision algorithm, then the reader finally sends the full serial number (NVB = 40 h) in the SELECT command, in order to select the card in question. The card with the detected serial number confirms this command by an SAK (SELECT-Acknowledge) and is thereby put into ACTIVE state, the selected state. A peculiarity, however, is that not all cards possess a 4-byte serial number (single size). The standard also permits serial numbers of 7 bytes (double size) and even 10 bytes (triple size). If the selected card has a double or triple size serial number, this will be signalled to the reader in

[4] Knowledge of this procedure is a prerequisite at this point. A step-by-step introduction into the method of functioning can be found in Section 7.2.4.3.

WAVELYNX EX. 1008, Pg. 68
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

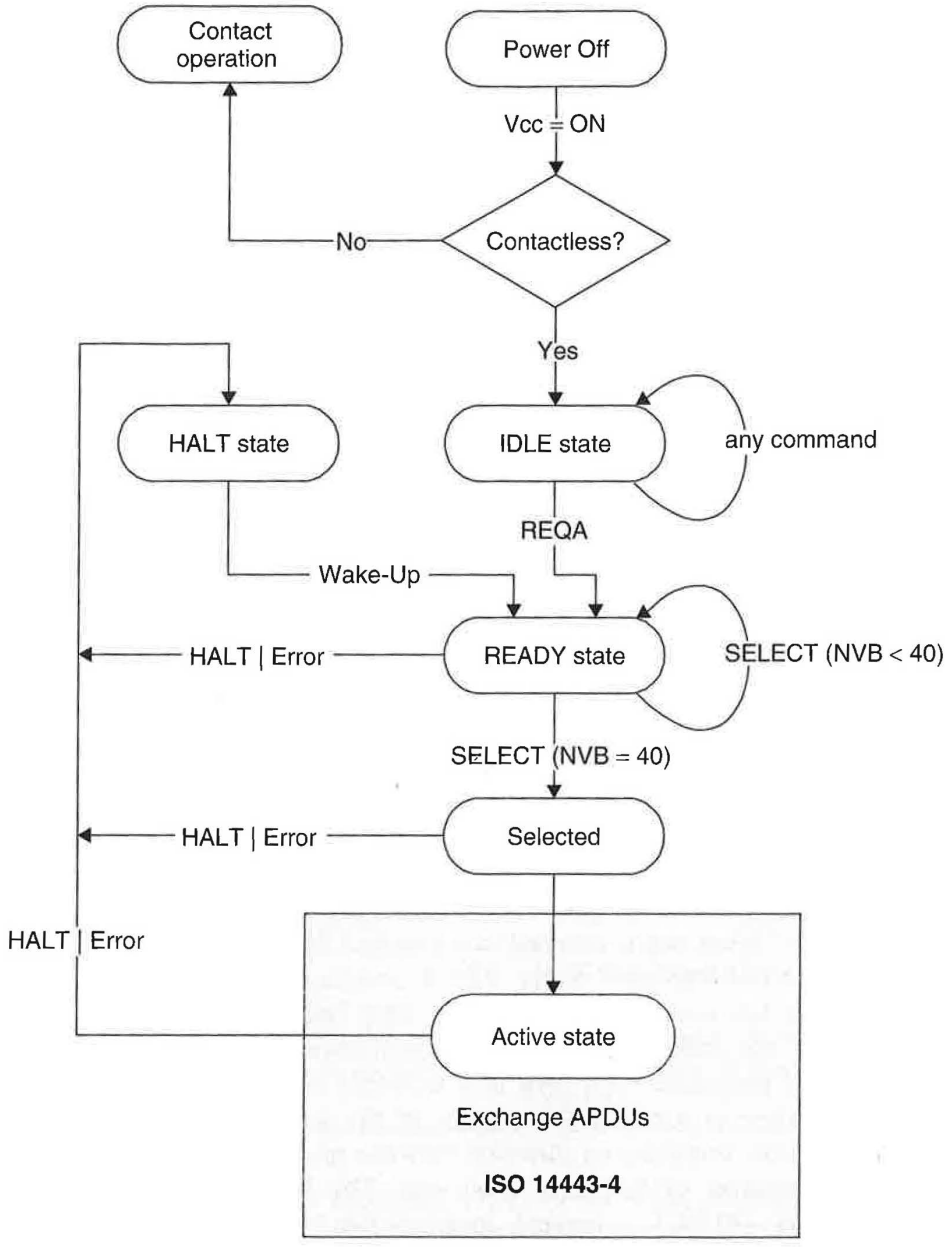


Figure 9.16 State diagram of a Type A smart card in accordance with ISO 14443 (Berger, 1998)

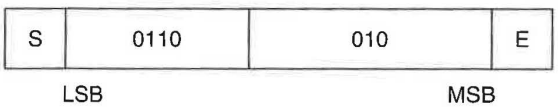


Figure 9.17 The reader's **Request command** for Type A cards (REQA) is made up of only 7 data bits. This reliably rules out the misinterpretation of useful data destined for another card as a REQUEST command (S = start of frame, E = end of frame)

WAVELYNX EX. 1008, Pg. 69
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

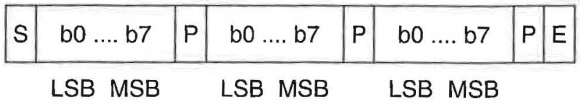


Figure 9.18 With the exception of the REQA command and data transmitted during the anti-collision routine, all data sent between reader and card (i.e. command, response and useful data) is transferred in the form of standard frames. This always begins with a start-of-frame signal (S), followed by any desired number of data bytes. Each individual data byte is protected against transmission errors by a parity bit. The data transmission is concluded by an end-of-frame signal (E)

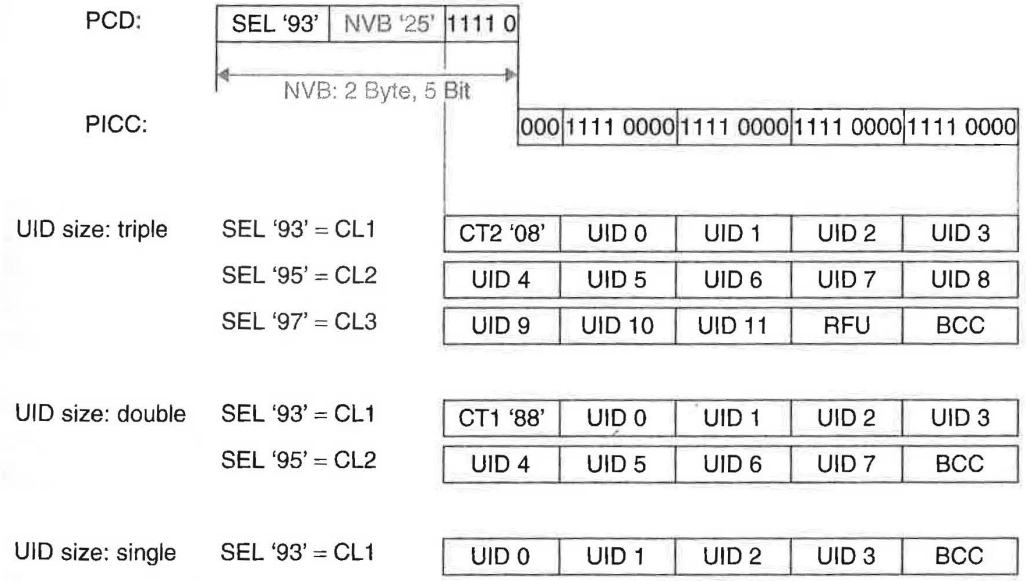


Figure 9.19 A dynamic binary search tree algorithm is used for the determination of the serial number of a card. The serial numbers can be 4, 7 or 10 bytes long, so the algorithm has to be run several times at different cascade levels (CL)

the card's SAK, by a set cascade bit (b3 = 1), with the card remaining in the READY state. This results in the anticollision algorithm being restarted in the reader so that it can detect the second part of the serial number. In a triple size serial number the anticollision algorithm must even be run a third time. To signal to the card which part of the serial number is to be detected by the algorithm that has been initiated, the SELECT command differentiates between three cascade levels (CL1, CL2, CL3) (Figure 9.19). However, the process of detecting a serial number always begins with cascade level 1. In order to rule out the possibility of fragments of a longer serial number corresponding by coincidence with a shorter serial number, so-called cascade tags (CT = 88 h) are inserted at a predetermined position in the double or triple size numbers. This value may therefore never occur at the corresponding byte positions in the shorter serial numbers.

Precise timing between a reader's command and the smart card's response should also be ensured. The standard prescribes a synchronous behaviour of the smart card,

WAVELYNX EX. 1008, Pg. 70
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

which means that the response may only be transmitted at defined moments in a fixed time grid (Table 9.9).

For the response to a REQA, WakeUp or SELECT command $N = 9$. For all other commands (e.g. application commands) N must be greater than or equal to 9 ($N = 9, 10, 11, 12, \ldots$).

Type B cards If a Type B smart card is brought within the interrogation field of a reader, the smart card, after the performance of a few initialisation routines, is initially put into IDLE mode and waits to receive a valid REQB (REQUEST-B) command (see Figure 9.20).

The transmission of a REQB command immediately initiates the anticollision algorithm in Type B cards. The procedure used here is a dynamic *slotted ALOHA procedure*,[5] in which the number of slots can be dynamically changed by the reader. The number of slots currently available is encoded in a parameter of the REQB command. In order to facilitate a preselection during the selection of a card, the REQB command has a further parameter, the Application Family Identifier (AFI), which allows a certain application group to be entered as a search criterion (Table 9.10).

After a card has received a valid *REQB command* it checks whether the application group preselected in the parameter AFI is present in the applications stored on the card. If so, the parameter M of the REQB command is evaluated to detect the number of slots available for anticollision (Table 9.11). If the number of available slots is greater than one, a random-check generator in the card is used to determine the number of the slot in which the card wishes to transmit its response to the reader. In order to guarantee the synchronisation of the cards with the slots, the reader transmits its own slot marker at the beginning of each slot. The card waits until the slot marker of the previously determined slot is received (Ready Requested State) and responds to the REQB command by sending an ATQB (Answer To Request B) See Figures 9.21 and 9.22.

A short time after the transmission of a slot marker (Figure 9.23) the reader can determine whether a smart card has begun to transmit an ATQB within the current slot. If not, the current slot can simply be interrupted by the transmission of the next slot marker in order to save time.

The request response ATQB sent by the smart card provides the reader with a range of information about important parameters of the smart card (Figure 9.22). In order to be able to select the card, the ATQB first of all contains a 4-byte serial number. In contrast to Type A cards, the serial number of a Type B card is not necessarily permanently linked to the microchip, but may even consist of a random number, which is newly determined after every Power-on reset (PUPI, pseudo unique PICC identifier).

Table 9.9 Required time grid for the transponder response during anticollision

Last received byte	Required behaviour
'1'	$t_{\text{RESPONSE}} = (n \cdot 128 + 84) \cdot t_0$
'0'	$t_{\text{RESPONSE}} = (n \cdot 128 + 20) \cdot t_0$

[5] Knowledge of this procedure is a prerequisite at this point. A step-by-step introduction into the method of functioning can be found in Section 7.2.4.2.

WAVELYNX EX. 1008, Pg. 71
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

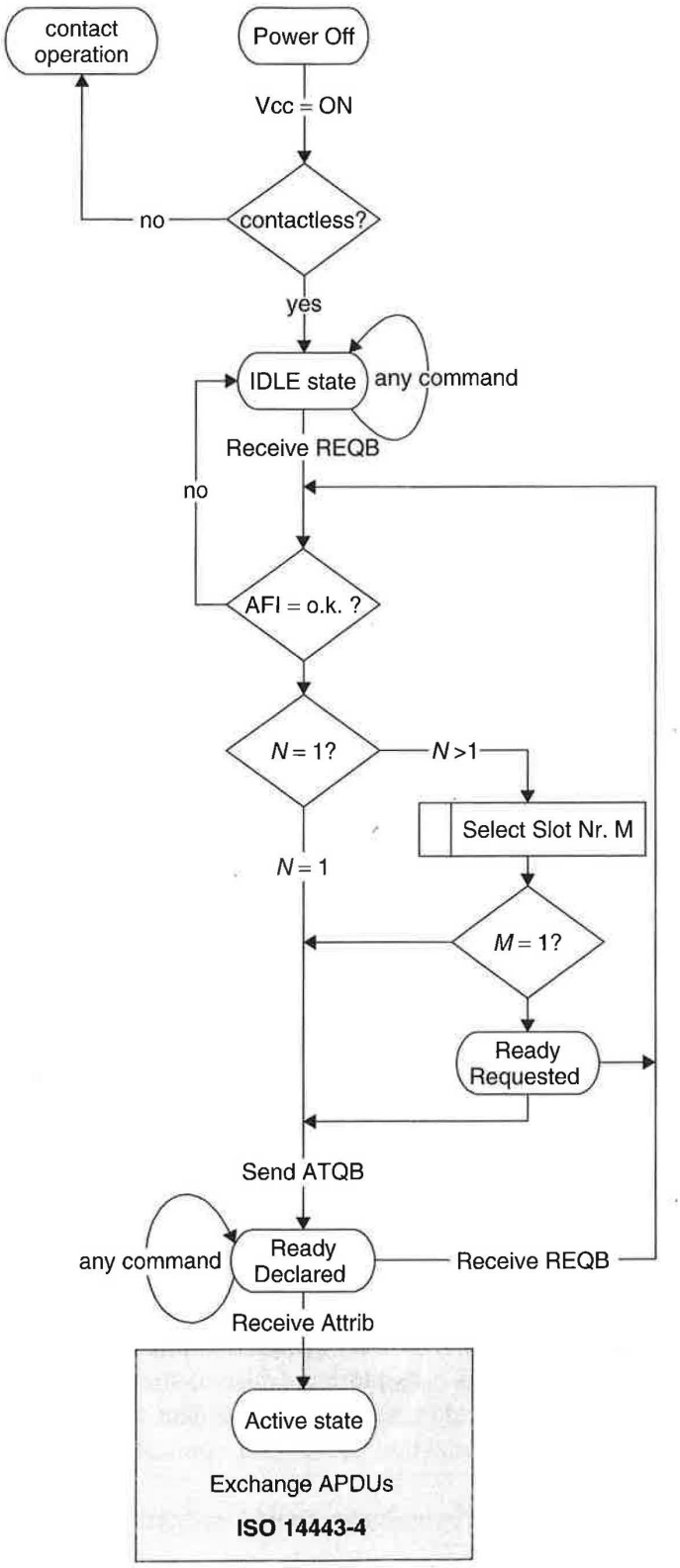


Figure 9.20 State diagram of a Type B smart card in accordance with ISO 14443

WAVELYNX EX. 1008, Pg. 72
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Table 9.10 The application family identifier (AFI) facilitates the preselection from a group of applications in the REQB command

AFI bit 7–bit 4 Application group	AFI bit 3–bit 0 Subgroup	Comment
0000	0000	All application groups and subgroups
—	0000	All subgroups of an application group
'X'	'Y'	Only subgroup Y of application group X
0001	—	Transport (local transport, airlines, ...)
0010	—	Payments (banks, tickets, ...)
0011	—	Identification (passport, driving licence)
0100	—	Telecommunication (telephone card, GSM, ...)
0101	—	Medicine (health insurance card, ...)
0110	—	Multimedia (internet service, Pay-TV)
0111	—	Games (casino card, lotto card)
1000	—	Data storage ('portable files', ...)
1001–1111	—	Reserved for future applications

Table 9.11 The number of available slots can be set by the parameter *M* in the REQB command

Para *M* byte (bit 2–bit 0)	Number of slots *N*
000	1
001	2
010	4
011	8
100	16
101	Reserved for future applications
11x	Reserved for future applications

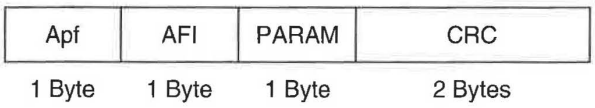


Figure 9.21 Structure of an REQB command. In order to reliably rule out errors the anticollision prefix (Apf) possess a reserved value (05h), which may not be used in the NAD parameter of a different command

Parameters of the contactless interface are encoded within the 'Protocol Info' parameter, for example the maximum possible baud rate of the smart card, the maximum frame size,[6] or information on alternative protocols. The 'Application Data' parameter can, moreover, include information on several applications available on the card (multi-application card).

[6] The maximum frame size that a card can process is determined by the size of the available reception buffer in the RAM memory of the microprocessor. Particularly in low cost applications, the size of the RAM memory can be very skimpily dimensioned.

WAVELYNX EX. 1008, Pg. 73
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

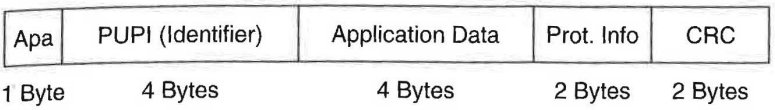


Figure 9.22 Structure of an ATQB (Answer To Request B)

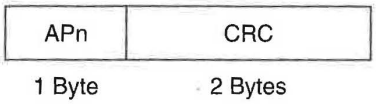


Figure 9.23 Structure of a slot marker. The sequential number of the following slot is coded in the parameter APn: APn = 'nnnn 0101b' = 'n5h'; n = slot marker 1–15

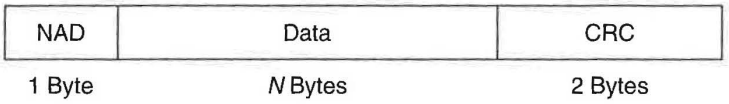


Figure 9.24 Structure of a standard frame for the transmission of application data in both directions between the reader and a Type B card. The value x5h (05h, 15h, 25h, ... E5h, F5h) of the NAD (node address) are subject to anticollision commands, in order to reliably rule out confusion with application commands

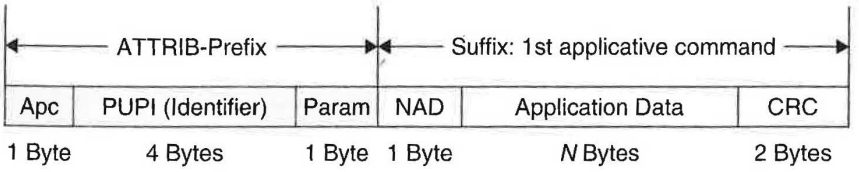


Figure 9.25 A card is selected by the sending of an application command preceded by the ATTRIB prefix, if the identifier of the card corresponds with the identifier (PUPI) of the prefix

As soon as the reader has received the ATQB of at least one smart card without errors the card can be selected. This takes place by means of the first application command transmitted by the reader. The structure of this command corresponds with that of a standard frame (Figure 9.24), but it is extended by additional information in a special prefix, the ATTRIB prefix (Figure 9.25).

The ATTRIB prefix itself is made up of the (previously determined) serial number (PUPI) of the card to be selected and a parameter byte. The parameter byte contains important information on the possible communication parameters of the reader, such as the smart card's minimum waiting time between a reader's command and the smart card's response, or the necessary waiting time between the switching on of the subcarrier system in the load modulator and the first data bit sent by the card.

9.2.2.4 Part 4 – Transmission protocols

After a communication relationship has been established between a reader and a proximity coupling smart card, commands for reading, writing and the processing of data

WAVELYNX EX. 1008, Pg. 74
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

can be sent to the card. This part of the standard describes the structure of the data protocol that this necessitates and the processing of transmission errors, so that data can be transferred between the communication participants without errors.

In the Type A card, additional information for the configuration of the protocol to different card and reader properties (e.g. possible baud rates, maximum size of the data blocks, etc.) must be transferred. In Type B cards this information has already been transferred during the anticollision process (ATQB, ATTRIB), so in the case of this card type, the protocol can be commenced immediately.

Protocol activation in Type A cards The selection of a Type A card in the anticollision loop is confirmed by the card by the transmission of a *SAK* (select acknowledge). The SAK contains information about whether a protocol in accordance with ISO 14443-4 has been implemented in this card, or whether the card has a proprietary protocol (e.g. MIFARE).

If a protocol in accordance with ISO 14443-4 is available in the card, the reader demands the card's *ATS* (answer to select) by transmitting a RATS command (request for answer to select) (Figure 9.26). The *RATS* command contains two parameters that are important for the subsequent communication: FSDI and CID.

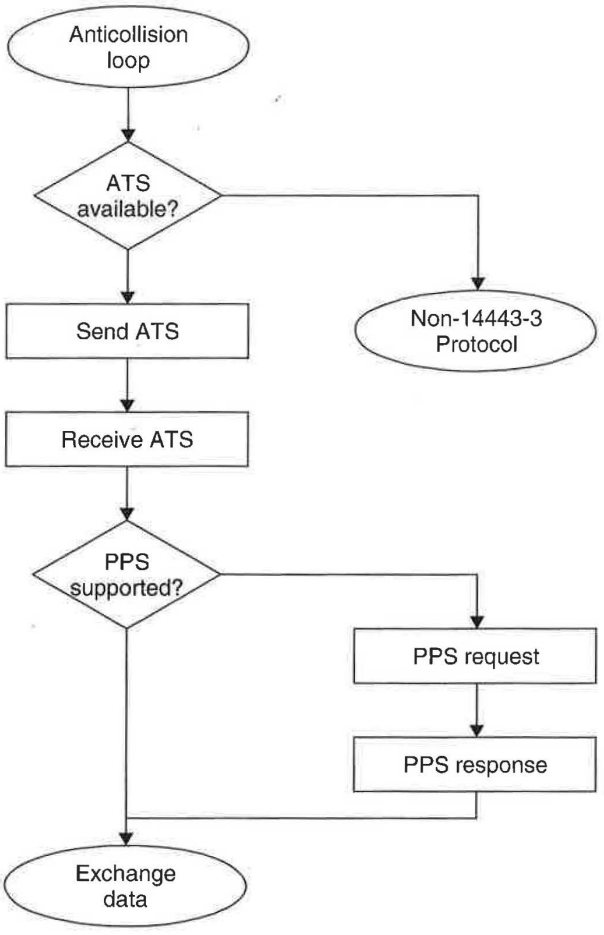


Figure 9.26 After anticollision the ATS of the card is requested

WAVELYNX EX. 1008, Pg. 75
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

FSDI (frame size device integer) defines the maximum number of bytes that may be sent from the card to the reader in one block. Possible values for this are 16, 24, 32, ... 128 and 256 bytes.

Furthermore, the smart card is allocated a CID (card identifier). Using the CID, it is possible for a reader to maintain several Type A cards in a selected state at the same time and to address an individual card selectively via its CID.

The ATS (answer to select) sent by the card in response to the RATS command corresponds with the function of the ATR (answer to reset) of a contact smart card and describes important protocol parameters of the smart card's operating system, so that the data transmission between card and reader can be optimised in relation to the properties of the implemented application.

Individually, the (optional) parameters listed in Table 9.12 can be contained in the ATS.

Immediately after receiving the ATS, the reader can still initiate the changeover of the transmission baud rates by sending out a special PPS command (protocol parameter selection). Based upon an initial baud rate of 106 Kbit/s, the baud rates in both transmission directions can be increased independently of one another by a factor of 2, 4 or 8 if the smart card has signalled the support of higher baud rates in the optional parameters DS and DR in the ATS.

Protocol The protocol described in ISO 14443-4 supports the transmission of application data (APDU = application data unit) between the reader and the smart card. The transmitted APDU can contain any desired data, such as command and response. The structure of this protocol is based heavily upon the *protocol* $T = 1$ (ISO 7816-3) that we know from contact smart cards, in order to keep the integration of this protocol

Table 9.12 The ATS describes important protocol parameters of the Type A card

Parameters	Comment
FSCI	frame size card integer: Maximum number of bytes that may be sent in a block from the reader to the card
DS	data rate send: Supported data rates of the smart card during the data transfer from the card to the reader (possible values: 106, 204, 408, 816 Kbit/s)
DR	data rate send: Supported data rates of the smart card during the data transmission from the reader to the card (possible values: 106, 204, 408, 816 Kbit/s)
FWI	frame waiting integer: This parameter defines the 'frame waiting time', i.e. the maximum time that a reader has to wait after transmitting a command for the response of the smart card. If no answer has been received from the card after the end of this time, then a 'timeout' error occurs in the communication
SFGI	startup frame guard integer: This parameter defines the 'startup frame waiting time', a special 'frame waiting time', that is valid exclusively for the performance of the first application command after the ATS
CID supported NAD supported	These parameters indicate whether the parameters CID (card identifier) and NAD (node address) are supported by the smart card's operating system
Historical bytes	The historical bytes contain additional, freely definable information on the operating system of the smart card, e.g. a version number

WAVELYNX EX. 1008, Pg. 76
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

into smart card operating systems that are already available, in particular dual interface smart cards, as simple as possible. The protocol defined in ISO 14443-4 is therefore often called $T = CL$.

The entire data transmission to an ISO 14443 card can also be represented in accordance with the *OSI layer model*, as Figure 9.27 shows. In this model, every layer independently takes on specific tasks and is thus transparent to the level above it. Layer 1, the physical layer, describes the transmission medium and the coding of the data at byte level. ISO 14443-2 provides two equivalent procedures here, Type A and Type B. Layer 2, the transport layer, controls the transmission of data between reader and smart card. Layer 2 automatically looks after the correct addressing of the data blocks (CID), the sequential transmission of excessively sized data blocks (chaining), the monitoring of the time procedure (FWT, WTX), and the handling of transmission errors. Layer 7, the application layer, contains the application data, i.e. the command to the smart card or the response to a command. In contactless smart cards the data structures used in the application layer are generally fully identical to those used in contact smart cards. This procedure is very worthwhile for dual interface smart cards in particular, because it means that the application layer is independent of the communications interface that is currently being used (contact, contactless). Layers 3 to 6 are used in complex networks for the determination and forwarding of data packets. In smart cards these layers of the OSI layer model are not used.

After the smart card has been activated (e.g. Type A after the transmission of the ATS and possibly a PPS) it waits for the first command from the reader. The sequence that now follows always corresponds with the master–slave principle, with the reader as master and the card as slave. The reader always sends a command to the smart card first, which executes the command and sends a response back to the reader. This pattern may never be broken; a smart card thus cannot initiate any communication with the reader.

The basic structure of a *data block (frame)* from the transport layer is shown in Figure 9.28. We differentiate between three types of blocks according to the method of functioning:

- *I block* (information block): Transmission of data from the application layer (APDU)
- *R block* (recovery block): Handling of transmission errors
- *S block* (supervisory block): Higher control of the protocol.

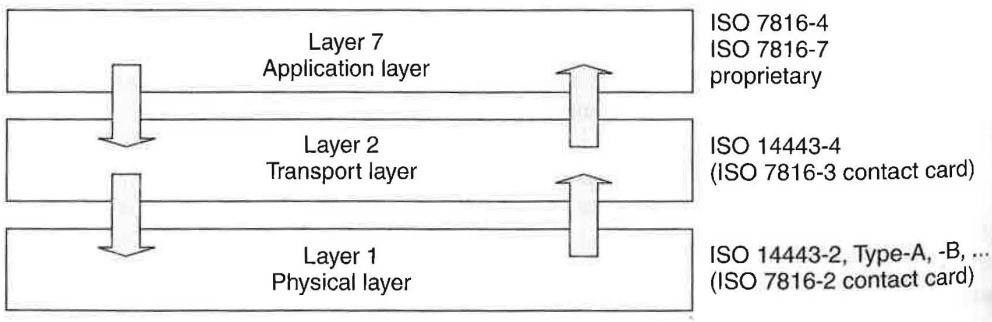


Figure 9.27 The ISO/OSI layer model in a smart card

WAVELYNX EX. 1008, Pg. 77
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

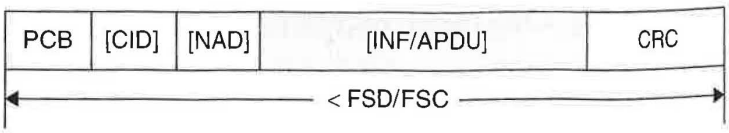


Figure 9.28 Structure of the frame in ISO 14443. The data of the application layer, Layer 7 (grey), are packed into the protocol frame of the transport layer (white)

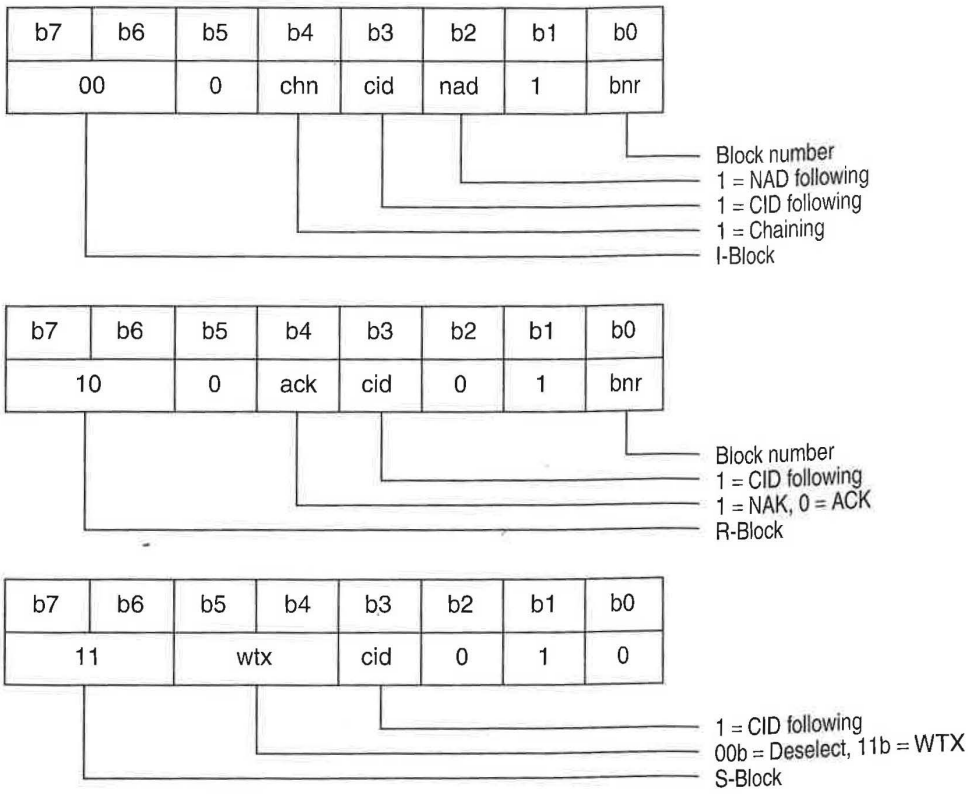


Figure 9.29 Coding of the PCB byte in a frame. The entire transmission behaviour is controlled by the PCB (protocol control byte) in the protocol

The blocks are differentiated by different coding of the PCB (protocol control byte), as shown in Figure 9.29.

The optional CID (card identifier) is used for addressing an individual smart card in the interrogation zone of the reader. Thus, several smart cards can be activated at the same time and addressed selectively using their CID. The NAD byte (node address) was introduced in order to ensure compatibility between ISO 14443-5 and ISO 7816-3 (T = 1). The use of this byte is therefore not further defined in ISO 14443.

In the case of an I block, the information field (INF) serves as a container for the data of the application layer (APDU). The content is transmitted entirely transparently. This means that the content of the protocol is forwarded directly without analysis or evaluation.

Finally, a 16-bit *CRC* is appended as an EDC (error detection code) for error control.

WAVELYNX EX. 1008, Pg. 78
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

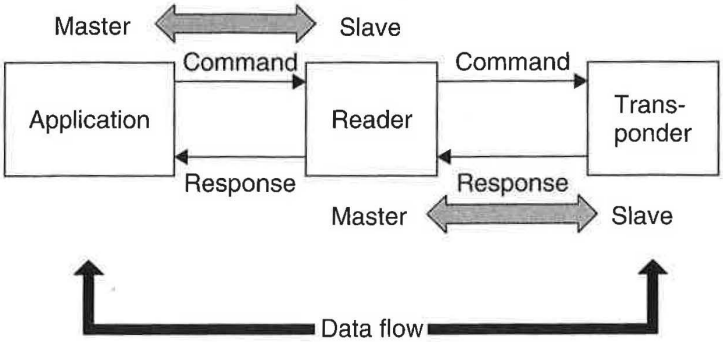


Figure 11.1 Master–slave principle between application software (application), reader and transponder

Table 11.1 Example of the execution of a read command by the application software, reader and transponder

Application ↔ reader	Reader ↔ transponder	Comment
→ Blockread_Address[00]		Read transponder memory [address]
	→ Request	Transponder in the field?
	← ATR_SNR[4712]	Transponder operates with serial number
	→ GET_Random	Initiate authentication
	← Random[081514]	
	→ SEND_Token1	
	← GET_Token2	Authentication successfully completed
	→ Read_@[00]	Read command [address]
	← Data[9876543210]	Data from transponder
← Data[9876543210]		Data to application

(inductive — electromagnetic), the communication sequence (FDX, HDX, SEQ), the data transmission procedure from the transponder to the reader (load modulation, backscatter, subharmonic) and, last but not least, the frequency range, all readers are similar in their basic operating principle and thus in their design.

Readers in all systems can be reduced to two fundamental functional blocks: the control system and the *HF interface*, consisting of a transmitter and receiver (Figure 11.2). Figure 11.3 shows a reader for an inductively coupled RFID system. On the right-hand side we can see the HF interface, which is shielded against undesired spurious emissions by a tinplate housing. The control system is located on the left-hand side of the reader and, in this case, it comprises an ASIC module and microcontroller. In order that it can be integrated into a software application, this reader has an RS232 interface to perform the data exchange between the reader (slave) and the external application software (master).

WAVELYNX EX. 1008, Pg. 79
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

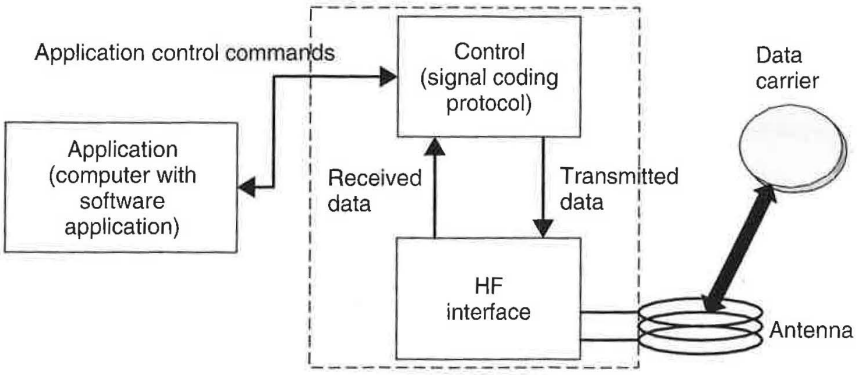


Figure 11.2 Block diagram of a reader consisting of control system and HF interface. The entire system is controlled by an external application via control commands

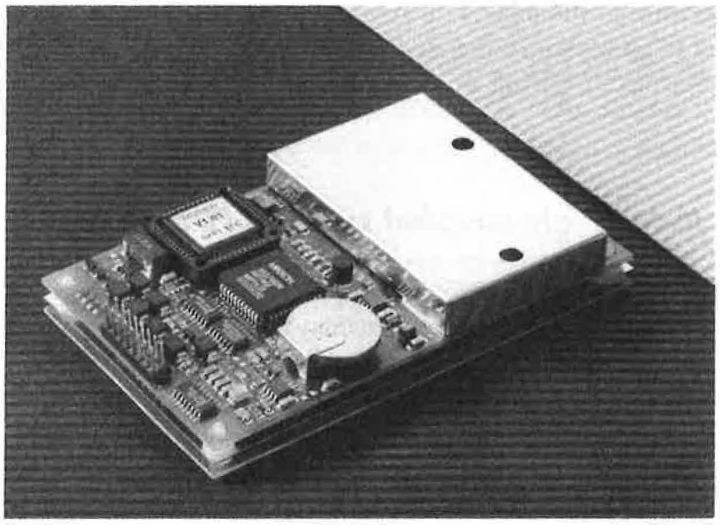


Figure 11.3 Example of a reader. The two functional blocks, HF interface and control system, can be clearly differentiated (MIFARE® reader, reproduced by permission of Philips Electronics N.V.)

11.2.1 HF interface

The reader's HF interface performs the following functions:

- generation of high frequency transmission power to activate the transponder and supply it with power;
- modulation of the transmission signal to send data to the transponder;
- reception and demodulation of HF signals transmitted by a transponder.

The HF interface contains two separate signal paths to correspond with the two directions of data flow from and to the transponder (Figure 11.4). Data transmitted to

WAVELYNX EX. 1008, Pg. 80
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

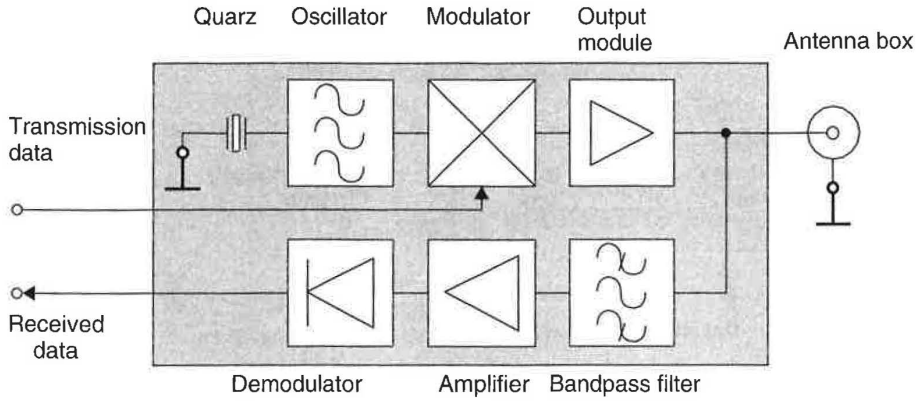


Figure 11.4 Block diagram of an HF interface for an inductively coupled RFID system

the transponder travels through the *transmitter arm*. Conversely, data received from the transponder is processed in the *receiver arm*. We will now analyse the two signal channels in more detail, giving consideration to the differences between the different systems.

11.2.1.1 Inductively coupled system, FDX/HDX

First, a signal of the required operating frequency, i.e. 135 kHz or 13.56 MHz, is generated in the transmitter arm by a stable (frequency) quartz oscillator. To avoid worsening the noise ratio in relation to the extremely weak received signal from the transponder, the *oscillator* is subject to high demands regarding phase stability and sideband noise.

The oscillator signal is fed into a modulation module controlled by the baseband signal of the signal coding system. This *baseband signal* is a keyed direct voltage signal (TTL level), in which the binary data is represented using a serial code (Manchester, Miller, NRZ). Depending upon the modulator type, *ASK* or *PSK modulation* is performed on the oscillator signal.

FSK modulation is also possible, in which case the baseband signal is fed directly into the frequency synthesiser.

The modulated signal is then brought to the required level by a power output module and can then be decoupled to the antenna box.

The *receiver arm* begins at the antenna box, with the first component being a steep edge bandpass filter or a notch filter. In FDX/HDX systems this filter has the task of largely blocking the strong signal from the transmission output module and filtering out just the response signal from the transponder. In subharmonic systems, this is a simple process, because transmission and reception frequencies are usually a whole octave apart. In systems with load modulation using a *subcarrier* the task of developing a suitable filter should not be underestimated because, in this case, the transmitted and received signals are only separated by the subcarrier frequency. Typical subcarrier frequencies in 13.56 MHz systems are 847 kHz or 212 kHz.

Some LF systems with load modulation and no subcarrier use a notch filter to increase the modulation depth (duty factor) — the ratio of the level to the load modulation sidebands — and thus the duty factor by reducing their own carrier signal.

WAVELYNX EX. 1008, Pg. 81
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

A different procedure is the rectification and thus demodulation of the (load) amplitude modulated voltage directly at the reader antenna. A sample circuit for this can be found in Section 11.3.

11.2.1.2 Microwave systems – half duplex

The main difference between *microwave systems* and low frequency inductive systems is the frequency synthesising: the operating frequency, typically 2.45 GHz, cannot be generated directly by the quartz oscillator, but is created by the multiplication (excitation of harmonics) of a lower oscillator frequency. Because the modulation is retained during frequency multiplication, modulation is performed at the lower frequency. See Figure 11.5.

Some microwave systems employ a *directional coupler* to separate the system's own transmission signal from the weak backscatter signal of the transponder (Integrated Silicon Design, 1996).

A directional coupler (Figure 11.6) consists of two continuously coupled homogeneous wires (Meinke and Gundlack, 1992). If all four ports are matched and power P_1 is supplied to port ①, then the power is divided between ports ② and ③, with no

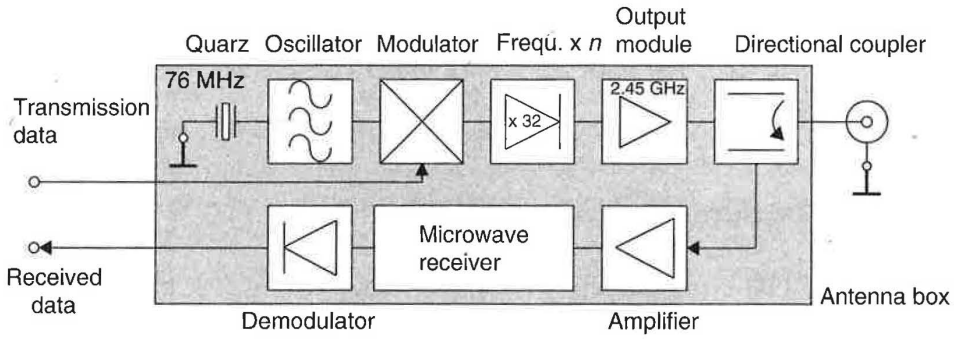


Figure 11.5 Block diagram of an HF interface for microwave systems

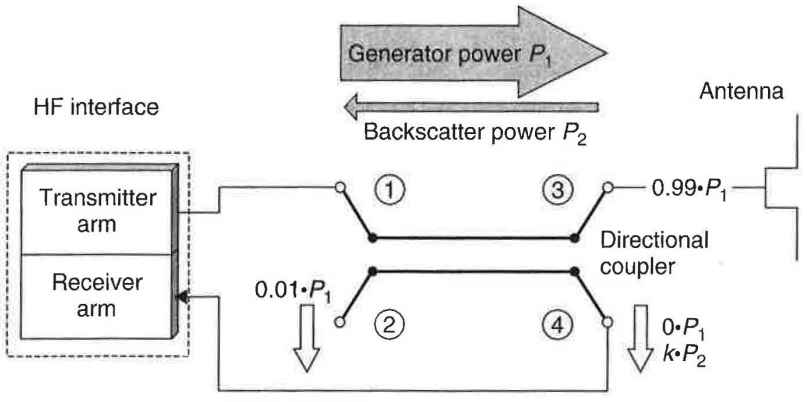


Figure 11.6 Layout and operating principle of a directional coupler for a backscatter RFID system

WAVELYNX EX. 1008, Pg. 82
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

power occurring at the decoupled port ④. The same applies if power is supplied to port ③, in which case the power is divided between ports ① and ②.

A directional coupler is described by its *coupling loss*:

$$a_k = -20 \cdot \ln |P② / P①| \tag{11.1}$$

and *directivity*:

$$a_D = -20 \cdot \ln |P④ / P②| \tag{11.2}$$

Directivity is the logarithmic magnitude of the ratio of undesired overcoupled power P_4 to desired coupled power P_2.

A directional coupler for a backscatter RFID reader should have the maximum possible directivity to minimise the decoupled signal of the transmitter arm at port ④. The coupling loss, on the other hand, should be low to decouple the maximum possible proportion of the reflected power P_2 from the transponder to the receiver arm at port ④. When a reader employing decoupling based upon a directional coupler is commissioned, it is necessary to ensure that the transmitter antenna is well (anechoically) set up. Power reflected from the antenna due to poor adjustment is decoupled at port ④ as backwards power. If the directional coupler has a good coupling loss, even a minimal mismatching of the transmitter antenna (e.g. by environmental influences) is sufficient to increase the backwards travelling power to the magnitude of the reflected transponder power. Nevertheless, the use of a directional coupler gives a significant improvement compared to the level ratios achieved with a direct connection of transmitter output module and receiver input.

11.2.1.3 Sequential systems – SEQ

In a sequential RFID system the HF field of the reader is only ever transmitted briefly to supply the transponder with power and/or send commands to the transponder.

The transponder transmits its data to the reader while the reader is not transmitting. The transmitter and receiver in the reader are thus active sequentially, like a walkie-talkie, which also transmits and receives alternately. See Figure 11.7.

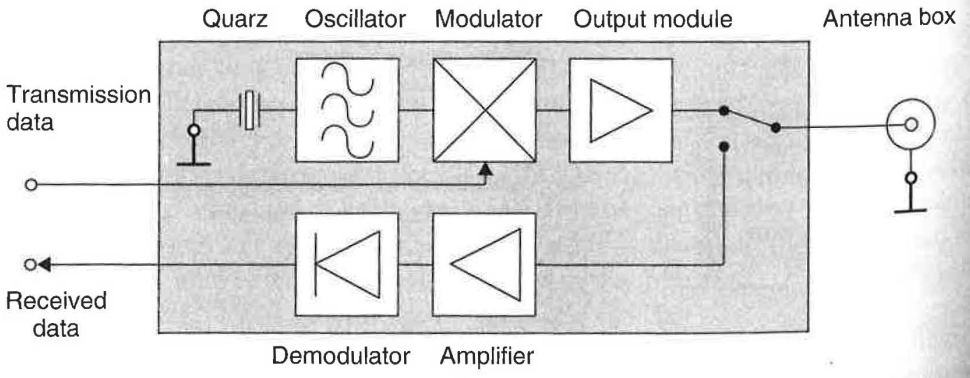


Figure 11.7 HF interface for a sequential reader system

WAVELYNX EX. 1008, Pg. 83
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

The reader contains an instantaneous switching unit to switch between transmitter and receiver mode. This function is normally performed by PIN diodes in radio technology.

No special demands are made of the receiver in an SEQ system. Because the strong signal of the transmitter is not present to cause interference during reception, the SEQ receiver can be designed to maximise sensitivity. This means that the range of the system as a whole can be increased to correspond with the *energy range*, i.e. the distance between reader and transponder at which there is just enough energy for the operation of the transponder.

11.2.1.4 Microwave system for SAW transponders

A short electromagnetic pulse transmitted by the reader's antenna is received by the antenna of the *surface wave transponder* and converted into a surface wave in a piezoelectric crystal. A characteristic arrangement of partially reflective structures in the propagation path of the surface wave gives rise to numerous pulses, which are transmitted back from the transponder's antenna as a response signal (a much more comprehensive description of this procedure can be found in Section 4.3).

Due to the propagation delay times in the piezoelectric crystal the coded signal reflected by the transponder can easily be separated in the reader from all other electromagnetic reflections from the vicinity of the reader (see Section 4.3.3). The block diagram of a reader for surface wave transponders is shown in Figure 11.8.

A stable frequency and phase oscillator with a surface wave resonator is used as the high-frequency source. Using a rapid HF switch, short HF pulses of around 80 ns duration are generated from the oscillator signal, which are amplified to around 36 dBm (4 W peak) by the connected power output stage, and transmitted by the reader's antenna.

If a SAW transponder is located in the vicinity of the reader it reflects a sequence of individual pulses after a propagation delay time of a few microseconds. The pulses

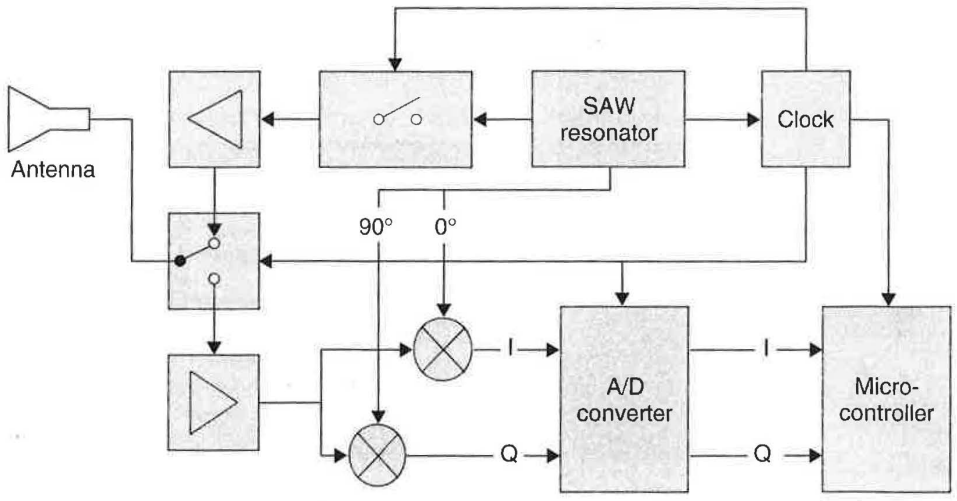


Figure 11.8 Block diagram of a reader for a surface wave transponder

WAVELYNX EX. 1008, Pg. 84
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

received by the reader's antenna pass through a low-noise amplifier and are then demodulated in a quadrature demodulator. This yields two orthogonal components (I and Q), which facilitate the determination of the phase angle between the individual pulses and between the pulses and the oscillator (Bulst *et al.*, 1998). The information obtained can be used to determine the distance or speed between SAW transponder and reader and for the measurement of physical quantities (see Section 10.4.3).

To be more precise, the reader circuit in Figure 11.8 corresponds with a *pulse radar*, like those used in flight navigation (although in this application the transmission power is much greater). In addition to the pulse radar shown here, other radar types (for example FM-CW radar) are also in development as readers for SAW transponders.

11.2.2 Control unit

The reader's control unit (Figure 11.9) performs the following functions:

- communication with the application software and the execution of commands from the application software;
- control of the communication with a transponder (master–slave principle);
- signal coding and decoding (Figure 11.10).

In more complex systems the following additional functions are available:

- execution of an anticollision algorithm;
- encryption and decryption of the data to be transferred between transponder and reader;
- performance of authentication between transponder and reader.

The control unit is usually based upon a microprocessor to perform these complex functions. Cryptological procedures, such as stream ciphering between transponder and reader, and also signal coding, are often performed in an additional ASIC module to relieve the processor of calculation intensive processes. For performance reasons the ASIC is accessed via the microprocessor bus (register orientated).

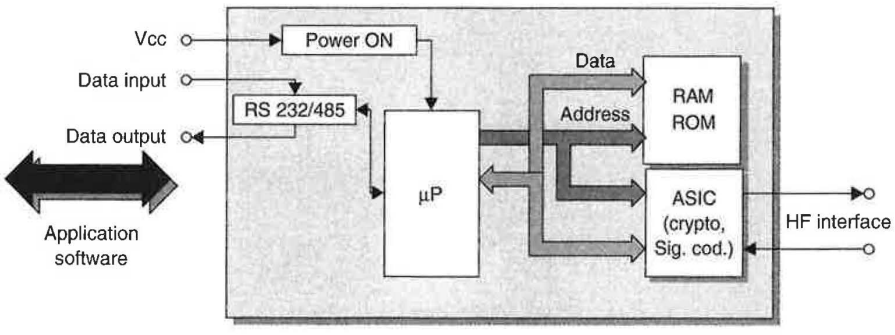


Figure 11.9 Block diagram of the control unit of a reader. There is a serial interface for communication with the higher application software

WAVELYNX EX. 1008, Pg. 85
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

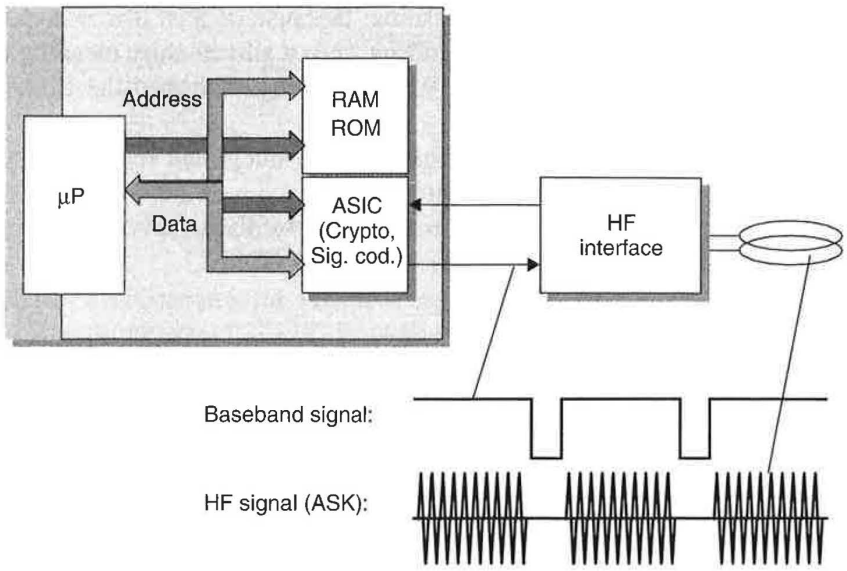


Figure 11.10 Signal coding and decoding is also performed by the control unit in the reader

Data exchange between *application software* and the reader's control unit is performed by an RS232 or RS485 interface. As is normal in the PC world, NRZ coding (8-bit asynchronous) is used. The baud rate is normally a multiple of 1200 Bd (4800 Bd, 9600 Bd, etc.). Various, often self-defined, protocols are used for the communication protocol. Please refer to the handbook provided by your system supplier.

The interface between the HF interface and the control unit represents the state of the HF interface as a binary number. In an ASK modulated system a logic '1' at the modulation input of the HF interface represents the state 'HF signal on'; a logic '0' represents the state 'HF signal off' (further information in Section 10.1.1).

11.3 Low Cost Configuration – Reader IC U2270B

It is typical of applications that use contactless identification systems that they require only a few readers, but a very large number of transponders. For example, in a public transport system, several tens of thousands of contactless smart cards are used, but only a few hundred readers are installed in vehicles. In applications such as animal identification or container identification, there is also a significant difference between the number of transponders used and the corresponding number of readers. There are also a great many different systems, because there are still no applicable standards for inductive or microwave RFID systems. As a result, readers are only ever manufactured in small batches of a few thousand.

Electronic *immobilisation* systems, on the other hand, require a vast number of readers. Because since 1995 almost all new cars have been fitted with electronic immobilisation systems as standard, the number of readers required has reached a completely new order of magnitude. Because the market for powered vehicles is also very price sensitive, cost reduction and miniaturisation by the integration of a small number of

WAVELYNX EX. 1008, Pg. 86
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

functional modules has become worth pursuing. Because of this, it is now possible to integrate the whole analogue section of a reader onto a silicon chip, meaning that only a few external components are required. We will briefly described the *U2270B* as an example of such a reader IC.

The reader IC U2270B by TEMIC serves as a fully integrated HF interface between a transponder and a microcontroller (Figure 11.11).

The IC contains the following modules: on-chip oscillator, driver, received signal conditioning and an integral power supply (Figure 11.12).

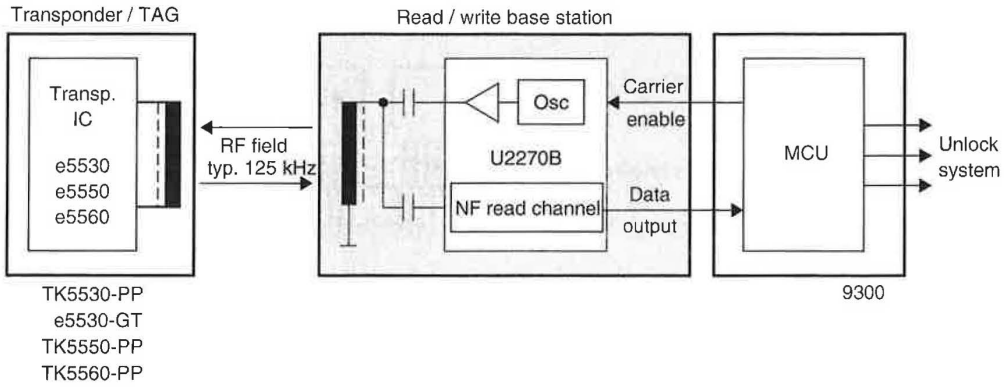


Figure 11.11 The low-cost reader IC U2270B represents a highly integrated HF interface. The control unit is realised in an external microprocessor (MCU) (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

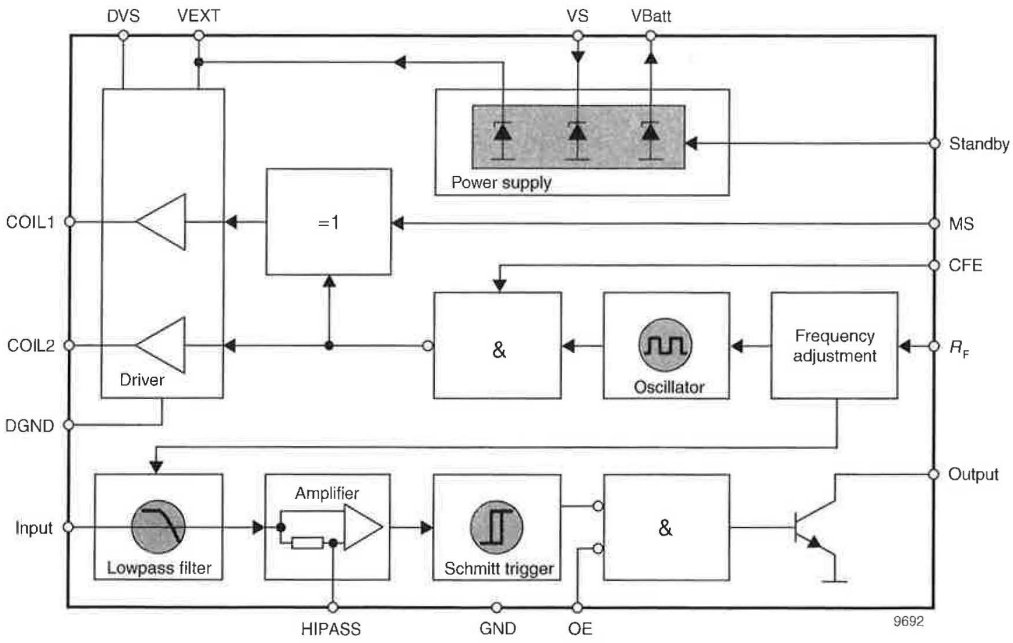


Figure 11.12 Block diagram of the reader IC U2270B. The transmitter arm consists of an oscillator and driver to supply the antenna coil. The receiver arm consists of filter, amplifier and a Schmitt trigger (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

WAVELYNX EX. 1008, Pg. 87
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

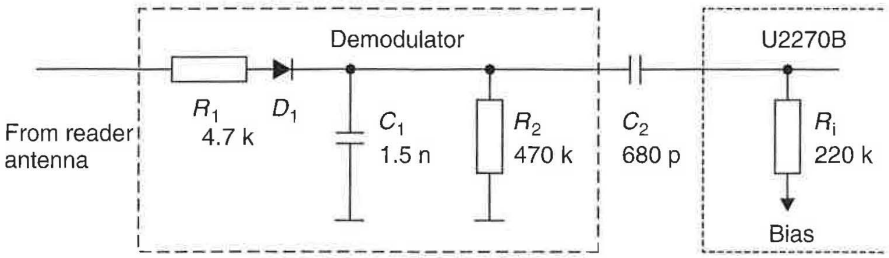


Figure 11.13 Rectification of the amplitude modulated voltage at the antenna coil of the reader (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

The on-chip oscillator generates the operating frequency in the range 100–150 kHz. The precise frequency is adjusted by an external resistor at pin R_F. The downstream driver generates the power required to control the antenna coil as push–pull output. If necessary, a baseband modulation signal can be fed into pin CFE as a TTL signal and this switches the HF signal on/off, generating an ASK modulation.

The *load modulation* procedure in the transponder generates a weak amplitude modulation of the reader's antenna voltage. The modulation in the transponder occurs in the baseband, i.e. without the use of a subcarrier. The transponder modulation signal can be reclaimed simply by demodulating the antenna voltage at the reader using a diode. The signal, which has been rectified by an external diode and smoothed using an RC low-pass filter, is fed into the 'Input' pin of the U2270B (Figure 11.13). Using a downstream Butterworth low-pass filter, an amplifier module and a Schmitt trigger, the demodulated signal is converted into a TTL signal, which can be evaluated by the downstream microprocessor. The time constants of the Butterworth filter are designed so that a Manchester or bi-phase code can be processed up to a data rate of $f_{osc}/25$ (approximately 4800 bit/s) (TEMIC, 1977).

A complete application circuit for the U2270B can be found in the following chapter.

11.4 Connection of Antennas for Inductive Systems

Reader antennas in inductively coupled RFID systems generate magnetic flux Φ, which is used for the power supply of the transponder and for sending messages between the reader and the transponder. This gives rise to three fundamental design requirements for a reader antenna:

- maximum current i_1 in the *antenna coil*, for maximum magnetic flux Φ;
- power matching so that the maximum available energy can be used for the generation of the magnetic flux;
- sufficient bandwidth for the undistorted transmission of a carrier signal modulated with data.

WAVELYNX EX. 1008, Pg. 88
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Depending upon the frequency range, different procedures can be used to connect the antenna coil to the transmitter output of the reader: direct connection of the antenna coil to the power output module using power matching or the supply of the antenna coil via coaxial cable.

11.4.1 Connection using current matching

In typical low cost readers in the frequency range below 135 kHz, the HF interface and antenna coil are mounted close together (a few centimetres apart), often on a single printed circuit board. Because the geometric dimensions of the antenna supply line and antenna are smaller than the wavelength of the generated HF current (2200 m) by powers of ten, the signals may be treated as stationary for simplification. This means that the wave characteristics of a high frequency current may be disregarded. The connection of an antenna coil is thus comparable to the connection of a loudspeaker to an NF output module from the point of view of circuitry.

The reader IC U2270B, which was described in the preceding section, can serve as an example of such a low cost reader (Figures 11.14–11.16).

Figure 11.14 shows an example of an antenna circuit. The antenna is fed by the push–pull bridge output of the reader IC. In order to maximise the current through the antenna coil, a *serial resonant circuit* is created by the serial connection of the antenna coil L_S to a capacitor C_S and a resistor R_S. Coil and capacitor are dimensioned such that the resonant frequency f_0 is as follows at the operating frequency of the reader:

$$f_0 = \frac{1}{2\pi\sqrt{L_s \cdot C_s}} \tag{11.3}$$

The coil current is then determined exclusively by the series resistor R_S.

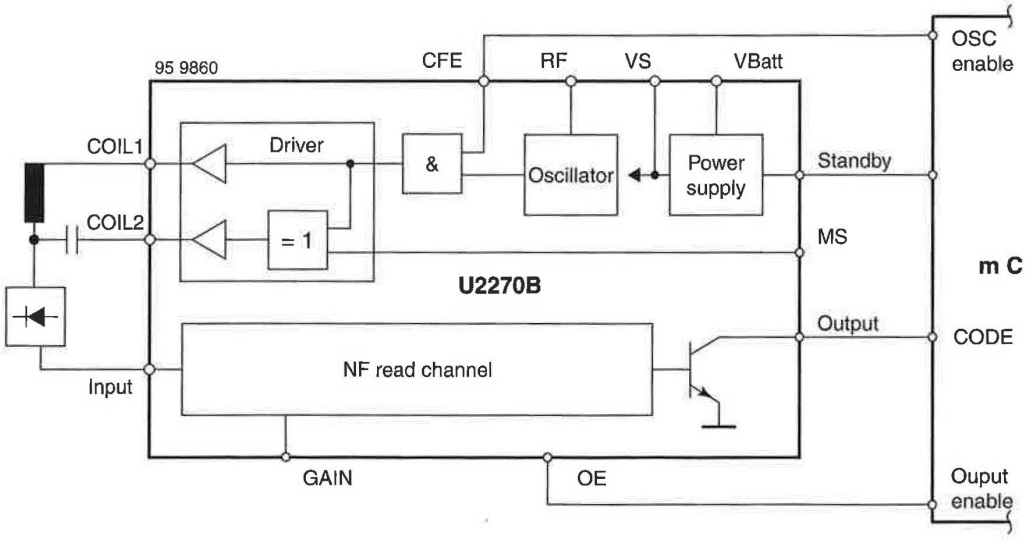


Figure 11.14 Block diagram for the reader IC U2270B with connected antenna coil at the push–pull output (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

WAVELYNX EX. 1008, Pg. 89
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

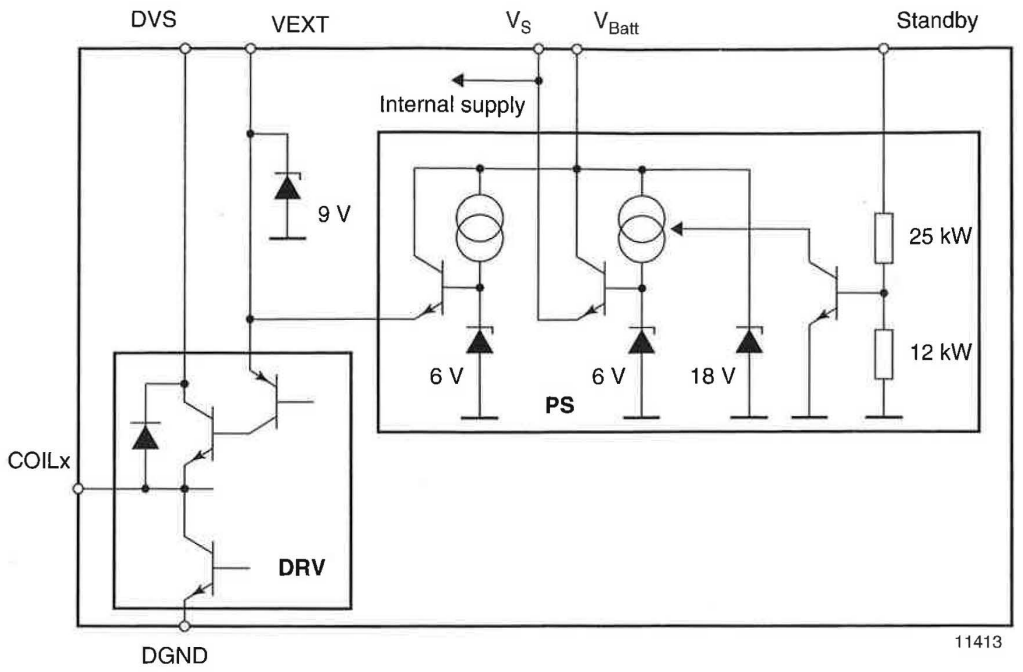


Figure 11.15 Driver circuit in the reader IC UU2270B (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

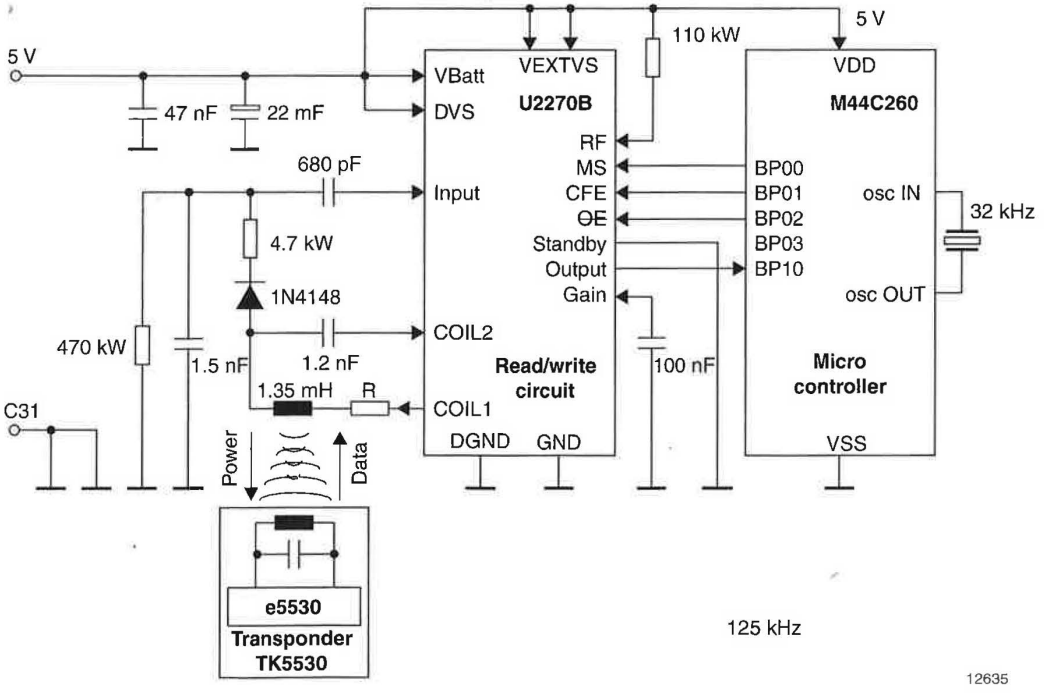


Figure 11.16 Complete example application for the low cost reader IC U2270B (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

WAVELYNX EX. 1008, Pg. 90
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

11.4.2 Supply via coaxial cable

At frequencies above 1 MHz, or in the frequency range 135 kHz if longer cables are used, the HF voltage can no longer be considered stationary, but must be treated as an *electromagnetic wave* in the cable. Connecting the antenna coil using a long, unshielded two core wire in the HF range would therefore lead to undesired effects, such as power reflections, impedance transformation and parasitic power emissions, due to the wave nature of a HF voltage. Because these effects are difficult to control when they are not exploited intentionally, shielded cable — so-called *coaxial cable* — is normally used in radio technology. Sockets, plugs and coaxial cable are uniformly designed for a cable impedance of 50 Ω and, being a mass produced product, are correspondingly cheap. RFID systems generally use 50 Ω components.

The block diagram of an inductively coupled RFID system using 50 Ω technology shows the most important HF components (Figure 11.17).

The antenna coil L_1 represents an impedance Z_L in the operating frequency range of the RFID system. To achieve power matching with the 50 Ω system, this impedance must be transformed to 50 Ω (matched) by a passive *matching circuit*. Power transmission from the reader output module to the matching circuit is achieved (almost) without losses or undesired radiation by means of a coaxial cable.

A suitable matching circuit can be realised using just a few components. The circuit illustrated in Figure 11.18, which can be constructed using just two capacitors, is very simple to design (Suckrow, 1997). This circuit is used in practice in various 13.56 MHz RFID systems.

Figure 11.19 shows a reader with an integral antenna for a 13.56 MHz system. Coaxial cable has not been used here, because a very short supply line can be realised

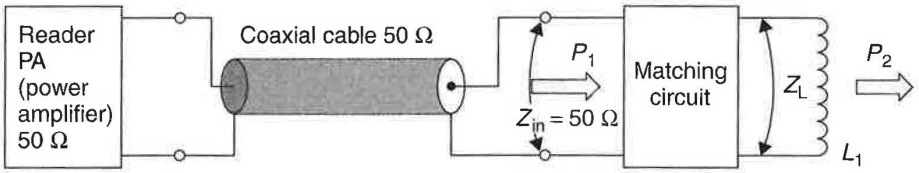


Figure 11.17 Connection of an antenna coil using 50 Ω technology

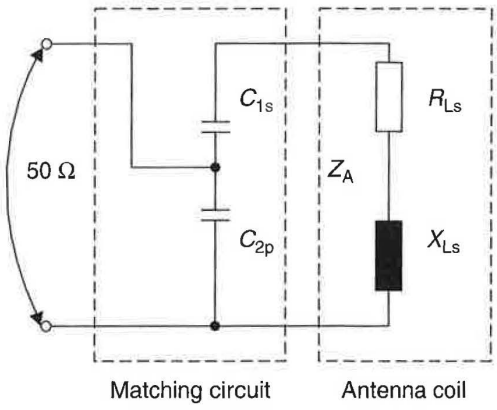


Figure 11.18 Simple matching circuit for an antenna coil

WAVELYNX EX. 1008, Pg. 91
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

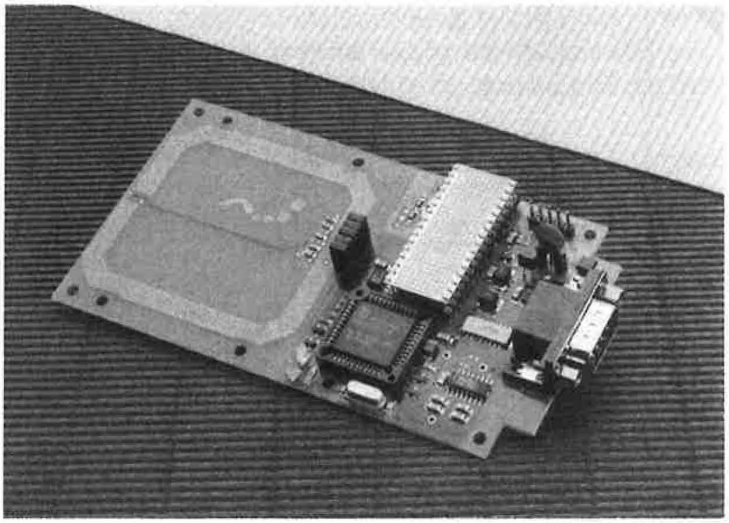


Figure 11.19 Reader with integral antenna and matching circuit (MIFARE®-reader, reproduced by permission of Philips Electronics N.V.)

by a suitable layout (stripline). The matching circuit is clearly visible on the inside of the antenna coil (SMD component).

Before we can dimension the circuit, we first need to determine the impedance Z_A of the antenna coil for the operating frequency by measurement. It is clear that the impedance of a real antenna coil is generated by the serial connection of the coil inductance L_S with the ohmic wire resistance RL_S of the wire. The serial connection from XL_S and RL_S can also be represented in the impedance level.

The function of the matching circuit is the transformation of the complex coil impedance Z_A to a value of 50 Ω real. A reactance (capacitance, inductance) in series with the coil impedance Z_A shifts the total impedance Z in the direction of the jX axis, while a parallel reactance shifts the total impedance away from the origin in a circular path (Figure 11.20).

The values of C_{2p} and C_{2s} are dimensioned such that the resulting coil impedance Z_A is transformed to the values desired to achieve 50 Ω.

The matching circuit from Figure 11.18 can be mathematically represented by equation 11.4:

$$Z_0 = 50\,\Omega = \frac{1}{-j\omega C_{2p} + \left(\dfrac{1}{\dfrac{1}{-j\omega C_{1s}} + R_{Ls} + j\omega L_s} \right)} \tag{11.4}$$

From the relationship between resistance and conductance in the complex impedance plane (Z-level), we find the following relationship for C_{2p}:

$$C_{2p} = \sqrt{\frac{Z_0 \cdot R_{Ls} - R_{Ls}^2}{\omega Z_0 R_{LS}}} \tag{11.5}$$

WAVELYNX EX. 1008, Pg. 92
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

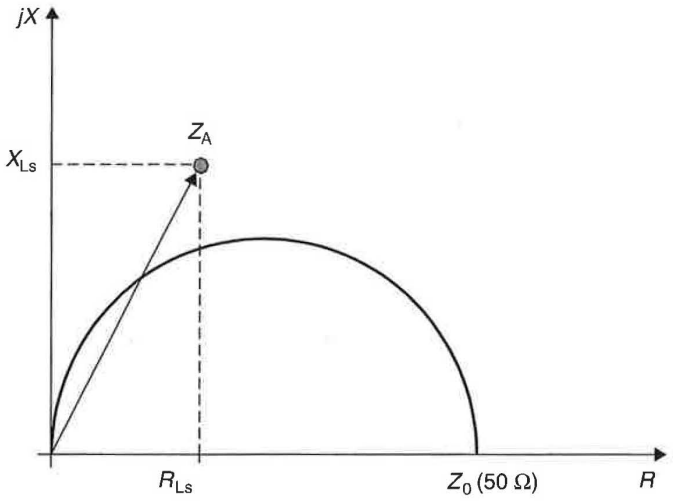


Figure 11.20 Representation of Z_A in the impedance level (Z plane)

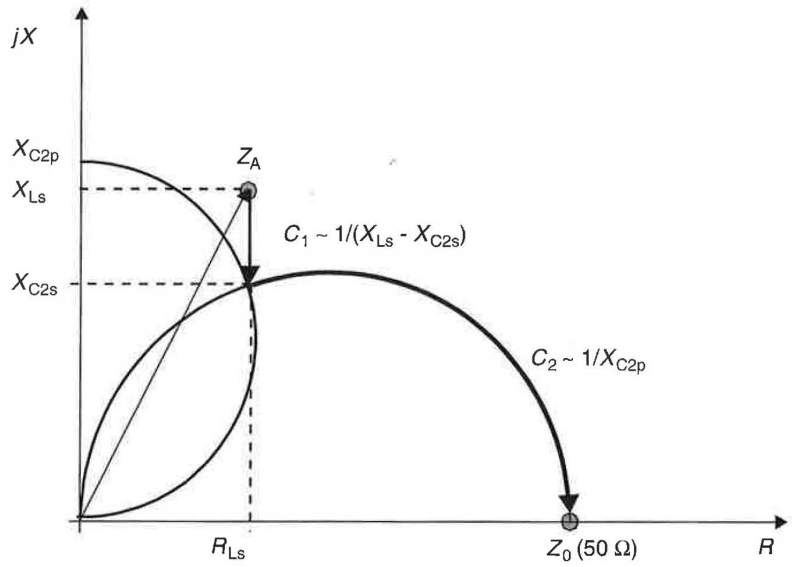


Figure 11.21 Transformation path with C_{ls} and C_{2p}

As is clear from the impedance plane in Figure 11.21, C_{2p} is determined exclusively by the serial resistance R_{ls} of the antenna coil. For a serial resistance R_{LS} of precisely 50 Ω, C_{2p} can be dispensed with altogether; however greater values for R_{ls} are not permissible, otherwise a different matching circuit should be selected (Fricke *et al.*, 1979).

We further find for C_{ls}:

$$C_{1s} = \frac{1}{\omega^2 \cdot \left(L_s - \frac{\sqrt{Z_0 R_{LS} - R_{LS}^2}}{\omega} \right)} \tag{11.6}$$

WAVELYNX EX. 1008, Pg. 93
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

The antenna current i_{LS} is of interest in this context, because this allows us to calculate the magnetic field strength H that is generated by the antenna coil (see Chapter 4).

To clarify the relationships, let us now modify the matching circuit from Figure 11.18 slightly (Figure 11.22).

The input impedance of the circuit at operating frequency is precisely 50 Ω. For this case, and only for this case(!), the voltage at the input of the matching circuit is very simple to calculate. Given a known transmitter output power P and known input impedance Z_0, the following is true: $P = U^2/Z_0$. The voltage calculated from this equation is the voltage at C_{2p} and the serial connection of C_{ls}, R_{ls} and X_{LS}, and is thus known. The antenna current i_2 can be calculated using the following equation:

$$i_2 = \frac{\sqrt{P \cdot Z_0}}{R_{Ls} + j\omega L_s - j\dfrac{1}{\omega C_{1s}}} \tag{11.7}$$

11.4.3 The influence of the Q factor

A reader antenna for an inductively coupled RFID system is characterised by its resonant frequency and by its *Q factor*. A high Q factor leads to high current in the antenna coil and thus improves the power transmission to the transponder. In contrast, the transmission bandwidth of the antenna is inversely proportional to the Q factor. A low bandwidth, caused by an excessively high Q factor, can therefore significantly reduce the modulation sideband received from the transponder.

The Q factor of an inductive reader antenna can be calculated from the ratio of the inductive coil resistance to the ohmic loss resistance and/or series resistance of the coil:

$$Q = \frac{2\pi \cdot f_0 \cdot L_{coil}}{R_{total}} \tag{11.8}$$

The bandwidth of the antenna can be simply calculated from the Q factor:

$$B = \frac{f_0}{Q} \tag{11.9}$$

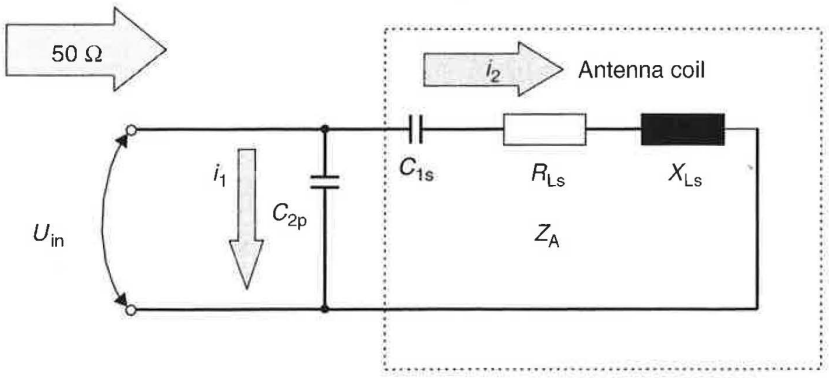


Figure 11.22 The matching circuit represented as a current divider

WAVELYNX EX. 1008, Pg. 94
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

The required bandwidth is derived from the bandwidth of the modulation sidebands of the reader and the load modulation products (if no other procedure is used). As a rule of thumb, the following can be taken as the bandwidth of an ASK modulated system.

$$B \cdot T = 1 \tag{11.10}$$

where T is the turn-on-time of the carrier signal, where modulation is used.

For many systems, the optimal Q factor is 10–30. However, it is impossible to generalise here because, as already mentioned, the Q factor depends upon the required bandwidth and thus upon the modulation procedure used (e.g. coding, modulation, subcarrier frequency).

11.5 Reader Designs

Different types and designs of readers are available for different applications. Readers can be generally classified into OEM readers, readers for industrial or portable use and numerous special designs.

11.5.1 OEM readers

OEM readers are available for integration into customers' own data capture systems, BDE terminals, access control systems, till systems, robots, etc. OEM readers are supplied in a shielded tin housing or as an unhoused board. Electrical connections are in the form of soldered, plug and socket or screw-on terminals. See Figure 11.23.

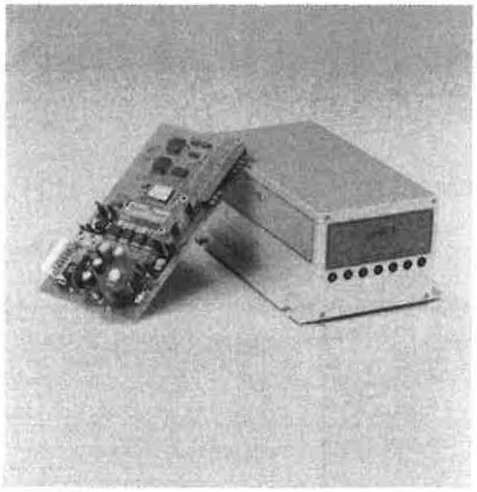


Figure 11.23 Example of an OEM reader for use in terminals or robots (photo: Long-Range/High-Speed Reader LHRI, reproduced by permission of SCEMTEC Transponder Technology GmbH, Reichshof-Wehnrath)

WAVELYNX EX. 1008, Pg. 95
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Table 11.2 Typical technical data

Supply voltage:	Typically 12 V
Antenna:	External
Antenna connection:	BNC box, terminal screw or soldered connection
Communication interface:	RS232, RS485
Communication protocol:	X-ON/X-OFF, 3964, ASCII
Environmental temperature:	0–50 °C

Table 11.3 Typical technical data

Supply voltage:	Typically 24 V
Antenna:	External
Antenna terminal:	BNC socket or terminal screw
Communication interface:	RS485, RS422
Communication protocol:	3964, InterBus-S, Profibus, etc.
Ambient temperature:	−25–+80 °C
Protection types, tests:	IP 54, IP 67, VDE

Table 11.4 Typical technical data

Supply voltage:	Typically 6 V or 9 V from batteries or accumulators
Antenna:	Internal, or as "sensor"
Antenna terminal:	—
Communication interface:	Optional RS232
Ambient temperature:	0–50 °C
Protection types, tests:	IP 54
Input/output elements	LCD display, keypad

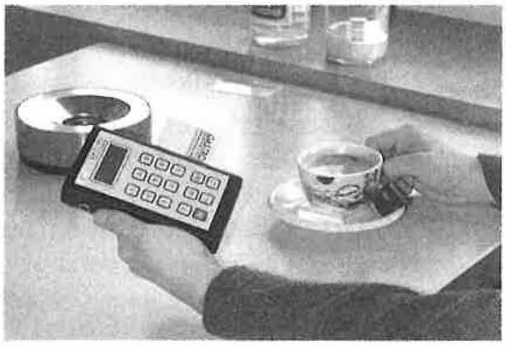


Figure 11.24 Reader for portable use in payment transactions or for service purposes. (Photo of LEGIC® reader reproduced by permission of Kaba Security Locking Systems AG, CH-Wetzikon)

11.5.2 Readers for industrial use

Industrial readers are available for use in assembly and manufacturing plant. These usually have a standardised field bus interface for simple integration into existing systems. In addition, these readers fulfil various protection types and explosion protected readers (EX) are also available.

WAVELYNX EX. 1008, Pg. 96
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

11.5.3 Portable readers

Portable readers are used for the identification of animals, as a control device in public transport, as a terminal for payments, as an aid in servicing and testing and in the commissioning of systems. Portable readers have an LCD display and a keypad for operation or entering data. An optional RS232-interface is usually provided for data exchange between the portable readers and a PC.

In addition to the extremely simple devices for system evaluation in the laboratory, particularly robust and splash-proof devices (IP 54) are available for use in harsh industrial environments.

12

The Manufacture of Transponders and Contactless Smart Cards

12.1 Glass and Plastic Transponders

A transponder is made up of two components: the electronic data carrier and the housing. Figure 12.1 gives a simplified representation of the manufacturing process for an inductively coupled transponder.

12.1.1 Module manufacture

In accordance with the normal semiconductor manufacturing procedure, the *microchip* is produced on a so-called *wafer*. This is a slice of silicon, which may be 6 inches in diameter, upon which several hundred microchips are produced simultaneously by repeated doping, exposure, etching and washing of the surface.

In the next stage of production, the microchips on the wafer are contacted using metal points and then each of the chips is individually tested for functionality. The chips have additional contact fields for this purpose, which give direct access — i.e. without going through the HF interface — to the chip's memory and security electronics. The chips are placed in so-called *test mode* during this procedure, which permits unlimited direct access to all functional groups upon the chip. The functional test can therefore be performed significantly more intensively and comprehensively than would be possible later on, when communication can only taken place via the contactless technology.

All defective chips are marked with a red ink dot at this stage, so that they can be identified and separated out in the subsequent stages of production. The test mode can also be used to programme a unique *serial number* into the chip, if the chip has an EEPROM. In read-only transponders, the serial number is programmed by cutting through predefined connecting lines on the chip using a laser beam.

After the successful completion of the test programme the test mode is deactivated by permanently breaking certain connections (so-called fuses) on the chip by a strong

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

WAVELYNX EX. 1008, Pg. 97
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

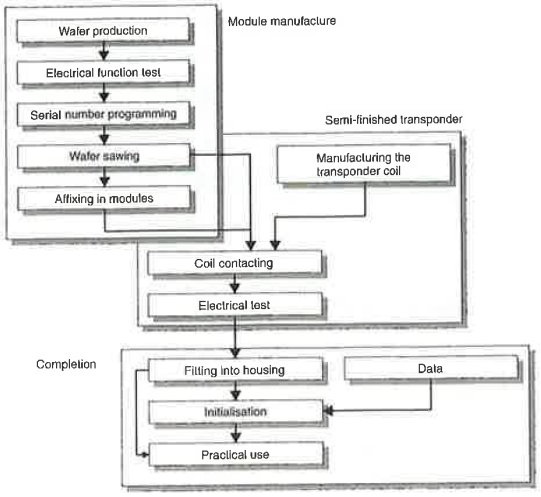


Figure 12.1 Transponder manufacture

current surge. This stage is important to prevent unauthorised reading of data at a later date by the manipulation of the test contacts on the chip.

After the chips have been tested the wafer is sawn up using a diamond saw to give individual transponder chips. A single chip in this state is known as a *die* (plural: dice). A plastic foil is attached to the reverse of the wafer prior to the sawing operation to prevent the dice from disintegrating (*saw on foil*).

After the sawing operation the dice can be removed from the plastic foil individually and fitted into a module. The connection to the contact surfaces of the module for the transponder coil is by bonding onto the reverse of the connection surfaces. Finally, the dice are extrusion coated with a moulding substance. This significantly increases the stability of the brittle and extremely breakable silicon dice. Very small dice, such as those for read-only transponders (area of die: 1–2 mm^2) are not fitted into a module for reasons of space and cost. See Figure 12.2.

12.1.2 Semi-finished transponder

In the next stage, the *transponder coil* is produced using an automatic winding machine. The copper wire used is given a coating of low-melting point *baked enamel* in addition



Figure 12.2 Size comparison of a sawn die with a cereal grain. The size of a transponder chip varies between 1 mm^2 and 15 mm^2 depending upon its function (photo: HITAG® Multimode-Chip, reproduced by permission of Philips Electronics N.V.)

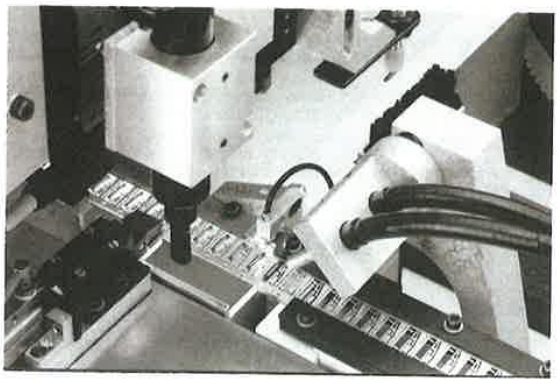


Figure 12.3 Manufacture of plastic transponders. In the figure an endless belt is fitted with transponder coils wound onto a ferrite core. After the transponder chip has been fitted and contacted, the transponder on the belt is sprayed with plastic (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)

to the normal insulating paint. The winding tool is heated to the melting point of the baked enamel during the winding operation. The enamel melts during winding and hardens rapidly when the coil has been removed from the winding tool, causing the individual windings of the transponder coil to stick together. This guarantees the mechanical stability of the transponder coil during the following stages of assembly. See Figure 12.3.

WAVELYNX EX. 1008, Pg. 98
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

Immediately after the winding of the transponder coil, the coil connections are welded to the contact surface of the transponder module using a spot welding machine. The shape and size of the transponder coil are determined by the format of the finished transponder.

In dice that are not immediately fitted into a module, the copper wire can be bonded directly to the die using a suitable procedure. However, this requires that the wire of the transponder coil is as thin as possible. For this reason, the transponder coil of a glass transponder is wound from wire that is only 30 µm thick.

Once the transponder coil has been contacted, the transponder is electrically functional. Therefore a contactless functional test is carried out at this stage to sort out those transponders that have been damaged during preceding stages. Transponders that have not yet been fitted into housings are called semi-finished transponders, as they can go from this stage into different housing formats.

12.1.3 Completion

In the next stage, the semi-finished transponder is inserted into a housing. This may take place by injection moulding (e.g. in ABS), casting, pasting up, insertion in a glass cylinder, or other procedures.

After a further functional test, the application data and/or application key can be loaded into the transponder, if required.

12.2 Contactless Smart Cards

Contactless smart cards represent a very common special type of transponder. DIN/ISO 7810 specifies the format for all ID and smart cards. The dimensions of a smart card are specified as 85.46 mm × 53.92 mm × 0.76 mm (± tolerances). The required thickness of just 0.76 mm represents a particular challenge for the manufacture of *contactless smart cards* because this places strict limits on the possible dimensions of the transponder coil and chip module.

A contactless smart card may, for example, be manufactured from four PVC foils of around 0.2 mm thickness: two *inlet foils* that are inserted in the inside of the card and two *overlay foils* that will form the outside of the card. Contactless smart cards are produced in sheets of 21, 24 or 48. The foils used thus have an area of around 0.1 to 0.3 m^2. The typical foil structure of a contactless smart card is shown in Figure 12.4. The two overlay foils are printed with the layout of the smart card. On modern printing machines a high-quality coloured print is possible, such as that familiar from telephone smart cards.

The antenna in the form of a coil is applied to one of the two inlet foils, the carrier foil, and connected to the chip module using a suitable connection technique. Four main procedures are used for the manufacture of the antenna coil: winding, embedding, screen printing and etching.

The carrier foil is covered by a second inlet foil, from which the area of the chip module has been stamped out. Often a filler is also dosed into the remaining hollow space. This filling is necessary to prevent the overlay foils applied after the lamination

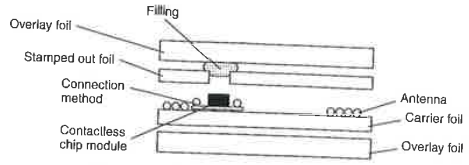


Figure 12.4 Foil structure of a contactless smart card

process (see Section 12.2.3) from collapsing around the chip module and to give a smooth and even card surface (Haghiri and Tarantino, 1999).

12.2.1 Coil manufacture

Winding In the *winding technique* the transponder coil is wound upon a winding tool in the normal way and affixed using baked enamel. After the chip module has been welded onto the antenna, the semi-finished transponder is placed on the inlet sheet and mechanically affixed using cemented joints (Figure 12.5).

For contactless smart cards in the frequency range <135 kHz the winding technique is the only procedure that can be used for the manufacture of transponder coils due to the high number of windings (typically 50–1500 windings).

Embedding Inlet manufacture using the *embedding technique* (Figures 12.6 and 12.7) is a relatively new procedure that is nevertheless increasing significantly in importance. In this technique, the chip module is first affixed in its intended location on a PVC foil. The wire is then embedded directly into the foil using a sonotrode. The *sonotrode* consists of an ultrasonic emitter with a passage in its head through which the wire is guided onto the foil. The ultrasound emitter is used to locally heat the wire to such a degree that it melts into the foil and is thus fixed in shape and position. The sonotrode is moved across the inlet foil in a similar manner to an X–Y plotter, while the wire is fed through, so that the transponder can be 'drawn' or embedded. At the start and the end of the coil a spot welding machine is used to make the electrical connection to the transponder module.

Screen printing The *screen printing technique* is a common printing technique in industrial production and is used, for example, in the production of wallpaper, (PVC) stickers, signs, and also in textile printing. A screen mesh made of synthetic or natural fibres or metal wires is stretched over a frame. The fineness of the screen mesh and the strength of the fibres are selected on the basis of the resolution of the print and the viscosity of the paint. The template is applied to the screen mesh manually or photomechanically. The actual print motif, in our case a coil, remains free. The template material may, for example, be a light-sensitive emulsion that is applied to the screen. If this coated screen is illuminated through a printing film, the emulsion hardens at the illuminated points. The points that have not been illuminated are washed out with water. Colour drawn over the screen with a rubber squeegee is pressed through these

WAVELYNX EX. 1008, Pg. 99
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730

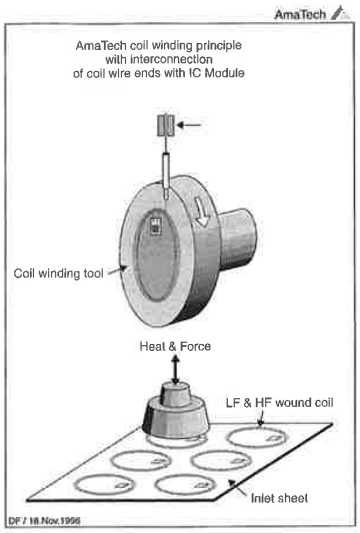


Figure 12.5 Production of a semi-finished transponder by winding and placing the semi-finished transponder on an inlet sheet (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)

open points and onto the chosen material. The screen is raised and the print is complete. All structures have a raster pattern due to the screen mesh. The elasticity of the screen guarantees extremely high accuracy.

This procedure is used to print a coil of any shape directly onto an inlet foil (Figure 12.8). So-called *polymer thick film pastes* (PTF) are used as the 'printing ink'. These consist of the powder of a conductive material (silver, copper, graphite), a light solvent, and a resin as the fixing agent. After drying out, a conductive film is left behind in the printed shape on the inlet. The *surface resistance* R_A[1] of the film is around 5–100 Ω/□[1] and falls back to around 50–80% after lamination, since the

[1] The surface resistance R_A of a quadratic conductive layer is dependent only upon the specific conductivity κ and the thickness d of the conductive layer and is quoted in Ω/□: $R_A = \frac{1}{\kappa \cdot d} = \frac{\rho}{d}$

To determine the conductive track resistance, the surface resistance is multiplied by the ratio of length l to breadth b of the conductive track: $R = R_A \cdot \frac{l}{b}$

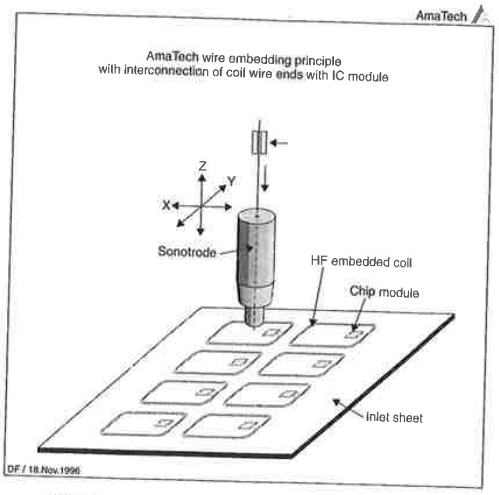


Figure 12.6 Manufacture of an inlet sheet using the embedding principle (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)

effect of heat and pressure during the lamination process increases the partial contact between the individual grains of the mixed (metal) powder.

Depending upon layer thickness, conductor track width, and number of windings, a typical coil resistance of 2–75 Ω (smart card with 2–7 windings) can be achieved. Due to the broad conductor track path (i.e. limited number of windings) this technology is, however, only suitable for frequency ranges above 8 MHz. Due to cost benefits, printed coils are also used for EAS tags (8 MHz) and Smart Labels (13.56 MHz).

Etching The *etching technique* is the standard procedure used in the electrical industry for the manufacture of printed circuit boards. Inlet foils for contactless smart cards can also be manufactured using this procedure. In a special procedure a full-sized copper foil of 35 µm to 70 µm thickness is first laminated onto a plastic foil without the use of adhesive. This copper layer is now coated with a light-sensitive photo-resist, which is dried and then illuminated through a positive film. The picture on the positive film is the subsequent form of the coil. In a chemical developing solution the illuminated points of the photo-resist are washed out, so that copper is once again exposed at these points. In the subsequent etching bath, all areas that are no longer covered by photo-resist are etched free of copper, so that finally only the desired coil form remains. The

WAVELYNX EX. 1008, Pg. 100
WaveLynx Technologies v. ASSA Abloy, IPR2023-00730