

 WILEY

# RFID HANDBOOK

Fundamentals and Applications in Contactless  
Smart Cards and Identification

Second Edition



KLAUS FINKENZELLER

# RFID Handbook

Fundamentals and Applications in Contactless Smart  
Cards and Identification

Second Edition

Klaus Finkenzeller

*Giesecke & Devrient GmbH, Munich, Germany*

Translated by

Rachel Waddington

*Member of the Institute of Translation and Interpreting*



First published under the title *RFID-Handbuch, 2 Auflage* by Carl Hanser Verlag  
© Carl Hanser Verlag, Munich/FRG, 1999 All rights reserved  
Authorized translation from the 2nd edition in the original German language  
published by Carl Hanser Verlag, Munich/FRG

Copyright © 2003      John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester,  
West Sussex PO19 8SQ, England  
Telephone (+44) 1243 779777

Email (for orders and customer service enquiries): [cs-books@wiley.co.uk](mailto:cs-books@wiley.co.uk)  
Visit our Home Page on [www.wileyeurope.com](http://www.wileyeurope.com) or [www.wiley.com](http://www.wiley.com)

Reprinted September 2003, March 2004

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher should be addressed to the Permissions Department, John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, or emailed to [permreq@wiley.co.uk](mailto:permreq@wiley.co.uk), or faxed to (+44) 1243 770620.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold on the understanding that the Publisher is not engaged in rendering professional services. If professional advice or other expert assistance is required, the services of a competent professional should be sought.

***Other Wiley Editorial Offices***

John Wiley & Sons Inc., 111 River Street, Hoboken, NJ 07030, USA

Jossey-Bass, 989 Market Street, San Francisco, CA 94103-1741, USA

Wiley-VCH Verlag GmbH, Boschstr. 12, D-69469 Weinheim, Germany

John Wiley & Sons Australia Ltd, 33 Park Road, Milton, Queensland 4064, Australia

John Wiley & Sons (Asia) Pte Ltd, 2 Clementi Loop #02-01, Jin Xing Distripark, Singapore 129809

John Wiley & Sons Canada Ltd, 22 Worcester Road, Etobicoke, Ontario, Canada M9W 1L1

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

***Library of Congress Cataloging-in-Publication Data***

Finkenzeller, Klaus.

[RFID Handbuch. English]

RFID handbook : fundamentals and applications in contactless smart cards and identification/Klaus Finkenzeller; translated by Rachel Waddington. — 2nd ed.

p. cm.

Includes bibliographical references and index.

ISBN 0-470-84402-7 (alk. paper)

1. Inventory control — Automation. 2. Radio frequency identification systems. 3. Smart cards. I. Title.

TS160.F5513 2003

658.7'87 — dc21

2002192439

***British Library Cataloguing in Publication Data***

A catalogue record for this book is available from the British Library

ISBN 0-470-84402-7

Typeset in 10/12pt Times by Laserwords Private Limited, Chennai, India

Printed and bound in Great Britain by Antony Rowe Ltd, Chippenham, Wiltshire

This book is printed on acid-free paper responsibly manufactured from sustainable forestry in which at least two trees are planted for each one used for paper production.

Verlag

ge

Gate, Chichester,

in a retrieval system or  
ying, recording, scanning or  
at 1988 or under the terms of a  
t Road, London W1T 4LP,  
blisher should be addressed to  
n Gate, Chichester, West  
to (+44) 1243 770620.

on in regard to the subject  
aged in rendering professional  
rvices of a competent

Australia  
ripark, Singapore 129809  
anada M9W 1L1  
ent that appears

rds and  
l ed.

ystems. 3. Smart.

2002192439

shire  
inable forestry  
m.

# Contents

PREFACE	xiii
LIST OF ABBREVIATIONS	xv
<b>1 Introduction</b>	<b>1</b>
1.1 Automatic Identification Systems	2
1.1.1 Barcode systems	2
1.1.2 Optical character recognition	3
1.1.3 Biometric procedures	4
1.1.3.1 Voice identification	4
1.1.3.2 Fingerprinting procedures (dactyloscopy)	4
1.1.4 Smart cards	5
1.1.4.1 Memory cards	5
1.1.4.2 Microprocessor cards	6
1.1.5 RFID systems	6
1.2 A Comparison of Different ID Systems	7
1.3 Components of an RFID System	7
<b>2 Differentiation Features of RFID Systems</b>	<b>11</b>
2.1 Fundamental Differentiation Features	11
2.2 Transponder Construction Formats	13
2.2.1 Disks and coins	13
2.2.2 Glass housing	14
2.2.3 Plastic housing	14
2.2.4 Tool and gas bottle identification	15
2.2.5 Keys and key fobs	17
2.2.6 Clocks	18
2.2.7 ID-1 format, contactless smart cards	18
2.2.8 Smart label	19
2.2.9 Coil-on-chip	20
2.2.10 Other formats	21
2.3 Frequency, Range and Coupling	22
2.4 Information Processing in the Transponder	23
2.4.1 Low-end systems	23
2.4.2 Mid-range systems	24
2.4.3 High-end systems	25
2.5 Selection Criteria for RFID Systems	25
2.5.1 Operating frequency	26
2.5.2 Range	26

2.5.3	Security requirements	27
2.5.4	Memory capacity	28
<b>3</b>	<b>Fundamental Operating Principles</b>	<b>29</b>
3.1	1-Bit Transponder	29
3.1.1	Radio frequency	30
3.1.2	Microwaves	33
3.1.3	Frequency divider	35
3.1.4	Electromagnetic types	36
3.1.5	Acoustomagnetic	37
3.2	Full and Half Duplex Procedure	40
3.2.1	Inductive coupling	41
3.2.1.1	Power supply to passive transponders	41
3.2.1.2	Data transfer transponder → reader	42
3.2.2	Electromagnetic backscatter coupling	47
3.2.2.1	Power supply to the transponder	47
3.2.2.2	Data transmission → reader	49
3.2.3	Close coupling	49
3.2.3.1	Power supply to the transponder	49
3.2.3.2	Data transfer transponder → reader	50
3.2.4	Electrical coupling	51
3.2.4.1	Power supply of passive transponders	51
3.2.4.2	Data transfer transponder → reader	53
3.2.5	Data transfer reader → transponder	53
3.3	Sequential Procedures	54
3.3.1	Inductive coupling	54
3.3.1.1	Power supply to the transponder	54
3.3.1.2	A comparison between FDX/HDX and SEQ systems	54
3.3.1.3	Data transmission transponder → reader	56
3.3.2	Surface acoustic wave transponder	57
<b>4</b>	<b>Physical Principles of RFID Systems</b>	<b>61</b>
4.1	Magnetic Field	61
4.1.1	Magnetic field strength $H$	61
4.1.1.1	Path of field strength $H(x)$ in conductor loops	62
4.1.1.2	Optimal antenna diameter	65
4.1.2	Magnetic flux and magnetic flux density	66
4.1.3	Inductance $L$	67
4.1.3.1	Inductance of a conductor loop	68
4.1.4	Mutual inductance $M$	68
4.1.5	Coupling coefficient $k$	70
4.1.6	Faraday's law	71
4.1.7	Resonance	73
4.1.8	Practical operation of the transponder	78
4.1.8.1	Power supply to the transponder	78
4.1.8.2	Voltage regulation	78

CONTENTS

27  
28  
**29**  
29  
30  
33  
35  
36  
37  
40  
41  
41  
42  
47  
47  
49  
49  
49  
50  
51  
51  
53  
53  
54  
54  
54  
54  
56  
57  
  
**61**  
61  
61  
62  
65  
66  
67  
68  
68  
70  
71  
73  
78  
78  
78

systems

ops

CONTENTS

vii

4.1.9 Interrogation field strength  $H_{\min}$  80  
 4.1.9.1 Energy range of transponder systems 82  
 4.1.9.2 Interrogation zone of readers 84  
 4.1.10 Total transponder — reader system 86  
 4.1.10.1 Transformed transponder impedance  $Z'_T$  88  
 4.1.10.2 Influencing variables of  $Z'_T$  90  
 4.1.10.3 Load modulation 97  
 4.1.11 Measurement of system parameters 103  
 4.1.11.1 Measuring the coupling coefficient  $k$  103  
 4.1.11.2 Measuring the transponder resonant frequency 105  
 4.1.12 Magnetic materials 106  
 4.1.12.1 Properties of magnetic materials and ferrite 107  
 4.1.12.2 Ferrite antennas in LF transponders 108  
 4.1.12.3 Ferrite shielding in a metallic environment 109  
 4.1.12.4 Fitting transponders in metal 110  
 4.2 Electromagnetic Waves 111  
 4.2.1 The generation of electromagnetic waves 111  
 4.2.1.1 Transition from near field to far field in conductor loops 112  
 4.2.2 Radiation density  $S$  114  
 4.2.3 Characteristic wave impedance and field strength  $E$  115  
 4.2.4 Polarisation of electromagnetic waves 116  
 4.2.4.1 Reflection of electromagnetic waves 117  
 4.2.5 Antennas 119  
 4.2.5.1 Gain and directional effect 119  
 4.2.5.2 EIRP and ERP 120  
 4.2.5.3 Input impedance 121  
 4.2.5.4 Effective aperture and scatter aperture 121  
 4.2.5.5 Effective length 124  
 4.2.5.6 Dipole antennas 125  
 4.2.5.7 Yagi-Uda antenna 127  
 4.2.5.8 Patch or microstrip antenna 128  
 4.2.5.9 Slot antennas 130  
 4.2.6 Practical operation of microwave transponders 131  
 4.2.6.1 Equivalent circuits of the transponder 131  
 4.2.6.2 Power supply of passive transponders 133  
 4.2.6.3 Power supply of active transponders 140  
 4.2.6.4 Reflection and cancellation 141  
 4.2.6.5 Sensitivity of the transponder 142  
 4.2.6.6 Modulated backscatter 143  
 4.2.6.7 Read range 145  
 4.3 Surface Waves 148  
 4.3.1 The creation of a surface wave 148  
 4.3.2 Reflection of a surface wave 150  
 4.3.3 Functional diagram of SAW transponders (Figure 4.95) 151  
 4.3.4 The sensor effect 153  
 4.3.4.1 Reflective delay lines 154  
 4.3.4.2 Resonant sensors 155

4.3.4.3	Impedance sensors	157
4.3.5	Switched sensors	159
<b>5</b>	<b>Frequency Ranges and Radio Licensing Regulations</b>	<b>161</b>
5.1	Frequency Ranges Used	161
5.1.1	Frequency range 9–135 kHz	161
5.1.2	Frequency range 6.78 MHz	163
5.1.3	Frequency range 13.56 MHz	163
5.1.4	Frequency range 27.125 MHz	163
5.1.5	Frequency range 40.680 MHz	165
5.1.6	Frequency range 433.920 MHz	165
5.1.7	Frequency range 869.0 MHz	166
5.1.8	Frequency range 915.0 MHz	166
5.1.9	Frequency range 2.45 GHz	166
5.1.10	Frequency range 5.8 GHz	166
5.1.11	Frequency range 24.125 GHz	166
5.1.12	Selection of a suitable frequency for inductively coupled RFID systems	167
5.2	European Licensing Regulations	169
5.2.1	CEPT/ERC REC 70-03	169
5.2.1.1	Annex 1: Non-specific short range devices	170
5.2.1.2	Annex 4: Railway applications	171
5.2.1.3	Annex 5: Road transport and traffic telematics	172
5.2.1.4	Annex 9: Inductive applications	172
5.2.1.5	Annex 11: RFID applications	172
5.2.1.6	Frequency range 868 MHz	173
5.2.2	EN 300 330: 9 kHz–25 MHz	173
5.2.2.1	Carrier power — limit values for H field transmitters	173
5.2.2.2	Spurious emissions	175
5.2.3	EN 300 220-1, EN 300 220-2	175
5.2.4	EN 300 440	176
5.3	National Licensing Regulations in Europe	177
5.3.1	Germany	177
5.4	National Licensing Regulations	179
5.4.1	USA	179
5.4.2	Future development: USA–Japan–Europe	180
<b>6</b>	<b>Coding and Modulation</b>	<b>183</b>
6.1	Coding in the Baseband	184
6.2	Digital Modulation Procedures	186
6.2.1	Amplitude shift keying (ASK)	186
6.2.2	2 FSK	189
6.2.3	2 PSK	190
6.2.4	Modulation procedures with subcarrier	191
<b>7</b>	<b>Data Integrity</b>	<b>195</b>
7.1	The Checksum Procedure	195

CONTENTS

	157
	159
<b>ations</b>	<b>161</b>
	161
	161
	163
	163
	163
	165
	165
	166
	166
	166
	166
	166
ipled RFID systems	167
	169
	169
as	170
	171
atics	172
	172
	172
	173
	173
ransmitters	173
	175
	175
	176
	177
	177
	179
	179
	180
	<b>183</b>
	184
	186
	186
	189
	190
	191
	<b>195</b>
	195

CONTENTS

ix

7.1.1	Parity checking	195
7.1.2	LRC procedure	196
7.1.3	CRC procedure	197
7.2	Multi-Access Procedures — Anticollision	200
7.2.1	Space division multiple access (SDMA)	202
7.2.2	Frequency domain multiple access (FDMA)	204
7.2.3	Time domain multiple access (TDMA)	205
7.2.4	Examples of anticollision procedures	206
7.2.4.1	ALOHA procedure	206
7.2.4.2	Slotted ALOHA procedure	208
7.2.4.3	Binary search algorithm	212
<b>8</b>	<b>Data Security</b>	<b>221</b>
8.1	Mutual Symmetrical Authentication	221
8.2	Authentication Using Derived Keys	223
8.3	Encrypted Data Transfer	224
8.3.1	Stream cipher	225
<b>9</b>	<b>Standardisation</b>	<b>229</b>
9.1	Animal Identification	229
9.1.1	ISO 11784 — Code structure	229
9.1.2	ISO 11785 — Technical concept	230
9.1.2.1	Requirements	230
9.1.2.2	Full/half duplex system	232
9.1.2.3	Sequential system	232
9.1.3	ISO 14223 — Advanced transponders	233
9.1.3.1	Part 1 — Air interface	233
9.1.3.2	Part 2 — Code and command structure	234
9.2	Contactless Smart Cards	236
9.2.1	ISO 10536 — Close coupling smart cards	237
9.2.1.1	Part 1 — Physical characteristics	238
9.2.1.2	Part 2 — Dimensions and locations of coupling areas	238
9.2.1.3	Part 3 — Electronic signals and reset procedures	238
9.2.1.4	Part 4 — Answer to reset and transmission protocols	239
9.2.2	ISO 14443 — Proximity coupling smart cards	240
9.2.2.1	Part 1 — Physical characteristics	240
9.2.2.2	Part 2 — Radio frequency interference	240
9.2.2.3	Part 3 — Initialisation and anticollision	245
9.2.2.4	Part 4 — Transmission protocols	251
9.2.3	ISO 15693 — Vicinity coupling smart cards	256
9.2.3.1	Part 1 — Physical characteristics	256
9.2.3.2	Part 2 — Air interface and initialisation	256
9.2.4	ISO 10373 — Test methods for smart cards	260
9.2.4.1	Part 4: Test procedures for close coupling smart cards	261
9.2.4.2	Part 6: Test procedures for proximity coupling smart cards	261
9.2.4.3	Part 7: Test procedure for vicinity coupling smart cards	264

9.3	ISO 69873 — Data Carriers for Tools and Clamping Devices	265
9.4	ISO 10374 — Container Identification	265
9.5	VDI 4470 — Anti-theft Systems for Goods	265
9.5.1	Part 1 — Detection gates — inspection guidelines for customers	265
9.5.1.1	Ascertaining the false alarm rate	266
9.5.1.2	Ascertaining the detection rate	267
9.5.1.3	Forms in VDI 4470	267
9.5.2	Part 2 — Deactivation devices, inspection guidelines for customers	268
9.6	Item Management	268
9.6.1	ISO 18000 series	268
9.6.2	GTAG initiative	269
9.6.2.1	GTAG transport layer (physical layer)	270
9.6.2.2	GTAG communication and application layer	271
<b>10</b>	<b>The Architecture of Electronic Data Carriers</b>	<b>273</b>
10.1	Transponder with Memory Function	273
10.1.1	HF interface	273
10.1.1.1	Example circuit — load modulation with subcarrier	274
10.1.1.2	Example circuit — HF interface for ISO 14443 transponder	276
10.1.2	Address and security logic	278
10.1.2.1	State machine	279
10.1.3	Memory architecture	280
10.1.3.1	Read-only transponder	280
10.1.3.2	Writable transponder	281
10.1.3.3	Transponder with cryptological function	281
10.1.3.4	Segmented memory	284
10.1.3.5	MIFARE® application directory	286
10.1.3.6	Dual port EEPROM	289
10.2	Microprocessors	292
10.2.1	Dual interface card	293
10.2.1.1	MIFARE® plus	295
10.2.1.2	Modern concepts for the dual interface card	296
10.3	Memory Technology	298
10.3.1	RAM	299
10.3.2	EEPROM	299
10.3.3	FRAM	300
10.3.4	Performance comparison FRAM — EEPROM	302
10.4	Measuring Physical Variables	302
10.4.1	Transponder with sensor functions	302
10.4.2	Measurements using microwave transponders	303
10.4.3	Sensor effect in surface wave transponders	305
<b>11</b>	<b>Readers</b>	<b>309</b>
11.1	Data Flow in an Application	309
11.2	Components of a Reader	309

CONTENTS

Devices	265
	265
	265
for customers	265
	266
	267
	267
es for customers	268
	268
	268
	269
	270
ayer	271
	<b>273</b>
	273
	273
subcarrier	274
14443 transponder	276
	278
	279
	280
	280
	281
	281
	284
	286
	289
	292
	293
	295
ard	296
	298
	299
	299
	300
	302
	302
	302
	303
	305
	<b>309</b>
	309
	309

CONTENTS

xi

11.2.1 HF interface	311
11.2.1.1 Inductively coupled system, FDX/HDX	312
11.2.1.2 Microwave systems — half duplex	313
11.2.1.3 Sequential systems — SEQ	314
11.2.1.4 Microwave system for SAW transponders	315
11.2.2 Control unit	316
11.3 Low Cost Configuration — Reader IC U2270B	317
11.4 Connection of Antennas for Inductive Systems	319
11.4.1 Connection using current matching	320
11.4.2 Supply via coaxial cable	322
11.4.3 The influence of the Q factor	325
11.5 Reader Designs	326
11.5.1 OEM readers	326
11.5.2 Readers for industrial use	327
11.5.3 Portable readers	328

**12 The Manufacture of Transponders and Contactless Smart Cards**

**329**

12.1 Glass and Plastic Transponders	329
12.1.1 Module manufacture	329
12.1.2 Semi-finished transponder	330
12.1.3 Completion	332
12.2 Contactless Smart Cards	332
12.2.1 Coil manufacture	333
12.2.2 Connection technique	336
12.2.3 Lamination	338

**13 Example Applications**

**341**

13.1 Contactless Smart Cards	341
13.2 Public Transport	342
13.2.1 The starting point	343
13.2.2 Requirements	344
13.2.2.1 Transaction time	344
13.2.2.2 Resistance to degradation, lifetime, convenience	344
13.2.3 Benefits of RFID systems	345
13.2.4 Fare systems using electronic payment	346
13.2.5 Market potential	346
13.2.6 Example projects	347
13.2.6.1 Korea — seoul	347
13.2.6.2 Germany — Lüneburg, Oldenburg	349
13.2.6.3 EU Projects — ICARE and CALYPSO	350
13.3 Ticketing	354
13.3.1 Lufthansa miles & more card	354
13.3.2 Ski tickets	356

13.4	Access Control	357
13.4.1	Online systems	357
13.4.2	Offline systems	358
13.4.3	Transponders	360
13.5	Transport Systems	361
13.5.1	Eurobalise S21	361
13.5.2	International container transport	363
13.6	Animal Identification	364
13.6.1	Stock keeping	364
13.6.2	Carrier pigeon races	367
13.7	Electronic Immobilisation	371
13.7.1	The functionality of an immobilisation system	372
13.7.2	Brief success story	375
13.7.3	Predictions	376
13.8	Container Identification	376
13.8.1	Gas bottles and chemical containers	376
13.8.2	Waste disposal	378
13.9	Sporting Events	379
13.10	Industrial Automation	381
13.10.1	Tool identification	381
13.10.2	Industrial production	385
	13.10.2.1 Benefits from the use of RFID systems	387
	13.10.2.2 The selection of a suitable RFID system	388
	13.10.2.3 Example projects	389
13.11	Medical Applications	392
<b>14</b>	<b>Appendix</b>	<b>394</b>
14.1	Contact Addresses, Associations and Technical Periodicals	394
14.1.1	Industrial associations	394
14.1.2	Technical journals	398
14.1.3	RFID on the internet	399
14.2	Relevant Standards and Regulations	400
14.2.1	Sources for standards and regulations	405
14.3	References	406
14.4	Printed Circuit Board Layouts	412
14.4.1	Test card in accordance with ISO 14443	412
14.4.2	Field generator coil	413
	<b>INDEX</b>	<b>419</b>

.3 GHz)  
93)  
(German Association of  
p Card (see ISO 15693)

gulation)

elektronics N.V.  
Security Locking

Instruments  
D systems

# 1

## Introduction

In recent years automatic identification procedures (Auto-ID) have become very popular in many service industries, purchasing and distribution logistics, industry, manufacturing companies and material flow systems. Automatic identification procedures exist to provide information about people, animals, goods and products in transit.

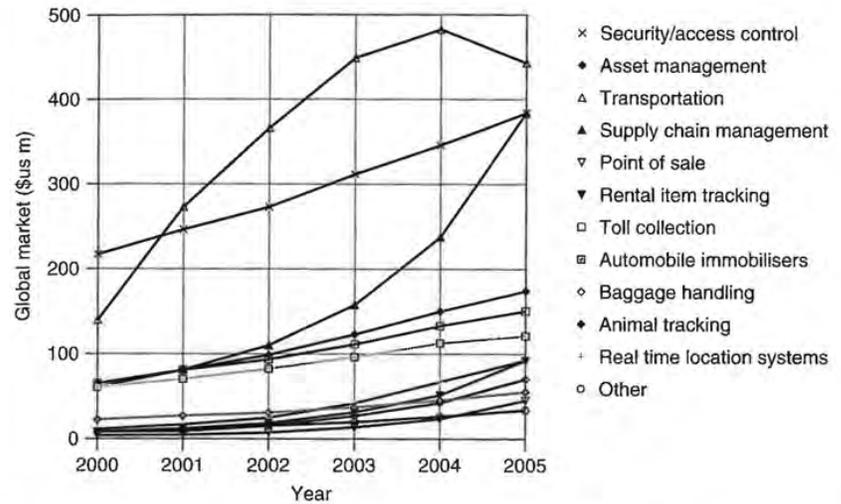
The omnipresent barcode labels that triggered a revolution in identification systems some considerable time ago, are being found to be inadequate in an increasing number of cases. Barcodes may be extremely cheap, but their stumbling block is their low storage capacity and the fact that they cannot be reprogrammed.

The technically optimal solution would be the storage of data in a silicon chip. The most common form of electronic data-carrying device in use in everyday life is the smart card based upon a contact field (telephone smart card, bank cards). However, the mechanical contact used in the smart card is often impractical. A contactless transfer of data between the data-carrying device and its reader is far more flexible. In the ideal case, the power required to operate the electronic data-carrying device would also be transferred from the reader using contactless technology. Because of the procedures used for the transfer of power and data, contactless ID systems are called *RFID systems* (Radio Frequency Identification).

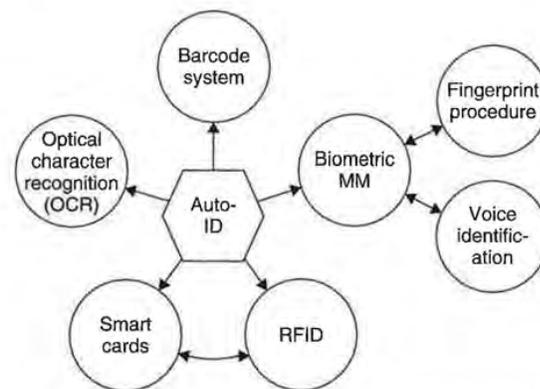
The number of companies actively involved in the development and sale of RFID systems indicates that this is a market that should be taken seriously. Whereas global sales of RFID systems were approximately 900 million \$US in the year 2000 it is estimated that this figure will reach 2650 million \$US in 2005 (Krebs, n.d.). The *RFID market* therefore belongs to the fastest growing sector of the radio technology industry, including mobile phones and cordless telephones, (Figure 1.1).

Furthermore, in recent years contactless identification has been developing into an independent interdisciplinary field, which no longer fits into any of the conventional pigeon holes. It brings together elements from extremely varied fields: HF technology and EMC, semiconductor technology, data protection and cryptography, telecommunications, manufacturing technology and many related areas.

As an introduction, the following section gives a brief overview of different automatic ID systems that perform similar functions to RFID (Figure 1.2).



**Figure 1.1** The estimated growth of the global market for RFID systems between 2000 and 2005 in million \$US, classified by application



**Figure 1.2** Overview of the most important auto-ID procedures

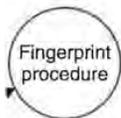
## 1.1 Automatic Identification Systems

### 1.1.1 Barcode systems

*Barcodes* have successfully held their own against other identification systems over the past 20 years. According to experts, the turnover volume for barcode systems totalled around 3 billion DM in Western Europe at the beginning of the 1990s (Virnich and Posten, 1992).

- × Security/access control
- ◆ Asset management
- ▲ Transportation
- ▲ Supply chain management
- ▼ Point of sale
- ▼ Rental item tracking
- Toll collection
- Automobile immobilisers
- ◇ Baggage handling
- ◆ Animal tracking
- Real time location systems
- Other

ID systems between 2000 and



o-ID procedures

**Items**

entification systems over the for barcode systems totalled 5 of the 1990s (Virnich and

The barcode is a binary code comprising a field of bars and gaps arranged in a parallel configuration. They are arranged according to a predetermined pattern and represent data elements that refer to an associated symbol. The sequence, made up of wide and narrow bars and gaps, can be interpreted numerically and alphanumerically. It is read by optical laser scanning, i.e. by the different reflection of a laser beam from the black bars and white gaps (*ident*, 1996). However, despite being identical in their physical design, there are considerable differences between the code layouts in the approximately ten different barcode types currently in use.

The most popular barcode by some margin is the *EAN code* (European Article Number), which was designed specifically to fulfil the requirements of the grocery industry in 1976. The EAN code represents a development of the UPC (Universal Product Code) from the USA, which was introduced in the USA as early as 1973. Today, the UPC represents a subset of the EAN code, and is therefore compatible with it (Virnich and Posten, 1992).

The EAN code is made up of 13 digits: the country identifier, the company identifier, the manufacturer's item number and a check digit (Figure 1.3).

In addition to the EAN code, the following barcodes are popular in other industrial fields (see Figure 1.4):

- Code Codabar: medical/clinical applications, fields with high safety requirements.
- Code 2/5 interleaved: automotive industry, goods storage, pallets, shipping containers and heavy industry.
- Code 39: processing industry, logistics, universities and libraries.

**1.1.2 Optical character recognition**

*Optical character recognition* (OCR) was first used in the 1960s. Special fonts were developed for this application that stylised characters so that they could be read both

Country identifier		Company identifier					Manufacturer's item number					CD
4	0	1	2	3	4	5	0	8	1	5	0	9
FRG		Company Name 1 Road Name 80001 Munich					Chocolate Rabbit 100 g					

**Figure 1.3** Example of the structure of a barcode in EAN coding

ISBN 0-471-98851-0



**Figure 1.4** This barcode is printed on the back of this book and contains the ISBN number of the book

in the normal way by people and automatically by machines. The most important advantage of OCR systems is the high density of information and the possibility of reading data visually in an emergency (or simply for checking) (Virnich and Posten, 1992).

Today, OCR is used in production, service and administrative fields, and also in banks for the registration of cheques (personal data, such as name and account number, is printed on the bottom line of a cheque in OCR type).

However, OCR systems have failed to become universally applicable because of their high price and the complicated readers that they require in comparison with other ID procedures.

### **1.1.3 Biometric procedures**

*Biometrics* is defined as the science of counting and (body) measurement procedures involving living beings. In the context of identification systems, biometry is the general term for all procedures that identify people by comparing unmistakable and individual physical characteristics. In practice, these are fingerprinting and handprinting procedures, voice identification and, less commonly, retina (or iris) identification.

#### **1.1.3.1 Voice identification**

Recently, specialised systems have become available to identify individuals using speaker verification (speaker recognition). In such systems, the user talks into a microphone linked to a computer. This equipment converts the spoken words into digital signals, which are evaluated by the identification software.

The objective of speaker verification is to check the supposed identity of the person based upon their voice. This is achieved by checking the speech characteristics of the speaker against an existing reference pattern. If they correspond, then a reaction can be initiated (e.g. 'open door').

#### **1.1.3.2 Fingerprinting procedures (dactyloscopy)**

Criminology has been using fingerprinting procedures for the identification of criminals since the early twentieth century. This process is based upon the comparison of papillae and dermal ridges of the fingertips, which can be obtained not only from the finger itself, but also from objects that the individual in question has touched.

When fingerprinting procedures are used for personal identification, usually for entrance procedures, the fingertip is placed upon a special reader. The system calculates a data record from the pattern it has read and compares this with a stored reference pattern. Modern fingerprint ID systems require less than half a second to recognise and check a fingerprint. In order to prevent violent frauds, fingerprint ID systems have even been developed that can detect whether the finger placed on the reader is that of a living person (Schmidhäusler, 1995).

chines. The most important in and the possibility of read- (Virnich and Posten, 1992). istrative fields, and also in s name and account number,

rsally applicable because of ire in comparison with other

ly) measurement procedures ems, biometry is the general unmistakable and individual ng and handprinting proce- iris) identification.

identify individuals using , the user talks into a micro- > spoken words into digital

posed identity of the person speech characteristics of the espond, then a reaction can

### oscopy)

ie identification of criminals 1 the comparison of papillae d not only from the finger has touched.

l identification, usually for ader. The system calculates his with a stored reference half a second to recognise fingerprint ID systems have ced on the reader is that of

## 1.1.4 Smart cards

A *smart card* is an electronic data storage system, possibly with additional computing capacity (microprocessor card), which — for convenience — is incorporated into a plastic card the size of a credit card. The first smart cards in the form of prepaid telephone smart cards were launched in 1984. Smart cards are placed in a reader, which makes a galvanic connection to the contact surfaces of the smart card using contact springs. The smart card is supplied with energy and a clock pulse from the reader via the contact surfaces. Data transfer between the reader and the card takes place using a bidirectional serial interface (I/O port). It is possible to differentiate between two basic types of smart card based upon their internal functionality: the memory card and the microprocessor card.

One of the primary advantages of the smart card is the fact that the data stored on it can be protected against undesired (read) access and manipulation. Smart cards make all services that relate to information or financial transactions simpler, safer and cheaper. For this reason, 200 million smart cards were issued worldwide in 1992. In 1995 this figure had risen to 600 million, of which 500 million were memory cards and 100 million were microprocessor cards. The *smart card market* therefore represents one of the fastest growing subsectors of the microelectronics industry.

One disadvantage of contact-based smart cards is the vulnerability of the contacts to wear, corrosion and dirt. Readers that are used frequently are expensive to maintain due to their tendency to malfunction. In addition, readers that are accessible to the public (telephone boxes) cannot be protected against vandalism.

### 1.1.4.1 Memory cards

In *memory cards* the memory — usually an EEPROM — is accessed using a sequential logic (state machine) (Figure 1.5). It is also possible to incorporate simple security algorithms, e.g. stream ciphering, using this system. The functionality of the memory card in question is usually optimised for a specific application. Flexibility of application is highly limited but, on the positive side, memory cards are very cost effective. For this reason, memory cards are predominantly used in price sensitive, large-scale

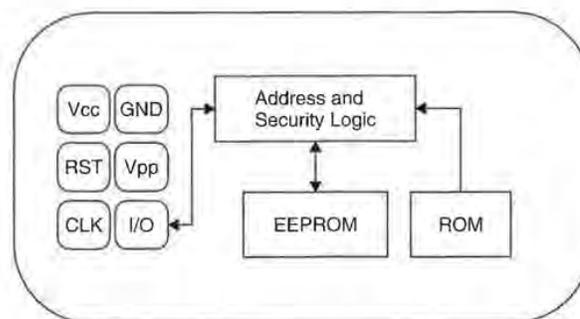


Figure 1.5 Typical architecture of a memory card with security logic

applications (Rankl and Effing, 1996). One example of this is the national insurance card used by the state pension system in Germany (Lemme, 1993).

#### 1.1.4.2 Microprocessor cards

As the name suggests, *microprocessor cards* contain a microprocessor, which is connected to a segmented memory (ROM, RAM and EEPROM segments).

The mask programmed ROM incorporates an *operating system* (higher programme code) for the microprocessor and is inserted during chip manufacture. The contents of the ROM are determined during manufacturing, are identical for all microchips from the same production batch, and cannot be overwritten.

The chip's EEPROM contains application data and application-related programme code. Reading from or writing to this memory area is controlled by the operating system.

The RAM is the microprocessor's temporary working memory. Data stored in the RAM are lost when the supply voltage is disconnected (Figure 1.6).

Microprocessor cards are very flexible. In modern smart card systems it is also possible to integrate different applications in a single card (multi-application). The application-specific parts of the programme are not loaded into the EEPROM until after manufacture and can be initiated via the operating system.

Microprocessor cards are primarily used in security sensitive applications. Examples are smart cards for GSM mobile phones and the new EC (electronic cash) cards. The option of programming the microprocessor cards also facilitates rapid adaptation to new applications (Rankl and Effing, 1996).

#### 1.1.5 RFID systems

RFID systems are closely related to the smart cards described above. Like smart card systems, data is stored on an electronic data-carrying device — the transponder. However, unlike the smart card, the power supply to the data-carrying device and the data exchange between the data-carrying device and the reader are achieved without the use of galvanic contacts, using instead magnetic or electromagnetic fields. The

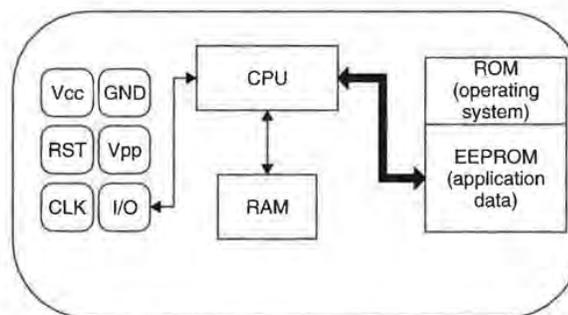


Figure 1.6 Typical architecture of a microprocessor card

his is the national insurance  
ie, 1993).

icroprocessor, which is con-  
M segments).

z system (higher programme  
manufacture. The contents of  
ical for all microchips from

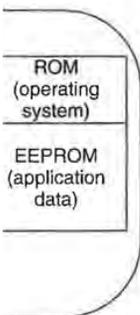
plication-related programme  
controlled by the operating

memory. Data stored in the  
figure 1.6).

mart card systems it is also  
ard (multi-application). The  
led into the EEPROM until  
system.

sitive applications. Examples  
(electronic cash) cards. The  
icilitates rapid adaptation to

ibed above. Like smart card  
ce — the transponder. How-  
ata-carrying device and the  
e reader are achieved with-  
electromagnetic fields. The



rocessor card

underlying technical procedure is drawn from the fields of radio and radar engineering. The abbreviation RFID stands for radio frequency identification, i.e. information carried by radio waves. Due to the numerous advantages of RFID systems compared with other identification systems, RFID systems are now beginning to conquer new mass markets. One example is the use of contactless smart cards as tickets for short-distance public transport.

## 1.2 A Comparison of Different ID Systems

A comparison between the identification systems described above highlights the strengths and weakness of RFID in relation to other systems (Table 1.1). Here too, there is a close relationship between contact-based smart cards and RFID systems; however, the latter circumvents all the disadvantages related to faulty contacting (sabotage, dirt, unidirectional insertion, time consuming insertion, etc.).

## 1.3 Components of an RFID System

An *RFID system* is always made up of two components (Figure 1.7):

- the *transponder*, which is located on the object to be identified;
- the interrogator or *reader*, which, depending upon the design and the technology used, may be a read or write/read device (in this book — in accordance with normal colloquial usage — the data capture device is always referred to as the *reader*, regardless of whether it can only read data or is also capable of writing).

A practical example is shown in Figure 1.8.

A reader typically contains a radio frequency module (transmitter and receiver), a control unit and a coupling element to the transponder. In addition, many readers are fitted with an additional interface (RS 232, RS 485, etc.) to enable them to forward the data received to another system (PC, robot control system, etc.).

The transponder, which represents the actual *data-carrying device* of an RFID system, normally consists of a *coupling element* and an electronic *microchip* (Figure 1.9).

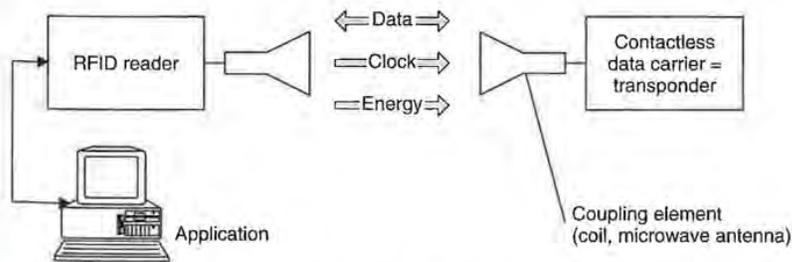


Figure 1.7 The reader and transponder are the main components of every RFID system

Table 1.1 Comparison of different RFID systems showing their advantages and disadvantages

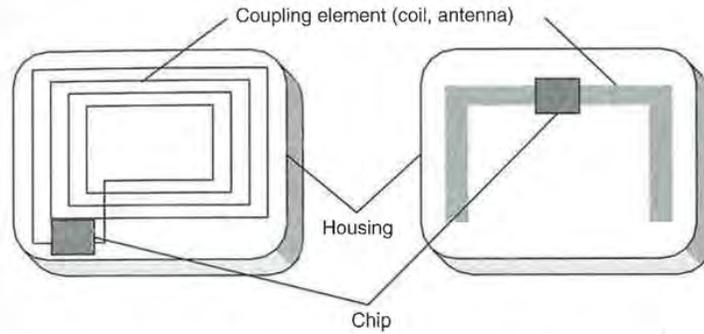
System parameters	Barcode	OCR	Voice recog.	Biometry	Smart card	RFID systems
Typical data quantity (bytes)	1-100	1-100	—	—	16-64 k	16-64 k
Data density	Low	Low	High	High	Very high	Very high
Machine readability	Good	Good	Expensive	Expensive	Good	Good
Readability by people	Limited	Simple	Simple	Difficult	Impossible	Impossible
Influence of dirt/damp	Very high	Very high	—	—	Possible (contacts)	No influence
Influence of (opt.) covering	Total failure	Total failure	—	Possible	—	No influence
Influence of direction and position	Low	Low	—	—	Unidirectional	No influence
Degradation/wear	Limited	Limited	—	—	Contacts	No influence
Purchase cost/reading electronics	Very low	Medium	Very high	Very high	Low	Medium
Operating costs (e.g. printer)	Low	Low	None	None	Medium (contacts)	None
Unauthorised copying/modification	Slight	Slight	Possible* (audio tape)	Impossible	Impossible	Impossible
Reading speed (including handling of data carrier)	Low	Low	Very low	Very low	Low	Very fast
Maximum distance between data carrier and reader	~4 s 0-50 cm	~3 s <1 cm Scanner	>5 s 0-50 cm	>5-10 s Direct contact**	~4 s Direct contact	~0.5 s 0-5-m, microwave

\*The danger of 'Replay' can be reduced by selecting the text to be spoken using a random generator, because the text that must be spoken is not known in advance.

\*\*This only applies for fingerprint ID. In the case of retina or iris evaluation direct contact is not necessary or possible.



**Figure 1.8** RFID reader and contactless smart card in practical use (reproduced by permission of Kaba Benzing GmbH)



**Figure 1.9** Basic layout of the RFID data-carrying device, the transponder. Left, inductively coupled transponder with antenna coil; right, microwave transponder with dipolar antenna

When the transponder, which does not usually possess its own voltage supply (battery), is not within the interrogation zone of a reader it is totally passive. The transponder is only activated when it is within the interrogation zone of a reader. The power required to activate the transponder is supplied to the transponder through the coupling unit (contactless), as are the timing pulse and data.

Reading speed (including handling of data carrier)	Low ~4 s	Very low >5 s	Very low >5-10 s	Low ~4 s	Very fast ~0,5 s
Maximum distance between data carrier and reader	Low ~4 s 0-50 cm	Very low >5 s 0-50 cm	Very low >5-10 s Direct contact**	Low ~4 s Direct contact	Very fast ~0,5 s 0-5-m, microwave

\*The danger of 'Replay' can be reduced by selecting the text to be spoken using a random generator, because the text that must be spoken is not known in advance.  
\*\*This only applies for fingerprint ID. In the case of retina or iris evaluation direct contact is not necessary or possible.

# 7

## Data Integrity

### 7.1 The Checksum Procedure

When transmitting data using contactless technology it is very likely that interference will be encountered, causing undesired changes to the transmitted data and thus leading to transmission errors (Figure 7.1).

A *checksum* can be used to recognise transmission errors and initiate corrective measures, for example the retransmission of the erroneous data blocks. The most common checksum procedures are parity checks, XOR sum and CRC.

#### 7.1.1 Parity checking

The *parity check* is a very simple and therefore a very popular checksum procedure. In this procedure a *parity bit* is incorporated into each byte and transmitted with it with the result that 9 bits are sent for every byte. Before data transfer takes place a decision needs to be made as to whether to check for odd or even parity, to ensure that the sender and receiver both check according to the same method.

The value of the parity bit is set such that if odd parity is used an odd number of the nine bits have the value 1 and if even parity is used an even number of bits have the value 1. The even parity bit can also be interpreted as the horizontal checksum (modulo 2) of the data bit. This horizontal checksum also permits the calculation of the exclusive OR logic gating (XOR logic gating) of the data bits.

However, the simplicity of this method is balanced by its poor error recognition (Pein, 1996). An odd number of inverted bits (1, 3, 5, ...) will always be detected, but if there is an even number of inverted bits (2, 4, 6, ...) the errors cancel each other out and the parity bit will appear to be correct.

#### **Example**

Using odd parity the number E5h has the binary representation 1110 0101  $p = 0$ .

A parity generator for even parity can be realised by the XOR logic gating of all the data bits in a byte (Tietze and Schenk, 1985). The order in which the XOR operations

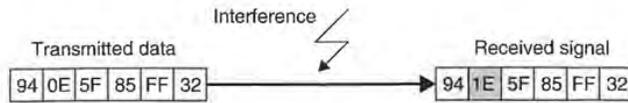


Figure 7.1 Interference during transmission can lead to errors in the data

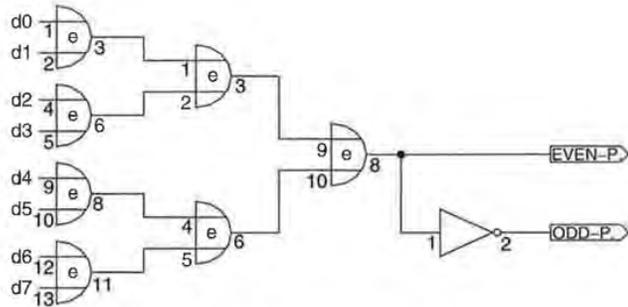


Figure 7.2 The parity of a byte can be determined by performing multiple exclusive-OR logic gating operations on the individual bits

take place is irrelevant. In the case of odd parity, the parity generator output is inverted (Figure 7.2).

### 7.1.2 LRC procedure

The XOR checksum known as the *longitudinal redundancy check (LRC)* can be calculated very simply and quickly (Figure 7.3).

The XOR checksum is generated by the recursive XOR gating of all the data bytes in a data block. Byte 1 is XOR gated with byte 2, the outcome of this gating is XOR gated with byte 3, and so on. If the LRC value is appended to a data block and transmitted with it, then a simple check for transmission errors can be performed in the receiver by generating an LRC from the data block + LRC byte. The result of

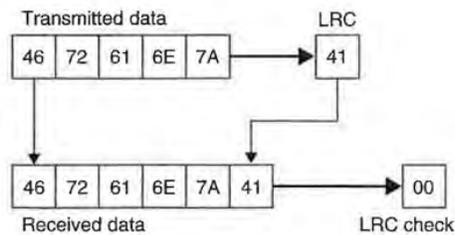


Figure 7.3 If the LCR is appended to the transmitted data, then a new LRC calculation incorporating all received data yields the checksum 00h. This permits a rapid verification of data integrity without the necessity of knowing the actual LRC sum

ed signal

85 FF 32

ors in the data

EVEN-P

ODD-P

iple exclusive-OR logic

tor output is inverted

k (LRC) can be cal-

; of all the data bytes  
me of this gating is  
ided to a data block  
ors can be performed  
C byte. The result of

LRC calculation incor-  
vid verification of data

this operation must always be zero; any other result indicates that transmission errors have occurred.

Due to the simplicity of the algorithm, LRCs can be calculated very simply and quickly. However, LRCs are not very reliable because it is possible for multiple errors to cancel each other out, and the check cannot detect whether bytes have been transposed within a data block (Rankl and Effing, 1996). LRCs are primarily used for the rapid checking of very small data blocks (e.g. 32 byte).

### 7.1.3 CRC procedure

The *CRC* (cyclic redundancy check) *procedure* was originally used in disk drives, and can generate a checksum that is reliable enough even for large data quantities. However, it is also excellently suited for error recognition in data transfer via wire-bound (telephone) or wireless interfaces (radio, RFID). The CRC procedure represents a highly reliable method of recognising transmission errors, although it cannot correct errors.

As the name suggests, the calculation of the CRC is a cyclic procedure. Thus the calculation of a CRC value incorporates the CRC value of the data byte to be calculated plus the CRC values of all previous data bytes. Each individual byte in a data block is checked to obtain the CRC value for the data block as a whole.

Mathematically speaking, a CRC checksum is calculated by the division of a polynomial using a so-called *generator polynomial*. The CRC value is the remainder obtained from this division. To illustrate this operation we have calculated a 4-bit CRC sum for a data block. The first byte of the data block is 7Fh, the generator polynomial is  $x^4 + x + 1 = 10011$  (Figure 7.4).

To calculate a 4-bit CRC, we first shift the data byte four positions to the left (eight positions for CRC 8, etc.). The four positions that become free are occupied by the starting value of the CRC calculation. In the example this is 00h. The generator polynomial is now gated with the data byte by a repeated XOR operation in accordance with the following rule: 'The highest value bit of the data byte is XOR logic gated with the generator polynomial. The initial zeros of the intermediate result are deleted and filled from the right with positions from the data byte or starting value, in order to carry out a new XOR gating with the generator polynomial. This operation is repeated until a 4 position remainder is left. This remainder is the CRC value for the data byte.'

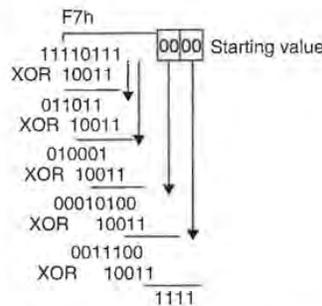


Figure 7.4 Step-by-step calculation of a CRC checksum

To calculate the CRC value for the entire data block, the CRC value from the preceding data byte is used as the starting value for the subsequent data byte.

If the CRC value that has just been calculated is appended to the end of the data block and a new CRC calculation performed, then the new CRC value obtained is zero. This particular feature of the CRC algorithm is exploited to detect errors in serial data transmission.

When a data block is transmitted, the CRC value of the data is calculated within the transmitter and this value is appended to the end of the data block and transmitted with it. The CRC value of the received data, including the appended CRC byte, is calculated in the receiver. The result is always zero, unless there are transmission errors in the received block. Checking for zero is a very easy method of analysing the CRC checksum and avoids the costly process of comparing checksums. However, it is necessary to ensure that both CRC calculations start from the same initial value. See Figure 7.5.

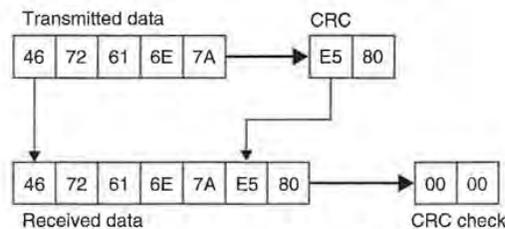
The great advantage of CRCs is the reliability of error recognition that is achieved in a small number of operations even where multiple errors are present (Rankl and Effing, 1996). A 16-bit CRC is suitable for checking the data integrity of data blocks up to 4 Kbytes in length — above this size performance falls dramatically. The data blocks transmitted in RFID systems are considerably shorter than 4 Kbytes, which means that 12- and 8-bit CRCs can also be used in addition to 16-bit CRCs.

Examples of different generator polynomials:

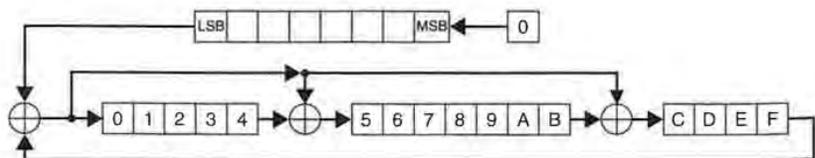
CRC-8 generator polynomial:  $x^8 + x^4 + x^3 + x^2 + 1$

CRC-16/disk controller generator polynomial:  $x^{16} + x^{15} + x^2 + 1$

CRC-16/CCITT generator polynomial:  $x^{16} + x^{12} + x^5 + 1$



**Figure 7.5** If the CRC is appended to the transmitted data a repeated CRC calculation of all received data yields the checksum 0000h. This facilitates the rapid checking of data integrity without knowing the CRC total



**Figure 7.6** Operating principle for the generation of a CRC-16/CCITT by shift registers

from the preceding e.

the end of the data lue obtained is zero. errors in serial data

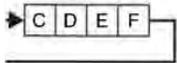
is calculated within lock and transmitted ended CRC byte, is re are transmission od of analysing the sums. However, it is ne initial value. See

tion that is achieved present (Rankl and ity of data blocks ally. The data blocks s, which means that

$$2^k + 1$$

]

CRC calculation of all king of data integrity



T by shift registers

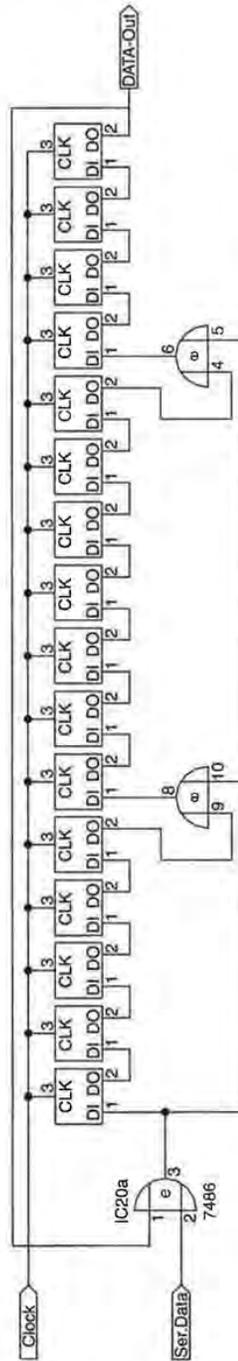


Figure 7.7 The circuit for the shift register configuration outlined in the text for the calculation of a CRC 16/CCITT

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).

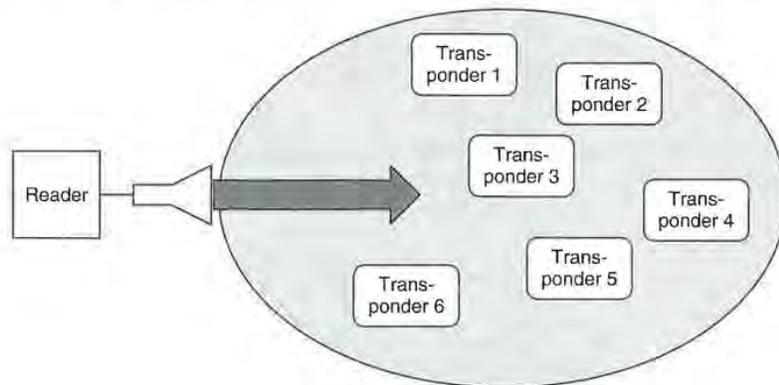
## 7.2 Multi-Access Procedures – Anticollision

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

rs, priority was given hardware circuit. This isters and XOR gates

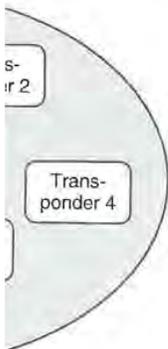
shift register is first hifting the data bits, er one after the other. R logic gating of the ough the register, the represents the desired

**Collision**

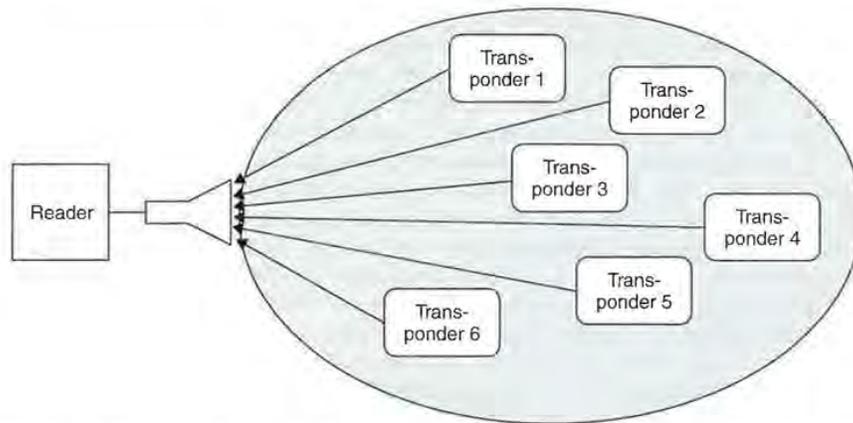
h numerous transpon- same time. In such a ber of 'participants', s of communication. ponders (Figure 7.8). ntaneously. This is o receivers of a news nication is therefore

n of data from many reader. This form of

which is determined the time span of its tween the individual



received simultaneously



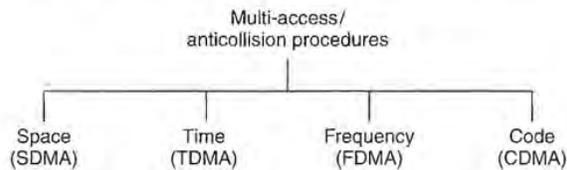
**Figure 7.9** Multi-access to a reader: numerous transponders attempt to transfer data to the reader simultaneously

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

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

tion zone of a reader, milliseconds. There may be an interrogation zone, at multi-access is not a passenger has two or three which he holds up to the multi-access procedure without any detectable difference between reader and transponder (see Figure 7.96) and we therefore

are necessary (e.g. during the

operation of these systems poses a few problems to prevent the transponder's receiver and thus the reader from the context of RFID the handling of multi-

transponder, e.g. by load balancing the interrogation zone of the reader systems. Therefore, a reader can address several transponders in the

interrogation zone generally prepared to handle multiple tags. More details can be found on the subject of this subject is, at the end of the chapter procedures.

4)

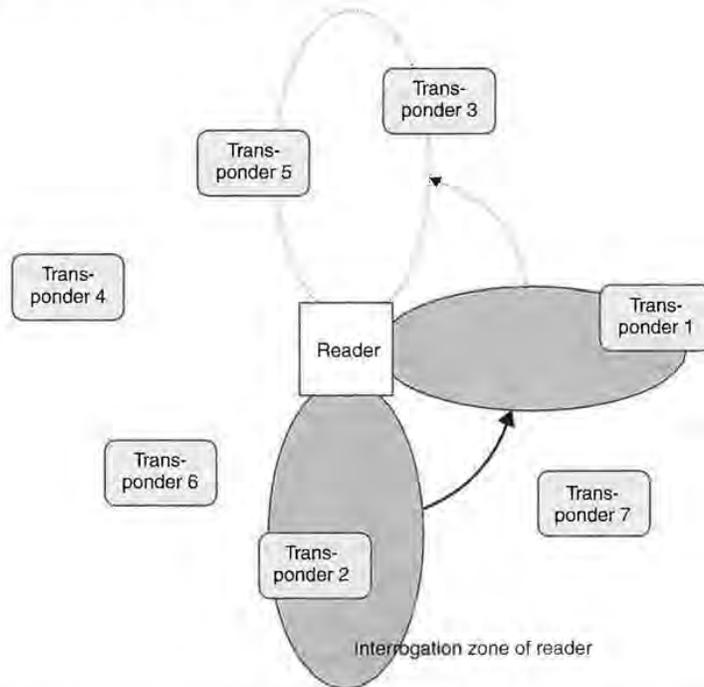
that reuse a certain frequency (see Figure 7.996).

reader, but to compensate for the narrow beam, thus forming an array, thus adjoining readers is commonly used in large-scale applications with transponders. Directional antennas are inserted into the reader's interrogation zone over the reader's output. A large number of transponders with different spatial distribution

are used with a directional antenna on the reader's output (adaptive

SDMA). So various transponders can be differentiated by their angular position in the interrogation zone of the reader.<sup>1</sup> 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

<sup>1</sup> 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.

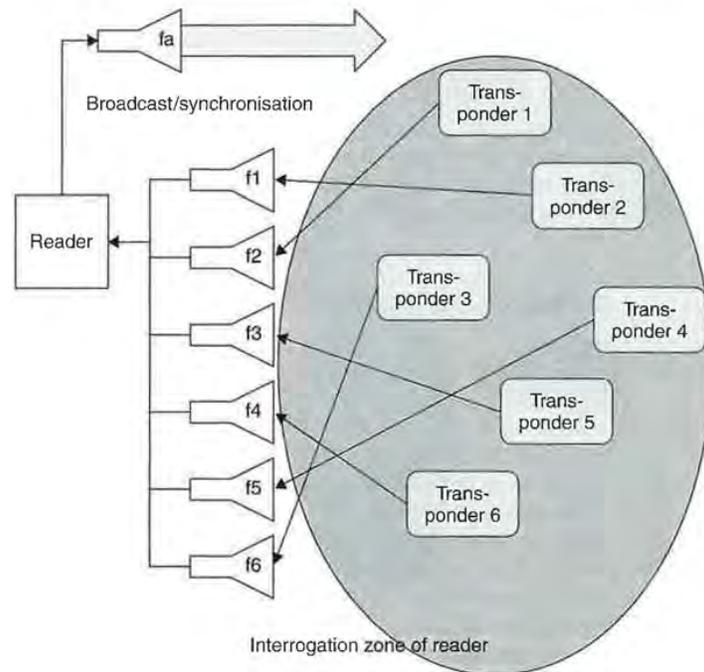
### 7.2.2 Frequency domain multiple access (FDMA)

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  $\rightarrow$  transponder (downlink): 135 kHz, transponder  $\rightarrow$  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

**DMA)**

ies in which several  
aneously available to

n a freely adjustable,  
transponder and the  
timally suited reader  
le response frequen-  
uency ranges can be  
eader → transponder  
annels in the range

tems is to use various  
1 the transponders to

igh cost of the read-  
ption channel. This  
applications.



available for the data

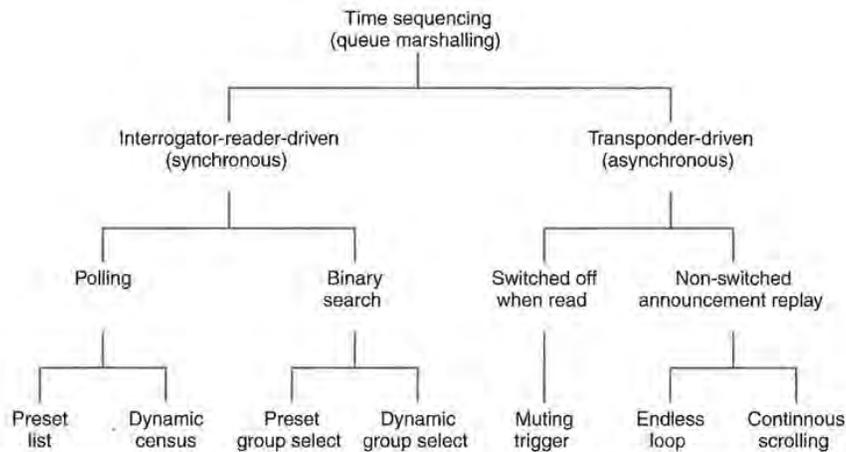
**7.2.3 Time domain multiple access (TDMA)**

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)

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  $t_0$  (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  $\tau$  of a data packet:

$$G = \sum_1^n \frac{\tau_n}{T} \cdot r_n \quad (7.1)$$

r serial numbers that  
re interrogated by the  
erial number responds.  
ie number of possible  
few known transpon-

re the most common,  
cted from a group by  
numbers transmitted  
f this procedure is to  
re precise bit position  
ensive description of

**S**

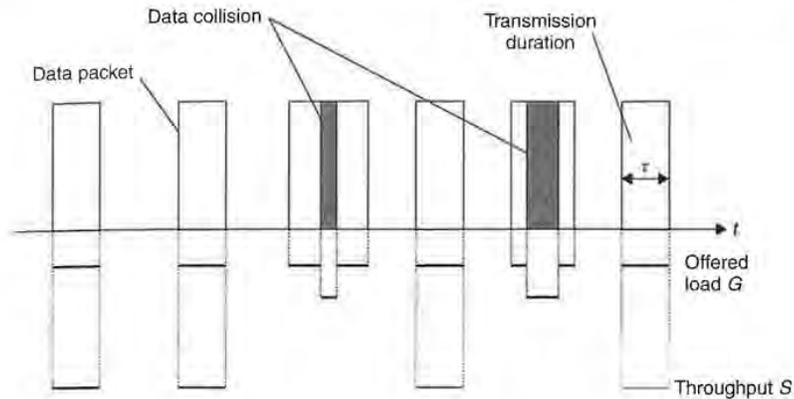
mples of anticollision  
entionally simplified  
stood without unnecc-

procedure, which got  
veloped in the 1970s  
Hawaii. As soon as  
the reader. This is a

lers, which generally  
, this data being sent  
me represents only a  
etween transmissions.  
differ slightly. There  
mit their data packets  
another.

system is shown in  
of transponders trans-  
, 3, ...). The average  
s extremely simple to

(7.1)



**Figure 7.14** Definition of the offered load  $G$  and throughput  $S$  of an ALOHA system: several transponders send their data packets at random points in time. Now and then this causes data collisions, as a result of which the (data) throughput  $S$  falls to zero for the data packets that have collided

where  $n = 1, 2, 3, \dots$  is the number of transponders in the system and  $r_n = 0, 1, 2, \dots$  is the number of data packets that are transmitted by transponder  $n$  during the observation period.

The throughput  $s$  is 1 for the transmission duration of an error-free (collision-free) data packet transmission. In all other cases, however, it is 0, since data was either not transmitted or could not be read without errors due to a collision. For the (average) throughput  $S$  of a transmission channel we find from the offered load  $G$ :

$$S = G \cdot e^{-2G} \tag{7.2}$$

If we consider the throughput  $S$  in relation to the offered load  $G$  (see Figure 7.15) we find a maximum of 18.4% at  $G = 0.5$ . For a smaller offered load the transmission channel would be unused most of the time; if the offered load was increased the number of collisions between the individual transponders would immediately increase sharply. More than 80% of the channel capacity thus remains unused. However, thanks to its simple implementation the ALOHA procedure is very well suited to use as an anticollision procedure for simple read-only transponder systems. Other fields of application for the ALOHA procedure are digital news networks such as packet radio, which is used worldwide by amateur radio enthusiasts for the exchange of written messages.

The probability of success  $q$  — the probability that an individual packet can be transmitted without collisions — can be calculated from the average offered load  $G$  and the throughput  $S$  (Fliege, 1996):

$$q = \frac{S}{G} = e^{-2G} \tag{7.3}$$

Derived from this equation, some datasheets provide figures on the time necessary to reliably read all transponders in the interrogation zone — which depends upon the number of transponders in the interrogation zone of a reader (TagMaster, 1997).

**Table 7.1** Average time consumption for reading all transponders in the interrogation zone of an example system

Number of transponders in the interrogation zone	Average (ms)	90% reliability (ms)	99.9% reliability (ms)
2	150	350	500
3	250	550	800
4	300	750	1000
5	400	900	1250
6	500	1200	1600
7	650	1500	2000
8	800	1800	2700

The probability  $p(k)$  of  $k$  error-free data packet transmissions in the observation period  $T$  can be calculated from the transmission duration  $\tau$  of a data packet and the average offered load  $G$ . The probability  $p(k)$  is a Poisson's distribution<sup>2</sup> with the mean value  $G/\tau$ :

$$p(k) = \frac{\left(G \cdot \frac{T}{\tau}\right)^k}{k!} \cdot e^{-\left(G \frac{T}{\tau}\right)} \quad (7.4)$$

#### 7.2.4.2 Slotted ALOHA procedure

One possibility for optimising the relatively low throughput of the ALOHA procedure is the *slotted ALOHA procedure*. In this procedure, transponders may only begin to transmit data packets at defined, synchronous points in time (slots). The synchronisation of all transponders necessary for this must be controlled by the reader. This is therefore a stochastic, interrogator-driven TDMA anticollision procedure.

The period in which a collision can occur (the *collision interval*) in this procedure is only half as great as is the case for the simple ALOHA procedure.

Assuming that the data packets are the same size (and thus have the same transmission duration  $\tau$ ) a collision will occur in the simple ALOHA procedure if two transponders want to transmit a data packet to the reader within a time interval  $T \leq 2\tau$ . Since, in the S-ALOHA procedure, the data packets may only ever begin at synchronous time points, the collision interval is reduced to  $T = \tau$ . This yields the following relationship for the throughput  $S$  of the S-ALOHA procedure (Fliege, 1996).

$$S = G \cdot e^{-G} \quad (7.5)$$

In the S-ALOHA procedure there is a maximum throughput  $S$  of 36.8% for an offered load  $G$  (see (Figure 7.15).

However, it is not necessarily the case that there will be a data collision if several data packets are sent at the same time: if one transponder is closer to the reader

<sup>2</sup> A random number has a Poisson's distribution if it takes on the countable number of possible values  $k = 0, 1, 2, \dots$  with a probability  $p(k) = \frac{\lambda^k}{k!} \cdot e^{-\lambda}$ .

the interrogation zone of

99.9% reliability (ms)
500
800
1000
1250
1600
2000
2700

ons in the observation of a data packet and the distribution<sup>2</sup> with the mean

$$(7.4)$$

the ALOHA procedure users may only begin to s). The synchronisation reader. This is therefore

erval) in this procedure edure.

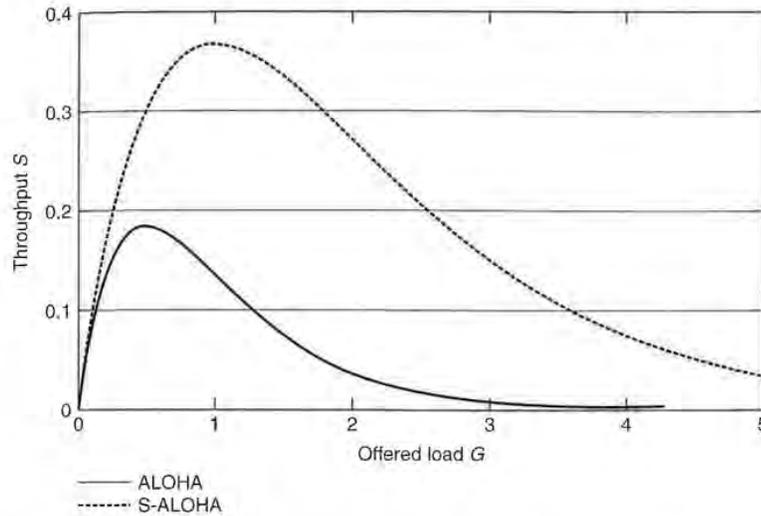
s have the same trans-DHA procedure if two within a time interval : may only ever begin  $T = \tau$ . This yields the procedure (Fliege, 1996).

$$(7.5)$$

ut  $S$  of 36.8% for an

lata collision if several s closer to the reader

number of possible values



**Figure 7.15** Comparison of the throughput curves of ALOHA and S-ALOHA. In both procedures the throughput tends towards zero as soon as the maximum has been exceeded

than the others that transponder may be able to override the data packets from other transponders as a result of the greater signal strength at the reader. This is known as the *capture effect*. The capture effect has a very beneficial effect upon throughput behaviour (Figure 7.16). Decisive for this is the threshold  $b$ , which indicates the amount by which a data packet must be stronger than others for it to be detected by the receiver without errors (Borgonovo and Zorzi, 1997; Zorzi, 1995).

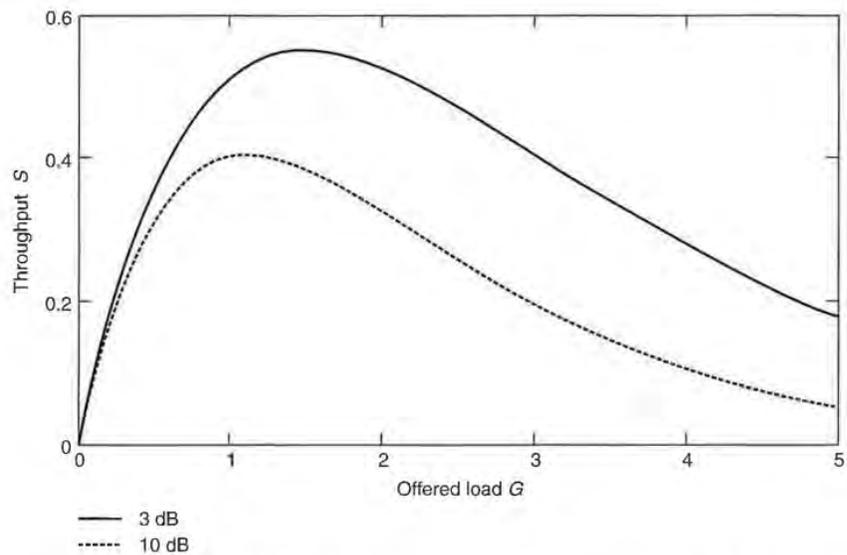
$$S = G \cdot e^{-\left(\frac{b \cdot G}{1+b}\right)} \tag{7.6}$$

The practical application of a slotted ALOHA anticollision procedure will now be considered in more detail on the basis of an example.

The transponder used must also have a unique *serial number* (i.e. one that has been allocated only once). In this example we use an 8-bit serial number; this means that a maximum of 256 transponders can be put into circulation if the uniqueness of serial numbers is to be guaranteed.

We define a set of commands in order to synchronise and control the transponders (Table 7.2).

A reader in wait mode transmits a *REQUEST command* at cyclical intervals. We now bring five transponders into the interrogation zone of a reader at the same time (Figure 7.17). As soon as the transponders have recognised the REQUEST command, each transponder selects one of the three available slots by means of a random-check generator, in order to send its own serial number to the reader. As a result of the random selection of slots in our example there are collisions between the transponders in slots 1 and 2. Only in slot 3 can the serial number of transponder 5 be transmitted without errors.



**Figure 7.16** Throughput behaviour taking into account the capture effect with thresholds of 3 dB and 10 dB

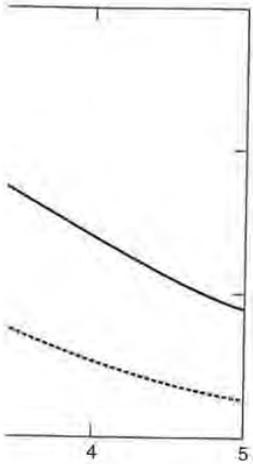
**Table 7.2** Command set for anticollision

REQUEST	This command synchronises all transponders in the reader's interrogation zone and prompts the transponders to transmit their serial numbers to the reader in one of the time slots that follow. In our example there are always three time slots available.
SELECT(SNR)	Sends a (previously determined) serial number (SNR) to the transponder as a parameter. The transponder with this serial number is thereby cleared to perform read and write commands (selected). Transponders with a different serial number continue to react only to a REQUEST command.
READ_DATA	The selected transponder sends stored data to the reader. (In a real system there are also commands for writing, authentication, etc.)

If a serial number is read without errors, then the detected transponder can be selected by the transmission of a SELECT command and then read or written without further collisions with other transponders. If no serial number were detected at the first attempt the REQUEST command is simply repeated cyclically.

When the previously selected transponder has been processed, further transponders in the interrogation zone of the reader can be sought by means of a new REQUEST command.

*Dynamic S-ALOHA procedure* As we have established, the throughput  $S$  of an S-ALOHA system is maximised at a offered load  $G$  of around 1. This means that there are the same number of transponders in the interrogation zone of the reader as



ire effect with thresholds of

m

ers in the reader's  
sponders to transmit their  
he time slots that follow. In  
e slots available.

mber (SNR) to the  
nder with this serial  
ad and write commands  
t serial number continue to

ia to the reader. (In a real  
iting, authentication, etc.)

cted transponder can be  
n read or written without  
were detected at the first  
ly.

sed, further transponders  
ans of a new REQUEST

the throughput  $S$  of an  
und 1. This means that  
on zone of the reader as

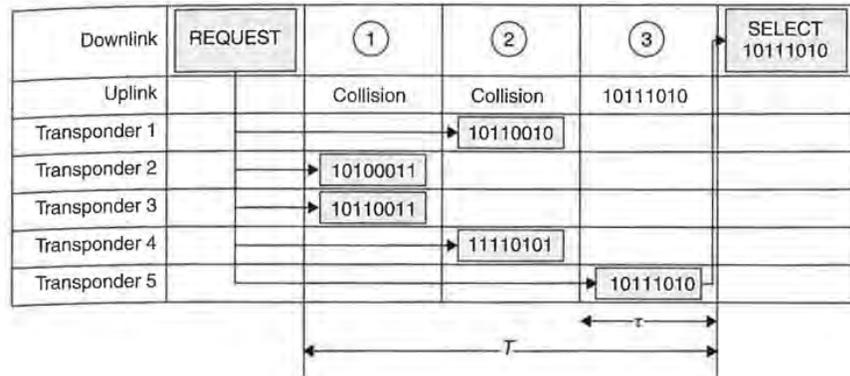


Figure 7.17 Transponder system with slotted ALOHA anticollision procedure

there are slots available. If many further transponders are added, then the throughput quickly falls to zero. In the worst case, no serial numbers can be detected even after an infinite number of attempts because no transponder succeeds in being the only one to transmit in one slot. This situation can be eased by the provision of a sufficient number of slots. However, this reduces the performance of the anticollision algorithm, since the system has to listen for possible transponders for the duration of all time slots — even if only a single transponder is located in the interrogation zone of the reader. Dynamic S-ALOHA procedures with a variable number of slots can help here.

One possibility is to transmit the number of slots (currently) available for the transponders with each REQUEST command as an argument: in wait mode the reader transmits REQUEST commands at cyclical intervals, which are followed by only one or two slots for possible transponders. If a greater number of transponders cause a bottleneck in both slots, then for each subsequent REQUEST command the number of slots made available is increased (e.g. 1, 2, 4, 8, ...) until finally an individual transponder can be detected.

However, a large number of slots (e.g. 16, 32, 48, ...) may also be constantly available. In order to nevertheless increase performance, the reader transmits a BREAK command as soon as a serial number has been recognised. Slots following the BREAK commands are 'blocked' to the transmission of transponder addresses (Figure 7.18).

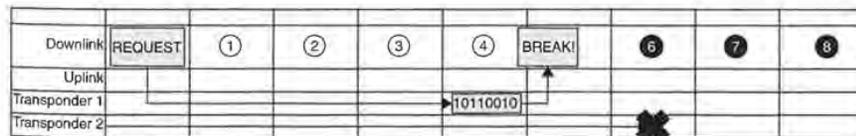


Figure 7.18 Dynamic S-ALOHA procedure with BREAK command. After the serial number of transponder 1 has been recognised without errors, the response of any further transponders is suppressed by the transmission of a BREAK command

### 7.2.4.3 Binary search algorithm

The implementation of a binary search algorithm requires that the precise bit position of a data collision is recognised in the reader. In addition, a suitable *bit coding* is required, so we will first compare the collision behaviour of *NRZ* (non-return-to-zero) and *Manchester coding* (Figure 7.19). The selected system is an inductively coupled transponder system with load modulation by an ASK modulated subcarrier. A 1 level in the baseband coding switches the subcarrier on, and a 0 level switches it off.

**NRZ Code** The value of a bit is defined by the static level of the transmission channel within a bit window ( $t_{\text{BIT}}$ ). In this example a logic 1 is coded by a static 'high' level; a logic 0 is coded by a static 'low' level.

If at least one of the two transponders sends a subcarrier signal, then this is interpreted by the reader as a 'high' level and in our example is assigned the logic value 1. The reader cannot detect whether the sequence of bits it is receiving can be traced back to the superposition of transmissions from several transponders or the signal from a single transponder. The use of a block checksum (parity, CRC) can only detect a transmission error 'somewhere' in the data block (see Figure 7.20).

**Manchester code** The value of a bit is defined by the change in level (negative or positive transition) within a bit window ( $t_{\text{BIT}}$ ). A logic 0 in this example is coded by a positive transition; a logic 1 is coded by a negative transition. The 'no transition' state is not permissible during data transmission and is recognised as an error.

If two (or more) transponders simultaneously transmit bits of different values then the positive and negative transitions of the received bits cancel each other out, so that a subcarrier signal is received for the duration of an entire bit. This state is not permissible in the Manchester coding system and therefore leads to an error. It is thus possible to trace a collision to an individual bit (see Figure 7.20).

We will use Manchester coding for our binary search algorithm. Let us now turn our attention to the algorithm itself.

A binary search algorithm consists of a predefined sequence (specification) of interactions (command and response) between a reader and several transponders with the objective of being able to select any desired transponder from a large group.

For the practical realisation of the algorithm we require a set of commands that can be processed by the transponder (Table 7.3). In addition, each transponder has a unique *serial number*. In our example we are using an 8-bit serial number, so if we

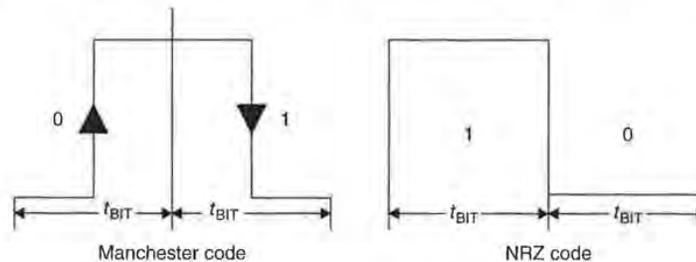


Figure 7.19 Bit coding using Manchester and NRZ code



**Table 7.3** Transponder commands for the binary search algorithm

REQUEST(SNR)	This command sends a serial number to the transponder as a parameter. If the transponder's own serial number is <b>less than</b> (or equal to) the received serial number, then the transponder sends its own serial number back to the reader. The group of transponders addressed can thus be preselected and reduced.
SELECT_(SNR)	Sends a (predetermined) serial number (SNR) to the transponder as a parameter. The transponder with the identical transponder address will become available for the processing of other commands (e.g. reading and writing data). This transponder is thus selected. Transponders with different addresses will thereafter only respond to a REQUEST command.
READ_DATA	The selected transponder sends stored data to the reader. (In a real system there are also commands for authentication or writing, debiting, crediting, etc.).
UNSELECT	The selection of a previously selected transponder is cancelled and the transponder is 'muted'. In this state, the transponder is completely inactive and does not even respond to a REQUEST command. To reactivate the transponder, it must be reset by temporarily removing it from the interrogation zone of the reader (= no power supply).

**Table 7.4** Serial numbers of the transponders used in this example

Transponder 1	10110010
Transponder 2	10100011
Transponder 3	10110011
Transponder 4	11100011

At bit 0, bit 4 and bit 6 of the received serial number there is a collision (X) as a result of the superposition of the different bit sequences of the responding transponders. The occurrence of one or more collisions in the received serial numbers leads to the conclusion that there are two or more transponders in the interrogation zone of the reader. To be more precise, the received bit sequence 1X1X001X yields eight possibilities for the serial numbers that have still to be detected (Table 7.5).

Bit 6 is the highest value bit at which a collision has occurred in the first iteration. This means that there is at least one transponder both in the range  $\text{SNR} \geq 11000000\text{b}$  and also in  $\text{SNR} \leq 10111111\text{b}$ .<sup>3</sup> In order to be able to select an individual transponder, we have to limit the search range for the next iteration according to the information obtained. We decide arbitrarily to continue our search in the range  $\leq 10111111\text{b}$ . To do this we simply set bit 6 equal to 0 (highest value bit with collision), and ignore all lower value bits by setting them to 1.

<sup>3</sup> Bit 6 is printed in bold type in each case. A careful evaluation of the results in Table 7.5 leads to the conclusion that there is at least one transponder in the ranges 11100010b–11110011b and 10100010b–10110011b.

search algorithm

to the transponder as a serial number is less than (or equal to) the transponder sends its serial number. The group of transponders is then reduced.

(SNR) to the transponder as a unique transponder address. The transponder is thus selected.

The transponder will thereafter only respond to the reader.

data to the reader. (In a real system, there is authentication or writing, but this is not shown.)

The transponder is cancelled and the search is continued. If, after a certain time, the transponder does not respond to a REQUEST command, it must be reset by the reader. This is done by the reader's interrogation zone of the reader.

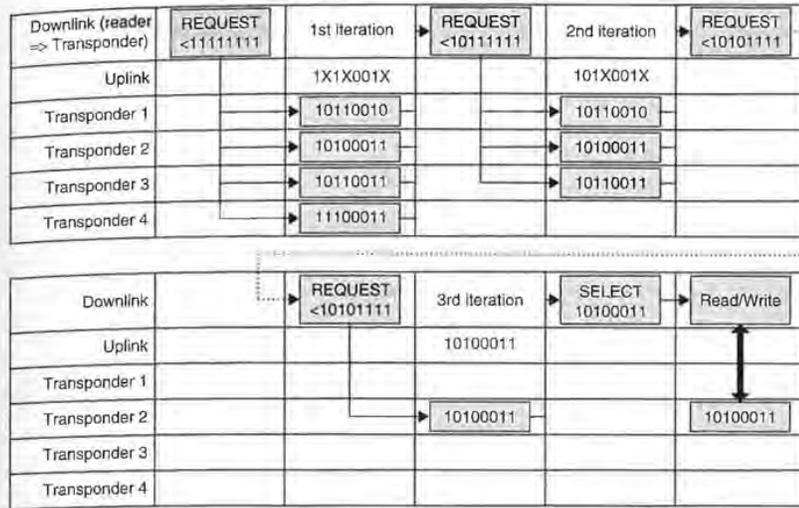


Figure 7.21 The different serial numbers that are sent back from the transponders to the reader in response to the REQUEST command lead to a collision. By the selective restriction of the preselected address range in further iterations, a situation can finally be reached in which only a single transponder responds

Table 7.5 Possible serial numbers after the evaluation of the received data and taking into account the collisions (X) that have occurred in the first iteration. Four of the possible transponder addresses (\*) actually arise in our example

Bit number:	7	6	5	4	3	2	1	0
Received data in the reader	1	X	1	X	0	0	1	X
Possible serial number A	1	0	1	0	0	0	1	0
Possible serial number B*	1	0	1	0	0	0	1	1
Possible serial number C*	1	0	1	1	0	0	1	0
Possible serial number D*	1	0	1	1	0	0	1	1
Possible serial number E	1	1	1	0	0	0	1	0
Possible serial number F*	1	1	1	0	0	0	1	1
Possible serial number G	1	1	1	1	0	0	1	0
Possible serial number H	1	1	1	1	0	0	1	1

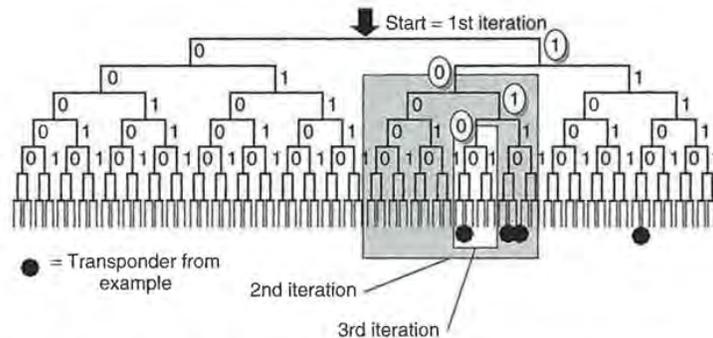
The general rule for limiting the search area (range) is shown in Table 7.6.

After the reader has transmitted the command REQUEST ( $\leq 10111111$ ), all transponders that fulfil this condition will respond by sending their own serial numbers to the reader. In our example these are the transponders 1, 2 and 3 (Figure 7.22). There is now a collision (X) at bit 0 and bit 4 of the received serial number. From this we can conclude that there are still at least two transponders in the search range of the second iteration. The received bit sequence 101X001X still permits four options for the serial numbers that remain to be detected (Table 7.7).

As shown in Table 7.5 leads to the conclusion that the possible serial numbers are 10110010b and 10100010b–10110011b.

**Table 7.6** General rule for forming the address parameter in a binary search tree. In each case, bit (X) is the highest value bit of the received transponder address in which a collision occurred in the previous iteration

Search command	1st iteration range	<i>n</i> th iteration range =
REQUEST $\geq$ Range	0	Bit(X) = 1, Bit(0 to X - 1) = 0
REQUEST $\leq$ Range	SNRmax	Bit(X) = 0, Bit(0 to X - 1) = 1



**Figure 7.22** Binary search tree. An individual transponder can finally be selected by a successive reduction of the range

**Table 7.7** Possible serial numbers in the search range after the evaluation of the 2nd iteration. The transponders marked (\*) are actually present

Bit number:	7	6	5	4	3	2	1	0
Received data at reader	1	0	1	X	0	0	1	X
Possible serial number A	1	0	1	0	0	0	1	0
Possible serial number B*	1	0	1	0	0	0	1	1
Possible serial number C*	1	0	1	1	0	0	1	0
Possible serial number D*	1	0	1	1	0	0	1	1

The renewed appearance of collisions in the second iteration necessitates a further restriction of the range in a third iteration. The use of the rule in Table 7.6 leads us to the search range  $\leq 10101111$ . The reader now transmits to the transponders the command REQUEST ( $\leq 10101111$ ). This condition is now only fulfilled by transponder 2 (10100011), which now responds to the command alone. We have thus detected a valid serial number — a further iteration is not necessary.

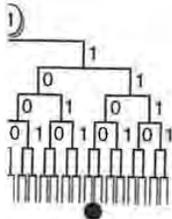
By means of a subsequent SELECT command, transponder 2 is selected using the detected transponder address and can now be read or written by the reader without interference from other transponders. All other transponders are silent as only a selected transponder responds to a write/read command — READ\_DATA.

After the completion of the write/read operations, transponder 2 can be fully deactivated by an UNSELECT command, so that it no longer responds to the next REQUEST

is a binary search tree.  
transponder address in

iteration range =

1, Bit(0 to X - 1) = 0  
2, Bit(0 to X - 1) = 1



ly be selected by a succes-

ge after the  
ked (\*) are

21	0
01	X
01	0
01	1
01	0
01	1

on necessitates a further  
rule in Table 7.6 leads  
to the transponders the  
fulfilled by transponder  
e have thus detected a

2 is selected using the  
by the reader without  
silent as only a selected  
FA.

r 2 can be fully deacti-  
s to the next REQUEST

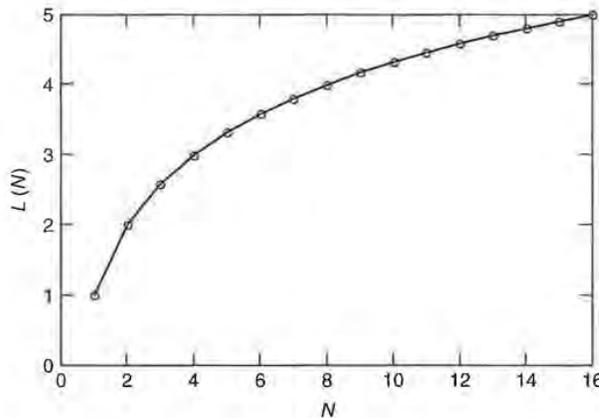
command. In this manner the number of iterations necessary for the selection of an individual transponder can be gradually reduced if a large number of transponders are 'waiting' for processing in the interrogation zone of the reader. In our example, running the anticollision algorithm again would thus automatically lead to the selection of one of the previously processed transponders 1, 3 or 4.

The average number of iterations  $L$  that are required to detect a single transponder from a large number depends upon the total number of transponders  $N$  in the interrogation zone of the reader, and can be calculated easily:

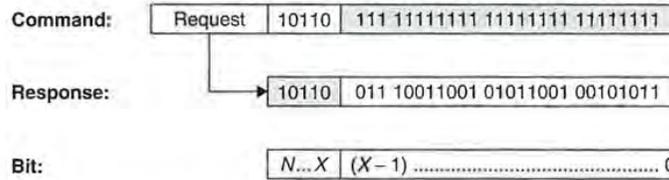
$$L(N) = \log_2(N) + 1 \tag{7.7}$$

If only a single transponder is located in the interrogation zone of the reader, precisely one iteration is required to detect the serial number of the transponder — a collision does not occur in this case. If there is more than one transponder in the interrogation zone of the reader, then the average number of iterations increases quickly, following the curve shown in Figure 7.23.

*Dynamic binary search procedure* In the binary search procedure described above, both the search criterion and the serial numbers of the transponders are always transmitted at their full length. In practice, however, the serial numbers of transponders do not consist of one byte, as in our example, but, depending upon the system, can be up to 10 bytes long, which means that a large quantity of data must be transferred in order to select an individual transponder. If we investigate the data flow between the reader and the individual transponders in more detail (Figure 7.24) we find that:



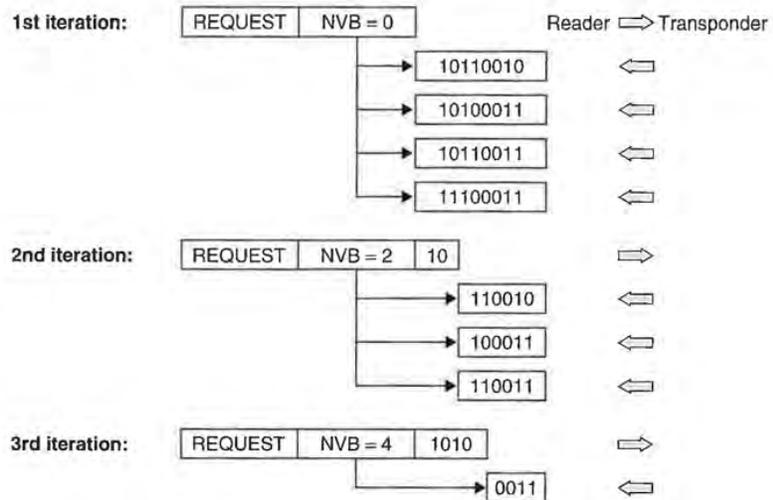
**Figure 7.23** The average number of iterations needed to determine the transponder address (serial number) of a single transponder as a function of the number of transponders in the interrogation zone of the reader. When there are 32 transponders in the interrogation zone an average of six iterations are needed, for 65 transponders on average seven iterations, for 128 transponders on average eight iterations, etc.



**Figure 7.24** Reader's command (*n*th iteration) and transponder's response when a 4-byte serial number has been determined. A large part of the transmitted data in the command and response is redundant (shown in grey). *X* is used to denote the highest value bit position at which a bit collision occurred in the previous iteration

- Bits  $(X - 1)$  to 0 of the command contain no additional information for the transponder since they are always set to 1.
- Bits *N* to *X* of the serial number in the transponder's response contain no additional information for the reader, as they are already known and predetermined.

We therefore see that complementary parts of the transmitted serial numbers are redundant and actually do not need to be transmitted. This quickly leads us to an optimized algorithm. Instead of transmitting the full length of the serial numbers in both directions, the transfer of a serial number or the search criterion is now simply split according to bit (*X*). The reader now sends only the known part (*N*–*X*) of the serial number to be determined as the search criterion in the REQUEST command and then interrupts the transmission. All transponders with serial numbers that correspond to the search criterion in the bits (*N*–*X*) now respond by transmitting the remaining bits



**Figure 7.25** The dynamic binary search procedure avoids the transmission of redundant parts of the serial number. The data transmission time is thereby noticeably reduced

1111 11111111

001 00101011

..... 0

sponse when a 4-byte serial  
the command and response  
bit position at which a bit

nal information for the

rse contain no additional  
predetermined.

itted serial numbers are  
quickly leads us to an  
of the serial numbers in  
criterion is now simply  
own part (N-X) of the  
EQUEST command and  
numbers that correspond  
itting the remaining bits

der => Transponder



mission of redundant parts  
y reduced

((X - 1) - 0) of their serial numbers. The transponders are informed of the number of subsequent bits by an additional parameter (NVB = number of valid bits) in the REQUEST command.

Let us now illustrate in more detail the sequence of a dynamic binary search algorithm on the basis of the example in Figure 7.25. We use the same transponder serial numbers as in the previous example. Since we are applying the rule (Table 7.6) unchanged, the sequence of individual iterations corresponds with that of the previous example. In contrast, however, the amount of data to be transferred — and thus the total time needed — can be reduced by up to 50%.

# 9

## Standardisation

The development of standards is the responsibility of the technical committee of the ISO. The ISO is the worldwide union of national standardisation institutions, such as DIN (Germany) and ANSI (USA).

The description of standards in this chapter merely serves to aid our technical understanding of the RFID applications dealt with in this book and no attempt has been made to describe the standards mentioned in their entirety. Furthermore, standards are updated from time to time and are thus subject to change. When working with the RFID applications in question the reader should not rely on the parameters specified in this chapter. We recommend that copies of the original versions in question are procured. The necessary addresses are listed in Section 14.2 at the end of this book.

### 9.1 Animal Identification

ISO standards 11784, 11785 and 14223 deal with the *identification of animals* using RFID systems.

- ISO 11784: 'Radio-frequency identification of animals — Code structure'
- ISO 11785: 'Radio-frequency identification of animals — Technical concept'
- ISO 14223: 'Radio-frequency identification of animals — Advanced transponders':
  - Part 1: Air interface
  - Part 2: Code and command structure
  - Part 3: Applications

The constructional form of the transponder used is not specified in the standards and therefore the form can be designed to suit the animal in question. Small, sterile glass transponders that can be injected into the fatty tissues of the animal are normally used for the identification of cows, horses and sheep. Ear tags or collars are also possible.

#### 9.1.1 ISO 11784 - Code structure

The identification code for animals comprises a total of 64 bits (8 bytes). Table 9.1 shows the significance of the individual bits.

---

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

Table 9.1 Identification codes for animals

Bit number	Information	Description
1	Animal (1)/non-animal application (0)	Specifies whether the transponder is used for animal identification or for other purposes
2–15	Reserved	Reserved for future applications
16	Data block (1) follows/no data block (0)	Specifies whether additional data will be transmitted after the identification code
17–26	Country code as per ISO 3166	Specifies the country of use (the code 999 describes a test transponder)
27–64	National identification code	Unique, country-specific registration number

The national identification code should be managed by the individual countries. Bits 27 to 64 may also be allocated to differentiate between different animal types, breeds, regions within the country, breeders etc., but this is not specified in this standard.

### 9.1.2 ISO 11785 – Technical concept

This standard defines the transmission method for the transponder data and the reader specifications for activating the data carrier (transponder). A central aim in the development of this standard was to facilitate the interrogation of transponders from an extremely wide range of manufacturers using a common reader. A reader for *animal identification* in compliance with the standard recognises and differentiates between transponders that use a full/half duplex system (load modulation) and transponders that use a sequential system.

#### 9.1.2.1 Requirements

The standard specifies the operating frequency for the reader as  $134.2 \text{ kHz} \pm 1.8 \text{ kHz}$ . The emitted field provides a power supply for the transponder and is therefore termed the 'activation field'.

The activation field is periodically switched on for 50 ms at a time and then switched off for 3 ms (1 in Figure 9.1). During the 50 ms period when it is switched on it waits

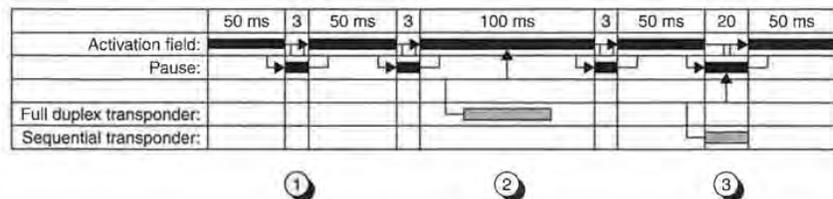


Figure 9.1 Path of the activation field of a reader over time: ① no transponder in interrogation zone, ② full/half duplex (= load modulated) transponder in interrogation zone, ③ sequential transponder in the interrogation zone of the reader

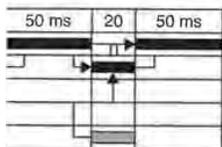
5  
**description**  
 transponder is used for  
 in or for other purposes  
 applications  
 additional data will be  
 the identification code  
 of use (the code 999  
 transponder)  
 identification registration number

individual countries. Bits  
 for animal types, breeds,  
 defined in this standard.

reader data and the reader  
 central aim in the devel-  
 opment of transponders from an  
 earlier. A reader for *animal*  
 1 differentiates between  
 (n) and transponders that

is 134.2 kHz ± 1.8 kHz.  
 and is therefore termed

time and then switched  
 is switched on it waits



③

transponder in interrogation  
 zone, ③ sequential

for the response from a full/half duplex transponder — a sequential transponder in the field requires the activation field to charge up its charging capacitor.

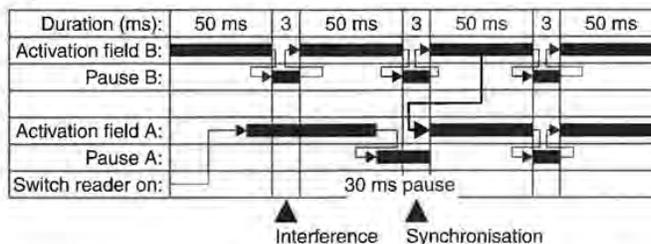
If a full/half duplex transponder is present within the range of the activation field, then this transponder sends its data during the operating interval of the field (2 in Figure 9.1). While data is being received the operating interval can be extended to 100 ms if the data transfer is not completed within the first 50 ms.

A sequential transponder in the range of the activation field (3 in Figure 9.1) begins to transmit data within the 3 ms pause. The duration of the pause is extended to a maximum of 20 ms to permit the complete transmission of a data record.

If portable or stationary readers are operated in the vicinity of one another, then there is a high probability that a reader will emit its activation field during the 3 ms pause of the other reader. This would result in neither of the readers being able to receive the data signal of a sequential transponder. Due to the relatively strong activation field in comparison to the field strength of a sequential transponder this effect occurs in a multiple of the reader's normal read radius. Appendix C of the standard therefore describes procedures for the *synchronisation* of several readers to circumvent this problem.

Portable and stationary readers can be tested for the presence of a second reader (B in Figure 9.2) in the vicinity by extending the pause duration to 30 ms. If the activation field of a second reader (B) is received within the 30 ms pause, then the standard stipulates that the activation field of the reader (A) should be switched on for a maximum of 50 ms as soon as the previously detected reader (B) switches its activation field on again after the next 3 ms pause. In this manner, a degree of synchronisation can be achieved between two neighbouring readers. Because data is only transmitted from the transponder to the reader (and the activation field thus always represents an unmodulated HF field), an individual transponder can be read by two portable readers simultaneously. To maintain the stability of the synchronisation, every tenth pause cycle is extended from 3 ms to 30 ms to detect any other readers that have recently entered the area.

Stationary readers also use a *synchronisation cable* connected to all readers in the system. The synchronisation signal at this cable is a simple logic signal with low and high levels. The resting state of the cable is a logic low level.



**Figure 9.2** Automatic synchronisation sequence between readers A and B. Reader A inserts an extended pause of a maximum of 30 ms after the first transmission pulse following activation so that it can listen for other readers. In the diagram, the signal of reader B is detected during this pause. The reactivation of the activation field of reader B after the next 3 ms pause triggers the simultaneous start of the pulse pause cycle of reader A

If one of the connected readers detects a transponder, then the synchronisation cable switches to the high level while data is transmitted from the transponder to the reader. All other readers extend their current phase (activation/pause).

If the detected data carrier is a full/half duplex transponder, then the synchronised readers are in the 'activation field' phase. The activation period of the activation field is now extended until the synchronisation cable is once again switched to low level (but with a maximum of 100 ms).

If the signal of a sequential transponder is received, the synchronised readers are in the 'pause' phase. The synchronisation signal at the cable extends the pause duration of all readers to 20 ms (fixed value).

### 9.1.2.2 Full/half duplex system

Full/half duplex transponders, which receive their power supply through an activation field, begin to transmit the stored identification data immediately. For this a *load modulation procedure* without a subcarrier is used, whereby the data is represented in a differential bi-phase code (DBP). The bit rate is derived by dividing the reader frequency by 32. At 134.2 kHz the transmission speed (bit rate) is 4194 bit/s.

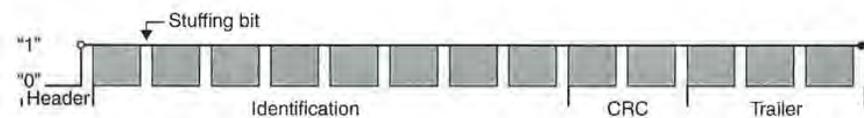
A full/half duplex data telegram comprises an 11-bit header, 64 bits (8 bytes) of useful data, 16-bit (2-byte) CRC and 24-bit (3-byte) trailer (Figure 9.3). After every eight transmitted bits a stuffing bit with a logic 1 level is inserted to avoid the chance occurrence of the header 0000000001. The transmission of the total of 128 bits takes around 30.5 ms at the given transmission speed.

### 9.1.2.3 Sequential system

After every 50 ms the activation field is switched off for 3 ms. A sequential transponder that has previously been charged with energy from the activation field begins to transmit the stored identification data approximately 1 to 2 ms after the activation field has been switched off.

The modulation method used by the transponder is frequency shift keying (2 FSK). The bit coding uses NRZ (comparable to RS232 on a PC). A logic 0 corresponds with the basic frequency 134.2 kHz; a logic 1 corresponds to the frequency 124.2 kHz.

The bit rate is derived by dividing the transmission frequency by 16. The bit rate varies between 8387 bit/s for a logic 0 and 7762 bit/s for a logic 1 depending upon the frequency shift keying.



**Figure 9.3** Structure of the load modulation data telegram comprising of starting sequence (header), ID code, checksum and trailer

ie synchronisation cable  
ansponder to the reader.

, then the synchronised  
d of the activation field  
1 switched to low level

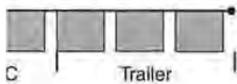
chronised readers are in  
ends the pause duration

ly through an activation  
liately. For this a *load*  
the data is represented  
by dividing the reader  
e) is 4194 bit/s.

der, 64 bits (8 bytes) of  
Figure 9.3). After every  
ted to avoid the chance  
ie total of 128 bits takes

A sequential transponder  
1 field begins to transmit  
activation field has been

oy shift keying (2 FSK).  
ogic 0 corresponds with  
equence 124.2 kHz.  
ncy by 16. The bit rate  
c 1 depending upon the



ising of starting sequence

The sequential data telegram comprises an 8-bit header 01111110b, 64 bits (8 bytes) of useful data, 16-bit (2-byte) CRC and 24-bit (3-byte) trailer. Stuffing bits are not inserted.

The transmission of the total of 112 bits takes a maximum of 14.5 ms at the given transmission speed ('1' sequence).

**9.1.3 ISO 14223 - Advanced transponders**

This standard defines the HF interface and the data structure of so-called *advanced transponders*. ISO 14223 is based upon the older standards ISO 11784 and ISO 11785 and represents a further development of these standards. Whereas transponders in accordance with ISO 11785 only transmit a permanently programmed identification code, in advanced transponders there is the possibility of managing a larger memory area. As a result, data can be read, written and even protected against overwriting (lock memory block), in blocks.

The standard consists of three parts: Part 1: 'Air Interface', Part 2 'Code and Command Structure' and Part 3 'Applications'. Since this standard is currently still in development we can only consider the content of Parts 1 and 2 here. Part 2 of the standard is based heavily upon the standard ISO/IEC 18000-2, which is still in development.

**9.1.3.1 Part 1 - Air interface**

As a further development of ISO 11785, ISO 14223 is downwards compatible with its predecessor standard and can thus only be considered in connection with ISO 11785. This means both that the identification number of each advanced transponder can be read by a simple ISO 11785 reader and that an ISO 11785 transponder is accepted by any advanced reader.

If an advanced transponder enters the interrogation field of an ISO 14223 compatible reader, then first of all the *ISO 11784 identification code* will always be read in accordance with the procedure in ISO 11785. To facilitate differentiation between an advanced transponder and a pure ISO 11785 transponder, bit 16 (data block follows) of the identification code is set to '1' in advanced transponders. Then, by means of a defined procedure, the transponder is switched into advanced mode, in which commands can also be sent to the transponder.

Advanced transponders can be subdivided into full duplex (FDX-B) and sequential (HDX-ADV) transponders.

The procedures and parameters defined in ISO 11785 apply to the data transmission from transponder to reader (uplink) in any operating state.

**FDX-B** If an advanced transponder of type FDX-B enters the interrogation field of a reader, then the transponder's identification code, as defined in ISO/IEC 11785, is continuously transmitted to the reader. The reader recognises that this is an *FDX-B transponder* by the setting of bit 16 (data block follows). In order to switch the transponder into *advanced mode* the field of the reader must first be completely switched off for 5 ms. If the field is switched back on, the transponder can be switched into advanced mode within a defined time window by the transmission of a 5-bit

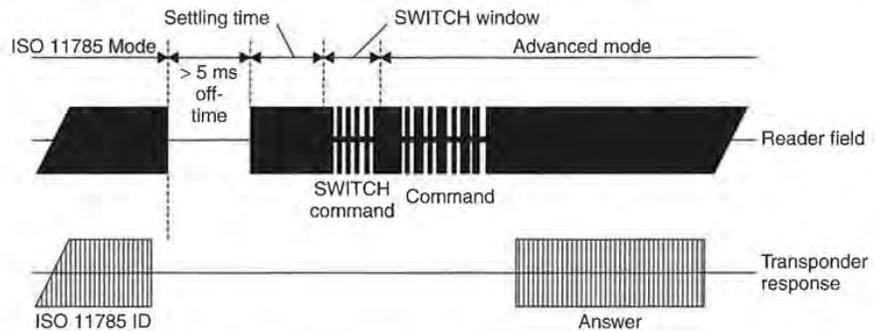


Figure 9.4 Signal path at the antenna of a reader

Table 9.2 Parameters of the transmission link from reader to transponder (downlinks)

Parameter	Mode switching	Advanced mode
Modulation procedure	ASK 90–100%	ASK 90–100%
Coding	Binary Pulse Length	PIE (Pulse interval encoding)
Baud rate	6000 bit/s (LSB first)	6000 bit/s (LSB first)
Mode switching code	5 bit pattern (00011)	—
Mode switching timing	Transponder settling time: $312.5/f_c = 2.33 \text{ ms}$ SWITCH window: $232.5/f_c = 1.73$	

'SWITCH' command. The transponder then awaits further commands from the reader. See Figure 9.4.

**HDX-ADV** A sequential transponder (HDX) charges its charging capacitor during the 50 ms period that the field is switched on. Within the 3 ms field pause the transponder begins to transmit the 64-bit identification code, as defined in ISO/IEC 11785. The duration of the pause is extended to a maximum of 20 ms to facilitate the complete transfer of the data block. An advanced transponder (HDX-ADV) is recognised by the setting of bit 16 (data block follows) in the identification code.

A sequential transponder can be switched to any interrogation cycle in advanced mode. To achieve this, a command is simply sent to the transponder in the second half of the 50 ms period in which the field is switched on (Figure 9.5). The transponder executes this command immediately and sends its response to the reader in the next pause. If no command is sent in an interrogation cycle, then the transponder automatically reverts to ISO 11785 mode and transmits its identification code to the reader in the next pause.

### 9.1.3.2 Part 2 - Code and command structure

This part of the standard describes the simple *transmission protocol* between transponder and reader, the memory organisation of the transponder, and commands that must be supported by advanced transponders.

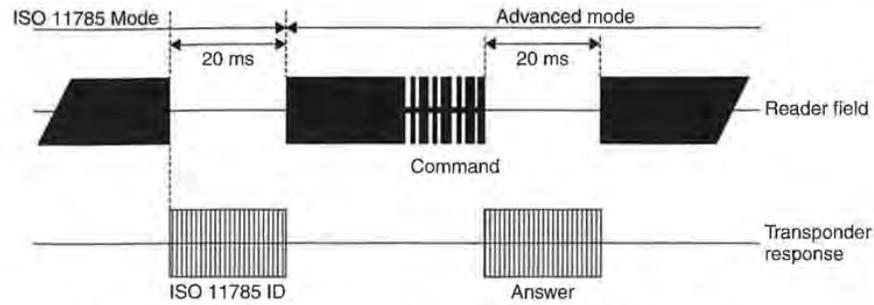
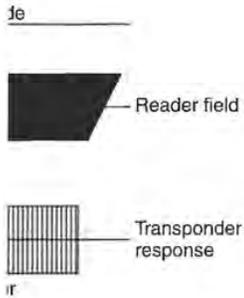


Figure 9.5 A sequential advanced transponder is switched into advanced mode by the transmission of any desired command

Table 9.3 Parameters of the transmission link from reader to transponder (downlink)

Parameter	Value
Modulation procedure	ASK 90–10%
Coding	Pulse Width Modulation (PWM)
Baud rate (downlink)	500 bit/s

ansponder (downlinks)

**Advanced mode**

90–100%  
Pulse interval encoding)  
bit/s (LSB first)

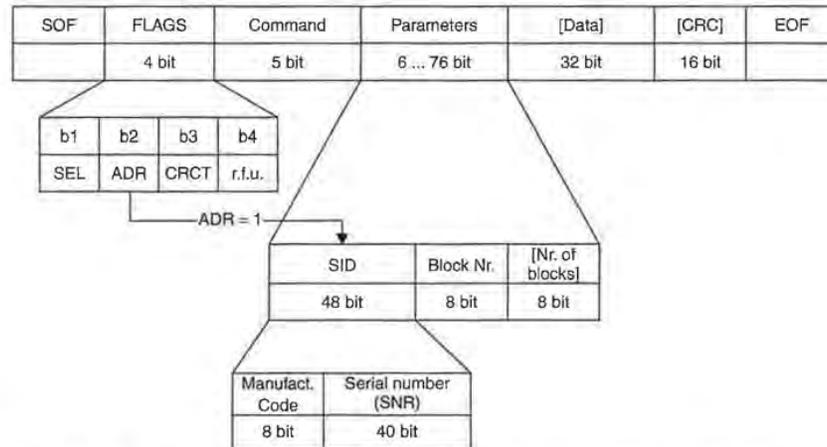
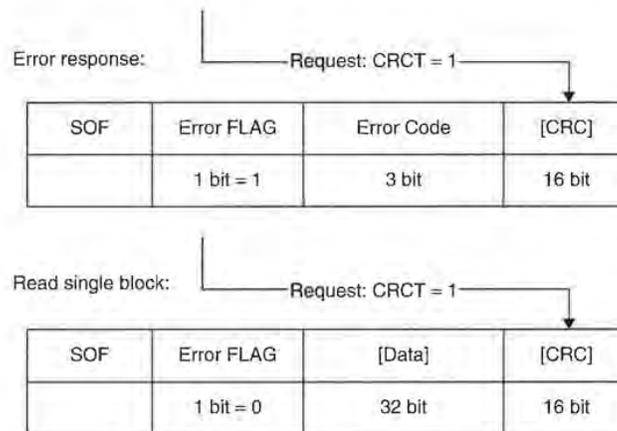


Figure 9.6 Structure of an ISO 14223 command frame for the transmission of data from reader to transponder

The structure of a command frame is identical for all types of transponder and is shown in Figure 9.6. The 5-bit command field allows 32 different commands to be defined. Command codes 00–19 are already defined in the standard and are supported in the same way by all advanced transponders. Command codes 20–31, on the other



**Figure 9.7** Structure of an ISO 14223 response frame for the transmission of data from transponder to the reader

hand, are freely definable by the chip manufacturer and can therefore be occupied by commands with an extremely wide range of functions. The parameters contain (in the case of read and write commands) the block address of a *memory block*, optionally the number of memory blocks to be processed by this command, and, again optionally, (ADR = 1) the previously determined UID in order to explicitly address a certain transponder. The four flags in the command frame facilitate the control of some additional options, such as an optional CRC at the end of the response frame (CRCT = 1), the explicit transponder addressing (ADR = 1) mentioned above, and access to the transponder in a special 'selected' status (SEL = 1).

The structure of the response frame is shown in Figure 9.7. This contains a flag that signals the error status of the transponder to the reader (error flag). The subsequent 3-bit status field contains a more precise interpretation of the error that has occurred.

The command set and the protocol structure of an advanced transponder correspond with the values defined in ISO 18000-2.

## 9.2 Contactless Smart Cards

There are currently three different standards for contactless smart cards based upon a broad classification of the range (Table 9.4).<sup>1</sup> See also Figure 9.8.

Most of the standard for close coupling smart cards — ISO 10536 — had already been developed by between 1992 and 1995. Due to the high manufacturing costs of this type of card<sup>2</sup> and the small advantages in comparison to contact smart cards,<sup>3</sup>

<sup>1</sup> The standards themselves contain no explicit information about a maximum range; rather, they provide guide values for the simple classification of the different card systems.

<sup>2</sup> The cards consist of a complex structure consisting of up to four inductive coupling elements and the same number of capacitive coupling elements.

<sup>3</sup> Close coupling smart cards also need to be inserted into a reader for operation, or at least precisely positioned on a stand.

Table 9.4 Available standards for contactless smart cards

Standard	Card type	Approximate range
ISO 10536	Close coupling	0–1 cm
ISO 14443	Proximity coupling	0–10 cm
ISO 15693	Vicinity coupling	0–1 m

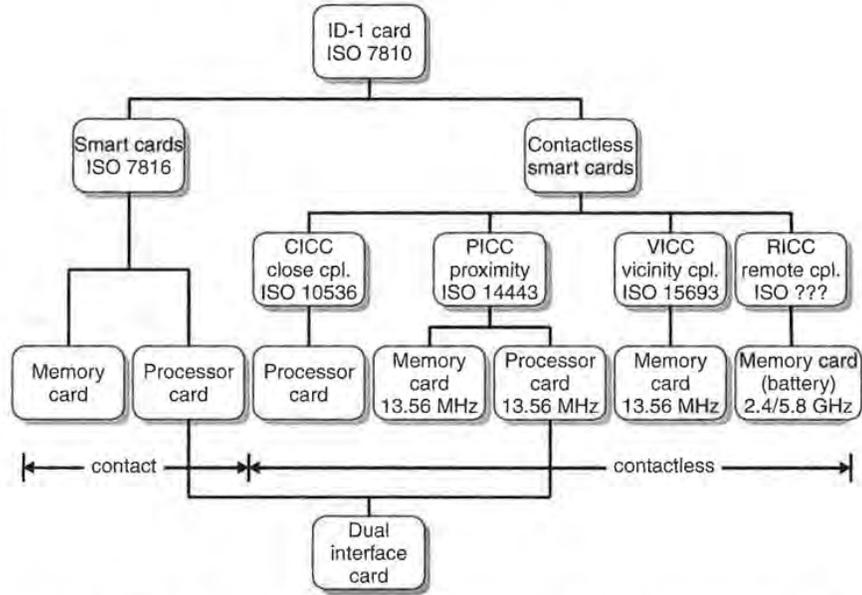


Figure 9.8 Family of (contactless and contact) smart cards, with the applicable standards

close coupling systems were never successful on the market and today they are hardly ever used.

### 9.2.1 ISO 10536 - Close coupling smart cards

The ISO standard 10536 entitled 'Identification cards — contactless integrated circuit(s) cards' describes the structure and operating parameters of contactless close coupling smart cards. *ISO 10536* consists of the following four sections:

- Part 1: Physical characteristics
- Part 2: Dimensions and location of coupling areas
- Part 3: Electronic signals and reset procedures
- Part 4: Answer to reset and transmission protocols (still under preparation)

### 9.2.1.1 Part 1 – Physical characteristics

The physical characteristics of close coupling cards are defined in Part 1 of the standard. The specifications regarding mechanical dimensions are identical to those for contact smart cards.

### 9.2.1.2 Part 2 – Dimensions and locations of coupling areas

Part 2 of the standard specifies the position and dimensions of the coupling elements. Both *inductive* (H1–4) and *capacitive coupling elements* (E1–4) are used. The arrangement of the coupling elements is selected so that a close coupling card can be operated in an insertion reader in all four positions (Figure 9.9).

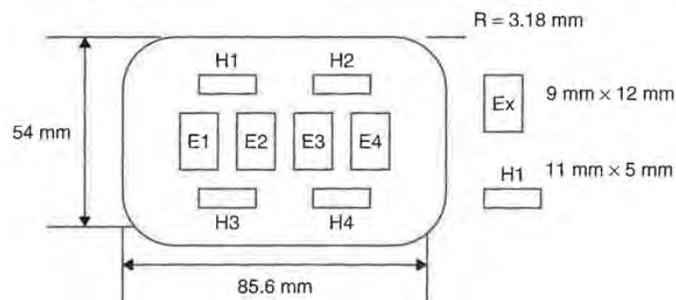
### 9.2.1.3 Part 3 – Electronic signals and reset procedures

**Power supply** The power supply for close coupling cards is derived from the four inductive coupling elements H1–H4. The inductive alternating field should have a frequency of 4.9152 MHz. The coupling elements H1 and H2 are designed as coils but have opposing directions of winding, so that if power is supplied to the coupling elements at the same time there must be a phase difference of  $180^\circ$  between the associated magnetic fields F1 and F2 (e.g. through a u-shaped core in the reader). The same applies for the coupling elements H3 and H4.

The readers must be designed such that power of 150 mW can be provided to the contactless card from any of the magnetic fields F1–F4. However, the card may not draw more than 200 mW via all four fields together.

**Data transmission card → reader** Either inductive or capacitive coupling elements may be used for data transmission between card and reader. However, it is not possible to switch between the two types of coupling during communication.

**Inductive Load modulation** with a *subcarrier* is used for the transmission of data via the coupling fields H1–H4. The *subcarrier frequency* is 307.2 kHz and the subcarrier is modulated using  $180^\circ$  PSK. The reader is designed such that a load change



**Figure 9.9** Position of capacitive (E1–E4) and inductive coupling elements (H1–H4) in a close coupling smart card

defined in Part 1 of the standard. identical to those for contact

**15 of coupling areas**

ons of the coupling elements. E1-4) are used. The arrange-coupling card can be operated

**reset procedures**

urds is derived from the four ernating field should have a nd H2 are designed as coils r is supplied to the coupling erence of 180° between the aped core in the reader). The

1mW can be provided to the However, the card may not

capacitive coupling elements r. However, it is not possible nunication.

used for the transmission of quency is 307.2 kHz and the igned such that a load change

= 3.18 mm

Ex 9 mm x 12 mm

H1 11 mm x 5 mm

upling elements (H1-H4) in a



**Figure 9.10** Half opened reader for close coupling smart cards in accordance with ISO 10536. In the centre of the insertion slot four capacitive coupling areas can be seen, surrounded by four inductive coupling elements (coils) (reproduced by permission of Denso Corporation, Japan — Aichi-ken)

of 10% of the base load at one or more of the fields F1-F4 can be recognised as a load modulation signal. The specified minimum load change for a card is 1 mW.

**Capacitive** In this procedure the coupling fields E1, E2 or E3, E4 are used as pairs. In both cases the paired coupling fields are controlled by a differential signal. The voltage difference  $U_{diff} = U_{E1} - U_{E2}$  should be measured such that a voltage level of at least 0.33 V is present at the reader coupling surfaces E1' and E2'. Data transmission takes place using *NRZ coding* in the baseband (i.e. no subcarrier). The data rate after reset is 9600 bit/s; however, a higher data rate can be used during operation.

**Data transmission reader → card** The standard gives preference to the inductive method for data transmission to the card. The modulation procedure is a 90° PSK of the fields F1-F4 and the phase position of all fields is modulated synchronously. Depending upon the position of the card in the insertion reader, the phase relationships shown in Tables 9.5 and 9.6 are possible between the coupling fields during modulation.

Data transmission takes place using *NRZ coding* in the baseband (i.e. no subcarrier). The data rate after reset is 9600 bit/s; however, a higher data rate can be used during operation.

**9.2.1.4 Part 4 - Answer to reset and transmission protocols**

This part of ISO 10536 describes the transmission protocol between reader and card. We will not describe Part 4 here because it is still under development by the standardisation committee in question, and may therefore be subject to change.

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

A	A'
$\Phi F$	$1\Phi'F1 = \Phi F1 - 90^\circ$
$\Phi F3 = \Phi F1 + 90^\circ$	$\Phi'F3 = \Phi F3 + 90^\circ$

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

A	A'
F1	$\Phi'F1 = \Phi'F1 + 90^\circ$
$\Phi F3 = \Phi F1 - 90^\circ$	$\Phi'F3 = \Phi'F3 - 90^\circ$

## 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.

ulated;

- 90°  
+ 90°

ulated;

+ 90°  
- 90°

**smart cards**

ximity integrated circuit(s) meters of contactless prox- : cards with an approximate field of ticketing. The data id they often have additional

ion).

the smart cards. The dimen- e. 85.72 mm × 54.03 mm ×

notes on the testing of the irradiation with UV, x-ray

**ence**

(PICC) is provided by the on frequency of 13.56 MHz.

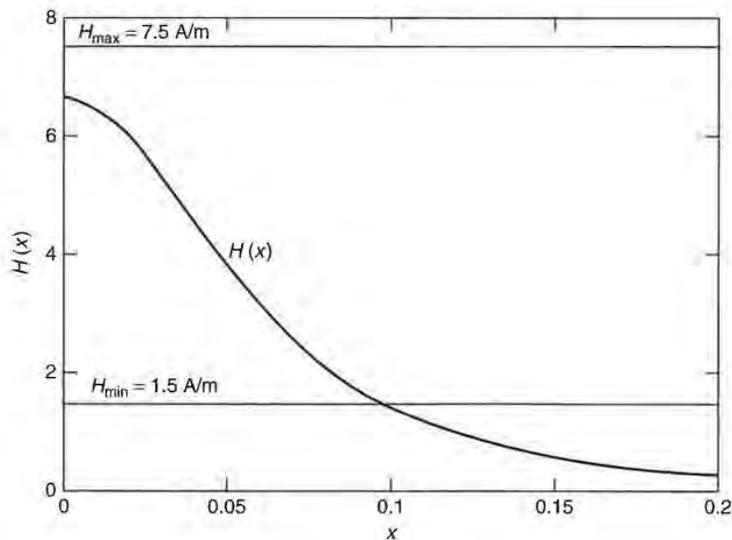
To this end the card incorporates a large area antenna coil typically with 3–6 windings of wire (see Figures 2.11 and 2.12).

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  $1.5 \text{ A/m}$  (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).

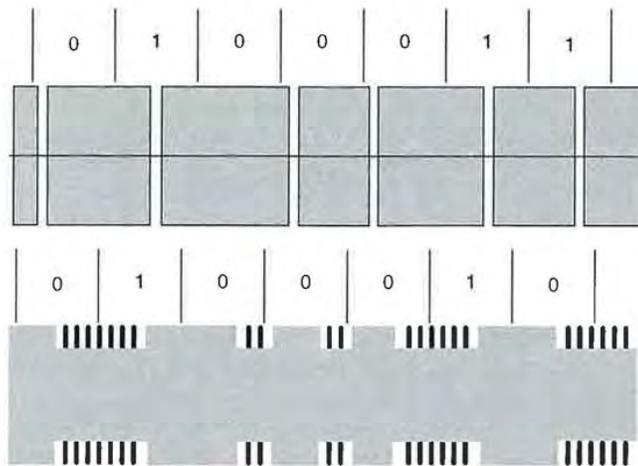
If the field strength curve of a reader and the interrogation field strength of a proximity coupling smart card are known, then the range of the system can be calculated. The field strength curve of a typical reader in accordance with ISO 14443 is shown in Figure 9.11 (see Section 4.1.1.1). In this case,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

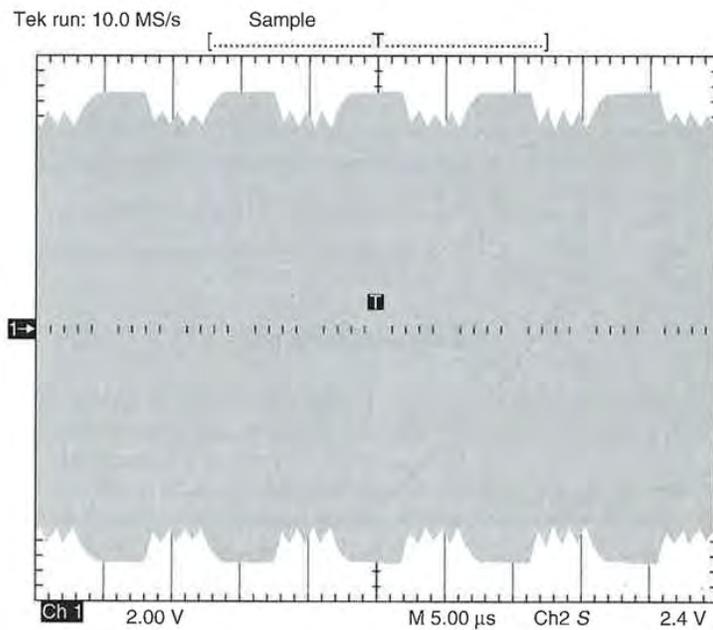
However, the reader may not switch between the two procedures during an existing communication relationship between reader and card.



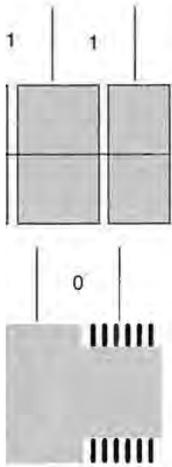
**Figure 9.11** Typical field strength curve of a reader for proximity coupling smart cards (antenna current  $i_1 = 1 \text{ A}$ , antenna diameter  $D = 15 \text{ cm}$ , number of windings  $N = 1$ )



**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



smart cards in accordance with modified Miller coding (voltage path with ASK modulated 847 kHz coil)



reader antenna by a Type A card

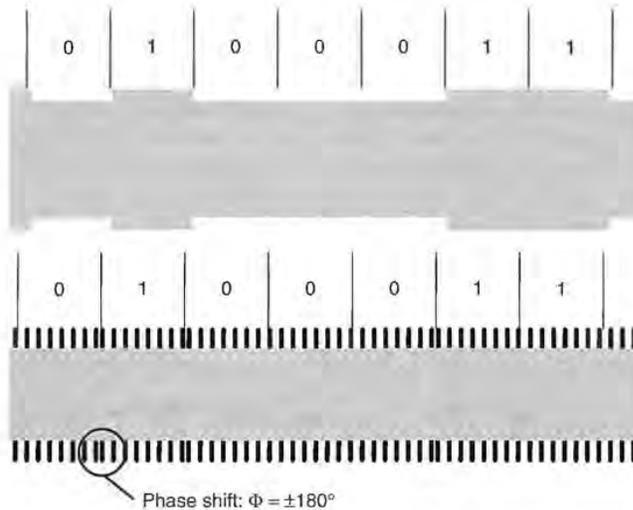
**Communication interface — Type A** In type A cards 100% ASK modulation with modified Miller coding (Figure 9.12) is defined as the modulation procedure used for the transfer of data from reader to card. In order to guarantee a continuous power supply to the card the length of the blanking intervals 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).

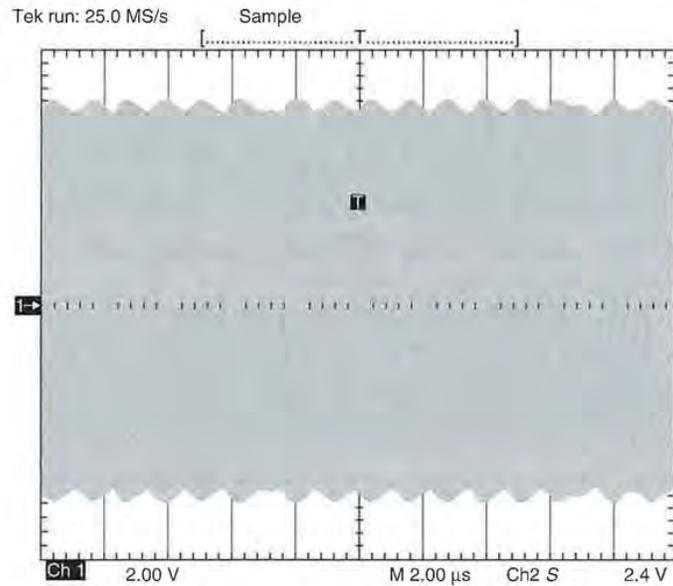
**Communication interface — Type B** In Type B cards 10% ASK modulation (Figure 9.14) is used as the modulation procedure for the data transfer from reader to card. A simple NRZ coding is used for bit coding. The transient response and transient characteristics of the HF signal in the 0/1 transitions 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)



**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 byte (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.



Figure 9.15: Antenna signal by a Type B card

(ICC) (Berger, 1998)

**Type B**

modulation index 8%–12%

1 stop bit per byte  
specification in Part 3)

(ICD) (Berger, 1998)

**Type B**

1 modulation with subcarrier  
17 kHz, BPSK modulated  
1 code  
1 stop bit per byte  
specification in Part 3)  
kBd

9.7 and 9.8 exist for the  
MIFARE system in accordance

**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*.<sup>4</sup> 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

<sup>4</sup> 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.

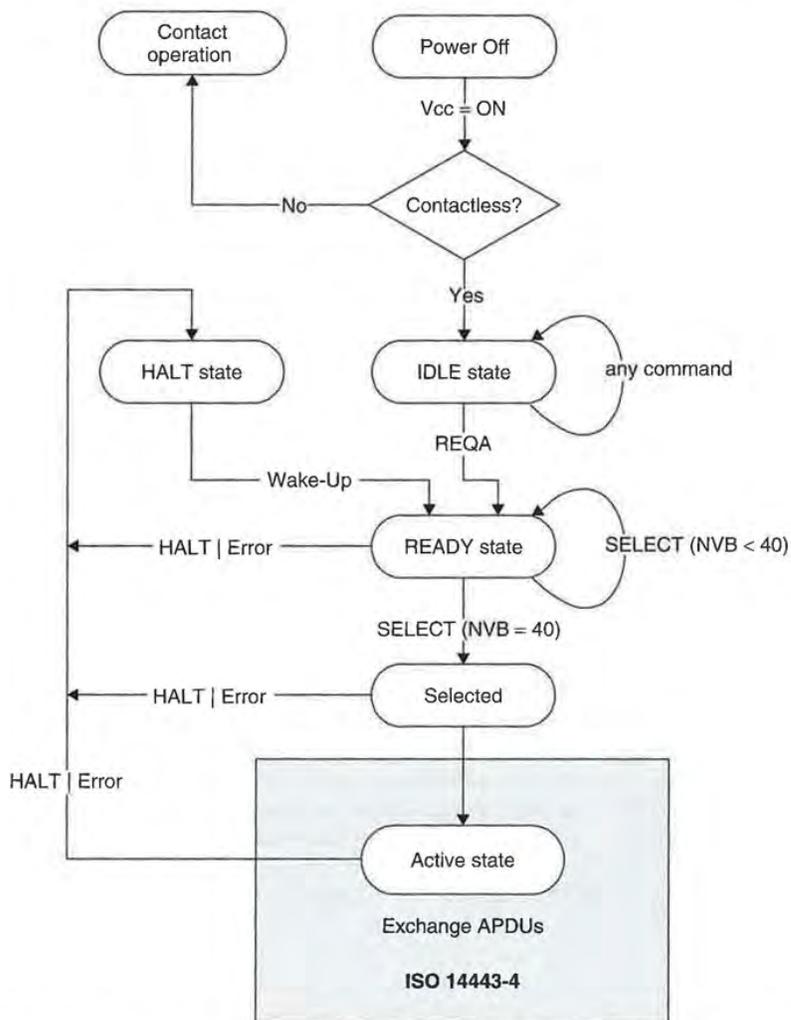


Figure 9.16 State diagram of a Type A smart card in accordance with ISO 14443 (Berger, 1998)

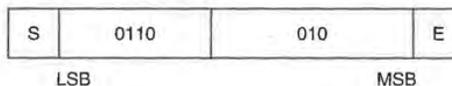
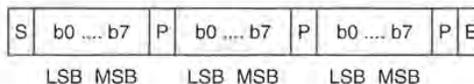
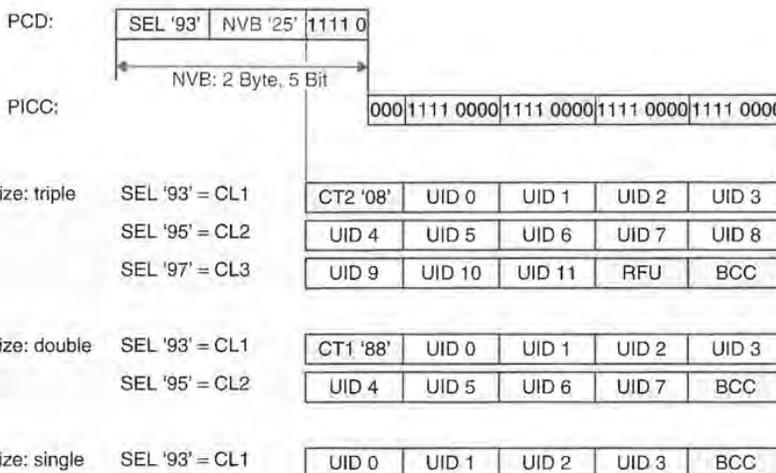
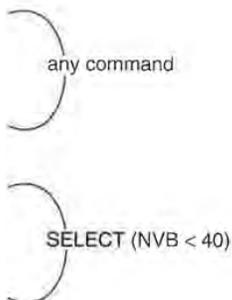


Figure 9.17 The reader's Request command for Type A cards (REQA) is made up of only 7 data bits. This reliably rules out the misinterpretation of useful data destined for another card as a REQUEST command (S = start of frame, E = end of frame)



**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 = 88h) 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,



ice with ISO 14443 (Berger,



B

(REQA) is made up of only data destined for another card

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 ( $N = 9, 10, 11, 12, \dots$ ).

**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*,<sup>5</sup> 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 (PUI, 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'	$t_{\text{RESPONSE}} = (n \cdot 128 + 20) \cdot t_0$

<sup>5</sup> 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.

defined moments in a fixed  
mand  $N = 9$ . For all other  
r than or equal to 9 ( $N =$

the interrogation field of a  
isation routines, is initially  
QUEST-B) command (see

ates the anticollision algo-  
mic *slotted ALOHA* proce-  
ranged by the reader. The  
er of the REQB command.  
card, the REQB command  
FI), which allows a certain  
9.10).

ks whether the application  
ications stored on the card.  
d to detect the number of  
of available slots is greater  
etermine the number of the  
e reader. In order to guar-  
ader transmits its own slot  
e slot marker of the previ-  
nd responds to the REQB  
e Figures 9.21 and 9.22.

(gure 9.23) the reader can  
ATQB within the current  
e transmission of the next

rovides the reader with a  
art card (Figure 9.22). In  
tains a 4-byte serial num-  
e B card is not necessarily  
f a random number, which  
o unique PICC identifier).

er response

**aviour**

$\{ + 84) \cdot t_0$

$\{ + 20) \cdot t_0$

ep introduction into the method

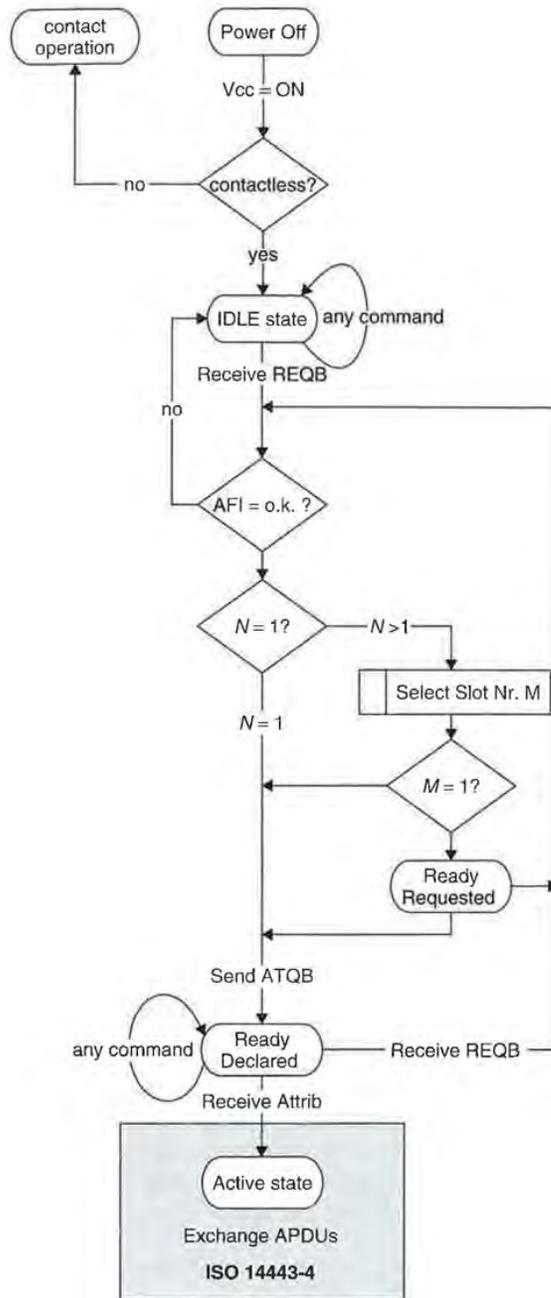


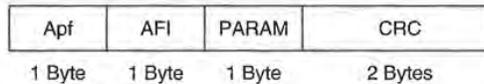
Figure 9.20 State diagram of a Type B smart card in accordance with ISO 14443

**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 <i>M</i> byte (bit 2-bit 0)	Number of slots <i>N</i>
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,<sup>6</sup> or information on alternative protocols. The 'Application Data' parameter can, moreover, include information on several applications available on the card (multi-application card).

<sup>6</sup>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.

preselection from a group of

**Comment**

roups and subgroups  
 an application group  
 of application group X  
 (transport, airlines, ...)  
 tickets, ...)  
 sport, driving licence)  
 n (telephone card, GSM, ...)  
 insurance card, ...)  
 net service, Pay-TV)  
 rd, lotto card)  
 'table files', ...)  
 re applications

by the parameter

**of slots N**

1  
 2  
 4  
 8  
 6  
 ture applications  
 ture applications

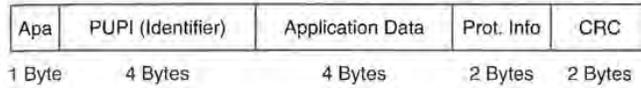


s

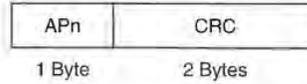
y rule out errors the anticollisions used in the NAD parameter

he 'Protocol Info' parameter smart card, the maximum 'Application Data' parameters available on the card

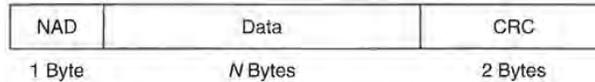
size of the available reception for most applications, the size of the



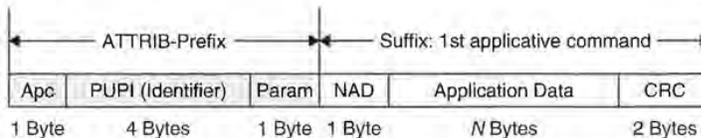
**Figure 9.22** Structure of an ATQB (Answer To Request B)



**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

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*.

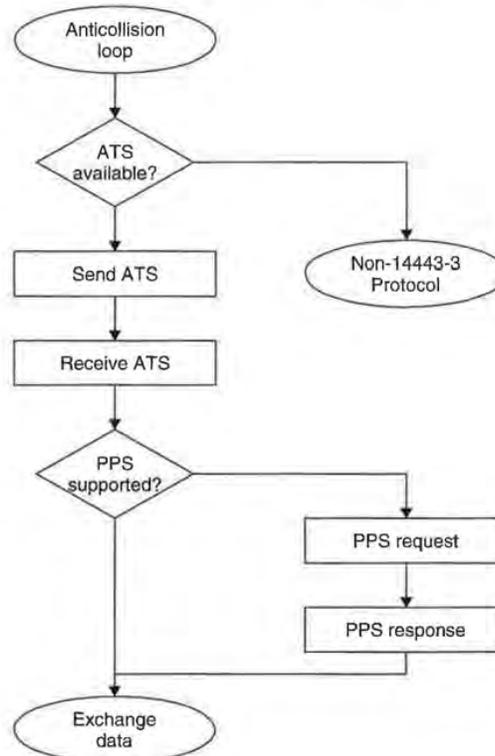


Figure 9.26 After anticollision the ATS of the card is requested

des the structure of the data  
mission errors, so that data  
s without errors.

figuration of the protocol to  
s, maximum size of the data  
formation has already been  
RIB), so in the case of this

ie A card in the anticollision  
 (select acknowledge). The  
cordance with ISO 14443-4  
has a proprietary protocol

able in the card, the reader  
a RATS command (request  
contains two parameters that  
d CID.

*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
FSDI	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 receive: 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	These parameters indicate whether the parameters CID (card identifier) and NAD (node address) are supported by the smart card's operating system
NAD supported	
Historical bytes	The historical bytes contain additional, freely definable information on the operating system of the smart card, e.g. a version number

143-3  
col

uest

onse

rd is requested

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.

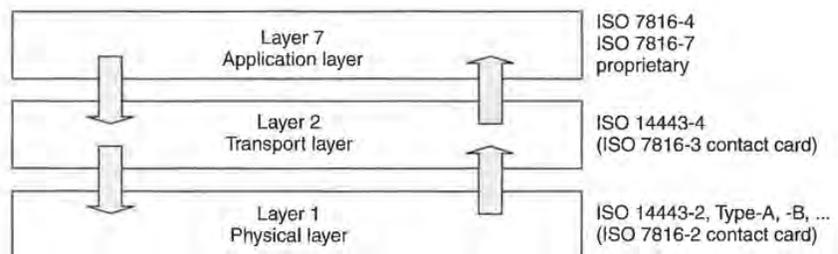


Figure 9.27 The ISO/OSI layer model in a smart card

e, in particular dual interface in ISO 14443-4 is therefore

also be represented in accor-

In this model, every layer is transparent to the level above it. The medium and the coding of the procedures here, Type A and B, and the handling of transmission data, i.e. the command data, are identical to those used in dual interface smart cards (which is independent of the command, contactless). Layers 3 to 6 are used for forwarding of data packets.

After the transmission of the command to the reader. The sequence is a command to the smart card to use back to the reader. This is the start of any communication with

transport layer is shown in blocks according to the method

the application layer (APDU)

errors

protocol.

ISO 7816-4  
ISO 7816-7  
proprietary

ISO 14443-4  
(ISO 7816-3 contact card)

ISO 14443-2, Type-A, -B, ...  
(ISO 7816-2 contact card)

smart card

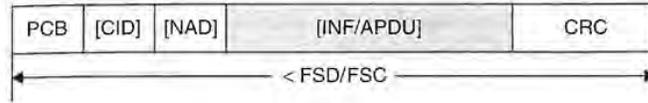


Figure 9.28 Structure of the frame in ISO 14443. The data of the application layer, Layer 7 (grey), are packed into the protocol frame of the transport layer (white)

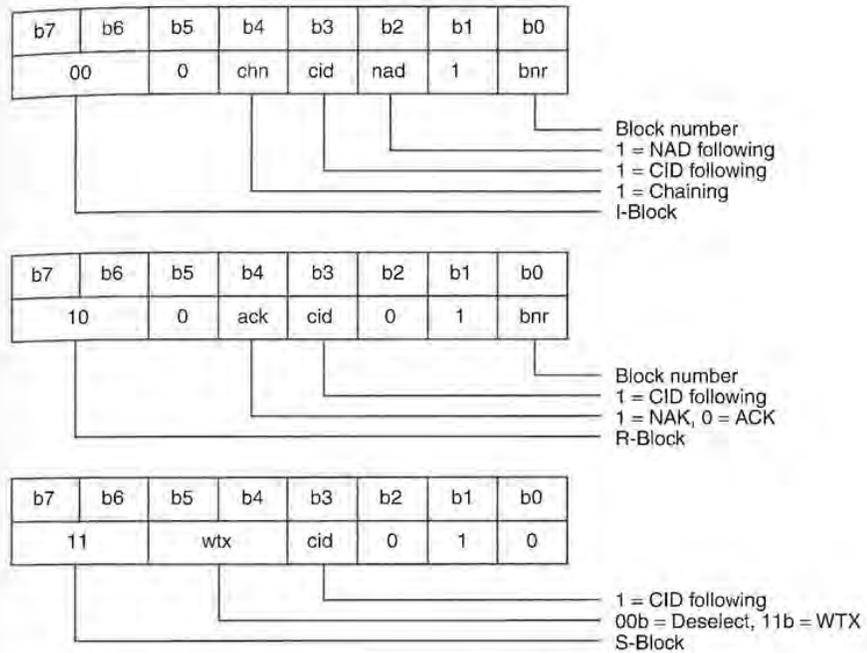


Figure 9.29 Coding of the PCB byte in a frame. The entire transmission behaviour is controlled by the PCB (protocol control byte) in the protocol

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.

### 9.2.3 ISO 15693 – Vicinity coupling smart cards

The ISO standard 15693 entitled ‘Identification cards — contactless integrated circuit(s) cards — Vicinity Cards’ describes the method of functioning and operating parameters of contactless *vicinity coupling smart cards*. These are smart cards with a range of up to 1 m, like those used in access control systems. The data carriers used in these smart cards are predominantly cheap memory modules with simple state machines (see Section 10.1.2.1).

The standard is made up of the following parts:

- Part 1: Physical characteristics
- Part 2: Radio frequency power, signal interface and frames (still in preparation)
- Part 3: Protocols (in preparation)
- Part 4: Registration of applications/issuers (in preparation)

#### 9.2.3.1 Part 1 – Physical characteristics

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

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

#### 9.2.3.2 Part 2 – Air interface and initialisation

The power supply of the inductively coupled *vicinity card (VICC)* is provided by the magnetic alternating field of a reader (*PCD*) at a transmission frequency of 13.56 MHz. The vicinity card incorporates a large area antenna coil for this purpose, typically with 3–6 windings of wire (see Figures 2.11 and 2.12).

The magnetic field to be generated by the reader must lie within the limit values  $115 \text{ mA/m} \leq H \leq 7.5 \text{ A/m}$ . Thus, it is automatically the case for the interrogation field strength  $H_{\min}$  of a proximity coupling smart card that  $H_{\min} \leq 115 \text{ mA/m}$ .

*Data transfer reader → card* Both 10% ASK and 100% ASK modulation are used for the data transfer from a reader to a vicinity smart card (see Section 6.2.1). Regardless of the selected modulation index, moreover, one of two different coding procedures can be selected: a ‘1 of 256’ code or a ‘1 of 4’ code.

A vicinity smart card must, in principle, support both modulation and coding procedures. However, not all combinations are equally practical. For example, 10% ASK modulation in combination with ‘1 of 256’ coding should be given preference in ‘long distance mode’. The lower field strength of the modulation sidebands in comparison to the field strength of the (13.56 MHz) carrier signal in this combination permits the full exploitation of the permissible magnetic field strength for the power supply of the

## Smart cards

contactless integrated circuit (IC) functioning and operating (these are smart cards with ICs) systems. The data carriers (IC modules with simple state

times (still in preparation)

on)

of proximity coupling smart cards as specified in ISO 7810,

additional notes for the testing of smart cards, plus irradiation with UV,

## Interrogation

(VICC) is provided by the carrier frequency of 13.56 MHz. For this purpose, typically with

fields lie within the limit values specified for the interrogation field  $\leq 115 \text{ mA/m}$ .

ASK modulation are used for smart cards (Section 6.2.1). Regardless of the different coding procedures

modulation and coding procedure. For example, 10% ASK modulation is given preference in 'long distance' sidebands in comparison with 100% ASK. This combination permits the use of the power supply of the

card (see FCC 15 Part 3: the permissible magnetic field strength of the modulation sidebands lies 50 dB below the maximum field strength of the carrier signal of  $42 \text{ dB}\mu\text{A/m}$  here). By contrast, 100% ASK modulation in combination with '1 of 4' coding in readers can be used with reduced range or even shielded readers ('tunnel' readers on conveyor belts).

**'1 of 256' coding** This coding procedure is a *pulse position modulation (PPM)* procedure. This means that the value of the digit to be transferred is unambiguously defined in the value range 0–255 by the time position of a modulation pulse (see Figure 9.30). Therefore, 8 bits (1 byte) can be transferred at the same time in one step. The total transmission time for a byte is 4.833 ms. This corresponds with 512 time slots of  $9.44 \mu\text{s}$ . A modulation pulse can only take place at an uneven time slot (counting begins at zero). The value  $n$  of a transferred digit can easily be determined from the pulse position:

$$\text{Pulse position} = (2 \cdot n) + 1 \quad (9.1)$$

The data rate resulting from the transmission period of a byte (4.833 ms) is 165 Kbit/s. The beginning and end of a data transmission are identified by defined frame signals — start-of-frame (SOF) and end-of-frame (EOF). The coding of the SOF and EOF signals selected in the standard is such that these digits cannot occur during a transmission of useful data (Figure 9.31). The unambiguity of the frame signals is thus always ensured.

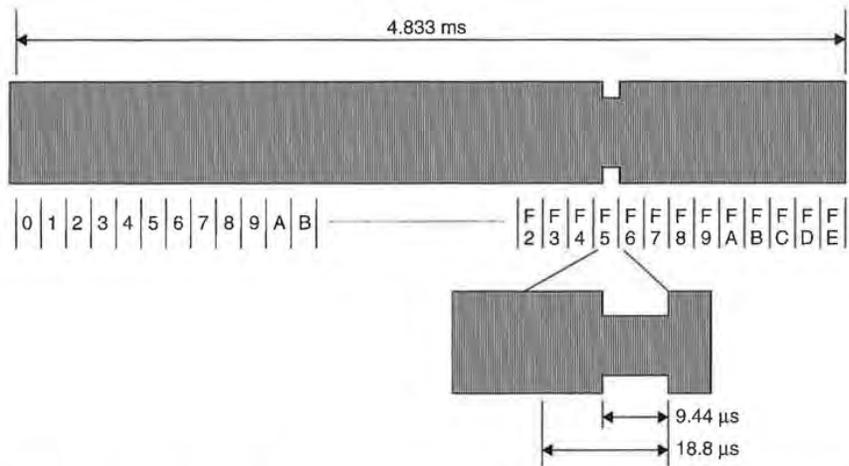
The SOF signal in '1 of 256' coding consists of two  $9.44 \mu\text{s}$  long modulation pulses separated by a time slot of  $56.65 \mu\text{s}$  ( $9.44 \mu\text{s} \times 4$ ) (Figure 9.32).

The EOF signal consists of a single modulation pulse lasting  $9.44 \mu\text{s}$ , which is sent at an even time slot in order to ensure its unambiguous differentiation from a data byte (Figure 9.33).

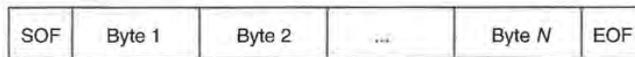
**'1 of 4' coding** In this coding too, the time position of a modulation pulse determines the value of a digit. Two bits are transmitted simultaneously in a single step; the value of the digit to be transferred thus lies in the value range 0–3. The total transmission time

**Table 9.13** Modulation and coding procedures in ISO 15693 (Berger, 1998)

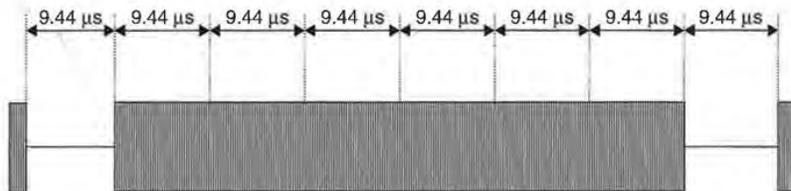
Parameter	Value	Comment
Power supply	$13.56 \text{ MHz} \pm 7 \text{ kHz}$	Inductive coupling
Data transfer reader → card		
Modulation	10% ASK, 100% ASK	Card supports both
Bit coding	'Long distance mode': '1 of 256' 'Fast mode': '1 of 4'	Card supports both
Baud rate	'Long distance mode': 1.65 Kbit/s 'Fast mode': 26.48 Kbit/s	
Data transfer card → reader		
Modulation	Load modulation with subcarrier	
Bit coding	Manchester, subcarrier is modulated with ASK (423 kHz) or FSK (423/485 kHz)	
Baud rate	'Long distance mode': 6.62 Kbit/s 'Fast mode': 26.48 Kbit/s	Selected by the reader



**Figure 9.30** The '1 of 256' coding is generated by the combination of 512 time slots of 9.44 μs length. The value of the digit to be transferred in the value range 0–255 can be determined from the position in time of a modulation pulse. A modulation pulse can only occur at an uneven time slot (1, 3, 5, 7, ...)



**Figure 9.31** Structure of a message block (framing) made up of frame start signal (SOF), data and frame end signal (EOF)

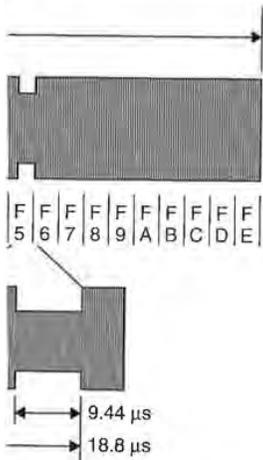


**Figure 9.32** Coding of the SOF signal at the beginning of a data transmission using '1 of 256' coding

for a byte is 75.52 μs, which corresponds with eight time slots of 9.44 μs. A modulation pulse can only be transmitted at an uneven time slot (counting begins at zero). The value *n* of a transmitted figure can easily be determined from the pulse position:

$$\text{Pulse position} = (2 \cdot n) + 1 \tag{9.2}$$

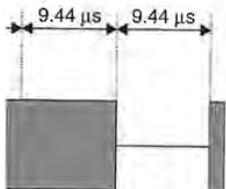
The data rate resulting from the time taken to transmit a byte (75.52 μs) is 26.48 Kbit/s.



in of 512 time slots of 9.44 μs -255 can be determined from can only occur at an uneven

byte N	EOF
--------	-----

frame start signal (SOF), data

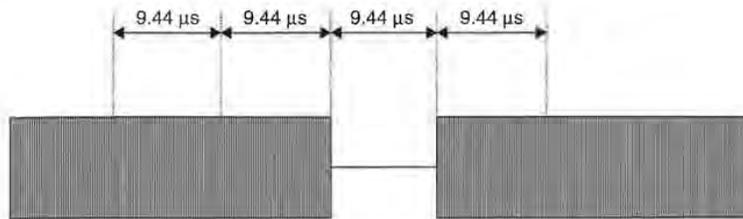


ata transmission using '1 of

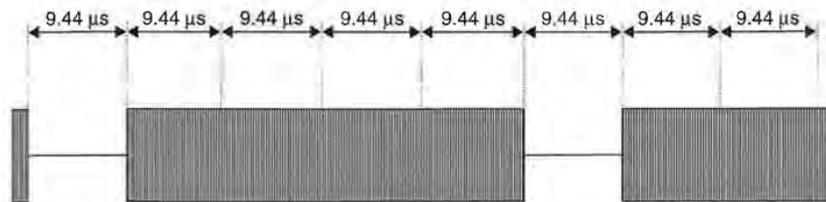
of 9.44 μs. A modulation (starting at zero). The position of the pulse position:

$$(9.2)$$

nit a byte (75.52 μs) is



**Figure 9.33** The EOF signal consists of a modulation pulse at an even time slot ( $t = 2$ ) and thus is clearly differentiated from useful data



**Figure 9.34** The SOF signal of '1 of 4' coding consists of two 9.44 μs long modulation pulses separated by an interval of 18.88 μs

In '1 of 4' coding the SOF signal is made up of two modulation pulses lasting 9.44 μs separated by an interval of 37.76 μs (Figure 9.34). The first digit of the useful data begins after an additional pause of 18.88 μs after the second modulation pulse of the SOF signal. See Figure 9.35.

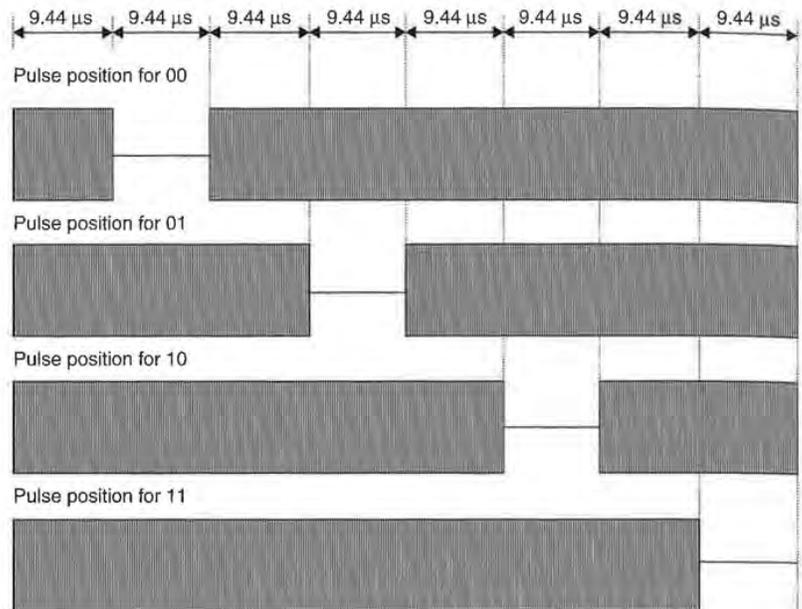
The conclusion of the transmission is identified by the familiar frame end signal (EOF).

*Data transfer card → reader* Load modulation with a modulated subcarrier is used for the data transfer from a vicinity card to a reader. The ohmic or capacitive modulation resistor is switched on and off in time with the subcarrier frequency. The subcarrier itself is modulated in time with the Manchester coded data stream, using ASK or FSK modulation (Table 9.14). The modulation procedure is selected by the reader using a flag bit (control bit) in the header of the transmission protocol defined in Part 3 of the standard. Therefore, in this case too, both procedures must be supported by the smart card.

The data rate can also be switched between two values (Table 9.15). The reader selects the data rate by means of a flag bit (control bit) in the header of the transmission protocol, which means that, in this case too, the card must support both procedures.

**Table 9.14** Subcarrier frequencies for an ASK and FSK modulated subcarrier

	ASK 'on-off keying'	FSK
Subcarrier frequency	423.75 kHz	423.75 kHz/484.28 kHz
Divider ratio to $f_c = 13.56$ MHz	$f_c/32$	$f_c/32; f_c/28$



**Figure 9.35** '1 of 4' coding arises from the combination of eight time slots of 9.44 μs length. The value of the digit to be transmitted in the value range 0–3 can be determined from the time position of a modulation pulse

**Table 9.15** Data rates of the two transmission modes

Data rate	ASK ('on-off keying')	FSK
'Long distance mode'	6.62 Kbit/s	6.62 Kbit/s/6.68 Kbit/s
'Fast mode'	26.48 Kbit/s	26.48 Kbit/s/26.72 Kbit/s

#### 9.2.4 ISO 10373 – Test methods for smart cards

ISO 10373 provided a standard relating to the testing of cards with and without a chip. In addition to tests for the general quality characteristics, such as bending stiffness, resistance to chemicals, dynamic torsional stress, flammability, and dimensions of cards or the ultra-violet light resistance of the data carrier (since EEPROM memories lose their content when irradiated with UV light a special test has been developed to ensure non-sensitivity to this), specific test procedures have also been developed for the latest methods of data transmission or storage (magnetic strips, contact, contactless, optical). The individual test procedures for testing magnetic strips (ISO 7811), contact smart cards (ISO 7816) or contactless smart cards (ISO 14443, ISO 15693) were summarised in independent parts of the standard for the sake of providing an overview (Table 9.16). However, in this section we will deal exclusively with the parts of the standard that are relevant to RFID systems, i.e. Part 4, Part 6 and Part 7.

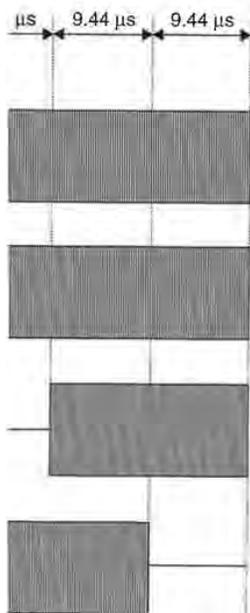


Figure 9.16 shows four time slots of 9.44 μs length. The time slots can be determined from the time

Transmission modes

FSK
6.62 Kbit/s/6.68 Kbit/s
12.648 Kbit/s/26.72 Kbit/s

**Smart cards**

Smart cards with and without a chip. Factors such as bending stiffness, mechanical strength, and dimensions of cards containing EEPROM memories lose mechanical strength. A test method has been developed to ensure mechanical strength. It has been developed for the latest smart cards (contact, contactless, optical). The test methods (ISO 7811), contact smart cards (ISO 15693) were summarised in Table 9.16. Table 9.16 is an overview (Table 9.16). Table 9.16 is an overview of the parts of the standard that

**Table 9.16** DIN/ISO 10373, 'Identification Cards — Test methods'

Part 1	General
Part 2	Magnetic strip technologies
Part 3	Integrated circuit cards (contact smart cards)
Part 4	Contactless integrated circuit cards (close coupling smart cards in accordance with ISO 10536)
Part 5	Optical memory cards
Part 6	Proximity cards (contactless smart cards in accordance with ISO 14443)
Part 7	Vicinity cards (contactless smart cards in accordance with ISO 15693) — currently still in preparation

**9.2.4.1 Part 4: Test procedures for close coupling smart cards**

This part of the standard describes procedures for the *functional testing* of the physical interface of contactless *close coupling smart cards* in accordance with ISO 10536. The test equipment consists of defined coils and capacitive coupling areas, which facilitate the evaluation of the power and data transmission between smart card and reader.

However, due to the secondary importance of close coupling smart cards we will not investigate this procedure further at this point.

**9.2.4.2 Part 6: Test procedures for proximity coupling smart cards**

This part of the standard describes test procedures for the *functional testing* of the physical interface between contactless *proximity coupling smart cards* and readers in accordance with ISO 14443-2. The test equipment consists of a *calibration coil*, a test setup for the measurement of the load modulation (PCD assembly test) and a *reference card* (reference PICC). This equipment is defined in the standard.

**Calibration coil** To facilitate the measurement of the magnetic field strength generated by a reader without complicated and expensive measuring equipment, the standard first describes the layout of a calibration coil that permits the measurement of magnetic field strengths in the frequency range of 13.56 MHz with sufficient accuracy even with a simple oscilloscope.

The calibration coil is based upon an industry-standard copper coated FR4 printed circuit board and smart card dimensions in accordance with ISO 7810 (72 mm × 42 mm × 0.76 mm). A conductor coil (i.e. a coil with one winding) with dimensions 72 mm × 42 mm is applied onto this base board using the normal procedure for the manufacture of printed circuits. The sensitivity of the calibration coil is 0.3 Vm/A. However, during the field strength measurement particular care should be taken to ensure that the calibration coil is only subjected to high-ohmic loads by the connected measuring device (sensing head of an oscilloscope), as every current flow in the calibration coil can falsify the measurement result.

If the measurement is performed using an oscilloscope, then the calibration coil is also suitable for the evaluation of the switching transitions of the ASK modulated

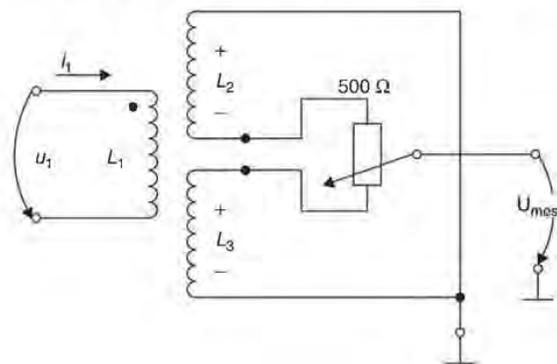
signal from a reader. Ideally, a reader under test will also have a test mode, which can transmit the endless sequence 10101010 for the simpler representation of the signal on the oscilloscope.

**Measuring the load modulation** The precise and reproducible measurement of the load modulation signal of a proximity coupling smart card at the antenna of a reader is very difficult due to the weak signal. In order to avoid the resulting problems, the standard defines a measuring bridge, which can be used to compensate the reader's (or test transmitter's) own strong signal. The measuring arrangement for this described in the standard consists of a *field generator coil* (transmission antenna) and two parallel sensor coils in phase opposition. The two sensor coils ('reference coil' and 'sense coil') are located on the front and back of the field generator coil, each at the same distance from it, and are connected in phase opposition to one another (Figures 9.36 and 9.37), so that the voltages induced in the coils cancel each other out fully. In the unloaded state, i.e. in the absence of a load from a smart card or another magnetically coupled circuit, the output voltage of this circuit arrangement therefore tends towards zero. A low residual voltage, which is always present between the two sensor coils as a result of tolerance-related asymmetries, can easily be compensated by the potentiometer.

The following procedure should be followed for the implementation of the measurement.

The smart card to be tested is first placed on the measuring bridge in the centre of the sense coil. As a result of the current flowing through the smart card coil, a voltage  $u_s$  is induced in the neighbouring sense coil. This reduces the symmetry of the measurement arrangement, so that an offset voltage is set at the output of the measurement circuit. To prevent the falsification of the measurement by an undefined offset voltage, the symmetry of the measurement arrangement must be recreated with the measurement object in place by tuning the potentiometer. The potentiometer is correctly set when the output voltage of the measurement bridge reaches a minimum ( $\rightarrow 0$ ).

After the measurement bridge has been adjusted, the reader connected to the field coil sends a REQUEST command to the smart card under test. Now, if the smart card begins to send a response to the reader by load modulation, the symmetry of



**Figure 9.36** Measuring bridge circuit for measuring the load modulation of a contactless smart card in accordance with ISO 14443

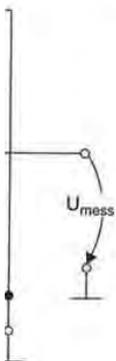
ave a test mode, which can  
resentation of the signal on

lucible measurement of the  
l at the antenna of a reader  
the resulting problems, the  
compensate the reader's (or  
ement for this described in  
1 antenna) and two parallel  
'reference coil' and 'sense  
ator coil, each at the same  
one another (Figures 9.36  
each other out fully. In the  
t card or another magnet-  
rrangement therefore tends  
ent between the two sensor  
ily be compensated by the

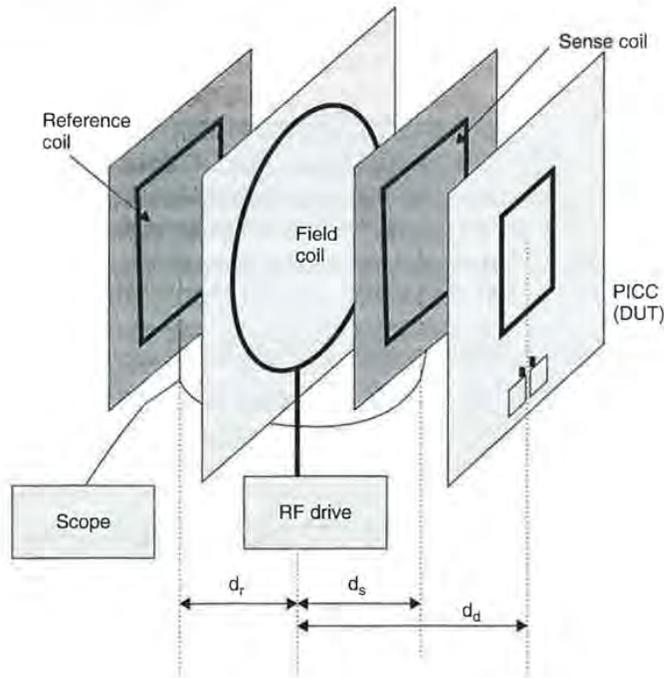
ie implementation of the

g bridge in the centre of the  
art card coil, a voltage  $u_s$  is  
metry of the measurement  
of the measurement circuit.  
defined offset voltage, the  
ted with the measurement  
meter is correctly set when  
nimum ( $\rightarrow 0$ ).

ader connected to the field  
er test. Now, if the smart  
dulation, the symmetry of



ulation of a contactless smart

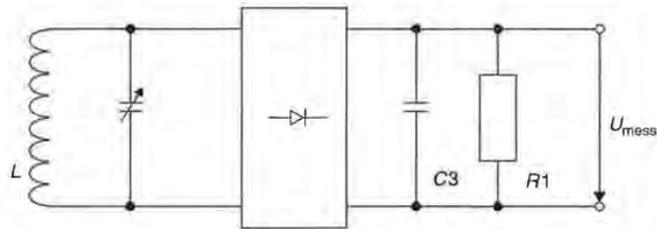


**Figure 9.37** Mechanical structure of the measurement bridge, consisting of the field generator coil (field coil), the two sensor coils (sense and reference coil) and a smart card (PICC) as test object (DUT) (reproduced by permission of Philips Semiconductors, Hamburg)

the measuring bridge is disrupted in time with the switching frequency (this corresponds with the subcarrier frequency  $f_s$ ) as a result of the modulation resistor in the smart card being switched on and off. As a result, a subcarrier modulated HF voltage can be measured at the measurement output of the measuring bridge. This signal is sampled over several periods using a digital oscilloscope and then brought into the frequency range by a discrete Fourier transformation. The amplitudes of the two modulation sidebands  $f_c \pm f_s$  that can be seen in the frequency range now serve as the quality criterion for the load modulator and should exceed the limit value defined in ISO 14443.

The layout of the required coils, a circuit to adapt the field coil to a  $50 \Omega$  transmitter output stage, and the precise mechanical arrangement of the coils in the measuring arrangement are specified in the Annex to the standard, in order to facilitate its duplication in the laboratory (see Section 14.4).

**Reference card** As a further aid, the standard defines two different reference cards that can be used to test the power supply of a card in the field of the reader, the transient response and transient characteristics of the transmitter in the event of ASK modulation, and the demodulator in the reader's receiver.



**Figure 9.38** Circuit of a reference card for testing the power supply of a contactless smart card from the magnetic HF field of a reader

**Power supply and modulation** With the aid of a defined *reference card* it is possible to test whether the magnetic field generated by the reader can provide sufficient energy for the operation of a contactless smart card. The principal circuit of such a reference card is shown in Figure 9.38. This consists primarily of a transponder resonant circuit with adjustable resonant frequency, a bridge rectifier, and a set of load resistors for the simulation of the data carrier.

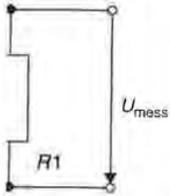
To carry out the test, the reference card is brought within the interrogation zone of a reader (the spatial characteristics of the reader's interrogation field are defined by the manufacturer of this device and should be known at the start of the measurement). The output voltage  $U_{\text{meas}}$  of the reference card is now measured at defined resonant frequencies ( $f_{\text{res}} = 13\text{--}19$  MHz) and load resistances ( $910\ \Omega$ ,  $1800\ \Omega$ ) of the reference card. The test has been passed if the voltage within the interrogation zone does not fall below a lower limit value of 3 V.

**Load modulation** A second *reference card* can be used to provide a test procedure that makes it possible to test the adherence of the receiver in the reader to a minimum necessary sensitivity. The circuit of this test card largely corresponds with the circuit from Figure 9.38, but it has an additional load modulator.

To carry out the test, this reference card is brought into the interrogation zone of a reader, this interrogation zone being defined by the manufacturer. The reference card thus begins to transmit a continuous subcarrier signal (847 kHz in accordance with ISO 14443) by load modulation to the reader and this signal should be recognised by the reader within a defined interrogation zone. The reader under test ideally possesses a test mode for this purpose, in which the operator can be alerted to the detection of a continuous subcarrier signal.

#### 9.2.4.3 Part 7: Test procedure for vicinity coupling smart cards

This part of the standard describes test procedures for the functional testing of the physical interface between contactless smart cards and readers in accordance with ISO 15693-2. The test equipment and testing procedure for this largely correspond with the testing equipment defined in Part 6. The only differences are the different subcarrier frequencies in the layout of the reference card (simulation of load modulation) and the different field strengths in operation.



supply of a contactless smart

a defined reference card it by the reader can provide rd. The principal circuit of primarily of a transponder : rectifier, and a set of load

n the interrogation zone of gation field are defined by start of the measurement). asured at defined resonant 2, 1800 Ω) of the reference interrogation zone does not

to provide a test procedure n the reader to a minimum rresponds with the circuit

the interrogation zone of a cturer. The reference card Hz in accordance with ISO ould be recognised by the er test ideally possesses a erted to the detection of a

**coupling**

functional testing of the rs in accordance with ISO argely correspond with the re the different subcarrier : load modulation) and the

**9.3 ISO 69873 – Data Carriers for Tools and Clamping Devices**

This standard specifies the dimensions for contactless data carriers and their mounting space in tools and cutters (Figure 9.39). Normally the data carriers are placed in a quick release taper shaft in accordance with ISO 69871 or in a retention knob in accordance with ISO 69872. The standard gives installation examples for this.

The dimensions of a data carrier are specified in ISO 69873 as  $d_1 = 10\text{ mm}$  and  $t_1 = 4.5\text{ mm}$ . The standard also gives the precise dimensions for the mounting space.

**9.4 ISO 10374 – Container Identification**

This standard describes an automatic identification system for containers based upon microwave transponders. The optical identification of containers is described in the standard ISO 6346 and is reflected in the data record of the transponder-based container identification.

Active — i.e. battery supported — microwave transponders are used. These are activated by an unmodulated carrier signal in the frequency ranges 850–950 MHz and 2400–2500 MHz. The sensitivity of the transponder is defined with an electric field strength  $E$  of a maximum of 150 mV/m. The transponder responds by backscatter modulation (modulated reflection cross-section), using a modified FSK subcarrier procedure (Figure 9.40). The signal is modulated between the two subcarrier frequencies 40 kHz and 20 kHz.

The transmitted data sequence corresponds with the example in Table 9.17.

**9.5 VDI 4470 – Anti-theft Systems for Goods**

**9.5.1 Part 1 – Detection gates – inspection guidelines for customers**

The VDI 4470 guideline provides a practical introduction to the inspection and testing of installed systems for electronic article surveillance (EAS) systems (see Figure 9.41).

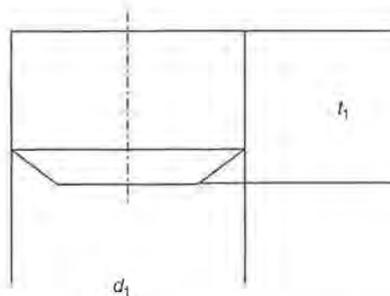


Figure 9.39 Format of a data carrier for tools and cutters

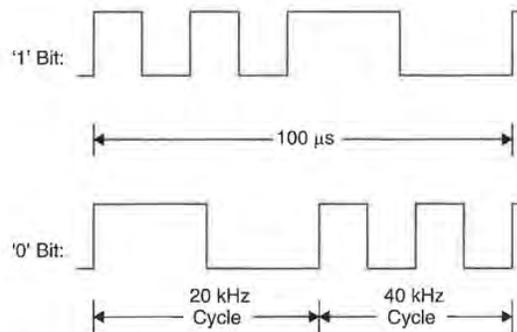


Figure 9.40 Coding of data bits using the modified FSK subcarrier procedure

Table 9.17 Data sequence of a container transponder

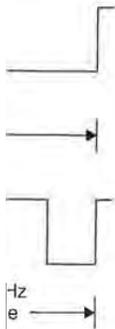
Bit number	Data	Unit	Minimum value	Maximum value
0-4	Object recognition	—	1	32
5-6	Reflector type	Type code	0	3
7-25	Owner code	alphabetic	AAAA	ZZZZ
26-45	Serial number	numeric	000000	999999
46-49	Check digit	numeric	0	9
50-59	Length	Centimetre	1	2000
60-61	Checksum	—	—	—
62-63	Structure bits	—	—	—
64	Length	—	—	—
65-73	Height	Centimetre	1	500
74-80	Width	Centimetre	200	300
81-87	Container format	Type code	0	127
88-96	Laden weight	100 kg	19	500
97-103	Tare weight	100 kg	0	99
104-105	Reserve	—	—	—
106-117	Security	—	—	—
118-123	Data format code	—	—	—
124-125	Check sum	—	—	—
126-127	Data frame end	—	—	—

It describes definitions and test procedures for checking the decisive system parameters — the *false alarm rate* and the *detection rate*.

The term 'false alarms' is used to mean alarms that are not triggered by an active security tag, whereas the detection rate represents the ratio of alarms to the total number of active tags.

### 9.5.1.1 Ascertaining the false alarm rate

The number of false alarms should be ascertained immediately after the installation of the EAS system during normal business. This means that all equipment, e.g. tills



K subcarrier procedure

ansponder

m value	Maximum value
1	32
0	3
AA	ZZZZ
000	999999
0	9
1	2000
-	—
-	—
-	—
i	500
200	300
0	127
19	500
0	99
-	—
-	—
-	—
-	—

e decisive system param-

not triggered by an active  
f alarms to the total number

ately after the installation  
at all equipment, e.g. tills



**Figure 9.41** Electronic article surveillance system in practical operation (reproduced by permission of METO EAS-System 2002, Esselte Meto, Hirschborn)

and computers, are in operation. During this test phase the products in the shop should not be fitted with security tags. During a monitoring period of one to three weeks an observer records all alarms and the conditions in which they occur (e.g. person in gates, cleaning, storm). Alarms that are caused by a security tag being carried through the gates by accident (e.g. a tag brought from another shop) are not counted.

### 9.5.1.2 Ascertaining the detection rate

The detection rate may be ascertained using either real or artificial products.

*Real products* In this case a number of representative products vulnerable to theft are selected and carried through the gateways by a test person in a number of typical hiding places — hood, breast pocket, shoe, carrier bag, etc. When selecting test products, remember that the material of a product (e.g. metal surfaces) may have a quite marked effect on the detection rate.

The detection rate of a system is calculated as the proportion of alarms triggered to the totality of tests carried out.

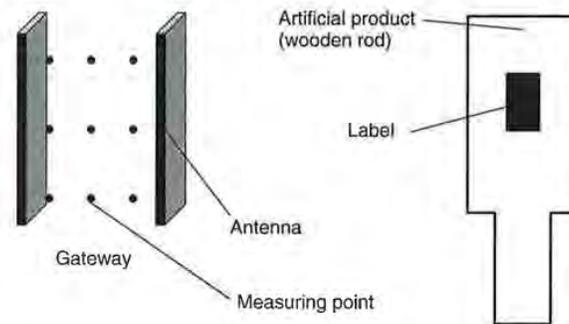
*Artificial products* This test uses a wooden rod with a tag in the form of a label attached to the middle. A test person carries this reference object through reference points in the gateway that are precisely defined by VDI 4470 at a constant speed. See Figure 9.42.

The detection rate of a system is calculated as the proportion of alarms triggered to the totality of tests carried out.

### 9.5.1.3 Forms in VDI 4470

In order to simplify the testing of objects and to allow tests to be performed in a consistent manner in all branches, VDI 4470 provides various forms:

- Form 1: 'Test for False Alarms'
- Form 2: 'Test with Real Products'



**Figure 9.42** Left, measuring points in a gateway for inspection using artificial products; right, artificial product

- Form 3a: 'Test with Artificial Products'
- Form 3b: 'Test with Artificial Products'
- Form 4a: 'Test with Artificial Products'
- Form 4b: 'Test with Artificial Products'

### 9.5.2 Part 2 – Deactivation devices, inspection guidelines for customers

As well as the option of removing hard tags (e.g. microwave systems) at the till, various tags can also be 'neutralised', i.e. deactivated (e.g. RF procedure, electromagnetic procedure).

The objective is to achieve the complete deactivation of all tags placed in a *deactivation device*, in order to avoid annoying or worrying customers by unjustified false alarms. Deactivation devices must therefore generate optical or acoustic signals, which indicate either a successful or an unsuccessful deactivation.

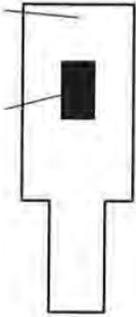
Deactivation devices are tested during the normal activities of the shop. A minimum of 60 protected products are required, which are checked for functionality before and after the test. The protected products are each put into/onto the deactivation device one after the other and the output from the signalling device recorded.

To ascertain the *deactivation rate* the successfully deactivated tags are divided by the total number of tags. This ratio must be 1, corresponding with a 100% deactivation rate. Otherwise, the test has not been successful.

## 9.6 Item Management

### 9.6.1 ISO 18000 series

A whole range of new standards on the subject of *item management* are currently under development. The purpose of these standards is ensure that *item management*



using artificial products; right,

## specification

rowave systems) at the till,  
RF procedure, electromag-

if all tags placed in a *deac-*  
stomers by unjustified false  
il or acoustic signals, which  
1.

ies of the shop. A minimum  
for functionality before and  
the deactivation device one  
ecorded.

ctivated tags are divided by  
tag with a 100% deactivation

*management* are currently  
sure that *item management*

requirements are taken into account in future transponder generations. The following standards are planned:

- ISO 15961: 'RFID for *Item Management*: Host Interrogator; Tag functional commands and other syntax features'
- ISO 15962: 'RFID for *Item Management*: Data Syntax'
- ISO 15963: 'Unique Identification of RF tag and Registration Authority to manage the uniqueness'
  - Part 1: Numbering System
  - Part 2: Procedural Standard
  - Part 3: Use of the unique identification of RF tag in the integrated circuit.
- ISO 18000: 'RFID for *Item Management*: Air Interface'
  - Part 1: Generic Parameter for Air Interface Communication for Globally Accepted Frequencies
  - Part 2: Parameters for Air Interface Communication below 135 kHz
  - Part 3: Parameters for Air Interface Communication at 13.56 MHz
  - Part 4: Parameters for Air Interface Communication at 2.45 GHz
  - Part 5: Parameters for Air Interface Communication at 5.8 GHz
  - Part 6: Parameters for Air Interface Communication — UHF Frequency Band
- ISO 18001: 'Information technology — RFID for *Item Management* — Application Requirements Profiles'

### 9.6.2 GTAG initiative

A further initiative, GTAG (Global Tag; see Figure 9.43) is jointly supported by the EAN (European Article Numbering Association) and the UCC (Universal Code Council). According to a statement by the two organisations themselves, the work of EAN and UCC is 'to improve supply chain management and other business processes that reduce costs and/or add value for both goods and services, EAN International and UCC develop, establish and promote global, open standards for identification and communication for the benefit of the users involved and the ultimate consumer' (EAN.UCC, 1999).

EAN.UCC systems are used worldwide by almost a million companies from extremely different industries for the identification of goods. The best known is the barcode, which can be found upon all consumer goods, and which is read at the supermarket till. The codes used, however, do not facilitate the classification of the



Radio Frequency Identification (RFID)  
Performance Standards Initiative

Figure 9.43 Official logo of the GTAG initiative (<http://www.ean-int.org>)

goods, but serve only as a unique identification (AI = *Application Identifier*) that allows the item to be looked up in a database.

Electronic Document Interchange (EDI) (defined in UN/EDIFACT) represents a further field of application of EAN.UCC systems (EAN.UCC, 2000).

The specifications currently under development facilitate the coexistence of *barcode* and transponder with full compatibility from the point of view of the user. This permits the flowing migration from barcodes to transponder systems, with the focus initially being placed upon applications relating to *transport containers* and reusable packaging (Osborne, n.d.). The requirements of such standardisation are diverse, since all parameters of such a system must be precisely specified in order to guarantee that the transponder can be implemented universally. The GTAG specification of EAN.UCC will therefore deal with three layers: the transport layer, the communication layer, and the application layer.

- The **transport layer** describes the physical interface between transponder and reader, i.e. transmission frequency, modulation frequency and data rate. The most important factor here is the selection of a suitable frequency so that EAN.UCC systems can be used worldwide without restrictions and can be manufactured at a low cost. Furthermore, the GTAG specification for the transport layer will flow into the future ISO 18000-6 standard (Osborne, n.d.).
- The **communication layer** describes the structure of the data blocks that are exchanged between transponder and reader. This also includes the definition of an anticollision procedure, plus the description of commands for the reading or writing of the transponder.
- The **application layer** includes the organisation and structure of the application data stored on the transponder. GTAG transponders will include at least an EAN.UCC Application Identifier (AI) (EAN.UCC, 2000). This AI was developed for data carriers with low storage capacity (barcodes). RFID transponders, however, permit additional data and provide the option of changing data in the memory, so that the GTAG specification will contain optional data fields and options.

The completion of the GTAG specification is planned for 2002 at the earliest. For this reason, only a brief overview of the technical details can be given in what follows.

### 9.6.2.1 GTAG transport layer (physical layer)

In order to be able to fulfil the requirements of range and transmission speed imposed on GTAG, the *UHF frequency range* has been selected for the transponders. However, one problem in this frequency range is local differences in frequency regulations. For example, 4 W transmission power is available for RFID systems in the frequency range 910–928 MHz in America. In Europe, on the other hand, the ERO (European Radio-communications Organisation) is currently being lobbied to allocate 2 W transmission power to the frequency range 865.6–867.6 MHz. Due to the different frequency ranges of the readers, GTAG transponders are designed so that they can be interrogated by a reader over the entire 862–928 MHz frequency range. It makes no difference in

**Table 9.18** Provisional technical parameters of a GTAG reader

Parameter	Value
Transmission frequency and power of the reader	862–928 MHz, 2–4 W (depending upon regulations)
Downlink	40% ASK Pulse Time Modulation, '1 of 5' coding
Anticollision procedure	Dynamic slotted ALOHA procedure
Maximum number of transponders in the field	250

**Table 9.19** Provisional technical parameters of a GTAG transponder

Parameter	Value
Minimum frequency range of transponder	862–928 MHz
Uplink	Backscatter (Delta RCS), bi-phase code
Bit rate	Slow: 10 Kbit/s, fast: 40 Kbit/s
Delta RCS	>0.005 m <sup>2</sup>

the case of backscatter transponders whether the reader uses a fixed transmission frequency (Europe) or changes the transmission frequency at periodic intervals (*frequency hopping spread spectrum*, USA and Canada).

### 9.6.2.2 GTAG communication and application layer

The GTAG communication and application layers are described in the MP&PR specification (minimum protocol and performance requirement). The MP&PR (GTAG-RP) defines the coding of data on the contactless transmission path, the construction of a communication relationship between reader and transponder (anticollision and polling), the memory organisation of a transponder, and numerous commands for the effective reading and writing of the transponder.

The memory of a GTAG transponder is organised into blocks each of 128 bits (16 bytes). The GTAG specification initially permits only the addressing of a maximum of 32 pages, so that a maximum of 512 bytes can be addressed. However, it should be assumed that for most applications it is sufficient for a data set identical to the barcode in accordance with EAN/UCC-128 to be stored in a page of the transponder.

# 10

## The Architecture of Electronic Data Carriers

Before we describe the functionality of the data carriers used in RFID systems we must first differentiate between two fundamental operating principles: there are *electronic data carriers* based upon integrated circuits (*microchips*) and data carriers that exploit physical effects for data storage. Both 1-bit transponders and surface wave components belong to the latter category.

Electronic data carriers are further subdivided into data carriers with a pure memory function and those that incorporate a programmable microprocessor (Figure 10.1).

This chapter deals exclusively with the functionality of electronic data carriers. The simple functionality of physical data carriers has already been described in Chapter 3.

### 10.1 Transponder with Memory Function

Transponders with a memory function range from the simple *read-only transponder* to the *high end transponder* with intelligent cryptological functions (Figure 10.2).

Transponders with a memory function contain RAM, ROM, EEPROM or FRAM and an *HF interface* to provide the *power supply* and permit communication with the reader. The main distinguishing characteristic of this family of transponders is the realisation of address and security logic on the chip using a *state machine*.

#### 10.1.1 HF interface

The HF interface forms the interface between the analogue, high frequency transmission channel from the reader to the transponder and the digital circuitry of the transponder. The HF interface therefore performs the functions of a classical modem (modulator–demodulator) used for analogue data transmission via telephone lines.

The modulated HF signal from the reader is reconstructed in the HF interface by *demodulation* to create a digital serial data stream for reprocessing in the address and security logic. A clock-pulse generation circuit generates the system clock for the data carrier from the carrier frequency of the HF field.

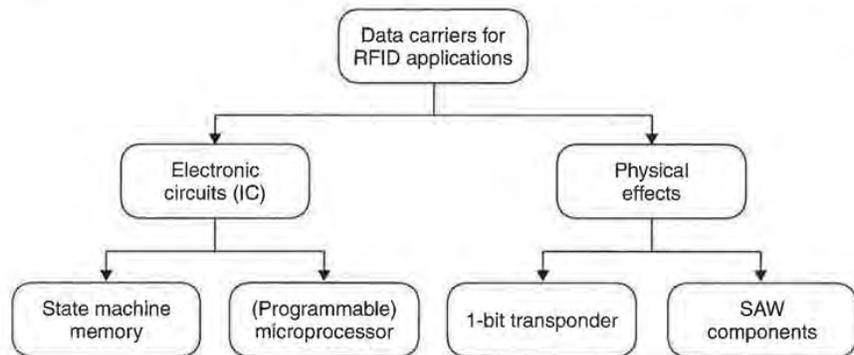


Figure 10.1 Overview of the different operating principles used in RFID data carriers

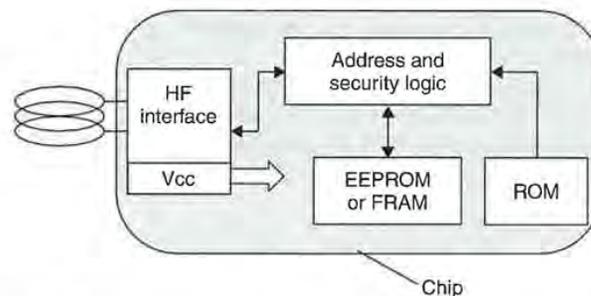


Figure 10.2 Block diagram of an RFID data carrier with a memory function

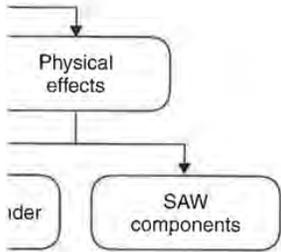
The HF interface incorporates a *load modulator* or *backscatter modulator* (or an alternative procedure, e.g. frequency divider), controlled by the digital data being transmitted, to return data to the reader (Figure 10.3).

*Passive transponders*, i.e. transponders that do not have their own power supply, are supplied with energy via the HF field of the reader. To achieve this, the HF interface draws current from the transponder antenna, which is rectified and supplied to the chip as a regulated supply voltage.

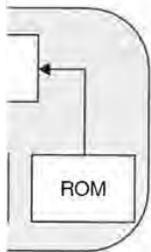
#### 10.1.1.1 Example circuit – load modulation with subcarrier

The principal basic circuit of a load modulator is shown in Figure 10.4. This generates an ohmic load modulation using an ASK or FSK modulated *subcarrier*. The frequency of the subcarrier and the baud rates are in accordance with the specifications of the standard ISO 15693 (Vicinity coupling smart cards).

The high-frequency input voltage  $u_2$  of the data carrier (transponder chip) serves as the time basis of the HF interface and is passed to the input of a binary divider.



used in RFID data carriers



with a memory function

scatter modulator (or an the digital data being trans-

their own power supply, are achieve this, the HF interface field and supplied to the chip

**on with subcarrier**

Figure 10.4. This generates d subcarrier. The frequency with the specifications of the

r (transponder chip) serves e input of a binary divider.

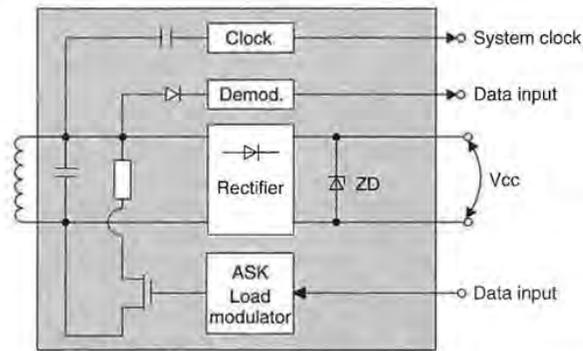


Figure 10.3 Block diagram of the HF interface of an inductively coupled transponder with a load modulator

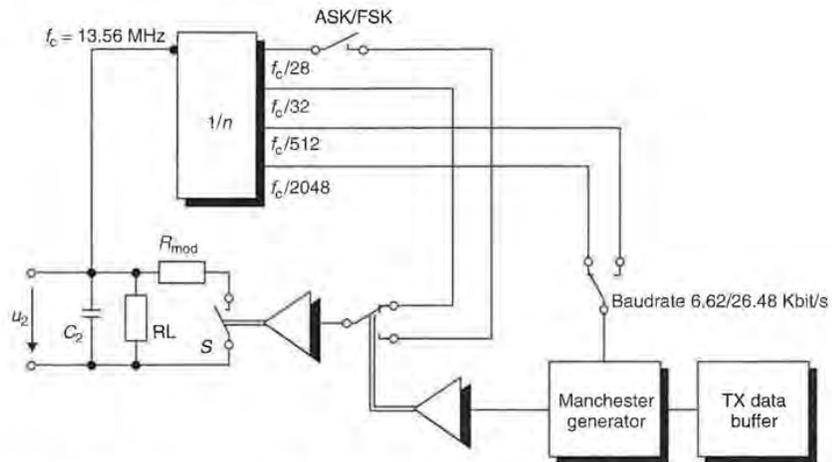


Figure 10.4 Generation of a load modulation with modulated subcarrier: the subcarrier frequency is generated by a binary division of the carrier frequency of the RFID system. The subcarrier signal itself is initially ASK or FSK modulated (switch position ASK/FSK) by the Manchester coded data stream, while the modulation resistor in the transponder is finally switched on and off in time with the modulated subcarrier signal

The frequencies specified in the standard for the subcarrier and the baud rate can be derived from the single binary division of the 13.56 MHz input signal (Table 10.1).

The serial data to be transmitted is first transferred to a Manchester generator. This allows the baud rate of the baseband signal to be adjusted between two values. The Manchester coded baseband signal is now used to switch between the two subcarrier frequencies  $f_1$  and  $f_2$  using the '1' and '0' levels of the signal, in order to generate an FSK modulated subcarrier signal. If the clock signal  $f_2$  is interrupted, this results in an ASK modulated subcarrier signal, which means that it is very simple to switch

**Table 10.1** The clock frequencies required in the HF interface are generated by the binary division of the 13.56 MHz carrier signal

Splitter N	Frequency	Use
1/28	485 kHz	$\phi 2$ of the FSK subcarrier
1/32	423 kHz	$\phi 1$ of the FSK subcarrier, plus ASK subcarrier
1/512	26.48 kHz	Bit clock signal for high baud rate
1/2048	6.62 kHz	Bit clock signal for slow baud rate

between ASK and FSK modulation. The modulated subcarrier signal is now transferred to switch  $S$ , so that the *modulation resistor* of the load modulator can be switched on and off in time with the subcarrier frequency.

### 10.1.1.2 Example circuit - HF interface for ISO 14443 transponder

The circuit in Figure 10.5 provides a further example of the layout of a HF interface. This was originally a simulator for contactless smart cards in accordance with ISO 14443, which can be used to simulate the data transmission from the smart card to a reader by load modulation. The circuit was taken from a proposal by Motorola for a contactless smart card in ISO 10373-6 (Baddeley and Ruiz, 1998).

A complete layout is available for the duplication of this test card (see Section 14.4.1). The circuit is built upon an FR4 printed circuit board. The transponder coil is realised in the form of a large area conductor loop with four windings of a printed conductor. The dimensions of the transponder coil correspond with the ratios in a real smart card.

The *transponder resonant circuit* of the test card is made up of the transponder coil  $L_1$  and the trimming capacitor  $CV_1$ . The resonant frequency of the transponder resonant circuit should be tuned to the transmission frequency of the reader, 13.56 MHz (compare Section 4.1.11.2). The HF voltage present at the transponder resonant circuit is rectified in the bridge rectifier  $D_1-D_4$  and maintained at approximately 3 V by the zener diode  $D_6$  for the power supply to the test card.

The binary divider  $U_1$  derives the required system clocks of 847.5 kHz (subcarrier, divider 1/16) and 105.93 kHz (baud rate, divider 1/128) from the carrier frequency 13.56 MHz.

The circuit made up of  $U_2$  and  $U_3$  is used for the ASK or BPSK modulation of the subcarrier signal (847.5 kHz) with the Manchester or NRZ coded data stream (jumper 1-4). In addition to the simple infinite bit sequences 1111 and 1010, the supply of an external data stream (jumper 10) is also possible. The test smart card thus supports both procedures for data transfer between smart card and reader defined in ISO 14443-2.

Either a capacitive ( $C_4, C_5$ ) or an ohmic ( $R_9$ ) load modulation can be selected. The 'open collector' driver  $U_4$  serves as the output stage ('switch') for the load modulator.

The *demodulation* of a data stream transmitted from the reader is not provided in this circuit. However, a very simple extension of the circuit (see Figure 10.6) facilitates the demodulation of at least a 100% ASK modulated signal. This requires only an

the HF interface are  
the carrier signal

Use

subcarrier  
subcarrier, plus  
or  
for high baud rate  
for slow baud rate

carrier signal is now transferred  
modulator can be switched on

for ISO 14443

The layout of a HF interface,  
reads in accordance with ISO  
from the smart card to a  
proposal by Motorola for a  
z, 1998).

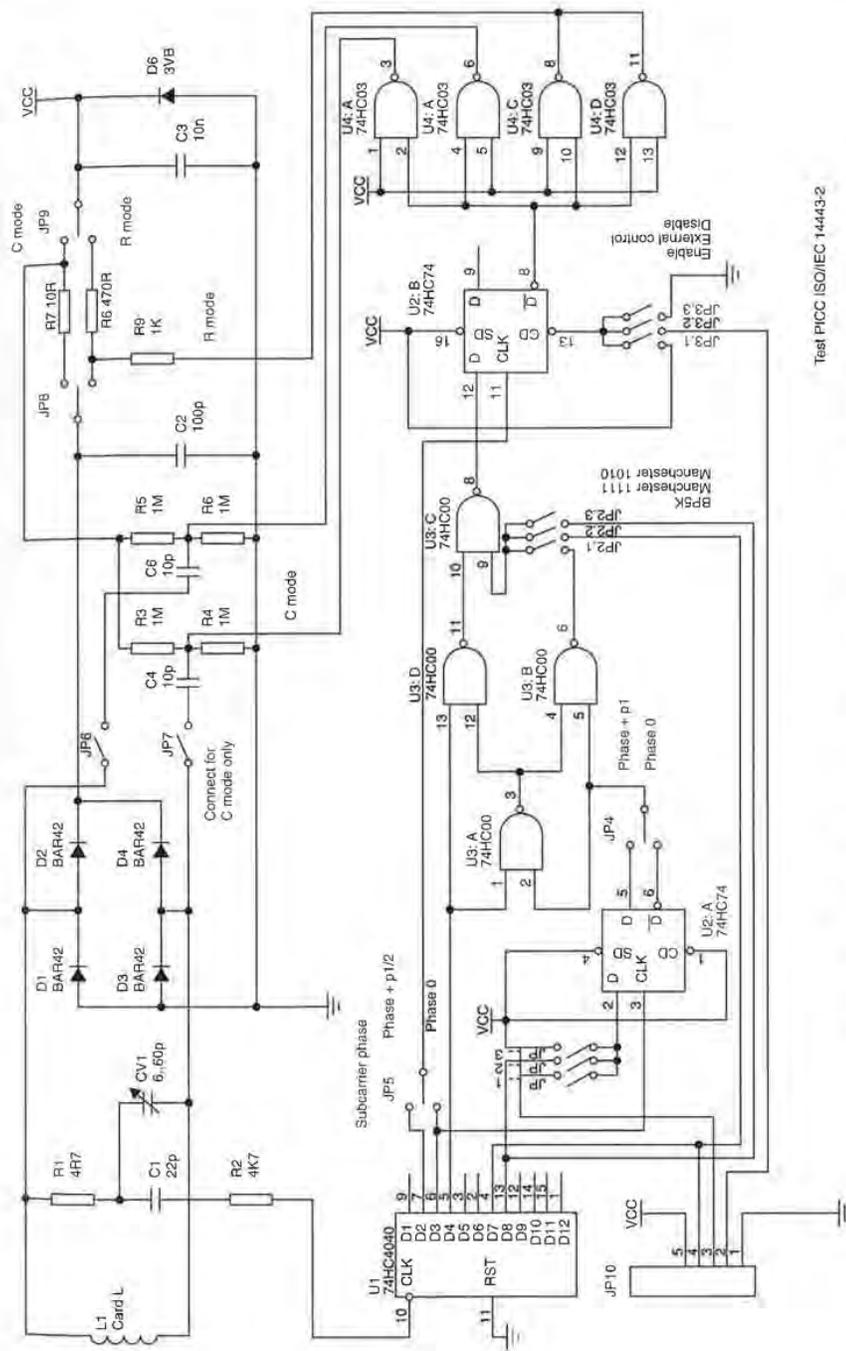
This test card (see Section  
board. The transponder coil  
with four windings of a printed  
board with the ratios in a real

made up of the transponder  
frequency of the transponder  
frequency of the reader, 13.56 MHz  
transponder resonant circuit  
at approximately 3 V by the

blocks of 847.5 kHz (subcar-  
/128) from the carrier fre-

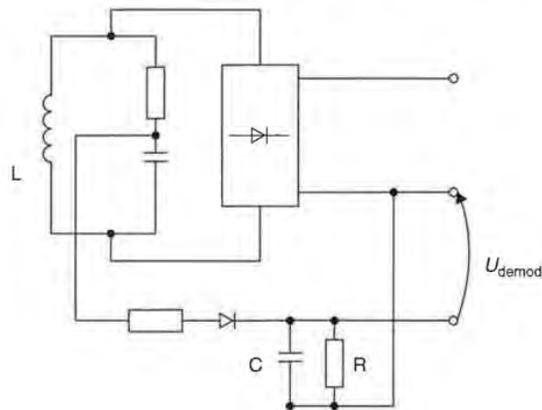
or BPSK modulation of the  
coded data stream (jumper  
and 1010, the supply of an  
smart card thus supports both  
as defined in ISO 14443-2.

modulation can be selected. The  
chip) for the load modulator.  
reader is not provided in this  
(see Figure 10.6) facilitates  
signal. This requires only an



Test PICC ISO/IEC 14443-2

Figure 10.5 Example circuit of a HF interface in accordance with ISO 14443



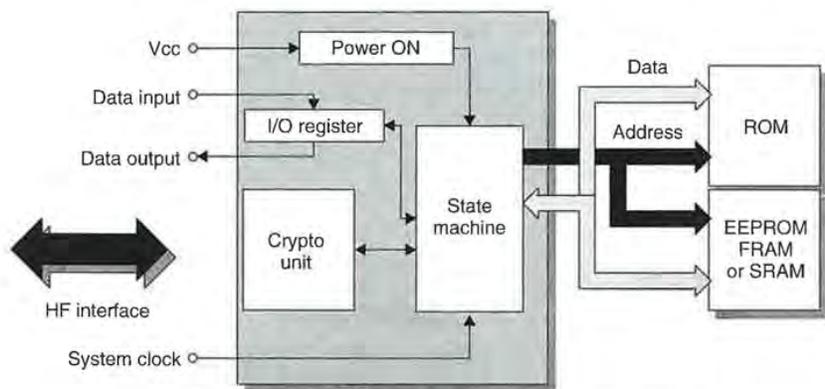
**Figure 10.6** A 100% ASK modulation can be simply demodulated by an additional diode

additional diode to rectify the HF voltage of the transponder resonant circuit. The time constant  $\tau = R \cdot C$  should be dimensioned such that the carrier frequency (13.56 MHz) is still effectively filtered out, but the modulation pulse ( $t_{pulse} = 3 \mu s$  in accordance with ISO 14443-2) is retained as far as is possible.

### 10.1.2 Address and security logic

The *address and security logic* forms the heart of the data carrier and controls all processes on the chip (Figure 10.7).

The *power on logic* ensures that the data carrier takes on a defined state as soon as it receives an adequate power supply upon entering the HF field of a reader. Special I/O registers perform the data exchange with the reader. An optional *cryptological unit* is required for authentication, data encryption and key administration.



**Figure 10.7** Block diagram of address and security logic module

The data memory, which comprises a ROM for permanent data such as serial numbers, and EEPROM or FRAM is connected to the address and security logic via the address and data bus inside the chip.

The *system clock* required for sequence control and system synchronisation is derived from the HF field by the HF interface and supplied to the address and security logic module. The state-dependent control of all procedures is performed by a state machine ('hard-wired software'). The complexity that can be achieved using state machines comfortably equals the performance of microprocessors (high end transponders). However the 'programme sequence' of these machines is determined by the chip design. The functionality can only be changed or modified by modifying the chip design and this type of arrangement is thus only of interest for very large production runs.

**10.1.2.1 State machine**

A *state machine* (also switching device, Mealy machine) is an arrangement used for executing logic operations, which also has the capability of storing variable states (Figure 10.8). The output variable  $Y$  depends upon both the input variable  $X$  and what has gone before, which is represented by the switching state of flip-flops (Tietze and Schenk, 1985).

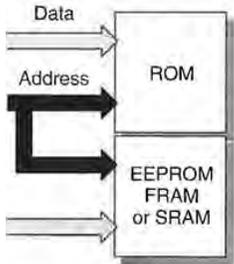
The state machine therefore passes through different states, which can be clearly represented in a *state diagram* (Figure 10.9). Each possible state  $S_Z$  of the system is represented by a circle. The transition from this state into another is represented by an arrow. The arrow caption indicates the conditions that the transition takes place under. An arrow with no caption indicates an unspecified transition (power on  $\rightarrow S_1$ ). The current new state  $S_Z(t + 1)$  is determined primarily by the old state  $S_Z(t)$  and, secondly, by the input variable  $x_i$ .

The order in which the states occur may be influenced by the input variable  $x$ . If the system is in state  $S_Z$  and the transition conditions that could cause it to leave this state are not fulfilled, the system remains in this state.

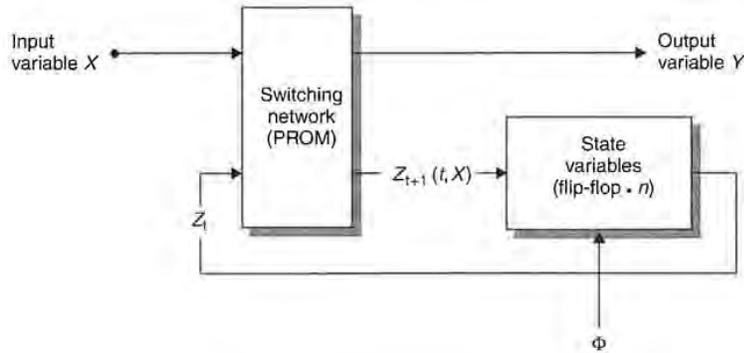
$U_{demod}$

ted by an additional diode  
 resonant circuit. The time  
 or frequency (13.56 MHz)  
 $= 3 \mu s$  in accordance with

carrier and controls all  
 a defined state as soon as  
 field of a reader. Special  
 optional *cryptological unit*  
 illustration.



logic module



**Figure 10.8** Block diagram of a state machine, consisting of the state memory and a backcoupled switching network

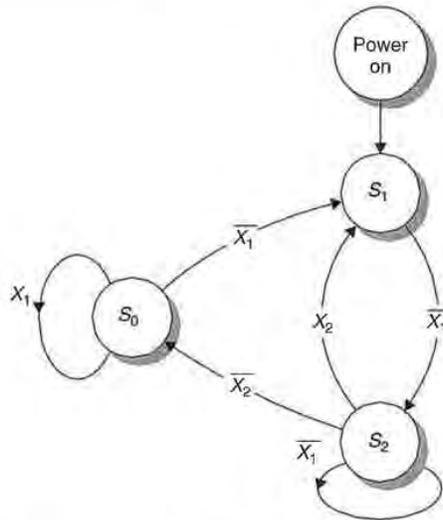


Figure 10.9 Example of a simple state diagram to describe a state machine

A switching network performs the required classification: If the state variable  $Z(t)$  and the input variable are fed into its inputs, then the new state  $Z(t + 1)$  will occur at the output (Figure 10.8). When the next timing signal is received this state is transferred to the output of (transition triggered) flip-flops and thus becomes the new system state  $S(t + 1)$  of the state machine.

### 10.1.3 Memory architecture

#### 10.1.3.1 Read-only transponder

This type of transponder represents the low-end, low-cost segment of the range of RFID data carriers. As soon as a *read-only transponder* enters the interrogation zone of a reader it begins to continuously transmit its own identification number (Figure 10.10). This identification number is normally a simple *serial number* of a few bytes with a check digit attached. Normally, the chip manufacturer guarantees that each serial number is only used once. More complex codes are also possible for special functions.

The transponder's unique identification number is incorporated into the transponder during chip manufacture. The user cannot alter this serial number, nor any data on the chip.

Communication with the reader is unidirectional, with the transponder sending its identification number to the reader continuously. Data transmission from the reader to the transponder is not possible. However, because of the simple layout of the data carrier and reader, read-only transponders can be manufactured extremely cheaply.

Read-only transponders are used in price-sensitive applications that do not require the option of storing data in the transponder. The classic fields of application are



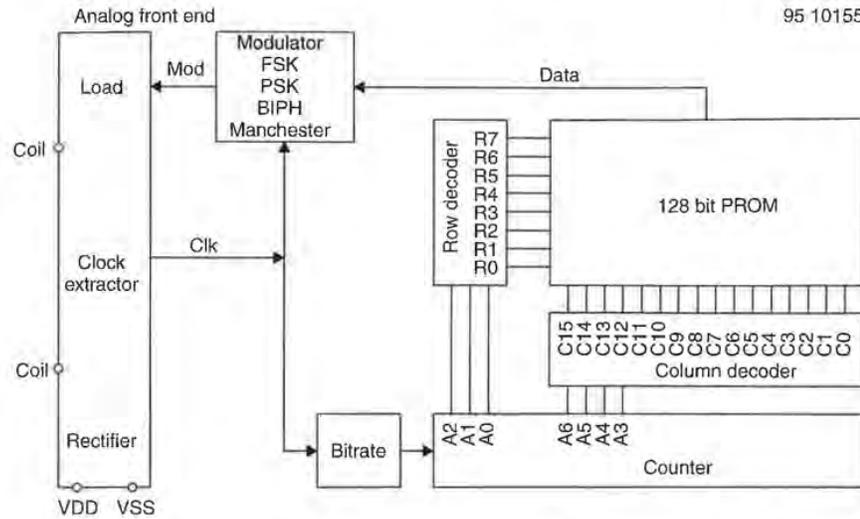
ribe a state machine

: If the state variable  $Z(t)$  state  $Z(t + 1)$  will occur at ved this state is transferred omes the new system state

ment of the range of RFID re interrogation zone of a on number (Figure 10.10). nber of a few bytes with arantees that each serial sible for special functions. rated into the transponder number, nor any data on

ie transponder sending its mission from the reader simple layout of the data red extremely cheaply. ations that do not require fields of application are

95 10155



**Figure 10.10** Block diagram of a read-only transponder. When the transponder enters the interrogation zone of a reader a counter begins to interrogate all addresses of the internal memory (PROM) sequentially. The data output of the memory is connected to a load modulator which is set to the baseband code of the binary code (modulator). In this manner the entire content of the memory (128-bit serial number) can be emitted cyclically as a serial data stream (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

therefore animal identification, access control and industrial automation with central data management.

A low-cost transponder chip is shown in Figure 10.11.

### 10.1.3.2 Writable transponder

Transponders that can be written with data by the reader are available with memory sizes ranging from just 1 byte ('pigeon transponder') to 64 Kbytes (microwave transponders with SRAM).

Write and read access to the transponder is often in blocks. Where this is the case, a block is formed by assembling a predefined number of bytes, which can then be read or written as a single unit. To change the data content of an individual block, the entire block must first be read from the transponder, after which the same block, including the modified bytes, can be written back to the transponder.

Current systems use block sizes of 16 bits, 4 bytes or 16 bytes. The *block structure* of the memory facilitates simple addressing in the chip and by the reader.

### 10.1.3.3 Transponder with cryptological function

If a writable transponder is not protected in some way, any reader that is part of the same RFID system can read from it, or write to it. This is not always desirable, because



**Figure 10.11** Size comparison: low-cost transponder chip in the eye of a needle (reproduced by permission of Philips Electronics N.V.)

sensitive applications may be impaired by unauthorised reading or writing of data in the transponder. Two examples of such applications are the contactless cards used as tickets in the public transport system and transponders in vehicle keys for electronic immobilisation systems.

There are various procedures for preventing unauthorised access to a transponder. One of the simplest mechanisms is read and write protection by checking a *password*. In this procedure, the card compares the transmitted password with a stored reference password and permits access to the data memory if the passwords correspond.

However, if mutual authorisation is to be sought or it is necessary to check that both components belong to the same application, then authentication procedures are used. Fundamentally, an *authentication procedure* always involves a comparison of two secret *keys*, which are not transmitted via the interface. (A detailed description of such procedures can be found in Chapter 8). Cryptological authentication is usually associated with the encryption of the data stream to be transmitted (Figure 10.12). This provides an effective protection against attempts to eavesdrop into the data transmission by monitoring the wireless transponder interface using a radio receiver.

In addition to the memory area allocated to application data, transponders with cryptological functions always have an additional memory area for the storage of the secret key and a *configuration register* (*access register*, Acc) for selectively write protecting selected address areas. The secret key is written to the *key memory* by the manufacturer before the transponder is supplied to the user. For security reasons, the key memory can never be read.

*Hierarchical key concept* Some systems provide the option of storing two separate keys — key A and key B — that give different access rights. The authentication between transponder and reader may take place using key A or key B. The option of



eye of a needle (reproduced

ding or writing of data in contactless cards used as vehicle keys for electronic

1 access to a transponder, by checking a password. rd with a stored reference words correspond.

s necessary to check that entication procedures are involves a comparison of (A detailed description of authentication is usually itted (Figure 10.12). This into the data transmission io receiver.

1 data, transponders with urea for the storage of the cc) for selectively write to the key memory by the For security reasons, the

ion of storing two separights. The authentication or key B. The option of

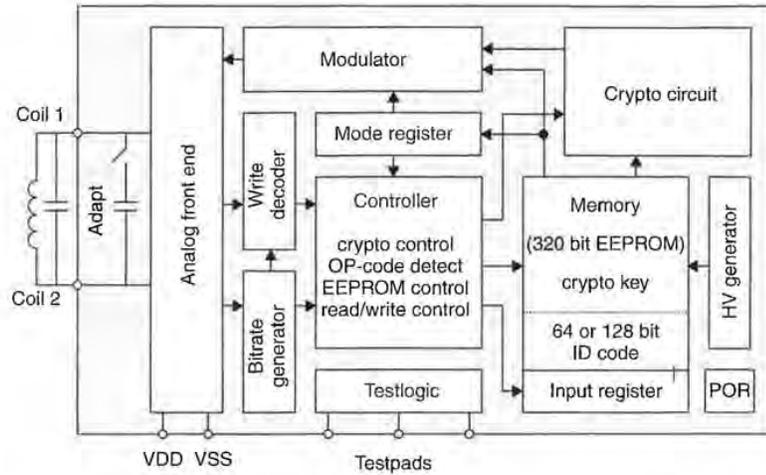


Figure 10.12 Block diagram of a writable transponder with a cryptological function to perform authentication between transponder and reader (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

allocating different access rights (Acc) to the two keys may therefore be exploited in order to define hierarchical security levels in an application.

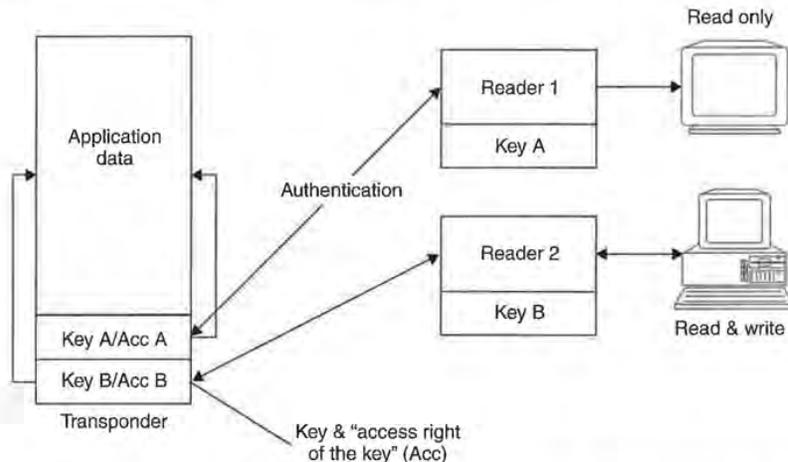
Figure 10.13 illustrates this principle for clarification. The transponder incorporates two key memories, which are initialised by the two keys A and B. The access rights that the readers are allocated after successful authentication depends upon the setting that has been selected in the transponder (access register) for the key that has been used.

Reader 1 is only in possession of key A. After successful authentication, the selected settings in the access register (Acc) only permit it to read from the transponder memory. Reader 2, on the other hand, is in possession of key B. After successful authentication using key B, the settings selected in the access register (Acc) permit it to write to the transponder memory as well as reading from it.

Sample application — hierarchical key Let us now consider the system of travel passes used by a public transport network as an example of the practical use of hierarchical keys. We can differentiate between two groups of readers: the 'devaluers' for fare payments and the 'revaluers' which revalue the contactless smart cards.

The access rights to the transponder's two access registers A and B are configured such that, after successful authentication using key A, the system only permits the deduction of monetary amounts (the devaluation of a counter in the transponder). Only after authentication with key B may monetary amounts be added (the revaluation of the same counter).

In order to protect against attempted fraud, the readers in vehicles or subway entrances, i.e. devaluers, are only provided with key A. This means that a transponder can never be revalued using a devaluer, not even if the software of a stolen devaluer is manipulated. The transponder itself refuses to add to the internal counter unless the transaction has been authenticated by the correct key.



**Figure 10.13** A transponder with two key memories facilitates the hierarchical allocation of access rights, in connection with the authentication keys used

The high-security key B is only loaded into selected secure readers that are protected against theft. The transponder can only be revalued using these readers.

#### 10.1.3.4 Segmented memory

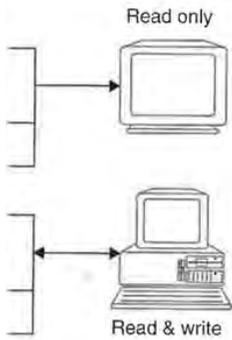
Transponders can also be protected from access by readers that belong to other applications using authentication procedures, as we described in a previous chapter. In transponders with large memory capacities, it is possible to divide the entire memory into small units called segments, and protect each of these from unauthorised access with a separate key. A *segmented transponder* like this permits data from different applications to be stored completely separately (Figure 10.14).

Access to an individual segment can only be gained after successful authentication with the appropriate key. Therefore, a reader belonging to one application can only gain access to its 'own' segment if it only knows the *application's own key*.

The majority of segmented memory systems use fixed segment sizes. In these systems, the storage space within a segment cannot be altered by the user. A fixed segment size has the advantage that it is very simple and cheap to realise upon the transponder's microchip.

However, it is very rare for the storage space required by an application to correspond with the segment size of the transponder. In small applications, valuable storage space on the transponder is wasted because the segments are only partially used. Very large applications, on the other hand, need to be distributed across several segments, which means that the application specific key must be stored in each of the occupied segments. This multiple storage of an identical key also wastes valuable storage space.

A much better use of space is achieved by the use of variable length segments (Figure 10.15). In this approach, the memory allocated to a segment can be matched to



the hierarchical allocation of

the readers that are protected by these readers.

that belong to other applications in a previous chapter. In order to divide the entire memory from unauthorised access, it permits data from different applications (4).

After successful authentication, only one application can only access its own key.

segment sizes. In these systems, the user. A fixed segment realises upon the transponder.

By an application to correlations, valuable storage is only partially used. Very often, it is spread across several segments, and in each of the occupied segments, it has valuable storage space. In variable length segments, a segment can be matched to

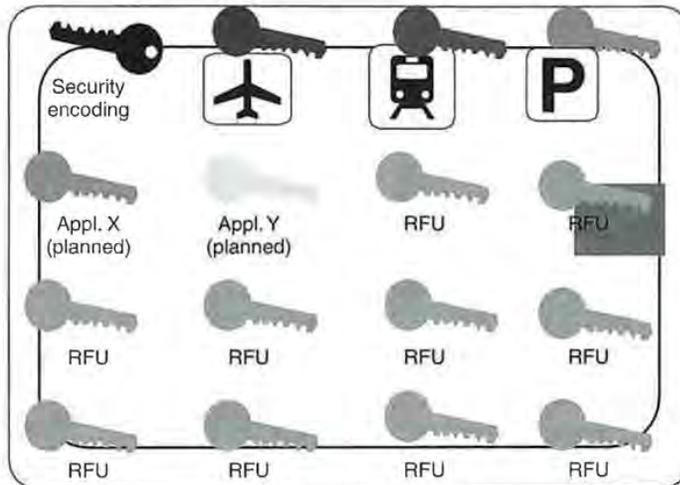


Figure 10.14 Several applications on one transponder — each protected by its own secret key

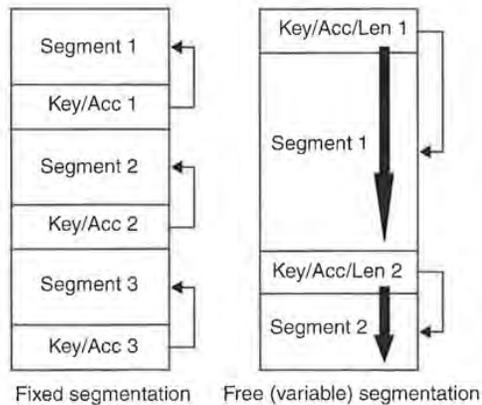
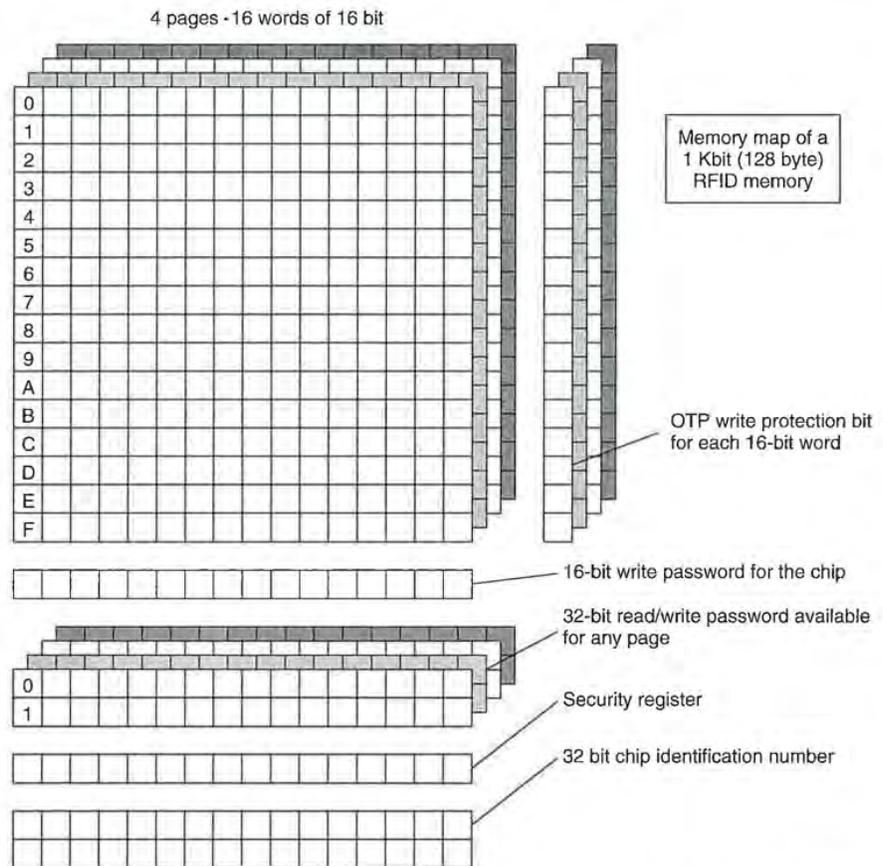


Figure 10.15 Differentiation between fixed segmentation and free segmentation

the requirements of the application using the memory area. Because of the difficulty in realising *variable segmentation*, this variant is rare in transponders with state machines.

Figure 10.16 illustrates the memory configuration of a transponder with fixed segmentation. The available memory, totalling 128 bytes, is divided into four segments, known as 'pages'. Each of the four segments can be protected against unauthorised reading or writing by its own password. The access register of this transponder ('OTP write protection') consists of an additional memory area of 16 bits per segment. Deleting a single bit from the access register permanently protects 16 bits of the application memory against overwriting.

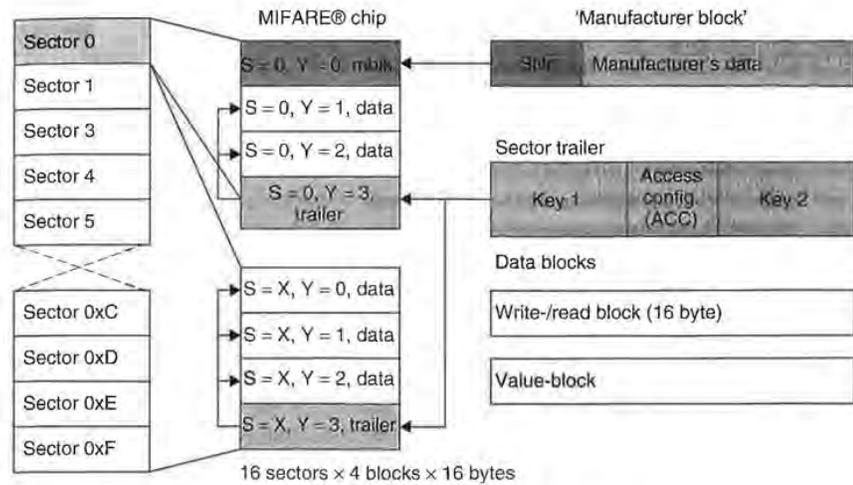
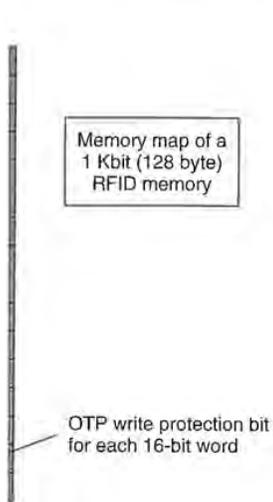


**Figure 10.16** Example of a transponder with fixed segmentation of the memory (IDESCO MICROLOG®). The four 'pages' can be protected against unauthorised reading or writing using different passwords (IDESCO, n.d.)

### 10.1.3.5 MIFARE® application directory

The memory of a *MIFARE®* transponder is divided into 16 independent segments, known as sectors. Each sector is protected against unauthorised access by two different keys (hierarchical structure). Different access rights can be allocated to each of the two keys in its own access register (config.). Thus, 16 independent *applications* that are protected from each other by secret keys can be loaded onto the transponder (Figure 10.17). None of the applications can be read without the secret key, not even for checking or identification. So it is not even possible to determine what applications are stored on the transponder.

Let us now assume that the city of Munich has decided to issue a contactless City-Card, which citizens can use to avail themselves of city services, and which occupies



**Figure 10.17** Memory configuration of a MIFARE® data carrier. The entire memory is divided into 16 independent sectors. Thus a maximum of separate 16 applications can be loaded onto a MIFARE® card

only a small part of the available memory on the card. The remaining memory units on the card could be used by other service providers for their own applications, such as local transport tickets, car rental, filling station cards, parking passes, bonus cards for restaurants and supermarket chains, and many others. However, we cannot find out which of the many possible applications are currently available on the card, because each reader belonging to an application only has access to its own sector, for which it also has the correct key.

To get around this problem, the author, in conjunction with Philips Semiconductors Gratkorn (was Mikron), has developed an *application directory* for the MIFARE® smart card. Figures 10.18 and 10.19 illustrate the data structure of this directory, the *MAD* (MIFARE® application directory).

Blocks 1 and 2 of sector 0 are reserved for the MAD, leaving 32 bytes available for the application directory. Two bytes of each make up a pointer, ID1 to ID\$F, to one of the remaining 15 sectors. Reading the content of the pointer yields 2 bytes, the *function cluster* and the *application code*, which can be used to look the application up in an external database. Even if the application we are looking for is not registered in the available database, we can still gain an approximate classification from the function cluster, for example 'airlines', 'railway services', 'bus services', 'city card services', 'ski ticketing', 'car parking', etc.

Each application is allocated a unique identification number, made up of the function cluster code and application code. It is possible to request an identification number from the developer of MIFARE® technology, Philips Semiconductors Gratkorn (Mikron) at Graz.

If a function cluster is set at 00h, then this is an *administration code* for the management of free or reserved sectors.

write password for the chip

read/write password available on page

chip register

chip identification number

function of the memory (IDESCO) used for reading or writing using

16 independent segments, each accessed by two different keys allocated to each of the independent applications that are loaded onto the transponder. It is possible to request the secret key, not even if you do not know what applications are loaded onto the transponder.

to issue a contactless City-Card, which occupies

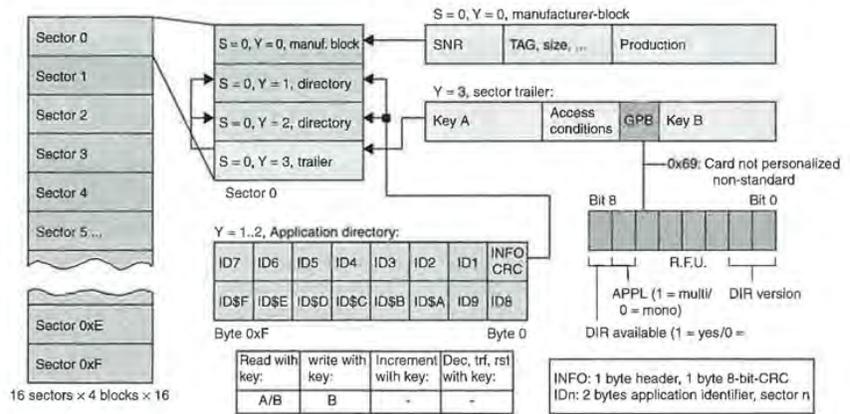


Figure 10.18 The data structure of the MIFARE® application directory consists of an arrangement of 15 pointers (ID1 to ID\$F), which point to the subsequent sectors

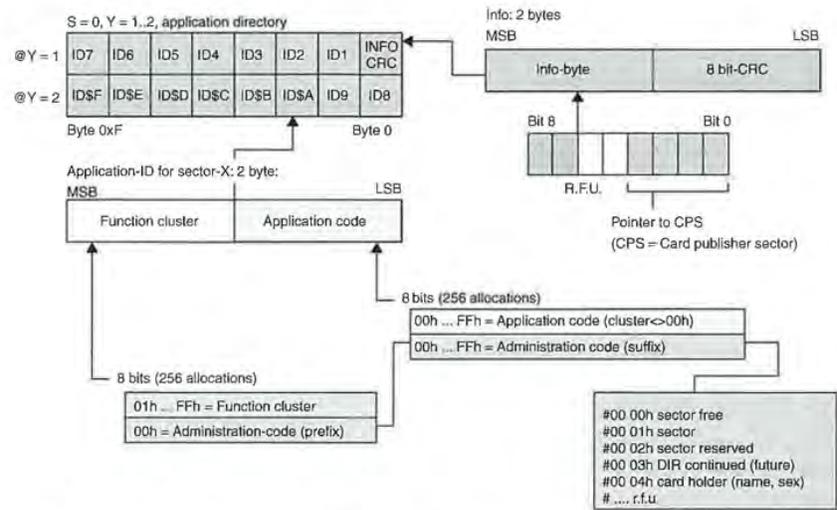
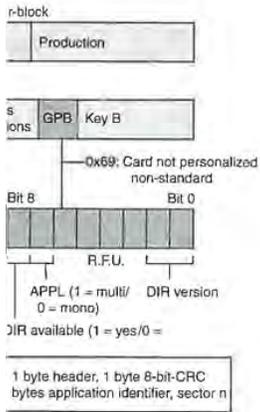
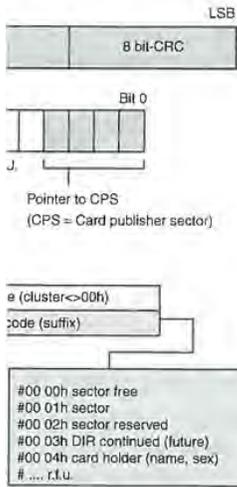


Figure 10.19 Data structure of the MIFARE® application directory: it is possible to find out what applications are located in each sector from the contents of the 15 pointers (ID1 to ID\$F)

Sector 0 itself does not require an ID pointer, because the MAD itself is stored in sector 0. The 2 bytes that this leaves free are used to store an 8-bit CRC, which is used to check the MAD structure for errors, and an info byte. A note can be recorded in the lowest 4 bits of the info byte, giving the sector ID of the card publisher. In our example, this would be the sector ID of one of the sectors in which the data belonging to the city of Munich is stored. This allows the reader to determine the card publisher, even if more than one application is recorded on the smart card.



actory consists of an arrange-  
: sectors



ory: it is possible to find out  
he 15 pointers (ID1 to ID\$F)

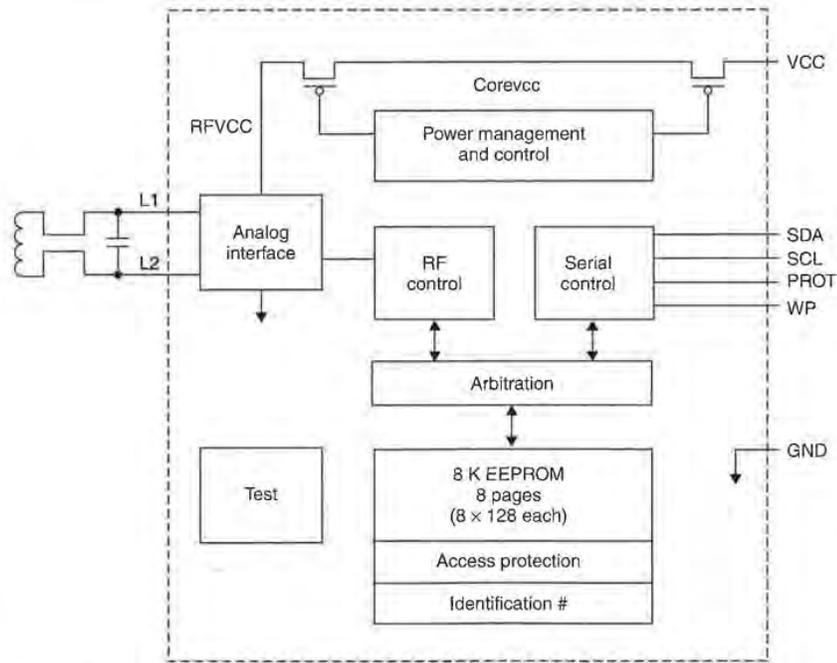
re MAD itself is stored in  
e an 8-bit CRC, which is  
e. A note can be recorded  
the card publisher. In our  
i which the data belonging  
ermine the card publisher,  
card.

Another special feature is MAD's key management system. While key A, which is required for reading the MAD, is published, key B, which is required for recording further applications, is managed by the card publisher. This means that joint use of the card by a secondary service provider is only possible after a joint use contract has been concluded and the appropriate key issued.

**10.1.3.6 Dual port EEPROM**

EEPROM modules with a serial I<sup>2</sup>C (IIC) bus interface established themselves years ago, particularly in consumer electronics. I<sup>2</sup>C bus is the abbreviation for Inter IC bus, because originally it was developed for the connection of microprocessors and other ICs on a common printed circuit board. The I<sup>2</sup>C bus is a serial bus and requires only two bidirectional lines, SDA (Serial Data) and SCL (Serial Clock). A serial EEPROM can be read or written by the transmission of defined commands via the two lines of the I<sup>2</sup>C bus.

Some of these serial EEPROM modules now also have an HF interface and can thus be read or written either via the two SDA and SCL lines or via the contactless interface. The block diagram of such a dual port EEPROM (Atmel, 1998) is shown in Figure 10.20.



**Figure 10.20** Block diagram of a dual port EEPROM. The memory can be addressed either via the contactless HF interface or an IIC bus interface (reproduced by permission of Atmel Corporation, San Jose, USA)

The EEPROM is accessed via two state machines ('RF control' and 'serial control') that are largely independent of each other. The additional arbitration logic prevents conflicts as a result of simultaneous access to the EEPROM via the HF and serial interfaces by simply blocking access to the other interface for the duration of a write or read operation.

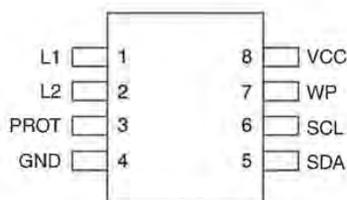
The HF interface of the module is designed for inductive coupling in the frequency range of 125 kHz. If no supply voltage is available via the  $V_{cc}$  pin of the module, then the dual port EEPROM can also be supplied with power entirely via the HF interface. The integral power management simply switches off parts of the circuit that are not required in pure contactless operation. The data transfer from the serial EEPROM to a contactless reader takes place by ohmic load modulation in the baseband. Commands from a reader are transferred to the dual port EEPROM by a simple ASK modulation (modulation index  $m > 10\%$ ). See Figures 10.21 and 10.22 for the pin assignment and memory configuration.

The total memory space of 1 Kbyte (8 Kbit) available on the dual port EEPROM was divided into eight segments (blocks 0–7). Each of these eight blocks was subdivided into eight subsegments (pages 0–7), each of 16 bytes. An additional 16 bytes are available as an *access protection page*. The structure of the access protection page is shown in Figure 10.23. The access protection page permits different access rights to the eight blocks of the EEPROM to be set independently of each other for the I<sup>2</sup>C bus and the HF interface. However, read and write access to the access protection page itself is only possible via the I<sup>2</sup>C bus interface.

The access rights of the HF interface on memory block  $Y$  are defined in the bits  $RF_Y$  of the access protection page (e.g.  $RF_7$  contains the access rights on block 7) (Table 10.2). In a similar manner, the access rights of the I<sup>2</sup>C bus interface are defined on a memory block  $Y$  in the bit  $PB_Y$  of the access protection page ( $PB_5$  contains access rights on block 5).

Furthermore, block 0 permits the access rights of the individual 16 byte pages of the block to be set independently of each other. Bits  $WP_7$ – $WP_0$  of the access protection page serve this purpose.

A peculiarity is the tamper bit in the access protection page. This bit can be set only to '1' by the HF interface and only to '0' by the I<sup>2</sup>C bus interface. In this manner a previous write or read access of the EEPROM via the HF interface can be signalled to the master of the connected I<sup>2</sup>C bus.



**Figure 10.21** Pin assignment of a dual port EEPROM. The transponder coil is contacted to pins  $L_1$  and  $L_2$ . All other pins of the module are reserved for connection to the I<sup>2</sup>C bus and for the power supply in 'contact mode' (reproduced by permission of Atmel Corporation, San Jose, USA)

control' and 'serial control')  
 al arbitration logic prevents  
 ROM via the HF and serial  
 e for the duration of a write

ve coupling in the frequency  
 $V_{cc}$  pin of the module, then  
 ntirely via the HF interface.  
 ts of the circuit that are not  
 om the serial EEPROM to a  
 in the baseband. Commands  
 y a simple ASK modulation  
 2 for the pin assignment and

on the dual port EEPROM  
 ese eight blocks was subdivi-  
 s. An additional 16 bytes are  
 he access protection page is  
 its different access rights to  
 of each other for the I<sup>2</sup>C bus  
 the access protection page

ck  $Y$  are defined in the bits  
 e access rights on block 7)  
 I<sup>2</sup>C bus interface are defined  
 on page ( $PB_5$  contains access

dividual 16 byte pages of the  
 $VP_0$  of the access protection

age. This bit can be set only  
 s interface. In this manner a  
 F interface can be signalled

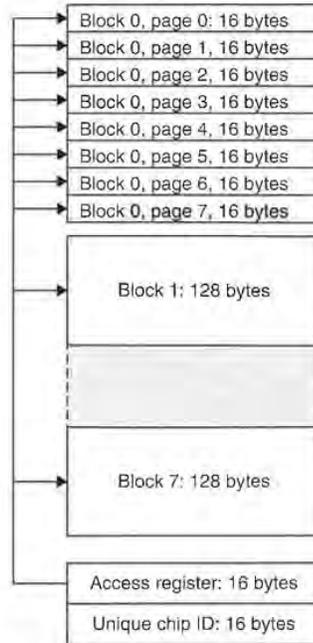
DC

P

DL

DA

ransponder coil is contacted to  
 connection to the I<sup>2</sup>C bus and  
 sion of Atmel Corporation, San



**Figure 10.22** Memory configuration of the AT24RF08. The available memory of 1 Kbyte is split into 16 segments (blocks 0–7) of 128 bytes each. An additional memory of 32 bytes contains the access protection page and the unique serial numbers. The access protection page permits different access rights to be set in the memory for the HF and I<sup>2</sup>C bus interface

	bit 7	bit 6	bit 5	bit 4	bit 3	bit 2	bit 1	bit 0	
SB0			RF0					PB0	Addr 0
SB1			RF1					PB1	Addr 1
SB2			RF2					PB2	Addr 2
SB3			RF3					PB3	Addr 3
SB4			RF4					PB4	Addr 4
SB5			RF5					PB5	Addr 5
SB6			RF6					PB6	Addr 6
SB7			RF7					PB7	Addr 7
SBAP								PBAP	Addr 8
WP7	WP6	WP5	WP4	WP3	WP2	WP1	WP0		Addr 9
DE	DC							Tamper	Addr A
Reserved									Addr B
Reserved									Addr C
Reserved									Addr D
Reserved									Addr E
Chip-revision									Addr F

**Figure 10.23** The access configuration matrix of the module AT24RF08 facilitates the independent setting of access rights to the blocks 0–7

**Table 10.2** Setting options for the access rights of the HF interface to individual memory blocks in the bits  $RF_0 - RF_7$  of the access protection page

MSB	LSB	Access rights via HF interface
0	0	No access to EEPROM
0	1	No access to EEPROM
1	0	Read access to EEPROM only
1	1	No restrictions

## 10.2 Microprocessors

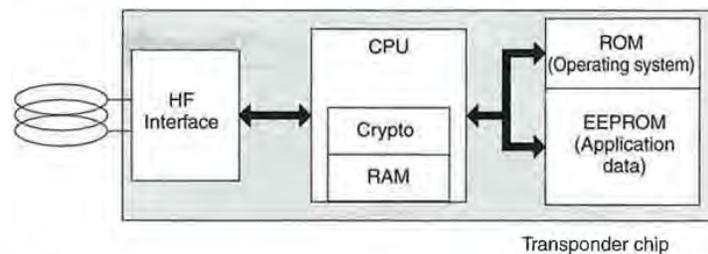
Transponders with *microprocessors* will become increasingly common in applications using contactless smart cards in the near future. Instead of the inflexible state machine, the transponder in these cards incorporates a microprocessor.

Industry standard microprocessors, such as the familiar 8051 or 6805, are used as the microprocessor at the heart of the chip. In addition, some manufacturers are offering simple mathematical coprocessors (cryptological unit) on the same chip, which permit the rapid performance of the calculations required for encryption procedures (Figure 10.24).

Contactless smart cards with microprocessors incorporate their own *operating system*, as has long been the case in contact-based cards. The tasks of the operating system in a contactless smart card are data transfer from and to the smart card, command sequence control, file management and the execution of cryptographic algorithms (e.g. encryption, authentication).

The programme modules are written in ROM code and are incorporated into the chip at the chip manufacturing stage by an additional exposure mask (mask programming).

The typical command processing sequence within a smart card operating system is as follows: commands sent from the reader to the contactless smart card are received by the smart card via the HF interface. Error recognition and correction mechanisms are performed by the I/O manager irrespective of higher-level procedures. An error-free command received by the secure messaging manager is decrypted or checked for integrity. After decryption the higher-level command interpreter attempts to decode



**Figure 10.24** Block diagram of a transponder with a microprocessor. The microprocessor contains a coprocessor (cryptological unit) for the rapid calculation of the cryptological algorithms required for authentication or data encryption

bits of the  
the bits

**Interface**

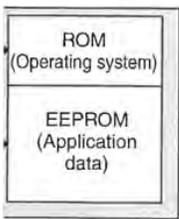
M only

common in applications  
inflexible state machine,

8051 or 6805, are used  
some manufacturers are  
on the same chip, which  
for encryption procedures

their own *operating sys-*  
tasks of the operating  
to the smart card, com-  
cryptographic algorithms

incorporated into the chip  
ask (mask programming).  
t card operating system is  
is smart card are received  
id correction mechanisms  
vel procedures. An error-  
decrypted or checked for  
reter attempts to decode



transponder chip

or. The microprocessor con-  
the cryptological algorithms

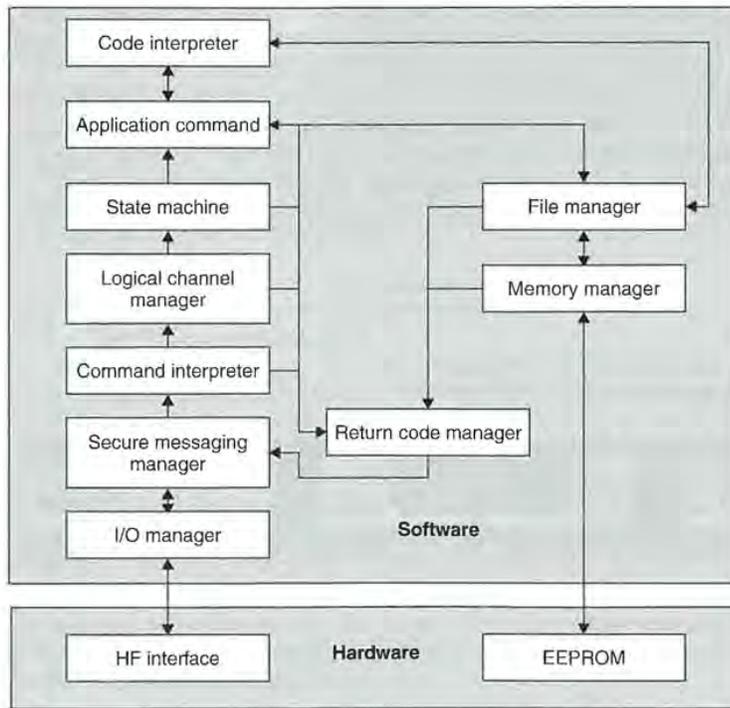
the command. If this is not possible, then the return code manager is called, which generates the appropriate return code and sends it back to the reader via the I/O manager (Figure 10.25).

If a valid command is received, then the actual programme code associated with this application command is executed. If access to the application data in the EEPROM is necessary, this is performed exclusively by the file management system and the memory manager, which convert all symbolic addresses into the corresponding physical addresses of the memory area. The file manager also checks access conditions (authorisation) for the data in question.

A more detailed introduction to the procedures for the development of operating systems and smart card applications can be found in the book *The Smart Card Handbook* published by John Wiley & Sons.

**10.2.1 Dual interface card**

The traditional key markets for *contact smart cards* are *payment applications* (cash card, electronic purse) and *mobile telephones* (SIM card for GSM mobile telephone), applications that necessitate a high degree of security in the processing and transmission



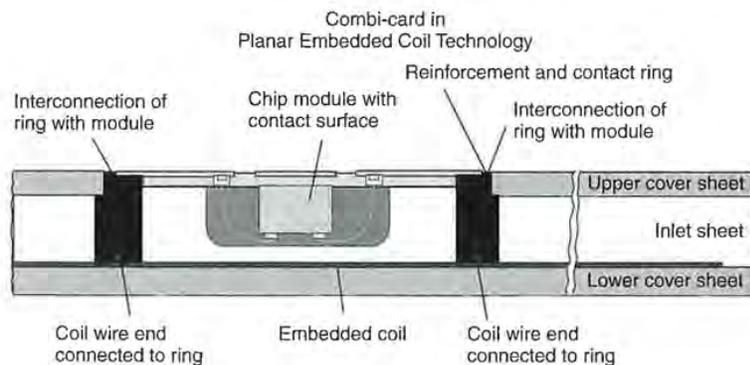
**Figure 10.25** Command processing sequence within a smart card operating system (Rankl and Effing, 1996)

of data. The resulting necessity of being able to quickly and simply calculate complex *cryptographic* algorithms led to the development of powerful cryptographic *coprocessors* on the card chips.

Contactless smart cards, on the other hand, are traditionally used in applications that require a combination of user-friendliness (access control) and short *transaction times* (ticketing). The trend towards combining payment applications with typical contactless applications (cash card with ticketing function) finally led to the development of the *dual interface card*, in which both a contact and a contactless interface are available on one chip. A dual interface card can thus be addressed either via the contactless or the contact interface.

The philosophy underlying the dual interface card is that the smart card interface is completely independent of the smart card logic or smart card software. The interface, whether contact or contactless, is completely transparent to the transmitted application data so that, from the point of view of the application software, the interface used is unimportant. The interface is thus exchangeable at will, and interface and logic components can be combined as desired. The greatest advantage of the dual interface card for the user and system operator is the option of being able to draw upon existing infrastructure (generally contact readers) when introducing new applications. Also, from the point of view of the *security requirements* of a smart card, there is no difference between a contact and a contactless smart card. Due to the transparency of the interface, the replay and fraud of security-related data that has been transmitted is effectively ruled out by the methods defined in ISO/IEC 7816 (e.g. 'secure messaging'), regardless of the interface used. See Figures 10.26 and 10.27.

The greatest difference between a contactless and a contact smart card is the power available. A contactless smart card in accordance with ISO 14443 has only around 5 mW available for operation at the maximum distance from the reader ( $H_{\min} = 1.5 \text{ A/m}$ ) (Mühlbauer, 2001). A contact smart card, on the other hand, may have 7.2 mW (GSM 11.13), 50 mW (GSM 11.11) or even up to 300 mW (ISO 7816-3 Class A: 5 V,



AmaTech

**Figure 10.26** Possible layout of a dual interface smart card. The chip module is connected to both contact surfaces (like a telephone smart card) and a transponder coil (reproduced by permission of Amatech GmbH & Co. KG, Pfronten)

simply calculate complex cryptographic processes

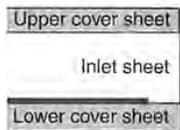
used in applications that need short transaction times as with typical contactless systems. The development of the contactless interface are available either via the contactless or

the smart card interface is implemented in software. The interface, the transmitted application software, the interface used, and interface and logic advantage of the dual interface being able to draw upon producing new applications. In a smart card, there is no due to the transparency of what has been transmitted is (e.g. 'secure messaging'),

the smart card is the power ISO 14443 has only around from the reader ( $H_{min} =$  on the other hand, may have 7.2 mW ISO 7816-3 Class A: 5 V,

contact ring

connection of module



ring



The chip module is connected to a ponder coil (reproduced by

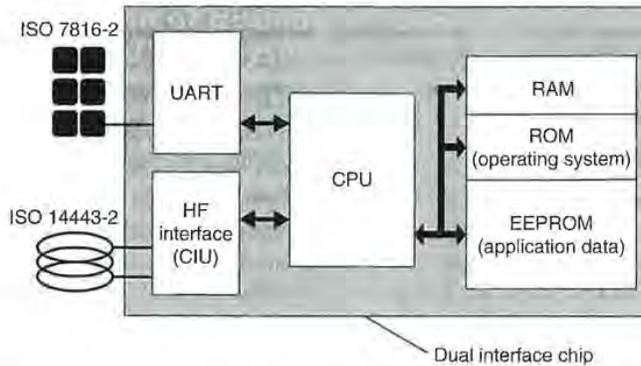


Figure 10.27 Block diagram of a dual interface card. Both smart card interfaces can be addressed independently of one another

60 mA) available depending upon its specification (Philipp, 2001). This calls for completely new concepts in the development of contactless microprocessor chips. For example, the use of a PMU (power management unit) on the chip, which can automatically separate inactive circuit parts of the chip from the power supply to save energy, is recommended. Furthermore, ultra-low-power and low-voltage technology is used in all dual interface chips so that the available power can be optimally exploited.

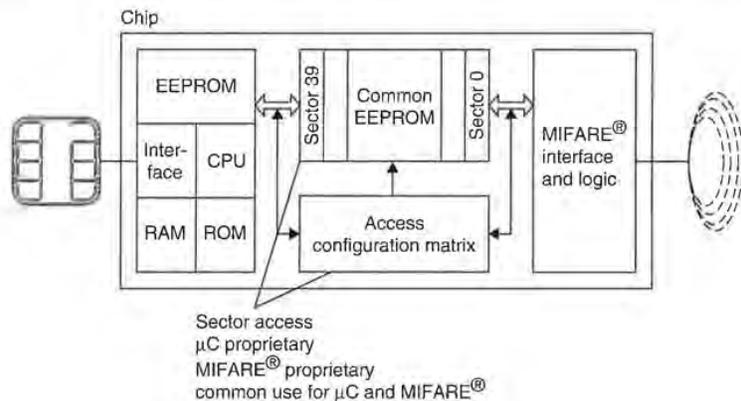
An explicit switching between contactless and contact operation on the chip is not necessary. In the simplest case it is sufficient to use the validity of the data received via one of the two interfaces as the evaluation criterion for further operation. Some chips provide the programmer with status flags that allow the currently active operating mode to be interrogated. Moreover, the signals (frequency, voltage) present at the HF interface or the chip contacts are evaluated.

### 10.2.1.1 MIFARE® plus

The block diagram in Figure 10.28 shows a very early approach to the dual interface card. This chip was developed jointly by Philips Semiconductors Gratkorn and Siemens HL (now Infineon AG) as early as 1997. Since it was not possible using the semiconductor technologies available at the time to reliably operate a microprocessor with the power available via the contactless interface, an unconventional solution was selected.

At the heart of this chip is an 8 Kbyte EEPROM memory, the Common EEPROM, in which the application data was stored. In a similar manner to a dual port RAM, this common EEPROM can be accessed via two interfaces that are completely separate from each other from the point of view of circuitry. The inactive interface at any time is completely separated from the power supply of the chip, so that the power available in contactless operation is used optimally.

The contactless interface is based upon a state machine, which forms a contactless MIFARE® memory card. From the point of view of a contactless reader this dual interface card thus behaves like a memory card with a segmented EEPROM memory,



**Figure 10.28** Block diagram of the MIFARE®-plus 'dual interface card' chip. In contactless operating mode the common EEPROM is accessed via a MIFARE®-compatible state machine. When operating via the contact interface a microprocessor with its own operating system accesses the same memory (reproduced by permission of SLE 44R42, Infineon AG, Munich)

in which the arrangement of the individual segments and memory blocks are identical to that of a conventional MIFARE® card (see Section 10.1.3.5).

The contact interface, on the other hand, is based upon a *microprocessor* with its own *smart card operating system*. The above-mentioned memory segmentation is once again present when the microprocessor accesses the common EEPROM. The operating system can therefore only read and write the common EEPROM in blocks within the corresponding sectors.

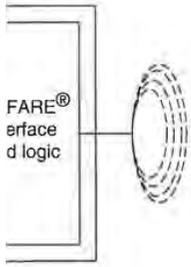
In addition, the write and read rights for individual memory blocks of the common EEPROM can be configured separately for the contactless and contact interface. These access rights are set in, and monitored by, the Access Configuration Matrix. This also facilitates the realisation of hierarchical security concepts.

### 10.2.1.2 Modern concepts for the dual interface card

Figure 10.29 shows the block diagram of a modern dual interface card. This card is based upon a 8051 microprocessor with a *smart card operating system*. The contactless interface is formed by a CIU (*contactless interface unit*), which can be configured by the CPU via register addresses or can also facilitate a status interrogation of the CIU.

A modern CIU automatically performs the transfer of a data block from and to a reader and thereby automatically performs the necessary coding or decoding of the data stream according to the specifications in the standard ISO/I EC14443-2 and ISO/I EC14443-3. Often it also performs the automatic calculation and verification of the transmitted CRCs.

To send a data block, the operating system only needs to store the data block to be sent in the RAM memory of the chip and load the corresponding memory address and block length into the configuration register of the CIU. The CPU is no longer actively involved in the initiated data transfer and can thus be switched into *power down mode*



the card' chip. In contactless ISO-14443-compatible state machine. The operating system accesses the CIU on AG, Munich)

memory blocks are identical (see Figure 10.25).

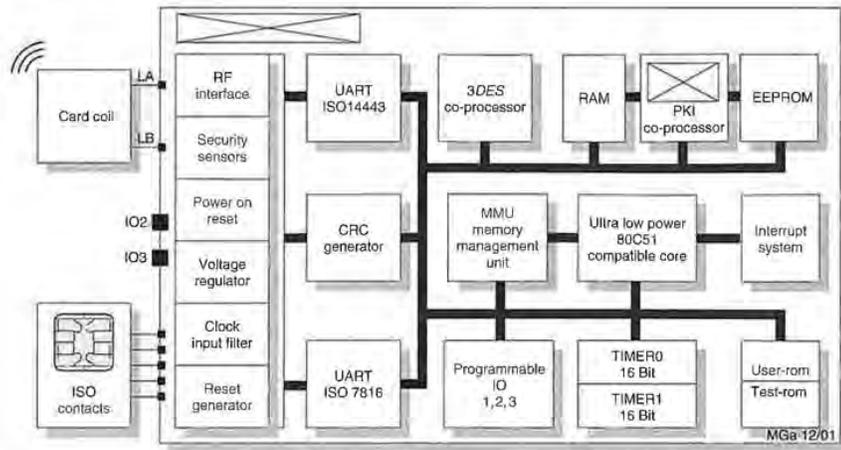
The *microprocessor* with its various memory segmentation is once again connected to EEPROM. The operating system accesses the CIU in blocks within the chip.

The various blocks of the common CIU are connected to the contact interface. These blocks are used for the duration of the transaction Matrix. This also

**Interface card**

Interface card. This card is used in a payment system. The contactless interface can be configured by interrogation of the CIU. The data block from and to a card is used for encoding or decoding of the data block according to ISO/IEC 14443-2 and ISO/IEC 15693-2 and verification of the data block.

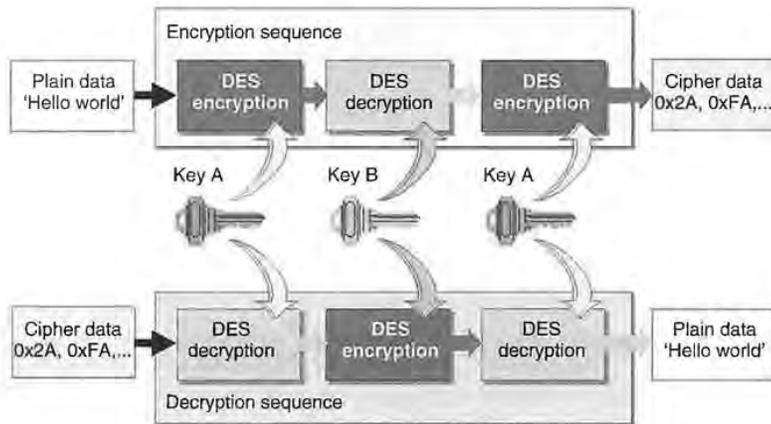
The data block to be stored in the memory address and the CIU is no longer actively used and is put into *power down mode*.



**Figure 10.29** Block diagram of the dual interface card chip 'MIFARE ProX' (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

(power saving mode) for the duration of the data transfer (Mühlbauer, 2001). When a data block is received, the data from the CIU is then automatically stored in the chip's RAM and the CRC of the received block is verified.

Short transaction times represent a particularly important requirement for contactless applications. For ticketing applications a maximum transaction time of 100 ms is a generally accepted value. In order to facilitate the calculation of cryptographic functions within this short time interval, many dual interface chips have *cryptographic coprocessors*. In banking applications, symmetrical encryption algorithms such as DES (data encryption standard) and triple DES are normally used (Figure 10.30). *Encryption*



**Figure 10.30** Calculation of the 3DES (triple DES). Encryption (above) and decryption (below) of a data block (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

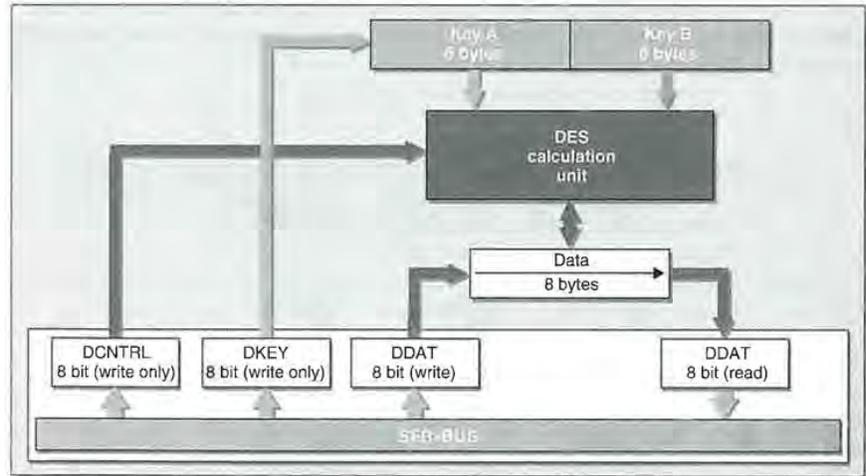
and *decryption* by software is time consuming and therefore not practical in a contactless application. DES encryption can be calculated several hundreds of times quicker using a coprocessor than is possible with the software solution (Mühlbauer, 2001). The CPU need only enter the data to be encrypted and the key in the correct register (DDAT and DKEY in Figure 10.31) and start the calculation by means of a control register (DCNTRL).

Asymmetric key algorithms ('public key' procedures such as *RSA*) will become increasingly important in future. Typical applications are electronic signatures (digital signature) or the validity testing of electronic documents (certification). Therefore, the first dual interface chips already have coprocessors for asymmetric algorithms (e.g. Fame PKI in Figure 10.29).

### 10.3 Memory Technology

After the state machine or microprocessor, the most important component of a data carrier is the memory that user data is read from or written to. Read-only data is defined at the manufacturing stage by the chip mask (exposure mask) or permanently burnt into the memory by a laser. The use of a laser also makes it possible to programme *unique numbers* (*serial numbers* that are issued only once) or consecutive numbers into the data carrier.

If data is to be written to the data carrier, then RAM, EEPROM or FRAM cells are also incorporated into the chip. However, only EEPROM and FRAM cells can store the written data for long periods (typical retention periods are 10 years) without a power supply.



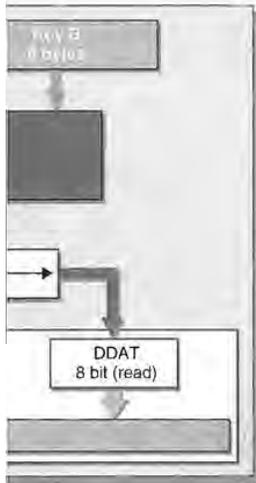
**Figure 10.31** Block diagram of a DES coprocessor. The CPU key and data can be transferred to the coprocessor by means of its own SFR (special function register) (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

not practical in a contact-  
hundreds of times quicker  
ation (Mühlbauer, 2001).  
cey in the correct register  
m by means of a control

ch as RSA) will become  
ctronic signatures (digital  
fication). Therefore, the  
mmetric algorithms (e.g.

ant component of a data  
Read-only data is defined  
sk) or permanently burnt  
it possible to programme  
or consecutive numbers

EEPROM or FRAM cells  
M and FRAM cells can  
ods are 10 years) without



and data can be transferred  
(reproduced by permission

**10.3.1 RAM**

RAM is memory that can be used for the storage of temporary data. When the power supply is removed, the stored data is lost forever. In transponders, RAM is mainly used for the temporary storage of data that exists briefly during operation in the interrogation zone of a reader. In active transponders that have their own battery, RAMs with battery backups are sometimes used for the long-term storage of data.

The main component of the (S)RAM memory cell is a D-flip-flop. Figure 10.32 shows the block diagram for a single memory cell. Each memory cell has the connections DI (Data Input), WE (Write Enable) and DO (Data Out). If data is only to be read from the memory cell, it is sufficient to activate the selected cell with logic 1 levels at the allocated address connections  $Y_i$  and  $X_i$ .

To write data to the memory cell, the WE connection must also be switched to the 1 level. If there is a 1 level at C1 input data is written to the flip-flop.

**10.3.2 EEPROM**

The operating principle of an EEPROM cell is based upon the ability of a capacitor (condenser) to store electric charge over long periods. An EEPROM therefore represents a tiny capacitor that can be charged or discharged. A charged capacitor represents a logic '1', a discharged capacitor represents a logic '0'.

In its simplest form, an EEPROM cell basically consists of a modified field effect transistor on a carrier material (substrate) made of silicon. The EEPROM cell contains an additional gate between the control gate of the field effect transistor and the substrate, which is not connected to an external power supply, and which is positioned at a very short distance (~10 nm) from the carrier material. This so-called *floating gate* can be charged or discharged via the substrate using the tunnel effect, and therefore represents a capacitor. For the tunnel effect to exist there must be a sufficiently large potential difference at the thin insulating tunnelling oxidation layer between the floating gate and the substrate (Figure 10.33).

The flow of current between source and drain can be controlled by the stored charge of the floating gate. A negatively charged floating gate gives rise to a high threshold

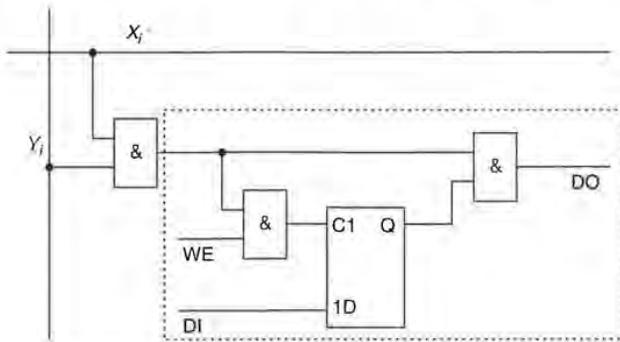
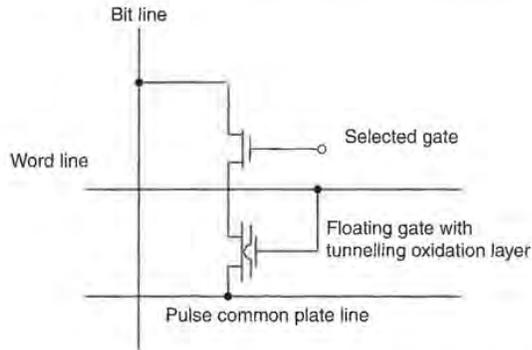


Figure 10.32 Simplified functional block diagram of a (S)RAM cell



**Figure 10.33** The EEPROM cell consists of a modified field effect transistor with an additional floating gate

voltage between the source and drain of the field effect transistor, meaning that this is practically blocked. The current flow through the field effect transistor of an EEPROM cell is evaluated by signal amplification of the memory chip, whereby the strength of the current clearly indicates a '0' or '1'.

To write a '0' or '1' to an EEPROM cell, a high positive or negative voltage is applied to the control gate, which activates the tunnel effect. The voltage required to charge the EEPROM cell is around 17 V at the control gate which falls to 12 V at the floating gate. However, RFID data carriers are supplied with 3 V or 5 V from the HF interface (or a battery). Therefore a voltage of 25 V is generated from the low supply voltage of the chip using a cascaded charging pump integrated into the chip, which provides the required 17 V after stabilisation.

It takes between 5 and 10 ms to charge an EEPROM cell. The number of possible write cycles is limited to between 10 000 and 100 000 for EEPROM cells. This is because in every write operation electrons are captured by the tunnelling oxidation layer and these are never released. These electrons influence the threshold voltage of the field effect transistor, with the effect becoming greater with every write operation. As soon as this parasitic effect of the tunnelling oxidation layer becomes greater than the primary influence of the floating gate the EEPROM cell has reached its *lifetime* (Rankl and Effing, 1996).

A charged floating gate loses its charge due to insulation losses and quantum mechanical effects. However, according to the semiconductor manufacturer's figures, EEPROMs still provide reliable data retention for 10 years. If the EEPROM cell is nearing its lifetime, then information is only stored for short periods, which are determined by the parasitic influence of the oxide layer. For this reason, a plausibility test should be carried out on stored data using checksums (e.g. CRC) in RFID data carriers with EEPROM memories.

### 10.3.3 FRAM

High power consumption during writing and high write times of around 5–10 ms have a detrimental effect on the performance of RFID systems that employ EEPROM

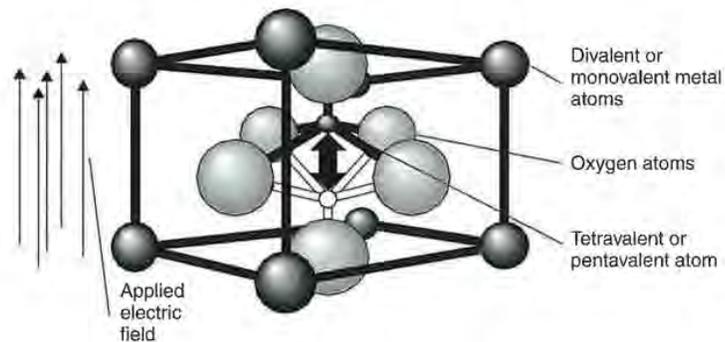
technology. A new, non-transient memory technology, which should improve this situation, has been under development for around 20 years: ferroelectrical RAM, or *FRAM*. At the end of the 1980s the company Ramtron was established, which collaborated with Hitachi on the development of this technology. The first RFID systems using FRAM technology were produced by the Ramtron subsidiary Racom. However, the development of FRAMs is still associated with many problems, and so RFID systems using FRAMs are still not widespread.

The principle underlying the FRAM cell is the ferroelectric effect, i.e. the capability of a material to retain an electrical polarisation even in the absence of an electric field. The polarisation is based upon the alignment of an elementary dipole within a crystal lattice in the ferroelectric material due to the effect of an electric field that is greater than the coercive force of the material. An opposing electric field causes the opposite alignment of the internal dipole. The alignment of the internal dipole takes on one of two stable states, which are retained after the electric field has been removed.

Figure 10.34 shows a simplified model of the ferroelectric lattice. The central atom moves into one of the two stable positions, depending upon the field direction of the external electric field. Despite this, FRAM memories are completely insensitive to foreign electric interference fields and magnetic fields.

To read the FRAM cell (Figure 10.35), an electric field ( $U_{CC}$ ) is applied to the ferroelectric capacitor via a switching transistor. If the stored information represents a logic '1' then the cell is in position A on the hysteresis loop. If, on the other hand, it represents a logic '0', the cell is in position C. By the application of the voltage  $U_{CC}$  we move to point B on the hysteresis loop, releasing electric charge, which is captured and evaluated by the signal amplifiers on the memory chip. The magnitude of escaping charge clearly indicates a '1' or '0', because a significantly greater charge escapes in the transition from state A to B than in the transition from state C to B.

After the external (read) field  $U_{CC}$  has been removed, the FRAM cell always returns to state C, and thus a stored '1' is lost, because state C represents a '0'. For this reason, as soon as a '1' is read, the memory chip's logic automatically performs a rewrite operation. This involves applying an opposing electric field  $-U_{CC}$  to the ferroelectric capacitor, which changes the state of the FRAM cell, moving it to point D on the



**Figure 10.34** Basic configuration of a ferroelectric crystal lattice: an electric field steers the inner atom between two stable states

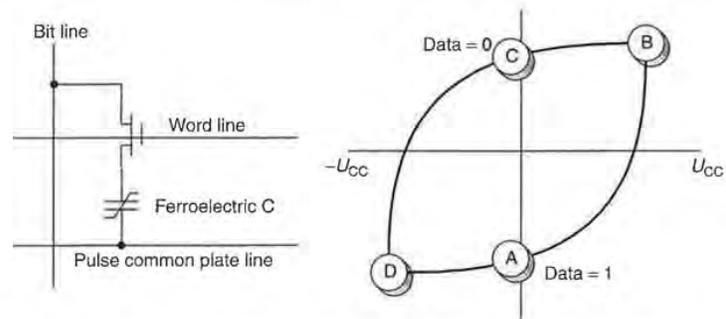


Figure 10.35 FRAM cell structure (1 bit) and hysteresis loop of the ferroelectric capacitor

Table 10.3 Comparison between FRAM and EEPROM (Panasonic, n.d.)

	FRAM	EEPROM
Size of memory cell	$\sim 80 \mu\text{m}^2$	$\sim 130 \mu\text{m}^2$
Lifetime in write cycles	$10^{12}$	$10^5$
Write voltage	2 V	12 V
Energy for writing	$0.0001 \mu\text{J}$	$100 \mu\text{J}$
Write time	$0.1 \mu\text{s}$	10 ms ( $10\,000 \mu\text{s}$ )

hysteresis loop. After the removal of the electric field the FRAM cell falls into state D, which recreates the originally stored state A (Haberland, 1996).

Writing a '1' or '0' to the FRAM cell is achieved simply by the application of an external voltage  $-U_{CC}$  or  $+U_{CC}$ . After the voltage is removed the FRAM cell returns to the corresponding residual state A or C.

### 10.3.4 Performance comparison FRAM – EEPROM

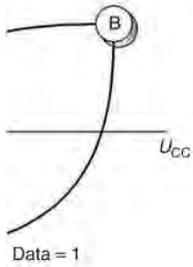
Unlike EEPROM cells, the write operation of a FRAM cell occurs at a high speed. Typical *write times* lie in the region of  $0.1 \mu\text{s}$ . FRAM memories can therefore be written in 'real time', i.e. in the bus cycle time of a microprocessor or the cycle time of a state machine.

FRAMs also beat EEPROMs in terms of power consumption by orders of magnitude. FRAM memory was therefore predestined for use in RFID systems. However, problems in combining CMOS processors (microprocessor) and analogue circuits (HF interface) with FRAM cells on a single chip still prevent the rapid spread of this technology (Table 10.3).

## 10.4 Measuring Physical Variables

### 10.4.1 Transponder with sensor functions

Battery operated *telemetry transmitters* in the frequency range 27.125 MHz or 433 MHz are normally used for the detection of *sensor data*. The fields of application of these



of the ferroelectric capacitor

1 (Panasonic, n.d.)

EEPROM
~130 $\mu\text{m}^2$
$10^5$
12 V
100 $\mu\text{J}$
10 ms (10 000 $\mu\text{s}$ )

FRAM cell falls into state 1996).

by the application of an electric field the FRAM cell returns

**- EEPROM**

It occurs at a high speed. Memories can therefore be accessed by processor or the cycle time

by orders of magnitude. systems. However, problems with gate circuits (HF interface) spread of this technology

25

ons

27.125 MHz or 433 MHz frequencies of application of these

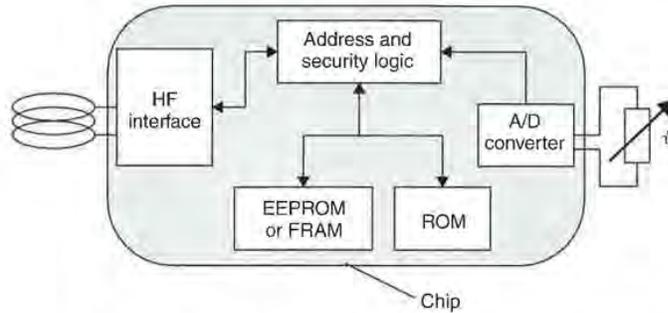


Figure 10.36 Inductively coupled transponder with additional temperature sensor

systems are very limited, however, and are restricted by their size and the lifetime of the battery.

Specially developed RFID transponders incorporating an additional *A/D converter* on the ASIC chip facilitate the measurement of physical variables. In principle, any sensor can be used, in which the resistance alters in proportion to physical variables. Due to the availability of miniaturised *temperature sensors* (NTC), this type of system was first developed for temperature measurement (Figure 10.36).

Temperature sensor, transponder ASIC, transponder coil and backup capacitors are located in a glass capsule, like those used in animal identification systems (see Section 13.6.1). (Ruppert, 1994). The passive RFID technology with no battery guarantees the lifelong functioning of the transponder and is also environmentally friendly.

The measured value of the A/D converter can be read by a special reader command. In read-only transponders the measured value can also be appended to a periodically emitted identification number (serial number).

Nowadays, the main field of application for transponders with sensor functions is wireless temperature measurement in animal keeping. In this application the body temperatures of domestic and working animals are measured for health monitoring and breeding and birth control. The measurement can be performed automatically at feed and watering points or manually using a portable reader (Ruppert, 1994).

In industrial usage, transponders with a sensor function may be used anywhere where physical variables need to be measured in rotating or moving parts where cable connections are impossible.

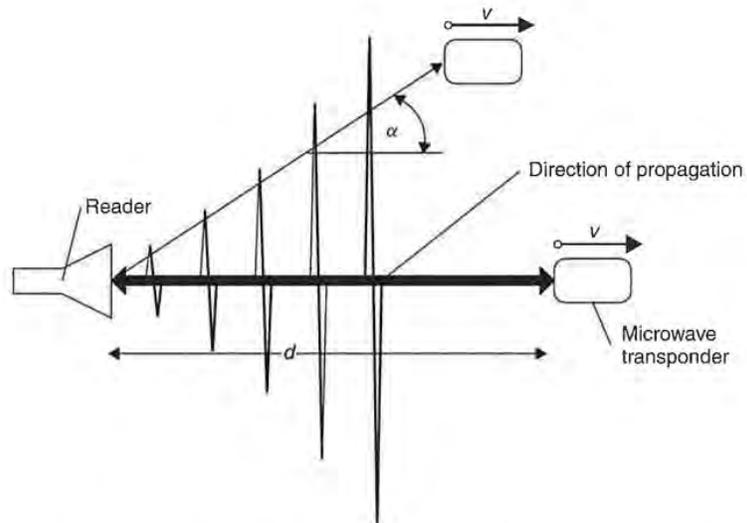
In addition to the classical *temperature sensors* a large number of sensors can already be integrated. Due to their power consumption, however, only certain sensors are suitable for passive (battery-free) transponders. Table 10.4 (Bögel *et al.*, 1998) shows an overview of sensors that can be used in active or passive transponders. Solutions that can be realised as a single chip are cheaper.

**10.4.2 Measurements using microwave transponders**

Industry standard microwave transponders can also be used to measure speed and distance by the analysis of the *Doppler effect* and *signal travelling times* (Figure 10.37).

**Table 10.4** Sensors that can be used in passive and active transponders (mm = micromechanic)

Sensor	Integratable	Passive transponder	Active transponder	Single chip transponder
Temperature	Yes	Yes	Yes	Yes
Moisture	Yes	Yes	Yes	Yes
Pressure	mm	Yes	Yes	Yes
Shock	mm	Yes	Yes	
Acceleration	mm		Yes	
Light	Yes	Yes	Yes	Yes
Flow	Yes		Yes	
PH value	Yes		Yes	
Gases	Yes		Yes	
Conductivity	Yes		Yes	Yes

**Figure 10.37** Distance and speed measurements can be performed by exploiting the Doppler effect and signal travelling times

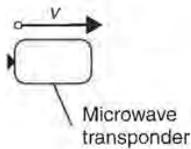
The Doppler effect occurs in all electromagnetic waves and is particularly easy to measure in microwaves. If there is a relative movement between the transmitter and a receiver, then the receiver detects a different frequency than the one emitted by the transmitter. If the receiver moves closer to the transmitter, then the wavelength will be shortened by the distance that the receiver has covered during one oscillation. The receiver thus detects a higher frequency.

If the electromagnetic wave is reflected back to the transmitter from an object that has moved, then the received wave contains twice the frequency shift. There is almost always an angle  $\alpha$  between the direction of propagation of the microwaves

readers (mm = micromechanic)

Active transponder	Single chip transponder
Yes	Yes
Yes	Yes
Yes	Yes
Yes	
Yes	
Yes	Yes
Yes	
Yes	
Yes	
Yes	Yes

direction of propagation



achieved by exploiting the Doppler

and is particularly easy to distinguish between the transmitter and the one emitted by the transponder. Then the wavelength will change during one oscillation. The

transmitter from an object moving with a frequency shift. There is a frequency shift. There is a frequency shift. There is a frequency shift.

Table 10.5 Doppler frequencies at different speeds

$f_d$ (Hz)	$V$ (m/s)	$V$ (km/h)
0	0	0
10	0.612	1.123
20	1.224	4.406
50	3.061	9.183
100	6.122	18.36
200	12.24	36.72
500	30.61	110.2
1000	61.22	220.39
2000	122.4	440.6

and the direction of movement of the 'target'. This leads to a second, expanded Doppler equation:

$$f_d = \frac{f_{TX} \cdot 2v}{c} \cdot \cos \alpha \tag{10.1}$$

$$v = \frac{f_d \cdot c}{2f_{TX} \cdot \cos \alpha} \tag{10.2}$$

The Doppler frequency  $f_d$  is the difference between the transmitted frequency  $f_{TX}$  and the received frequency  $f_{RX}$ . The relative speed of the object is  $v \cdot \cos \alpha$ ,  $c$  is the speed of light,  $3 \times 10^8$  m/s.

A transmission frequency of 2.45 GHz yields the Doppler frequencies shown in Table 10.5 at different speeds.

To measure the distance  $d$  of a transponder, we analyse the travelling time  $t_d$  of a microwave pulse reflected by a transponder:

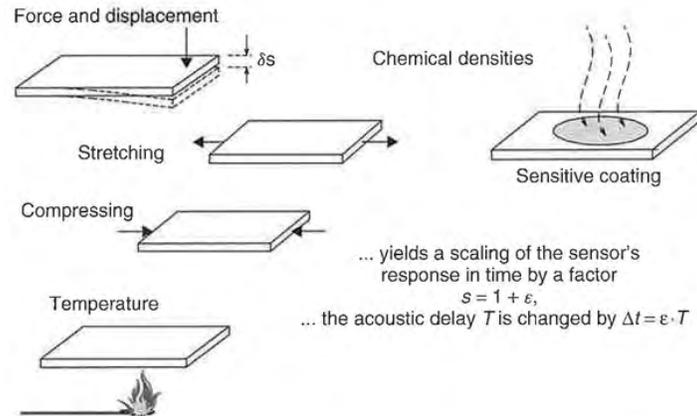
$$d = \frac{1}{2} \cdot t_d \cdot c \tag{10.3}$$

The measurement of the speed or distance of a transponder is still possible if the transponder is already a long way outside the normal interrogation zone of the reader, because this operation does not require communication between reader and transponder.

### 10.4.3 Sensor effect in surface wave transponders

Surface wave transponders are excellently suited to the measurement of *temperature* or mechanical quantities such as *stretching*, *compression*, *bending* or *acceleration*. The influence of these quantities leads to changes in the velocity  $v$  of the surface wave on the piezocrystal (Figure 10.38). This leads to a linear change of the phase difference between the response pulses of the transponder. Since only the differences of *phase position* between the *response pulses* are evaluated, the measuring result is fully independent of the distance between transponder and reader.

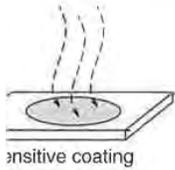
A precise explanation of the physical relationships can be found in Section 4.3.4.



**Figure 10.38** Influence of quantities on the velocity  $v$  of the surface wave in piezocrystal shear, tension, compression and temperature. Even chemical quantities can be detected if the surface of the crystal is suitably coated (reproduced by permission of Technische Universität Wien, Institut für allgemeine Elektrotechnik und Elektronik)



**Figure 10.39** Arrangement for measuring the temperature and torque of a drive shaft using surface wave transponders. The antenna of the transponder for the frequency range 2.45 GHz is visible on the picture (reproduced by permission of Siemens AG, ZT KM, Munich)

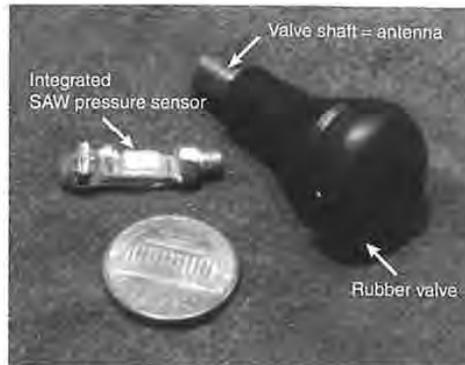


the sensor's  
by a factor  
changed by  $\Delta f = \epsilon \cdot T$

Surface wave in piezocrystal  
properties can be detected if the  
of Technische Universität



Frequency of a drive shaft using  
frequency range 2.45 GHz is  
ZT KM, Munich)



**Figure 10.40** A surface wave transponder is used as a pressure sensor in the valve shaft of a car tyre valve for the wireless measurement of tyre pressure in a moving vehicle (reproduced by permission of Siemens AG, ZT KM, Munich)

The working range of surface wave transponders extends to low temperatures of  $-196^{\circ}\text{C}$  (liquid nitrogen) and in a vacuum it even extends to very low temperatures.<sup>1</sup>

The normal surface wave crystals have only limited suitability for high temperatures. For example, in lithium niobate segregation occurs at a temperature of just  $300^{\circ}\text{C}$ ; in quartz there is a phase transition at  $573^{\circ}\text{C}$ . Moreover, at temperatures above  $400^{\circ}\text{C}$  the aluminium structure of the interdigital transducer is damaged.

However, if we use a crystal that is suitable for high temperatures such as langasite with platinum electrodes, surface wave sensors up to temperatures as high as around  $1000^{\circ}\text{C}$  can be used (Reindl *et al.*, 1998b).

Figures 10.39 and 10.40 show transponders used for measuring physical properties.

<sup>1</sup> At very low temperatures, however, the sensitivity  $S$  of a SAW transponder ultimately tends towards zero.

# RFID HANDBOOK

Fundamentals and Applications in Contactless  
Smart Cards and Identification

Second Edition

**KLAUS FINKENZELLER**

*Giesecke & Devrient GmbH, Munich, Germany*

*Translated by Rachel Waddington, Swadlincote, UK*

Developments in RFID (Radio-Frequency Identification) are yielding larger memory capacities, wider reading ranges and quicker processing, making it one of the fastest growing sectors of the radio technology industry.

RFID has become indispensable in a wide range of automated data capture and identification applications, from ticketing and access control to industrial automation. The second edition of Finkenzeller's comprehensive handbook brings together the disparate information on this versatile technology. Features include:

-  Essential new information on the industry standards and regulations, including ISO 14443 (contactless ticketing), ISO 15693 (smartlabel) and ISO 14223 (animal identification).
-  Complete coverage of the physical principles behind RFID technologies such as inductive coupling, surface acoustic waves and the emerging UHF and microwave backscatter systems.
-  A detailed description of common algorithms for anticollision.
-  An exhaustive appendix providing listings of RFID associations, journals and standards.
-  A sample test card layout in accordance with ISO 14443.
-  Numerous sample applications including e-ticketing in public transport systems and animal identification.

End users of RFID products, electrical engineering students and newcomers to the field will value this introduction to the functionality of RFID technology and the physical principles involved. Experienced ADC professionals will benefit from the breadth of applications examples combined within this single resource.

 **WILEY**  
wiley.com

