WILEY

RFID HANDBOOK

Fundamentals and Applications in Contactless Smart Cards and Identification

Second Edition



KLAUS FINKENZELLER

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

RFID Handbook

Second Edition

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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



HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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
Visit our Home Page on www.wileyeurope.com or www.wiley.com

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, or faxed to (+44) 1243 770571.

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 identifcation/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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Contents

PREFACE xiii
LIST OF ABBREVIATIONS xv

1 Introduction 1
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

2 Differentiation Features of RFID Systems 11
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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

2.5.3 Security requirements 27
2.5.4 Memory capacity 28

3 Fundamental Operating Principles 29
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

4 Physical Principles of RFID Systems 61
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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

4.3.4.3 Impedance sensors 157
4.3.5 Switched sensors 159

5 Frequency Ranges and Radio Licensing Regulations 161
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

6 Coding and Modulation 183
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

7 Data Integrity 195
7.1 The Checksum Procedure 195

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

8 Data Security 221
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

9 Standardisation 229
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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

10 The Architecture of Electronic Data Carriers **273**
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

11 Readers **309**
11.1 Data Flow in an Application 309
11.2 Components of a Reader 309

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

14 Appendix **394**
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

INDEX **419**

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Preface to the 2nd Edition

This book is aimed at an extremely wide range of readers. First and foremost it is intended for students and engineers who find themselves confronted with RFID technology for the first time. A few basic chapters are provided for this audience describing the functionality of RFID technology and the physical and IT-related principles underlying this field. The book is also intended for practitioners who, as users, wish to or need to obtain as comprehensive and detailed an overview of the various technologies, the legal framework or the possible applications of RFID as possible.

Although a wide range of individual articles are now available on this subject, the task of gathering all this scattered information together when it is needed is a tiresome and time-consuming one — as researching this book has proved. This book therefore aims to fill a gap in the range of literature on the subject of RFID. The need for well-founded technical literature in this field is proven by the fortunate fact that this book has now also appeared in Chinese and Japanese translation. Further information on the German version of the RFID handbook and the translations can be found on the homepage of this book, http://RFID-handbook.com.

This book uses numerous pictures and diagrams to attempt to give a graphic representation of RFID technology in the truest sense of the word. Particular emphasis is placed on the physical principles of RFID, which is why the chapter on this subject is by far the most comprehensive of the book. However, practical considerations are also assigned great importance. For this reason the chapter entitled 'Example Applications' is also particularly comprehensive.

Technological developments in the field of RFID technology are proceeding at such a pace that although a book like this can explain the general scientific principles it is not dynamic enough to be able to explore the latest trends regarding the most recent products on the market and the latest standards and regulations. I am therefore grateful for any suggestions and advice — particularly from the field of industry. The basic concepts and underlying physical principles remain, however, and provide a good background for understanding the latest developments.

Unfortunately, the market overview that was previously included has had to be omitted from the 2nd edition of the book, as the growing number of providers has made it increasingly difficult to retain an overview of the numerous transponders available on the market. However, a detailed introduction to the physical principles of UHF and microwave systems (Section 4.2), which will become increasingly important in Europe with the approval of the corresponding frequency ranges in the 868 MHz band, has been added. The chapter on standardisation has been extended in order to keep up with the rapid development in this field.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

At this point I would also like to express my thanks to those companies which were kind enough to contribute to the success of this project by providing numerous technical data sheets, lecture manuscripts, drawings and photographs.

Klaus Finkenzeller

Munich, Summer 2002

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

List of Abbreviations

μP	Microprocessor
μs	Microsecond (10^{-6} seconds)
ABS	Acrylnitrilbutadienstyrol
ACM	Access Configuration Matrix
AFC	Automatic Fare Collection
AFI	Application Family Identifier (see ISO 14443-3)
AI	Application Identifier
AM	Amplitude Modulation
APDU	Application Data Unit
ASIC	Application Specific Integrated Circuit
ASCII	American Standard Code for Information Interchange
ASK	Amplitude Shift Keying
ATQ	Answer to Request (ATQA, ATQB: see ISO 14443-3)
ATR	Answer to Reset
AVI	Automatic Vehicle Identification (for Railways)
BAPT	Bundesamt für Post und Telekommunikation
Bd	Baud, transmission speed in bit/s
BGT	Block Guard Time
BMBF	Bundesministerium für Bildung und Forschung (Ministry for Education and Research, was BMFT)
BP	Bandpass filter
C	Capacitance (of a capacitor)
CCG	Centrale für Coorganisation GmbH (central allocation point for EAN codes in Germany)
CEN	Comité Européen de Normalisation
CEPT	Conférence Européene des Postes et Télécommunications
CICC	Close Coupling Integrated Circuit Chip Card
CIU	Contactless Interface Unit (transmission/receiving module for contactless microprocessor interfaces)
CLK	Clock (timing signal)
CRC	Cyclic Redundancy Checksum
CCITT	Comité Consultatif International Télégraphique et Téléphonique
dBm	Logarithmic measure of power, related to 1 mW HF-power (0 dBm = 1 mW, 30 dBm = 1 W)
DBP	Differential Bi-Phase encoding
DIN	Deutsche Industrienorm (German industrial standard)
EAN	European Article Number (barcode on groceries and goods)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

EAS	Electronic Article Surveillance
EC	Eurocheque or electronic cash
ECC	European Communications Committee
EDI	Electronic Document Interchange
EEPROM	Electric Erasable and Programmable Read-Only Memory
EMC	Electromagnetic Compatibility
EOF	End of Frame
ERC	European Radiocommunications Committee
ERM	Electromagnetic Compatibility and Radio Spectrum Matters
ERO	European Radiocommunications Organisation
ERO	European Radio Office
ERP	Equivalent Radiated Power
ETCS	European Train Control System
ETS	European Telecommunication Standard
ETSI	European Telecommunication Standards Institute
EVC	European Vital Computer (part of ETCS)
FCC	Federal Commission of Communication
FDX	Full-Duplex
FHSS	Frequency Hopping Spread Spectrum
FM	Frequency modulation
FRAM	Ferroelectric Random Access Memory
FSK	Frequency Shift Keying
GSM	Global System for Mobile Communication (was Groupe Spécial Mobile)
GTAG	Global-Tag (RFID Initiative of EAN and the UCC)
HDX	Half-Duplex
HF	High Frequency (3 . . . 30 MHz)
I^2C	Inter-IC-Bus
ICC	Integrated Chip Card
ID	Identification
ISM	Industrial Scientific Medical (frequency range)
ISO	International Organization for Standardization
L	Loop (inductance of a coil)
LAN	Local Area Network
LF	Low Frequency (30 . . . 300 kHz)
LPD	Low Power Device (low power radio system for the transmission of data or speech over a few hundred metres)
LRC	Longitudinal Redundancy Check
LSB	Least Significant Bit
MAD	MIFARE® Application Directory
MSB	Most Significant Bit
NAD	Node Address
nomL	Non-public mobile land radio (industrial radio, transport companies, taxi radio, etc.)
NRZ	Non-Return-to-Zero Encoding

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

NTC	Negative Temperature Coefficient (thermal resistor)
NVB	Number of Valid Bits (see ISO 14443-3)
OCR	Optical Character Recognition
OEM	Original Equipment Manufacturer
OTP	One Time Programmable
PC	Personal Computer
PCD	Proximity Card Device (see ISO 14443)
PICC	Proximity Integrated Contactless Chip Card (see ISO 14443)
PKI	Public Key Infrastructure
PMU	Power Management Unit
PP	Plastic Package
PPS	Polyphenylensulfide
PSK	Phase Shift Keying
PUPI	Pseudo Unique PICC Identifier (see ISO 14443-3)
PVC	Polyvinylchloride
R&TTE	Radio and Telecommunication Terminal Equipment (The Radio Equipment and Telecommunications Terminal Equipment Directive (1999/5/EC))
RADAR	Radio Detecting and Ranging
RAM	Random Access Memory
RCS	Radar Cross-Section
REQ	Request
RFID	Radio Frequency Identification
RFU	Reserved for Future Use
RTI	Returnable Trade Items
RTI	Road Transport Information System
RTTT	Road Transport & Traffic Telematics
RWD	Read Write Device
SAM	Security Authentication Module
SAW	Surface Acoustic Wave
SCL	Serial Clock (I^2C Bus Interface)
SDA	Serial Data Address Input Output (I^2C Bus Interface)
SEQ	Sequential System
SMD	Surface Mounted Devices
SNR	Serial Number
SOF	Start of Frame
SRAM	Static Random Access Memory
SRD	Short Range Devices (low power radio systems for the transmission of data or voice over short distances, typically a few hundred metres)
TR	Technische Richtlinie (Technical Guideline)
UART	Universal Asynchronous Receiver Transmitter (transmission/receiving module for computer interfaces)
UCC	Universal Code Council (American standard for barcodes on groceries and goods)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

UHF	Ultra High Frequency (300 MHz . . . 3 GHz)
UPC	Universal Product Code
VCD	Vicinity Card Device (see ISO 15693)
VDE	Verein Deutscher Elektrotechniker (German Association of Electrical Engineers)
VICC	Vicinity Integrated Contactless Chip Card (see ISO 15693)
VSWR	Voltage Standing Wave Ratio
XOR	eXclusive-OR
ZV	Zulassungsvorschrift (Licensing Regulation)
HITAG® and MIFARE®	are registered trademarks of Philips elektronics N.V.
LEGIC®	is a registered trademark of Kaba Security Locking Systems AG
MICROLOG®	is a registered trademark of Idesco
TIRIS®	is a registered trademark of Texas Instruments
TROVAN®	is a registered trademark of AEG ID systems

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

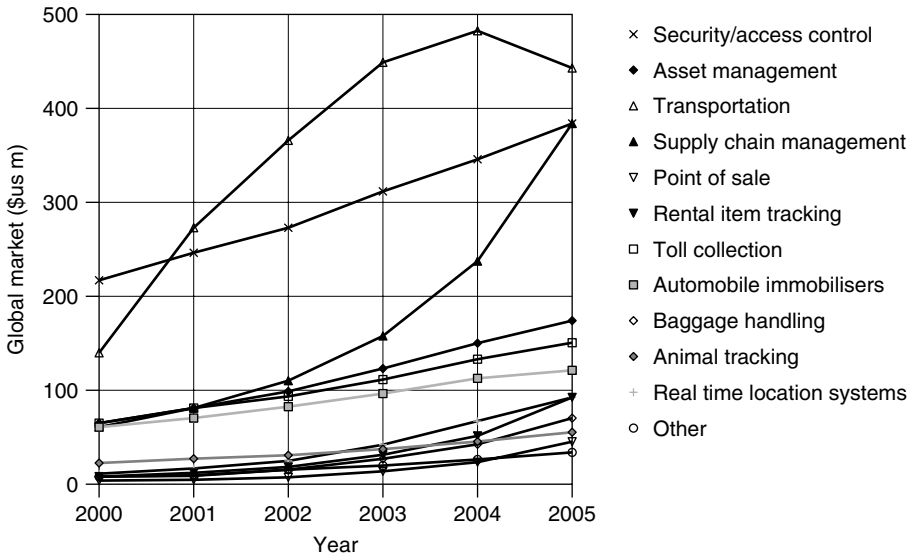


Figure 1.1 The estimated growth of the global market for RFID systems between 2000 and 2005 in million $US, classified by application

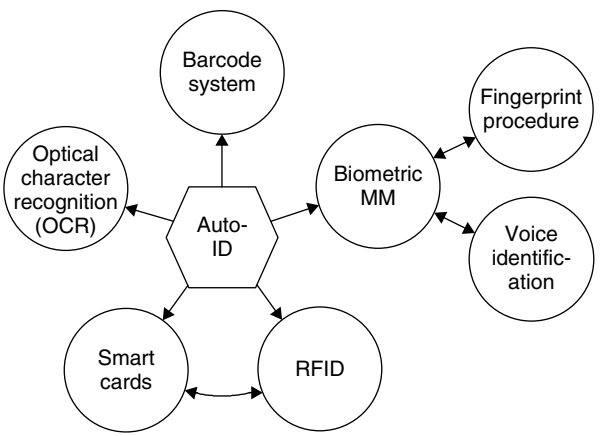


Figure 1.2 Overview of the most important auto-ID procedures

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).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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



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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

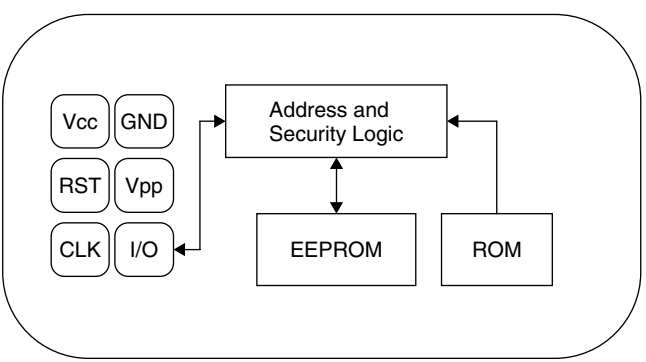


Figure 1.5 Typical architecture of a memory card with security logic

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

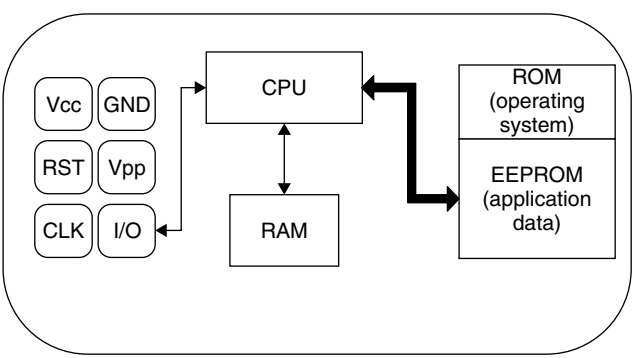


Figure 1.6 Typical architecture of a microprocessor card

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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).

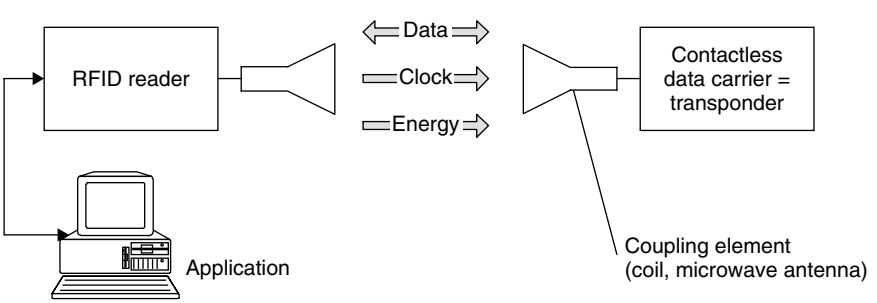


Figure 1.7 The reader and transponder are the main components of every RFID system

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 ~4 s	Low ~3 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	0–50 cm	<1 cm Scanner	0–50 cm	Direct contact**	Direct contact	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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

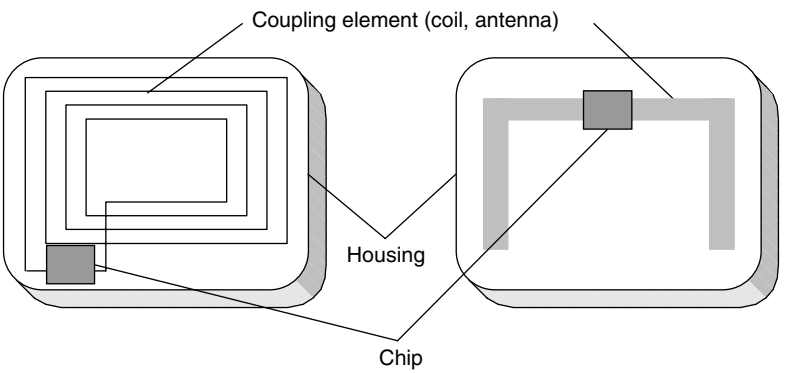


Figure 1.9 Basic layout of the RFID data-carrying device, the transponder. Left, inductively coupled transponder with antenna coil; right, microwave transponder with dipolar antenna

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

2

Differentiation Features of RFID Systems

2.1 Fundamental Differentiation Features

RFID systems exist in countless variants, produced by an almost equally high number of manufacturers. If we are to maintain an overview of RFID systems we must seek out features that can be used to differentiate one RFID system from another (Figure 2.1).

RFID systems operate according to one of two basic procedures: full duplex (FDX)/ half duplex (HDX) systems, and sequential systems (SEQ).

In *full* and *half duplex* systems the transponder's response is broadcast when the reader's RF field is switched on. Because the transponder's signal to the receiver antenna can be extremely weak in comparison with the signal from the reader itself, appropriate transmission procedures must be employed to differentiate the transponder's signal from that of the reader. In practice, data transfer from transponder to reader takes place using load modulation, load modulation using a subcarrier, but also (sub)harmonics of the reader's transmission frequency.

In contrast, *sequential procedures* employ a system whereby the field from the reader is switched off briefly at regular intervals. These gaps are recognised by the transponder and used for sending data from the transponder to the reader. The disadvantage of the sequential procedure is the loss of power to the transponder during the break in transmission, which must be smoothed out by the provision of sufficient auxiliary capacitors or batteries.

The data capacities of RFID transponders normally range from a few bytes to several kilobytes. So-called 1-bit transponders represent the exception to this rule. A data quantity of exactly 1-bit is just enough to signal two states to the reader: 'transponder in the field' or 'no transponder in the field'. However, this is perfectly adequate to fulfil simple monitoring or signalling functions. Because a 1-bit transponder does not need an electronic chip, these transponders can be manufactured for a fraction of a penny. For this reason, vast numbers of 1-bit transponders are used in *Electronic Article Surveillance* (EAS) to protect goods in shops and businesses. If someone attempts to leave the shop with goods that have not been paid for the reader installed in the exit recognises the state 'transponder in the field' and initiates the appropriate reaction. The 1-bit transponder is removed or deactivated at the till when the goods are paid for.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

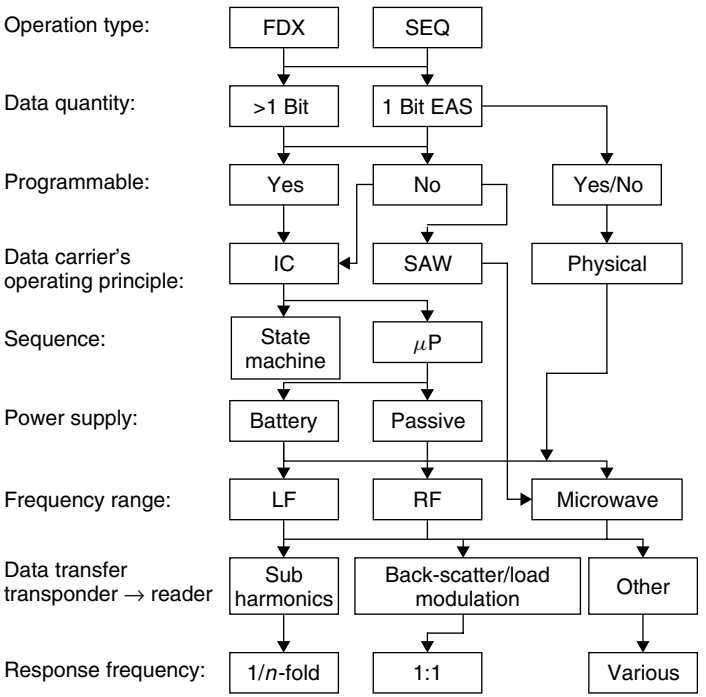


Figure 2.1 The various features of RFID systems (Integrated Silicon Design, 1996)

The possibility of writing data to the transponder provides us with another way of classifying RFID systems. In very simple systems the transponder's data record, usually a simple (serial) number, is incorporated when the chip is manufactured and cannot be altered thereafter. In writable transponders, on the other hand, the reader can write data to the transponder. Three main procedures are used to store the data: in inductively coupled RFID systems EEPROMs (electrically erasable programmable read-only memory) are dominant. However, these have the disadvantages of high power consumption during the writing operation and a limited number of write cycles (typically of the order of 100 000 to 1 000 000). FRAMs (ferromagnetic random access memory) have recently been used in isolated cases. The read power consumption of FRAMs is lower than that of EEPROMs by a factor of 100 and the writing time is 1000 times lower. Manufacturing problems have hindered its widespread introduction onto the market as yet.

Particularly common in microwave systems, SRAMs (static random access memory) are also used for data storage, and facilitate very rapid write cycles. However, data retention requires an uninterruptible power supply from an auxiliary battery.

In programmable systems, write and read access to the memory and any requests for write and read authorisation must be controlled by the data carrier's internal logic. In the simplest case these functions can be realised by a state machine (see Chapter 10 for further information). Very complex sequences can be realised using *state machines*. However, the disadvantage of state machines is their inflexibility regarding changes to the programmed functions, because such changes necessitate changes to the circuitry.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

of the silicon chip. In practice, this means redesigning the chip layout, with all the associated expense.

The use of a microprocessor improves upon this situation considerably. An operating system for the management of application data is incorporated into the processor during manufacture using a mask. Changes are thus cheaper to implement and, in addition, the software can be specifically adapted to perform very different applications.

In the context of contactless smart cards, writable data carriers with a state machine are also known as 'memory cards', to distinguish them from 'processor cards'.

In this context, we should also mention transponders that can store data by utilising physical effects. This includes the read-only surface wave transponder and 1-bit transponders that can usually be deactivated (set to 0), but can rarely be reactivated (set to 1).

One very important feature of RFID systems is the *power supply* to the transponder. *Passive transponders* do not have their own power supply, and therefore all power required for the operation of a passive transponder must be drawn from the (electrical/magnetic) field of the reader. Conversely, *active transponders* incorporate a battery, which supplies all or part of the power for the operation of a microchip.

One of the most important characteristics of RFID systems is the *operating frequency* and the resulting range of the system. The operating frequency of an RFID system is the frequency at which the reader transmits. The transmission frequency of the transponder is disregarded. In most cases it is the same as the *transmission frequency* of the reader (load modulation, backscatter). However, the transponder's 'transmitting power' may be set several powers of ten lower than that of the reader.

The different transmission frequencies are classified into the three basic ranges, LF (low frequency, 30–300 kHz), HF (high frequency)/RF radio frequency (3–30 MHz) and UHF (ultra high frequency, 300 MHz–3 GHz)/microwave (>3 GHz). A further subdivision of RFID systems according to range allows us to differentiate between close-coupling (0–1 cm), remote-coupling (0–1 m), and long-range (>1 m) systems.

The different procedures for sending data from the transponder back to the reader can be classified into three groups: (i) the use of reflection or backscatter (the frequency of the reflected wave corresponds with the transmission frequency of the reader → frequency ratio 1:1) or (ii) load modulation (the reader's field is influenced by the transponder → frequency ratio 1:1), and (iii) the use of subharmonics ($1/n$ fold) and the generation of harmonic waves (n-fold) in the transponder.

2.2 Transponder Construction Formats

2.2.1 Disks and coins

The most common construction format is the so-called *disk* (coin), a transponder in a round (ABS) injection moulded housing, with a diameter ranging from a few millimetres to 10 cm (Figure 2.2). There is usually a hole for a fastening screw in the centre. As an alternative to (ABS) injection moulding, polystyrol or even epoxy resin may be used to achieve a wider operating temperature range.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

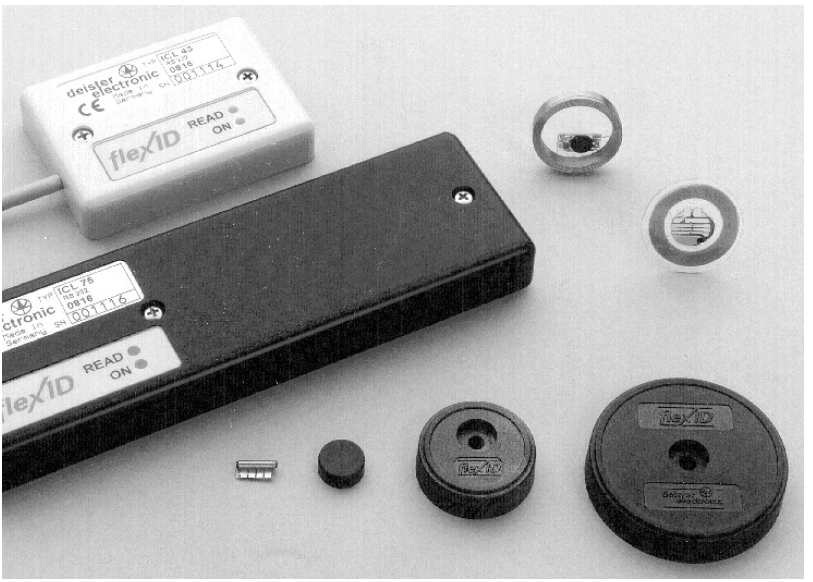


Figure 2.2 Different construction formats of disk transponders. Right, transponder coil and chip prior to fitting in housing; left, different construction formats of reader antennas (reproduced by permission of Deister Electronic, Barsinghausen)

2.2.2 Glass housing

Glass transponders (Figure 2.3) have been developed that can be injected under the skin of an animal for identification purposes (see Chapter 13).

Glass tubes of just 12–32 mm contain a microchip mounted upon a carrier (PCB) and a chip capacitor to smooth the supply current obtained. The transponder coil incorporates wire of just 0.03 mm thickness wound onto a ferrite core. The internal components are embedded in a soft adhesive to achieve mechanical stability (Figure 2.4).

2.2.3 Plastic housing

The *plastic housing* (*plastic package*, PP) was developed for applications involving particularly high mechanical demands. This housing can easily be integrated into other products, for example into *car keys* for *electronic immobilisation systems* (Figure 2.5).

The wedge made of moulding substance (IC casting compound) contains almost the same components as the glass transponder, but its longer coil gives it a greater functional range (Figure 2.6). Further advantages are its ability to accept larger microchips and its greater tolerance to mechanical vibrations, which is required by the automotive industry, for example. The *PP transponder* has proved completely satisfactory with regard to other quality requirements, such as temperature cycles or fall tests (Bruhnke, 1996).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

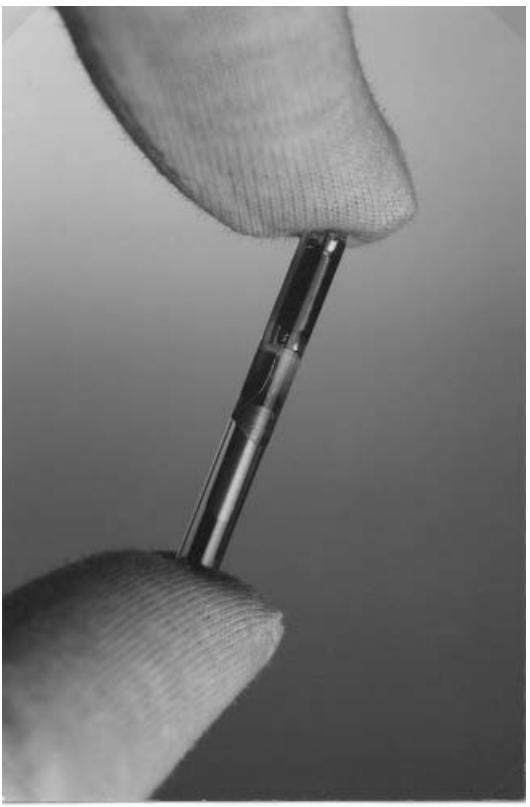


Figure 2.3 Close-up of a 32 mm glass transponder for the identification of animals or further processing into other construction formats (reproduced by permission of Texas Instruments)

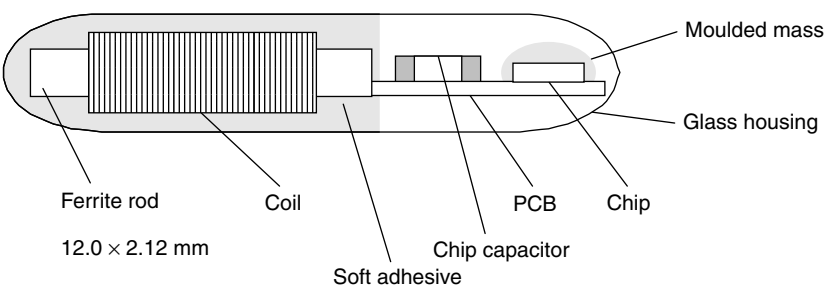


Figure 2.4 Mechanical layout of a glass transponder

2.2.4 Tool and gas bottle identification

Special construction formats have been developed to install inductively coupled transponders into *metal surfaces*. The transponder coil is wound in a ferrite pot core. The transponder chip is mounted on the reverse of the *ferrite pot core* and contacted with the transponder coil.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

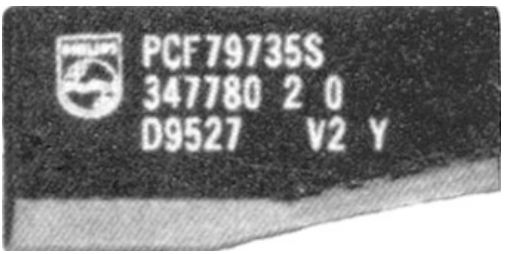


Figure 2.5 Transponder in a plastic housing (reproduced by permission of Philips Electronics B.V.)

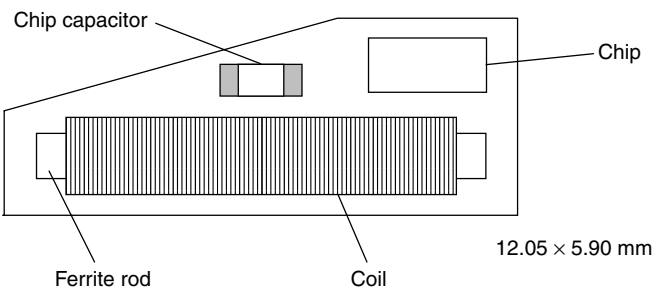


Figure 2.6 Mechanical layout of a transponder in a plastic housing. The housing is just 3 mm thick



Figure 2.7 Transponder in a standardised construction format in accordance with ISO 69873, for fitting into one of the retention knobs of a CNC tool (reproduced by permission of Leitz GmbH & Co., Oberkochen)

In order to obtain sufficient mechanical stability, vibration and heat tolerance, transponder chip and ferrite pot core are cast into a PPS shell using epoxy resin (Link, 1996, 1997). The external dimensions of the transponder and their fitting area have been standardised in *ISO 69873* for incorporation into a retention knob or quick-release taper for tool identification (Figure 2.7). Different designs are used for the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

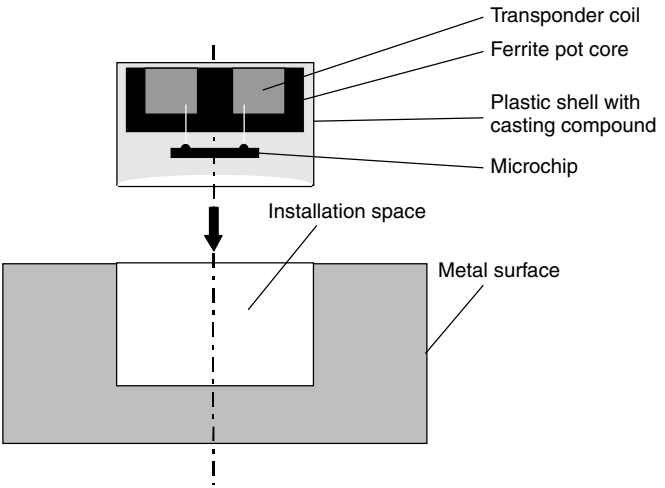


Figure 2.8 Mechanical layout of a transponder for fitting into metal surfaces. The transponder coil is wound around a U-shaped ferrite core and then cast into a plastic shell. It is installed with the opening of the U-shaped core uppermost



Figure 2.9 Keyring transponder for an access system (reproduced by permission of Intermarketing)

identification of gas bottles. Figure 2.8 shows the mechanical layout of a transponder for fitting into a metal surface.

2.2.5 Keys and key fobs

Transponders are also integrated into mechanical keys for immobilisers or door locking applications with particularly high security requirements. These are generally based upon a transponder in a plastic housing, which is cast or injected into the key fob.

The keyring transponder design has proved very popular for systems providing access to office and work areas (Figure 2.9).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



Figure 2.10 Watch with integral transponder in use in a contactless access authorisation system (reproduced by permission of Junghans Uhren GmbH, Schramberg)

2.2.6 Clocks

This construction format was developed at the beginning of the 1990s by the Austrian company Ski-Data and was first used in ski passes. These *contactless clocks* were also able to gain ground in access control systems (Figure 2.10). The clock contains a frame antenna with a small number of windings printed onto a thin printed circuit board, which follows the clock housing as closely as possible to maximise the area enclosed by the antenna coil — and thus the range.

2.2.7 ID-1 format, contactless smart cards

The ID-1 format familiar from credit cards and telephone cards (85.72 mm × 54.03 mm × 0.76 mm ± tolerances) is becoming increasingly important for *contactless smart cards* in RFID systems (Figure 2.11). One advantage of this format for inductively coupled RFID systems is the large coil area, which increases the range of the smart cards.

Contactless smart cards are produced by the lamination of a transponder between four PVC foils. The individual foils are baked at high pressure and temperatures above 100 °C to produce a permanent bond (the manufacture of contactless smart cards is described in detail in Chapter 12).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

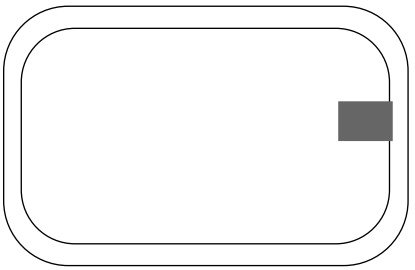


Figure 2.11 Layout of a contactless smart card: card body with transponder module and antenna

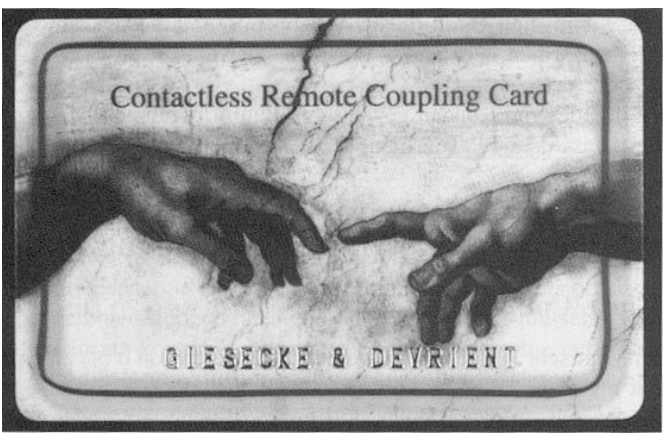


Figure 2.12 Semitransparent contactless smart card. The transponder antenna can be clearly seen along the edge of the card (reproduced by permission of Giesecke & Devrient, Munich)

Contactless smart cards of the design ID-1 are excellently suited for carrying adverts and often have artistic overprints, like those on telephone cards, for example (Figure 2.12).

However, it is not always possible to adhere to the maximum thickness of 0.8 mm specified for ID-1 cards in ISO 7810. Microwave transponders in particular require a thicker design, because in this design the transponder is usually inserted between two PVC shells or packed using an (ABS) injection moulding procedure (Figure 2.13).

2.2.8 Smart label

The term *smart label* refers to a paper-thin transponder format. In transponders of this format the transponder coil is applied to a plastic foil of just 0.1 mm thickness by *screen printing* or *etching*. This foil is often laminated using a layer of paper and its back coated with adhesive. The transponders are supplied in the form of self-adhesive stickers on an endless roll and are thin and flexible enough to be stuck to luggage, packages and goods of all types (Figures 2.14, 2.15). Since the *sticky labels* can easily

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



Figure 2.13 Microwave transponders in plastic shell housings (reproduced by permission of Pepperl & Fuchs GmbH)

be overprinted, it is a simple matter to link the stored data to an additional barcode on the front of the *label*.

2.2.9 Coil-on-chip

In the construction formats mentioned previously the transponders consist of a separate transponder coil that functions as an antenna and a transponder chip (hybrid technology). The transponder coil is bonded to the transponder chip in the conventional manner.



Figure 2.14 Smart label transponders are thin and flexible enough to be attached to luggage in the form of a self-adhesive label (reproduced by permission of i-code-Transponder, Philips Semiconductors, A-Gratkorn)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

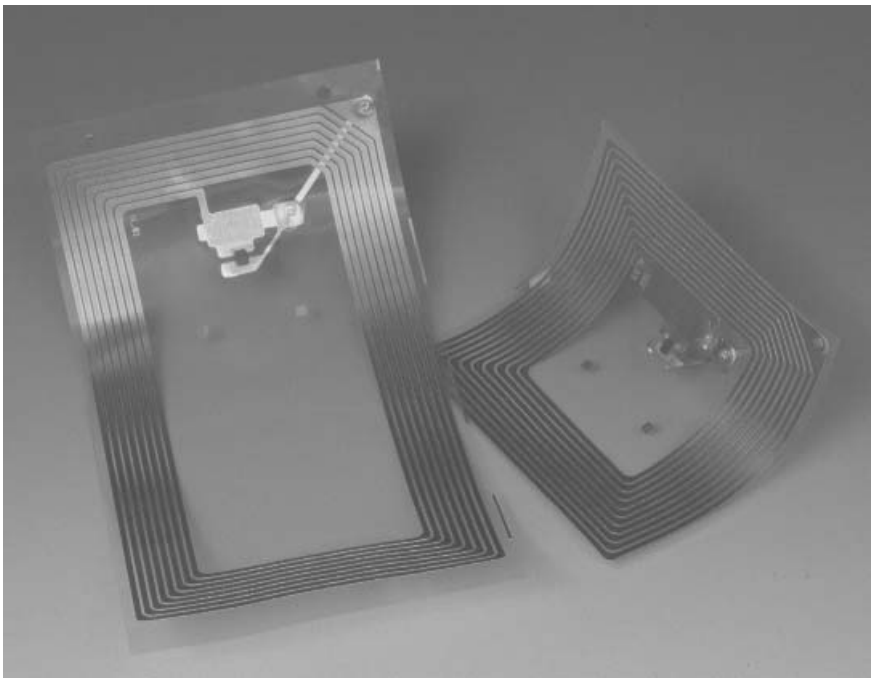


Figure 2.15 A smart label primarily consists of a thin paper or plastic foil onto which the transponder coil and transponder chip can be applied (Tag-It Transponder, reproduced by permission of Texas Instruments, Friesing)

An obvious step down the route of miniaturisation is the integration of the coil onto the chip (*coil-on-chip*) (Figure 2.16). This is made possible by a special microgalvanic process that can take place on a normal CMOS wafer. The coil is placed directly onto the isolator of the silicon chip in the form of a planar (single layer) spiral arrangement and contacted to the circuit below by means of conventional openings in the passivation layer (Jurisch, 1995, 1998). The conductor track widths achieved lie in the range of 5–10 µm with a layer thickness of 15–30 µm. A final passivation onto a polyamide base is performed to guarantee the mechanical loading capacity of the contactless memory module based upon coil-on-chip technology.

The size of the silicon chip, and thus the entire transponder, is just 3 mm × 3 mm. The transponders are frequently embedded in a plastic shell for convenience and at ⊘6 mm × 1.5 mm are among the smallest RFID transponders available on the market.

2.2.10 Other formats

In addition to these main designs, several application-specific special designs are also manufactured. Examples are the 'racing pigeon transponder' or the 'champion chip' for sports timing. Transponders can be incorporated into any design required by the customer. The preferred options are glass or PP transponders, which are then processed further to obtain the ultimate form.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

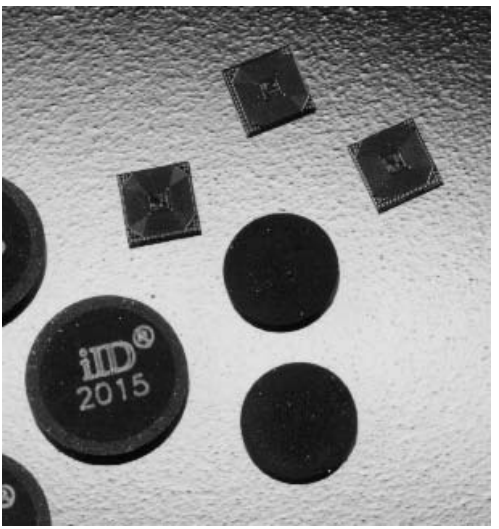


Figure 2.16 Extreme miniaturisation of transponders is possible using coil-on-chip technology (reproduced by permission of Micro Sensys, Erfurt)

2.3 Frequency, Range and Coupling

The most important differentiation criteria for RFID systems are the operating frequency of the reader, the physical coupling method and the range of the system. RFID systems are operated at widely differing frequencies, ranging from 135 kHz longwave to 5.8 GHz in the microwave range. *Electric, magnetic* and *electromagnetic fields* are used for the physical coupling. Finally, the achievable range of the system varies from a few millimetres to above 15 m.

RFID systems with a very small range, typically in the region of up to 1 cm, are known as *close coupling systems*. For operation the transponder must either be inserted into the reader or positioned upon a surface provided for this purpose. Close coupling systems are coupled using both electric and magnetic fields and can theoretically be operated at any desired frequency between DC and 30 MHz because the operation of the transponder does not rely upon the radiation of fields. The close coupling between data carrier and reader also facilitates the provision of greater amounts of power and so even a microprocessor with non-optimal power consumption, for example, can be operated. Close coupling systems are primarily used in applications that are subject to strict security requirements, but do not require a large range. Examples are electronic door locking systems or contactless smart card systems with payment functions. Close coupling transponders are currently used exclusively as ID-1 format contactless smart cards (ISO 10536). However, the role of close coupling systems on the market is becoming less important.

Systems with write and read ranges of up to 1 m are known by the collective term of remote coupling systems. Almost all *remote coupled systems* are based upon an *inductive (magnetic) coupling* between reader and transponder. These systems are therefore also known as *inductive radio systems*. In addition there are also a few systems with

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

capacitive (electric) coupling (motorola Inc., 1999). At least 90% of all RFID systems currently sold are inductively coupled systems. For this reason there is now an enormous number of such systems on the market. There is also a series of standards that specify the technical parameters of transponder and reader for various standard applications, such as contactless smart cards, animal identification or industrial automation. These also include *proximity coupling* (ISO 14443, *contactless smart cards*) and *vicinity coupling systems* (ISO 15693, *smart label* and contactless smart cards). Frequencies below 135 kHz or 13.56 MHz are used as transmission frequencies. Some special applications (e.g. Eurobalise) are also operated at 27.125 MHz.

RFID systems with ranges significantly above 1 m are known as *long-range systems*. All long-range systems operate using electromagnetic waves in the *UHF* and *microwave range*. The vast majority of such systems are also known as *backscatter systems* due to their physical operating principle. In addition, there are also long-range systems using *surface acoustic wave transponders* in the microwave range. All these systems are operated at the UHF frequencies of 868 MHz (Europe) and 915 MHz (USA) and at the microwave frequencies of 2.5 GHz and 5.8 GHz. Typical ranges of 3 m can now be achieved using passive (battery-free) backscatter transponders, while ranges of 15 m and above can even be achieved using active (battery-supported) backscatter transponders. The battery of an active transponder, however, never provides the power for data transmission between transponder and reader, but serves exclusively to supply the microchip and for the retention of stored data. The power of the electromagnetic field received from the reader is the only power used for the data transmission between transponder and reader.

In order to avoid reference to a possibly erroneous range figure, this book uses only the terms *inductively* or *capacitively coupled system* and *microwave system* or *backscatter system* for classification.

2.4 Information Processing in the Transponder

If we classify RFID systems according to the range of information and data processing functions offered by the transponder and the size of its data memory, we obtain a broad spectrum of variants. The extreme ends of this spectrum are represented by low-end and high-end systems (Figure 2.17).

2.4.1 Low-end systems

EAS systems (Electronic Article Surveillance systems; see Section 3.1) represent the bottom end of *low-end systems*. These systems check and monitor the possible presence of a transponder in the interrogation zone of a detection unit's reader using simple physical effects.

Read-only transponders with a microchip are also classified as low-end systems. These transponders have a permanently encoded data set that generally consists only of a unique *serial number* (unique number) made up of several bytes. If a read-only transponder is placed in the HF field of a reader, the transponder begins to continuously

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

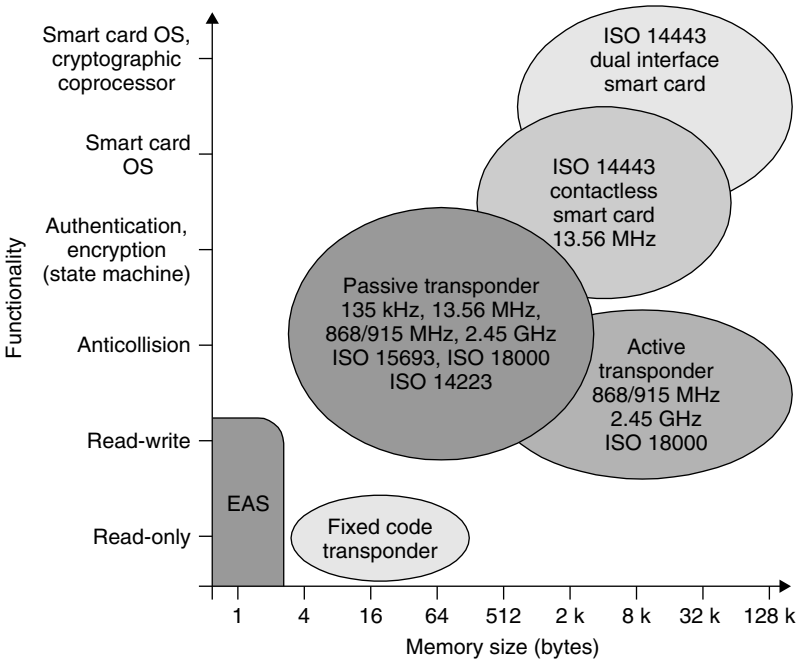


Figure 2.17 RFID systems can be classified into low-end and high-end systems according to their functionality

broadcast its own serial number. It is not possible for the reader to address a read-only transponder — there is a unidirectional flow of data from the transponder to the reader. In practical operation of a read-only system, it is also necessary to ensure that there is only ever one transponder in the reader's interrogation zone, otherwise the two or more transponders simultaneously transmitting would lead to a data collision. The reader would no longer be able to detect the transponder. Despite this limitation, read-only transponders are excellently suited for many applications in which it is sufficient for one unique number to be read. Because of the simple function of a read-only transponder, the chip area can be minimised, thus achieving low power consumption and a low manufacturing cost.

Read-only systems are operated at all frequencies available to RFID systems. The achievable ranges are generally very high thanks to the low power consumption of the microchip.

Read-only systems are used where only a small amount of data is required or where they can replace the functionality of barcode systems, for example in the control of product flows, in the identification of pallets, containers and gas bottles (ISO 18000), but also in the identification of animals (ISO 11785).

2.4.2 Mid-range systems

The mid-range is occupied by a variety of systems with writable data memory, which means that this sector has by far the greatest diversity of types. Memory sizes range

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

from a few bytes to over 100 Kbyte EEPROM (passive transponder) or SRAM (active, i.e. transponder with battery backup). These transponders are able to process simple reader commands for the selective reading and writing of the data memory in a permanently encoded *state machine*. In general, the transponders also support *anticollision procedures*, so that several transponders located in the reader's interrogation zone at the same time do not interfere with one another and can be selectively addressed by the reader (see Section 7.2).

Cryptological procedures, i.e. *authentication* between transponder and reader, and data stream encryption (see Chapter 8) are also common in these systems. These systems are operated at all frequencies available to RFID systems.

2.4.3 High-end systems

The *high-end* segment is made up of systems with a microprocessor and a smart card operating system (smart card OS). The use of microprocessors facilitates the realisation of significantly more complex encryption and authentication algorithms than would be possible using the hard-wired logic of a state machine. The top end of high-end systems is occupied by modern *dual interface smart cards* (see Section 10.2.1), which have a cryptographic *coprocessor*. The enormous reduction in computing times that results from the use of a coprocessor means that contactless smart cards can even be used in applications that impose high requirements on the secure encryption of the data transmission, such as electronic purse or ticketing systems for public transport.

High-end systems are almost exclusively operated at the 13.56 MHz frequency. Data transmission between transponder and reader is described in the standard ISO 14443.

2.5 Selection Criteria for RFID Systems

There has been an enormous upsurge in the popularity of RFID systems in recent years. The best example of this phenomenon is the contactless smart cards used as electronic tickets for public transport. Five years ago it was inconceivable that tens of millions of contactless tickets would now be in use. The possible fields of application for contactless identification systems have also multiplied recently.

Developers of RFID systems have taken this development into account, with the result that countless systems are now available on the market. The technical parameters of these systems are optimised for various fields of application — *ticketing, animal identification, industrial automation* or *access control*. The technical requirements of these fields of application often overlap, which means that the clear classification of suitable systems is no simple matter. To make matters more difficult, apart from a few special cases (animal identification, close coupling smart cards), no binding standards are as yet in place for RFID systems.

It is difficult even for a specialist to retain an overview of the range of RFID systems currently on offer. Therefore, it is not always easy for users to select the system best suited to their needs.

In what follows there are some points for consideration when selecting RFID systems.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

2.5.1 Operating frequency

RFID systems that use frequencies between approximately 100 kHz and 30 MHz operate using inductive coupling. By contrast, microwave systems in the frequency range 2.45–5.8 GHz are coupled using electromagnetic fields.

The specific *absorption rate* (damping) for water or non-conductive substances is lower by a factor of 100 000 at 100 kHz than it is at 1 GHz. Therefore, virtually no absorption or damping takes place. Lower frequency HF systems are primarily used due to the better penetration of objects (Schürmann, 1994). An example of this is the bolus, a transponder placed in the omasum (rumen) of cattle, which can be read from outside at an interrogation frequency of <135 kHz.

Microwave systems have a significantly higher *range* than inductive systems, typically 2–15 m. However, in contrast to inductive systems, microwave systems require an additional backup battery. The transmission power of the reader is generally insufficient to supply enough power for the operation of the transponder.

Another important factor is sensitivity to *electromagnetic interference fields*, such as those generated by welding robots or strong electric motors. Inductive transponders are at a significant disadvantage here. Microwave systems have therefore particularly established themselves in the production lines and painting systems of the automotive industry. Other factors are the high memory capacity (up to 32 Kbyte) and the high temperature resistance of microwave systems (Bachthaler, 1997).

2.5.2 Range

The required range of an application is dependent upon several factors (Figure 2.18):

- the positional accuracy of the transponder;
- the minimum distance between several transponders in practical operation;
- the speed of the transponder in the interrogation zone of the reader.

For example, in contactless payment applications — e.g. public transport tickets — the positioning speed is very low, since the transponder is guided to the reader by hand. The minimum distance between several transponders in this case corresponds with the distance between two passengers entering a vehicle. For such systems there is an optimal range of 5–10 cm. A greater range would only give rise to problems in this case, since several passengers' tickets might be detected by the reader simultaneously. This would make it impossible to reliably allocate the ticket to the correct passenger.

Different vehicle models of varying dimensions are often constructed simultaneously on the production lines of the automotive industry. Thus great variations in the distance between the transponder on the vehicle and the reader are pre-programmed (Bachthaler, 1997). The write/read distance of the RFID system used must therefore be designed for the maximum required range. The distance between the transponders must be such that only one transponder is ever within the interrogation zone of the reader at a time. In this situation, microwave systems in which the field has a *directional beam* offer clear advantages over the broad, nondirectional fields of inductively coupled systems.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

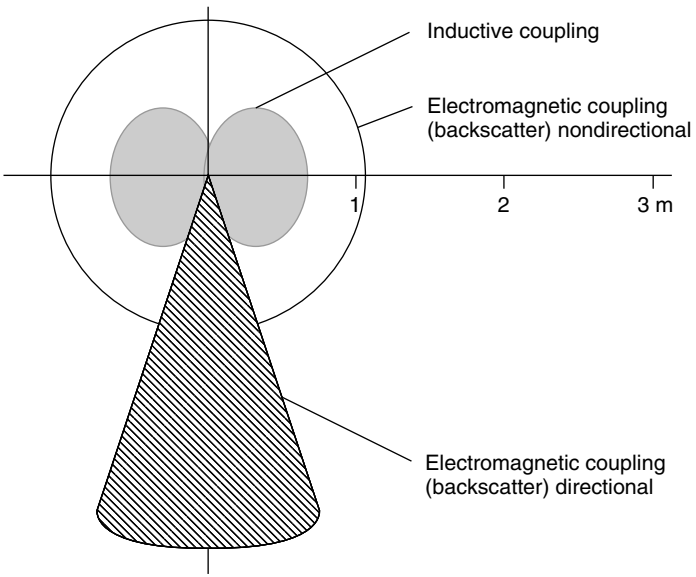


Figure 2.18 Comparison of the relative interrogation zones of different systems

The speed of transponders, relative to readers, together with the maximum write/read distance, determines the length of time spent in the reader's interrogation zone. For the identification of vehicles, the required range of the RFID system is designed such that at the maximum vehicle speed the length of time spent in the interrogation zone is sufficient for the transmission of the required data.

2.5.3 Security requirements

Security requirements to be imposed on a planned RFID application, i.e. *encryption* and *authentication*, should be assessed very precisely to rule out any nasty surprises in the implementation phase. For this purpose, the incentive that the system represents to a potential attacker as a means of procuring money or material goods by manipulation should be evaluated. In order to be able to assess this attraction, we divide applications into two groups:

- industrial or closed applications;
- public applications connected with money and material goods.

This can be illustrated on the basis of two contrasting application examples.

Let us once again consider an assembly line in the automotive industry as a typical example of an industrial or closed application. Only authorised persons have access to this RFID system, so the circle of potential attackers remains reasonably small. A malicious *attack* on the system by the alteration or falsification of the data on a transponder could bring about a critical malfunction in the operating sequence, but the attacker would not gain any personal benefit. The probability of an attack can thus be

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

set equal to zero, meaning that even a cheap low-end system without security logic can be used.

Our second example is a ticketing system for use in public transport. Such a system, primarily data carriers in the form of contactless smart cards, is accessible to anyone. The circle of potential attackers is thus enormous. A successful attack on such a system could represent large-scale financial damage to the public transport company in question, for example in the event of the organised sale of falsified travel passes, to say nothing of the damage to the company's image. For such applications a high-end transponder with authentication and encryption procedures is indispensable. For applications with maximum security requirements, for example banking applications with an electronic purse, only transponders with microprocessors should be used.

2.5.4 Memory capacity

The chip size of the data carrier — and thus the price class — is primarily determined by its *memory capacity*. Therefore, permanently encoded read-only data carriers are used in price-sensitive mass applications with a low local information requirement. However, only the identity of an object can be defined using such a data carrier. Further data is stored in the central database of the controlling computer. If data is to be written back to the transponder, a transponder with EEPROM or RAM memory technology is required.

EEPROM memories are primarily found in inductively coupled systems. Memory capacities of 16 bytes to 8 Kbytes are available.

SRAM memory devices with a battery backup, on the other hand, are predominantly used in microwave systems. The memory capacities on offer range from 256 bytes to 64 Kbytes.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

3

Fundamental Operating Principles

This chapter describes the basic interaction between transponder and reader, in particular the power supply to the transponder and the data transfer between transponder and reader (Figure 3.1). For a more in-depth description of the physical interactions and mathematical models relating to inductive coupling or backscatter systems please refer to Chapter 4.

3.1 1-Bit Transponder

A bit is the smallest unit of information that can be represented and has only two states: 1 and 0. This means that only two states can be represented by systems based upon a *1-bit transponder*: 'transponder in interrogation zone' and 'no transponder in interrogation zone'. Despite this limitation, 1-bit transponders are very widespread — their main field of application is in electronic *anti-theft devices* in shops (*EAS*, electronic article surveillance).

An EAS system is made up of the following components: the antenna of a 'reader' or interrogator, the *security element* or *tag*, and an optional *deactivation device* for deactivating the tag after payment. In modern systems deactivation takes place when the price code is registered at the till. Some systems also incorporate an *activator*, which is used to reactivate the security element after deactivation (Gillert, 1997). The main performance characteristic for all systems is the recognition or *detection rate* in relation to the gate width (maximum distance between transponder and interrogator antenna).

The procedure for the inspection and testing of installed article surveillance systems is specified in the guideline *VDI 4470* entitled 'Anti-theft systems for goods — detection gates. Inspection guidelines for customers'. This guideline contains definitions and testing procedures for the calculation of the detection rate and false alarm ratio. It can be used by the retail trade as the basis for sales contracts or for monitoring the performance of installed systems on an ongoing basis. For the product manufacturer, the Inspection Guidelines for Customers represents an effective benchmark in the development and optimisation of integrated solutions for security projects (in accordance with VDI 4470).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

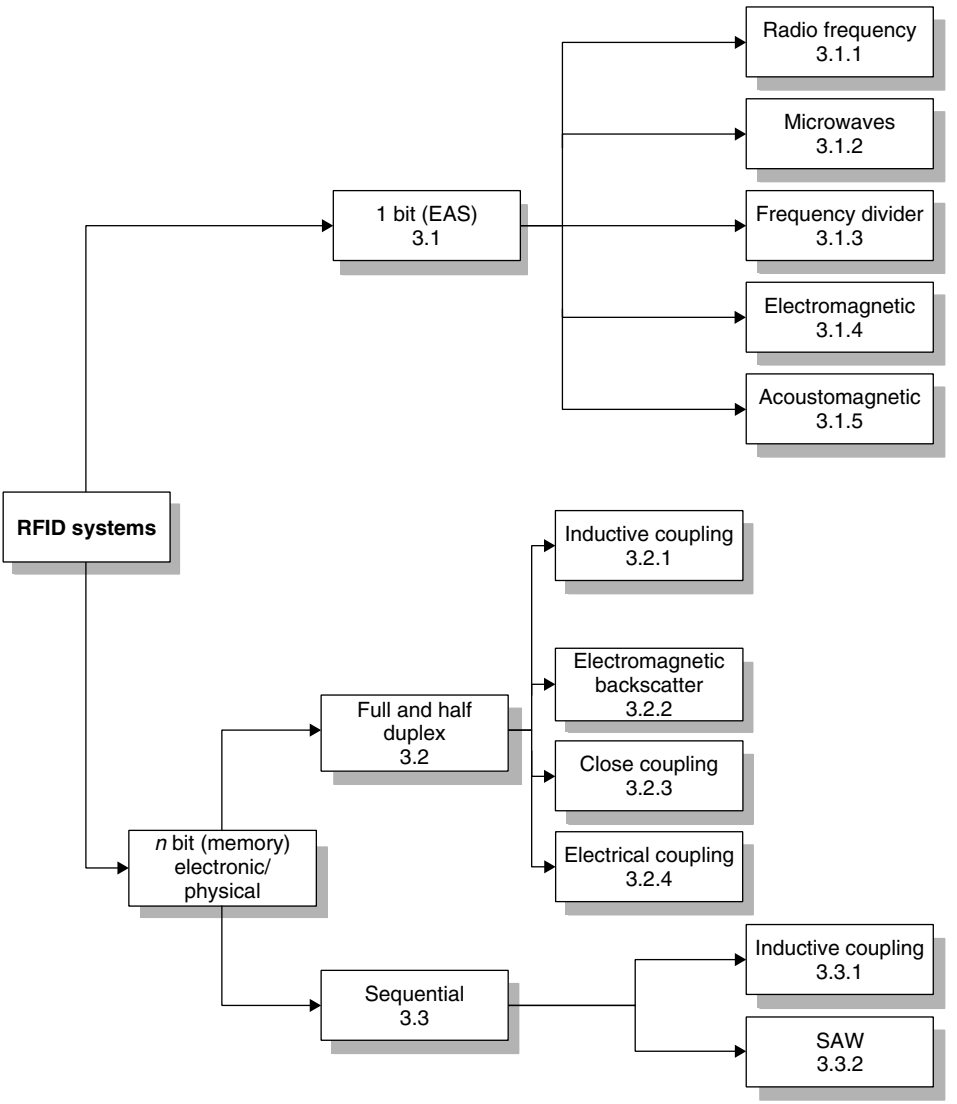


Figure 3.1 The allocation of the different operating principles of RFID systems into the sections of the chapter

3.1.1 Radio frequency

The *radio frequency (RF) procedure* is based upon LC resonant circuits adjusted to a defined resonant frequency f_R. Early versions employed inductive resistors made of wound enamelled copper wire with a soldered on capacitor in a plastic housing (*hard tag*). Modern systems employ coils etched between foils in the form of stick-on labels. To ensure that the damping resistance does not become too high and reduce the quality of the resonant circuit to an unacceptable level, the thickness of

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

the aluminium conduction tracks on the 25 μm thick *polyethylene foil* must be at least 50 μm (Jörn, 1994). Intermediate foils of 10 μm thickness are used to manufacture the capacitor plates.

The reader (detector) generates a magnetic alternating field in the radio frequency range (Figure 3.2). If the LC resonant circuit is moved into the vicinity of the magnetic alternating field, energy from the alternating field can be induced in the resonant circuit via its coils (Faraday's law). If the frequency f_G of the alternating field corresponds with the resonant frequency f_R of the LC resonant circuit the resonant circuit produces a *sympathetic oscillation*. The current that flows in the resonant circuit as a result of this acts against its cause, i.e. it acts against the external magnetic alternating field (see Section 4.1.10.1). This effect is noticeable as a result of a small change in the voltage drop across the transmitter's generator coil and ultimately leads to a weakening of the measurable magnetic field strength. A change to the induced voltage can also be detected in an optional sensor coil as soon as a resonant oscillating circuit is brought into the magnetic field of the generator coil.

The relative magnitude of this dip is dependent upon the gap between the two coils (generator coil — security element, security element — sensor coil) and the quality Q of the induced resonant circuit (in the security element).

The relative magnitude of the changes in voltage at the generator and sensor coils is generally very low and thus difficult to detect. However, the signal should be as clear as possible so that the security element can be reliably detected. This is achieved using a bit of a trick: the frequency of the magnetic field generated is not constant, it is 'swept'. This means that the generator frequency continuously crosses the range between minimum and maximum. The frequency range available to the swept systems is 8.2 MHz ±10% (Jörn, 1994).

Whenever the swept generator frequency exactly corresponds with the resonant frequency of the resonant circuit (in the transponder), the transponder begins to oscillate, producing a clear dip in the voltages at the generator and sensor coils (Figure 3.3). Frequency tolerances of the security element, which depend upon manufacturing tolerances

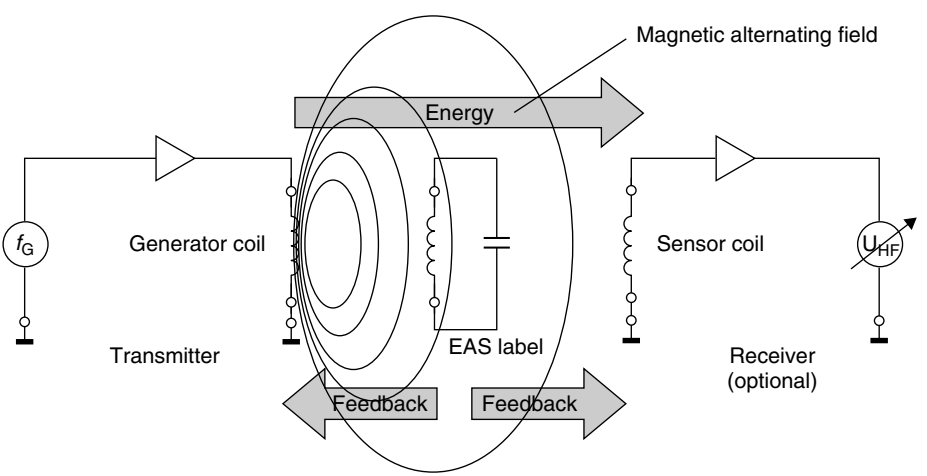


Figure 3.2 Operating principle of the EAS radio frequency procedure

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

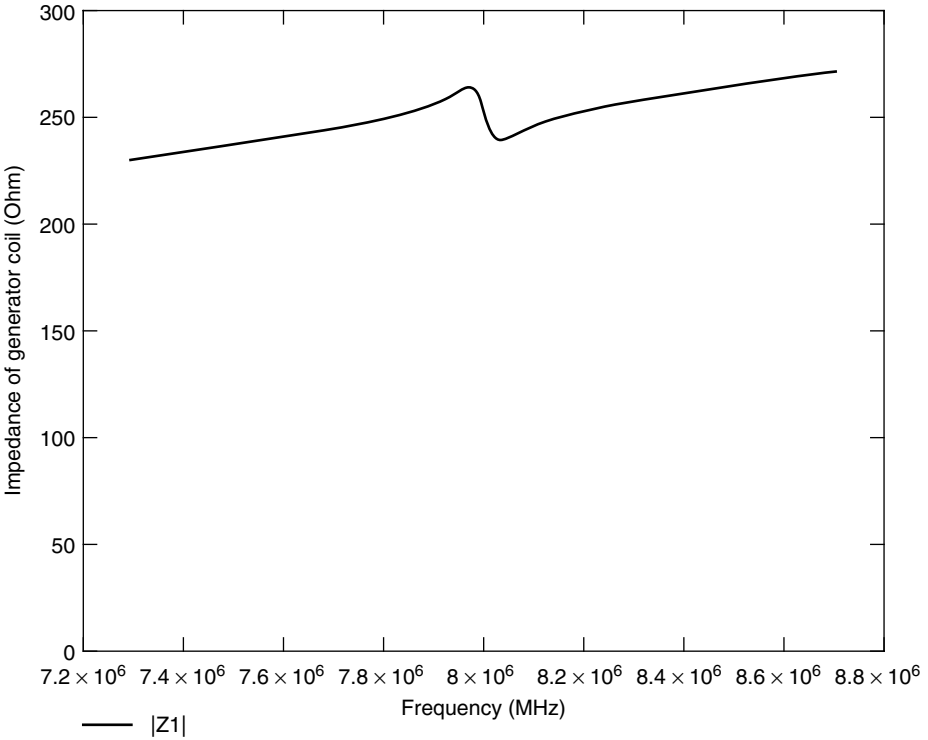


Figure 3.3 The occurrence of an impedance 'dip' at the generator coil at the resonant frequency of the security element ($Q = 90$, $k = 1\%$). The generator frequency f_G is continuously swept between two cut-off frequencies. An RF tag in the generator field generates a clear dip at its resonant frequency f_R

and vary in the presence of a metallic environment, no longer play a role as a result of the 'scanning' of the entire frequency range.

Because the tags are not removed at the till, they must be altered so that they do not activate the anti-theft system. To achieve this, the cashier places the protected product into a device — the deactivator — that generates a sufficiently high magnetic field that the induced voltage destroys the foil capacitor of the transponder. The capacitors are designed with intentional short-circuit points, so-called *dimples*. The breakdown of the capacitors is irreversible and detunes the resonant circuit to such a degree that this can no longer be excited by the *sweep signal*.

Large area *frame antennas* are used to generate the required magnetic alternating field in the detection area. The frame antennas are integrated into columns and combined to form gates. The classic design that can be seen in every large department store is illustrated in Figure 3.4. Gate widths of up to 2 m can be achieved using the RF procedure. The relatively low detection rate of 70% (Gillert, 1997) is disproportionately influenced by certain product materials. Metals in particular (e.g. food tins) affect the resonant frequency of the tags and the coupling to the detector coil and thus have a negative effect on the detection rate. Tags of 50 mm × 50 mm must be used to achieve the gate width and detection rate mentioned above.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

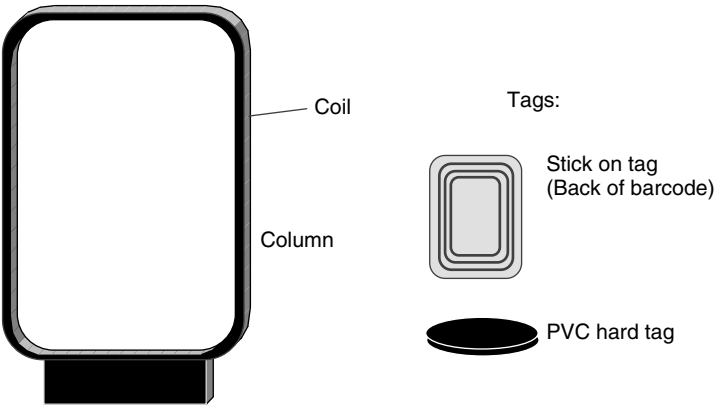


Figure 3.4 Left, typical frame antenna of an RF system (height 1.20–1.60 m); right, tag designs

Table 3.1 Typical system parameters for RF systems (VDI 4471)

Quality factor Q of the security element	>60–80
Minimum deactivation field strength H_D	1.5 A/m
Maximum field strength in the deactivation range	0.9 A/m

Table 3.2 Frequency range of different RF security systems (Plotzke *et al.*, 1994)

	System 1	System 2	System 3	System 4
Frequency (MHz)	1.86–2.18	7.44–8.73	7.30–8.70	7.40–8.60
Sweep frequency (Hz)	141	141	85	85

The range of products that have their own resonant frequencies (e.g. cable drums) presents a great challenge for system manufacturers. If these resonant frequencies lie within the sweep frequency 8.2 MHz ± 10% they will always trigger false alarms.

3.1.2 Microwaves

EAS systems in the *microwave range* exploit the generation of harmonics at components with nonlinear characteristic lines (e.g. diodes). The *harmonic* of a sinusoidal voltage A with a defined frequency f_A is a sinusoidal voltage B, whose frequency f_B is an integer multiple of the frequency f_A. The subharmonics of the frequency f_A are thus the frequencies $2f_A$, $3f_A$, $4f_A$ etc. The Nth multiple of the output frequency is termed the Nth harmonic (Nth harmonic wave) in radio-engineering; the output frequency itself is termed the carrier wave or first harmonic.

In principle, every two-terminal network with a nonlinear characteristic generates harmonics at the first harmonic. In the case of *nonlinear resistances*, however, energy is consumed, so that only a small part of the first harmonic power is converted into the harmonic oscillation. Under favourable conditions, the multiplication of f_A to $n \times f_A$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

occurs with an efficiency of $\eta = 1/n^2$. However, if nonlinear energy storage is used for multiplication, then in the ideal case there are no losses (Fleckner, 1987).

Capacitance diodes are particularly suitable nonlinear energy stores for frequency multiplication. The number and intensity of the harmonics that are generated depend upon the capacitance diode's *dopant profile* and characteristic line gradient. The exponent n (also γ) is a measure for the gradient (=capacitance-voltage characteristic). For simple diffused diodes, this is 0.33 (e.g. BA110), for alloyed diodes it is 0.5 and for tuner diodes with a hyper-abrupt P-N junction it is around 0.75 (e.g. BB 141) (Intermetal Semiconductors ITT, 1996).

The capacitance-voltage characteristic of alloyed capacitance diodes has a quadratic path and is therefore best suited for the doubling of frequencies. Simple diffused diodes can be used to produce higher harmonics (Fleckner, 1987).

The layout of a 1-bit transponder for the generation of harmonics is extremely simple: a capacitance diode is connected to the base of a *dipole* adjusted to the carrier wave (Figure 3.5). Given a carrier wave frequency of 2.45 GHz the dipole has a total length of 6 cm. The carrier wave frequencies used are 915 MHz (outside Europe), 2.45 GHz or 5.6 GHz. If the transponder is located within the transmitter's range, then the flow of current within the diode generates and re-emits harmonics of the carrier wave. Particularly distinctive signals are obtained at two or three times the carrier wave, depending upon the type of diode used.

Transponders of this type cast in plastic (hard tags) are used mainly to protect textiles. The tags are removed at the till when the goods are paid for and they are subsequently reused.

Figure 3.6 shows a transponder being placed within the range of a microwave transmitter operating at 2.45 GHz. The second harmonic of 4.90 GHz generated in the diode characteristic of the transponder is re-transmitted and detected by a receiver, which is adjusted to this precise frequency. The reception of a signal at the frequency of the second harmonic can then trigger an alarm system.

If the amplitude or frequency of the carrier wave is modulated (ASK, FSK), then all harmonics incorporate the same modulation. This can be used to distinguish between 'interference' and 'useful' signals, preventing false alarms caused by external signals.

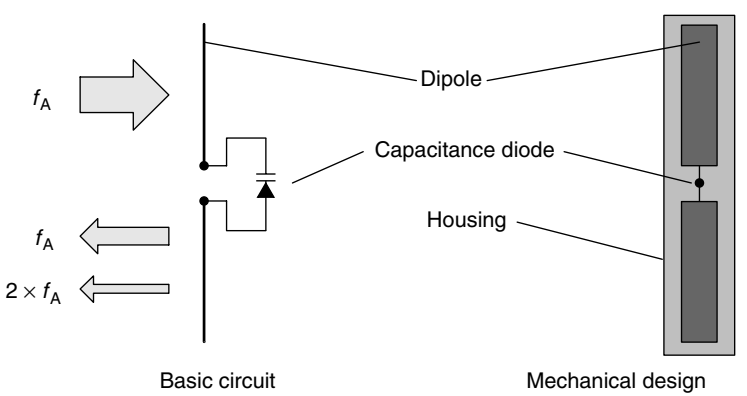


Figure 3.5 Basic circuit and typical construction format of a microwave tag

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

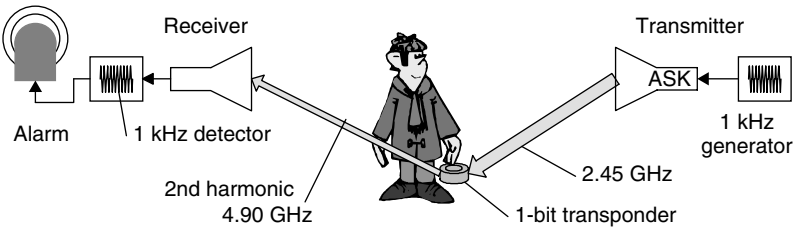


Figure 3.6 Microwave tag in the interrogation zone of a detector

In the example above, the amplitude of the carrier wave is modulated with a signal of 1 kHz (100% ASK). The second harmonic generated at the transponder is also modulated at 1 kHz ASK. The signal received at the receiver is demodulated and forwarded to a 1 kHz detector. Interference signals that happen to be at the reception frequency of 4.90 GHz cannot trigger false alarms because these are not normally modulated and, if they are, they will have a different modulation.

3.1.3 Frequency divider

This procedure operates in the long wave range at 100–135.5 kHz. The security tags contain a semiconductor circuit (microchip) and a resonant circuit coil made of wound enamelled copper. The resonant circuit is made to resonate at the operating frequency of the EAS system using a soldered capacitor. These transponders can be obtained in the form of hard tags (plastic) and are removed when goods are purchased.

The microchip in the transponder receives its power supply from the magnetic field of the security device (see Section 3.2.1.1). The frequency at the self-inductive coil is divided by two by the microchip and sent back to the security device. The signal at half the original frequency is fed by a tap into the resonant circuit coil (Figure 3.7).

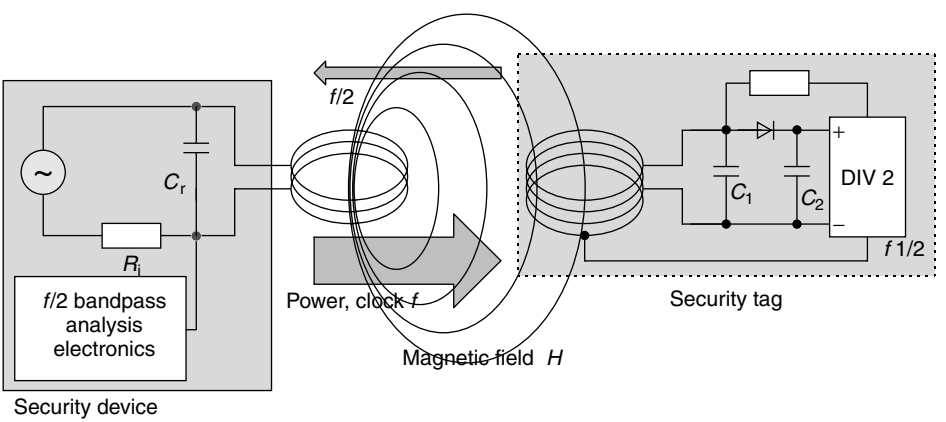


Figure 3.7 Basic circuit diagram of the EAS frequency division procedure: security tag (transponder) and detector (evaluation device)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 3.3 Typical system parameters (Plotzke *et al.*, 1994)

Frequency	130 kHz
Modulation type:	100% ASK
Modulation frequency/modulation signal:	12.5 Hz or 25 Hz, rectangle 50%

The magnetic field of the security device is pulsed at a lower frequency (ASK modulated) to improve the detection rate. Similarly to the procedure for the generation of harmonics, the modulation of the carrier wave (ASK or FSK) is maintained at half the frequency (*subharmonic*). This is used to differentiate between 'interference' and 'useful' signals. This system almost entirely rules out false alarms.

Frame antennas, described in Section 3.1.1, are used as sensor antennas.

3.1.4 Electromagnetic types

Electromagnetic types operate using strong magnetic fields in the *NF range* from 10 Hz to around 20 kHz. The security elements contain a soft magnetic *amorphous metal* strip with a steep flanked hysteresis curve (see also Section 4.1.12). The magnetisation of these strips is periodically reversed and the strips taken to magnetic saturation by a strong magnetic alternating field. The markedly nonlinear relationship between the applied field strength H and the magnetic flux density B near saturation (see also Figure 4.50), plus the sudden change of flux density B in the vicinity of the zero crossover of the applied field strength H, generates harmonics at the basic frequency of the security device, and these harmonics can be received and evaluated by the security device.

The electromagnetic type is optimised by superimposing additional signal sections with higher frequencies over the main signal. The marked nonlinearity of the strip's hysteresis curve generates not only harmonics but also signal sections with summation and differential frequencies of the supplied signals. Given a main signal of frequency $f_S = 20\,\text{Hz}$ and the additional signals $f_1 = 3.5$ and $f_2 = 5.3\,\text{kHz}$, the following signals are generated (first order):

$$f_1 + f_2 = f_{1+2} = 8.80\,\text{kHz}$$

$$f_1 - f_2 = f_{1-2} = 1.80\,\text{kHz}$$

$$f_S + f_1 = f_{S+1} = 3.52\,\text{kHz and so on}$$

The security device does not react to the harmonic of the basic frequency in this case, but rather to the summation or differential frequency of the extra signals.

The tags are available in the form of self-adhesive strips with lengths ranging from a few centimetres to 20 cm. Due to the extremely low operating frequency, electromagnetic systems are the only systems suitable for products containing metal. However, these systems have the disadvantage that the function of the tags is dependent upon position: for reliable detection the magnetic field lines of the security device must run vertically through the amorphous metal strip. Figure 3.8 shows a typical design for a security system.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

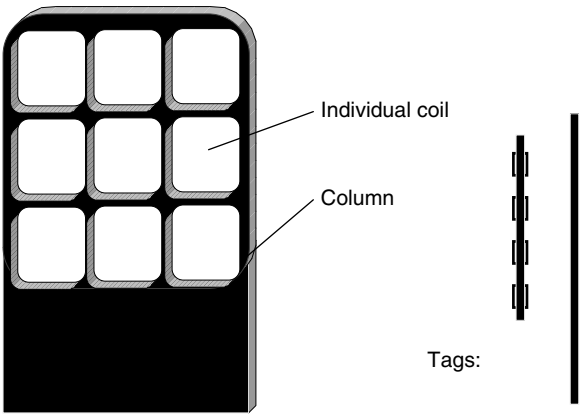


Figure 3.8 Left, typical antenna design for a security system (height approximately 1.40 m); right, possible tag designs

For deactivation, the tags are coated with a layer of hard magnetic metal or partially covered by hard magnetic plates. At the till the cashier runs a strong *permanent magnet* along the metal strip to deactivate the security elements (Plotzke *et al.*, 1994). This magnetises the hard magnetic metal plates. The metal strips are designed such that the remanence field strength (see Section 4.1.12) of the plate is sufficient to keep the amorphous metal strips at saturation point so that the magnetic alternating field of the security system can no longer be activated.

The tags can be reactivated at any time by demagnetisation. The process of deactivation and reactivation can be performed any number of times. For this reason, electromagnetic goods protection systems were originally used mainly in lending libraries. Because the tags are small (min. 32 mm short strips) and cheap, these systems are now being used increasingly in the grocery industry. See Figure 3.9.

In order to achieve the field strength necessary for demagnetisation of the permalloy strips, the field is generated by two coil systems in the columns at either side of a narrow passage. Several individual coils, typically 9 to 12, are located in the two pillars, and these generate weak magnetic fields in the centre and stronger magnetic fields on the outside (Plotzke *et al.*, 1994). Gate widths of up to 1.50 m can now be realised using this method, while still achieving detection rates of 70% (Gillert, 1997) (Figure 3.10).

3.1.5 Acoustomagnetic

Acoustomagnetic systems for security elements consist of extremely small plastic boxes around 40 mm long, 8 to 14 mm wide depending upon design, and just a millimetre

Table 3.4 Typical system parameters (Plotzke *et al.*, 1997)

Frequency	70 Hz
Optional combination frequencies of different systems	12 Hz, 215 Hz, 3.3 kHz, 5 kHz
Field strength H_{eff} in the detection zone	25–120 A/m
Minimum field strength for deactivation	16 000 A/m

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



Figure 3.9 Electromagnetic labels in use (reproduced by permission of Schreiner Codedruck, Munich)



Figure 3.10 Practical design of an antenna for an article surveillance system (reproduced by permission of METO EAS System 2200, Esselte Meto, Hirschborn)

high. The boxes contain two metal strips, a *hard magnetic metal strip* permanently connected to the plastic box, plus a strip made of *amorphous metal*, positioned such that it is free to vibrate mechanically (Zechbauer, 1999).

Ferromagnetic metals (nickel, iron etc.) change slightly in length in a magnetic field under the influence of the field strength H. This effect is called *magnetostriction* and results from a small change in the interatomic distance as a result of magnetisation. In

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

a magnetic alternating field a magnetostrictive metal strip vibrates in the longitudinal direction at the frequency of the field. The amplitude of the vibration is especially high if the frequency of the magnetic alternating field corresponds with that of the (acoustic) resonant frequency of the metal strip. This effect is particularly marked in amorphous materials.

The decisive factor is that the magnetostrictive effect is also reversible. This means that an oscillating magnetostrictive metal strip emits a magnetic alternating field. *Acoustomagnetic security systems* are designed such that the frequency of the magnetic alternating field generated precisely coincides with the resonant frequencies of the metal strips in the security element. The amorphous metal strip begins to oscillate under the influence of the magnetic field. If the magnetic alternating field is switched off after some time, the excited magnetic strip continues to oscillate for a while like a tuning fork and thereby itself generates a magnetic alternating field that can easily be detected by the security system (Figure 3.11).

The great advantage of this procedure is that the security system is not itself transmitting while the security element is responding and the detection receiver can thus be designed with a corresponding degree of sensitivity.

In their activated state, acoustomagnetic security elements are magnetised, i.e. the above-mentioned hard magnetic metal strip has a high remanence field strength and thus forms a permanent magnet. To deactivate the security element the hard magnetic metal strip must be demagnetised. This detunes the resonant frequency of the amorphous

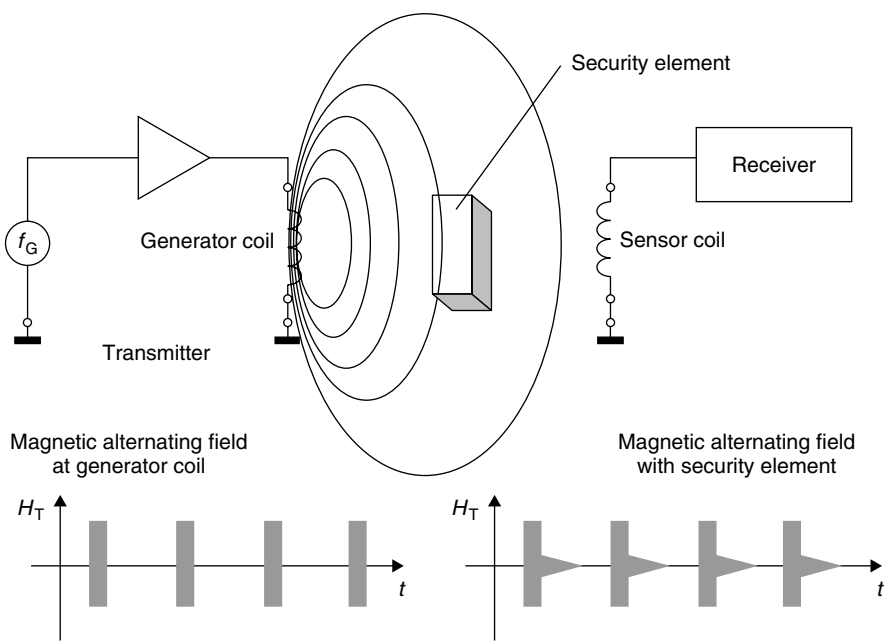


Figure 3.11 Acoustomagnetic system comprising transmitter and detection device (receiver). If a security element is within the field of the generator coil this oscillates like a tuning fork in time with the pulses of the generator coil. The transient characteristics can be detected by an analysing unit

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 3.5 Typical operating parameters of acoustomagnetic systems (VDI 4471)

Parameter	Typical value
Resonant frequency f_0	58 kHz
Frequency tolerance	±0.52%
Quality factor Q	>150
Minimum field strength H_A for activation	>16 000 A/m
ON duration of the field	2 ms
Field pause (OFF duration)	20 ms
Decay process of the security element	5 ms

metal strip so it can no longer be excited by the operating frequency of the security system. The hard magnetic metal strip can only be demagnetised by a strong magnetic alternating field with a slowly decaying field strength. It is thus absolutely impossible for the security element to be manipulated by permanent magnets brought into the store by customers.

3.2 Full and Half Duplex Procedure

In contrast to 1-bit transponders, which normally exploit simple physical effects (oscillation stimulation procedures, stimulation of harmonics by diodes or the nonlinear hysteresis curve of metals), the transponders described in this and subsequent sections use an electronic microchip as the data-carrying device. This has a data storage capacity of up to a few kilobytes. To read from or write to the data-carrying device it must be possible to transfer data between the transponder and a reader. This transfer takes place according to one of two main procedures: full and half duplex procedures, which are described in this section, and sequential systems, which are described in the following section.

In the *half duplex procedure* (HDX) the data transfer from the transponder to the reader alternates with data transfer from the reader to the transponder. At frequencies below 30 MHz this is most often used with the load modulation procedure, either with or without a subcarrier, which involves very simple circuitry. Closely related to this is the modulated reflected cross-section procedure that is familiar from radar technology and is used at frequencies above 100 MHz. Load modulation and modulated reflected cross-section procedures directly influence the magnetic or electromagnetic field generated by the reader and are therefore known as *harmonic* procedures.

In the *full duplex procedure* (FDX) the data transfer from the transponder to the reader takes place at the same time as the data transfer from the reader to the transponder. This includes procedures in which data is transmitted from the transponder at a fraction of the frequency of the reader, i.e. a *subharmonic*, or at a completely independent, i.e. an *anharmonic*, frequency.

However, both procedures have in common the fact that the transfer of energy from the reader to the transponder is continuous, i.e. it is independent of the direction of data flow. In sequential systems (SEQ), on the other hand, the transfer of energy from the transponder to the reader takes place for a limited period of time only (pulse

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

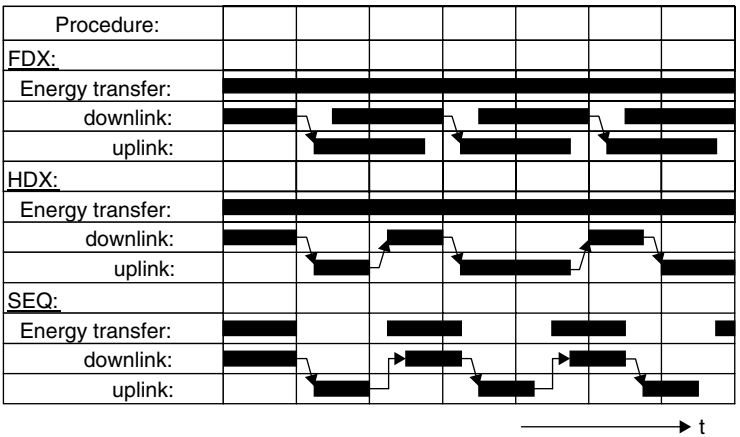


Figure 3.12 Representation of full duplex, half duplex and sequential systems over time. Data transfer from the reader to the transponder is termed downlink, while data transfer from the transponder to the reader is termed uplink

operation → *pulsed system*). Data transfer from the transponder to the reader occurs in the pauses between the power supply to the transponder. See Figure 3.12 for a representation of full duplex, half duplex and sequential systems.

Unfortunately, the literature relating to RFID has not yet been able to agree a consistent nomenclature for these system variants. Rather, there has been a confusing and inconsistent classification of individual systems into full and half duplex procedures. Thus pulsed systems are often termed half duplex systems — this is correct from the point of view of data transfer — and all unpulsed systems are falsely classified as full duplex systems. For this reason, in this book pulsed systems — for differentiation from other procedures, and unlike most RFID literature(!) — are termed sequential systems (SEQ).

3.2.1 Inductive coupling

3.2.1.1 Power supply to passive transponders

An inductively coupled transponder comprises an electronic data-carrying device, usually a single microchip, and a large area coil that functions as an antenna.

Inductively coupled transponders are almost always operated passively. This means that all the energy needed for the operation of the microchip has to be provided by the reader (Figure 3.13). For this purpose, the reader's antenna coil generates a strong, high frequency electromagnetic field, which penetrates the cross-section of the coil area and the area around the coil. Because the wavelength of the frequency range used (<135 kHz: 2400 m, 13.56 MHz: 22.1 m) is several times greater than the distance between the reader's antenna and the transponder, the electromagnetic field may be treated as a simple magnetic alternating field with regard to the distance between transponder and antenna (see Section 4.2.1.1 for further details).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

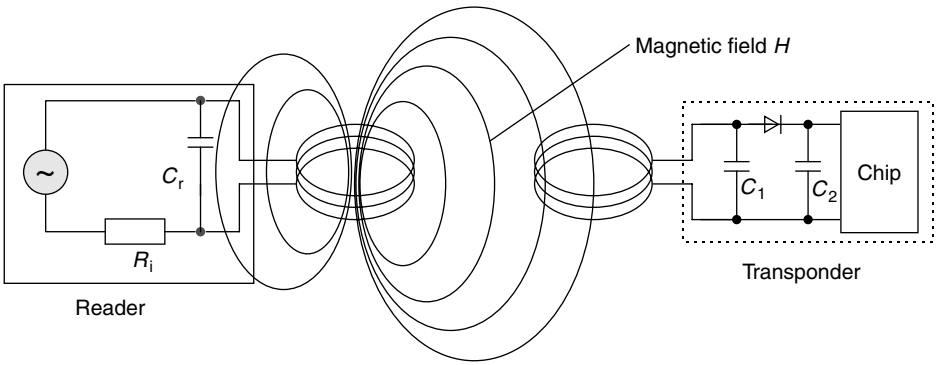


Figure 3.13 Power supply to an inductively coupled transponder from the energy of the magnetic alternating field generated by the reader

A small part of the emitted field penetrates the antenna coil of the transponder, which is some distance away from the coil of the reader. A voltage U_i is generated in the transponder's antenna coil by inductance. This voltage is rectified and serves as the power supply for the data-carrying device (microchip). A capacitor C_r is connected in parallel with the reader's antenna coil, the capacitance of this capacitor being selected such that it works with the coil inductance of the antenna coil to form a parallel resonant circuit with a resonant frequency that corresponds with the transmission frequency of the reader. Very high currents are generated in the antenna coil of the reader by resonance step-up in the parallel resonant circuit, which can be used to generate the required field strengths for the operation of the remote transponder.

The antenna coil of the transponder and the capacitor C_1 form a resonant circuit tuned to the transmission frequency of the reader. The voltage U at the transponder coil reaches a maximum due to resonance step-up in the parallel resonant circuit.

The layout of the two coils can also be interpreted as a transformer (*transformer coupling*), in which case there is only a very weak coupling between the two windings (Figure 3.14). The efficiency of power transfer between the antenna coil of the reader and the transponder is proportional to the operating frequency f, the number of windings n, the area A enclosed by the transponder coil, the angle of the two coils relative to each other and the distance between the two coils.

As frequency f increases, the required coil inductance of the transponder coil, and thus the number of windings n decreases (135 kHz: typical 100–1000 windings, 13.56 MHz: typical 3–10 windings). Because the voltage induced in the transponder is still proportional to frequency f (see Chapter 4), the reduced number of windings barely affects the efficiency of power transfer at higher frequencies. Figure 3.15 shows a reader for an inductively coupled transponder.

3.2.1.2 Data transfer transponder → reader

Load modulation As described above, inductively coupled systems are based upon a *transformer-type coupling* between the primary coil in the reader and the secondary coil in the transponder. This is true when the distance between the coils does not exceed

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



Figure 3.14 Different designs of inductively coupled transponders. The photo shows half finished transponders, i.e. transponders before injection into a plastic housing (reproduced by permission of AmaTech GmbH & Co. KG, D-Pfronten)



Figure 3.15 Reader for inductively coupled transponder in the frequency range <135 kHz with integral antenna (reproduced by permission of easy-key System, micron, Halbergmoos)

0.16 λ, so that the transponder is located in the *near field* of the transmitter antenna (for a more detailed definition of the near and far fields, please refer to Chapter 4).

If a resonant transponder (i.e. a transponder with a self-resonant frequency corresponding with the transmission frequency of the reader) is placed within the magnetic alternating field of the reader's antenna, the transponder draws energy from the magnetic field. The resulting feedback of the transponder on the reader's antenna can be

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 3.6 Overview of the power consumption of various RFID-ASIC building blocks (Atmel, 1994). The minimum supply voltage required for the operation of the microchip is 1.8 V, the maximum permissible voltage is 10 V

	Memory (Bytes)	Write/read distance	Power consumption	Frequency	Application
ASIC#1	6	15 cm	10 µA	120 kHz	Animal ID
ASIC#2	32	13 cm	600 µA	120 kHz	Goods flow, access check
ASIC#3	256	2 cm	6 µA	128 kHz	Public transport
ASIC#4	256	0.5 cm	<1 mA	4 MHz*	Goods flow, public transport
ASIC#5	256	<2 cm	~1 mA	4/13.56 MHz	Goods flow
ASIC#6	256	100 cm	500 µA	125 kHz	Access check
ASIC#7	2048	0.3 cm	<10 mA	4.91 MHz*	Contactless chip cards
ASIC#8	1024	10 cm	~1 mA	13.56 MHz	Public transport
ASIC#9	8	100 cm	<1 mA	125 kHz	Goods flow
ASIC#10	128	100 cm	<1 mA	125 kHz	Access check

*Close coupling system.

represented as *transformed impedance* Z_T in the antenna coil of the reader. Switching a *load resistor* on and off at the transponder's antenna therefore brings about a change in the impedance Z_T, and thus voltage changes at the reader's antenna (see Section 4.1.10.3). This has the effect of an amplitude modulation of the voltage U_L at the reader's antenna coil by the remote transponder. If the timing with which the load resistor is switched on and off is controlled by data, this data can be transferred from the transponder to the reader. This type of data transfer is called *load modulation*.

To reclaim the data at the reader, the voltage tapped at the reader's antenna is rectified. This represents the demodulation of an amplitude modulated signal. An example circuit is shown in Section 11.3.

Load modulation with subcarrier Due to the weak coupling between the reader antenna and the transponder antenna, the voltage fluctuations at the antenna of the reader that represent the useful signal are smaller by orders of magnitude than the output voltage of the reader.

In practice, for a 13.56 MHz system, given an antenna voltage of approximately 100 V (voltage step-up by resonance) a useful signal of around 10 mV can be expected (=80 dB signal/noise ratio). Because detecting this slight voltage change requires highly complicated circuitry, the modulation sidebands created by the amplitude modulation of the antenna voltage are utilised (Figure 3.16).

If the additional load resistor in the transponder is switched on and off at a very high elementary frequency f_S, then two spectral lines are created at a distance of $\pm f_S$ around the transmission frequency of the reader f_{READER}, and these can be easily detected (however f_S must be less than f_{READER}). In the terminology of radio technology the new elementary frequency is called a *subcarrier*). Data transfer is by ASK, FSK or PSK modulation of the subcarrier in time with the data flow. This represents an amplitude modulation of the subcarrier.

Load modulation with a subcarrier creates two modulation sidebands at the reader's antenna at the distance of the subcarrier frequency around the operating frequency f_{READER} (Figure 3.17). These modulation sidebands can be separated from

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

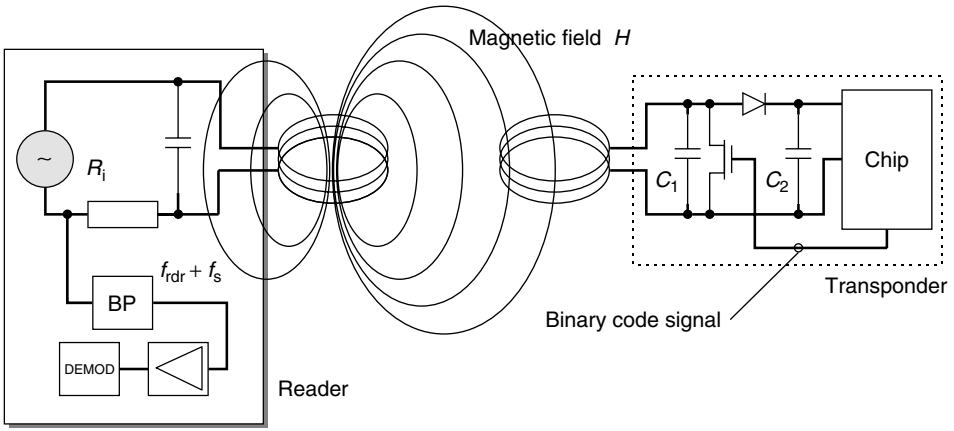


Figure 3.16 Generation of load modulation in the transponder by switching the drain-source resistance of an FET on the chip. The reader illustrated is designed for the detection of a subcarrier

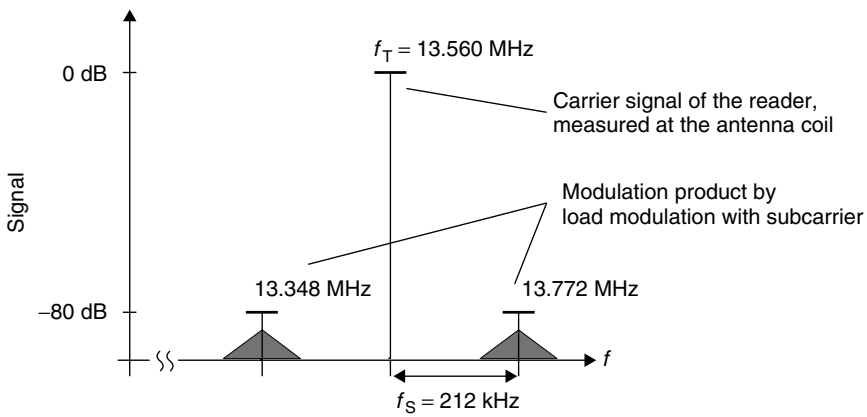


Figure 3.17 Load modulation creates two sidebands at a distance of the subcarrier frequency f_S around the transmission frequency of the reader. The actual information is carried in the sidebands of the two subcarrier sidebands, which are themselves created by the modulation of the subcarrier

the significantly stronger signal of the reader by bandpass (BP) filtering on one of the two frequencies $f_{READER} \pm f_S$. Once it has been amplified, the subcarrier signal is now very simple to demodulate.

Because of the large bandwidth required for the transmission of a subcarrier, this procedure can only be used in the ISM frequency ranges for which this is permitted, 6.78 MHz, 13.56 MHz and 27.125 MHz (see also Chapter 5).

Example circuit–load modulation with subcarrier Figure 3.18 shows an example circuit for a transponder using load modulation with a subcarrier. The circuit is designed for an operating frequency of 13.56 MHz and generates a subcarrier of 212 kHz.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

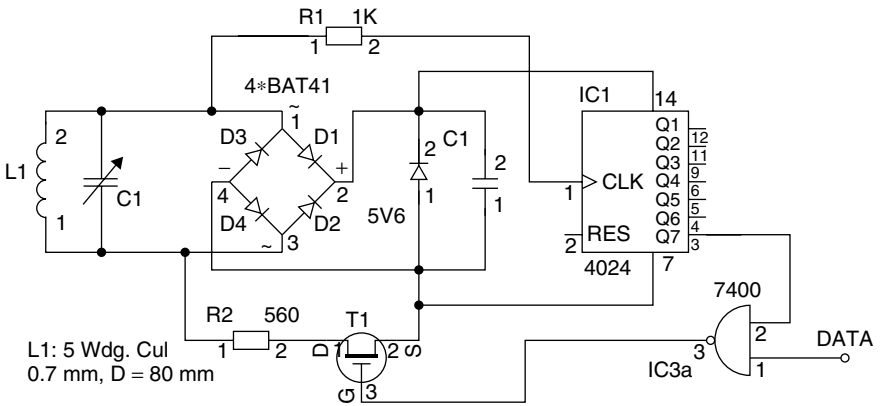


Figure 3.18 Example circuit for the generation of load modulation with subcarrier in an inductively coupled transponder

The voltage induced at the antenna coil L1 by the magnetic alternating field of the reader is rectified using the bridge rectifier (D1–D4) and after additional smoothing (C1) is available to the circuit as supply voltage. The parallel regulator (ZD 5V6) prevents the supply voltage from being subject to an uncontrolled increase when the transponder approaches the reader antenna.

Part of the high frequency antenna voltage (13.56 MHz) travels to the frequency divider's timing input (CLK) via the protective resistor (R1) and provides the transponder with the basis for the generation of an internal clocking signal. After division by $2^6 (= 64)$ a subcarrier clocking signal of 212 kHz is available at output Q7. The subcarrier clocking signal, controlled by a serial data flow at the data input (DATA), is passed to the switch (T1). If there is a logical HIGH signal at the data input (DATA), then the subcarrier clocking signal is passed to the switch (T1). The load resistor (R2) is then switched on and off in time with the subcarrier frequency.

Optionally in the depicted circuit the transponder resonant circuit can be brought into resonance with the capacitor C1 at 13.56 MHz. The range of this 'minimal transponder' can be significantly increased in this manner.

Subharmonic procedure The subharmonic of a sinusoidal voltage A with a defined frequency f_A is a sinusoidal voltage B, whose frequency f_B is derived from an integer division of the frequency f_A. The subharmonics of the frequency f_A are therefore the frequencies $f_A/2$, $f_A/3$, $f_A/4 \ldots$.

In the subharmonic transfer procedure, a second frequency f_B, which is usually lower by a factor of two, is derived by digital division by two of the reader's transmission frequency f_A. The output signal f_B of a binary divider can now be modulated with the data stream from the transponder. The modulated signal is then fed back into the transponder's antenna via an output driver.

One popular operating frequency for subharmonic systems is 128 kHz. This gives rise to a transponder response frequency of 64 kHz.

The transponder's antenna consists of a coil with a central tap, whereby the power supply is taken from one end. The transponder's return signal is fed into the coil's second connection (Figure 3.19).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

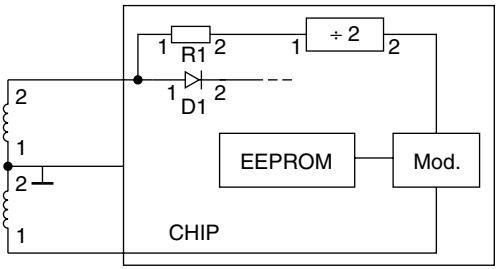


Figure 3.19 Basic circuit of a transponder with subharmonic back frequency. The received clocking signal is split into two, the data is modulated and fed into the transponder coil via a tap

3.2.2 Electromagnetic backscatter coupling

3.2.2.1 Power supply to the transponder

RFID systems in which the gap between reader and transponder is greater than 1 m are called *long-range systems*. These systems are operated at the *UHF frequencies* of 868 MHz (Europe) and 915 MHz (USA), and at the *microwave frequencies* 2.5 GHz and 5.8 GHz. The short wavelengths of these frequency ranges facilitate the construction of antennas with far smaller dimensions and greater efficiency than would be possible using frequency ranges below 30 MHz.

In order to be able to assess the energy available for the operation of a transponder we first calculate the *free space path loss* a_F in relation to the distance r between the transponder and the reader's antenna, the gain G_T and G_R of the transponder's and reader's antenna, plus the transmission frequency f of the reader:

$$a_F = -147.6 + 20\log(r) + 20\log(f) - 10\log(G_T) - 10\log(G_R) \qquad (3.1)$$

The free space path loss is a measure of the relationship between the HF power emitted by a reader into 'free space' and the HF power received by the transponder.

Using current low power semiconductor technology, transponder chips can be produced with a power consumption of no more than 5 μW (Friedrich and Annala, 2001). The efficiency of an integrated rectifier can be assumed to be 5–25% in the UHF and microwave range (Tanneberger, 1995). Given an efficiency of 10%, we thus require received power of $P_e = 50\,\mu W$ at the terminal of the transponder antenna for the operation of the transponder chip. This means that where the reader's transmission power is $P_s = 0.5$ W EIRP (effective isotropic radiated power) the free space path loss may not exceed 40 dB ($P_s/P_e = 10\,000/1$) if sufficiently high power is to be obtained at the transponder antenna for the operation of the transponder. A glance at Table 3.7 shows that at a transmission frequency of 868 MHz a *range* of a little over 3 m would be realisable; at 2.45 GHz a little over 1 m could be achieved. If the transponder's chip had a greater power consumption the achievable range would fall accordingly.

In order to achieve long ranges of up to 15 m or to be able to operate transponder chips with a greater power consumption at an acceptable range, backscatter transponders often have a backup battery to supply power to the transponder chip (Figure 3.20). To prevent this battery from being loaded unnecessarily, the microchips generally have

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 3.7 Free space path loss a_F at different frequencies and distances. The gain of the transponder's antenna was assumed to be 1.64 (dipole), the gain of the reader's antenna was assumed to be 1 (isotropic emitter)

Distance r	868 MHz	915 MHz	2.45 GHz
0.3 m	18.6 dB	19.0 dB	27.6 dB
1 m	29.0 dB	29.5 dB	38.0 dB
3 m	38.6 dB	39.0 dB	47.6 dB
10 m	49.0 dB	49.5 dB	58.0 dB

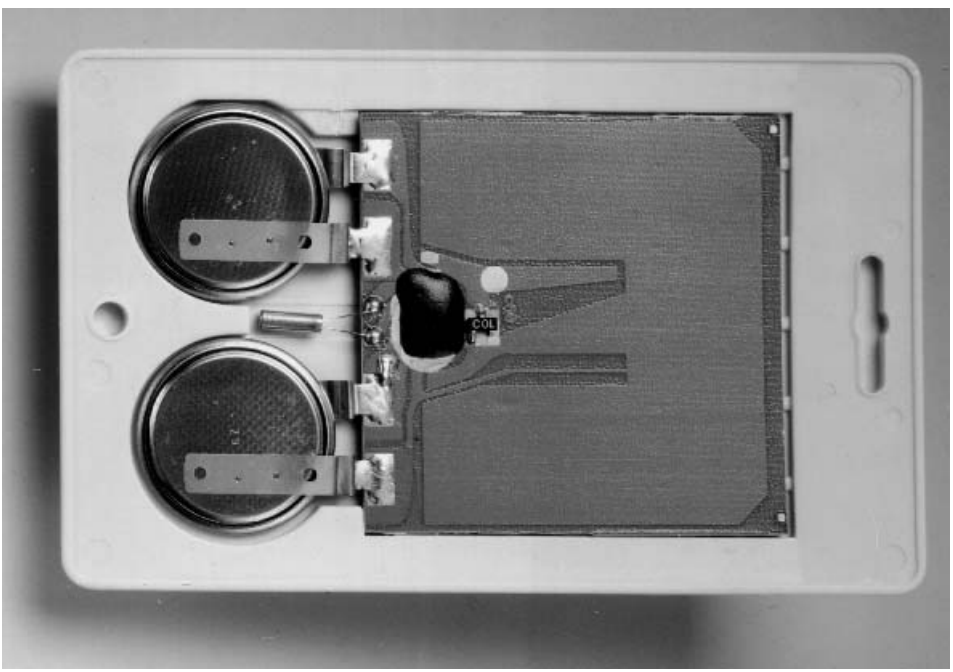


Figure 3.20 Active transponder for the frequency range 2.45 GHz. The data carrier is supplied with power by two *lithium batteries*. The transponder's microwave antenna is visible on the printed circuit board in the form of a u-shaped area (reproduced by permission of Pepperl & Fuchs, Mannheim)

a power saving 'power down' or 'stand-by' mode. If the transponder moves out of range of a reader, then the chip automatically switches over to the power saving 'power down' mode. In this state the power consumption is a few μA at most. The chip is not reactivated until a sufficiently strong signal is received in the read range of a reader, whereupon it switches back to normal operation. However, the battery of an active transponder never provides power for the transmission of data between transponder and reader, but serves exclusively for the supply of the microchip. Data transmission between transponder and reader relies exclusively upon the power of the electromagnetic field emitted by the reader.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

3.2.2.2 Data transmission → reader

Modulated reflection cross-section We know from the field of *radar technology* that electromagnetic waves are reflected by objects with dimensions greater than around half the wavelength of the wave. The efficiency with which an object reflects electromagnetic waves is described by its *reflection cross-section*. Objects that are in resonance with the wave front that hits them, as is the case for antennas at the appropriate frequency, for example, have a particularly large reflection cross-section.

Power P_1 is emitted from the reader's antenna, a small proportion of which (free space attenuation) reaches the transponder's antenna (Figure 3.21). The power P_1' is supplied to the antenna connections as HF voltage and after rectification by the diodes D_1 and D_2 this can be used as turn-on voltage for the deactivation or activation of the power saving 'power down' mode. The diodes used here are *low barrier Schottky diodes*, which have a particularly low threshold voltage. The voltage obtained may also be sufficient to serve as a power supply for short ranges.

A proportion of the incoming power P_1' is reflected by the antenna and returned as power P_2. The *reflection characteristics* (=reflection cross-section) of the antenna can be influenced by altering the load connected to the antenna. In order to transmit data from the transponder to the reader, a load resistor R_L connected in parallel with the antenna is switched on and off in time with the data stream to be transmitted. The amplitude of the power P_2 reflected from the transponder can thus be modulated (→ modulated backscatter).

The power P_2 reflected from the transponder is radiated into free space. A small proportion of this (free space attenuation) is picked up by the reader's antenna. The reflected signal therefore travels into the antenna connection of the reader in the backwards direction and can be decoupled using a *directional coupler* and transferred to the receiver input of a reader. The forward signal of the transmitter, which is stronger by powers of ten, is to a large degree suppressed by the directional coupler.

The ratio of power transmitted by the reader and power returning from the transponder (P_1/P_2) can be estimated using the radar equation (for an explanation, refer to Chapter 4).

3.2.3 Close coupling

3.2.3.1 Power supply to the transponder

Close coupling systems are designed for ranges between 0.1 cm and a maximum of 1 cm. The transponder is therefore inserted into the reader or placed onto a marked surface ('*touch & go*') for operation.

Inserting the transponder into the reader, or placing it on the reader, allows the transponder coil to be precisely positioned in the *air gap* of a ring-shaped or U-shaped core. The functional layout of the transponder coil and reader coil corresponds with that of a transformer (Figure 3.22). The reader represents the primary winding and the transponder coil represents the secondary winding of a transformer. A high frequency alternating current in the primary winding generates a high frequency magnetic field in the core and air gap of the arrangement, which also flows through the transponder coil. This power is rectified to provide a power supply to the chip.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

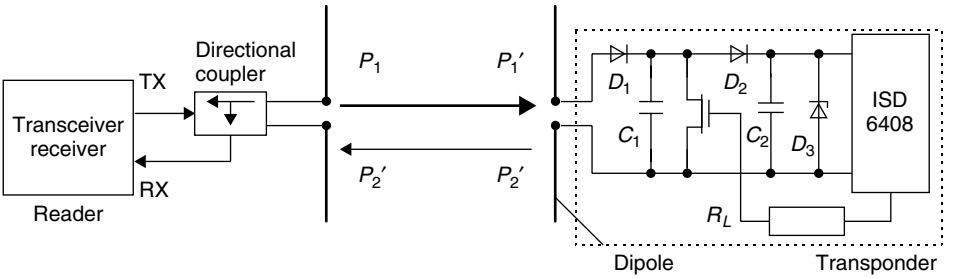


Figure 3.21 Operating principle of a backscatter transponder. The impedance of the chip is 'modulated' by switching the chip's FET (Integrated Silicon Design, 1996)

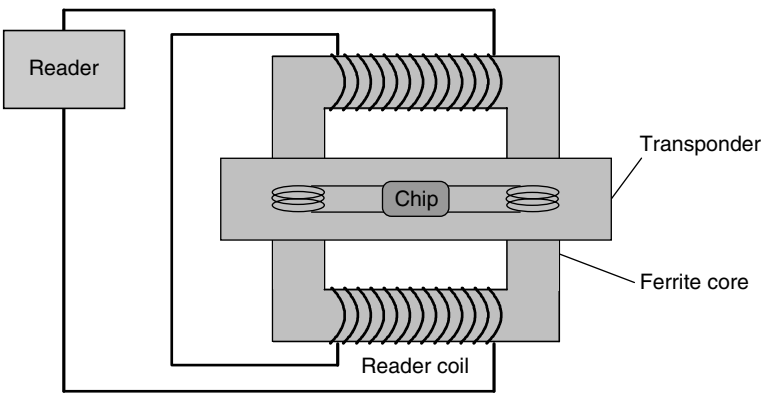


Figure 3.22 Close coupling transponder in an insertion reader with magnetic coupling coils

Because the voltage U induced in the transponder coil is proportional to the frequency f of the exciting current, the frequency selected for power transfer should be as high as possible. In practice, frequencies in the range 1–10 MHz are used. In order to keep the losses in the transformer core low, a ferrite material that is suitable for this frequency must be selected as the core material.

Because, in contrast to inductively coupled or microwave systems, the efficiency of power transfer from reader to transponder is very good, close coupling systems are excellently suited for the operation of chips with a high power consumption. This includes microprocessors, which still require some 10 mW power for operation (Sickert, 1994). For this reason, the close coupling chip card systems on the market all contain microprocessors.

The mechanical and electrical parameters of contactless close coupling chip cards are defined in their own standard, ISO 10536. For other designs the operating parameters can be freely defined.

3.2.3.2 Data transfer transponder → reader

Magnetic coupling Load modulation with subcarrier is also used for magnetically coupled data transfer from the transponder to the reader in close coupling systems.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

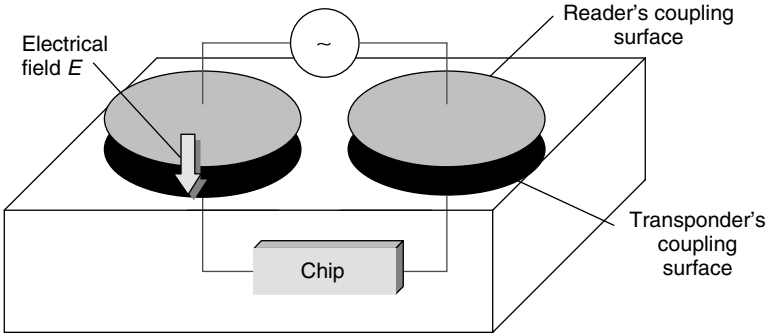


Figure 3.23 Capacitive coupling in close coupling systems occurs between two parallel metal surfaces positioned a short distance apart from each other

Subcarrier frequency and modulation is specified in ISO 10536 for close coupling chip cards.

Capacitive coupling Due to the short distance between the reader and transponder, close coupling systems may also employ *capacitive coupling* for data transmission. Plate capacitors are constructed from coupling surfaces isolated from one another, and these are arranged in the transponder and reader such that when a transponder is inserted they are exactly parallel to one another (Figure 3.23).

This procedure is also used in close coupling smart cards. The mechanical and electrical characteristics of these cards are defined in ISO 10536.

3.2.4 Electrical coupling

3.2.4.1 Power supply of passive transponders

In *electrically* (i.e. *capacitively*) coupled systems the reader generates a strong, high-frequency *electrical field*. The reader's antenna consists of a large, electrically conductive area (*electrode*), generally a metal foil or a metal plate. If a high-frequency voltage is applied to the electrode a high-frequency electric field forms between the electrode and the earth potential (ground). The voltages required for this, ranging between a few hundred volts and a few thousand volts, are generated in the reader by voltage rise in a resonant circuit made up of a coil L_1 in the reader, plus the parallel connection of an internal capacitor C_1 and the capacitance active between the electrode and the earth potential $C_{\text{R-GND}}$. The resonant frequency of the resonant circuit corresponds with the transmission frequency of the reader.

The antenna of the transponder is made up of two conductive surfaces lying in a plane (electrodes). If the transponder is placed within the electrical field of the reader, then an electric voltage arises between the two transponder electrodes, which is used to supply power to the transponder chips (Figure 3.24).

Since a capacitor is active both between the transponder and the transmission antenna ($C_{\text{R-T}}$) and between the transponder antenna and the earth potential ($C_{\text{T-GND}}$) the equivalent circuit diagram for an electrical coupling can be considered in a simplified form

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

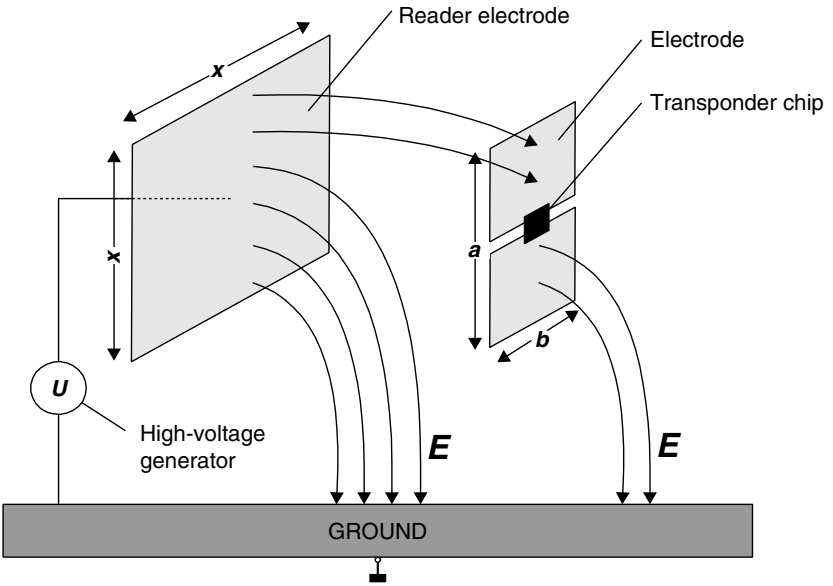


Figure 3.24 An electrically coupled system uses electrical (electrostatic) fields for the transmission of energy and data

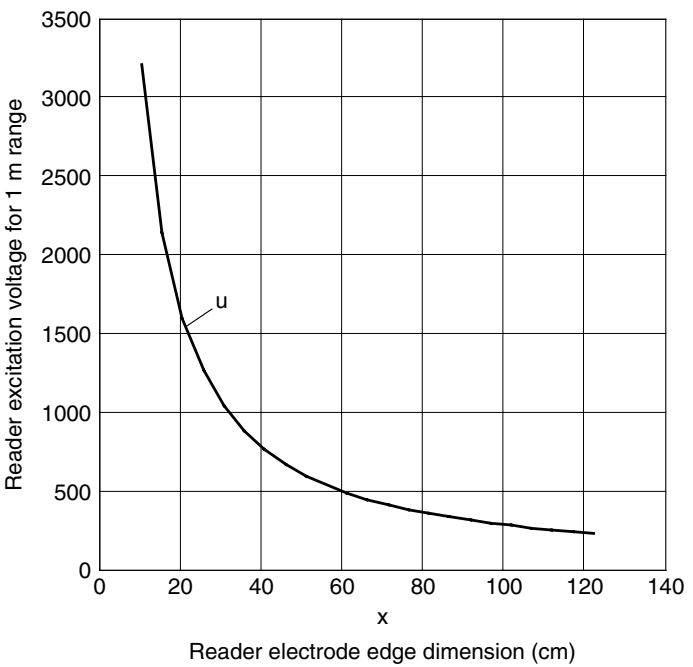


Figure 3.25 Necessary electrode voltage for the reading of a transponder with the electrode size a × b = 4.5 cm × 7 cm (format corresponds with a smart card), at a distance of 1 m ($f = 125$ kHz)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

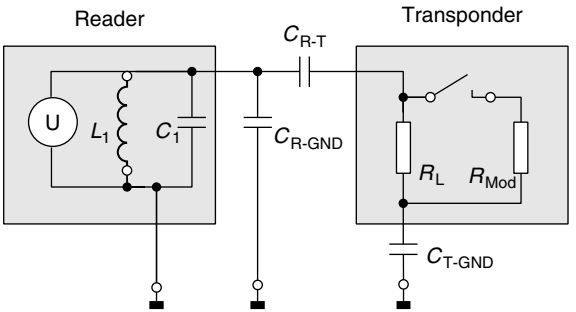


Figure 3.26 Equivalent circuit diagram of an electrically coupled RFID system

as a *voltage divider* with the elements $C_{R\text{-}T}$, R_L (input resistance of the transponder) and $C_{T\text{-}GND}$ (see Figure 3.26). Touching one of the transponder's electrodes results in the capacitance $C_{T\text{-}GND}$, and thus also the *read range*, becoming significantly greater.

The currents that flow in the electrode surfaces of the transponder are very small. Therefore, no particular requirements are imposed upon the conductivity of the electrode material. In addition to the normal metal surfaces (metal foil) the electrodes can thus also be made of conductive colours (e.g. a *silver conductive paste*) or a *graphite coating* (Motorola, Inc., 1999).

3.2.4.2 Data transfer transponder → reader

If an electrically coupled transponder is placed within the interrogation zone of a reader, the input resistance R_L of the transponder acts upon the resonant circuit of the reader via the coupling capacitance $C_{R\text{-}T}$ active between the reader and transponder electrodes, damping the resonant circuit slightly. This damping can be switched between two values by switching a modulation resistor R_{mod} in the transponder on and off. Switching the modulation resistor R_{mod} on and off thereby generates an amplitude modulation of the voltage present at L_1 and C_1 by the remote transponder. By switching the modulation resistor R_{mod} on and off in time with data, this data can be transmitted to the reader. This procedure is called *load modulation*.

3.2.5 Data transfer reader → transponder

All known digital modulation procedures are used in data transfer from the reader to the transponder in full and half duplex systems, irrespective of the operating frequency or the coupling procedure. There are three basic procedures:

- ASK: amplitude shift keying
- FSK: frequency shift keying
- PSK: phase shift keying

Because of the simplicity of demodulation, the majority of systems use ASK modulation.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

3.3 Sequential Procedures

If the transmission of data and power from the reader to the data carrier alternates with data transfer from the transponder to the reader, then we speak of a *sequential procedure* (SEQ).

The characteristics used to differentiate between SEQ and other systems have already been described in Section 3.2.

3.3.1 Inductive coupling

3.3.1.1 Power supply to the transponder

Sequential systems using inductive coupling are operated exclusively at frequencies below 135 kHz. A transformer type coupling is created between the reader's coil and the transponder's coil. The induced voltage generated in the transponder coil by the effect of an alternating field from the reader is rectified and can be used as a power supply.

In order to achieve higher efficiency of data transfer, the transponder frequency must be precisely matched to that of the reader, and the quality of the transponder coil must be carefully specified. For this reason the transponder contains an *on-chip trimming capacitor* to compensate for resonant frequency manufacturing tolerances.

However, unlike full and half duplex systems, in sequential systems the reader's transmitter does not operate on a continuous basis. The energy transferred to the transmitter during the transmission operation charges up a *charging capacitor* to provide an energy store. The transponder chip is switched over to stand-by or power saving mode during the charging operation, so that almost all of the energy received is used to charge up the charging capacitor. After a fixed charging period the reader's transmitter is switched off again.

The energy stored in the transponder is used to send a reply to the reader. The minimum capacitance of the charging capacitor can be calculated from the necessary operating voltage and the chip's power consumption:

$$C = \frac{Q}{U} = \frac{It}{[V_{\max} - V_{\min}]} \tag{3.2}$$

where $V_{\max}$, $V_{\min}$ are limit values for operating voltage that may not be exceeded, I is the power consumption of the chip during operation and t is the time required for the transmission of data from transponder to reader.

For example, the parameters $I = 5\,\mu\text{A}$, $t = 20\,\text{ms}$, $V_{\max} = 4.5\,\text{V}$ and $V_{\min} = 3.5\,\text{V}$ yield a charging capacitor of $C = 100\,\text{nF}$ (Schürmann, 1993).

3.3.1.2 A comparison between FDX/HDX and SEQ systems

Figure 3.27 illustrates the different conditions arising from full/half duplex (FDX/HDX) and sequential (SEQ) systems.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

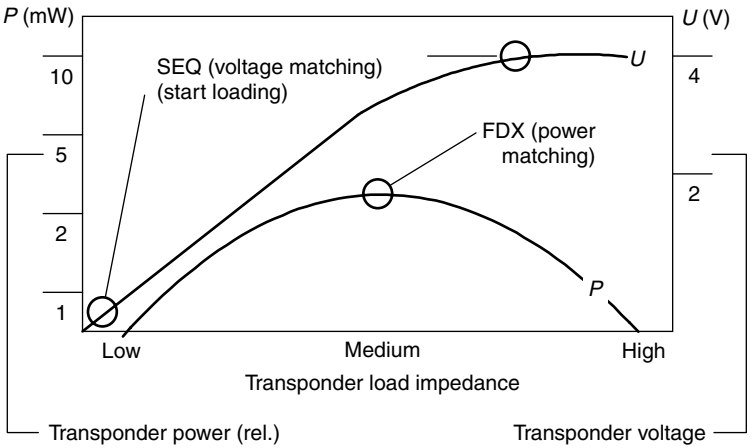


Figure 3.27 Comparison of induced transponder voltage in FDX/HDX and SEQ systems (Schürmann, 1993)

Because the power supply from the reader to the transponder in full duplex systems occurs at the same time as data transfer in both directions, the chip is permanently in operating mode. *Power matching* between the transponder antenna (current source) and the chip (current consumer) is desirable to utilise the transmitted energy optimally. However, if precise power matching is used only half of the source voltage (=open circuit voltage of the coil) is available. The only option for increasing the available operating voltage is to increase the impedance (=load resistance) of the chip. However, this is the same as decreasing the power consumption.

Therefore the design of full duplex systems is always a compromise between power matching (maximum power consumption P_{chip} at $U_{\text{chip}} = 1/2U_{\text{O}}$) and voltage matching (minimum power consumption P_{chip} at maximum voltage $U_{\text{chip}} = U_{\text{O}}$).

The situation is completely different in sequential systems: during the charging process the chip is in stand-by or power saving mode, which means that almost no power is drawn through the chip.

The charging capacitor is fully discharged at the beginning of the charging process and therefore represents a very low ohmic load for the voltage source (Figure 3.27: start loading). In this state, the maximum amount of current flows into the charging capacitor, whereas the voltage approaches zero (=*current matching*). As the charging capacitor is charged, the charging current starts to decrease according to an exponential function, and reaches zero when the capacitor is fully charged. The state of the charged capacitor corresponds with *voltage matching* at the transponder coil.

This achieves the following advantages for the chip power supply compared to a full/half duplex system:

- The full source voltage of the transponder coil is available for the operation of the chip. Thus the available operating voltage is up to twice that of a comparable full/half duplex system.
- The energy available to the chip is determined only by the capacitance of the charging capacitor and the charging period. Both values can in theory (!) be given any

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

required magnitude. In full/half duplex systems the maximum power consumption of the chip is fixed by the power matching point (i.e. by the coil geometry and field strength H).

3.3.1.3 Data transmission transponder → reader

In sequential systems (Figure 3.28) a full read cycle consists of two phases, the charging phase and the reading phase (Figure 3.29).

The end of the charging phase is detected by an *end of burst detector*, which monitors the path of voltage at the transponder coil and thus recognises the moment when the reader field is switched off. At the end of the charging phase an on-chip oscillator, which uses the resonant circuit formed by the transponder coil as a frequency determining component, is activated. A weak magnetic alternating field is generated by the transponder coil, and this can be received by the reader. This gives an improved signal-interference distance of typically 20 dB compared to full/half duplex systems, which has a positive effect upon the ranges that can be achieved using sequential systems.

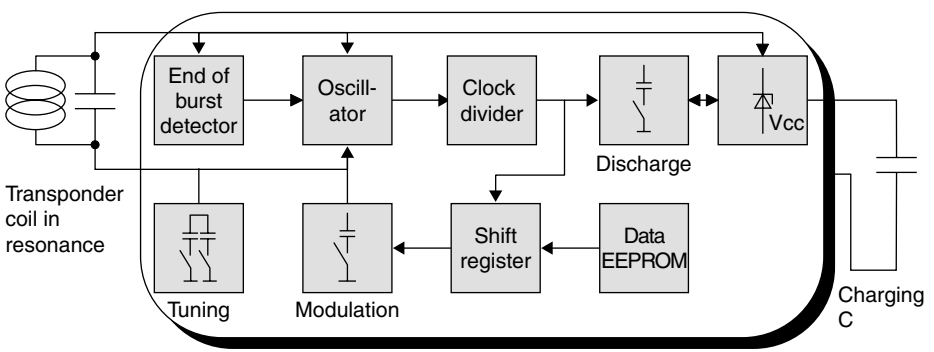


Figure 3.28 Block diagram of a sequential transponder by Texas Instruments TIRIS® Systems, using inductive coupling

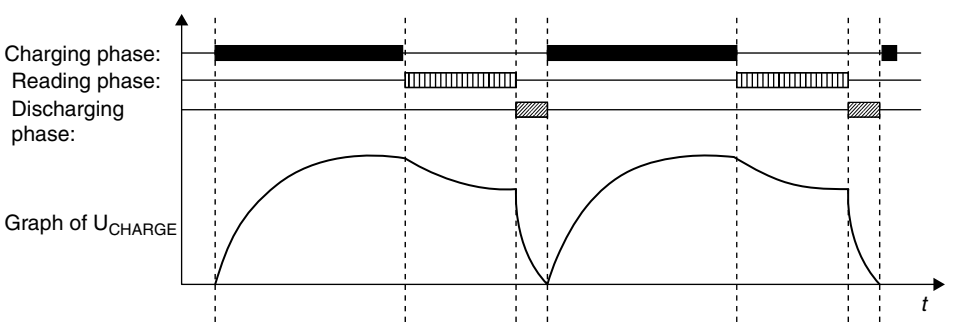


Figure 3.29 Voltage path of the charging capacitor of an inductively coupled SEQ transponder during operation

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The transmission frequency of the transponder corresponds with the resonant frequency of the transponder coil, which was adjusted to the transmission frequency of the reader when it was generated.

In order to be able to modulate the HF signal generated in the absence of a power supply, an additional modulation capacitor is connected in parallel with the resonant circuit in time with the data flow. The resulting frequency shift keying provides a *2 FSK modulation*.

After all the data has been transmitted, the discharge mode is activated to fully discharge the charging capacitor. This guarantees a safe Power-On-Reset at the start of the next charging cycle.

3.3.2 Surface acoustic wave transponder

Surface acoustic wave (SAW) devices are based upon the piezoelectric effect and on the surface-related dispersion of elastic (=acoustic) waves at low speed. If an (ionic) crystal is elastically deformed in a certain direction, surface charges occur, giving rise to electric voltages in the crystal (application: piezo lighter). Conversely, the application of a surface charge to a crystal leads to an elastic deformation in the crystal grid (application: piezo buzzer). Surface acoustic wave devices are operated at microwave frequencies, normally in the ISM range 2.45 GHz.

Electroacoustic transducers (interdigital transducers) and *reflectors* can be created using planar electrode structures on piezoelectric substrates. The normal substrate used for this application is *lithium niobate* or *lithium tantalate*. The electrode structure is created by a photolithographic procedure, similar to the procedure used in microelectronics for the manufacture of integrated circuits.

Figure 3.30 illustrates the basic layout of a surface wave transponder. A finger-shaped electrode structure — the *interdigital transducer* — is positioned at the end of a long piezoelectrical substrate, and a suitable *dipole antenna* for the operating frequency is attached to its busbar. The interdigital transducer is used to convert between electrical signals and acoustic surface waves.

An electrical impulse applied to the busbar causes a mechanical deformation to the surface of the substrate due to the piezoelectrical effect between the electrodes (fingers), which disperses in both directions in the form of a surface wave (rayleigh wave). For a normal substrate the dispersion speed lies between 3000 and 4000 m/s. Similarly, a *surface wave* entering the converter creates an electrical impulse at the busbar of the interdigital transducer due to the piezoelectric effect.

Individual electrodes are positioned along the remaining length of the surface wave transponder. The edges of the electrodes form a reflective strip and reflect a small proportion of the incoming surface waves. Reflector strips are normally made of aluminium; however some reflector strips are also in the form of etched grooves (Meinke, 1992).

A high frequency *scanning pulse* generated by a reader is supplied from the dipole antenna of the transponder into the interdigital transducer and is thus converted into an acoustic surface wave, which flows through the substrate in the longitudinal direction. The frequency of the surface wave corresponds with the carrier frequency of the sampling pulse (e.g. 2.45 GHz) (Figure 3.31). The carrier frequency of the reflected

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

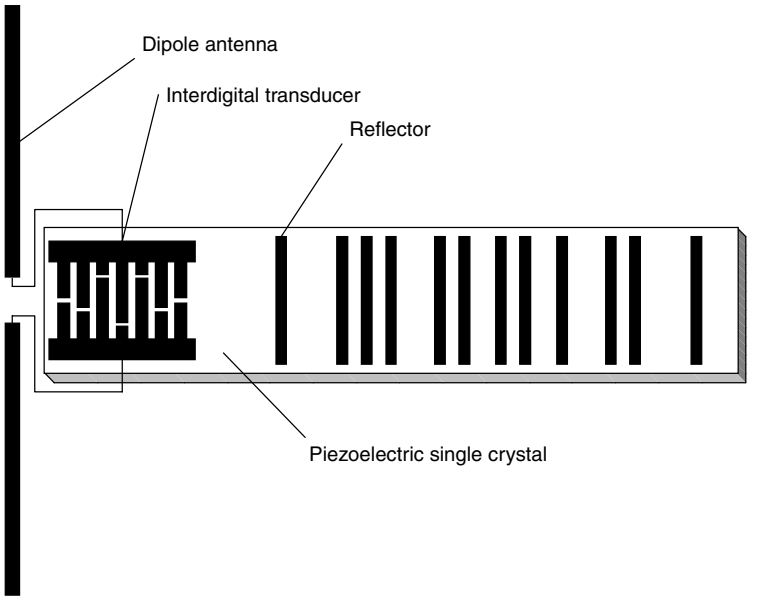


Figure 3.30 Basic layout of an SAW transponder. Interdigital transducers and reflectors are positioned on the piezoelectric crystal

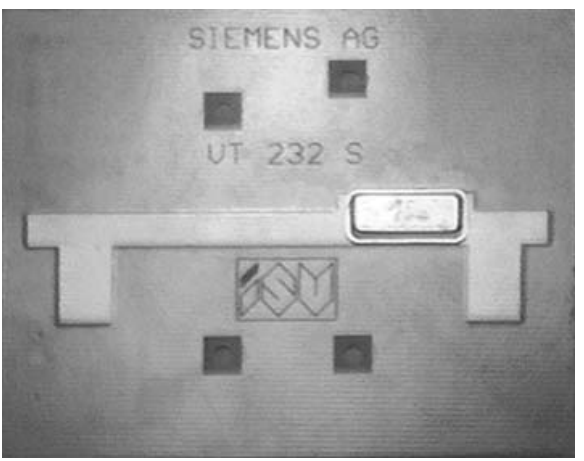


Figure 3.31 Surface acoustic wave transponder for the frequency range 2.45 GHz with antenna in the form of microstrip line. The piezocrystal itself is located in an additional metal housing to protect it against environmental influences (reproduced by permission of Siemens AG, ZT KM, Munich)

and returned pulse sequence thus corresponds with the transmission frequency of the sampling pulse.

Part of the surface wave is reflected off each of the reflective strips that are distributed across the substrate, while the remaining part of the surface wave continues to travel to the end of the substrate and is absorbed there.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The reflected parts of the wave travel back to the interdigital transducer, where they are converted into a high frequency pulse sequence and are emitted by the dipole antenna. This pulse sequence can be received by the reader. The number of pulses received corresponds with the number of reflective strips on the substrate. Likewise, the delay between the individual pulses is proportional to the spatial distance between the reflector strips on the substrate, and so the spatial layout of the reflector strips can represent a binary sequence of digits.

Due to the slow dispersion speed of the surface waves on the substrate the first response pulse is only received by the reader after a dead time of around 1.5 ms after the transmission of the scanning pulse. This gives decisive advantages for the reception of the pulse.

Reflections of the scanning pulse on the metal surfaces of the environment travel back to the antenna of the reader at the speed of light. A reflection over a distance of 100 m to the reader would arrive at the reader 0.6 ms after emission from the reader's antenna (travel time there and back, the signal is damped by >160 dB). Therefore, when the transponder signal returns after 1.5 ms all reflections from the environment of the reader have long since died away, so they cannot lead to errors in the pulse sequence (Dziggel, 1997).

The data storage capacity and data transfer speed of a surface wave transponder depend upon the size of the substrate and the realisable minimum distance between the reflector strips on the substrate. In practice, around 16–32 bits are transferred at a data transfer rate of 500 kbit/s (Siemens, n.d.).

The range of a surface wave system depends mainly upon the transmission power of the scanning pulse and can be estimated using the radar equation (Chapter 4). At the permissible transmission power in the 2.45 GHz ISM frequency range a range of 1–2 m can be expected.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

4

Physical Principles of RFID Systems

The vast majority of RFID systems operate according to the principle of *inductive coupling*. Therefore, understanding of the procedures of power and data transfer requires a thorough grounding in the physical principles of magnetic phenomena. This chapter therefore contains a particularly intensive study of the theory of magnetic fields from the point of view of RFID.

Electromagnetic fields — radio waves in the classic sense — are used in RFID systems that operate at above 30 MHz. To aid understanding of these systems we will investigate the propagation of waves in the far field and the principles of radar technology.

Electric fields play a secondary role and are only exploited for capacitive data transmission in close coupling systems. Therefore, this type of field will not be discussed further.

4.1 Magnetic Field

4.1.1 Magnetic field strength *H*

Every moving charge (electrons in wires or in a vacuum), i.e. flow of current, is associated with a *magnetic field* (Figure 4.1). The intensity of the magnetic field can be demonstrated experimentally by the forces acting on a magnetic needle (compass) or a second electric current. The magnitude of the magnetic field is described by the *magnetic field strength* H regardless of the material properties of the space.

In the general form we can say that: 'the contour integral of magnetic field strength along a closed curve is equal to the sum of the current strengths of the currents within it' (Kuchling, 1985).

$$\sum I = \oint \vec{H} \cdot \vec{ds} \tag{4.1}$$

We can use this formula to calculate the field strength H for different types of conductor. See Figure 4.2.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

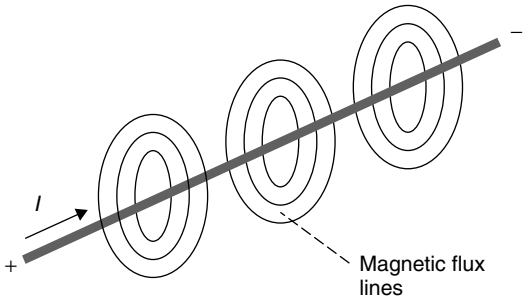


Figure 4.1 Lines of magnetic flux are generated around every current-carrying conductor

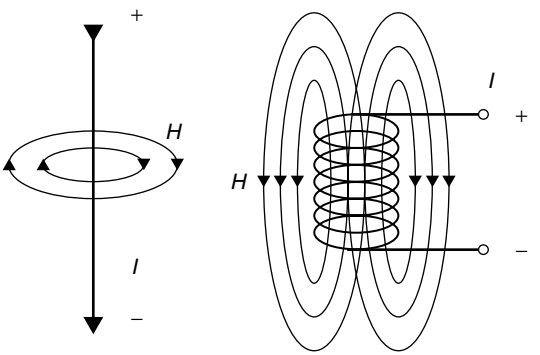


Figure 4.2 Lines of magnetic flux around a current-carrying conductor and a current-carrying cylindrical coil

Table 4.1 Constants used

Constant	Symbol	Value and unit
Electric field constant	ε_0	8.85×10^{-12} As/Vm
Magnetic field constant	μ_0	1.257×10^{-6} Vs/Am
Speed of light	c	299 792 km/s
Boltzmann constant	k	$1.380\,662 \times 10^{-23}$ J/K

In a straight conductor the field strength H along a circular *flux line* at a distance r is constant. The following is true (Kuchling, 1985):

$$H = \frac{1}{2\pi r} \tag{4.2}$$

4.1.1.1 Path of field strength H(x) in conductor loops

So-called 'short cylindrical coils' or conductor loops are used as magnetic antennas to generate the *magnetic alternating field* in the write/read devices of inductively coupled RFID systems (Figure 4.3).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 4.2 Units and abbreviations used

Variable	Symbol	Unit	Abbreviation
Magnetic field strength	H	Ampere per meter	A/m
Magnetic flux (n = number of windings)	Φ	Volt seconds	Vs
	$\Psi = n\Phi$		
Magnetic inductance	B	Volt seconds per meter squared	Vs/m^2
Inductance	L	Henry	H
Mutual inductance	M	Henry	H
Electric field strength	E	Volts per metre	V/m
Electric current	I	Ampere	A
Electric voltage	U	Volt	V
Capacitance	C	Farad	F
Frequency	f	Hertz	Hz
Angular frequency	$\omega = 2\pi f$	1/seconds	1/s
Length	l	Metre	m
Area	A	Metre squared	m^2
Speed	v	Metres per second	m/s
Impedance	Z	Ohm	Ω
Wavelength	λ	Metre	m
Power	P	Watt	W
Power density	S	Watts per metre squared	W/m^2

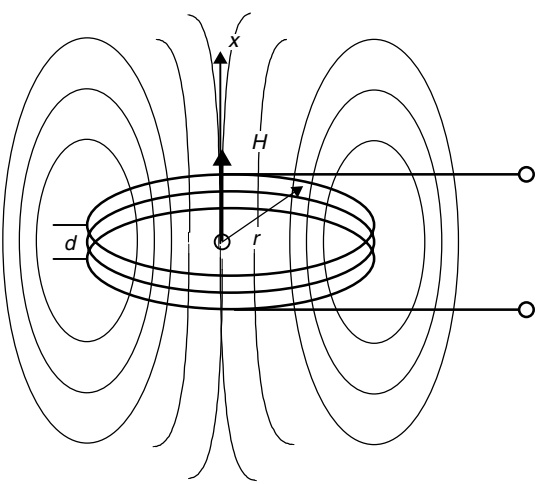


Figure 4.3 The path of the lines of magnetic flux around a short cylindrical coil, or conductor loop, similar to those employed in the transmitter antennas of inductively coupled RFID systems

If the measuring point is moved away from the centre of the coil along the coil axis (x axis), then the strength of the field H will decrease as the distance x is increased. A more in-depth investigation shows that the field strength in relation to the radius (or area) of the coil remains constant up to a certain distance and then falls rapidly (see Figure 4.4). In free space, the decay of field strength is approximately 60 dB per

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

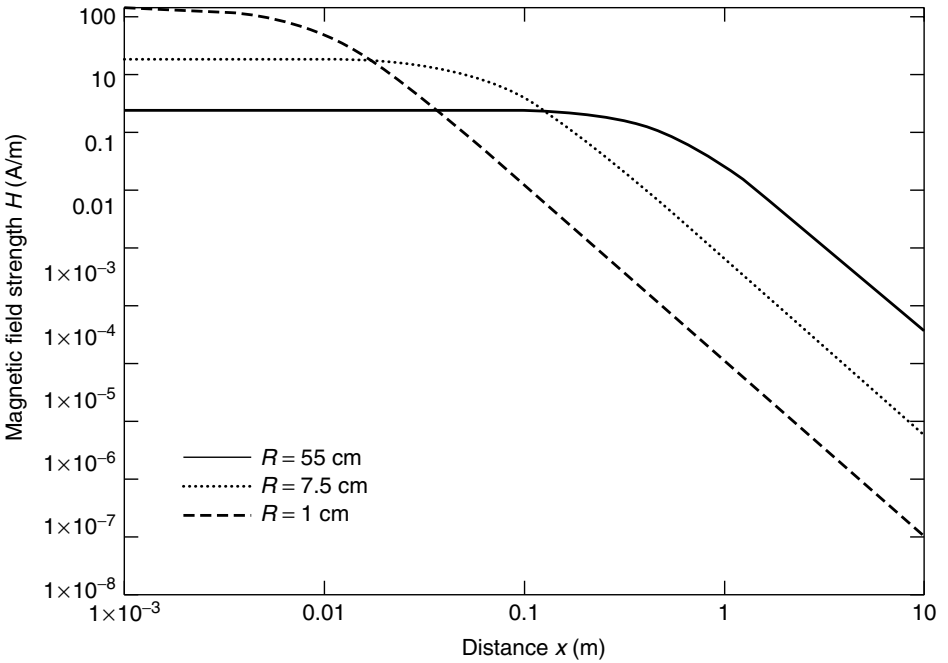


Figure 4.4 Path of magnetic field strength H in the near field of short cylinder coils, or conductor coils, as the distance in the x direction is increased

decade in the near field of the coil, and flattens out to 20 dB per decade in the far field of the electromagnetic wave that is generated (a more precise explanation of these effects can be found in Section 4.2.1).

The following equation can be used to calculate the path of field strength along the x axis of a round coil (= conductor loop) similar to those employed in the transmitter antennas of inductively coupled RFID systems (Paul, 1993):

$$H = \frac{I \cdot N \cdot R^2}{2\sqrt{(R^2 + x^2)^3}} \tag{4.3}$$

where N is the number of windings, R is the circle radius r and x is the distance from the centre of the coil in the x direction. The following boundary condition applies to this equation: $d \ll R$ and $x < \lambda/2\pi$ (the transition into the electromagnetic far field begins at a distance $>2\pi$; see Section 4.2.1).

At distance 0 or, in other words, at the centre of the antenna, the formula can be simplified to (Kuchling, 1985):

$$H = \frac{I \cdot N}{2R} \tag{4.4}$$

We can calculate the *field strength path* of a rectangular conductor loop with edge length $a \times b$ at a distance of x using the following equation. This format is often used

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

as a transmitter antenna.

$$H = \frac{N \cdot I \cdot ab}{4\pi\sqrt{\left(\frac{a}{2}\right)^2 + \left(\frac{b}{2}\right)^2 + x^2}} \cdot \left(\frac{1}{\left(\frac{a}{2}\right)^2 + x^2} + \frac{1}{\left(\frac{b}{2}\right)^2 + x^2} \right) \tag{4.5}$$

Figure 4.4 shows the calculated field strength path $H(x)$ for three different antennas at a distance 0–20 m. The number of windings and the antenna current are constant in each case; the antennas differ only in radius R. The calculation is based upon the following values: $H1$: $R = 55$ cm, $H2$: $R = 7.5$ cm, $H3$: $R = 1$ cm.

The calculation results confirm that the increase in field strength flattens out at short distances ($x < R$) from the antenna coil. Interestingly, the smallest antenna exhibits a significantly higher field strength at the centre of the antenna (distance = 0), but at greater distances ($x > R$) the largest antenna generates a significantly higher field strength. It is vital that this effect is taken into account in the design of antennas for inductively coupled RFID systems.

4.1.1.2 Optimal antenna diameter

If the radius R of the transmitter antenna is varied at a constant distance x from the transmitter antenna under the simplifying assumption of constant coil current I in the transmitter antenna, then field strength H is found to be at its highest at a certain ratio of distance x to antenna radius R. This means that for every *read range* of an RFID system there is an optimal antenna radius R. This is quickly illustrated by a glance at Figure 4.4: if the selected antenna radius is too great, the field strength is too low even at a distance $x = 0$ from the transmission antenna. If, on the other hand, the selected antenna radius is too small, then we find ourselves within the range in which the field strength falls in proportion to x^3.

Figure 4.5 shows the graph of field strength H as the coil radius R is varied. The optimal coil radius for different read ranges is always the maximum point of the graph $H(R)$. To find the mathematical relationship between the maximum field strength H and the coil radius R we must first find the inflection point of the function $H(R)$ (see equation 4.3) (Lee, 1999). To do this we find the first derivative $H'(R)$ by differentiating $H(R)$ with respect to R:

$$H'(R) = \frac{\mathrm{d}}{\mathrm{d}R} H(R) = \frac{2 \cdot I \cdot N \cdot R}{\sqrt{(R^2 + x^2)^3}} - \frac{3 \cdot I \cdot N \cdot R^3}{(R^2 + x^2) \cdot \sqrt{(R^2 + x^2)^3}} \tag{4.6}$$

The inflection point, and thus the maximum value of the function $H(R)$, is found from the following zero points of the derivative $H'(R)$:

$$R_1 = x \cdot \sqrt{2}; \qquad R_2 = -x \cdot \sqrt{2} \tag{4.7}$$

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

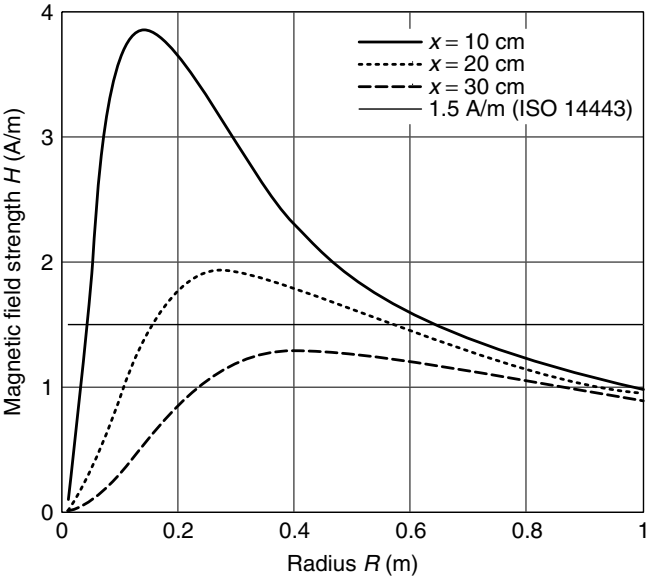


Figure 4.5 Field strength H of a transmission antenna given a constant distance x and variable radius R, where $I = 1$ A and $N = 1$

The optimal radius of a transmission antenna is thus twice the maximum desired read range. The second zero point is negative merely because the magnetic field H of a conductor loop propagates in both directions of the x axis (see also Figure 4.3).

However, an accurate assessment of a system's maximum read range requires knowledge of the *interrogation field strength* $H_{\min}$ of the transponder in question (see Section 4.1.9). If the selected antenna radius is too great, then there is the danger that the field strength H may be too low to supply the transponder with sufficient operating energy, even at a distance $x = 0$.

4.1.2 Magnetic flux and magnetic flux density

The magnetic field of a (cylindrical) coil will exert a force on a magnetic needle. If a soft iron core is inserted into a (cylindrical) coil — all other things remaining equal — then the force acting on the magnetic needle will increase. The quotient $I \times N$ (Section 4.1.1) remains constant and therefore so does field strength. However, the flux density — the total number of flux lines — which is decisive for the force generated (cf. Pauls, 1993), has increased.

The total number of lines of magnetic flux that pass through the inside of a cylindrical coil, for example, is denoted by *magnetic flux* Φ. Magnetic flux density B is a further variable related to area A (this variable is often referred to as 'magnetic inductance B in the literature') (Reichel, 1980). Magnetic flux is expressed as:

$$\Phi = B \cdot A \qquad (4.8)$$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

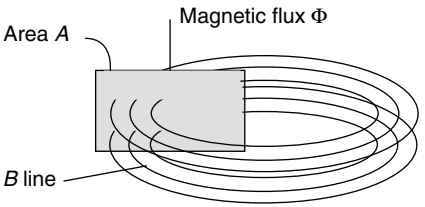


Figure 4.6 Relationship between magnetic flux Φ and flux density B

The material relationship between flux density B and field strength H (Figure 4.6) is expressed by the material equation:

$$B = \mu_0 \mu_r H = \mu H \tag{4.9}$$

The constant μ_0 is the magnetic field constant ($\mu_0 = 4\pi \times 10^{-6}$ Vs/Am) and describes the permeability (= magnetic conductivity) of a vacuum. The variable μ_r is called relative permeability and indicates how much greater than or less than μ_0 the permeability of a material is.

4.1.3 Inductance *L*

A magnetic field, and thus a magnetic flux Φ, will be generated around a conductor of any shape. This will be particularly intense if the conductor is in the form of a loop (coil). Normally, there is not one conduction loop, but N loops of the same area A, through which the same current I flows. Each of the conduction loops contributes the same proportion Φ to the total flux ψ (Paul, 1993).

$$\Psi = \sum_N \Phi_N = N \cdot \Phi = N \cdot \mu \cdot H \cdot A \tag{4.10}$$

The ratio of the interlinked flux ψ that arises in an area enclosed by current I, to the current in the conductor that encloses it (conductor loop) is denoted by *inductance* L (Figure 4.7):

$$L = \frac{\Psi}{I} = \frac{N \cdot \Phi}{I} = \frac{N \cdot \mu \cdot H \cdot A}{I} \tag{4.11}$$

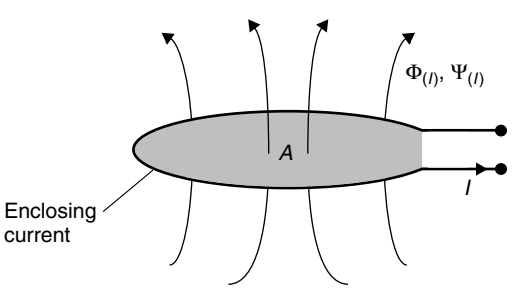


Figure 4.7 Definition of inductance L

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Inductance is one of the characteristic variables of conductor loops (coils). The inductance of a conductor loop (coil) depends totally upon the material properties (permeability) of the space that the flux flows through and the geometry of the layout.

4.1.3.1 Inductance of a conductor loop

If we assume that the diameter d of the wire used is very small compared to the diameter D of the conductor coil ($d/D < 0.0001$) a very simple approximation can be used:

$$L = N^2 \mu_0 R \cdot \ln\left(\frac{2R}{d}\right) \tag{4.12}$$

where R is the radius of the conductor loop and d is the diameter of the wire used.

4.1.4 Mutual inductance *M*

If a second conductor loop 2 (area A_2) is located in the vicinity of conductor loop 1 (area A_1), through which a current is flowing, then this will be subject to a proportion of the total magnetic flux Φ flowing through A_1. The two circuits are connected together by this partial flux or coupling flux. The magnitude of the coupling flux ψ_{21} depends upon the geometric dimensions of both conductor loops, the position of the conductor loops in relation to one another, and the magnetic properties of the medium (e.g. permeability) in the layout.

Similarly to the definition of the (self) inductance L of a conductor loop, the *mutual inductance* M_{21} of conductor loop 2 in relation to conductor loop 1 is defined as the ratio of the partial flux ψ_{21} enclosed by conductor loop 2, to the current I_1 in conductor loop 1 (Paul, 1993):

$$M_{21} = \frac{\Psi_{21}(I_1)}{I_1} = \oint_{A2} \frac{B_2(I_1)}{I_1} \cdot dA_2 \tag{4.13}$$

Similarly, there is also a mutual inductance M_{12}. Here, current I_2 flows through the conductor loop 2, thereby determining the coupling flux ψ_{12} in loop 1. The following relationship applies:

$$M = M_{12} = M_{21} \tag{4.14}$$

Mutual inductance describes the coupling of two circuits via the medium of a magnetic field (Figure 4.8). Mutual inductance is always present between two electric circuits. Its dimension and unit are the same as for inductance.

The coupling of two electric circuits via the magnetic field is the physical principle upon which inductively coupled RFID systems are based. Figure 4.9 shows a calculation of the mutual inductance between a transponder antenna and three different reader antennas, which differ only in diameter. The calculation is based upon the following values: M_1: $R = 55\,\text{cm}$, M_2: $R = 7.5\,\text{cm}$, M_3: $R = 1\,\text{cm}$, transponder: $R = 3.5\,\text{cm}$. $N = 1$ for all reader antennas.

The graph of *mutual inductance* shows a strong similarity to the graph of magnetic field strength H along the x axis. Assuming a homogeneous magnetic field, the mutual

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

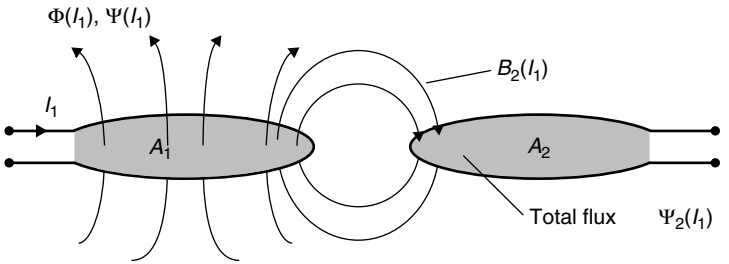


Figure 4.8 The definition of mutual inductance M_{21} by the coupling of two coils via a partial magnetic flow

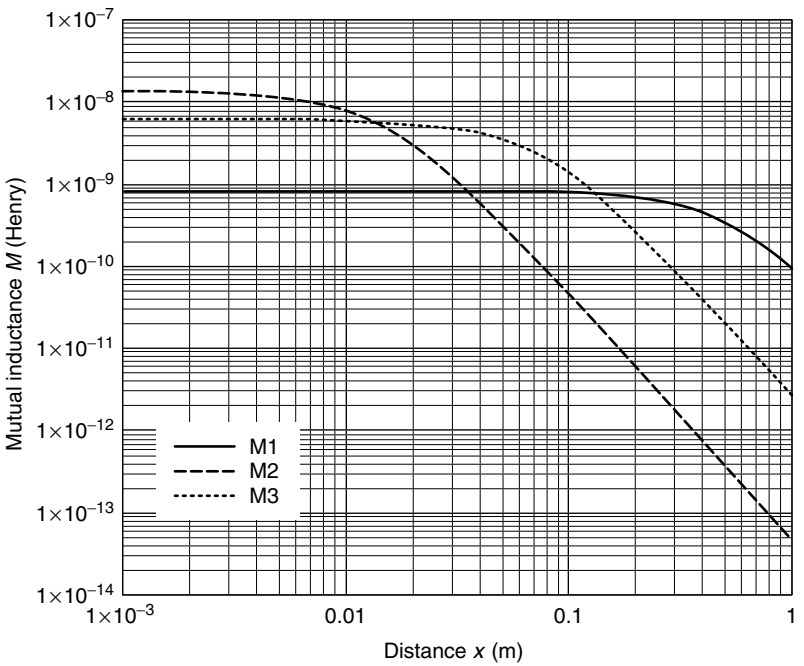


Figure 4.9 Graph of mutual inductance between reader and transponder antenna as the distance in the x direction increases

inductance M_{12} between two coils can be calculated using equation (4.13). It is found to be:

$$M_{12} = \frac{B_2(I_1) \cdot N_2 \cdot A_2}{I_1} = \frac{\mu_0 \cdot H(I_1) \cdot N_2 \cdot A_2}{I_1} \tag{4.15}$$

We first replace $H(I_1)$ with the expression in equation (4.4), and substitute $R^2\pi$ for A, thus obtaining:

$$M_{12} = \frac{\mu_0 \cdot N_1 \cdot R_1^2 \cdot N_2 \cdot R_2^2 \cdot \pi}{2\sqrt{(R_1^2 + x^2)^3}} \tag{4.16}$$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

In order to guarantee the homogeneity of the magnetic field in the area A_2 the condition $A_2 \leq A_1$ should be fulfilled. Furthermore, this equation only applies to the case where the x axes of the two coils lie on the same plane. Due to the relationship $M = M_{12} = M_{21}$ the mutual inductance can be calculated as follows for the case $A_2 \geq A_1$:

$$M_{21} = \frac{\mu_0 \cdot N_1 \cdot R_1^2 \cdot N_2 \cdot R_2^2 \cdot \pi}{2\sqrt{(R_2^2 + x^2)^3}} \tag{4.17}$$

4.1.5 Coupling coefficient *k*

Mutual inductance is a quantitative description of the flux coupling of two conductor loops. The *coupling coefficient* k is introduced so that we can make a qualitative prediction about the coupling of the conductor loops independent of their geometric dimensions. The following applies:

$$k = \frac{M}{\sqrt{L_1 \cdot L_2}} \tag{4.18}$$

The coupling coefficient always varies between the two extreme cases $0 \leq k \leq 1$.

- $k = 0$: Full decoupling due to great distance or magnetic shielding.
- $k = 1$: Total coupling. Both coils are subject to the same magnetic flux Φ. The transformer is a technical application of total coupling, whereby two or more coils are wound onto a highly permeable iron core.

An analytic calculation is only possible for very simple antenna configurations. For two parallel conductor loops centred on a single x axis the coupling coefficient according to Roz and Fuentes (n.d.) can be approximated from the following equation. However, this only applies if the radii of the conductor loops fulfil the condition $r_{\text{Transp}} \leq r_{\text{Reader}}$. The distance between the conductor loops on the x axis is denoted by x.

$$k(x) \approx \frac{r_{\text{Transp}}^2 \cdot r_{\text{Reader}}^2}{\sqrt{r_{\text{Transp}} \cdot r_{\text{Reader}}} \cdot \left(\sqrt{x^2 + r_{\text{Reader}}^2}\right)^3} \tag{4.19}$$

Due to the fixed link between the coupling coefficient and mutual inductance M, and because of the relationship $M = M_{12} = M_{21}$, the formula is also applicable to transmitter antennas that are smaller than the transponder antenna. Where $r_{\text{Transp}} \geq r_{\text{Reader}}$, we write:

$$k(x) \approx \frac{r_{\text{Transp}}^2 \cdot r_{\text{Reader}}^2}{\sqrt{r_{\text{Transp}} \cdot r_{\text{Reader}}} \cdot \left(\sqrt{x^2 + r_{\text{Transp}}^2}\right)^3} \tag{4.20}$$

The coupling coefficient $k(x) = 1$ (= 100%) is achieved where the distance between the conductor loops is zero ($x = 0$) and the antenna radii are identical ($r_{\text{Transp}} = r_{\text{Reader}}$).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

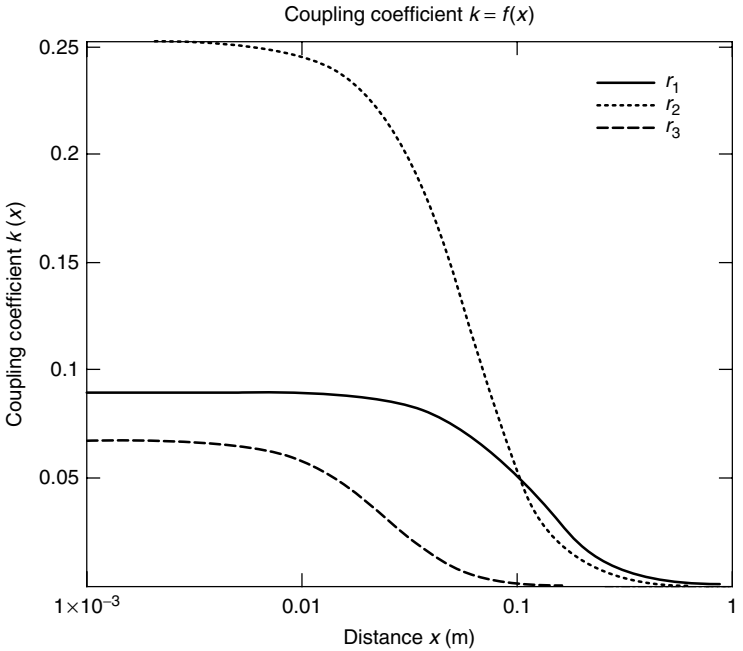


Figure 4.10 Graph of the coupling coefficient for different sized conductor loops. Transponder antenna: $r_{\text{Transp}} = 2\,\text{cm}$, reader antenna: $r_1 = 10\,\text{cm}$, $r_2 = 7.5\,\text{cm}$, $r_3 = 1\,\text{cm}$

because in this case the conductor loops are in the same place and are exposed to exactly the same magnetic flux ψ.

In practice, however, inductively coupled transponder systems operate with coupling coefficients that may be as low as 0.01 (<1%) (Figure 4.10).

4.1.6 Faraday's law

Any change to the magnetic flux Φ generates an electric field strength E_i. This characteristic of the magnetic field is described by *Faraday's law*.

The effect of the electric field generated in this manner depends upon the material properties of the surrounding area. Figure 4.11 shows some of the possible effects (Paul, 1993):

- Vacuum: in this case, the field strength E gives rise to an *electric rotational field*. Periodic changes in magnetic flux (high frequency current in an antenna coil) generate an electromagnetic field that propagates itself into the distance.
- Open conductor loop: an open circuit voltage builds up across the ends of an almost closed conductor loop, which is normally called *induced voltage*. This voltage corresponds with the line integral (path integral) of the field strength E that is generated along the path of the conductor loop in space.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

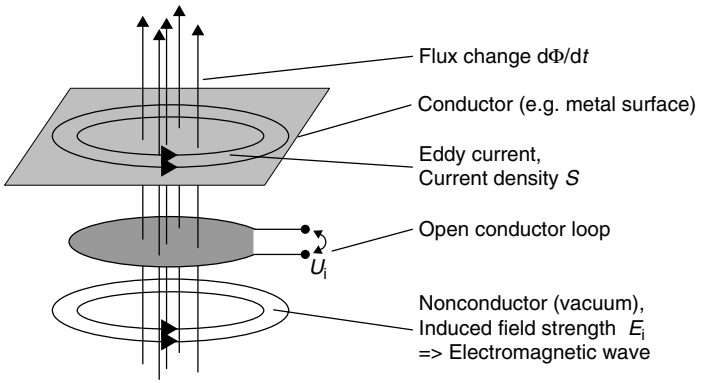


Figure 4.11 Induced electric field strength E in different materials. From top to bottom: metal surface, conductor loop and vacuum

- Metal surface: an electric field strength E is also induced in the metal surface. This causes free charge carriers to flow in the direction of the electric field strength. Currents flowing in circles are created, so-called *eddy currents*. This works against the exciting magnetic flux (Lenz's law), which may significantly damp the magnetic flux in the vicinity of *metal surfaces*. However, this effect is undesirable in inductively coupled RFID systems (installation of a transponder or reader antenna on a metal surface) and must therefore be prevented by suitable countermeasures (see Section 4.1.12.3).

In its general form Faraday's law is written as follows:

$$u_i = \oint E_i \cdot ds = -\frac{d\Psi(t)}{dt} \tag{4.21}$$

For a conductor loop configuration with N windings, we can also say that $u_i = N \cdot d\Psi/dt$. (The value of the contour integral $\int E_i \cdot ds$ can be increased N times if the closed integration path is carried out N times; Paul, 1993).

To improve our understanding of inductively coupled RFID systems we will now consider the effect of inductance on magnetically coupled conduction loops.

A time variant current $i_1(t)$ in conduction loop L_1 generates a time variant magnetic flux $d\Phi(i_1)/dt$. In accordance with the inductance law, a voltage is induced in the conductor loops L_1 and L_2 through which some degree of magnetic flux is flowing. We can differentiate between two cases:

- *Self-inductance*: the flux change generated by the current change di_n/dt induces a voltage u_n in the same conductor circuit.
- *Mutual inductance*: the flux change generated by the current change di_n/dt induces a voltage in the adjacent conductor circuit L_m. Both circuits are coupled by mutual inductance.

Figure 4.12 shows the equivalent circuit diagram for coupled conductor loops. In an inductively coupled RFID system L_1 would be the transmitter antenna of the reader.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

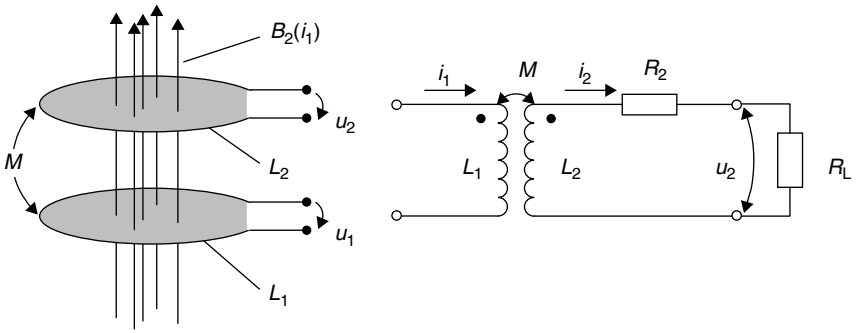


Figure 4.12 Left, magnetically coupled conductor loops; right, equivalent circuit diagram for magnetically coupled conductor loops

L_2 represents the antenna of the transponder, where R_2 is the *coil resistance* of the transponder antenna. The current consumption of the data memory is symbolised by the load resistor R_L.

A time varying flux in the conductor loop L_1 induces voltage u_{2i} in the conductor loop L_2 due to mutual inductance M. The flow of current creates an additional voltage drop across the coil resistance R_2, meaning that the voltage u_2 can be measured at the terminals. The current through the load resistor R_L is calculated from the expression u_2/R_L. The current through L_2 also generates an additional magnetic flux, which opposes the magnetic flux $\Psi_1(i_1)$. The above is summed up in the following equation:

$$u_2 = +\frac{d\Psi_2}{dt} = M\frac{di_1}{dt} - L_2\frac{di_2}{dt} - i_2R_2 \tag{4.22}$$

Because, in practice, i_1 and i_2 are sinusoidal (HF) alternating currents, we write equation (4.22) in the more appropriate complex notation (where $\omega = 2\pi f$):

$$u_2 = j\omega M \cdot i_1 - j\omega L_2 \cdot i_2 - i_2R_2 \tag{4.23}$$

If i_2 is replaced by u_2/R_L in equation (4.23), then we can solve the equation for u_2:

$$u_2 = \frac{j\omega M \cdot i_1}{1 + \dfrac{j\omega L_2 + R_2}{R_L}} \quad \begin{cases} R_L \to \infty\text{: } u_2 = j\omega M \cdot i_1 \\ R_L \to 0\text{: } u_2 \to 0 \end{cases} \tag{4.24}$$

4.1.7 Resonance

The voltage u_2 induced in the transponder coil is used to provide the power supply to the data memory (*microchip*) of a passive transponder (see Section 4.1.8.1). In order to significantly improve the efficiency of the equivalent circuit illustrated in Figure 4.12, an additional capacitor C_2 is connected in parallel with the transponder coil L_2 to form a *parallel resonant circuit* with a *resonant frequency* that corresponds with the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

operating frequency of the RFID system in question.[1] The resonant frequency of the parallel resonant circuit can be calculated using the Thomson equation:

$$f = \frac{1}{2\pi\sqrt{L_2 \cdot C_2}} \tag{4.25}$$

In practice, C_2 is made up of a parallel capacitor C_2' and a parasitic capacitance C_p from the real circuit. $C_2 = (C_2' + C_p)$. The required capacitance for the parallel capacitor C_2' is found using the Thomson equation, taking into account the parasitic capacitance C_p:

$$C_2' = \frac{1}{(2\pi f)^2 L_2} - C_p \tag{4.26}$$

Figure 4.13 shows the equivalent circuit diagram of a real transponder. R_2 is the natural resistance of the transponder coil L_2 and the current consumption of the data carrier (chip) is represented by the load resistor R_L.

If a voltage $u_{Q2} = u_i$ is induced in the coil L_2, the following voltage u_2 can be measured at the data carrier load resistor R_L in the equivalent circuit diagram shown in Figure 4.13:

$$u_2 = \frac{u_{Q2}}{1 + (j\omega L_2 + R_2) \cdot \left(\frac{1}{R_L} + j\omega C_2\right)} \tag{4.27}$$

We now replace the induced voltage $u_{Q2} = u_i$ by the factor responsible for its generation, $u_{Q2} = u_i = j\omega M \cdot i_1 = \omega \cdot k \cdot \sqrt{L_1 \cdot L_2} \cdot i_1$, thus obtaining the relationship

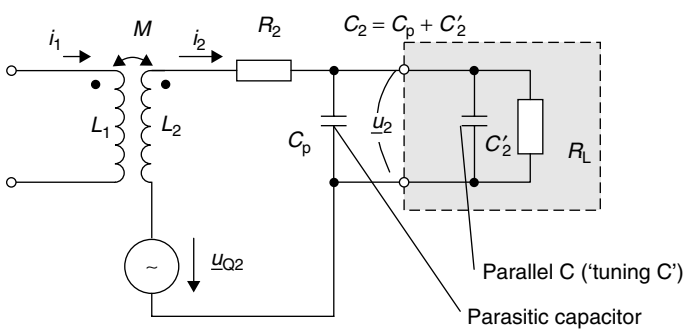


Figure 4.13 Equivalent circuit diagram for magnetically coupled conductor loops. Transponder coil L_2 and parallel capacitor C_2 form a parallel resonant circuit to improve the efficiency of voltage transfer. The transponder's data carrier is represented by the grey box

[1] However, in 13.56 MHz systems with anticollision procedures, the resonant frequency selected for the transponder is often 1–5 MHz higher to minimise the effect of the interaction between transponders on overall performance. This is because the overall resonant frequency of two transponders directly adjacent to one another is always lower than the resonant frequency of a single transponder.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

between voltage u_2 and the magnetic coupling of transmitter coil and transponder coil:

$$u_2 = \frac{j\omega M \cdot i_1}{1 + (j\omega L_2 + R_2) \cdot \left(\frac{1}{R_L} + j\omega C_2\right)} \tag{4.28}$$

and:

$$u_2 = \frac{j\omega \cdot k \cdot \sqrt{L_1 \cdot L_2} \cdot i_1}{1 + (j\omega L_2 + R_2) \cdot \left(\frac{1}{R_L} + j\omega C_2\right)} \tag{4.29}$$

or in the non-complex form (Jurisch, 1994):

$$u_2 = \frac{\omega \cdot k \cdot \sqrt{L_1 L_2} \cdot i_1}{\sqrt{\left(\frac{\omega L_2}{R_L} + \omega R_2 C_2\right)^2 + \left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)^2}} \tag{4.30}$$

where $C_2 = C_2' + C_p$.

Figure 4.14 shows the simulated graph of u_2 with and without resonance over a large frequency range for a possible transponder system. The current i_1 in the transmitter antenna (and thus also $\Phi(i_1)$), inductance L_2, mutual inductance M, R_2 and R_L are held constant over the entire frequency range.

We see that the graph of voltage u_2 for the circuit with the coil alone (circuit from Figure 4.12) is almost identical to that of the *parallel resonant circuit* (circuit from

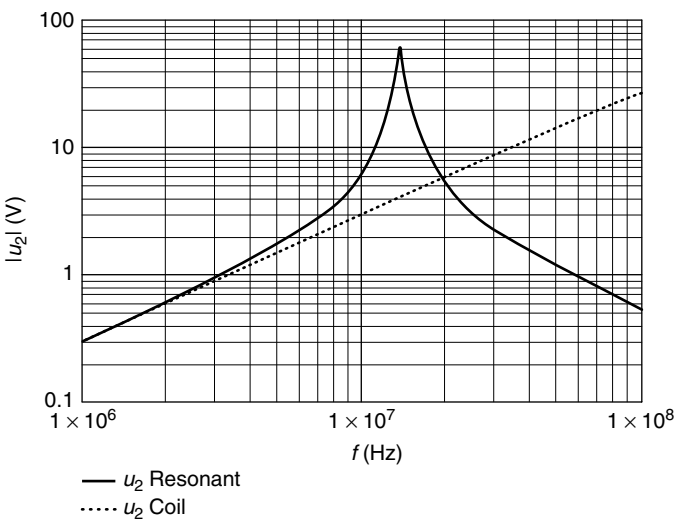


Figure 4.14 Plot of voltage at a transponder coil in the frequency range 1 to 100 MHz, given a constant magnetic field strength H or constant current i_1. A transponder coil with a parallel capacitor shows a clear voltage step-up when excited at its resonant frequency ($f_{RES} = 13.56$ MHz)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Figure 4.13) at frequencies well below the resonant frequencies of both circuits, but that when the resonant frequency is reached, voltage u_2 increases by more than a power of ten in the parallel resonant circuit compared to the voltage u_2 for the coil alone. Above the resonant frequency, however, voltage u_2 falls rapidly in the parallel resonant circuit, even falling below the value for the coil alone.

For transponders in the frequency range below 135 kHz, the transponder coil L_2 is generally connected in parallel with a chip capacitor ($C_2' = 20–220$ pF) to achieve the desired resonant frequency. At the higher frequencies of 13.56 MHz and 27.125 MHz, the required capacitance C_2 is usually so low that it is provided by the input capacitance of the data carrier together with the parasitic capacitance of the transponder coil.

Let us now investigate the influence of the circuit elements R_2, R_L and L_2 on voltage u_2. To gain a better understanding of the interactions between the individual parameters we will now introduce the Q factor (the Q factor crops up again when we investigate the connection of transmitter antennas in Section 11.4.1.3). We will refrain from deriving formulas because the electric resonant circuit is dealt with in detail in the background reading.

The *Q factor* is a measure of the voltage and current step-up in the resonant circuit at its resonant frequency. Its reciprocal 1/Q denotes the expressively named *circuit damping d*. The Q factor is very simple to calculate for the equivalent circuit in Figure 4.13. In this case ω is the angular frequency ($\omega = 2\pi f$) of the transponder resonant circuit:

$$Q = \frac{1}{R_2 \cdot \sqrt{\frac{C_2}{L_2}} + \frac{1}{R_L} \cdot \sqrt{\frac{L_2}{C_2}}} = \frac{1}{\frac{R_2}{\omega L_2} + \frac{\omega L_2}{R_L}} \tag{4.31}$$

A glance at equation (4.31) shows that when $R_2 \to \infty$ and $R_L \to 0$, the Q factor also tends towards zero. On the other hand, when the transponder coil has a very low coil resistance $R_2 \to 0$ and there is a high load resistor $R_L \gg 0$ (corresponding with very low transponder chip power consumption), very high Q factors can be achieved. The voltage u_2 is now proportional to the quality of the resonant circuit, which means that the dependency of voltage u_2 upon R_2 and R_L is clearly defined.

Voltage u_2 thus tends towards zero where $R_2 \to \infty$ and $R_L \to 0$. At a very low transponder coil resistance $R_2 \to 0$ and a high value load resistor $R_L \gg 0$, on the other hand, a very high voltage u_2 can be achieved (compare equation (4.30)).

It is interesting to note the path taken by the graph of voltage u_2 when the inductance of the transponder coil L_2 is changed, thus maintaining the resonance condition (i.e. $C_2 = 1/\omega^2 L_2$ for all values of L_2). We see that for certain values of L_2, voltage u_2 reaches a clear peak (Figure 4.15).

If we now consider the graph of the Q factor as a function of L_2 (Figure 4.16), then we observe a maximum at the same value of transponder inductance L_2. The maximum voltage $u_2 = f(L_2)$ is therefore derived from the maximum Q factor, $Q = f(L_2)$, at this point.

This indicates that for every pair of parameters (R_2, R_L), there is an inductance value L_2 at which the Q factor, and thus also the supply voltage u_2 to the data carrier, is at a maximum. This should always be taken into consideration when designing a transponder, because this effect can be exploited to optimise the energy range of

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

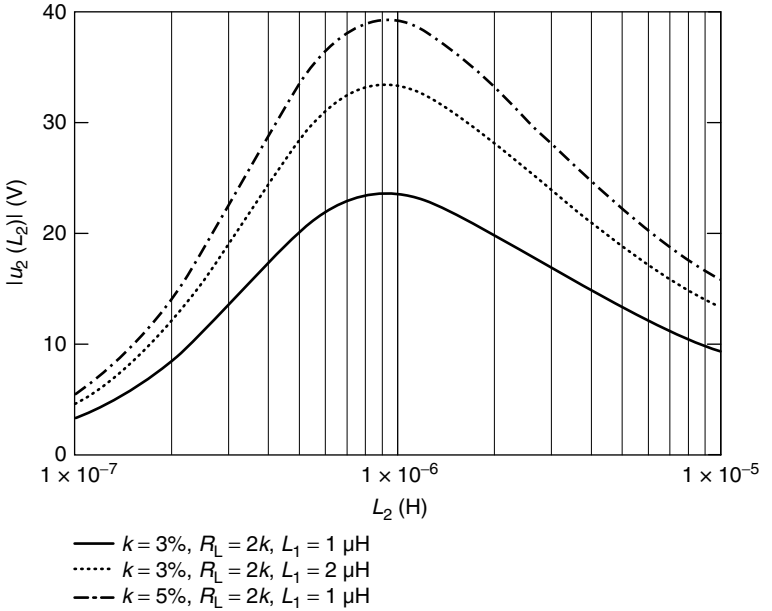


Figure 4.15 Plot of voltage u_2 for different values of transponder inductance L_2. The resonant frequency of the transponder is equal to the transmission frequency of the reader for all values of L_2 ($i_1 = 0.5\,\text{A}$, $f = 13.56\,\text{MHz}$, $R_2 = 1\,\Omega$)

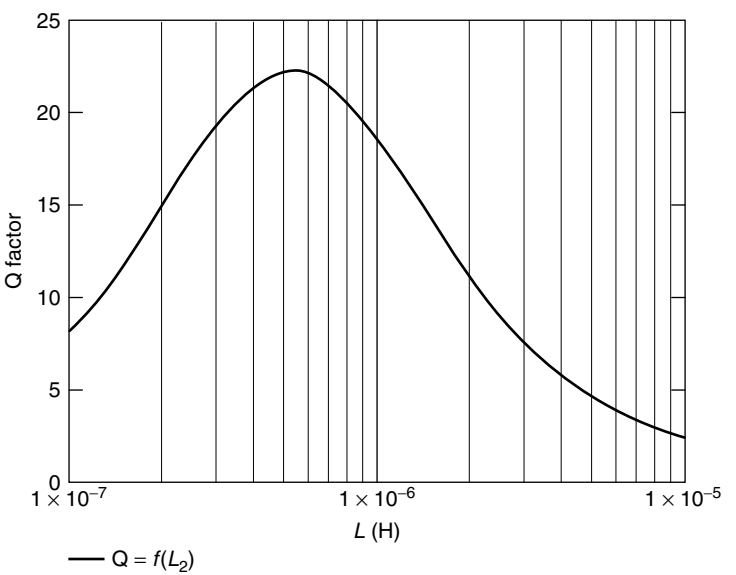


Figure 4.16 Graph of the Q factor as a function of transponder inductance L_2, where the resonant frequency of the transponder is constant ($f = 13.56\,\text{MHz}$, $R_2 = 1\,\Omega$)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

an inductively coupled RFID system. However, we must also bear in mind that the influence of component tolerances in the system also reaches a maximum in the Q_{max} range. This is particularly important in systems designed for mass production. Such systems should be designed so that reliable operation is still possible in the range $Q \ll Q_{max}$ at the maximum distance between transponder and reader.

R_L should be set at the same value as the input resistance of the data carrier after setting the 'power on' reset, i.e. before the activation of the voltage regulator, as is the case for the maximum energy range of the system.

4.1.8 Practical operation of the transponder

4.1.8.1 Power supply to the transponder

Transponders are classified as active or passive depending upon the type of power supply they use.

Active transponders incorporate their own battery to provide the power supply to the data carrier. In these transponders, the voltage u_2 is generally only required to generate a 'wake up' signal. As soon as the voltage u_2 exceeds a certain limit this signal is activated and puts the data carrier into operating mode. The transponder returns to the power saving 'sleep' or 'stand-by mode' after the completion of a transaction with the reader, or when the voltage u_2 falls below a minimum value.

In *passive transponders* the data carrier has to obtain its power supply from the voltage u_2. To achieve this, the voltage u_2 is converted into direct current using a low loss bridge rectifier and then smoothed. A simple basic circuit for this application is shown in Figure 3.18.

4.1.8.2 Voltage regulation

The induced voltage u_2 in the transponder coil very rapidly reaches high values due to resonance step-up in the resonant circuit. Considering the example in Figure 4.14, if we increase the coupling coefficient k — possibly by reducing the gap between reader and transponder — or the value of the load resistor R_L, then voltage u_2 will reach a level much greater than 100 V. However, the operation of a data carrier requires a constant *operating voltage* of 3–5 V (after rectification).

In order to regulate voltage u_2 independently of the coupling coefficient k or other parameters, and to hold it constant in practice, a voltage-dependent shunt resistor R_S is connected in parallel with the load resistor R_L. The equivalent circuit diagram for this is shown in Figure 4.17.

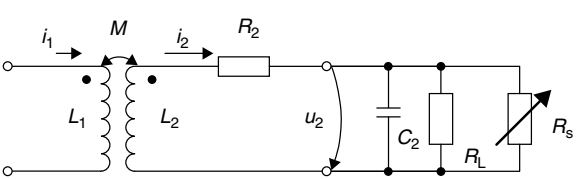


Figure 4.17 Operating principle for voltage regulation in the transponder using a shunt regulator

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

As induced voltage $u_{Q2} = u_i$ increases, the value of the shunt resistor R_S falls, thus reducing the quality of the transponder resonant circuit to such a degree that the voltage u_2 remains constant. To calculate the value of the shunt resistor for different variables, we refer back to equation (4.29) and introduce the parallel connection of R_L and R_S in place of the constant load resistor R_L. The equation can now be solved with respect to R_S. The variable voltage u_2 is replaced by the constant voltage u_{Transp} — the desired input voltage of the data carrier — giving the following equation for R_S:

$$R_S = \left| \frac{1}{\left(\frac{j\omega \cdot k \cdot \sqrt{L_1 L_2} \cdot i_1}{u_{Transp}} \right) - 1} \right| u_{2\text{-unreg}} > u_{Transp} \qquad (4.32)$$

Figure 4.18 shows the graph of voltage u_2 when such an 'ideal' shunt regulator is used. Voltage u_2 initially increases in proportion with the coupling coefficient k. When u_2 reaches its desired value, the value of the shunt resistor begins to fall in inverse proportion to k, thus maintaining an almost constant value for voltage u_2.

Figure 4.19 shows the variable value of the shunt resistor R_S as a function of the coupling coefficient. In this example the value range for the shunt resistor covers several powers of ten. This can only be achieved using a semiconductor circuit, therefore so-called *shunt* or *parallel regulators* are used in inductively coupled transponders. These terms describe an electronic regulator circuit, the internal resistance of which

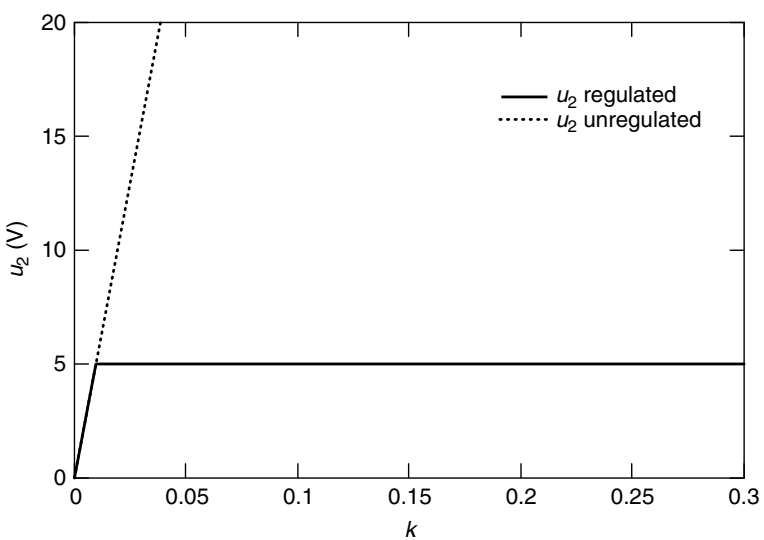


Figure 4.18 Example of the path of voltage u_2 with and without shunt regulation in the transponder, where the coupling coefficient k is varied by altering the distance between transponder and reader antenna. (The calculation is based upon the following parameters: $i_1 = 0.5\,A$, $L_1 = 1\,\mu H$, $L_2 = 3.5\,\mu H$, $R_L = 2\,k\Omega$, $C_2 = 1/\omega_2 L_2$)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

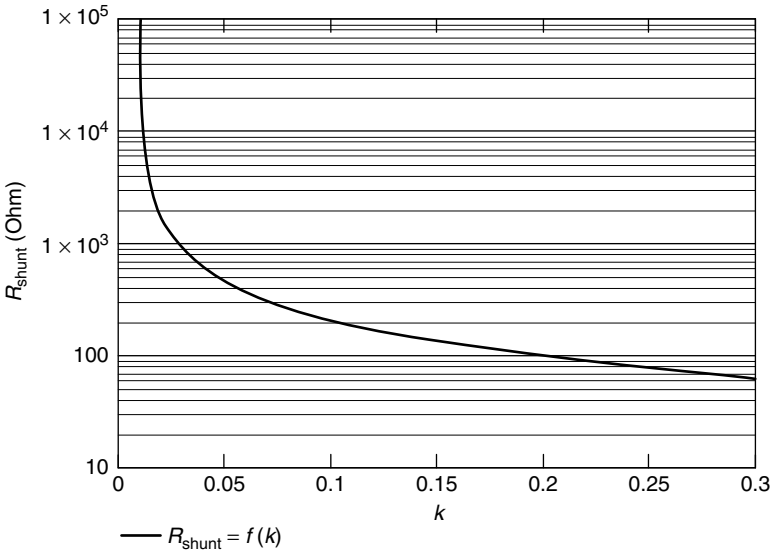


Figure 4.19 The value of the shunt resistor R_S must be adjustable over a wide range to keep voltage u_2 constant regardless of the coupling coefficient k (parameters as Figure 4.18)

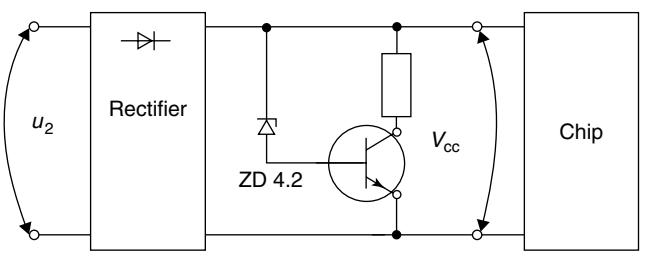


Figure 4.20 Example circuit for a simple shunt regulator

falls disproportionately sharply when a threshold voltage is exceeded. A simple shunt regulator based upon a zener diode (Nührmann, 1994) is shown in Figure 4.20.

4.1.9 Interrogation field strength H_{min}

We can now use the results obtained in Section 4.1.7 to calculate the *interrogation field strength* of a transponder. This is the minimum field strength H_{min} (at a maximum distance x between transponder and reader) at which the supply voltage u_2 is just high enough for the operation of the data carrier.

However, u_2 is not the internal operating voltage of the data carrier (3V or 5V) here; it is the *HF input voltage* at the terminal of the transponder coil L_2 on the data carrier, i.e. prior to rectification. The voltage regulator (shunt regulator) should not yet be active at this supply voltage. R_L corresponds with the input resistance of the data carrier after the 'power on reset', C_2 is made up of the input capacitance

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

C_p of the data carrier (chip) and the parasitic capacitance of the transponder layout $C_2' : C_2 = (C_2' + C_p)$.

The inductive voltage (source voltage $u_{Q2} = u_i$) of a transponder coil can be calculated using equation (4.21) for the general case. If we assume a homogeneous, sinusoidal magnetic field in air (permeability constant $= \mu_0$) we can derive the following, more appropriate, formula:

$$u_i = \mu_0 \cdot A \cdot N \cdot \omega \cdot H_{eff} \tag{4.33}$$

where H_{eff} is the effective field strength of a sinusoidal magnetic field, ω is the angular frequency of the magnetic field, N is the number of windings of the transponder coil L_2, and A is the cross-sectional area of the transponder coil.

We now replace $u_{Q2} = u_i = j\omega M \cdot i_1$ from equation (4.29) with equation (4.33) and thus obtain the following equation for the circuit in Figure 4.13:

$$u_2 = \frac{j\omega \cdot \mu_0 \cdot H_{eff} \cdot A \cdot N}{1 + (j\omega L_2 + R_2)\left(\frac{1}{R_L} + j\omega C_2\right)} \tag{4.34}$$

Multiplying out the denominator:

$$u_2 = \frac{j\omega \cdot \mu_0 \cdot H_{eff} \cdot A \cdot N}{j\omega\left(\frac{L_2}{R_L} + R_2 C_2\right) + \left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)} \tag{4.35}$$

We now solve this equation for H_{eff} and obtain the value of the complex form. This yields the following relationship for the interrogation field H_{min} in the general case:

$$H_{min} = \frac{u_2 \cdot \sqrt{\left(\frac{\omega L_2}{R_L} + \omega R_2 C_2\right)^2 + \left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)^2}}{\omega \cdot \mu_0 \cdot A \cdot N} \tag{4.36}$$

A more detailed analysis of equation (4.36) shows that the interrogation field strength is dependent upon the frequency $\omega = 2\pi f$ in addition to the antenna area A, the number of windings N (of the transponder coil), the minimum voltage u_2 and the input resistance R_2. This is not surprising, because we have determined a resonance step-up of u_2 at the resonant frequency of the transponder resonant circuit. Therefore, when the transmission frequency of the reader corresponds with the resonant frequency of the transponder, the interrogation field strength H_{min} is at its minimum value.

To optimise the interrogation sensitivity of an inductively coupled RFID system, the resonant frequency of the transponder should be matched precisely to the transmission frequency of the reader. Unfortunately, this is not always possible in practice. First, tolerances occur during the manufacture of a transponder, which lead to a deviation in the transponder resonant frequency. Second, there are also technical reasons for setting the resonant frequency of the transponder a few percentage points higher than the transmission frequency of the reader (for example in systems using anticollision procedures to keep the interaction of nearby transponders low).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Some semiconductor manufacturers incorporate additional smoothing capacitors into the transponder chip to smooth out frequency deviations in the transponder caused by manufacturing tolerances (see Figure 3.28, 'tuning C'). During manufacture the transponder is adjusted to the desired frequency by switching individual smoothing capacitors on and off (Schürmann, 1993).

In equation (4.36) the resonant frequency of the transponder is expressed as the product L_2C_2. This is not recognisable at first glance. In order to make a direct prediction regarding the frequency dependency of interrogation sensitivity, we rearrange equation (4.25) to obtain:

$$L_2C_2 = \frac{1}{(2\pi\ f_0)^2} = \frac{1}{\omega_0^2} \tag{4.37}$$

By substituting this expression into the right-hand term under the root of equation (4.36) we obtain a function in which the dependence of the interrogation field strength $H_{\min}$ on the relationship between the transmission frequency of the reader (ω) and the resonant frequency of the transponder (ω_0) is clearly expressed. This is based upon the assumption that the change in the resonant frequency of the transponder is caused by a change in the capacitance of C_2 (e.g. due to temperature dependence or manufacturing tolerances of this capacitance), whereas the inductance L_2 of the coil remains constant. To express this, the capacitor C_2 in the left-hand term under the root of equation (4.36) is replaced by $C_2 = (\omega_0^2 \cdot L_2)^{-1}$:

$$H_{\min} = \frac{u_2 \cdot \sqrt{\omega^2 \left(\frac{L_2}{R_L} + \frac{R_2}{\omega_0^2 L_2}\right)^2 + \left(\frac{\omega_0^2 - \omega^2}{\omega_0^2} + \frac{R_2}{R_L}\right)^2}}{\omega\mu_0 \cdot A \cdot N} \tag{4.38}$$

Therefore a deviation of the transponder resonant frequency from the transmission frequency of the reader will lead to a higher transponder interrogation field strength and thus to a lower *read range* (Figure 4.21).

4.1.9.1 Energy range of transponder systems

If the interrogation field strength of a transponder is known, then we can also assess the energy range associated with a certain reader. The *energy range* of a transponder is the distance from the reader antenna at which there is just enough energy to operate the transponder (defined by $u_{2\,\min}$ and R_L). However, the question of whether the energy range obtained corresponds with the maximum functional range of the system also depends upon whether the data transmitted from the transponder can be detected by the reader at the distance in question.

Given a known antenna current[2] I, radius R, and number of windings of the transmitter antenna N_1, the path of the field strength in the x direction can be calculated using equation (4.3) (see Section 4.1.1.1). If we solve the equation with respect to x

[2] If the antenna current of the transmitter antenna is not known it can be calculated from the measured field strength $H(x)$ at a distance x, where the antenna radius R and the number of windings N_1 are known (see Section 4.1.1.1).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

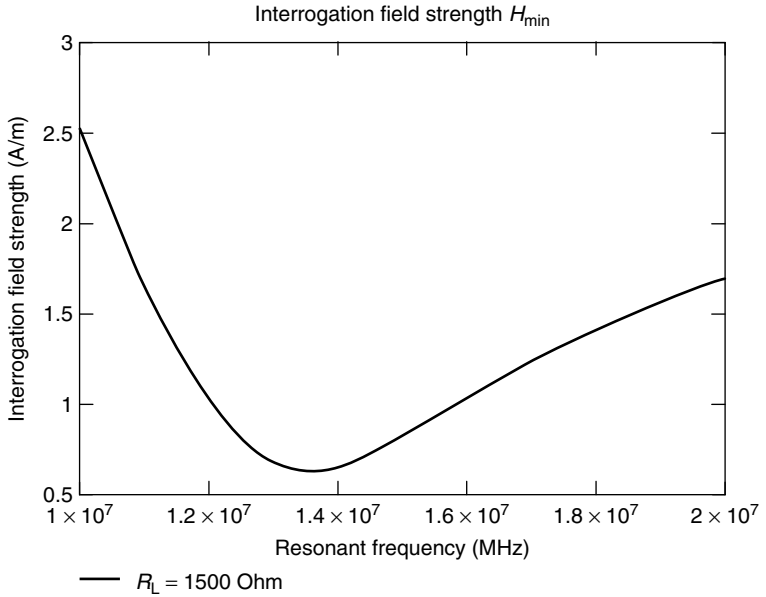


Figure 4.21 Interrogation sensitivity of a contactless smart card where the transponder resonant frequency is detuned in the range 10–20 MHz ($N = 4$, $A = 0.05 \times 0.08\,\text{m}^2$, $u_2 = 5\text{V}$, $L_2 = 3.5\,\mu\text{H}$, $R_2 = 5\,\Omega$, $R_L = 1.5\,\text{k}\Omega$). If the transponder resonant frequency deviates from the transmission frequency (13.56 MHz) of the reader an increasingly high field strength is required to address the transponder. In practical operation this results in a reduction of the read range

we obtain the following relationship between the energy range and interrogation field H_{min} of a transponder for a given reader:

$$x = \sqrt{\sqrt[3]{\left(\frac{I \cdot N_1 \cdot R^2}{2 \cdot H_{min}}\right)^2} - R^2} \tag{4.39}$$

As an example (see Figure 4.22), let us now consider the energy range of a transponder as a function of the power consumption of the data carrier ($R_L = u_2 / i_2$). The reader in this example generates a field strength of 0.115 A/m at a distance of 80 cm from the transmitter antenna (radius R of transmitter antenna: 40 cm). This is a typical value for RFID systems in accordance with ISO 15693.

As the current consumption of the transponder (lower R_L) increases, the interrogation sensitivity of the transponder also increases and the energy range falls.

The maximum energy range of the transponder is determined by the distance between transponder and reader antenna at which the minimum power supply $u_{2\,min}$ required for the operation of the data carrier exists even with an unloaded transponder resonant circuit (i.e. $i_2 \to 0$, $R_L \to \infty$). Where distance $x = 0$ the maximum current i_2 represents a limit, above which the supply voltage for the data carrier falls below $u_{2\,min}$, which means that the reliable operation of the data carrier can no longer be guaranteed in this operating state.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

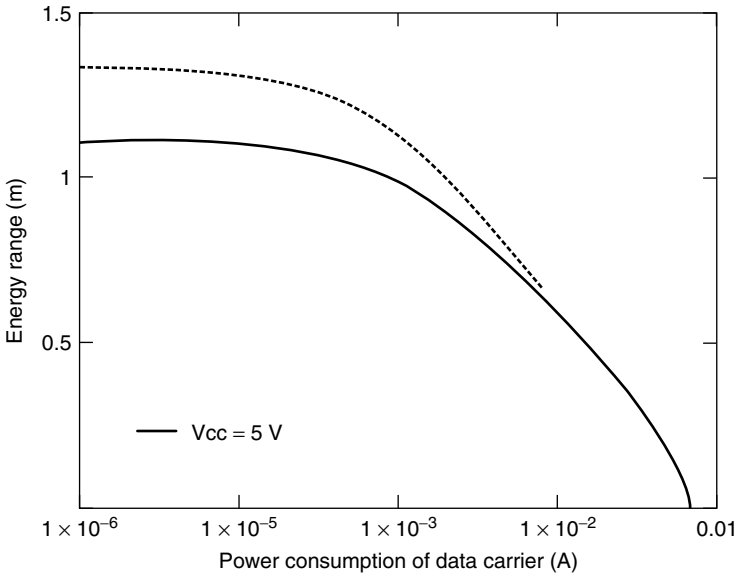


Figure 4.22 The energy range of a transponder also depends upon the power consumption of the data carrier (R_L). The transmitter antenna of the simulated system generates a field strength of 0.115 A/m at a distance of 80 cm, a value typical for RFID systems in accordance with ISO 15693 (transmitter: $I = 1\text{A}$, $N_1 = 1$, $R = 0.4\,\text{m}$. Transponder: $A = 0.048 \times 0.076\,\text{m}^2$ (smart card), $N = 4$, $L_2 = 3.6\,\mu\text{H}$, $u_{2\,\min} = 5\text{V}/3\text{V}$)

4.1.9.2 Interrogation zone of readers

In the calculations above the implicit assumption was made of a homogeneous magnetic field H parallel to the coil axis x. A glance at Figure 4.23 shows that this only applies for an arrangement of reader coil and transponder coil with a common central axis x. If the transponder is tilted away from this central axis or displaced in the direction of the y or z axis this condition is no longer fulfilled.

If a coil is magnetised by a magnetic field H, which is tilted by the angle ϑ in relation to the central axis of the coil, then in very general terms the following applies:

$$u_{0\vartheta} = u_0 \cdot \cos(\vartheta) \tag{4.40}$$

where u_0 is the voltage that is induced when the coil is perpendicular to the magnetic field. At an angle $\vartheta = 90^\circ$, in which case the field lines run in the plane of the coil radius R, no voltage is induced in the coil.

As a result of the bending of the *magnetic field lines* in the entire area around the reader coil, here too there are different angles ϑ of the magnetic field H in relation to the transponder coil. This leads to a characteristic *interrogation zone* (Figure 4.24, grey area) around the reader antenna. Areas with an angle $\vartheta = 0^\circ$ in relation to the transponder antenna — for example along the coil axis x, but also to the side of the antenna windings (returning field lines) — give rise to an optimal read range. Areas in which the magnetic field lines run parallel to the plane of the transponder coil radius

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

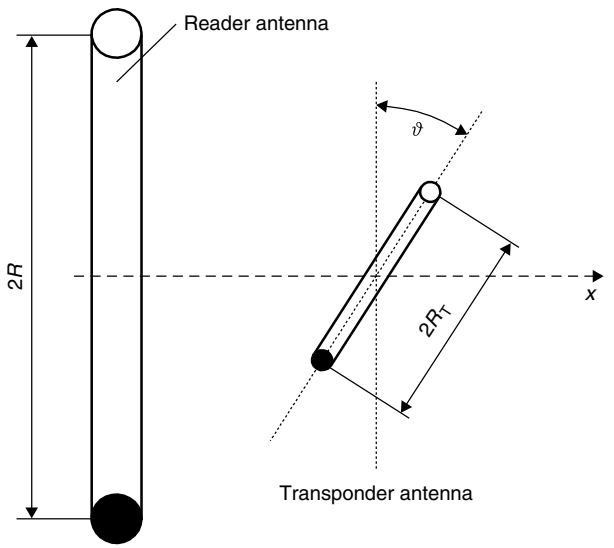


Figure 4.23 Cross-section through reader and transponder antennas. The transponder antenna is tilted at an angle ϑ in relation to the reader antenna

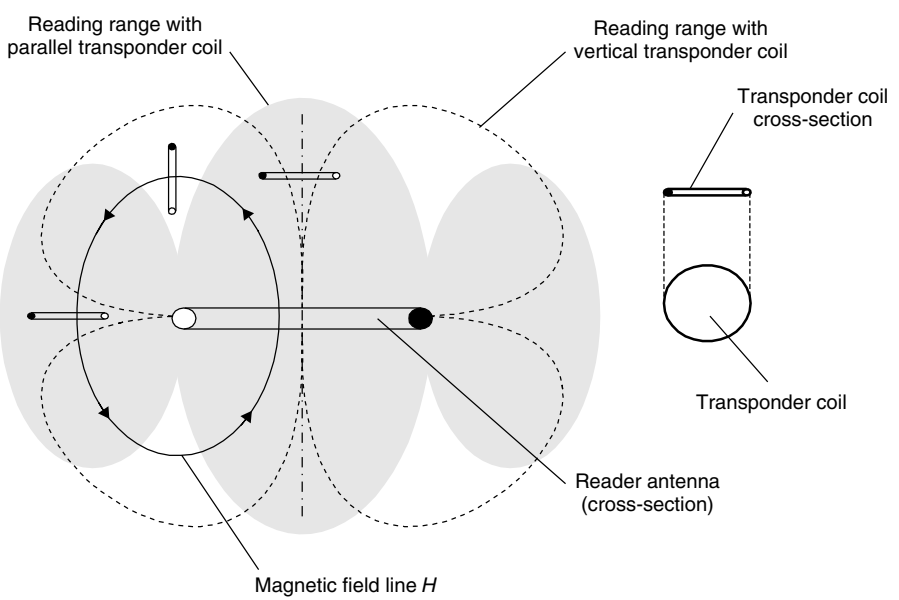


Figure 4.24 Interrogation zone of a reader at different alignments of the transponder coil

R — for example, exactly above and below the coil windings — exhibit a significantly reduced read range. If the transponder itself is tilted through 90° a completely different picture of the interrogation zone emerges (Figure 4.24, dotted line). Field lines that run parallel to the R-plane of the reader coil now penetrate the transponder coil at an angle $\vartheta = 0°$ and thus lead to an optimal *range* in this area.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

4.1.10 Total transponder – reader system

Up to this point we have considered the characteristics of inductively coupled systems primarily from the point of view of the transponder. In order to analyse in more detail the interaction between transponder and *reader* in the system, we need to take a slightly different view and first examine the electrical properties of the reader so that we can then go on to study the system as a whole.

Figure 4.25 shows the equivalent circuit diagram for a reader (the practical realisation of this circuit configuration can be found in Section 11.4). The *conductor loop* necessary to generate the magnetic alternating field is represented by the coil L_1. The series resistor R_1 corresponds with the ohmic losses of the wire resistance in the conductor loop L_1. In order to obtain maximum current in the conductor coil L_1 at the reader *operating frequency* f_{TX}, a *series resonant circuit* with the resonant frequency $f_{RES} = f_{TX}$ is created by the serial connection of the capacitor C_1. The resonant frequency of the series resonant circuit can be calculated very easily using the Thomson equation (4.25). The operating state of the reader can be described by:

$$f_{TX} = f_{RES} = \frac{1}{2\pi\sqrt{L_1 \cdot C_1}} \tag{4.41}$$

Because of the series configuration, the total impedance Z_1 of the series resonant circuit is the sum of individual impedances, i.e.:

$$Z_1 = R_1 + j\omega\, L_1 + \frac{1}{j\omega C_1} \tag{4.42}$$

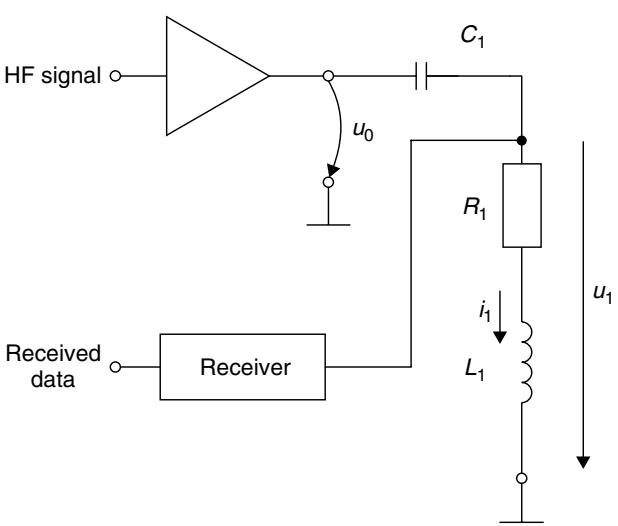


Figure 4.25 Equivalent circuit diagram of a reader with antenna L_1. The transmitter output branch of the reader generates the HF voltage u_0. The receiver of the reader is directly connected to the antenna coil L_1

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

At the resonant frequency f_{RES}, however, the impedances of L_1 and C_1 cancel each other out. In this case the total impedance Z_1 is determined by R_1 only and thus reaches a minimum.

$$j\omega L_1 + \frac{1}{j\omega C_1} = 0 \Big|_{\omega = 2\pi \cdot f_{RES}} \Rightarrow Z_1(f_{RES}) = R_1 \tag{4.43}$$

The *antenna current* i_1 reaches a maximum at the resonant frequency and is calculated (based upon the assumption of an ideal voltage source where $R_i = 0$) from the source voltage u_0 of the transmitter high level stage, and the ohmic coil resistance R_1.

$$i_1(f_{res}) = \frac{u_0}{Z_1(f_{RES})} = \frac{u_0}{R_1} \tag{4.44}$$

The two voltages, u_1 at the conductor loop L_1, and u_{C1} at the capacitor C_1, are in antiphase and cancel each other out at the resonant frequency because current i_1 is the same. However, the individual values may be very high. Despite the low source voltage u_0, which is usually just a few volts, figures of a few hundred volts can easily be reached at L_1 and C_1. Designs for *conductor loop antennas* for high currents must therefore incorporate sufficient voltage resistance in the components used, in particular the capacitors, because otherwise these would easily be destroyed by arcing. Figure 4.26 shows an example of voltage step-up at resonance.

Despite the fact that the voltage may reach very high levels, it is completely safe to touch the voltage-carrying components of the reader antenna. Because of the additional

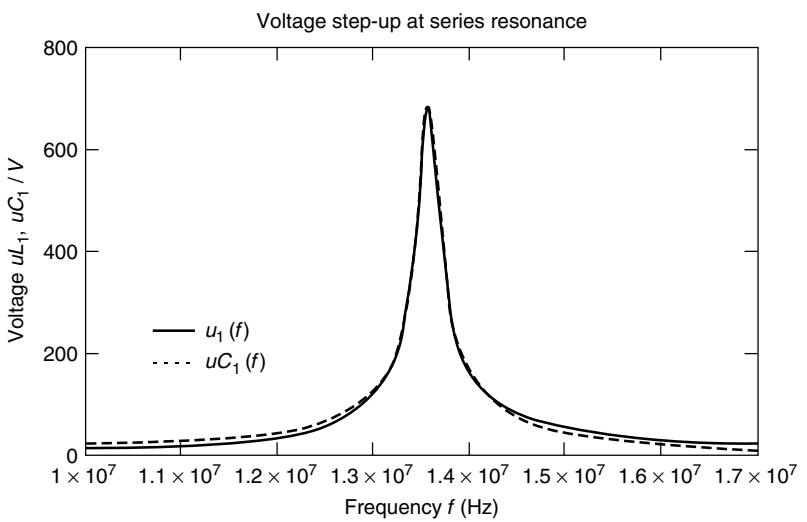


Figure 4.26 Voltage step-up at the coil and capacitor in a series resonant circuit in the frequency range 10–17 MHz ($f_{RES} = 13.56$ MHz, $u_0 = 10$V(!), $R_1 = 2.5\,\Omega$, $L_1 = 2\,\mu$H, $C_1 = 68.8$ pF). The voltage at the conductor coil and series capacitor reaches a maximum of above 700 V at the resonant frequency. Because the resonant frequency of the reader antenna of an inductively coupled system always corresponds with the transmission frequency of the reader, components should be sufficiently voltage resistant

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

capacitance of the hand, the series resonant circuit is rapidly detuned, thus reducing the resonance step-up of voltage.

4.1.10.1 Transformed transponder impedance Z'_T

If a transponder enters the magnetic alternating field of the conductor coil L_1 a change can be detected in the current i_1. The current i_2 induced in the transponder coil thus acts upon current i_1 responsible for its generation via the magnetic *mutual inductance* M.[3]

In order to simplify the mathematical description of the mutual inductance on the current i_1, let us now introduce an imaginary impedance, the *complex transformed transponder impedance* Z'_T. The electrical behaviour of the reader's series resonant circuit in the presence of mutual inductance is as if the imaginary impedance Z'_T were actually present as a discrete component: Z'_T takes on a finite value $|Z'_T| > 0$. If the mutual inductance is removed, e.g. by withdrawing the transponder from the field of the conductor loop, then $|Z'_T| = 0$. We will now derive the calculation of this transformed impedance step by step.

The source voltage u_0 of the reader can be divided into the individual voltages u_{C1}, u_{R1}, u_{L1} and u_{ZT} in the series resonant circuit, as illustrated in Figure 4.27. Figure 4.28 shows the vector diagram for the individual voltages in this circuit at resonance.

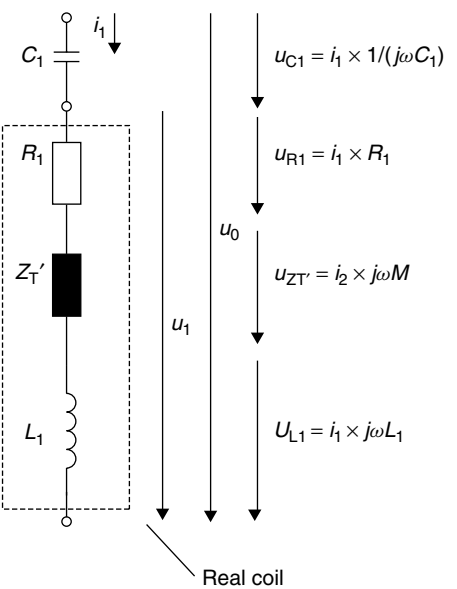


Figure 4.27 Equivalent circuit diagram of the series resonant circuit — the change in current i_1 in the conductor loop of the transmitter due to the influence of a magnetically coupled transponder is represented by the impedance Z'_T

[3] This is in accordance with Lenz's law, which states that 'the induced voltage always attempts to set up a current in the conductor circuit, the direction of which opposes that of the voltage that induced it' (Paul, 1993).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

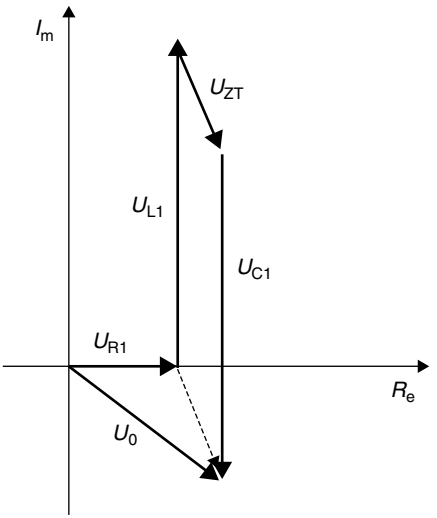


Figure 4.28 The vector diagram for voltages in the series resonance circuit of the reader antenna at resonant frequency. The figures for individual voltages u_{L1} and u_{C1} can reach much higher levels than the total voltage u_0

Due to the constant current i_1 in the series circuit, the source voltage u_0 can be represented as the sum of the products of the individual impedances and the current i_1. The transformed impedance Z'_T is expressed by the product $j\omega M \cdot i_2$:

$$u_0 = \frac{1}{j\omega C_1} \cdot i_1 + j\omega L_1 \cdot i_1 + R_1 \cdot i_1 - j\omega M \cdot i_2 \tag{4.45}$$

Since the series resonant circuit is operated at its *resonant frequency*, the individual impedances $(j\omega C_1)^{-1}$ and $j\omega L_1$ cancel each other out. The voltage u_0 is therefore only divided between the resistance R_1 and the transformed transponder impedance Z'_T, as we can see from the vector diagram (Figure 4.28). Equation 4.45 can therefore be further simplified to:

$$u_0 = R_1 \cdot i_1 - j\omega M \cdot i_2 \tag{4.46}$$

We now require an expression for the current i_2 in the coil of the transponder, so that we can calculate the value of the transformed transponder impedance. Figure 4.29 gives an overview of the currents and voltages in the transponder in the form of an equivalent circuit diagram:

The source voltage u_{Q2} is induced in the transponder coil L_2 by mutual inductance M. The current i_2 in the transponder is calculated from the quotient of the voltage u_2 divided by the sum of the individual impedances $j\omega L_2$, R_2 and Z_2 (here Z_2 represents the total input impedance of the data carrier and the parallel capacitor C_2). In the next step, we replace the voltage u_{Q2} by the voltage responsible for its generation $u_{Q2} = j\omega M \cdot i_1$, yielding the following expression for u_0:

$$u_0 = R_1 \cdot i_1 - j\omega M \cdot \frac{u_{Q2}}{R_2 + j\omega L_2 + Z_2} = R_1 \cdot i_1 - j\omega M \cdot \frac{j\omega M \cdot i_1}{R_2 + j\omega L_2 + Z_2} \tag{4.47}$$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

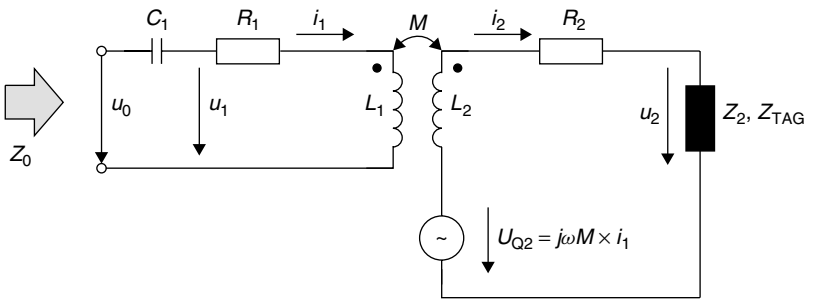


Figure 4.29 Simple equivalent circuit diagram of a transponder in the vicinity of a reader. The impedance Z_2 of the transponder is made up of the load resistor R_L (data carrier) and the capacitor C_2

As it is generally impractical to work with the mutual inductance M, in a final step we replace M with $M = k\sqrt{L_1 \cdot L_2}$ because the values k, L_1 and L_2 of a transponder are generally known. We write:

$$u_0 = R_1 \cdot i_1 + \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{R_2 + j\omega L_2 + Z_2} \cdot i_1 \tag{4.48}$$

Dividing both sides of equation (4.48) by i_1 yields the total impedance $Z_0 = u_0/i_1$ of the series resonant circuit in the reader as the sum of R_1 and the transformed transponder impedance Z'_T. Thus Z'_T is found to be:

$$Z'_T = \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{R_2 + j\omega L_2 + Z_2} \tag{4.49}$$

Impedance Z_2 represents the parallel connection of C_2 and R_L in the transponder. We replace Z_2 with the full expression containing C_2 and R_L and thus finally obtain an expression for Z'_T that incorporates all components of the transponder and is thus applicable in practice:

$$Z'_T = \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{R_2 + j\omega L_2 + \dfrac{R_L}{1 + j\omega R_L C_2}} \tag{4.50}$$

4.1.10.2 Influencing variables of Z'_T

Let us now investigate the influence of individual parameters on the *transformed transponder impedance* Z'_T. In addition to line diagrams, locus curves are also suitable for this investigation: there is precisely one vector in the complex Z plane for every parameter value x in the function $Z'_T = f(x)$ and thus exactly one point on the curve.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 4.3 Parameters for line diagrams and locus curves, if not stated otherwise

$L_1 = 1\,\mu\text{H}$	$L_2 = 3.5\,\mu\text{H}$
$C_1 = 1/(\omega_{\text{TX}})^2 \cdot L_1$ (resonance)	$R_2 = 5\,\Omega$
$C_2 = 1/(\omega_{\text{RX}})^2 \cdot L_2$ (resonance)	$R_{\text{L}} = 5\,\text{k}\Omega$
$f_{\text{RES}} = f_{\text{TX}} = 13.56\,\text{MHz}$	$k = 15\%$

All line diagrams and locus curves from Section 4.1.10 are — unless stated otherwise — calculated using the constant parameter values listed in Table 4.3.

Transmission frequency f_{TX} Let us first change the *transmission frequency* f_{TX} of the reader, while the transponder resonant frequency f_{RES} is kept constant. Although this case does not occur in practice it is very useful as a theoretical experiment to help us to understand the principles behind the transformed transponder impedance Z'_{T}.

Figure 4.30 shows the locus curve $Z'_{\text{T}} = f(f_{\text{TX}})$ for this case. The impedance vector Z'_{T} traces a circle in the clockwise direction in the complex Z plane as transmission frequency f_{TX} increases.

In the frequency range below the transponder resonant frequency ($f_{\text{TX}} < f_{\text{RES}}$) the impedance vector Z'_{T} is initially found in quadrant I of the complex Z plane. The transformed transponder impedance Z'_{T} is inductive in this frequency range.

If the transmission frequency precisely corresponds with the transponder resonant frequency ($f_{\text{TX}} = f_{\text{RES}}$) then the reactive impedances for L_2 and C_2 in the transponder

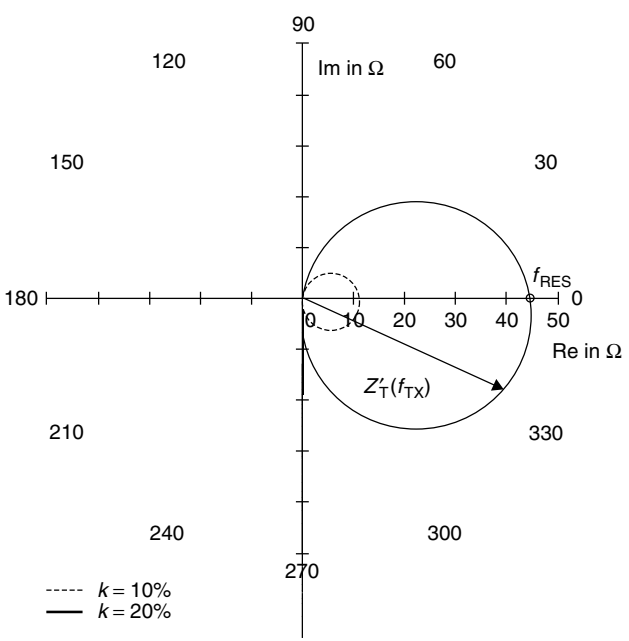


Figure 4.30 The impedance locus curve of the complex transformed transponder impedance Z'_{T} as a function of transmission frequency ($f_{\text{TX}} = 1\text{–}30\,\text{MHz}$) of the reader corresponds with the impedance locus curve of a parallel resonant circuit

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

cancel each other out. Z'_T acts as an ohmic (real) resistor — the locus curve thus intersects the real x axis of the complex Z plane at this point.

In the frequency range above the transponder resonant frequency ($f_{TX} > f_{RES}$), the locus curve finally passes through quadrant IV of the complex Z plane — Z'_T has a capacitive effect in this range.

The impedance locus curve of the complex transformed transponder impedance Z'_T corresponds with the impedance locus curve of a damped parallel resonant circuit with a parallel resonant frequency equal to the resonant frequency of the transponder. Figure 4.31 shows an equivalent circuit diagram for this. The complex current i_2 in the coil L_2 of the transponder resonant circuit is transformed by the magnetic mutual inductance M in the antenna coil L_1 of the reader and acts there as a parallel resonant circuit with the (frequency dependent) impedance Z'_T. The value of the real resistor R' in the equivalent circuit diagram corresponds with the point of intersection of the locus curve Z'_T with the real axis in the Z plane.

Coupling coefficient k Given constant geometry of the transponder and reader antenna, the *coupling coefficient* is defined by the distance and angle of the two coils in relation to each other (see Section 4.1.5). The influence of metals in the vicinity of the transmitter or transponder coil on the coupling coefficient should not be disregarded (e.g. shielding effect caused by eddy current losses). In practice, therefore, the coupling coefficient is the parameter that varies the most. Figure 4.32 shows the locus curve of the complex transformed transponder impedance for the range $0 \leq k \leq 1$. We differentiate between three ranges:

- $k = 0$: If the transponder coil L_2 is removed from the field of the reader antenna L_1 entirely, then no mutual inductance occurs. For this limit case, the transformed transponder impedance is no longer effective, that is $Z'_T(k = 0) = 0$.
- $0 < k < 1$: If the transponder coil L_2 is slowly moved towards the reader antenna L_1, then the coupling coefficient, and thus also the mutual inductance M between the two coils, increases continuously. The value of complex transformed transponder impedance increases proportionately, whereby $Z'_T \sim k_2$. When f_{TX} exactly

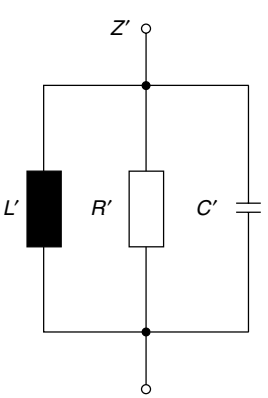


Figure 4.31 The equivalent circuit diagram of complex transformed transponder impedance Z'_T is a damped parallel resonant circuit

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

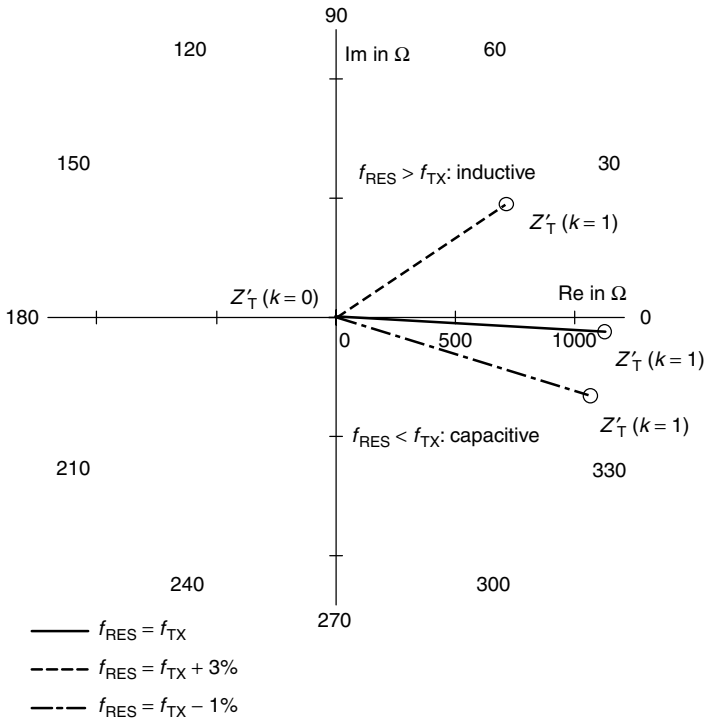


Figure 4.32 The locus curve of $Z'_T(k = 0–1)$ in the complex impedance plane as a function of the coupling coefficient k is a straight line

corresponds with f_{RES}, $Z'_T(k)$ remains real for all values of k.[4] Given a detuning of the transponder resonant frequency ($f_{RES} \neq f_{TX}$), on the other hand, Z'_T also has an inductive or capacitive component.

- $k = 1$: This case only occurs if both coils are identical in format, so that the windings of the two coils L_1 and L_2 lie directly on top of each other at distance $d = 0$. $Z'_T(k)$ reaches a maximum in this case. In general the following applies: $|Z'_T(k)_{max}| = |Z'_T(K_{max})|$.

Transponder capacitance C_2 We will now change the value of transponder capacitance C_2, while keeping all other parameters constant. This naturally detunes the resonant frequency f_{RES} of the transponder in relation to the transmission frequency f_{TX} of the reader. In practice, different factors may be responsible for a change in C_2:

- manufacturing tolerances, leading to a static deviation from the target value;
- a dependence of the data carrier's input capacitance on the input voltage u_2 due to effects in the semiconductor: $C_2 = f(u_2)$;

[4] The low angular deviation in the locus curve in Figure 4.32 where $f_{RES} = f_{TX}$ is therefore due to the fact that the resonant frequency calculated according to equation (4.34) is only valid without limitations for the undamped parallel resonant circuit. Given damping by R_L and R_2, on the other hand, there is a slight detuning of the resonant frequency. However, this effect can be largely disregarded in practice and thus will not be considered further here.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

- intentional variation of the capacitance of C_2 for the purpose of data transmission (we will deal with so-called 'capacitive load modulation' in more detail in Section 4.1.10.3).
- detuning due to environmental influences such as metal, temperature, moisture, and 'hand capacitance' when the smart card is touched.

Figure 4.33 shows the locus curve for $Z'_T(C_2)$ in the complex impedance plane. As expected, the locus curve obtained is the circle in the complex Z plane that is typical of a parallel resonant circuit. Let us now consider the extreme values for C_2:

- $C_2 = 1/\omega_{TX}^2 L_2$: The resonant frequency of the transponder in this case precisely corresponds with the transmission frequency of the reader (see equation (4.25)). The current i_2 in the transponder coil reaches a maximum at this value due to resonance step-up and is real. Because $Z'_T \sim j\omega M \cdot i_2$ the value for impedance Z'_T also reaches a maximum — the locus curve intersects the real axis in the complex Z plane. The following applies: $|Z'_T(C_2)|_{max} = |Z'_T(C_2 = 1/\omega_{TX})^2 \cdot L_2)|$.
- $C_2 \neq 1/\omega^2 L_2$: If the capacitance C_2 is less than or greater than $C_2 = 1/\omega_{TX}^2 L_2$ then the resonant frequency of the transponder will be detuned and will vary significantly from the transmission frequency of the reader. The polarity of the current i_2 in the resonant circuit of the transponder varies when the resonant frequency is exceeded,

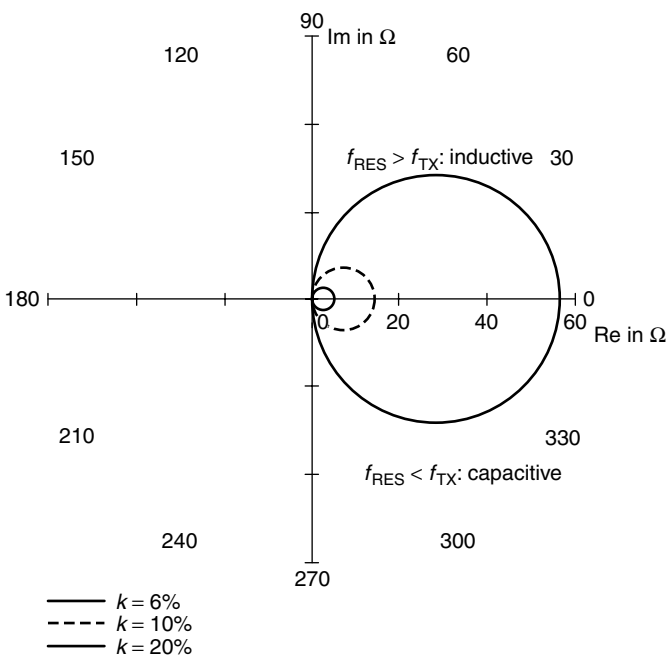


Figure 4.33 The locus curve of Z'_T ($C_2 = 10-110\,pF$) in the complex impedance plane as a function of the capacitance C_2 in the transponder is a circle in the complex Z plane. The diameter of the circle is proportional to k_2

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

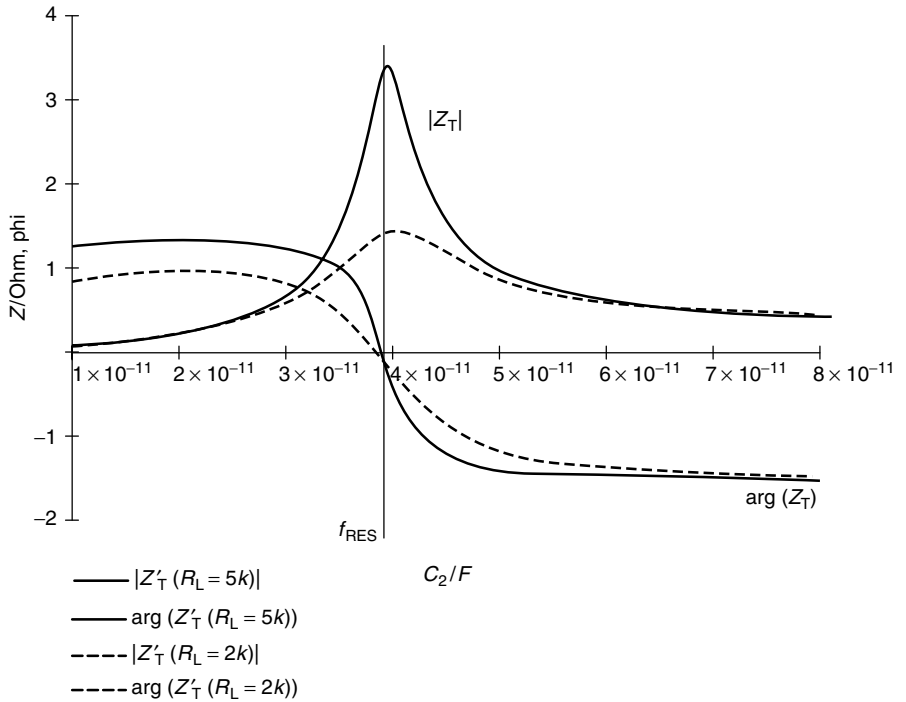


Figure 4.34 Value and phase of the transformed transponder impedance Z'_{T} as a function of C_2. The maximum value of Z'_{T} is reached when the transponder resonant frequency matches the transmission frequency of the reader. The polarity of the phase angle of Z'_{T} varies

as we can see from Figure 4.34. Similarly, the locus curve of Z'_{T} describes the familiar circular path in the complex Z plane. For both extreme values:

$$Z'_{\mathrm{T}}(C_2 \to 0) = \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{j\omega L_2 + R_2 + R_{\mathrm{L}}} \tag{4.51}$$

(no resonance step-up)

$$Z'_{\mathrm{T}}(C_2 \to \infty) = \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{j\omega L_2 + R_2} \tag{4.52}$$

('short-circuited' transponder coil).

Load resistance R_{L} The *load resistance* R_{L} is an expression for the *power consumption* of the data carrier (microchip) in the transponder. Unfortunately, the load resistance is generally not constant, but falls as the coupling coefficient increases due to the influence of the shunt regulator (voltage regulator). The power consumption of the data carrier also varies, for example during the read or write operation. Furthermore, the value of the load resistance is often intentionally altered in order to transmit data to the reader (see Section 4.1.10.3).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

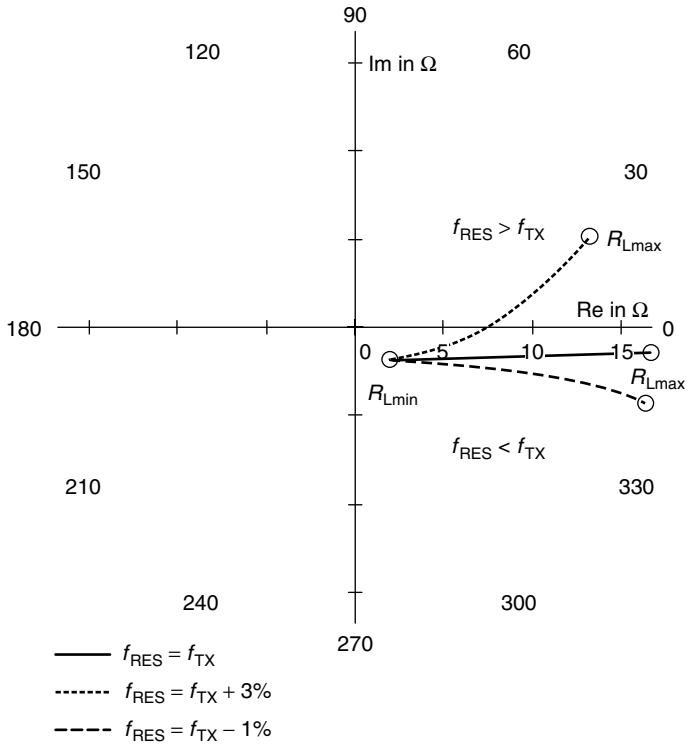


Figure 4.35 Locus curve of Z'_T ($R_L = 0.3–3\,k\Omega$) in the impedance plane as a function of the load resistance R_L in the transponder at different transponder resonant frequencies

Figure 4.35 shows the corresponding locus curve for $Z'_T = f(R_L)$. This shows that the transformed transponder impedance is proportional to R_L. Increasing load resistance R_L, which corresponds with a lower(!) current in the data carrier, thus also leads to a greater value for the transformed transponder impedance Z'_T. This can be explained by the influence of the load resistance R_L on the Q factor: a high-ohmic load resistance R_L leads to a high Q factor in the resonant circuit and thus to a greater current step-up in the transponder resonant circuit. Due to the proportionality $Z'_T \sim j\omega M \cdot i_2$ — and not to i_{RL} — we obtain a correspondingly high value for the transformed transponder impedance.

If the transponder resonant frequency is detuned we obtain a curved locus curve for the transformed transponder impedance Z'_T. This can also be traced back to the influence of the Q factor, because the phase angle of a detuned parallel resonant circuit also increases as the Q factor increases ($R_L \uparrow$), as we can see from a glance at Figure 4.34.

Let us reconsider the two extreme values of R_L:

$$Z'_T(R_L \to 0) = \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{R_2 + j\omega L_2} \tag{4.52}$$

HANSHOW-EX. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

('short-circuited' transponder coil)

$$Z'_{\mathrm{T}}(R_L \to \infty) = \frac{\omega^2 k^2 \cdot L_1 \cdot L_2}{j\omega L_2 + R_2 + \dfrac{1}{j\omega C_2}} \tag{4.54}$$

(unloaded transponder resonant circuit).

Transponder inductance L_2 Let us now investigate the influence of inductance L_2 on the transformed transponder impedance, whereby the resonant frequency of the transponder is again held constant, so that $C_2 = 1/\omega_{\mathrm{TX}}^2 L_2$.

Transformed transponder impedance reaches a clear peak at a given inductance value, as a glance at the line diagram shows (Figure 4.36). This behaviour is reminiscent of the graph of voltage $u_2 = f(L_2)$ (see also Figure 4.15). Here too the peak transformed transponder impedance occurs where the Q factor, and thus the current i_2 in the transponder, is at a maximum ($Z'_{\mathrm{T}} \sim j\omega M \cdot i_2$). Please refer to Section 4.1.7 for an explanation of the mathematical relationship between load resistance and the Q factor.

4.1.10.3 Load modulation

Apart from a few other methods (see Chapter 3), so-called *load modulation* is the most common procedure for *data transmission* from transponder to reader by some margin.

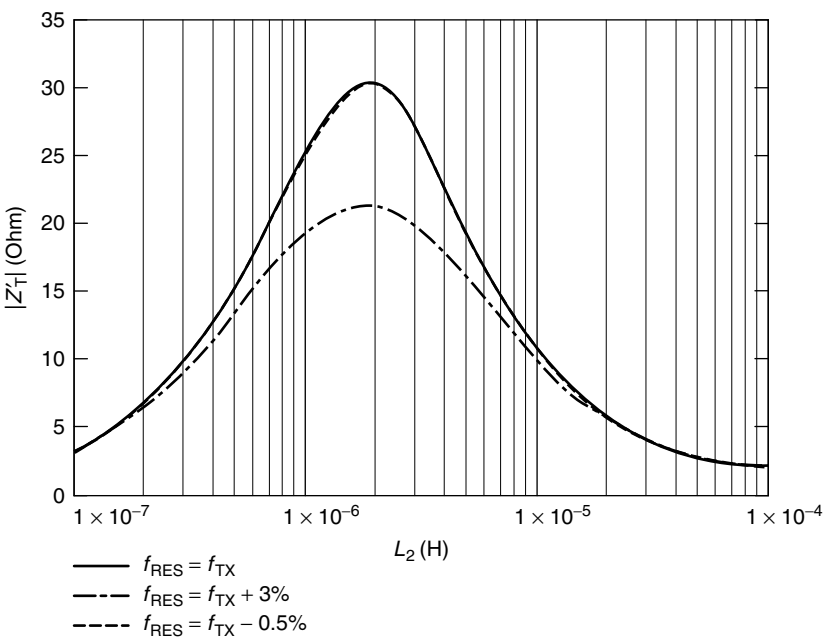


Figure 4.36 The value of Z'_{T} as a function of the transponder inductance L_2 at a constant resonant frequency f_{RES} of the transponder. The maximum value of Z'_{T} coincides with the maximum value of the Q factor in the transponder

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

By varying the circuit parameters of the *transponder resonant circuit* in time with the data stream, the magnitude and phase of the *transformed transponder impedance* can be influenced (modulation) such that the data from the transponder can be reconstructed by an appropriate evaluation procedure in the reader (demodulation).

However, of all the circuit parameters in the transponder resonant circuit, only two can be altered by the data carrier: the load resistance R_L and the parallel capacitance C_2. Therefore RFID literature distinguishes between ohmic (or real) and capacitive load modulation.

Ohmic load modulation In this type of load modulation a parallel resistor R_{mod} is switched on and off within the data carrier of the transponder in time with the data stream (or in time with a modulated subcarrier) (Figure 4.37). We already know from the previous section that the parallel connection of R_{mod} ($\rightarrow$ reduced total resistance) will reduce the Q factor and thus also the transformed transponder impedance Z'_T. This is also evident from the locus curve for the ohmic load modulator: Z'_T is switched between the values Z'_T (R_L) and Z'_T ($R_L \| R_{mod}$) by the load modulator in the transponder (Figure 4.38). The phase of Z'_T remains almost constant during this process (assuming $f_{TX} = f_{RES}$).

In order to be able to reconstruct (i.e. demodulate) the transmitted data, the falling voltage u_{ZT} at Z'_T must be sent to the receiver (RX) of the reader. Unfortunately, Z'_T is not accessible in the reader as a discrete component because the voltage u_{ZT} is induced in the real antenna coil L_1. However, the voltages u_{L1} and u_{R1} also occur at the antenna coil L_1, and they can only be measured at the terminals of the antenna coil as the total voltage u_{RX}. This total voltage is available to the receiver branch of the reader (see also Figure 4.25).

The vector diagram in Figure 4.39 shows the magnitude and phase of the voltage components u_{ZT}, u_{L1} and u_{R1} which make up the total voltage u_{RX}. The magnitude and phase of u_{RX} is varied by the modulation of the voltage component u_{ZT} by the load modulator in the transponder. *Load modulation* in the transponder thus brings about the *amplitude modulation* of the reader antenna voltage u_{RX}. The transmitted data is therefore not available in the baseband at L_1; instead it is found in the modulation products (= modulation sidebands) of the (load) modulated voltage u_1 (see Chapter 6).

Capacitive load modulation In *capacitive load modulation* it is an additional capacitor C_{mod}, rather than a modulation resistance, that is switched on and off in time with the data stream (or in time with a modulated subcarrier) (Figure 4.40). This causes the resonant frequency of the transponder to be switched between two frequencies.

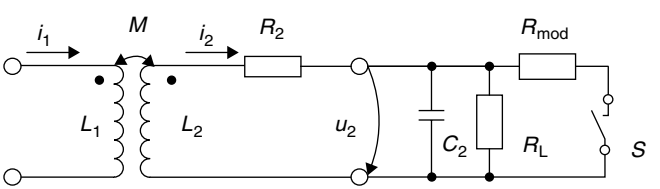


Figure 4.37 Equivalent circuit diagram for a transponder with load modulator. Switch S is closed in time with the data stream — or a modulated subcarrier signal — for the transmission of data

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

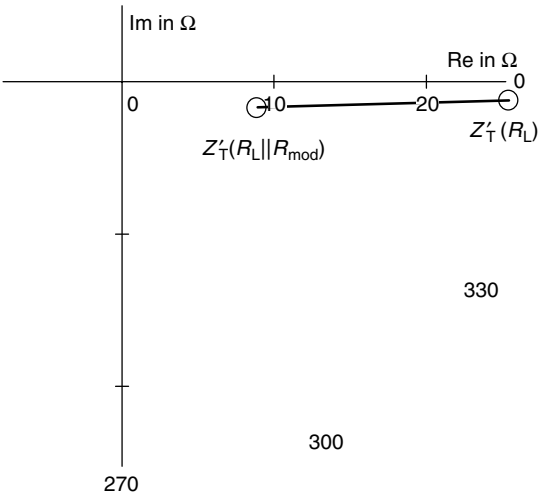


Figure 4.38 Locus curve of the transformed transponder impedance with ohmic load modulation ($R_L \| R_{mod} = 1.5\text{–}5\,k\Omega$) of an inductively coupled transponder. The parallel connection of the *modulation resistor* R_{mod} results in a lower value of Z'_T

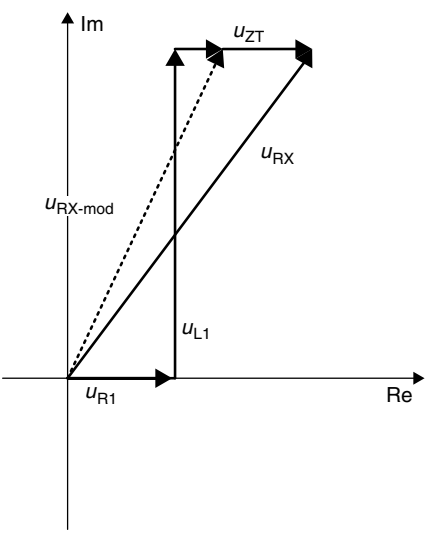


Figure 4.39 Vector diagram for the total voltage u_{RX} that is available to the receiver of a reader. The magnitude and phase of u_{RX} are modulated at the antenna coil of the reader (L_1) by an ohmic load modulator

We know from the previous section that the detuning of the transponder resonant frequency markedly influences the magnitude and phase of the transformed transponder impedance Z'_T. This is also clearly visible from the locus curve for the capacitive load modulator (Figure 4.41): Z'_T is switched between the values $Z'_T(\omega_{RES1})$ and $Z'_T(\omega_{RES2})$ by the load modulator in the transponder. The locus curve for Z'_T thereby passes

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

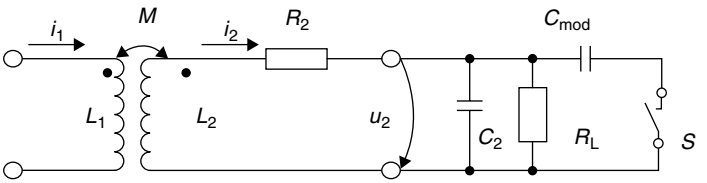


Figure 4.40 Equivalent circuit diagram for a transponder with capacitive load modulator. To transmit data the switch S is closed in time with the data stream — or a modulated subcarrier signal

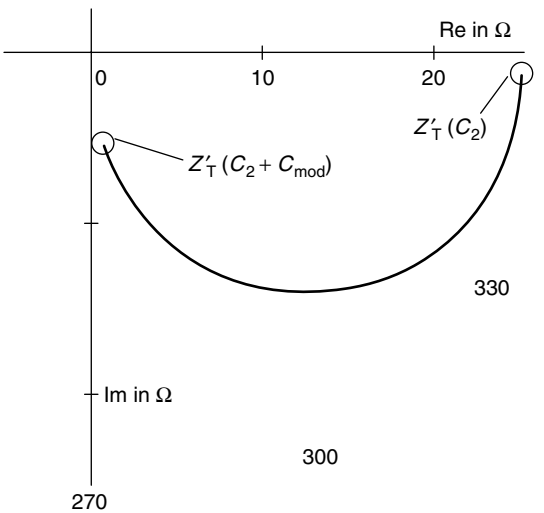


Figure 4.41 Locus curve of transformed transponder impedance for the capacitive load modulation ($C_2 \| C_{mod} = 40–60$ pF) of an inductively coupled transponder. The parallel connection of a *modulation capacitor* C_{mod} results in a modulation of the magnitude and phase of the transformed transponder impedance Z'_T

through a segment of the circle in the complex Z plane that is typical of the parallel resonant circuit.

Demodulation of the data signal is similar to the procedure used with ohmic load modulation. Capacitive *load modulation* generates a combination of *amplitude and phase modulation* of the reader antenna voltage u_{RX} and should therefore be processed in an appropriate manner in the receiver branch of the reader. The relevant vector diagram is shown in Figure 4.42.

Demodulation in the reader For transponders in the frequency range <135 kHz the load modulator is generally controlled directly by a serial data stream encoded in the baseband, e.g. a Manchester encoded bit sequence. The modulation signal from the transponder can be recreated by the rectification of the amplitude modulated voltage at the antenna coil of the reader (see Section 11.3).

In higher frequency systems operating at 6.78 MHz or 13.56 MHz, on the other hand, the transponder's load modulator is controlled by a modulated subcarrier signal.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

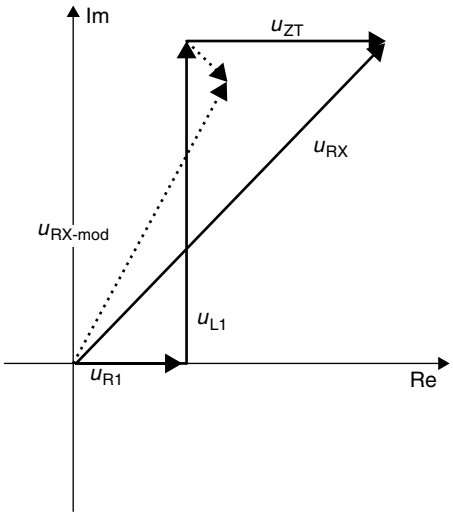


Figure 4.42 Vector diagram of the total voltage u_{RX} available to the receiver of the reader. The magnitude and phase of this voltage are modulated at the antenna coil of the reader (L_1) by a capacitive load modulator

(see Section 6.2.4). The subcarrier frequency f_H is normally 847 kHz (ISO 14443-2), 423 kHz (ISO 15693) or 212 kHz.

Load modulation with a subcarrier generates two sidebands at a distance of $\pm f_H$ to either side of the transmission frequency (see Section 6.2.4). The information to be transmitted is held in the two sidebands, with each sideband containing the same information. One of the two sidebands is filtered in the reader and finally demodulated to reclaim the baseband signal of the modulated data stream.

The influence of the Q factor As we know from the preceding section, we attempt to maximise the *Q factor* in order to maximise the energy range and the retroactive transformed transponder impedance. From the point of view of the energy range, a high Q factor in the transponder resonant circuit is definitely desirable. If we want to transmit data from or to the transponder a certain minimum bandwidth of the transmission path from the data carrier in the transponder to the receiver in the reader will be required. However, the bandwidth B of the *transponder resonant circuit* is inversely proportional to the Q factor.

$$B = \frac{f_{RES}}{Q} \tag{4.55}$$

Each load modulation operation in the transponder causes a corresponding amplitude modulation of the current i_2 in the transponder coil. The modulation sidebands of the current i_2 that this generates are damped to some degree by the bandwidth of the transponder resonant circuit, which is limited in practice. The bandwidth B determines a frequency range around the resonant frequency f_{RES}, at the limits of which the modulation sidebands of the current i_2 in the transponder reach a damping of 3 dB relative to the resonant frequency (Figure 4.43). If the Q factor of the transponder is

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

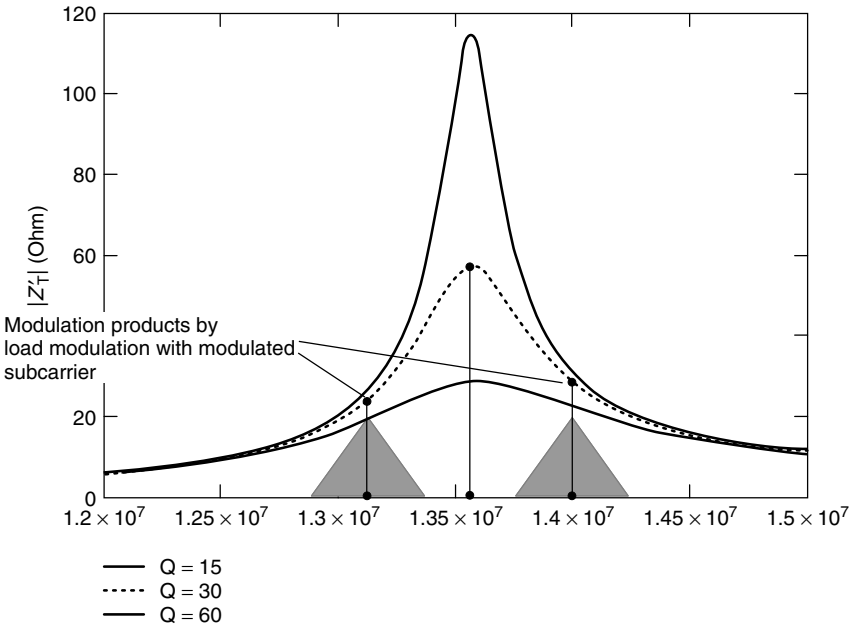


Figure 4.43 The transformed transponder impedance reaches a peak at the resonant frequency of the transponder. The amplitude of the modulation sidebands of the current i_2 is damped due to the influence of the bandwidth B of the transponder resonant circuit (where $f_H = 440\,\text{kHz}$, $Q = 30$)

too high, then the modulation sidebands of the current i_2 are damped to such a degree due to the low bandwidth that the range is reduced (transponder signal range).

Transponders used in 13.56 MHz systems that support an *anticollision algorithm* are adjusted to a resonant frequency of 15–18 MHz to minimise the mutual influence of several transponders. Due to the marked detuning of the transponder resonant frequency relative to the transmission frequency of the reader the two modulation sidebands of a load modulation system with subcarrier are transmitted at a different level (see Figure 4.44).

The term bandwidth is problematic here (the frequencies of the reader and the modulation sidebands may even lie outside the bandwidth of the transponder resonant circuit). However, the selection of the correct Q factor for the transponder resonant circuit is still important, because the Q factor can influence the transient effects during load modulation.

Ideally, the 'mean Q factor' of the transponder will be selected such that the energy range and transponder signal range of the system are identical. However, the calculation of an ideal Q factor is non-trivial and should not be underestimated because the Q factor is also strongly influenced by the *shunt regulator* (in connection with the distance d between transponder and reader antenna) and by the *load modulator* itself. Furthermore, the influence of the bandwidth of the transmitter antenna (series resonant circuit) on the level of the load modulation sidebands should not be underestimated.

Therefore, the development of an inductively coupled RFID system is always a compromise between the system's range and its data transmission speed (baud

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

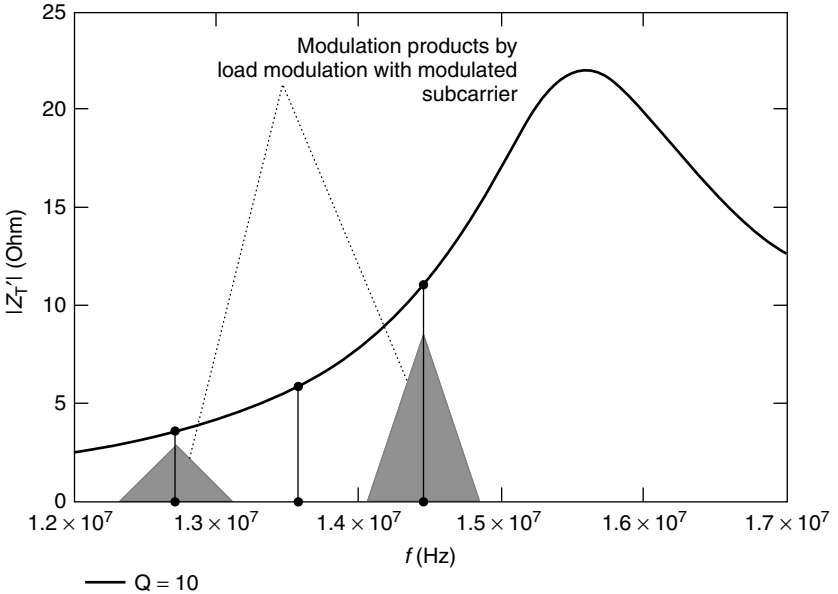


Figure 4.44 If the transponder resonant frequency is markedly detuned compared to the transmission frequency of the reader the two modulation sidebands will be transmitted at different levels. (Example based upon subcarrier frequency $f_H = 847\,\text{kHz}$)

rate/subcarrier frequency). Systems that require a short transaction time (that is, rapid data transmission and large bandwidth) often only have a range of a few centimetres, whereas systems with relatively long transaction times (that is, slow data transmission and low bandwidth) can be designed to achieve a greater range. A good example of the former case is provided by contactless smart cards for local public transport applications, which carry out authentication with the reader within a few 100 ms and must also transmit booking data. Contactless smart cards for 'hands free' access systems that transmit just a few bytes — usually the serial number of the data carrier — within 1–2 seconds are an example of the latter case. A further consideration is that in systems with a 'large' transmission antenna the data rate of the reader is restricted by the fact that only small sidebands may be generated because of the need to comply with the radio licensing regulations (ETS, FCC). Table 4.4 gives a brief overview of the relationship between range and bandwidth in inductively coupled RFID systems.

4.1.11 Measurement of system parameters

4.1.11.1 Measuring the coupling coefficient k

The coupling coefficient k and the associated mutual inductance M are the most important parameters for the design of an inductively coupled RFID system. It is precisely these parameters that are most difficult to determine analytically as a result of the — often complicated — field pattern. Mathematics may be fun, but has its limits.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 4.4 Typical relationship between range and bandwidth in 13.56 MHz systems. An increasing Q factor in the transponder permits a greater range in the transponder system. However, this is at the expense of the bandwidth and thus also the data transmission speed (baud rate) between transponder and reader

System	Baud rate	$f_{Subcarrier}$	f_{TX}	Range
ISO 14443	106 kBd	847 kHz	13.56 MHz	0–10 cm
ISO 15693 short	26.48 kBd	484 kHz	13.56 MHz	0–30 cm
ISO 15693 long	6.62 kBd	484 kHz	13.56 MHz	0–70 cm
Long-range system	9.0 kBd	212 kHz	13.56 MHz	0–1 m
LF system	−0–10 kBd	No subcarrier	<125 kHz	0–1.5 m

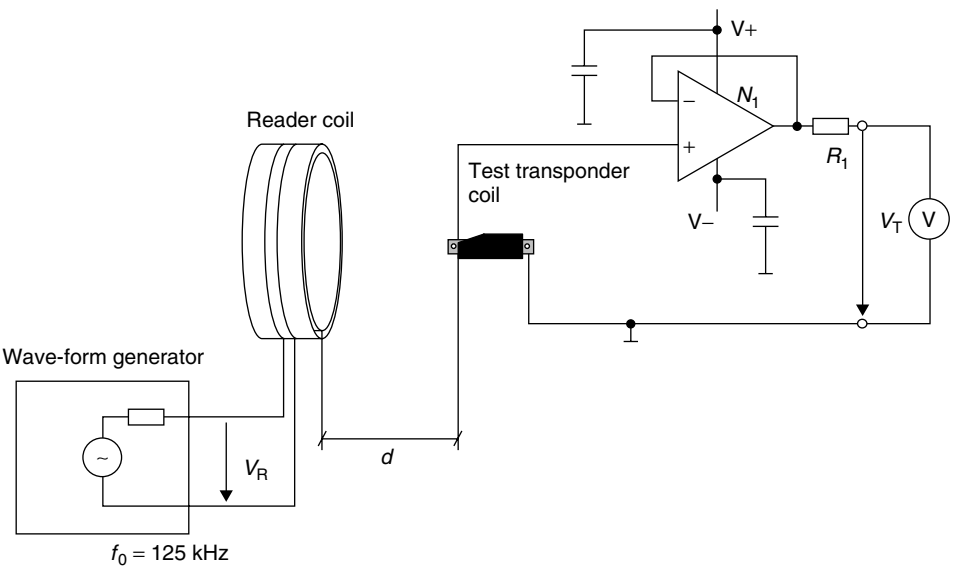


Figure 4.45 Measurement circuit for the measurement of the magnetic coupling coefficient k. N1: TL081 or LF 356N, R1: 100–500 Ω (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

Furthermore, the software necessary to calculate a numeric simulation is often unavailable — or it may simply be that the time or patience is lacking.

However, the coupling coefficient k for an existing system can be quickly determined by means of a simple measurement. This requires a test transponder coil with electrical and mechanical parameters that correspond with those of the 'real' transponder. The coupling coefficient can be simply calculated from the measured voltages U_R at the reader coil and U_T at the transponder coil (in Figure 4.45 these are denoted as V_R and V_T):

$$k = A_k \cdot \frac{U_T}{U_R} \cdot \sqrt{\frac{L_R}{L_T}} \tag{4.56}$$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

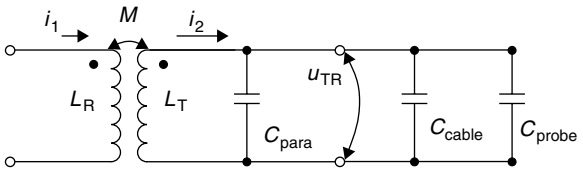


Figure 4.46 Equivalent circuit diagram of the test transponder coil with the parasitic capacitances of the measuring circuit

where U_T is the voltage at the transponder coil, U_R is the voltage at the reader coil, L_T and L_R are the inductance of the coils and A_K is the correction factor (<1).

The parallel, parasitic capacitances of the measuring circuit and the test transponder coil itself influence the result of the measurement because of the undesired current i_2. To compensate for this effect, equation (4.56) includes a correction factor A_K. Where $C_{TOT} = C_{para} + C_{cable} + C_{probe}$ (see Figure 4.46) the correction factor is defined as:

$$A_k = 2 - \frac{1}{1 - (\omega^2 \cdot C_{TOT} \cdot L_T)} \tag{4.57}$$

In practice, the correction factor in the low capacitance layout of the measuring circuit is $A_K \sim 0.99 - 0.8$ (TEMIC, 1977).

4.1.11.2 Measuring the transponder resonant frequency

The precise measurement of the transponder resonant frequency so that deviations from the desired value can be detected is particularly important in the manufacture of inductively coupled transponders. However, since transponders are usually packed in a glass or plastic housing, which renders them inaccessible, the measurement of the resonant frequency can only be realised by means of an inductive coupling.

The measurement circuit for this is shown in Figure 4.47. A coupling coil (conductor loop with several windings) is used to achieve the inductive coupling between transponder and measuring device. The self-resonant frequency of this coupling coil should be significantly higher (by a factor of at least 2) than the self-resonant frequency of the transponder in order to minimise measuring errors.

A phase and impedance analyser (or a network analyser) is now used to measure the impedance Z_1 of the coupling coil as a function of frequency. If Z_1 is represented

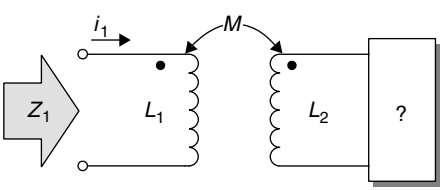


Figure 4.47 The circuit for the measurement of the *transponder resonant frequency* consists of a coupling coil L_1 and a measuring device that can precisely measure the complex impedance of Z_1 over a certain frequency range

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

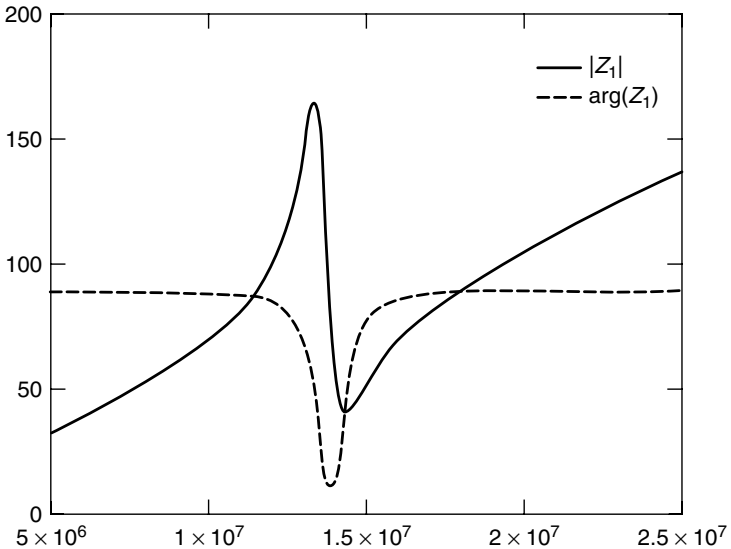


Figure 4.48 The measurement of impedance and phase at the measuring coil permits no conclusion to be drawn regarding the frequency of the transponder

in the form of a line diagram it has a curved path, as shown in Figure 4.48. As the measuring frequency rises the line diagram passes through various local maxima and minima for the magnitude and phase of Z_1. The sequence of the individual maxima and minima is always the same.

In the event of mutual inductance with a transponder the impedance Z_1 of the coupling coil L_1 is made up of several individual impedances:

$$Z_1 = R_1 + j\omega L_1 + Z'_T \tag{4.58}$$

Apart from at the transponder resonant frequency f_{RES}, Z'_T tends towards zero, so $Z_1 = R_L + j\omega L_1$. The locus curve in this range is a line parallel to the imaginary y axis of the complex Z plane at a distance of R_1 from it. If the measuring frequency approaches the transponder resonant frequency this straight line becomes a circle as a result of the influence of Z'_T. The locus curve for this is shown in Figure 4.49. The transponder resonant frequency corresponds with the maximum value of the real component of Z_1 (however this is not visible in the line diagram shown in Figure 4.48). The appearance of the individual maxima and minima of the line diagram can also be seen in the locus curve. A precise measurement of the transponder resonant frequency is therefore only possible using measuring devices that permit a separate measurement of R and X or can display a locus curve or line diagram.

4.1.12 Magnetic materials

Materials with a relative *permeability* >1 are termed ferromagnetic materials. These materials are iron, cobalt, nickel, various alloys and ferrite.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

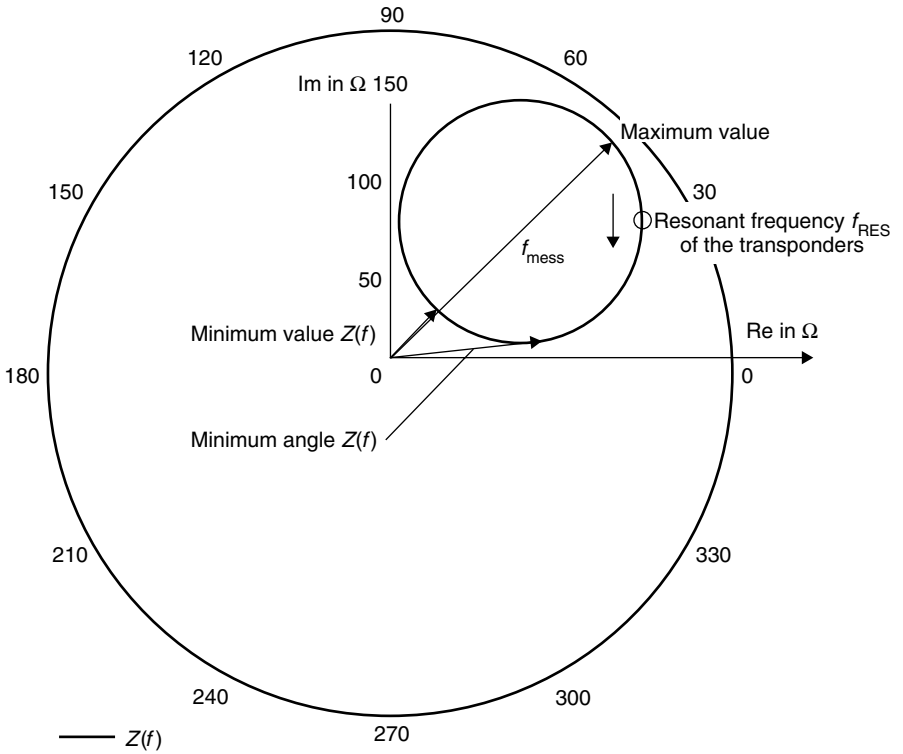


Figure 4.49 The locus curve of impedance Z_1 in the frequency range 1–30 MHz

4.1.12.1 Properties of magnetic materials and ferrite

One important characteristic of a magnetic material is the *magnetisation characteristic* or *hysteresis curve*. This describes $B = f(\mathrm{H})$, which displays a typical path for all ferromagnetic materials.

Starting from the unmagnetized state of the ferromagnetic material, the virgin curve $A \rightarrow B$ is obtained as the magnetic field strength H increases. During this process, the molecular magnets in the material align themselves in the B direction. (Ferromagnetism is based upon the presence of molecular magnetic dipoles. In these, the electron circling the atomic core represents a current and generates a magnetic field. In addition to the movement of the electron along its path, the rotation of the electron around itself, the spin, also generates a magnetic moment, which is of even greater importance for the material's magnetic behaviour.) Because there is a finite number of these molecular magnets, the number that remain to be aligned falls as the magnetic field increases, thus the gradient of the hysteresis curve falls. When all molecular magnets have been aligned, B rises in proportion to H only to the same degree as in a vacuum (Figure 4.50).

When the field strength H falls to $H = 0$, the flux density B falls to the positive residual value B_R, the remanence. Only after the application of an opposing field

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

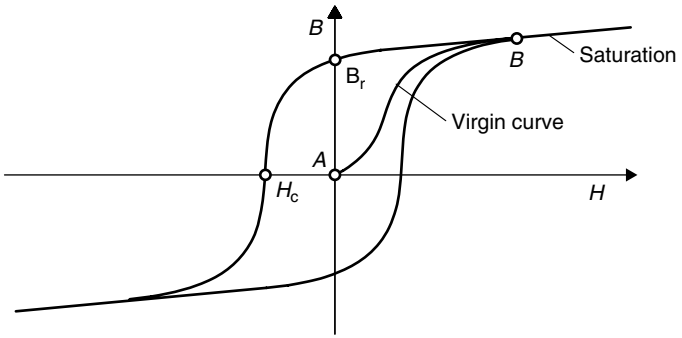


Figure 4.50 Typical magnetisation or hysteresis curve for a ferromagnetic material

$(-H)$ does the flux density B fall further and finally return to zero. The field strength necessary for this is termed the coercive field strength H_C.

Ferrite is the main material used in high frequency technology. This is used in the form of soft magnetic ceramic materials (low B_r), composed mainly of mixed crystals or compounds of iron oxide (Fe_2O_3) with one or more oxides of bivalent metals (NiO, ZnO, MnO etc.) (Vogt. Elektronik, 1990). The manufacturing process is similar to that for ceramic technologies (sintering).

The main characteristic of ferrite is its high specific electrical resistance, which varies between 1 and 10^6 Ωm depending upon the material type, compared to the range for metals, which vary between 10^{-5} and 10^{-4} Ωm. Because of this, eddy current losses are low and can be disregarded over a wide frequency range.

The relative permeability of ferrites can reach the order of magnitude of $\mu_r = 2000$.

An important characteristic of ferrite materials is their material-dependent limit frequency, which is listed in the datasheets provided by the ferrite manufacturer. Above the limit frequency increased losses occur in the ferrite material, and therefore ferrite should not be used outside the specified frequency range.

4.1.12.2 Ferrite antennas in LF transponders

Some applications require extremely small transponder coils (Figure 4.51). In transponders for animal identification, typical dimensions for cylinder coils are $d \times l = 5\,\text{mm} \times 0.75\,\text{mm}$. The mutual inductance that is decisive for the power supply of the transponder falls sharply due to its proportionality with the cross-sectional area of the coil ($M \sim A$; equation (4.13)). By inserting a ferrite material with a high permeability μ into the coil ($M \sim \Psi \rightarrow M \sim \mu \cdot H \cdot A$; equation (4.13)), the mutual inductance can be significantly increased, thus compensating for the small cross-sectional area of the coil.

The inductance of a *ferrite antenna* can be calculated according to the following equation (Philips Components, 1994):

$$L = \frac{\mu_0 \mu_{\text{Ferrite}} \cdot n^2 \cdot A}{l} \tag{4.50}$$

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

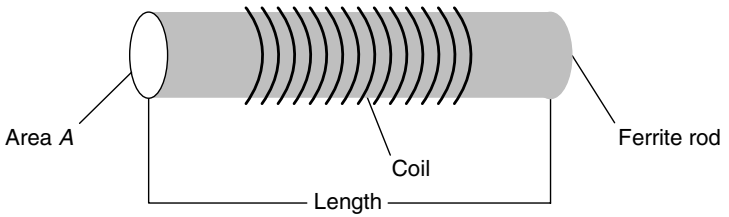


Figure 4.51 Configuration of a ferrite antenna in a 135 kHz glass transponder

4.1.12.3 Ferrite shielding in a metallic environment

The use of (inductively coupled) RFID systems often requires that the reader or transponder antenna be mounted directly upon a metallic surface. This might be the reader antenna of an automatic ticket dispenser or a transponder for mounting on gas bottles (see Figure 4.52).

However, it is not possible to fit a magnetic antenna directly onto a metallic surface. The magnetic flux through the metal surface induces eddy currents within the metal, which oppose the field responsible for their creation, i.e. the reader's field (Lenz's law), thus damping the magnetic field in the surface of the metal to such a degree that communication between reader and transponder is no longer possible. It makes no difference here whether the magnetic field is generated by the coil mounted upon the metal surface (reader antenna) or the field approaches the metal surface from 'outside' (transponder on metal surface).

By inserting highly permeable ferrite between the coil and metal surface it is possible to largely prevent the occurrence of eddy currents. This makes it possible to mount the antenna on metal surfaces.

When fitting antennas onto ferrite surfaces it is necessary to take into account the fact that the inductance of the conductor loop or coils may be significantly increased by

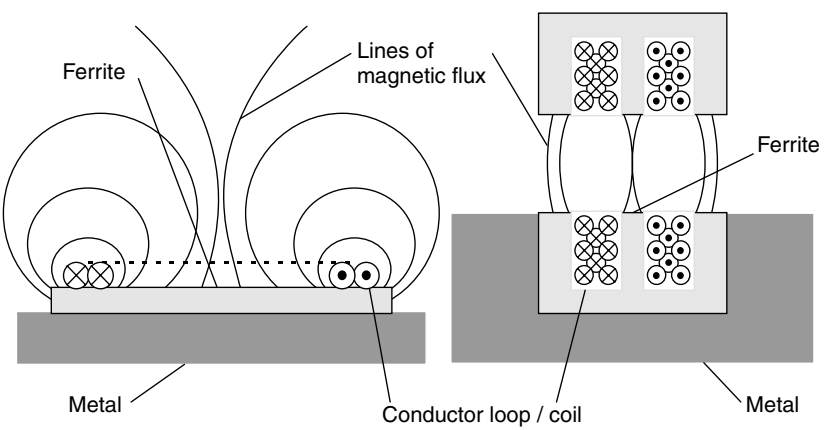


Figure 4.52 Reader antenna (left) and gas bottle transponder in a u-shaped core with read head (right) can be mounted directly upon or within metal surfaces using ferrite shielding

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

the permeability of the ferrite material, and it may therefore be necessary to readjust the resonant frequency or even redimension the matching network (in readers) altogether (see Section 11.4).

4.1.12.4 Fitting transponders in metal

Under certain circumstances it is possible to fit transponders directly into a metallic environment (Figure 4.53). *Glass transponders* are used for this because they contain a coil on a highly permeable *ferrite rod*. If such a transponder is inserted horizontally into a long groove on the metal surface somewhat larger than the transponder itself, then the transponder can be read without any problems. When the transponder is fitted horizontally the field lines through the transponder's ferrite rod run in parallel to the *metal surface* and therefore the eddy current losses remain low. The insertion of the transponder into a vertical bore would be unsuccessful in this situation, since the field lines through the transponder's ferrite rod in this arrangement would end at the top of the bore at right angles to the metal surface. The *eddy current losses* that occur in this case hinder the interrogation of a transponder.

It is even possible to cover such an arrangement with a *metal lid*. However, a narrow gap of dielectric material (e.g. paint, plastic, air) is required between the two metal surfaces in order to interrogate the transponder. The field lines running parallel

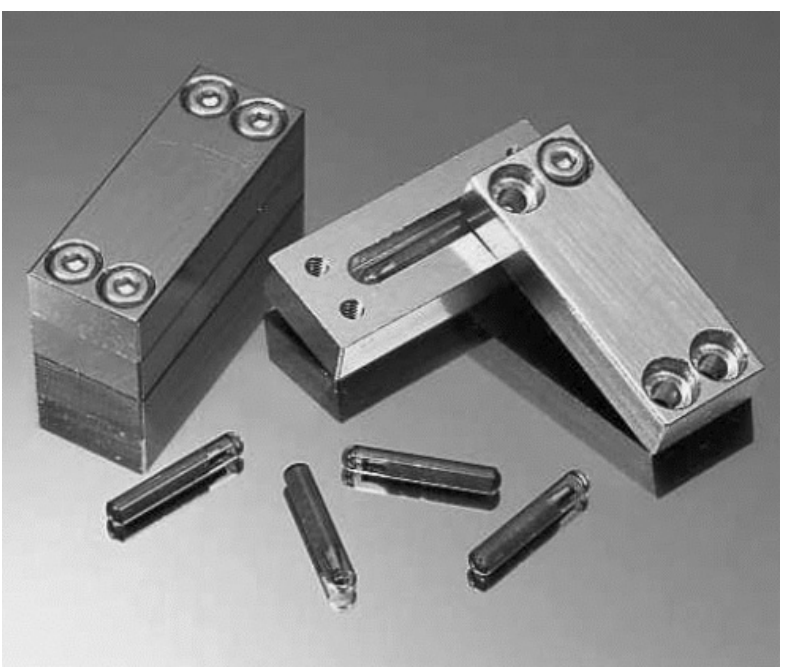


Figure 4.53 Right, fitting a glass transponder into a metal surface; left, the use of a thin dielectric gap allows the transponders to be read even through a metal casing (Photo: HANEX HXID system with Sokymat glass transponder in metal, reproduced by permission of HANEX Co. Ltd, Japan)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

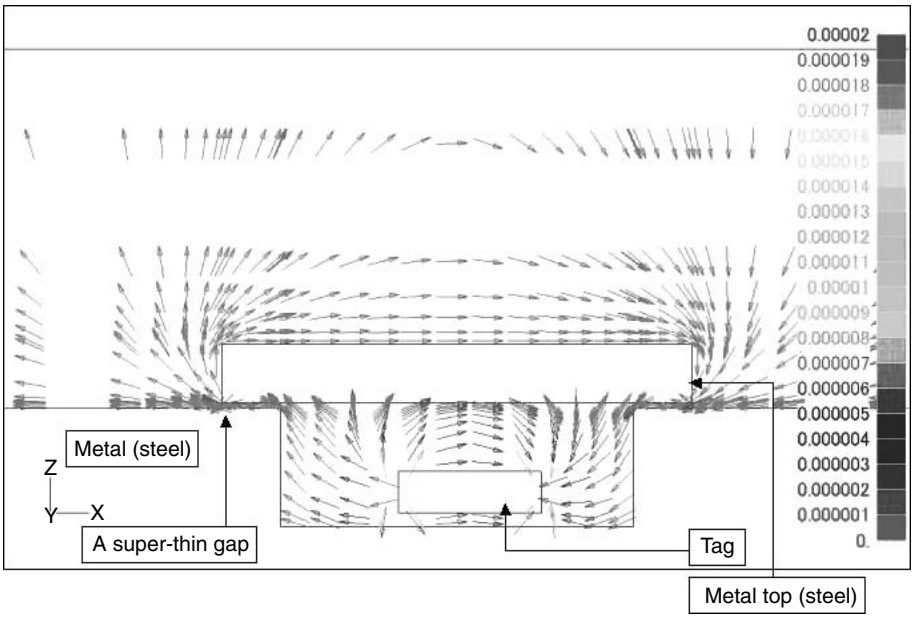


Figure 4.54 Path of field lines around a transponder encapsulated in metal. As a result of the dielectric gap the field lines run in parallel to the metal surface, so that eddy current losses are kept low (reproduced by permission of HANEX Co. Ltd, Japan)

to the metal surface enter the cavity through the *dielectric gap* (see Figure 4.54), so that the transponder can be read. Fitting transponders in metal allows them to be used in particularly hostile environments. They can even be run over by vehicles weighing several tonnes without suffering any damage.

Disk tags and contactless smart cards can also be embedded between metal plates. In order to prevent the magnetic field lines from penetrating into the metal cover, metal foils made of a highly permeable *amorphous metal* are placed above and below the tag (Hanex, n.d.). It is of crucial importance for the functionality of the system that the amorphous foils each cover only one half of the tag.

The magnetic field lines enter the amorphous material in parallel to the surface of the metal plates and are carried through it as in a conductor (Figure 4.55). At the gap between the two part foils a magnetic flux is generated through the transponder coil, so that this can be read.

4.2 Electromagnetic Waves

4.2.1 The generation of electromagnetic waves

Earlier in the book we described how a time varying *magnetic field* in space induces an *electric field* with closed field lines (rotational field) (see also Figure 4.11). The electric field surrounds the magnetic field and itself varies over time. Due to the variation of the electric rotational field over time, a magnetic field with closed field lines occurs in

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

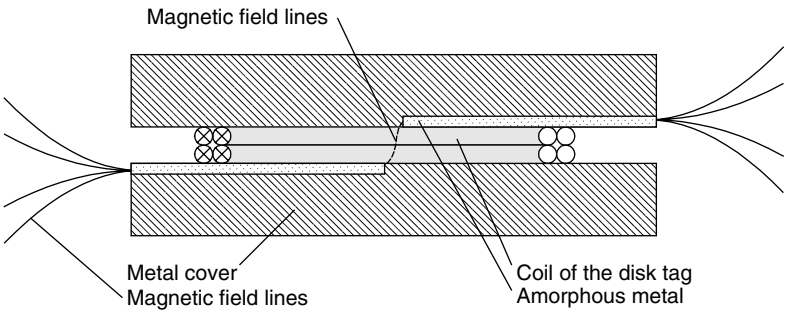


Figure 4.55 Cross-section through a sandwich made of disk transponder and metal plates. Foils made of amorphous metal cause the magnetic field lines to be directed outwards

space (rotational field). It surrounds the electric field and itself varies over time, thus generating another electric field. Due to the mutual dependence of the time varying fields there is a chain effect of electric and magnetic fields in space (Fricke *et al.*, 1979).

Radiation can only occur given a finite propagation speed ($c \approx 300\,000$ km/s; *speed of light*) for the electromagnetic field, which prevents a change in the voltage at the antenna from being followed immediately by the field in the vicinity of the change. Figure 4.56 shows the creation of an *electromagnetic wave* at a *dipole antenna*. Even at the alternating voltage's zero crossover (Figure 4.56c), the field lines remaining in space from the previous half wave cannot end at the antenna, but close into themselves, forming eddies. The eddies in the opposite direction that occur in the next half wave propel the existing eddies, and thus the energy stored in this field, away from the emitter at the speed of light c. The magnetic field is interlinked with the varying electrical field that propagates at the same time. When a certain distance is reached, the fields are released from the emitter, and this point represents the beginning of electromagnetic radiation ($\rightarrow$ far field). At high frequencies, that is small wavelengths, the radiation generated is particularly effective, because in this case the separation takes place in the direct vicinity of the emitter, where high field strengths still exist (Fricke *et al.*, 1979).

The distance between two field eddies rotating in the same direction is called the *wavelength* λ of the electromagnetic wave, and is calculated from the quotient of the speed of light c and the frequency of the radiation:

$$\lambda = \frac{c}{f} \tag{4.60}$$

4.2.1.1 Transition from near field to far field in conductor loops

The primary magnetic field generated by a *conductor loop* begins at the antenna (see also Section 4.1.1.1). As the magnetic field propagates an electric field increasingly also develops by induction (compare Figure 4.11). The field, which was originally purely magnetic, is thus continuously transformed into an electromagnetic field. Moreover,

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

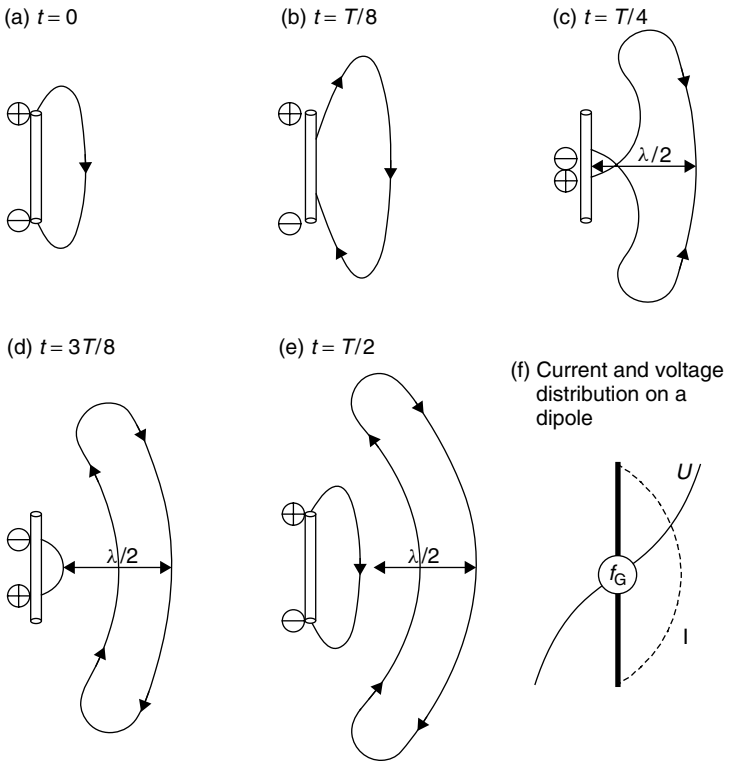


Figure 4.56 The creation of an electromagnetic wave at a dipole antenna. The electric field E is shown. The magnetic field H forms as a ring around the antenna and thus lies at right angles to the electric field

at a distance of $\lambda/2\pi$ the electromagnetic field begins to separate from the antenna and wanders into space in the form of an electromagnetic wave. The area from the antenna to the point where the electromagnetic field forms is called the *near field* of the antenna. The area after the point at which the electromagnetic wave has fully formed and separated from the antenna is called the *far field*.

A separated electromagnetic wave can no longer retroact upon the antenna that generated it by inductive or capacitive coupling. For inductively coupled RFID systems this means that once the far field has begun a *transformer (inductive) coupling* is no

Table 4.5 Frequency and wavelengths of different VHF–UHF frequencies

Frequency	Wavelength (cm)
433 MHz	69 (70 cm band)
868 MHz	34
915 MHz	33
2.45 GHz	12
5.8 GHz	5.2

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 4.6 r_F and λ for different frequency ranges

Frequency	Wavelength λ (m)	$\lambda/2\pi$ (m)
<135 kHz	>2222	>353
6.78 MHz	44.7	7.1
13.56 MHz	22.1	3.5
27.125 MHz	11.0	1.7

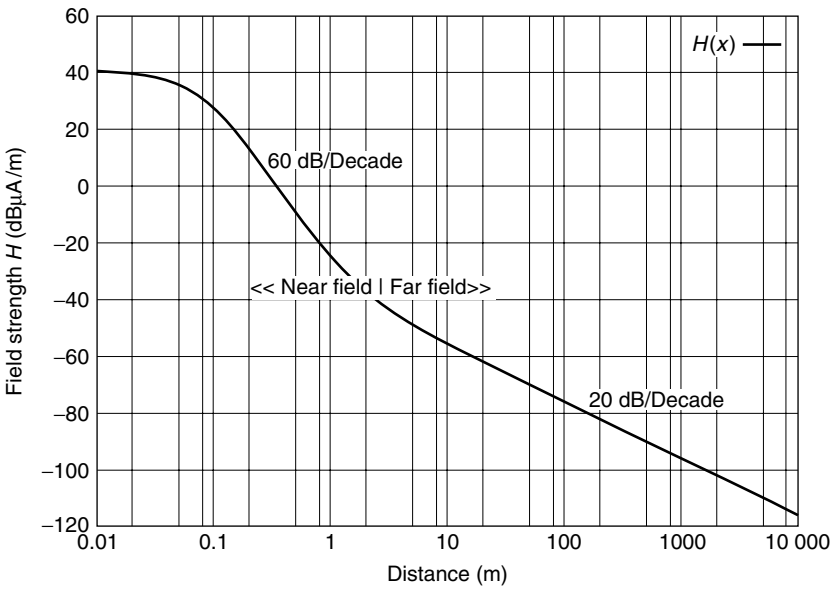


Figure 4.57 Graph of the magnetic field strength H in the transition from near to far field at a frequency of 13.56 MHz

longer possible. The beginning of the far field (the radius $r_F = \lambda/2\pi$ can be used as a rule of thumb) around the antenna thus represents an insurmountable *range limit* for inductively coupled systems.

The field strength path of a magnetic antenna along the coil x axis follows the relationship $1/d^3$ in the near field, as demonstrated above. This corresponds with a damping of 60 dB per decade (of distance). Upon the transition to the far field, on the other hand, the damping path flattens out, because after the separation of the field from the antenna only the *free space attenuation* of the electromagnetic waves is relevant to the field strength path (Figure 4.57). The field strength then decreases only according to the relationship $1/d$ as distance increases (see equation (4.65)). This corresponds with a damping of just 20 dB per decade (of distance).

4.2.2 Radiation density *S*

An *electromagnetic wave* propagates into space spherically from the point of its creation. At the same time, the electromagnetic wave transports energy in the surrounding

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

space. As the distance from the radiation source increases, this energy is divided over an increasing sphere surface area. In this connection we talk of the *radiation power* per unit area, also called *radiation density* S.

In a *spherical emitter*, the so-called *isotropic emitter*, the energy is radiated uniformly in all directions. At distance r the radiation density S can be calculated very easily as the quotient of the energy supplied by the emitter (thus the transmission power P_{EIRP}) and the surface area of the sphere.

$$S = \frac{P_{\mathrm{EIRP}}}{4\pi r^2} \tag{4.61}$$

4.2.3 Characteristic wave impedance and field strength *E*

The energy transported by the electromagnetic wave is stored in the electric and magnetic field of the wave. There is therefore a fixed relationship between the radiation density S and the field strengths E and H of the interconnected electric and magnetic fields. The electric field with electric field strength E is at right angles to the magnetic field H. The area between the vectors E and H forms the wave front and is at right angles to the direction of propagation. The radiation density S is found from the Poynting radiation vector S as a vector product of E and H (Figure 4.58).

$$S = E \times H \tag{4.62}$$

The relationship between the field strengths E and H is defined by the permittivity and the dielectric constant of the propagation medium of the electromagnetic wave. In a vacuum and also in air as an approximation:

$$E = H \cdot \sqrt{\mu_0 \varepsilon_0} = H \cdot Z_{\mathrm{F}} \tag{4.63}$$

Z_{F} is termed the *characteristic wave impedance* ($Z_{\mathrm{F}} = 120\pi\,\Omega = 377\,\Omega$). Furthermore, the following relationship holds:

$$E = \sqrt{S \cdot Z_{\mathrm{F}}} \tag{4.64}$$

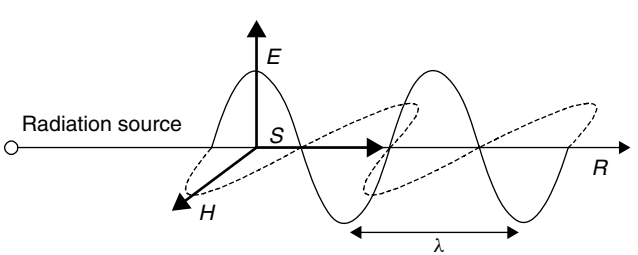


Figure 4.58 The Poynting radiation vector S as the vector product of E and H

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Therefore, the field strength E at a certain distance r from the radiation source can be calculated using equation (4.61). P_{EIRP} is the transmission power emitted from the isotropic emitter:

$$E = \sqrt{\frac{P_{\mathrm{EIRP}} \cdot Z_{\mathrm{F}}}{4\pi r^2}} \tag{4.65}$$

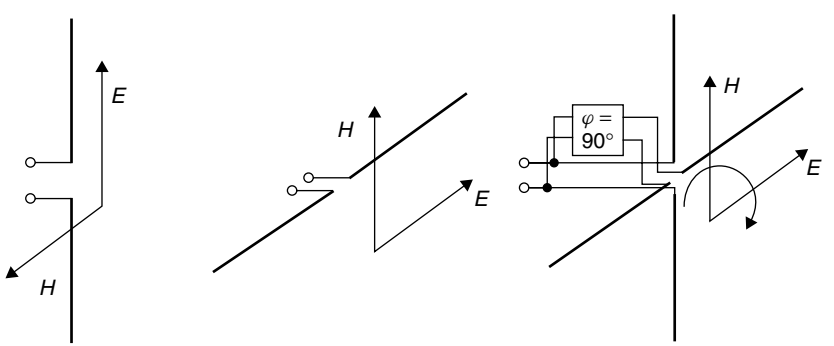
4.2.4 Polarisation of electromagnetic waves

The *polarisation* of an electromagnetic wave is determined by the direction of the electric field of the wave. We differentiate between *linear polarisation* and *circular polarisation*. In linear polarisation the direction of the field lines of the electric field E in relation to the surface of the earth provide the distinction between *horizontal* (the electric field lines run parallel to the surface of the earth) and *vertical* (the electric field lines run at right angles to the surface of the earth) *polarisation*.

So, for example, the dipole antenna is a linear polarised antenna in which the electric field lines run parallel to the dipole axis. A dipole antenna mounted at right angles to the earth's surface thus generates a vertically polarised electromagnetic field.

The transmission of energy between two linear polarised antennas is optimal if the two antennas have the same polarisation direction. Energy transmission is at its lowest point, on the other hand, when the polarisation directions of transmission and receiving antennas are arranged at exactly 90° or 270° in relation to one another (e.g. a horizontal antenna and a vertical antenna). In this situation an additional damping of 20 dB has to be taken into account in the power transmission due to *polarisation losses* (Rothammel, 1981), i.e. the receiving antenna draws just 1/100 of the maximum possible power from the emitted electromagnetic field.

In RFID systems, there is generally no fixed relationship between the position of the portable transponder antenna and the reader antenna. This can lead to fluctuations in the read range that are both high and unpredictable. This problem is aided by the use of circular polarisation in the reader antenna. The principle generation of circular polarisation is shown in Figure 4.59: two dipoles are fitted in the form of a cross. One of the two dipoles is fed via a 90° ($\lambda/4$) delay line. The polarisation direction of



(a) Vertical polarisation (b) Horizontal polarisation (c) Circular polarisation

Figure 4.59 Definition of the polarisation of electromagnetic waves

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

the electromagnetic field generated in this manner rotates through 360° every time the wave front moves forward by a wavelength. The rotation direction of the field can be determined by the arrangement of the delay line. We differentiate between left-handed and right-handed circular polarisation.

A polarisation loss of 3 dB should be taken into account between a linear and a circular polarised antenna; however, this is independent of the polarisation direction of the receiving antenna (e.g. the transponder).

4.2.4.1 Reflection of electromagnetic waves

An *electromagnetic wave* emitted into the surrounding space by an antenna encounters various objects. Part of the high frequency energy that reaches the object is absorbed by the object and converted into heat; the rest is scattered in many directions with varying intensity.

A small part of the reflected energy finds its way back to the transmitter antenna. *Radar technology* uses this reflection to measure the distance and position of distant objects (Figure 4.60).

In RFID systems the reflection of electromagnetic waves (*backscatter system, modulated radar cross-section*) is used for the transmission of data from a transponder to a reader. Because the *reflective properties* of objects generally increase with increasing frequency, these systems are used mainly in the frequency ranges of 868 MHz (Europe), 915 MHz (USA), 2.45 GHz and above.

Let us now consider the relationships in an RFID system. The antenna of a reader emits an electromagnetic wave in all directions of space at the transmission power P_{EIRP}. The *radiation density* S that reaches the location of the transponder can easily be calculated using equation (4.61). The transponder's antenna reflects a power P_{S} that is proportional to the power density S and the so-called *radar cross-section* σ is:

$$P_{\mathrm{S}} = \sigma \cdot S \tag{4.66}$$

The reflected electromagnetic wave also propagates into space spherically from the point of reflection. Thus the radiation power of the reflected wave also decreases in proportion to the square of the distance (r^2) from the radiation source (i.e. the reflection). The following power density finally returns to the reader's antenna:

$$S_{\mathrm{Back}} = \frac{P_{\mathrm{S}}}{4\pi r^2} = S \cdot \frac{\sigma}{4\pi r^2} = \frac{P_{\mathrm{EIRP}}}{4\pi r^2} \cdot \frac{\sigma}{4\pi r^2} = \frac{P_{\mathrm{EIRP}} \cdot \sigma}{(4\pi)^2 \cdot r^4} \tag{4.67}$$

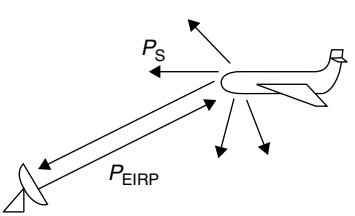


Figure 4.60 Reflection off a distant object is also used in radar technology

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The radar cross-section σ (RCS, scatter aperture) is a measure of how well an object reflects electromagnetic waves. The radar cross-section depends upon a range of parameters, such as object size, shape, material, surface structure, but also wavelength and polarisation.

The radar cross-section can only be calculated precisely for simple surfaces such as spheres, flat surfaces and the like (for example see Baur, 1985). The material also has a significant influence. For example, *metal surfaces* reflect much better than plastic or composite materials. Because the dependence of the radar cross-section σ on wavelength plays such an important role, objects are divided into three categories:

- Rayleigh range: the wavelength is large compared with the object dimensions. For objects smaller than around half the wavelength, σ exhibits a λ^{-4} dependency and so the reflective properties of objects smaller than 0.1 λ can be completely disregarded in practice.
- Resonance range: the wavelength is comparable with the object dimensions. Varying the wavelength causes σ to fluctuate by a few decibels around the geometric value. Objects with sharp resonance, such as sharp edges, slits and points may, at certain wavelengths, exhibit resonance step-up of σ. Under certain circumstances this is particularly true for antennas that are being irradiated at their resonant wavelengths (resonant frequency).
- Optical range: the wavelength is small compared to the object dimensions. In this case, only the geometry and position (angle of incidence of the electromagnetic wave) of the object influence the radar cross-section.

Backscatter RFID systems employ antennas with different construction formats as reflection areas. Reflections at transponders therefore occur exclusively in the resonance range. In order to understand and make calculations about these systems we need to know the radar cross-section σ of a resonant antenna. A detailed introduction to the calculation of the radar cross-section can therefore be found in the following sections.

It also follows from equation (4.67) that the power reflected back from the transponder is proportional to the fourth root of the power transmitted by the reader (Figure 4.61). In other words: if we wish to double the power density S of the reflected

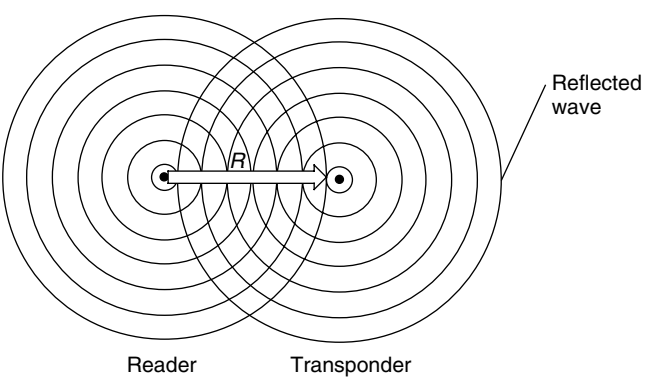


Figure 4.61 Propagation of waves emitted and reflected at the transponder

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

signal from the transponder that arrives at the reader, then, all other things being equal, the transmission power must be multiplied by sixteen!

4.2.5 Antennas

The creation of electromagnetic waves has already been described in detail in the previous section (see also Sections 4.1.6 and 4.2.1). The laws of physics tell us that the radiation of electromagnetic waves can be observed in all conductors that carry voltage and/or current. In contrast to these effects, which tend to be parasitic, an *antenna* is a component in which the radiation or reception of electromagnetic waves has been to a large degree optimised for certain frequency ranges by the fine-tuning of design properties. In this connection, the behaviour of an antenna can be precisely predicted and is exactly defined mathematically.

4.2.5.1 Gain and directional effect

Section 4.2.2 demonstrated how the power P_{EIRP} emitted from an *isotropic emitter* at a distance r is distributed in a fully uniform manner over a spherical surface area. If we integrate the power density S of the electromagnetic wave over the entire surface area of the sphere the result we obtain is, once again, the power P_{EIRP} emitted by the isotropic emitter.

$$P_{\mathrm{EIRP}} = \int_{A_{\mathrm{sphere}}} S \cdot \mathrm{d}A \tag{4.68}$$

However, a real antenna, for example a dipole, does not radiate the supplied power uniformly in all directions. For example, no power at all is radiated by a *dipole antenna* in the axial direction in relation to the antenna.

Equation (4.68) applies for all types of antennas. If the antenna emits the supplied power with varying intensity in different directions, then equation (4.68) can only be fulfilled if the radiation density S is greater in the preferred direction of the antenna than would be the case for an isotropic emitter. Figure 4.62 shows the *radiation pattern* of a dipole antenna in comparison to that of an isotropic emitter. The length of the vector $G(\Theta)$ indicates the relative radiation density in the direction of the vector. In the *main radiation direction* (G_{i}) the radiation density can be calculated as follows:

$$S = \frac{P_{\mathrm{l}} \cdot G_{\mathrm{i}}}{4\pi \cdot r^2} \tag{4.69}$$

P_{l} is the power supplied to the antenna. G_{i} is termed the gain of the antenna and indicates the factor by which the radiation density S is greater than that of an isotropic emitter at the same transmission power.

An important radio technology term in this connection is the *EIRP* (effective isotropic radiated power).

$$P_{\mathrm{EIRP}} = P_{\mathrm{l}} \cdot G_{\mathrm{i}} \tag{4.70}$$

This figure can often be found in radio licensing regulations (e.g. Section 5.2.4) and indicates the transmission power at which an isotropic emitter (i.e. $G_{\mathrm{i}} = 1$) would

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

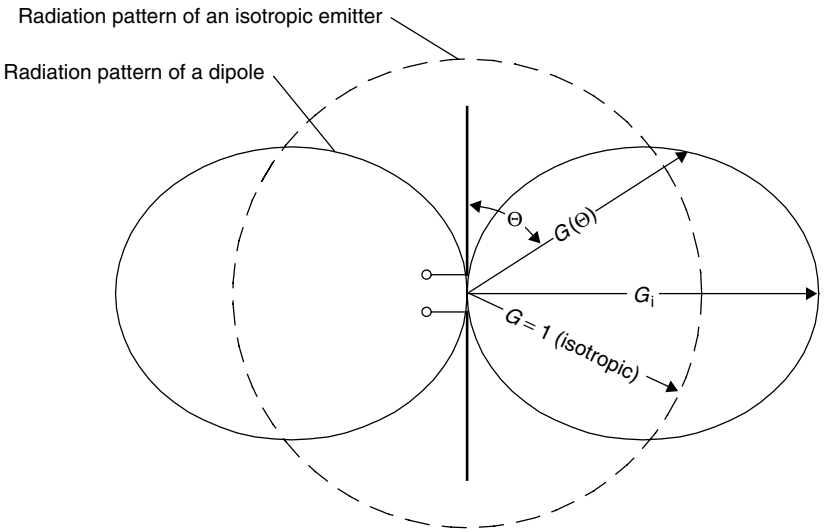


Figure 4.62 Radiation pattern of a dipole antenna in comparison to the radiation pattern of an isotropic emitter

have to be supplied in order to generate a defined radiation power at distance r. An antenna with a gain G_i may therefore only be supplied with a transmission power P_1 that is lower by this factor so that the specified limit value is not exceeded:

$$P_1 = \frac{P_{EIRP}}{G_i} \tag{4.71}$$

4.2.5.2 EIRP and ERP

In addition to power figures in EIRP we frequently come across the power figure ERP (equivalent radiated power) in radio regulations and technical literature. The ERP is also a reference power figure. However, in contrast to the EIRP, ERP relates to a dipole antenna rather than a spherical emitter. An ERP power figure thus expresses the transmission power at which a dipole antenna must be supplied in order to generate a defined emitted power at a distance of r. Since the gain of the dipole antenna

Table 4.7 In order to emit a constant EIRP in the main radiation direction less transmission power must be supplied to the antenna as the antenna gain G increases

EIRP = 4 W	**Power P_1 fed to the antenna**
Isotropic emitter $G_i = 1$	4 W
Dipole antenna	2.44 W
Antenna $G_i = 3$	1.33 W

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

($G_i = 1.64$) in relation to an isotropic emitter is known, it is easy to convert between the two figures:

$$P_{EIRP} = P_{ERP} \cdot 1.64 \tag{4.72}$$

4.2.5.3 Input impedance

A particularly important property of the antenna is the complex *input impedance* Z_A. This is made up of a complex resistance X_A, a loss resistance R_V and the so-called *radiation resistance* R_r:

$$Z_A = R_r + R_V + jX_A \tag{4.73}$$

The loss resistance R_V is an effective resistance and describes all losses resulting from the ohmic resistance of all current-carrying line sections of the antenna (Figure 4.63). The power converted by this resistance is converted into heat.

The radiation resistance R_r also takes the units of an effective resistance but the power converted within it corresponds with the power emitted from the antenna into space in the form of electromagnetic waves.

At the operating frequency (i.e. the resonant frequency of the antenna) the complex resistance X_A of the antenna tends towards zero. For a loss-free antenna (i.e. $R_V = 0$):

$$Z_A(f_{RES}) = R_r \tag{4.74}$$

The input impedance of an ideal antenna in the resonant case is thus a real resistance with the value of the radiation resistance R_r. For a $\lambda/2$ dipole the radiation resistance $R_r = 73\,\Omega$.

4.2.5.4 Effective aperture and scatter aperture

The maximum received power that can be drawn from an antenna, given optimal alignment and correct polarisation, is proportional to the power density S of an incoming

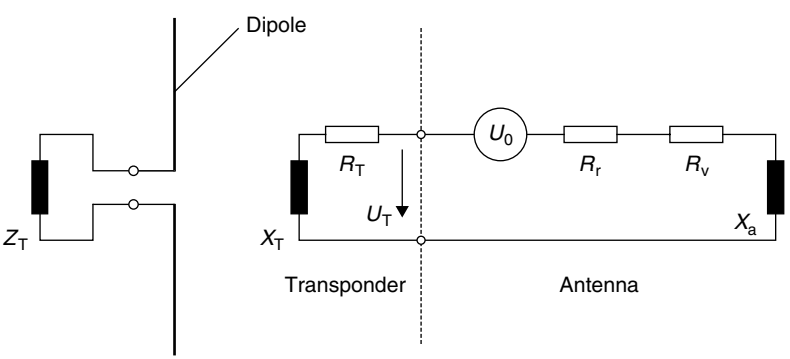


Figure 4.63 Equivalent circuit of an antenna with a connected transponder

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

plane wave and a proportionality factor. The proportionality factor has the dimension of an area and is thus called the *effective aperture* A_e. The following applies:

$$P_e = A_e \cdot S \tag{4.75}$$

We can envisage A_e as an area at right angles to the direction of propagation, through which, at a given radiation density S, the power P_e passes (Meinke and Gundlach, 1992). The power that passes through the effective aperture is absorbed and transferred to the connected terminating impedance Z_T (Figure 4.64).

In addition to the effective aperture A_e, an antenna also possesses a *scatter aperture* $\sigma = A_s$ at which the electromagnetic waves are reflected.

In order to improve our understanding of this, let us once again consider Figure 4.63. When an electromagnetic field with radiation density S is received a voltage U_0 is induced in the antenna, which represents the cause of a current I through the antenna impedance Z_A and the terminating impedance Z_T. The current I is found from the quotient of the induced voltage U_0 and the series connection of the individual impedances (Kraus, 1988):

$$\mathrm{I} = \frac{\mathrm{U}_0}{\mathrm{Z}_\mathrm{T} + \mathrm{Z}_\mathrm{A}} = \frac{\mathrm{U}_0}{\sqrt{(\mathrm{R}_\mathrm{r} + \mathrm{R}_\mathrm{V} + \mathrm{R}_\mathrm{T})^2 + (\mathrm{X}_\mathrm{A} + \mathrm{X}_\mathrm{T})^2}} \tag{4.76}$$

Furthermore for the received power P_e transferred to Z_T:

$$P_e = I^2 \cdot R_T \tag{4.77}$$

Let us now substitute I^2 in equation (4.77) for the expression in equation (4.76), obtaining:

$$P_e = \frac{U_0^2 \cdot R_T}{(R_r + R_V + R_T)^2 + (X_A + X_T)^2} \tag{4.78}$$

According to equation (4.75) the effective aperture A_e is the quotient of the received power P_e and the radiation density S. This finally yields:

$$A_e = \frac{P_e}{S} = \frac{U_0^2 \cdot R_T}{S \cdot [(R_r + R_V + R_T)^2 + (X_A + X_T)^2]} \tag{4.79}$$

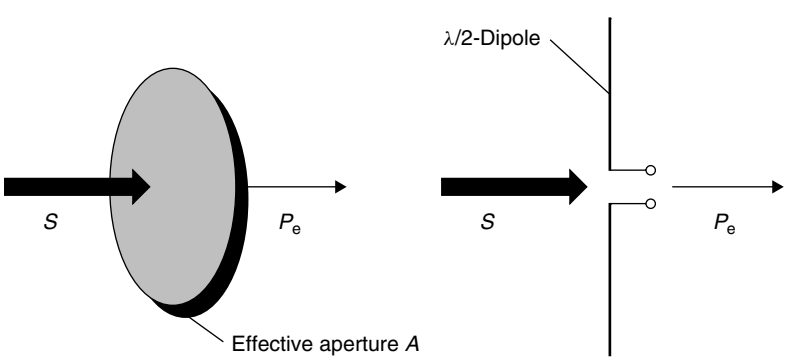


Figure 4.64 Relationship between the radiation density S and the received power P of an antenna

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

If the antenna is operated using power matching, i.e. $R_T = R_V$ and $X_T = -X_A$, then the following simplification can be used:

$$A_e = \frac{{U_0}^2}{4SR_r} \tag{4.80}$$

As can be seen from Figure 4.63 the current I also flows through the radiation resistance R_r of the antenna. The converted power P_S is emitted from the antenna and it makes no difference whether the current I was caused by an incoming electromagnetic field or by supply from a transmitter. The power P_S emitted from the antenna, i.e. the reflected power in the received case, can be calculated from:

$$P_S = I^2 \cdot R_r \tag{4.81}$$

Like the derivation for equation (4.79), for the scatter aperture A_s we find:

$$\sigma = A_S = \frac{P_S}{S} = \frac{I^2 \cdot R_r}{S} = \frac{{U_0}^2 \cdot R_r}{S \cdot [(R_r + R_V + R_T)^2 + (X_A + X_T)^2]} \tag{4.82}$$

If the antenna is again operated using power matching and is also loss-free, i.e. $R_V = 0$, $R_T = R_r$ and $X_T = -X_A$, then as a simplification:

$$\sigma = A_S = \frac{U_0^2}{4SR_r} \tag{4.83}$$

Therefore, in the case of the power matched antenna $\sigma = A_s = A_e$. This means that only half of the total power drawn from the electromagnetic field is supplied to the terminating resistor R_T; the other half is reflected back into space by the antenna.

The behaviour of the scatter aperture A_s at different values of the terminating impedance Z_T is interesting. Of particular significance for RFID technology is the limit case $Z_T = 0$. This represents a short-circuit at the terminals of the antennas. From equation (4.82) this is found to be:

$$\sigma_{max} = A_{S\text{-}max} = \frac{{U_0}^2}{SR_r} = 4A_e|_{Z_T=0} \tag{4.84}$$

The opposite limit case consists of the connection of an infinitely high-ohmic terminating resistor to the antenna, i.e. $Z_T \to \infty$. From equation (4.82) it is easy to see that the scatter aperture A_s, just like the current I, tends towards zero.

$$\sigma_{min} = A_{S\text{-}min} = 0|_{Z_T \to \infty} \tag{4.85}$$

The scatter aperture can thus take on any desired value in the range 0–4 A_e at various values of the terminating impedance Z_T (Figure 4.65). This property of antennas is utilised for the data transmission from transponder to reader in backscatter RFID systems (see Section 4.2.6.6).

Equation (4.82) shows only the relationship between the scatter aperture A_S and the individual resistors of the equivalent circuit from Figure 4.63. However, if we are

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

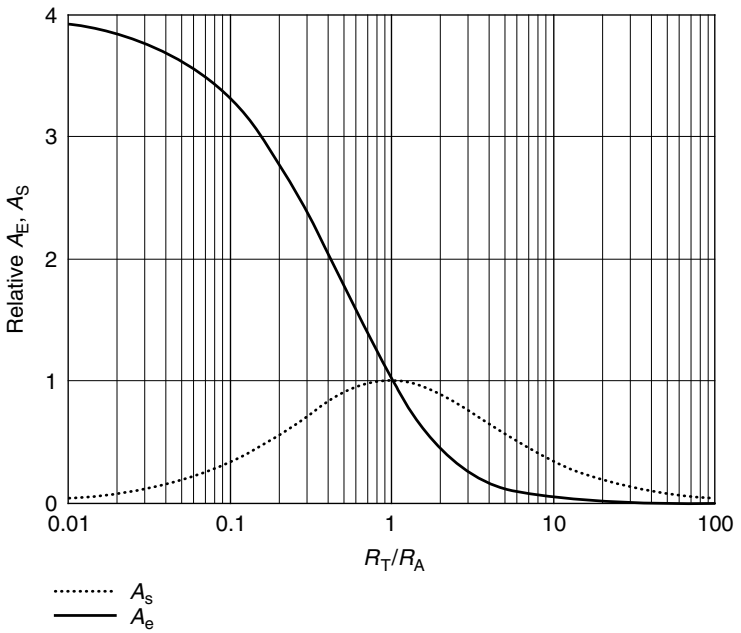


Figure 4.65 Graph of the relative effective aperture A_e and the relative scatter aperture σ in relation to the ratio of the resistances R_A and R_r. Where $R_T/R_A = 1$ the antenna is operated using power matching ($R_T = R_r$). The case $R_T/R_A = 0$ represents a short-circuit at the terminals of the antenna

to calculate the reflected power P_S of an antenna (see Section 4.2.4.1) we need the absolute value for A_S. The *effective aperture* A_e of an antenna is proportional to its gain G (Kraus, 1988; Meinke and Gundlach, 1992). Since the gain is known for most antenna designs, the effective aperture A_e, and thus also the scatter aperture A_S, is simple to calculate for the case of matching ($Z_A = Z_T$). The following is true[5]:

$$\sigma = A_e = \frac{\lambda_0^2}{4\pi} \cdot G \tag{4.86}$$

From equation (4.75) it thus follows that:

$$P_e = A_e \cdot S = \frac{\lambda_0^2}{4\pi} \cdot G \cdot S \tag{4.87}$$

4.2.5.5 Effective length

As we have seen, a voltage U_0 is induced in the antenna by an electromagnetic field. The voltage U_0 is proportional to the electric field strength E of the incoming wave.

[5] The derivation of this relationship is not important for the understanding of RFID systems, but can be found in Kraus (1988, chapter 2–22) if required.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The proportionality factor has the dimension of a length and is therefore called the *effective length* l_0 (also *effective height* h) (Meinke and Gundlach, 1992). The following is true:

$$U_0 = l_0 \cdot E = l_0 \cdot \sqrt{S \cdot Z_F} \tag{4.88}$$

For the case of the matched antenna (i.e. $R_r = R_T$) the effective length can be calculated from the effective aperture A_e (Kraus, 1988):

$$l_0 = 2\sqrt{\frac{A_e \cdot R_r}{Z_F}} \tag{4.89}$$

If we substitute the expression in equation (4.86) for A_e, then the effective length of a matched antenna can be calculated from the gain G, which is normally known (or easy to find by measuring):

$$l_0 = \lambda_0\sqrt{\frac{G \cdot R_r}{\pi \cdot Z_F}} \tag{4.90}$$

4.2.5.6 Dipole antennas

In its simplest form the *dipole antenna* consists solely of a straight piece of line (e.g. a copper wire) of a defined length (Figure 4.66). By suitable shaping the characteristic properties, in particular the *radiation resistance* and bandwidth, can be influenced.

A simple, extended *half-wave dipole* ($\lambda/2$ dipole) consists of a piece of line of length $l = \lambda/2$, which is interrupted half way along. The dipole is supplied at this break-point (Figure 4.67).

The parallel connection of two $\lambda/2$ pieces of line a small distance apart ($d < 0.05\lambda$) creates the *2-wire folded dipole*. This has around four times the radiation resistance of

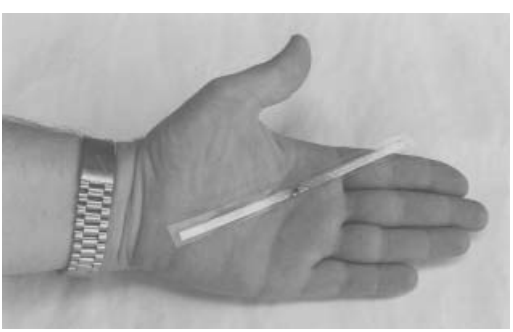


Figure 4.66 915 MHz transponder with a simple, extended dipole antenna. The transponder can be seen half way along (reproduced by permission of Trolleyscan, South Africa)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

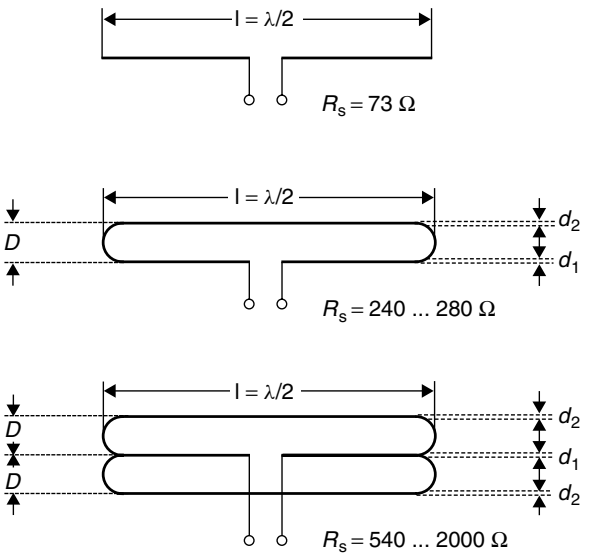


Figure 4.67 Different dipole antenna designs — from top to bottom: simple extended dipole, 2-wire folded dipole, 3-wire folded dipole

the single $\lambda/2$ dipole ($R_r = 240-280\,\Omega$). According to Rothammel (1981) the following relationship applies:

$$R_r = 73.2\,\Omega \cdot \left(\frac{\lg\left(\frac{4D^2}{d_1 \cdot d_2}\right)}{\lg\left(\frac{2D}{d_2}\right)} \right)^2 \tag{4.91}$$

A special variant of the loop dipole is the 3-wire folded dipole. The radiation resistance of the 3-wire folded dipole is greatly dependent upon the conductor diameter and the distance between the $\lambda/2$ line sections. In practice, the radiation resistance of the 3-wire folded dipole takes on values of $540-2000\,\Omega$. According to Rothammel (1981) the following relationship applies:

$$R_r = 73.2\,\Omega \cdot \left(\frac{\lg\left(\frac{4D^3}{d_1^2 \cdot d_2}\right)}{\lg\left(\frac{D}{d_2}\right)} \right)^2 \tag{4.92}$$

The bandwidth of a dipole can be influenced by the ratio of the diameter of the $\lambda/2$ line section to its length, increasing as the diameter increases. However, the dipole must then be shortened somewhat in order to allow it to resonate at the desired frequency. In practice, the *shortening factor* is around 0.90–0.99. For a more precise calculation

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 4.8 Electrical properties of the dipole and 2-wire folded dipole

Parameter	Gain G	Effective aperture	Effective length	Apex angle
$\lambda/2$ dipole	1.64	$0.13\,\lambda^2$	$0.32\,\lambda$	78°
$\lambda/2$ 2-wire folded dipole	1.64	$0.13\,\lambda^2$	$0.64\,\lambda$	78°

of this topic, the reader is referred to the antenna literature, e.g. Rothammel (1981), Kraus (1988).

4.2.5.7 Yagi–Uda antenna

The *Yagi–Uda antenna*, named after its inventors, could well be the most important variant of a *directional antenna* in radio technology.

The antenna is an alignment array, made up of a driven emitter and a series of parasitic elements. A typical Yagi-Uda antenna is shown in Figure 4.68. Parasitic dipoles are arranged in front of the driven emitter (usually a dipole or 2-wire folded dipole) in the desired *direction of maximum radiation*. These parasitic dipoles function as *directors*, while a rod, usually a single rod, behind the exciter acts as a *reflector*. To create the directional transmission, the rods acting as directors must be shorter, and the rod acting as a reflector must be longer, than the exciter operating at resonance (Meinke and Gundlach, 1992). Compared to an isotropic emitter, gains of 9 dBi (based upon three elements) to 12 dB (based upon seven elements) can be achieved with a Yagi–Uda antenna. So-called 'long' Yagi antennas (10, 15 or more elements) can even achieve gains of up to 15 dBi in the main radiation direction.

Due to their size, Yagi–Uda antennas are used exclusively as antennas for readers. Like a torch, the Yagi–Uda antenna transmits in only one direction of maximum radiation, at a precisely known apex angle. Interference from adjacent devices or readers to the side can thus be suppressed and tuned out.

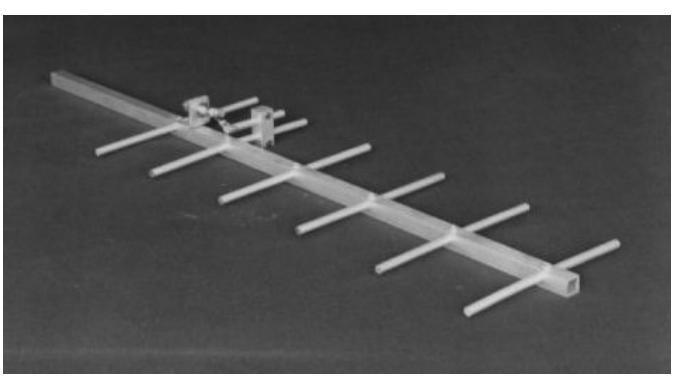


Figure 4.68 Typical design of a Yagi–Uda directional antenna (six elements), comprising a driven emitter (second transverse rod from left), a reflector (first transverse rod from left) and four directors (third to sixth transverse rods from left) (reproduced by permission of Trolleyscan, South Africa)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Due to the popularity of the Yagi–Uda antenna both as an antenna for radio and television reception and also in commercial radio technology, there is a huge amount of literature on the operation and construction of this antenna design. Therefore, we will not deal with this antenna in more detail at this point.

4.2.5.8 Patch or microstrip antenna

Patch antennas (also known as *microstrip* or *planar antennas*) can be found in many modern communication devices. For example, they are used in the latest generations of GPS receivers and mobile telephones, which are becoming smaller all the time. Thanks to their special construction format, patch antennas also offer some advantages for RFID systems.

In its simplest form, a patch antenna comprises a printed circuit board (e.g. Teflon or PTFE for higher frequencies) coated (i.e. metallised) on both sides, the underside of which forms a continuous ground (Kraus, 2000). On the top there is a small rectangle, which is supplied via a microstrip feed on one side, feeders through the base plate (see Figure 4.71) or capacitive coupling via an intermediate layer (aperture coupled patch antenna; see Kossel (n.d.), Fries and Kossel (n.d.)). Planar antennas can therefore be manufactured cheaply and with high levels of reproducibility using PCB etching technology (see Figures 4.69 and 4.70).

The length L_p of the patch determines the resonant frequency of the antenna. Under the condition $h_D \leq \lambda$:

$$L_P = \frac{\lambda}{2} - h_D \tag{4.93}$$

Normally the substrate thickness h_D is 1–2% of the wavelength.

The width w_p influences the resonant frequency of the antenna only slightly, but determines the *radiation resistance* R_r of the antenna (Krug, 1985). Where $w_p < \lambda/2$:

$$R_r = \frac{90}{\frac{\varepsilon_r + 1}{2} + (\varepsilon_r - 1)\sqrt{4 + \frac{48 \cdot h_p}{w_p}}} \cdot \left(\frac{\lambda}{w_p}\right)^2 \tag{4.94}$$

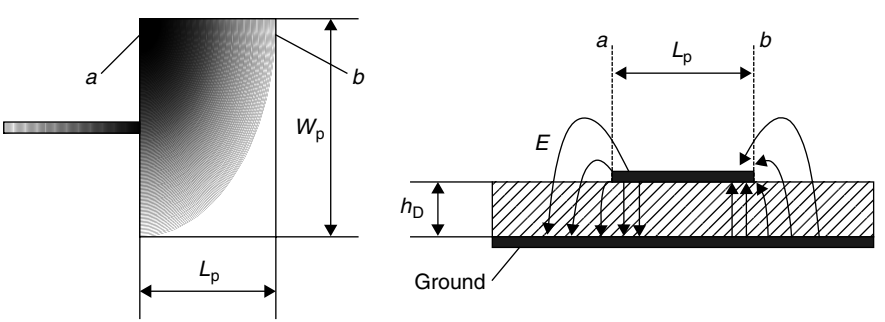


Figure 4.69 Fundamental layout of a patch antenna. The ratio of L_p to h_D is not shown to scale

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

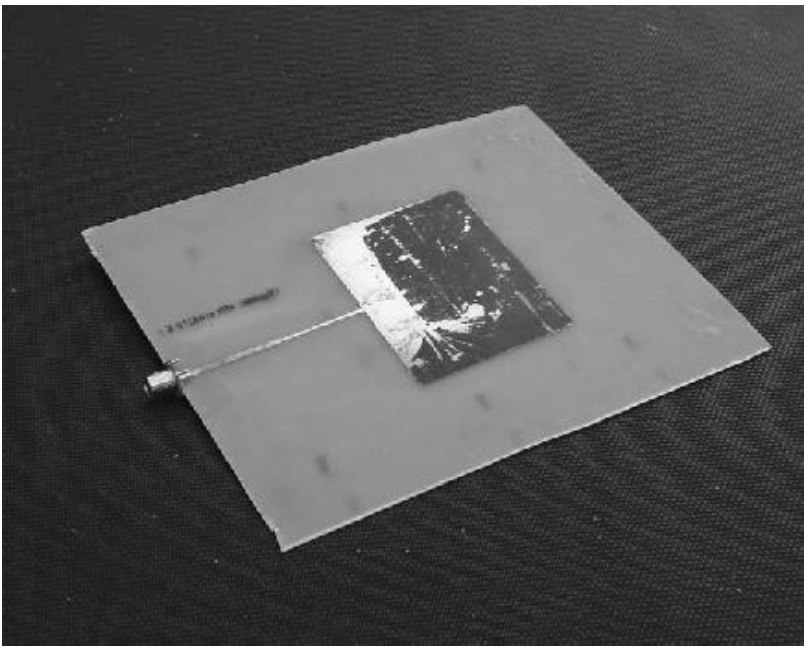


Figure 4.70 Practical layout of a patch antenna for 915 MHz on a printed circuit board made of epoxy resin (reproduced by permission of Trolleyscan, South Africa)

where $w_p > 3\lambda/2$:

$$R_r = \frac{120}{\frac{\varepsilon_r + 1}{2} + (\varepsilon_r - 1)\sqrt{4 + \frac{48 \cdot h_p}{w_p}}} \cdot \frac{\lambda}{w_p} \tag{4.95}$$

If the patch antenna is operated at its resonant frequency the phase difference between the patch edges a and b is precisely 180°. Figure 4.69 shows the path of the electrical field lines. At the entry and exit edges of the patch the field lines run in phase. The patch edges a and b thus behave like two in-phase fed slot antennas. The polarisation of the antenna is linear and parallel to the longitudinal edge L_p. See Figure 4.71.

Due to the type of power supply, patch antennas can also be used with *circular polarisation*. To generate circular polarisation, an emitter element must be supplied with signals with a phase angle of 90° at only two edges that are geometrically offset by 90°.

It is a relatively simple matter to amalgamate patch antennas to form *group antennas* (Figure 4.72). As a result, the gain increases in relation to that of an individual element. The layout shown in the figure comprises in-phase fed emitter elements. The approximately $\lambda/2$ long patch elements are fed via almost non-radiative line sections of around $\lambda/2$ in length connected in series, so that the transverse edges $a-a$ or $b-b$ of the patch element lie precisely wavelength λ apart. Thus the in-phase feed to the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

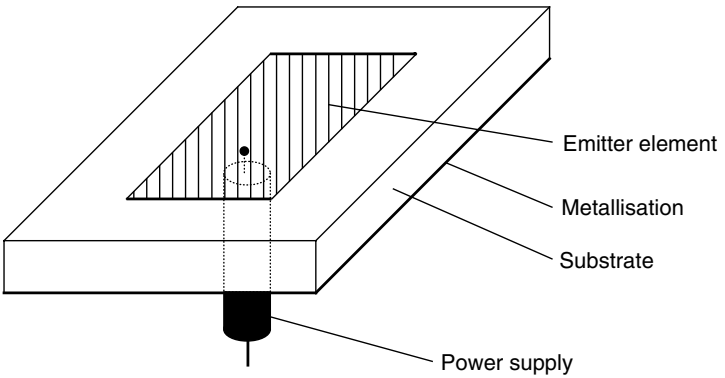


Figure 4.71 Supply of a $\lambda/2$ emitter quad of a patch antenna via the supply line on the reverse

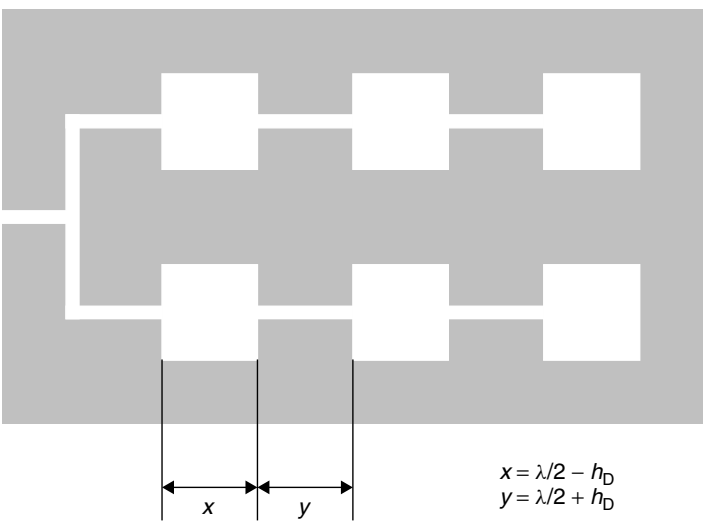


Figure 4.72 The interconnection of patch elements to form a group increases the directional effect and gain of the antenna

individual elements is guaranteed. The arrangement is polarised in the direction of the line sections.

4.2.5.9 Slot antennas

If we cut a strip of length $\lambda/2$ out of the centre of a large metal surface the slot can be used as an emitter (Rothammel, 1981). The width of the slot must be small in relation to its length. The base point of the emitter is located at the mid-point of its longitudinal side (Figure 4.73).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

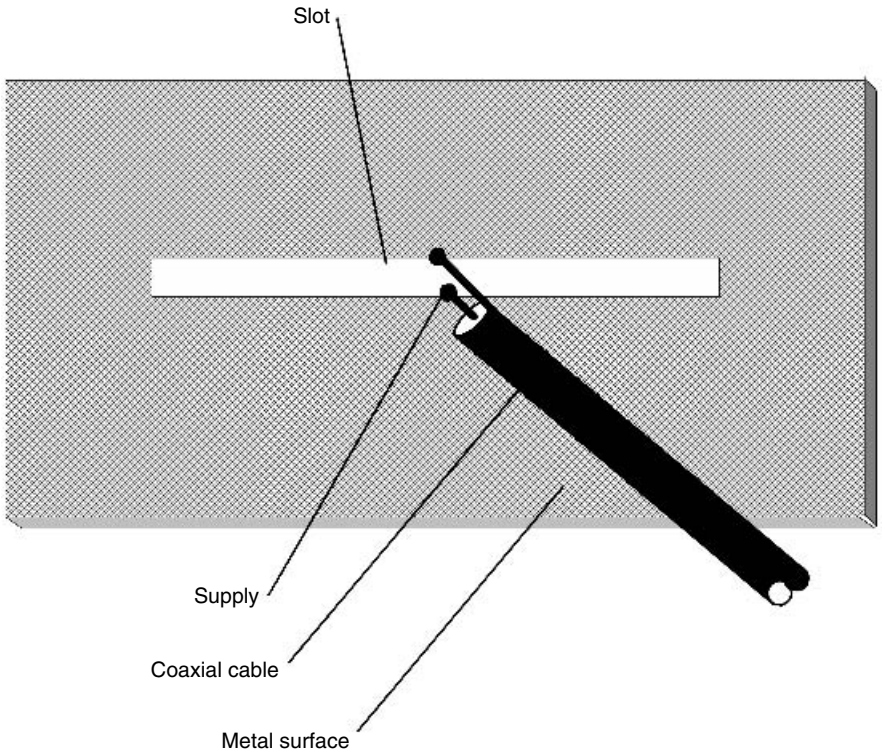


Figure 4.73 Layout of a slot antenna for the UHF and microwave range

4.2.6 Practical operation of microwave transponders

Let us now turn our attention to practical operation when a transponder is located in the *interrogation zone* of a reader. Figure 4.74 shows the simplified model of such a *backscatter system*. The reader emits an electromagnetic wave with the effective radiated power $P_1 \cdot G_1$ into the surrounding space. Of this, a transponder receives power $P_2 = P_e$, proportional to the field strength E, at distance r.

Power P_S is also reflected by the transponder's antenna, of which power P_3 is again received by the reader at distance r.

4.2.6.1 Equivalent circuits of the transponder

In the previous sections we have quoted the simplified equation for the impedance of the transformer $Z_T = R_T + jX_T$ (simplified equivalent circuit). In practice, however, the *input impedance* of a transponder can be represented more clearly in the form of the parallel circuit consisting of a *load resistor* R_L, an *input capacitor* C_2, and possibly a modulation impedance Z_{mod} (see also Section 4.2.6.6) (functional equivalent circuit).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

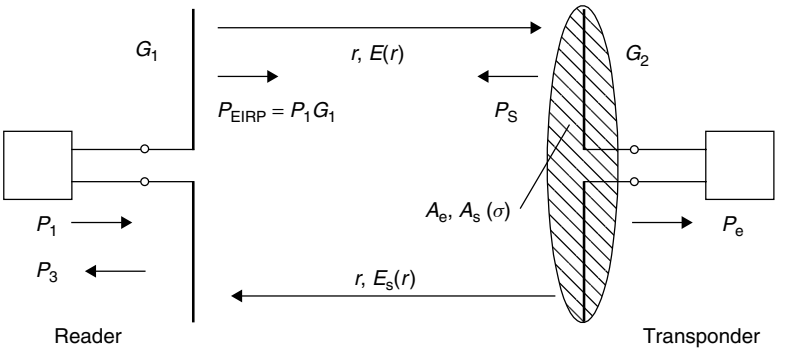


Figure 4.74 Model of a microwave RFID system when a transponder is located in the interrogation zone of a reader. The figure shows the flow of HF power throughout the entire system

It is relatively simple to make the conversion between the components of the two equivalent circuits. For example, the transponder impedance Z_T can be determined from the functional or the simplified equivalent circuit, as desired (Figure 4.75).

$$Z_T = jX_T + R_T = \frac{1}{j\omega C_2 + \dfrac{1}{R_L} + \dfrac{1}{Z_{mod}}} \tag{4.96}$$

The individual components R_T and X_T of the simplified equivalent circuit can also be simply determined from the components of the functional equivalent circuit. The following is true:

$$R_T = \mathrm{Re}\left(\frac{1}{j\omega C_2 + \dfrac{1}{R_L} + \dfrac{1}{Z_{mod}}} \right) \tag{4.97}$$

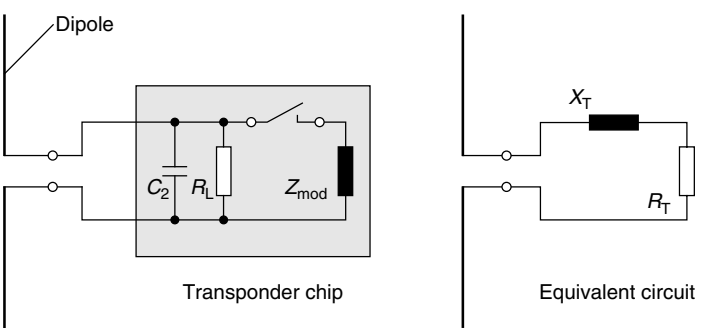


Figure 4.75 Functional equivalent circuit of the main circuit components of a microwave transponder (left) and the simplified equivalent circuit (right)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

$$X_T = \mathrm{Im}\left(\frac{1}{j\omega C_2 + \frac{1}{R_L} + \frac{1}{Z_{mod}}}\right) \tag{4.98}$$

4.2.6.2 Power supply of passive transponders

A passive transponder does not have its own *power supply* from an internal voltage source, such as a battery or solar cell. If the transponder is within range of the reader a voltage U_0 is induced in the transponder antenna by the field strength E that occurs at distance r. Part of this voltage is available at the terminals of the antenna as voltage U_T. Only this voltage U_T is rectified and is available to the transponder as supply voltage (rectenna) (Jurianto and Chia, n.d. a, b).

In the case of power matching between the radiation resistor R_r and the input impedance Z_T of the transponder, power $P_2 = P_e$ can be derived from equation (4.87). Figure 4.76 shows the power available in RFID systems at different distances at the

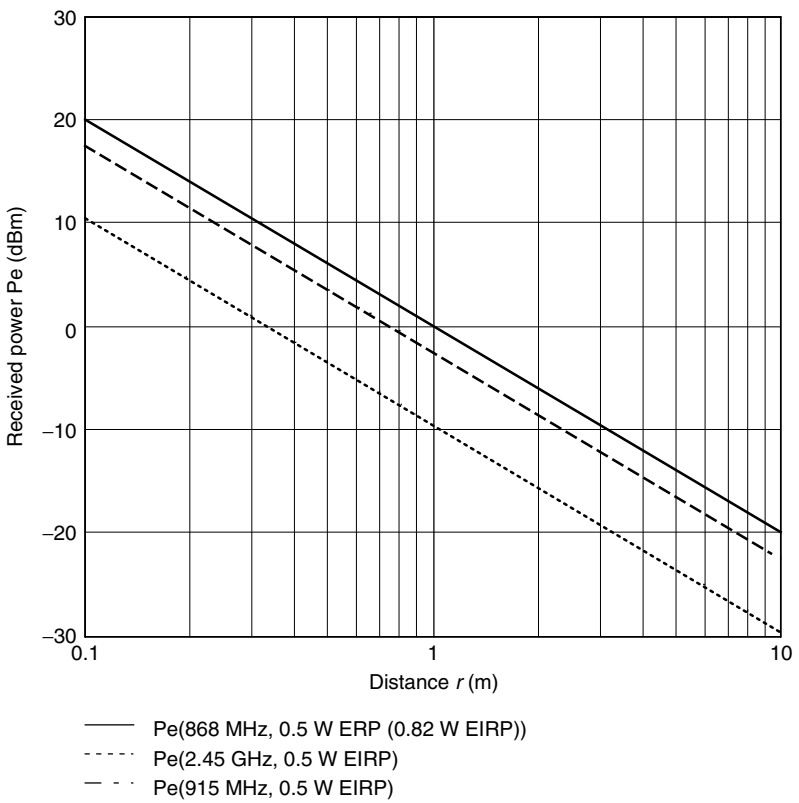


Figure 4.76 The maximum power $P_e(0\,\mathrm{dBm} = 1\,\mathrm{mW})$ available for the operation of the transponder, in the case of power matching at the distance r, using a dipole antenna at the transponder

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

reader's normal transmission power. In order to use this low power as effectively as possible a *Schottky detector* with *impedance matching* is typically used as a rectifier.

A *Schottky diode* consists of a metal–semiconductor sequence of layers. At the boundary layer there is, as in the p-n junction, a charge-free space-charge zone and a potential barrier that hinders charge transport. The current–voltage characteristic of the metal–semiconductor transition has a diode characteristic. Schottky diodes function as a rectifier at wavelengths below the microwave range since, unlike the pn diode, there are no inertia effects caused by minority carrier injection. Further advantages in comparison to pn diodes are the low voltage drop in the direction of flow and the low noise. A possible layout of a Schottky diode is shown in Figure 4.77 (Agilent Technologies, n.d.).

A Schottky diode can be represented by a linear *equivalent circuit* (Figure 4.77b). C_j represents the parasitic *junction capacitance* of the chip and R_s is the loss resistance in the terminals of the diode. R_j is the *junction resistor* of the diode, which can be calculated as follows (Agilent Technologies, n.d.):

$$R_j = \frac{8.33 \cdot 10^{-5} \cdot n \cdot T}{I_s + I_b} \tag{4.99}$$

where n is the ideality factor, T the temperature in Kelvin, I_s the saturation current and I_b the bias current through the Schottky diode.

By a suitable combination of the p- or n-doped semiconductor with the various metals the properties of the Schottky diode can be varied across a wide range. In RFID transponders primarily p-doped Schottky diodes are used, since these are particularly suitable for detectors with no zero bias in small signal operation, i.e. for the conditions that occur in every transponder (Hewlett Packard, 988).

The circuit of a Schottky detector for voltage rectification is shown in Figure 4.78. Such a Schottky detector has different operating ranges. If it is driven at power above −10 dBm (0.1 mW) the Schottky detector lies in the range of *linear detection* (Hewlett Packard, 986). Here there is *peak value rectification*, as is familiar from the field of power electronics. The following holds:

$$u_{chip} \sim \hat{u}_{in} \Rightarrow u_{chip} \sim \sqrt{P_{in}} \tag{4.100}$$

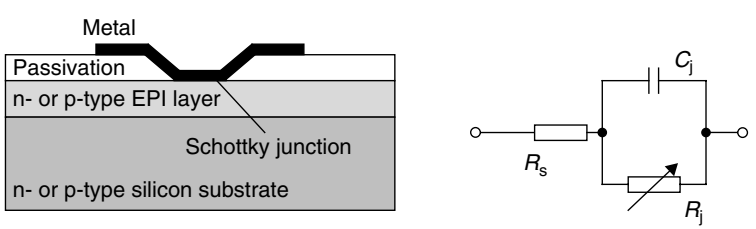
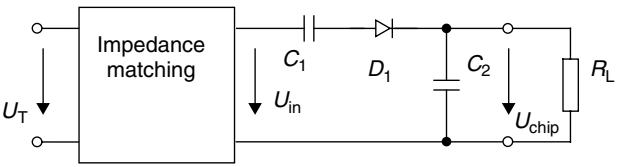
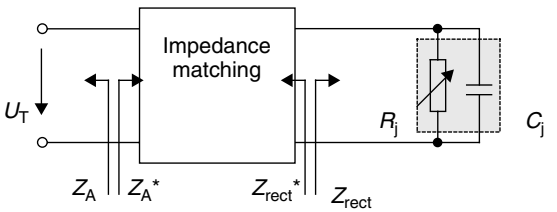


Figure 4.77 A Schottky diode is created by a metal–semiconductor junction. In small signal operation a Schottky diode can be represented by a linear equivalent circuit

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



(a) Practical circuit: voltage doubler with impedance matching



(b) AC equivalent circuit

Figure 4.78 (a) Circuit of a Schottky detector with impedance transformation for power matching at the voltage source and (b) the HF equivalent circuit of the Schottky detector

In the case of operation at powers below $-20\,\mathrm{dBm}$ ($10\,\mu\mathrm{W}$) the detector is in the range of square law detection. The following holds (Hewlett Packard, 986):

$$u_{\mathrm{chip}} \sim \hat{u}_{\mathrm{in}}^2 \Rightarrow u_{\mathrm{chip}} \sim P_{\mathrm{in}} \tag{4.101}$$

Schottky detectors in RFID transponders operate in the range of *square law detection* at greater distances from the reader, but also in the transition range to linear detection at smaller distances (Figure 4.79).

The relationship between the input power and output voltage of a Schottky detector can be expressed using a Bessel function of the zeroth order (Hewlett Packard, 1088):

$$I0\left(\frac{\Lambda}{n}\sqrt{8R_{\mathrm{g}}\cdot P_{\mathrm{in}}}\right) = \left(1+\frac{I_{\mathrm{b}}}{I_{\mathrm{s}}}+\frac{u_{\mathrm{chip}}}{R_{\mathrm{L}}\cdot I_{\mathrm{s}}}\right)\cdot \mathrm{e}^{\left[\left(1+\frac{R_{\mathrm{g}}+R_{\mathrm{s}}}{R_{\mathrm{L}}}\right)\cdot\frac{\Lambda\cdot u_{\mathrm{chip}}}{n}+\frac{\Lambda\cdot R_{\mathrm{s}}\cdot I_{\mathrm{b}}}{n}\right]} \tag{4.102}$$

Where $\Lambda = q/(k\cdot T)$, q is the elementary charge, k is the Boltzmann constant, T is the temperature of the diode in Kelvin, R_{g} is the internal resistance of the voltage source (in transponders this is the *radiation resistance* R_{r} of the antenna), P_{in} is the supplied power, R_{L} is the connected load resistor (transponder chip) and u_{chip} is the output voltage (supply voltage of the transponder chip).

By numerical iteration using a program such as Mathcad (n.d.) this equation can easily be solved, yielding a diagram $u_{\mathrm{chip}}(P_{\mathrm{in}})$ (see Figure 4.81). The transition from square law detection to linear law detection at around -20 ($10\,\mu\mathrm{W}$) to $-10\,\mathrm{dBM}$ ($0.1\,\mathrm{mW}$) input power is clearly visible in this figure.

Evaluating equation (4.102), we see that a higher saturation current I_{s} leads to good sensitivity in the square law detection range. However, in the range that is of interest for RFID transponders, with output voltages u_{chip} of 0.8–3 V, this effect is unfortunately no longer marked.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

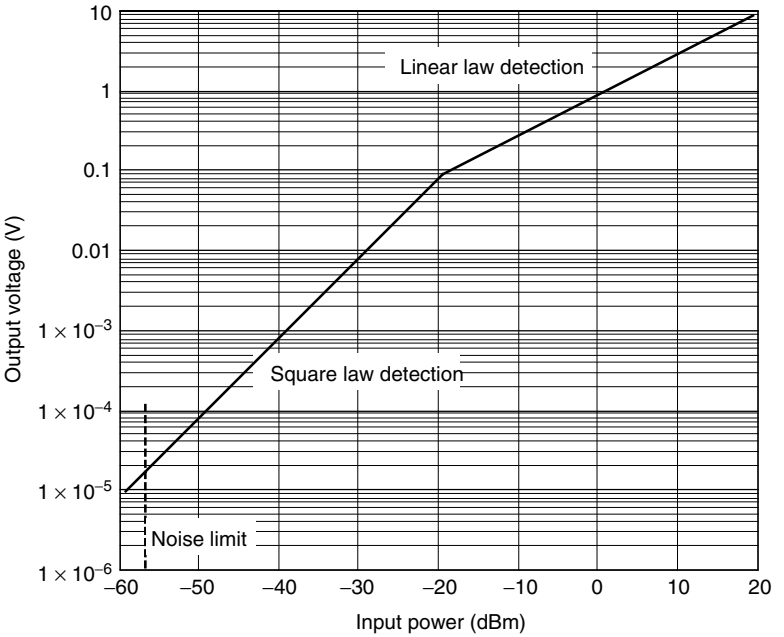


Figure 4.79 When operated at powers below −20 dBm (10 μW) the Schottky diode is in the square law range

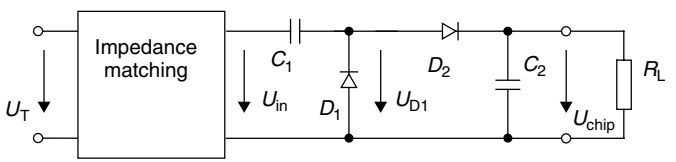


Figure 4.80 Circuit of a Schottky detector in a voltage doubler circuit (villard-rectifier)

In order to further increase the output voltage, *voltage doublers* (Hewlett Packard, 956-4) are used. The circuit of a voltage doubler is shown in Figure 4.80. The output voltage u_{chip} at constant input power P_{in} is almost doubled in comparison to the single Schottky detector (Figure 4.81). The Bessel function (equation (4.102)) can also be used for the calculation of the relationship of P_{in} to u_{chip} in voltage doublers. However, the value used for R_g should be doubled, the value R_L should be halved, and the calculated values for the output voltage u_{chip} should also be doubled (Figure 4.81).

The influence of various operating frequencies on the output voltage is not taken into account in equation (4.102). In practice, however, a frequency-dependent current flows through the parasitic capacitor C_j, which has a detrimental effect upon the efficiency of the Schottky detector. The influence of the junction capacitance on the output voltage can be expressed by a factor M (Hewlett Packard, 1088). The following holds:

$$M = \frac{1}{1 + \omega^2 C_j^2 R_s R_j} \tag{4.103}$$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

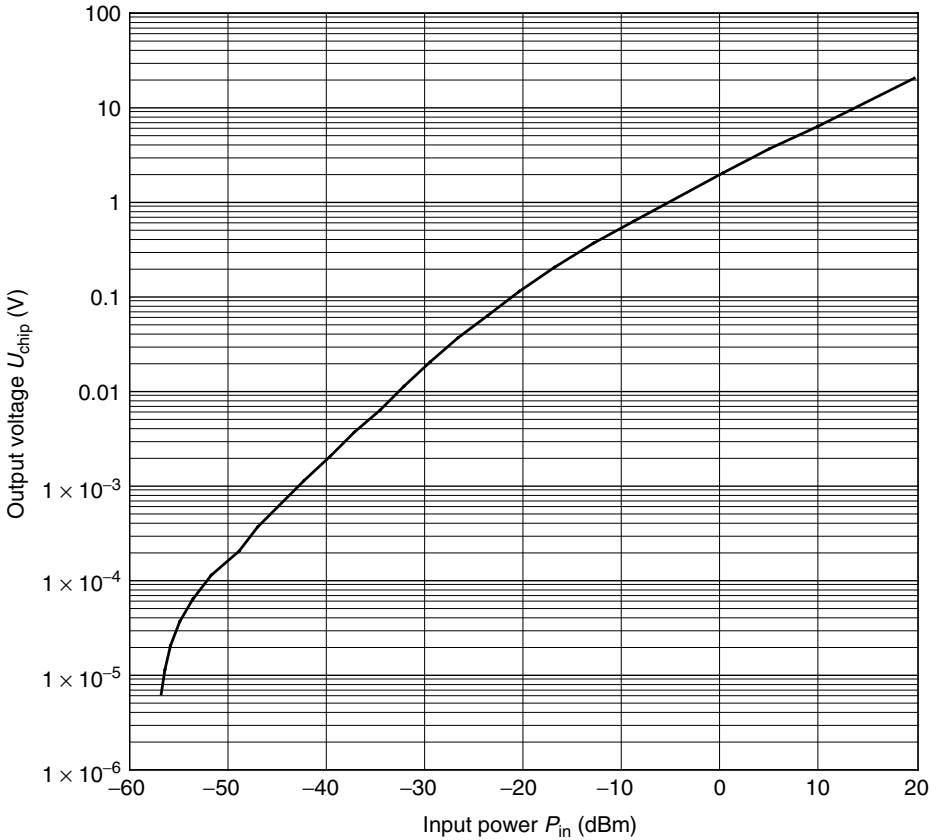


Figure 4.81 Output voltage of a Schottky detector in a voltage doubler circuit. In the input power range −20 to −10 dBm the transition from square law to linear law detection can be clearly seen ($R_L = 500\,k\Omega$, $I_s = 2\,\mu A$, $n = 1.12$)

However, in the range that is of interest for RFID transponders at output voltages u_{chip} 0.8–3 V and the resulting junction resistances R_j in the range <250 Ω (Hewlett Packard, 1088) the influence of the junction capacitance can largely be disregarded (Figure 4.82; see also Figure 4.81).

In order to utilise the received power P_e as effectively as possible, the input impedance Z_{rect} of the Schottky detector would have to represent the complex conjugate of the antenna impedance Z_A (voltage source), i.e. $Z_{rect} = Z_A^*$. If this condition is not fulfilled, then only part of the power is available to the Schottky detector, as a glance at Figure 4.65 makes unmistakably clear.

The HF equivalent circuit of a Schottky detector is shown in Figure 4.78. It is the job of the capacitor C_2 to filter out all HF components of the generated direct voltage and it is therefore dimensioned such that X_{C2} tends towards zero at the transmission frequency of the reader. In this frequency range the diode (or the equivalent circuit of the diode) thus appears to lie directly parallel to the input of the circuit. The load resistor R_L is short-circuited by the capacitor C_2 for the HF voltages and is thus not present in the HF equivalent circuit. R_L, however, determines the current I_L through

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

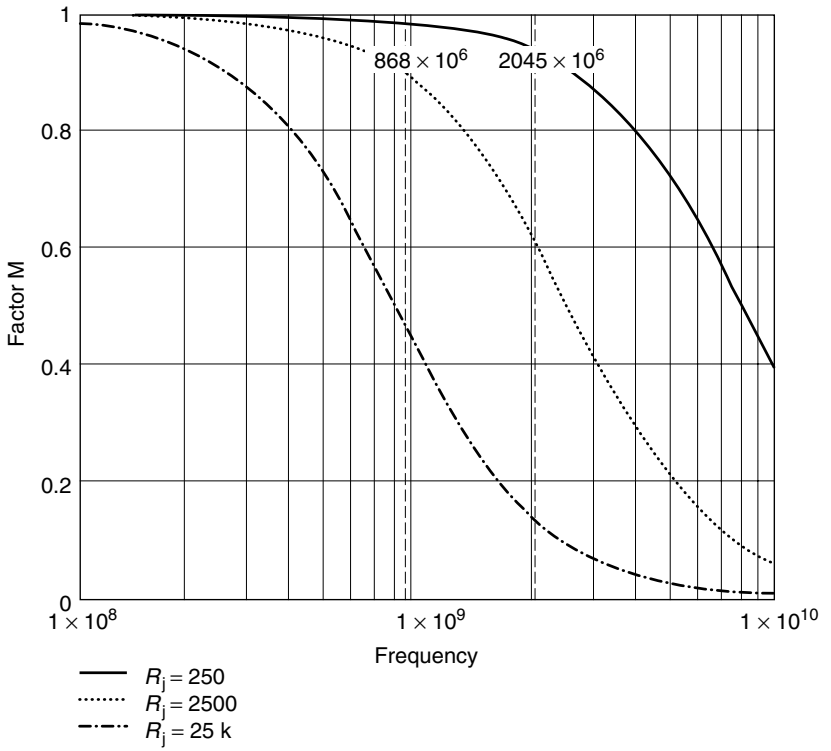


Figure 4.82 The factor M describes the influence of the parasitic junction capacitance C_j upon the output voltage u_{chip} at different frequencies. As the junction resistance R_j falls, the influence of the junction capacitance C_j also declines markedly. Markers at 868 MHz and 2.45 GHz

the Schottky detector and thus also the junction resistance R_j of the Schottky diode. The HF equivalent circuit of a voltage doubler correspondingly consists of the parallel connection of two Schottky diodes.

In order to now achieve the required power matching between the antenna and the Schottky detector, the input impedance Z_{rect} of the Schottky detector must be matched by means of a circuit for the impedance matching at the antenna impedance Z_A. In HF technology, discrete components, i.e. L and C, but also line sections of differing impedances (line transformation), can be used for this.

At ideal matching, the voltage sensitivity $\gamma 2xs$ (in mV/μW) of a Schottky detector can be simply calculated (Figure 4.83; Hewlett Packard, 963, 1089):

$$\gamma^2 = \frac{0.52}{(I_s + I_b) \cdot (1 + \varpi^2 C_j^2 R_s R_j) \cdot \left(1 + \frac{R_j}{R_L}\right)} \tag{4.104}$$

The theoretical maximum of $\gamma 2$ lies at 200 mV/μW (868 MHz) for a Schottky diode of type HSM 2801, and occurs at a total diode current $I_T = I_s + I_b$ of 0.65 μA. The saturation current I_s of the selected Schottky diode is, however, as low as 2 μA, which means that in theory this voltage sensitivity is completely out of reach even.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

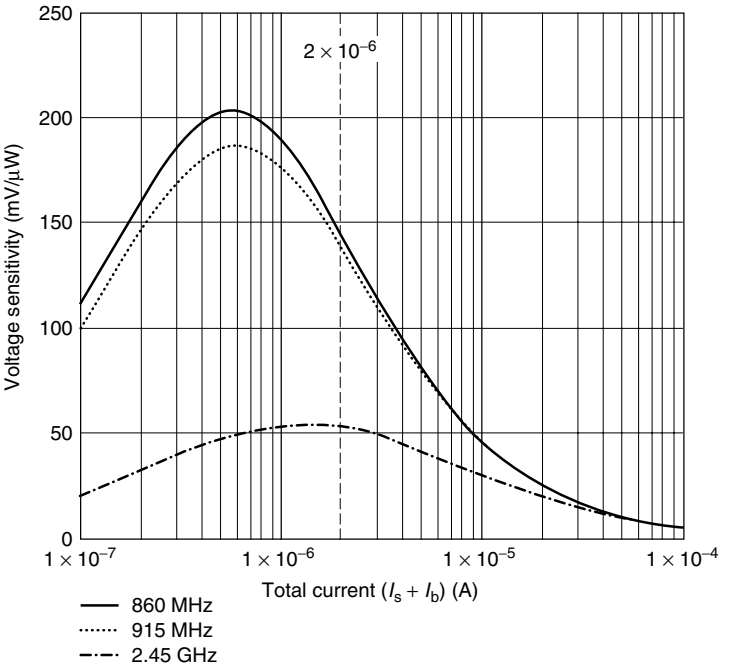


Figure 4.83 Voltage sensitivity $\gamma 2$ of a Schottky detector in relation to the total current $I_T \cdot C_j = 0.25\,\text{pF},\ R_s = 25\,\Omega,\ R_L = 100\,\text{k}\Omega$

at an operating current $I_b = 0$. Additionally, the junction resistance $R_j = 40\,\text{k}\Omega$ that results at $I_T = 0.65\,\mu\text{A}$ can hardly be approximately transformed without loss using real components at the low-ohmic source impedance of the antenna $Z_A = 73\,\Omega + j0\,\Omega$. Finally, the influence of the parasitic junction capacitance C_j at such high-ohmic junction resistances is clearly visible, and shows itself in a further reduction in the voltage sensitivity, particularly at 2.45 GHz.

In practice, Schottky detectors are operated at currents of 2.5–25 μA, which leads to a significantly lower junction resistance. In practice, values around 50 mV/μW can be assumed for voltage sensitivity (Hewlett Packard, 1089).

Due to the influencing parameters described above it is a great challenge for the designer designing a Schottky detector for an RFID transponder to select a suitable Schottky diode for the operating case in question and to set all operating parameters such that the voltage sensitivity of the Schottky detector is as high as possible.

Let us finally consider another example of the *matching* of a Schottky voltage doubler to a dipole antenna. Based upon two Schottky diodes connected in parallel in the HF equivalent circuit ($L_p = 2\,\text{nH},\ C_p = 0.08\,\text{pF},\ R_s = 20\,\Omega,\ C_j = 0.16\,\text{pF},\ I_T = 3\,\mu\text{A},\ R_j = 8.6\,\text{k}\Omega$) we obtain an impedance $Z_{rect} = 37 - \text{j}374\,\Omega\,(|Z_{rect}| = 375\,\Omega)$. The Smith diagram in Figure 4.84 shows a possible transformation route, plus the values and sequence of the components used in this example that would be necessary to perform a matching to 72 Ω (dipole in resonance).

It is not always sensible or desirable to perform *impedance matching* between transponder chip and antenna by means of discrete components. Particularly in the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

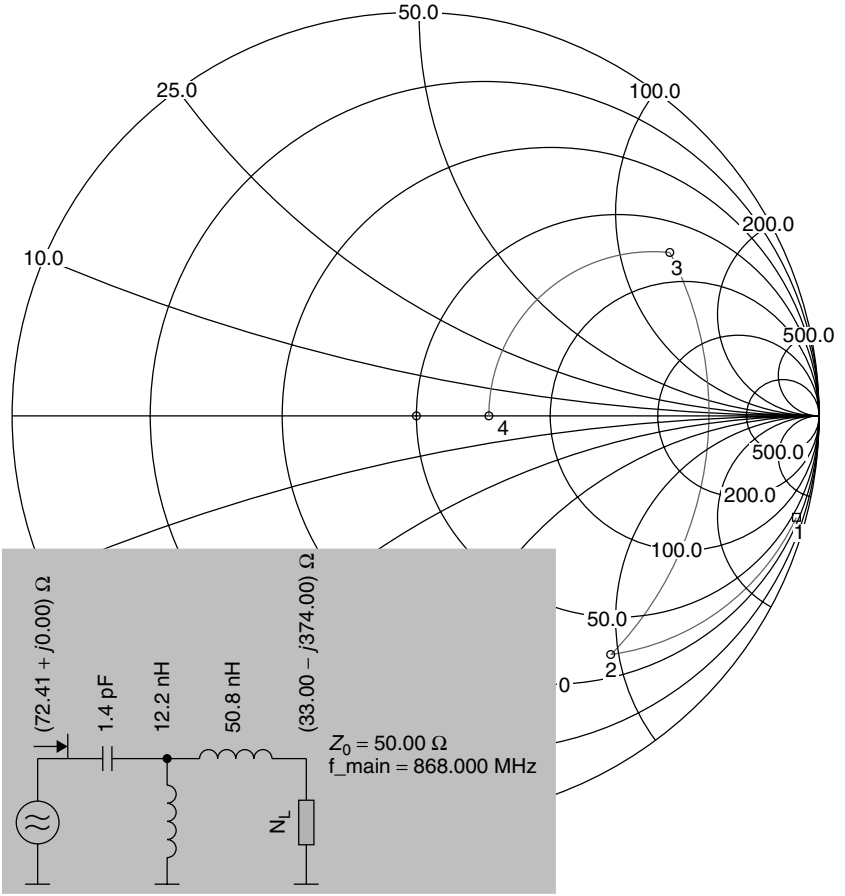


Figure 4.84 Matching of a Schottky detector (point 1) to a dipole antenna (point 4) by means of the series connection of a coil (point 1–2), the parallel connection of a second coil (point 2–3), and finally the series connection of a capacitor (point 3–4)

case of labels, in which the transponder chip is mounted directly upon foil, additional components are avoided where possible.

If the elements of a dipole are shortened or lengthened (i.e. operated at above or below their resonant frequency), then the impedance Z_A of the antenna contains an inductive or capacitive component $X_T \neq 0$. Furthermore, the radiation resistance R_s can be altered by the construction format. By a suitable antenna design it is thus possible to set the input impedance of the antenna to be the complex conjugate of the input impedance of the transponder, i.e. $Z_T = Z_A^*$ (Figure 4.85). The power matching between transponder chip and antenna is thereby only realised by the antenna.

4.2.6.3 Power supply of active transponders

In active transponders the power supply of the semiconductor chip is provided by a *battery*. Regardless of the distance between transponder and reader the voltage is

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

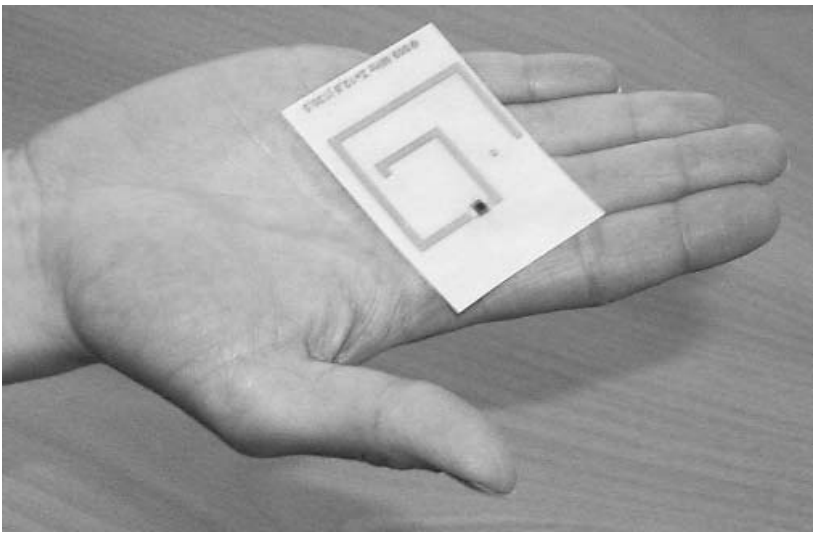


Figure 4.85 By suitable design of the transponder antenna the impedance of the antenna can be designed to be the complex conjugate of the input impedance of the transponder chip (reproduced by permission of Rafsec, Palomar-Konsortium, PALOMAR-Transponder)

always high enough to operate the circuit. The voltage supplied by the antenna is used to activate the transponder by means of a detection circuit. In the absence of external activation the transponder is switched into a power saving mode in order to save the battery from unnecessary discharge.

Depending upon the type of evaluation circuit a much lower received power P_e is needed to activate the transponder than is the case for a comparable passive transponder. Thus the read range is greater compared to a passive transponder. In practice, ranges of over 10 m are normal.

4.2.6.4 Reflection and cancellation

The electromagnetic field emitted by the reader is not only reflected by a transponder, but also by all objects in the vicinity, the spatial dimension of which is greater than the wavelength λ_o of the field (see also Section 4.2.4.1). The reflected fields are superimposed upon the primary field emitted by the reader. This leads alternately to a local damping or even so-called *cancellation* (antiphase superposition) and an amplification (in-phase superposition) of the field at intervals of $\lambda_0/2$ between the individual minima. The simultaneous occurrence of many individual reflections of varying intensity at different distances from the reader leads to a very erratic path of field strength E around the reader, with many local zones of cancellation of the field. Such effects should be expected particularly in an environment containing large metal objects, e.g. in an industrial operation (machines, metal pipes etc.).

We are all familiar with the effect of *reflection* and cancellation in our daily lives. In built-up areas it is not unusual to find that when you stop your car at traffic lights you are in a 'radio gap' (i.e. a local cancellation) and instead of your favourite radio station

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

all you can hear from the radio is noise. Experience shows that it is generally sufficient to roll the car forward just a short way, thus leaving the area of local cancellation, in order to restore the reception.

In RFID systems these effects are much more disruptive, since a transponder at a local field strength minimum may not have enough power at its disposal for operation. Figure 4.86 shows the results of the measurement of the reader's field strength E at an increasing distance from the transmission antenna when reflections occur in close proximity to the reader.

4.2.6.5 Sensitivity of the transponder

Regardless of the type of power supply of the transponder a minimum *field strength* E is necessary to activate the transponder or supply it with sufficient energy for the operation of the circuit. The minimum field strength is called the *interrogation field strength* $E_{\min}$ and is simple to calculate. Based upon the minimum required HF input power $P_{\text{e-min}}$ of the *Schottky detector* and of the transponder antenna gain G we find:

$$E_{\min} = \sqrt{\frac{4\pi \cdot Z_{\text{F}} \cdot P_{\text{e-min}}}{\lambda_0^2 \cdot G}} \tag{4.105}$$

This is based upon the prerequisite that the *polarisation directions* of the reader and transponder antennas precisely correspond. If the transponder is irradiated with a field that has a different polarisation direction, then $E_{\min}$ increases accordingly.

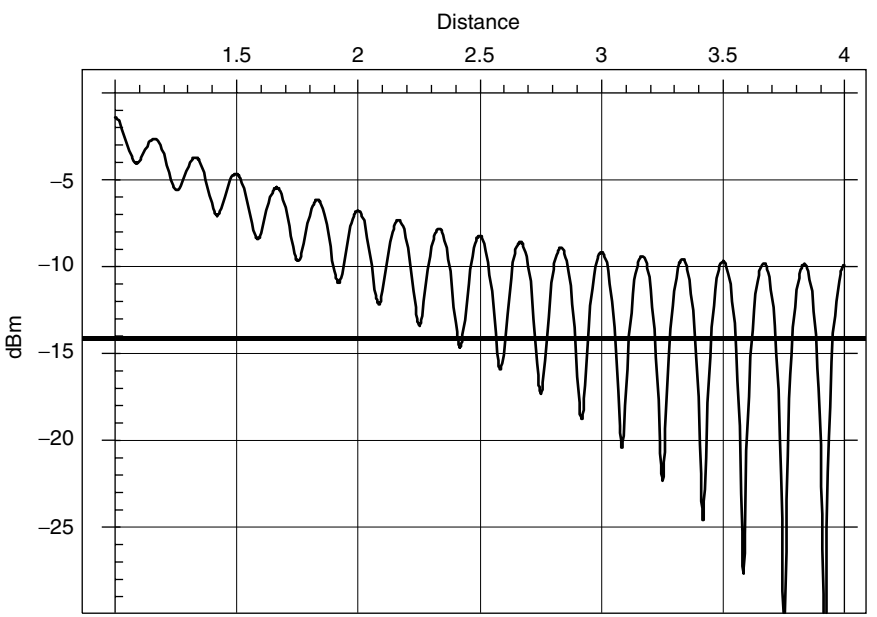


Figure 4.86 The superposition of the field originally emitted with reflections from the environment leads to local cancellations. x axis, distance from reader antenna; y axis, path attenuation in decibels (reproduced by permission of Rafsec, Palomar-Konsortium)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

4.2.6.6 Modulated backscatter

As we have already seen, the transponder antenna reflects part of the irradiated power at the *scatter aperture* σ (A_s) of the *transponder antenna*. In this manner, a small part of the power P_1 that was originally emitted by the reader returns to the reader via the transponder as received power P_3.

The dependence of the scatter aperture σ on the relationship between Z_T and Z_A established in Section 4.2.5.4 is used in RFID transponders to send data from the transponder to the reader. To achieve this, the input impedance Z_T of the transponder is altered in time with the data stream to be transmitted by the switching on and off of an additional impedance Z_{mod} in time with the data stream to be transmitted. As a result, the scatter aperture σ, and thus the power P_S reflected by the transponder, is changed in time with the data, i.e. it is modulated. This procedure is therefore also known as *modulated backscatter* or *σ-modulation* (Figure 4.87).

In order to investigate the relationships in a RFID transponder more precisely, let us now refer back to equation (4.82), since this equation expresses the influence of the transponder impedance $Z_T = R_T + X_T$ on the scatter aperture σ. In order to replace U_0^2 by the general properties of the transponder antenna we first substitute equation (4.90) into equation (4.88) and obtain:

$$U_0 = \lambda_0 \cdot \sqrt{\frac{G \cdot R_r}{\pi \cdot Z_F}} \cdot \sqrt{S \cdot Z_F} = \lambda_0 \cdot \sqrt{\frac{G \cdot R_r \cdot S}{\pi}} \tag{4.106}$$

We now replace U_0 in equation (4.82) by the right-hand expression in equation (4.106) and finally obtain (PALOMAR, 18000):

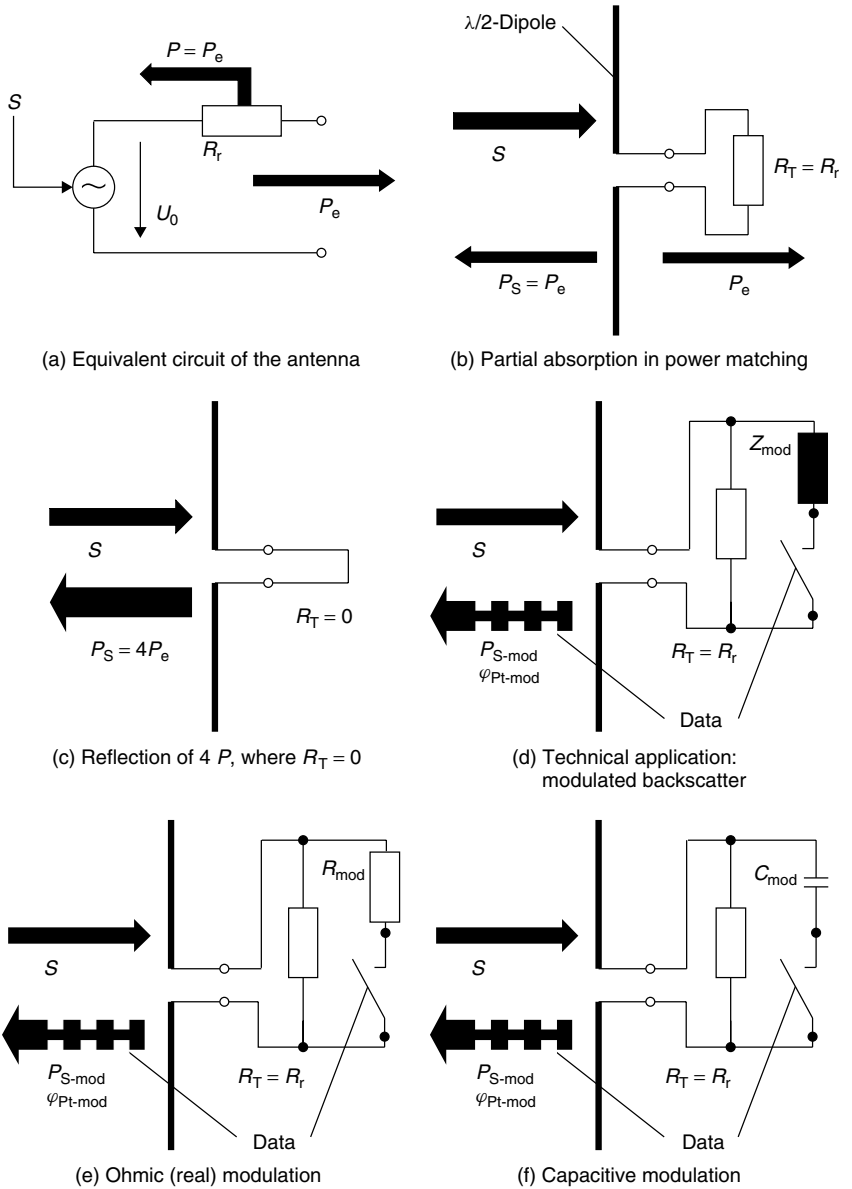
$$\sigma = \frac{{\lambda_0}^2 \cdot R_r^2 \cdot G}{\pi \cdot [(R_r + R_V + R_T)^2 + (X_A + X_T)^2]} \tag{4.107}$$

where G is the gain of the transponder antenna.

However, a drawback of this equation is that it only expresses the value of the scatter aperture σ (PALOMAR, 18000). If, for the clarification of the resulting problems, we imagine a transponder, for which the imaginary component of the input impedance Z_T in unmodulated state takes the value $X_{Toff} = -X_A + \Delta X_{mod}$, but in the modulated state (modulation impedance Z_{mod} connected in parallel) it is $X_{Ton} = -X_A - \Delta X_{mod}$. We further assume that the real component R_T of the input impedance Z_T is not influenced by the modulation. For this special case the imaginary part of the impedance during modulation between the values $(+\Delta X_{mod})^2$ and $(-\Delta X_{mod})^2$ is switched. As can be clearly seen, the value of the scatter aperture σ remains constant. Equation (4.81), on the other hand, shows that the reflected power P_S is proportional to the square of the current I in the antenna. However, since by switching the imaginary part of the impedances between $-\Delta X_{mod}$ and $+\Delta X_{mod}$ we also change the phase θ of the current I, we can conclude that the phase θ of the reflected power P_S also changes to the same degree.

To sum up, therefore, we can say that modulating the input impedance Z_T of the transponder results in the modulation of the value and/or phase of the reflected power P_S and thus also of the scatter aperture σ. P_S and σ should thus not be considered

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



(a) Equivalent circuit of the antenna

(b) Partial absorption in power matching

(c) Reflection of 4 P, where $R_T = 0$

(d) Technical application: modulated backscatter

(e) Ohmic (real) modulation

(f) Capacitive modulation

Figure 4.87 Generation of the modulated backscatter by the modulation of the transponder impedance $Z_T(= R_T)$

as real quantities in RFID systems, but as complex quantities. The relative change in value and phase of the scatter aperture σ can be expressed using the following equation (PALOMAR, 18000):

$$\Delta\sigma = \frac{\lambda_0^2 \cdot G \cdot \Delta Z_{\text{mod}}}{4 \cdot \pi \cdot R_r} \tag{4.108}$$

HANSHOW-EX. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

RFID transponders' property of generating mixed phase and amplitude modulation must also be taken into account in the development of readers. Modern readers thus often operate using I/Q demodulators in order to ensure that the transponder's signal can always be demodulated. See Figure 4.88.

4.2.6.7 Read range

Two conditions must be fulfilled for a reader to be able to communicate with a transponder.

First, the transponder must be supplied with sufficient power for its activation. We have already discussed the conditions for this in Section 4.2.6.2. Furthermore, the signal reflected by the transponder must still be sufficiently strong when it reaches the reader for it to be able to be detected without errors. The *sensitivity of a receiver* indicates how great the field strength or the induced voltage U must be at the receiver input for a signal to be received without errors. The level of *noise* that travels through the antenna and the primary stage of the receiver input, interfering with signals that are too weak or suppressing them altogether, is decisive for the sensitivity of a receiver.

In backscatter readers the permanently switched on transmitter, which is required for the activation of the transponder, induces a significant amount of additional noise, thereby drastically reducing the sensitivity of the receiver in the reader. This noise arises largely as a result of *phase noise* of the *oscillator* in the transmitter. As a rule of thumb in practice we can assume that for the transponder to be detected, the transponder's signal may lie no more than 100 dB below the level of the transmitter's

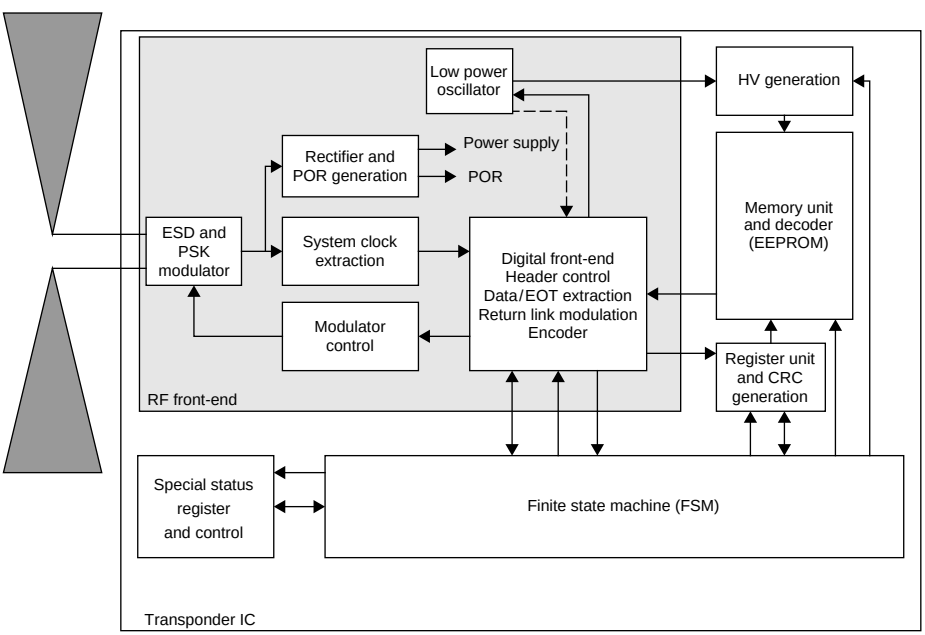


Figure 4.88 Block diagram of a passive UHF transponder (reproduced by permission of Rafsec, Palomar-Konsortium, PALOMAR Transponder)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

carrier signal (GTAG, 2001). In order to make a precise prediction regarding the sensitivity of a reader, however, this value must be established for the individual case by measurement.

For the transmission of data the signal reflected by the transponder is modulated. It should be noted in this connection that as part of the process of *modulation* the reflected power P_S is broken down into a reflected 'carrier signal' and two sidebands. In pure ASK modulation with a theoretical modulation index of 100%[6] the two sidebands would each contain 25% of the total reflected power P_S (i.e. P_3 — 6 dB), and at a lower modulation index correspondingly less. Since the information is transmitted exclusively in the *sidebands*, a lower wanted signal should be specified according to the modulation index. The reflected carrier contains no information, but cannot be received by the reader since it is completely masked by a transmission signal of the same frequency, as Figure 4.89 shows.

Let us now consider the magnitude of the power P_3 arriving at the reader that is reflected by the transponder.

As in equation (4.75) the received power P_3 at the receiver of the reader is:

$$P_3 = A_{e\cdot Reader} \cdot S_{Back} \tag{4.109}$$

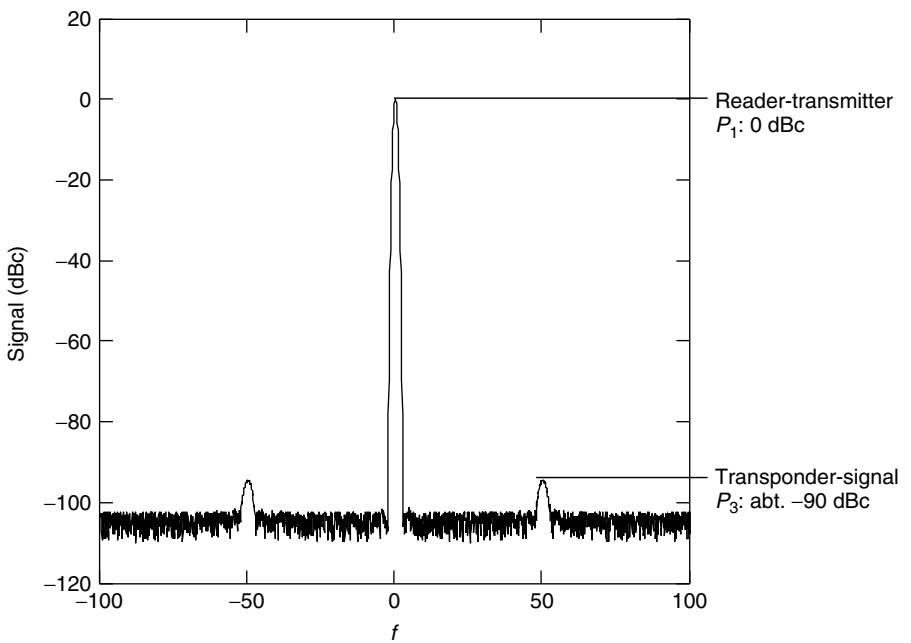


Figure 4.89 Example of the level relationships in a reader. The noise level at the receiver of the reader lies around 100 dB below the signal of the carrier. The modulation sidebands of the transponder can clearly be seen. The reflected carrier signal cannot be seen, since the level of the carrier signal of the reader's transmitter, which is the same frequency, is higher by orders of magnitude

[6] In practice 100% ASK modulation of the reflected signal cannot be achieved, since Z_T would have to have an infinite value in the modulated state.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The radiation density S_{Back} is found from equation (4.67). We thus obtain:

$$P_3 = A_{\text{e-Reader}} \cdot \frac{P_1 \cdot G_{\text{Reader}} \cdot \sigma}{(4\pi)^2 \cdot r^4} \tag{4.110}$$

We now replace $A_{\text{e-Reader}}$ by the expression in equation (4.86), since we have already used the gain G_{Reader} of the reader's antenna in the radar equation:

$$P_3 = \frac{P_1 \cdot G_{\text{Reader}}^2 \cdot \lambda_0^2 \cdot \sigma}{(4\pi)^3 \cdot r^4} \tag{4.111}$$

In the same way we replace $A_s = \sigma$ by equation (4.86), and thus finally obtain:

$$P_3 = \frac{P_1 \cdot G_{\text{Reader}}^2 \cdot \lambda_0^4 \cdot G_T^2}{(4\pi r)^4} \tag{4.112}$$

This equation naturally only applies in the case of power matching between the transponder's antenna and the connected consumer Z_T. In practical operation the scatter aperture σ can take on values between 0 and $4A_e$, as was shown in Section 4.2.5.4. In generalised form the following applies:

$$P_3 = \left. \frac{k \cdot P_1 \cdot G_{\text{Reader}}^2 \cdot \lambda_0^4 \cdot G_T^2}{(4\pi r)^4} \right|_{k=0..4} \tag{4.113}$$

The precise value for k is found from the relationship between the radiation resistance of the antenna R_r and the input impedance Z_T of the transponder chip and can be derived from Figure 4.65.

We solve equation (4.113) with respect to r, obtaining:

$$r = \frac{\lambda_0}{4\pi} \cdot \left. \sqrt[4]{\frac{k \cdot P_1 \cdot G_{\text{Reader}}^2 \cdot G_T^2}{P_3}} \right|_{k=0..4} \tag{4.114}$$

At known sensitivity of the reader's receiver $P_{3\,\min}$ the maximum distance between transponder and reader at which the transponder's signal can just be received by the reader can thus be calculated (Figure 4.90). The fact that P_3 represents the total power reflected by the transponder must be taken into account. The splitting of power P_3 into a carrier signal and the two sidebands (i.e. $P_3 = P_{\text{carrier}} + P_{\text{USB}} + P_{\text{LSB}}$)[7] has not yet been taken into account here. In order to be able to detect a single sideband of the reflected, modulated signal, P_3 must be correspondingly greater.

[7] USB = upper sideband, i.e. the modulation sideband at the higher frequency position; LSB = lower sideband, i.e. the modulation sideband at the lower frequency position.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

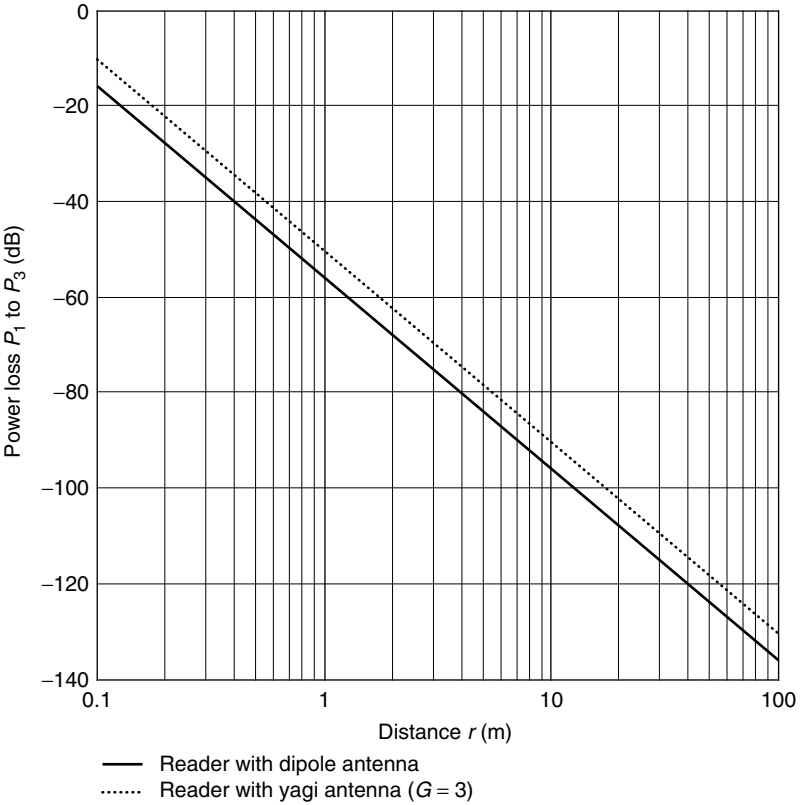


Figure 4.90 Damping of a signal on the way to and from the transponder

4.3 Surface Waves

4.3.1 The creation of a surface wave

If a voltage is applied to the electrodes of a *piezoelectric crystal* such as *quartz* (SiO_2), *lithium niobate* ($LiNbO_3$) or *lithium tantalate* ($LiTaO_3$) mechanical distortions arise in the *crystal lattice* as a result of the *piezoeffect*. This effect is used to generate *surface acoustic waves* on the crystal. To achieve this, electrode structures made of approximately 0.1 μm thick aluminium are applied to the polished surface of a piezoelectric single crystal in the form of an electroacoustic converter. When an alternating voltage is applied to the electroacoustic converter, surface acoustic waves — so-called *Rayleigh waves* — propagate on the surface of the crystal (Meinke and Gundlach, 1992). The deflections in the crystal lattice decrease exponentially as the depth increases.

The majority of the induced acoustic power is thus concentrated within a thin layer with a depth of approximately one wavelength λ on the surface of the crystal. The propagation of a surface acoustic wave on the highly polished surface of a substrate is almost undamped and dispersion free. The propagation speed v is approximately 3000 to 4000 m/s, i.e. only around 1/100 000 of the speed of light c.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

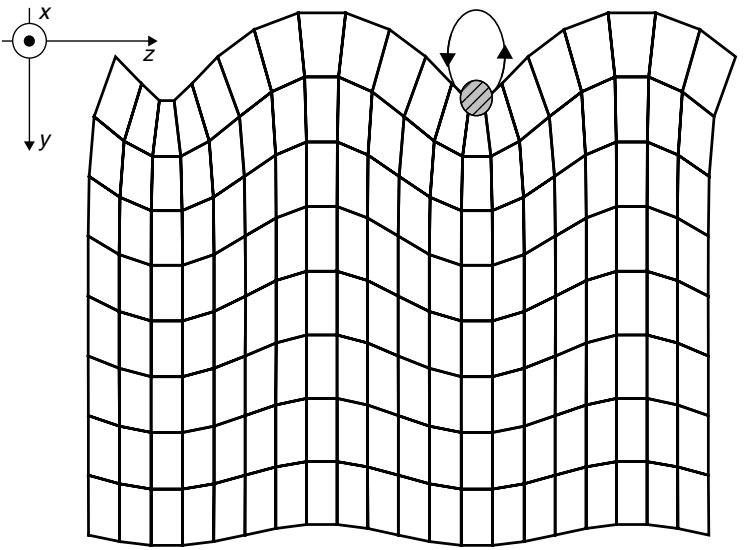


Figure 4.91 The section through a crystal shows the surface distortions of a surface wave propagating in the z-direction (reproduced by permission of Siemens AG, ZT KM, Munich)

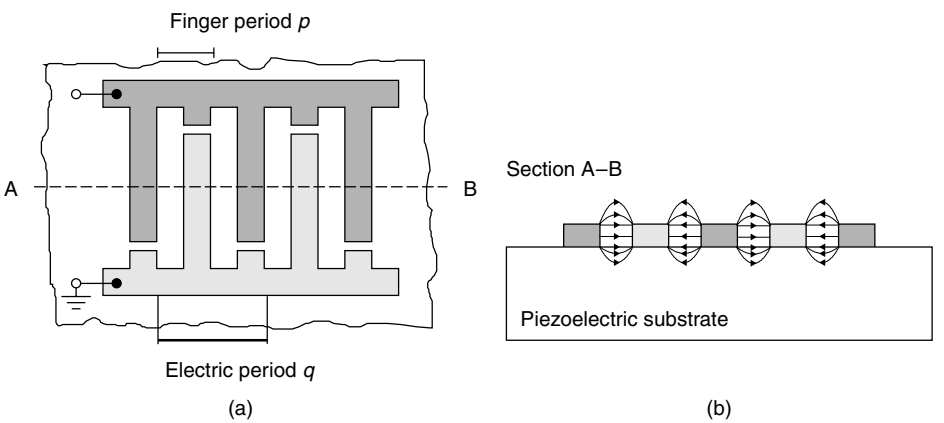


Figure 4.92 Principal structure of an interdigital transducer. Left, arrangement of the finger-shaped electrodes of an interdigital transducer; right, the creation of an electric field between electrodes of different polarity (reproduced by permission of Siemens AG, ZT KM, Munich)

Interdigital electrode structures in the form of interleaved fingers make effective electroacoustic transducers. Each pair of such interleaved fingers (Figure 4.91) form a so-called *interdigital transducer* (Latin *digitus* = finger, *inter* = between). A δ-shaped electrical pulse applied to the busbar of an interdigital transducer results in a mechanical deformation at the surface of the substrate between fingers of different polarity due to the piezoelectric effect. This deformation is proportional to the electrical field and propagates as a surface wave in both directions at velocity v (see Figure 4.92). Conversely, a surface wave entering the converter generates a signal proportional to

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

the finger structure at the busbar as a result of the piezoelectric effect (Meinke and Gundlach, 1992).

The distance between two fingers of the same polarity is termed the electrical period q of the interdigital transducer. The maximum electroacoustic interaction is obtained at the frequency f_0, the mid-frequency of the transducer. At this frequency the wavelength λ_0 of the surface acoustic wave precisely corresponds with the electrical period q of the interdigital transducer, so that all wave trains are superimposed in-phase and transmission is maximized (Reindl and Mágori; 1995).

$$\frac{v}{f_0} = \lambda_0 = q \tag{4.115}$$

The relationship between the electrical and mechanical power density of a surface wave is described by the material-dependent piezoelectric coupling coefficient k^2. Around k^{-2} overlaps of the transducer are required to convert the entire electrical power applied to the interdigital transducer into the acoustic power of a surface wave.

The bandwidth B of a transducer can be influenced by the length of the converter and is:

$$B = 2f_0/N (N = \text{number of fingers}) \tag{4.116}$$

4.3.2 Reflection of a surface wave

If a surface wave meets a mechanical or electrical discontinuity on the surface a small part of the surface wave is reflected. The transition between free and metallised surface represents such a discontinuity, therefore a periodic arrangement of N reflector strips can be used as a reflector. If the reflector period p (see Figure 4.93) is equal to half a wavelength λ_0, then all reflections are superimposed in-phase. The degree of reflection

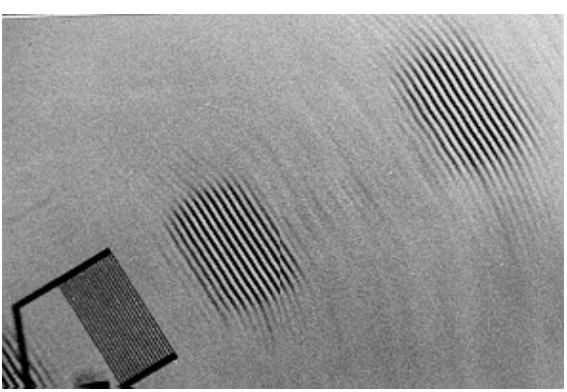


Figure 4.93 Scanning electron microscope photograph of several surface wave packets on a piezoelectric crystal. The interdigital transducer itself can be seen to the bottom left of the picture. An electric alternating voltage at the electrodes of the interdigital transducer generates a surface wave in the crystal lattice as a result of the piezoelectric effect. Conversely, an incoming surface wave generates an electric alternating voltage of the same frequency at the electrodes of the transducer (reproduced by permission of Siemens AG, ZT KM, Munich)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

thus reaches its maximum value for the associated frequency, the so-called Bragg frequency f_B. See Figure 4.94.

$$f_B = \frac{v}{2p} \tag{4.117}$$

4.3.3 Functional diagram of SAW transponders (Figure 4.95)

A surface wave transponder is created by the combination of an interdigital transducer and several reflectors on a piezoelectric monocrystal, with the two busbars of the interdigital transducer being connected by a (dipole) antenna.

A high-frequency *interrogation pulse* is emitted by the antenna of a reader at periodic intervals. If a surface wave transponder is located in the interrogation zone of the reader part of the power emitted is received by the transponder's antenna and travels to the terminals of the interdigital converter in the form of a high-frequency voltage pulse. The interdigital transducer converts part of this received power into a surface acoustic wave, which propagates in the crystal at right angles to the fingers of the transducer.[8]



Figure 4.94 Geometry of a simple reflector for surface waves (reproduced by permission of Siemens AG, ZT KM, Munich)

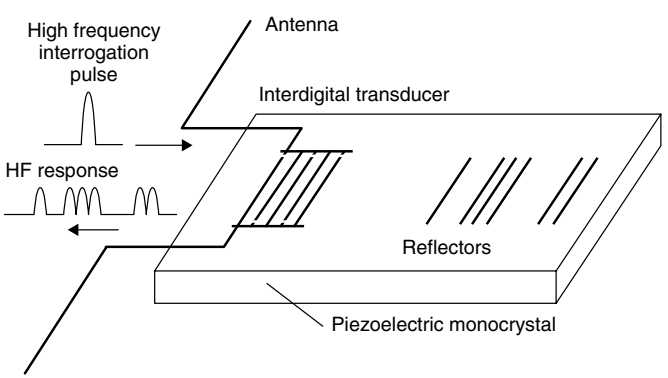


Figure 4.95 Functional diagram of a surface wave transponder (reproduced by permission of Siemens AG, ZT KM, Munich)

[8] To convert as much of the received power as possible into acoustic power, firstly the transmission frequency f_0 of the reader should correspond with the mid-frequency of the interdigital converter. Secondly, however, the number of transducer fingers should be matched to the coupling coefficient k_2.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Reflectors are now applied to the crystal in a characteristic sequence along the propagation path of the surface wave. At each of the reflectors a small part of the surface wave is reflected and runs back along the crystal in the direction of the interdigital transducer. Thus a number of pulses are generated from a single interrogation pulse. In the interdigital transducer the incoming acoustic pulses are converted back into high-frequency voltage pulses and are emitted from the antenna of the transponder as the transponder's response signal. Due to the low propagation speed of the surface wave the first response pulses arrive at the reader after a delay of a few microseconds. After this time delay the *interference reflections* from the vicinity of the reader have long since decayed and can no longer interfere with the transponder's response pulse. Interference reflections from a radius of 100 m around the reader have decayed after around 0.66 µs (propagation time for 2 × 100 m). A surface wave on a quartz substrate ($v = 3158$ m/s) covers 2 mm in this time and thus just reaches the first reflectors on the substrate. This type of surface wave transponder is therefore also known as 'reflective delay lines' (Figure 4.96).

Surface wave transponders are completely linear and thus respond with a defined phase in relation to the interrogation pulse (see Figure 4.97). Furthermore, the phase angle $\phi_{2\text{-}1}$ and the differential propagation time $\tau_{2\text{-}1}$ between the reflected individual signals is constant. This gives rise to the possibility of improving the *range* of a surface wave transponder by taking the mean of weak transponder response signals from many interrogation pulses. Since a read operation requires only a few microseconds, several hundreds of thousands of read cycles can be performed per second.

The range of a surface wave transponder system can be determined using the radar equation (see Section 4.2.4.1). The influence of coherent averaging is taken into account as 'integration time' t_I (Reindl *et al.*, 1998a).

$$d = \sqrt[4]{\frac{P_T \cdot G_T^2 \cdot G_R^2 \cdot t_i \cdot \lambda^4}{k \cdot T_0 \cdot F \cdot \frac{S}{N} \cdot IL}} \tag{4.118}$$

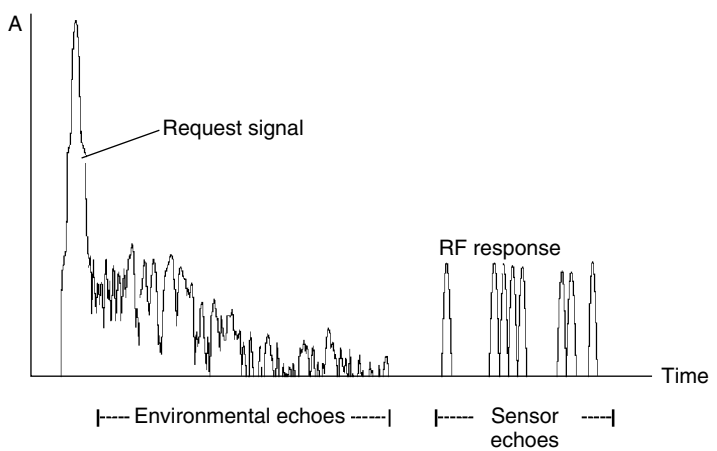


Figure 4.96 Sensor echoes from the surface wave transponder do not arrive until environmental echoes have decayed (reproduced by permission of Siemens AG, ZT KM, Munich)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

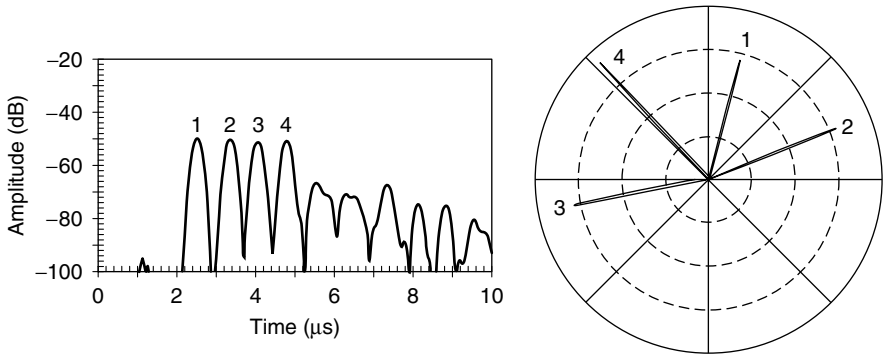


Figure 4.97 Surface wave transponders operate at a defined phase in relation to the interrogation pulse. Left, interrogation pulse, consisting of four individual pulses; right, the phase position of the response pulse, shown in a clockface diagram, is precisely defined (reproduced by permission of Siemens AG, ZT KM, Munich)

The relationship between the number of read cycles and the range of the system is shown in Figure 4.98 for two different frequency ranges. The calculation is based upon the system parameters listed in Table 4.9, which are typical of surface wave systems.

4.3.4 The sensor effect

The velocity v of a surface wave on the substrate, and thus also the propagation time τ and the mid-frequency f_0 of a surface wave component, can be influenced by a range of physical variables (Reindl and Mágori, 1995). In addition to temperature, mechanical forces such as static elongation, compression, shear, bending and acceleration have a particular influence upon the surface wave velocity v. This facilitates the remote interrogation of mechanical forces by surface wave sensors (Reindl and Mágori, 1995).

In general, the sensitivity S of the quantity x to a variation of the influence quantity y can be defined as:

$$S_y^x = \frac{1}{x} \cdot \frac{\partial x}{\partial y} \tag{4.119}$$

Table 4.9 System parameters for the range calculation shown in Figure 4.97

Value	At 433 MHz	At 2.45 GHz
P_S: transmission power	+14 dBm	
G_T: gain of transmission antenna	0 dB	
G_R: gain of transponder antenna	−3 dBl	0 dBl
Wavelength λ	70 cm	12 cm
F: Noise number of the receiver (reader)	12 dB	
S/N: Required signal/noise distance for error-free data detection	20 dB	
IL: Insertion loss: This is the additional damping of the electromagnetic response signal on the return path in the form of a surface wave	35 dB	40 dB
T_0: Noise temperature of the receiving antenna	300 K	

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

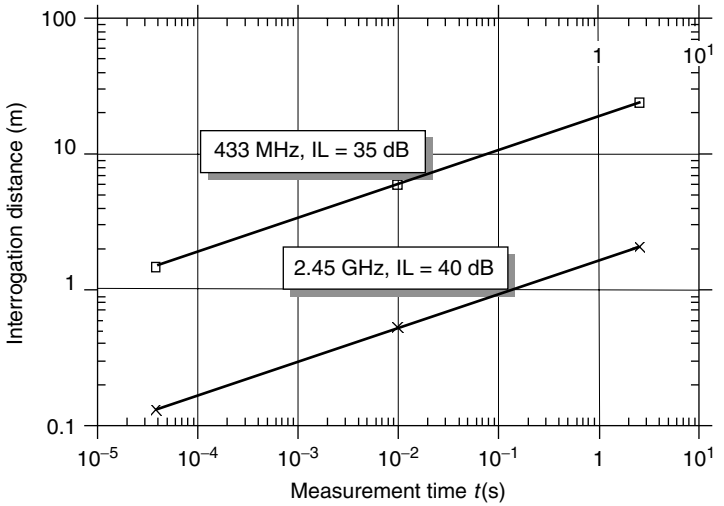


Figure 4.98 Calculation of the system range of a surface wave transponder system in relation to the integration time t_i at different frequencies (reproduced by permission of Siemens AG, ZT KM, Munich)

The sensitivity S to a certain influence quantity y is dependent here upon substrate material and crystal section. For example, the influence of temperature T upon propagation speed v for a surface wave on quartz is zero. Surface wave transponders are therefore particularly temperature stable on this material. On other substrate materials the propagation speed v varies with the temperature T.

The temperature dependency is described by the sensitivity S_T^v (also called the temperature coefficient Tk). The influence of temperature on the propagation speed v, the mid-frequency f_0 and the propagation time τ can be calculated as follows (Reindl and Mágori, 1995):

$$v(T) = v(T_0) \cdot [1 - S_T^v \cdot (T - T_0)] \tag{4.120}$$

$$f_0(T) = f_0(T_0) \cdot [1 - S_T^v \cdot (T - T_0)] \tag{4.121}$$

$$\tau(T) = \tau(T_0) \cdot [1 + S_T^v \cdot (T - T_0)] \tag{4.122}$$

4.3.4.1 Reflective delay lines

If only the differential propagation times or the differential phases between the individual reflected pulses are evaluated, the sensor signal is independent of the distance between the reader and the transponder. The differential propagation time $\tau_{2\text{-}1}$, and the differential phase $\theta_{2\text{-}1}$ between two received response pulses is obtained from the distance $L_{2\text{-}1}$ between the two reflectors, the velocity v of the surface wave and the frequency f of the interrogation pulse.

$$\tau_{2-1} = \frac{2 \cdot L_{2-1}}{v} \tag{4.123}$$

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 4.10 The properties of some common surface wave substrate materials

Material	Crystal direction		V	k^2	S_T^v (Tk)	Damping (dB/μs)	
	Section ①	Prop ②	(m/s)	(%)	(ppm/°C)	433 MHz	2.45 GHz
Quartz	ST	X	3158	0.1	0	0.75	18.6
Quartz	37° rot-Y	90° rot-X	5092	=0.1	00	③	③
$LiNbO_3$	Y	Z	3488	4.1	94	0.25	5.8
$LiNbO_3$	128° rot-Y	X	3980	5.5	75	0.27	5.2
$LiTaO_3$	36° rot-Y	X	4112	=6.6	30	1.35 ③	20.9 ③
$LiTaO_3$	X	112° rot-Y	3301	0.88	18	—	—

① Section — surface normal to crystal axis.
② Crystal axis of the wave propagation.
③ Strong dependency of the value on the layer thickness.

$$\varphi_{2-1} = 2\pi f \cdot \tau_{2-1} = \frac{4\pi f \cdot L_{2-1}}{v} \tag{4.124}$$

The measurable change $\Delta\tau_{2\text{-}1}$ or $\Delta\theta_{2\text{-}1}$ when a physical quantity y is changed by the amount Δy is thus:

$$\Delta\tau_{2-1} = \tau_{2-1} \cdot S_y^\tau \cdot \Delta y \tag{4.125}$$

$$\Delta\varphi_{2-1} = 2\pi f \cdot \tau_{2-1} \cdot S_y^\tau \cdot \Delta y \tag{4.126}$$

The influence of the physical quantity y on the surface wave transponder can thus be determined only by the evaluation of the phase difference between the different pulses of the response signal. The measurement result is therefore also independent of the distance between reader and transponder.

For lithium niobate ($LiNbO_3$, YZ section), the linear temperature coefficient $T_k = S_T^v$ is approximately 90 ppm/°C. A reflective delay line on this crystal is thus a sensitive *temperature sensor* that can be interrogated by radio. Figure 4.99 shows the example of the pulse response of a temperature sensor and the temperature dependency of the associated phase values (Reindl *et al.*, 1998b). The precision of a temperature measurement based upon the evaluation of the associated phase value $\theta_{2\text{-}1}$ is approximately ±0.1°C and this precision can even be increased by special measures such as the use of longer propagation paths $L_{2\text{-}1}$ (see equation (4.124)) in the crystal. The unambiguity of the phase measurement can be assured over the entire measuring range by three to four correctly positioned reflectors.

4.3.4.2 Resonant sensors

In a reflective delay line the available path is used twice. However, if the interdigital transducer is positioned between two fully reflective structures, then the acoustic path can be used a much greater number of times due to multiple reflection. Such an arrangement (see Figure 4.99) is called a surface wave *one-port resonator*. The distance between the two reflectors must be an integer multiple of the half wavelength λ_0 at the resonant frequency f_1.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

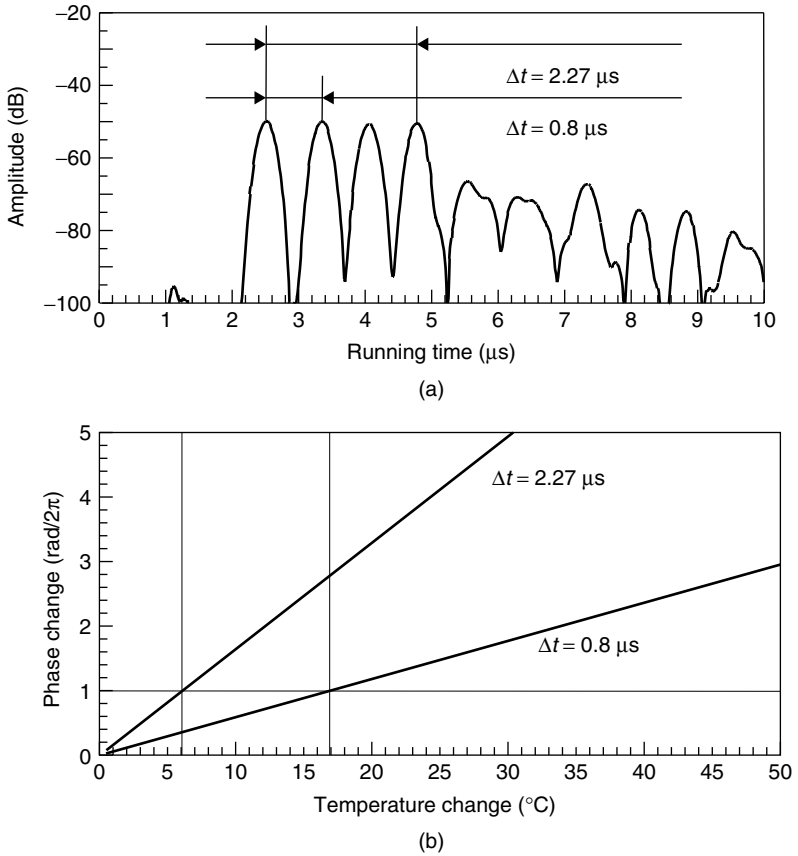


Figure 4.99 Impulse response of a temperature sensor and variation of the associated phase values between two pulses ($\Delta\tau = 0.8\,\mu s$) or four pulses ($\Delta\tau = 2.27\,\mu s$). The high degree of linearity of the measurement is striking (reproduced by permission of Siemens AG, ZT KM, Munich)

The number of wave trains stored in such a *resonator* will be determined by its loaded Q factor. Normally a *Q factor* of 10 000 is achieved at 434 MHz and at 2.45 GHz a Q factor of between 1500 and 3000 is reached (Reindl *et al.*, 1998b). The displacement of the mid-frequency Δf_1 and the displacement of the associated phase $\Delta\theta_1$ of a resonator due to a change of the physical quantity y with the loaded Q factor are (Reindl *et al.*, 1998a):

$$\Delta f_1 = -f_1(y_0) \cdot S_{y,1} \cdot \Delta y \tag{4.127}$$

and

$$\Delta\varphi = 2\mathrm{Q} \cdot \frac{\Delta f}{f} \tag{4.128}$$

where f_1 is the unaffected resonant frequency of the resonator.

In practice, the same sensitivity is obtained as for a reflective delay line, but with a significant reduction in chip size (Reindl *et al.*, 1998b) (Figure 4.100).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

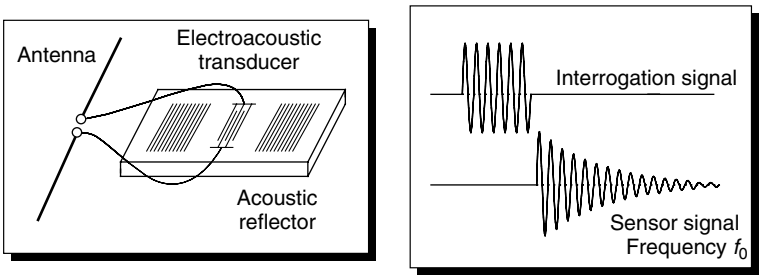


Figure 4.100 Principal layout of a resonant surface wave transponder and the associated pulse response (reproduced by permission of Siemens AG, ZT KM, Munich)

If, instead of one resonator, several resonators with different frequencies are placed on a crystal (Figure 4.101), then the situation is different: instead of a pulse sequence in the time domain, such an arrangement emits a characteristic line spectrum back to the interrogation device (Reindl *et al.*, 1998b,c), which can be obtained from the received sensor signal by a Fourier transformation (Figure 4.102).

The difference $\Delta f_{2\text{-}1}$ between the resonant frequencies of the two resonators is determined to measure a physical quantity y in a surface wave transponder with two resonators. Similarly to equation (4.127), this yields the following relationship (Reindl *et al.*, 1998c).

$$\Delta f_{2-1} = -[f_2(y_0) \cdot S_{y,2} - f_1(y_0) \cdot S_{y,1}] \cdot \Delta y \tag{4.129}$$

4.3.4.3 Impedance sensors

Using surface wave transponders, even conventional sensors can be passively interrogated by radio if the impedance of the sensor changes as a result of the change of a physical quantity y (e.g. photoresistor, Hall sensor, NTC or PTC resistor). To achieve this a second interdigital transducer is used as a reflector and connected to the external sensor (Figure 4.103). A measured quantity Δy thus changes the terminating impedance of the additional interdigital transducer. This changes the acoustic transmission and reflection ρ of the converter that is connected to this load, and thus also

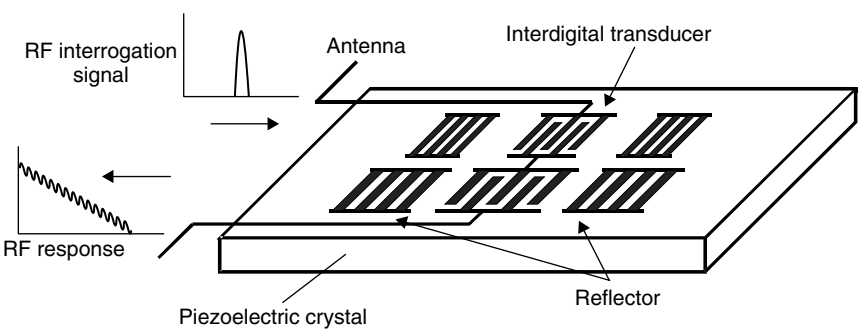


Figure 4.101 Principal layout of a surface wave transponder with two resonators of different frequency (f_1, f_2) (reproduced by permission of Siemens AG, ZT KM, Munich)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

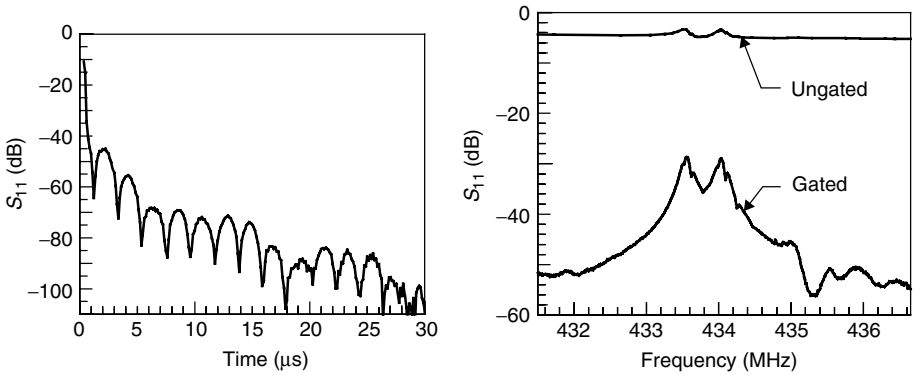


Figure 4.102 Left, measured impulse response of a surface wave transponder with two resonators of different frequency; right, after the Fourier transformation of the impulse response the different resonant frequencies of the two resonators are visible in the line spectrum (here: approx. 433.5 MHz and 434 MHz) (reproduced by permission of Siemens AG, ZT KM, Munich)

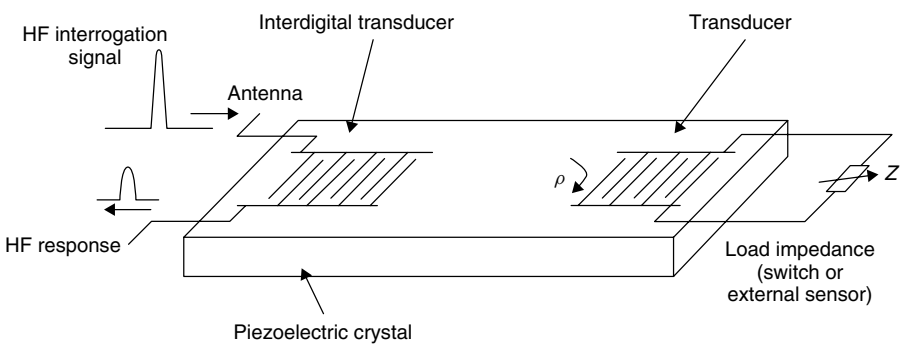


Figure 4.103 Principal layout of a passive surface wave transponder connected to an external sensor (reproduced by permission of Siemens AG, ZT KM, Munich)

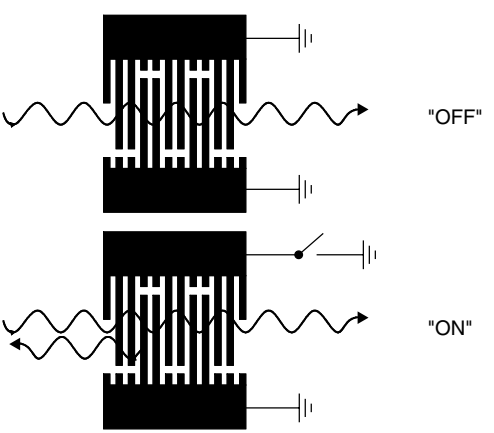


Figure 4.104 Passive recoding of a surface wave transponder by a switched interdigital transducer (reproduced by permission of Siemens AG, ZT KM, Munich)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

changes the magnitude and phase of the reflected HF pulse, which can be detected by the reader.

4.3.5 Switched sensors

Surface wave transponders can also be passively recoded (Figure 4.104). As is the case for an impedance sensor, a second interdigital transducer is used as a reflector. External circuit elements of the interdigital transducer's busbar make it possible to switch between the states 'short-circuited' and 'open'. This significantly changes the acoustic transmission and reflection ρ of the transducer and thus also the magnitude and phase of the reflected HF impulse that can be detected by the reader.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

5

Frequency Ranges and Radio Licensing Regulations

5.1 Frequency Ranges Used

Because RFID systems generate and radiate electromagnetic waves, they are legally classified as *radio systems*. The function of other *radio services* must under no circumstances be disrupted or impaired by the operation of RFID systems. It is particularly important to ensure that RFID systems do not interfere with nearby radio and television, mobile radio services (police, security services, industry), marine and aeronautical radio services and mobile telephones.

The need to exercise care with regard to other radio services significantly restricts the range of suitable operating frequencies available to an RFID system (Figure 5.1). For this reason, it is usually only possible to use frequency ranges that have been reserved specifically for industrial, scientific or medical applications. These are the frequencies classified worldwide as *ISM frequency ranges* (Industrial–Scientific–Medical), and they can also be used for RFID applications.

In addition to ISM frequencies, the entire *frequency range* below 135 kHz (in North and South America and Japan: <400 kHz) is also suitable, because it is possible to work with high magnetic field strengths in this range, particularly when operating inductively coupled RFID systems.

The most important frequency ranges for RFID systems are therefore 0–135 kHz, and the ISM frequencies around 6.78 (not yet available in Germany), 13.56 MHz, 27.125 MHz, 40.68 MHz, 433.92 MHz, 869.0 MHz, 915.0 MHz (not in Europe), 2.45 GHz, 5.8 GHz and 24.125 GHz.

An overview of the estimated distribution of RFID transponders at the various *frequencies* is shown in Figure 5.2.

5.1.1 Frequency range 9–135 kHz

The range below 135 kHz is heavily used by other radio services because it has not been reserved as an ISM frequency range. The propagation conditions in this *long wave*

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

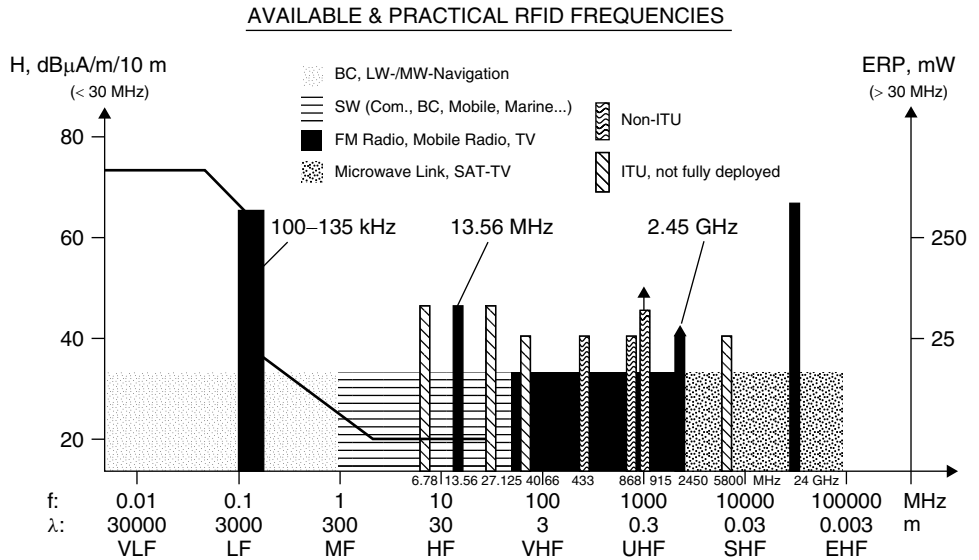


Figure 5.1 The frequency ranges used for RFID systems range from the myriametric range below 135 kHz, through short wave and ultrashort wave to the microwave range, with the highest frequency being 24 GHz. In the frequency range above 135 kHz the ISM bands available worldwide are preferred

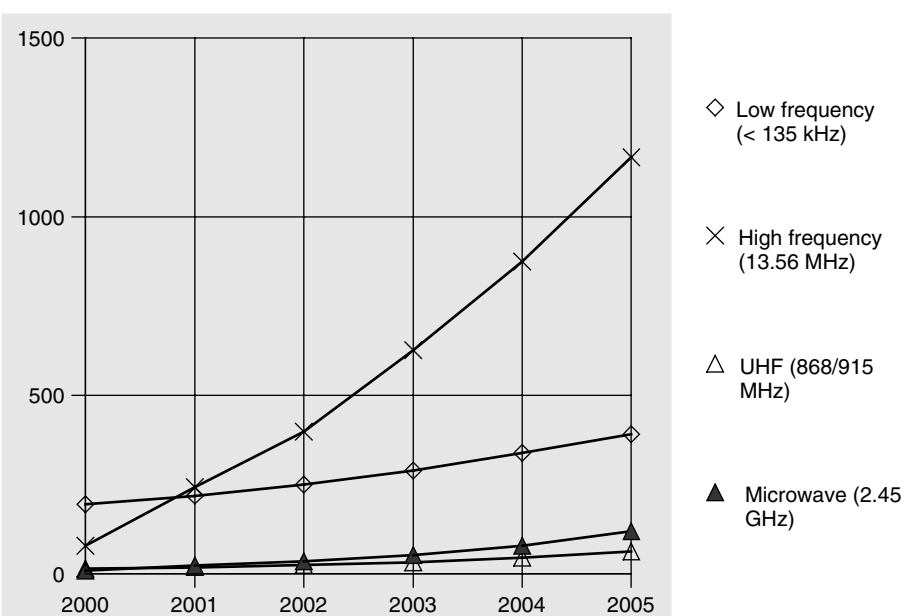


Figure 5.2 The estimated distribution of the global market for transponders over the various frequency ranges in million transponder units (Krebs, n.d.)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

5.1.2 Frequency range 6.78 MHz

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

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

5.1.3 Frequency range 13.56 MHz

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

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

5.1.4 Frequency range 27.125 MHz

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

5.1.5 Frequency range 40.680 MHz

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

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

5.1.6 Frequency range 433.920 MHz

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

5.1.7 Frequency range 869.0 MHz

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

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

5.1.8 Frequency range 915.0 MHz

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

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

5.1.9 Frequency range 2.45 GHz

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

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

5.1.10 Frequency range 5.8 GHz

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

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

5.1.11 Frequency range 24.125 GHz

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

5.1.12 Selection of a suitable frequency for inductively coupled RFID systems

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

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

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

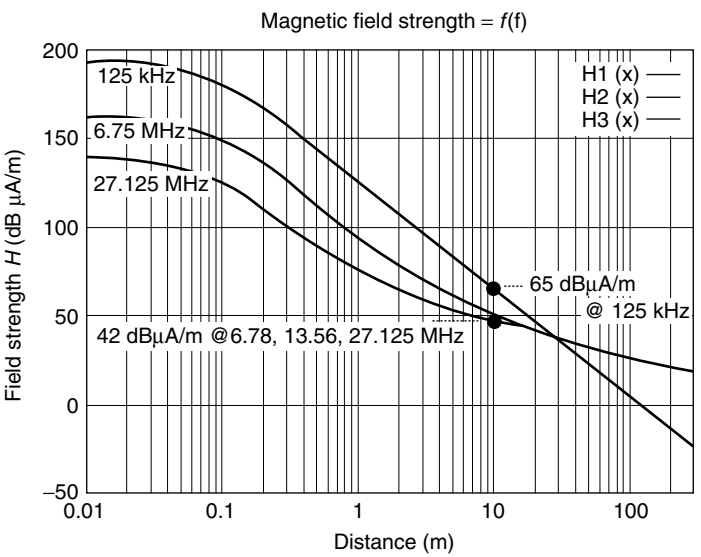


Figure 5.3 Different permissible field strengths for inductively coupled systems measured at a distance of 10 m (the distance specified for licensing procedures) and the difference in the distance at which the reduction occurs at the transition between near and far field lead to marked differences in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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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

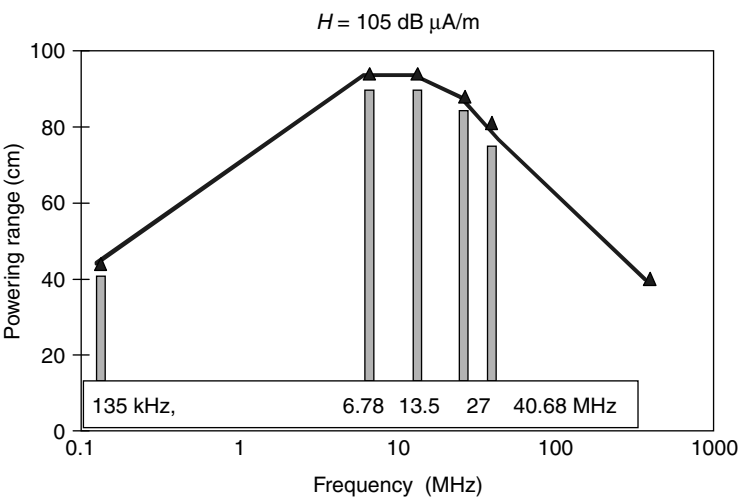


Figure 5.4 Transponder range at the same field strength. The induced voltage at a transponder is measured with the antenna area and magnetic field strength of the reader antenna held constant (reproduced by permission of Texas Instruments)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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

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

5.2 European Licensing Regulations

5.2.1 CEPT/ERC REC 70-03

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

October 1997. The old national regulations for Short Range Devices (SRDs) are thus being successively replaced by a harmonised European regulation. In the new version of February 2002 the REC 70-03 also includes comprehensive notes on national restrictions for the specified applications and frequency ranges in the individual member states of CEPT (REC 70-03, Appendix 3 – National Restrictions). For this reason, Section 5.3 bases its discussion of the national regulations in a CEPT member state solely upon the example of Germany. Current notes on the regulation of short range devices in all other CEPT members states can be found in the current version of REC 70-03. The document is available to download on the home page of the ERO (*European Radio Office*), http://www.ero.dk/EROWEB/SRD/SRD-index.htm.

REC 70-03 defines *frequency bands, power levels, channel spacing,* and the transmission duration (duty cycle) of short range devices. In CEPT members states that use the R&TTE Directive (1999/5/EC), short range devices in accordance with article 12 (CE marking) and article 7.2 (putting into service of radio equipment) can be put into service without further licensing if they are marked with a CE mark and do not infringe national regulatory restrictions in the member states in question (EC, 1995) (see also Section 5.3).

REC 70-03 deals with a total of 13 different applications of short range devices at the various frequency ranges, which are described comprehensively in its own Annexes (Table 5.2).

REC 70-03 also refers to the harmonised ETSI standards (e.g. EN 300 330), which contain measurement and testing guidelines for the licensing of radio devices.

5.2.1.1 Annex 1: Non-specific short range devices

Annex 1 describes frequency ranges and permitted transmission power for *short range devices* that are not further specified (Table 5.3). These frequency ranges can expressly also be used by RFID systems, if the specified levels and powers are adhered to.

Table 5.2 Short range device applications from REC 70-03

Annex	Application
Annex 1	Non-specific Short Range Devices
Annex 2	Devices for Detecting Avalanche Victims
Annex 3	Local Area Networks, RLANs and HIPERLANs
Annex 4	Automatic Vehicle Identification for Railways (AVI)
Annex 5	Road Transport and Traffic Telematics (RTTT)
Annex 6	Equipment for Detecting Movement and Equipment for Alert
Annex 7	Alarms
Annex 8	Model Control
Annex 9	Inductive Applications
Annex 10	Radio Microphones
Annex 11	RFID
Annex 12	Ultra Low Power Active Medical Implants
Annex 13	Wireless Audio Applications

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 5.3 Non-specific short range devices

Frequency band	Power	Comment
6785–6795 kHz	42 dBμA/m @ 10 m	
13.553–13.567 MHz	42 dBμA/m @ 10 m	
26.957–27.283 MHz	42 dBμA/m	(10 mW ERP)
40.660–40.700 MHz	10 mW ERP	
138.2–138.45 MHz	10 mW ERP	Only available in some states
433.050–434.790 MHz	10 mW ERP	<10% duty cycle
433.050–434.790 MHz	1 mW ERP	Up to 100% duty cycle
868.000–868.600 MHz	25 mW ERP	<1% duty cycle
868.700–869.200 MHz	25 mW ERP	<0.1% duty cycle
869.300–869.400 MHz	10 mW ERP	
869.400–860.650 MHz	500 mW ERP	<10% duty cycle
869.700–870.000 MHz	5 mW ERP	
2400–2483.5 MHz	10 mW EIRP	
5725–5875 MHz	25 mW EIRP	
24.00–24.25 GHz	100 mW	
61.0–61.5	100 mW EIRP	
122–123 GHz	100 mW EIRP	
244–246 GHz	10 mW EIRP	

Relevant harmonised standards: EN 300 220, EN 300 330, EN 300 440.

5.2.1.2 Annex 4: Railway applications

Annex 4 describes frequency ranges and permitted transmission power for short range devices in application for *rail traffic* applications. RFID transponder systems such as the *Eurobalise* S21 (see Section 13.5.1) or *vehicle identification* by transponder (see Section 13.5.2) are among these applications.

Table 5.4 Railway applications

Frequency band	Power	Comment
4515 kHz	7 dB μA/m @ 10 m	Euroloop (spectrum mask available)
27.095 MHz	42 dB μA/m	Eurobalise (5 dBμA/m @ ±200 kHz
2446–2454 MHz	500 mW EIRP	Transponder applications (AVI)

Relevant harmonised standards: EN 300 761, EN 300 330.

Table 5.5 Road Transport and Traffic Telematics (RTTT)

Frequency band	Power	Comment
5795–5815 MHz	8 W EIRP	Road toll systems
63–64 GHz	t.b.d.	Vehicle — vehicle communication
76–77 GHz	55 dBm peak	Vehicle — radar systems

Relevant harmonised standards: EN 300 674, EN 301 091, EN 201 674.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 5.6 Inductive applications

Frequency band	Power	Comment
9.000–59.750 kHz 60.250–70.000 kHz 119–135 kHz	See comment	72 dBμ A/m at 30 kHz, descending by −3 dB/Ok
59.750–60.250 kHz 70–119 kHz	42 dB μA/m @ 10 m	
6765–6795 kHz	42 dB μA/m @ 10 m	
7400–8800 kHz	9 dB μA/m	EAS systems
13.553–13.567 MHz	42 dB μA/m @ 10 m	(9 dBμA/m@ ± 150 kHz)
26.957–27.283 MHz	42 dB μA/m @ 10 m	(9 dBμA/m@ ± 150 kHz)

Relevant harmonised standards: EN 300 330.

Table 5.7 RFID applications

Frequency band	Power	Comment
2446–2454 MHz	500 mW EIRP	100% duty cycle
	4 W EIRP	<15% duty cycle; only within buildings

Relevant harmonised standards: EN 300 440.

Table 5.8 Proposal for a further frequency range for RFID systems

Frequency band	Power	Comment
865.0–868.0 MHz:		Channels with 100 kHz channel spacing
865.0–865.6 MHz	100 mW EIRP	
865.6–867.6 MHz	2 W EIRP	
867.6–868.0 MHz	100 mW EIRP	

5.2.1.3 Annex 5: Road transport and traffic telematics

Annex 5 describes frequency ranges and permitted transmission power for short range devices in *traffic telematics* and *vehicle identification* applications. These applications include the use of RFID transponders in *road toll systems*.

5.2.1.4 Annex 9: Inductive applications

Annex 9 describes frequency ranges and permitted transmission power for *inductive radio systems*. These include RFID transponders and *Electronic Article Surveillance (EAS)* in shops.

5.2.1.5 Annex 11: RFID applications

Annex 11 describes the frequency ranges and permitted transmission power for RFID systems. An 8 MHz segment of the 2.45 GHz frequency band is cleared for operation at an increased transmission power.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

5.2.1.6 Frequency range 868 MHz

The subject of possible future frequency ranges and transmission power for RFID systems in the 868 MHz range is currently under discussion by the European Radiocommunications Committee (ERC). In addition to the frequency range 869.4–869.65 MHz (500 mW EIRP at 10% duty cycle, Annex 1) that is already available, a future frequency range is being considered for RFID systems. A final decision is still awaited from the ERC.

5.2.2 EN 300 330: 9 kHz–25 MHz

The standards drawn up by *ETSI* (European Telecommunications Standards Institute) serve to provide the national telecommunications authorities with a basis for the creation of national regulations for the administration of radio and telecommunications.

The ETSI EN 300 330 standard forms the basis for European *licensing regulations for inductive radio system*:

> ETSI EN 300 330: 'Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz'.
> Part 1: 'Technical characteristics and test methods'
> Part 2: 'Harmonized EN under article 3.2 of the R&TTE Directive'

In addition to inductive radio systems, *EN 300330* also deals with *Electronic Article Surveillance* (for shops), alarm systems, *telemetry transmitters*, and short range telecontrol systems, which are considered under the collective term Short Range Devices (SRDs).

In addition to the CEPT member states, this regulation is also used by many Asiatic and American states in the licensing of RFID systems.

EN 3003300 thus primarily defines measurement procedures for transmitter and receiver that can be used to reproducibly verify adherence to the prescribed limit values in relation to ERC REC 70-03.

Inductive loop coil transmitters in accordance with EN 300330 are characterised by the fact that the antenna is formed by a loop of wire with one or more windings. EN 300330 differentiates between four product classes (Table 5.9).

All the inductively coupled RFID systems in the frequency range 9 kHz–30 MHz described in EN 300 330 belong to the class 1 and class 2 types. Therefore class 3 and class 4 types will not be further considered in this book.

5.2.2.1 Carrier power – limit values for H field transmitters

In class 1 and class 2 inductive loop coil transmitters (integral antenna) the *H field* of the radio system is measured in the direction in which the field strength reaches a maximum. The measurement should be performed in free space, with a distance

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 5.9 Classification of the product types

Class 1	Transmitter with inductive *loop antenna*, in which the antenna is integrated into the device or permanently connected to it. Enclosed antenna area $<30\,m^2$.
Class 2	Transmitter with inductive loop antenna, in which the antenna is manufactured to the customer's requirements. Devices belonging to class 2, like class 1 devices, are tested using two typical customer-specific antennas. The enclosed antenna area must be less than $30\,m^2$.
Class 3	Transmitter with large inductive loop antenna, $>30\,m^2$ antenna area. Class 3 devices are tested without an antenna.
Class 4	E field transmitter. These devices are tested with an antenna.

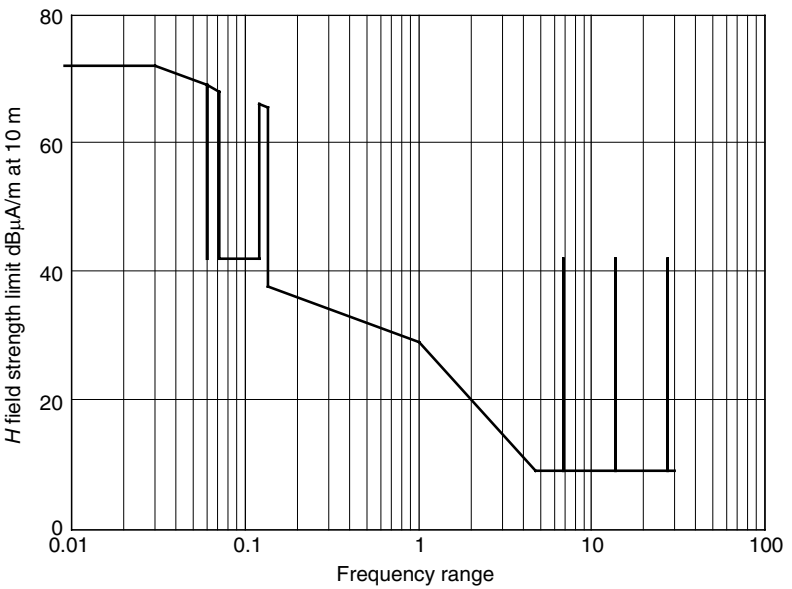


Figure 5.5 Limit values for the magnetic field strength H measured at a distance of 10 m, according to Table 5.10

of 10 m between measuring antenna and measurement object. The transmitter is not modulated during the field strength measurement.

The limit values listed in Table 5.10 have been defined. See Figure 5.5.

In loop antennas with an antenna area between $0.05\,m^2$ (diameter 24 cm) and $0.16\,m^2$ (diameter 44 cm) a correction factor must be subtracted from the values in Table 5.10. The following is true:

$$\text{limit value} = \text{table value} = 10\log\left(\frac{\text{antenna-area}}{0.16\,m^2}\right) \tag{5.1}$$

For a typical RFID antenna with a diameter of 32 cm there would be a correction factor of -3 dB and thus at 13.56 MHz the maximum field strength would be 39 dBµV/m at a distance of 10 m.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 5.10 Maximum permitted magnetic field strength at a distance of 10 m

Frequency range (MHz)	Maximum *H* field at a distance of 10 m
0.009–0.030	72 dBμA/m
0.030–0.070	72 dBμA/m at 0.030 MHz descending by −3 dB/octave
0.05975–0.06025	42 dBμA/m
0.070–0.119	
0.119–0.135	72 dBμA/m at 0.03 MHz, descending by −3 dB/oct
0.135–1.0	37.7 dBμA/m at 0.135 MHz, descending by −3 dB/octave
1.0–4.642	29 dBμA/m at 1.0 MHz, descending by −9 dB/octave
4.643–30	9 dBμA/m
6.675–6.795	42 dBμA/m
13.553–13.567	
25.957–27.283	

For loop antennas with an antenna area less than 0.05 m^2 (diameter <24 cm) a constant correction factor of 10 dB must be subtracted from the table values.

5.2.2.2 Spurious emissions

Spurious emissions are emissions that are not part of the carrier frequency or the modulation sidebands, for example harmonics and parasitic compounds. Spurious emissions must be minimised. Intentional out-of-band emissions are forbidden (regardless of their level).

The limit values specified in Section 5.2.1 must be adhered to for spurious emissions in the frequency range 0–30 MHz. For the frequency range 30–1000 MHz the values specified in Table 5.11 must be adhered to, giving particular consideration to the frequency range of public radio and television, which is susceptible to interference.

5.2.3 EN 300 220-1, EN 300 220-2

The standard *EN 300 220*, entitled *'Radio Equipment and Systems (RES); Short range devices, Technical characteristics and test methods for radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW'*, provides the basis for national European licensing regulations for low power radio systems

Table 5.11 Permissible limit values for spurious emissions

System state	47–74 MHz 87.5–118 MHz 174–230 MHz 470–862 MHz	All other frequencies in the range 30–1000 MHz
Operation	4 nW	250 nW
Standby	2 nW	2 nW

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

and comprises two sections: EN 300 220-1 for transmitters and their power characteristics and EN 300 220-2, in which the characteristics for the receiver are defined.

EN 300 220 classifies devices into four types — classes I to IV — which are not defined in more detail. This standard covers low power radio systems, both within the ISM bands and throughout the entire frequency range (e.g. estate radio and pagers on 466.5 MHz). Typical ISM applications in these ranges are telemetry, alarm and remote control radio systems plus LPD radio telephony applications (10 mW at 433.920 MHz).

RFID systems are not mentioned explicitly, the frequency range below 30 MHz (27.125 MHz) being in any case covered by EN 300 330 and the frequency ranges 40.680 MHz and 433.920 MHz being less typical for RFID applications.

Unlike EN 300 330, which defines a maximum permitted field strength at a distance of 10 m from the measurement object, EN 300 220 specifies a maximum permitted *transmitter output power* at 50 Ω (Table 5.12).

This standard also defines testing methods and limit values for spurious emissions, which we will not, however, consider in more detail here.

5.2.4 EN 300 440

The *EN 300 440* standard, entitled *'Radio Equipment and Systems (RES); Short range devices, technical characteristics and test methods for radio equipment to be used in the 1 GHz to 25 GHz frequency range with power levels ranging up to 500 mW,'* forms the basis for national European regulations for low power radio systems. EN 300 440 classifies devices according to three types — classes I to III.

RFID systems with *backscatter transponders* are classified as class II systems. Further details are governed by the CEPT recommendation *T/R 60-01* 'Low power radiolocation equipment for detecting movement and for alert' (EAS) and T/R 22-04 'Harmonisation of frequency bands for Road Transport Information Systems (RTI)' (toll systems, freight identification).

Various ISM and short range applications are classified as class I and III systems. Typical applications in these classes are movement sensors (for alarm systems, door openers and similar applications), data transmission systems (wireless LAN for PC), remote control systems and telemetry.

EN 300 440 defines the maximum values listed in Table 5.13 for effective isotropic radiated power (EIR[1]).

Table 5.12 Device classes within and outside the ISM bands

		Permissible transmission power		
Class	Range (MHz)	ISM − 27 MHz	ISM − 40 MHz	ISM − 433 MHz
I	25–1000	10 mW	10 mW	10 mW
II	300–1000	—	—	25 mW
III	25–300	100 mW	100 mW	—
IV	300–1000	—	—	100 mW

[1] EIRP represents the power that a fictional isotropic source ($G = 0$ dB) would have to emit in order to generate the same power flux density at the reception location as at the device under test

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 5.13 Permitted transmission power in accordance with EN 300 440

	Frequency (GHz)		
Class	**1.0–5.0**	**5.0–20**	**>20**
I	10 mW	25 mW	100 mW
II*	500 mW	500 mW	500 mW
III	500 mW	2 W	2 W

*Reflective transponder systems.

The following frequency ranges are reserved for ISM applications:

- 2.400–2.4835 GHz
- 5.725–5.875 GHz
- 24.00–24.25 GHz

This standard also defines testing methods and limit values for spurious emissions, which we will not, however, consider in more detail here.

5.3 National Licensing Regulations in Europe

In Europe, the recommendations of the ERC serve as the basis for *national legislative and licensing regulations* for radio systems. For RFID systems REC 70-03 (short range devices, SRD) applies. The website of the ERO (European Radio Office) provides current notes on the national regulation of SRDs in the member states of CEPT (see Section 5.2.1).

In all member states of the EU and the member states of CEPT that apply the EU Directive *1999/5/EC* ('Radio and Telecommunications Terminal Equipment Directive', R&TTE Directive), SRDs can be offered for sale without further licensing (ERC, 2000). This is the case, under the prerequisite that the applicable licensing regulations for the frequency ranges and applications in question are adhered to. The manufacturer needs only to confirm that the relevant regulations have been adhered to for each product (EC Declaration of Conformity), which it does by displaying a *CE mark* upon the product.

Notes on the procedure regarding the CE marking and sale of radio and telecommunications systems can be found on the *R&TTE homepage* of the EU at http://europa.eu.int/comm/enterprise/rtte.

Basic notes on the new legislation regarding the CE marking of products can be found at http://europa.eu.int/comm/enterprise/newapproach/legislation/guide/legislation.htm.

5.3.1 Germany

In Germany, the licensing of RFID systems is regulated by two decrees ($R_{EG}TP$, 2000a,b) which were published in the *Amtsblatt der Regulierungsbehörde für Telekommunikation und Post* (RegTP) (*Gazette of the Regulatory Authorities for Telecommunications and Post*) in summer 2000. These decrees converted the recommendations

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

of the REC 70-03 into national legislation. Here, too, national restrictions (e.g. lower power level in some frequency ranges below 135.00 kHz) should be taken into consideration.

All radio systems that have a German licence or were put into operation in accordance with the provisions of Directive 1999/5/EC (R&TTE Directive), and are marked accordingly (CE marking), may be operated. Of course, national restrictions must still be adhered to.

The licensing of inductively coupled RFID systems is regulated in decree 61/2000, entitled 'Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für induktive Funkanlagen des nichtöffentlichen mobilen Landfunks (nömL)' ('General allocation of frequencies for use by the general public for inductive radio systems relating to private mobile national radio'). General allocation covers numerous applications of inductive radio systems, such as lorry barriers (RFID), EAS, traffic control systems, metal detectors, recognition systems for people, animals and goods (RFID), but also data and voice transmission over short distances (e.g. for alarm systems). See Figure 5.6.

Only the frequency ranges listed in Table 5.14 may be used for the above-mentioned radio applications.

The licensing of RFID systems in the frequency ranges up to 24 GHz is regulated in decree 73/200 entitled 'Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für Funkanlagen geringer Leistung des nichtöffentlichen mobilen Landfunks (nömL) in ISM Frequenzbereichen; SRD (Short Range Devices)' ('General allocation of frequencies for use by the general public for low power radio systems relating to private mobile national radio in ISM frequency ranges; SRD (Short Range

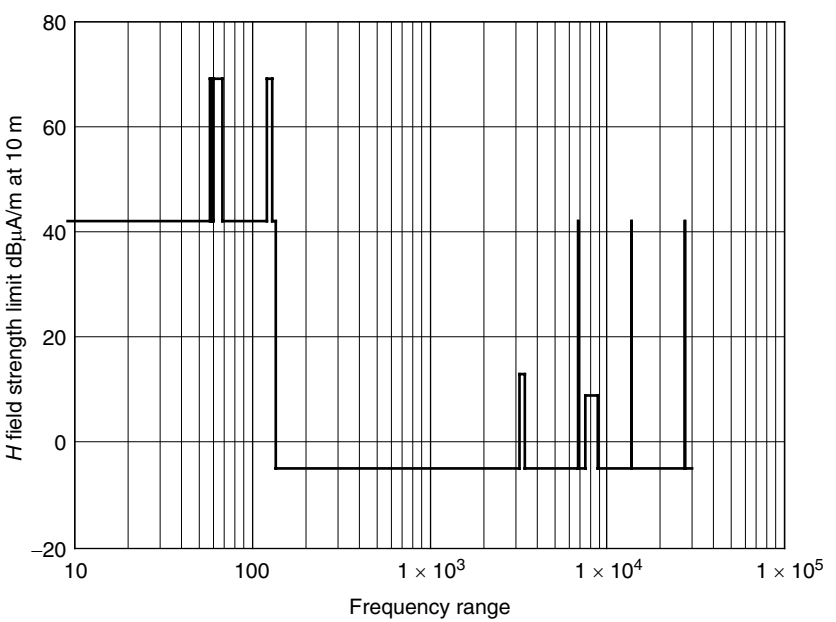


Figure 5.6 The permitted frequency range up to 30 MHz and the maximum field strength at a distance of 10 m in Germany

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 5.14 Permitted frequency ranges and field strengths at a distance of 10 m

Frequency range (MHz)	Field strength H @ 10 m (dBμA/m)
0.009–0.057	42
0.057–0.05975	69
0.05975–0.06025	42
0.06025–0.067	69
0.067–0.119	42
0.119–0.127	69
0.127–0.135	42
0.135–30.000	5
3.155–3.400	13.5 (EAS)
6.765–6.795	42
7.400–8.800	9 (EAS)
13.553–13.567	42
26.957–27.283	42

Table 5.15 Permissible frequency ranges and power levels for short range devices

Frequency range (MHz)	Power level
6.765–6.975	42 dBμA/m @ 10 m
13.553–13.567	42 dBμA/m @ 10 m
26.957–27.283	42 dBμA/m @ 10 m, 10 mW ERP
40.660–40.700	10 mW ERP
433.05–434.79	10 mW ERP
2400.0–2483.5	10 mW ERP
5725.0–5875.0	25 mW ERP
24.000–24.250	100 mW ERP

Devices)'). The general allocation covers numerous SRD applications and is not limited to RFID systems. Only the frequency ranges listed in Table 5.15 may be used for these applications with the corresponding maximum magnetic field strength or the maximum radiated power.

5.4 National Licensing Regulations

5.4.1 USA

In the USA, RFID systems must be licensed in accordance with licensing regulation '*FCC Part 15*'. This regulation covers the frequency range from 9 kHz to above 64 GHz and deals with the intentional generation of electromagnetic fields by low and minimum power transmitters (intentional radiators) plus the unintentional generation of electromagnetic fields (spurious radiation) by electronic devices such as radio and television receivers or computer systems. The category of low power transmitters covers a

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

wide variety of applications, for example cordless telephones, biometry and telemetry transmitters, on-campus radio stations, toy remote controls and door openers for cars. Inductively coupled or backscatter RFID systems are not explicitly mentioned in the FCC regulation, but they automatically fall under its scope due to their transmission frequencies, which are typically in the ISM bands, and their low transmission power.

Table 5.16 lists the frequency ranges that are important for RFID systems. In all other frequency ranges the permissible limit values for spurious radiation given in Table 5.17 apply to RFID systems. It should be noted here that, unlike the European licensing regulation ETS 300 330, the maximum permissible field strength of a reader is principally defined by the electrical field strength E. The measuring distance is selected such that a measurement is made in the far field of the generated field. This also applies for inductively coupled RFID systems in the frequency range below 30 MHz, which primarily generate a magnetic high frequency field.

5.4.2 Future development: USA–Japan–Europe

The USA and Japan are currently planning to adapt their national regulations for RFID systems to 13.56 MHz, and to the values permitted in Europe in accordance with REC 70-03. At the time of preparation of this book a final decision had not been taken on

Table 5.16 Permissible field strengths for RFID systems in accordance with FCC Part 15

Frequency range (MHz)	Max. E field	Measuring distance (m)	Section
1.705–10.000	100 µV/m	30	15.223
13.553–13.567	10 mV/m	30	15.225
26.960–27.280	10 mV/m	30	15.227
40.660–40.700	1 mV/m	3	15.229
49.820–49.900	10 mV/m	3	15.235
902.0–928.0	50 mV/m	3	15.249
2435–2465	50 mV/m	3	15.249
5785–5815	50 mV/m	3	15.249
24075–24175	250 mV/m	3	15.249

Table 5.17 Permissible interference field strength in all other frequency ranges in accordance with FCC Part 15, Section 15.209

Frequency range (MHz)	Maximum E field	Measuring distance (m)
0.009–0.490	2400/f µV/m	300
0.490–1.705	24/f mV/m	30
1.705–30.00	30 µV/m	30
30.00–88.00	100 µV/m	3
88.00–216	150 µV/m	3
216–960	200 µV/m	3
>960	500 µV/m	3

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

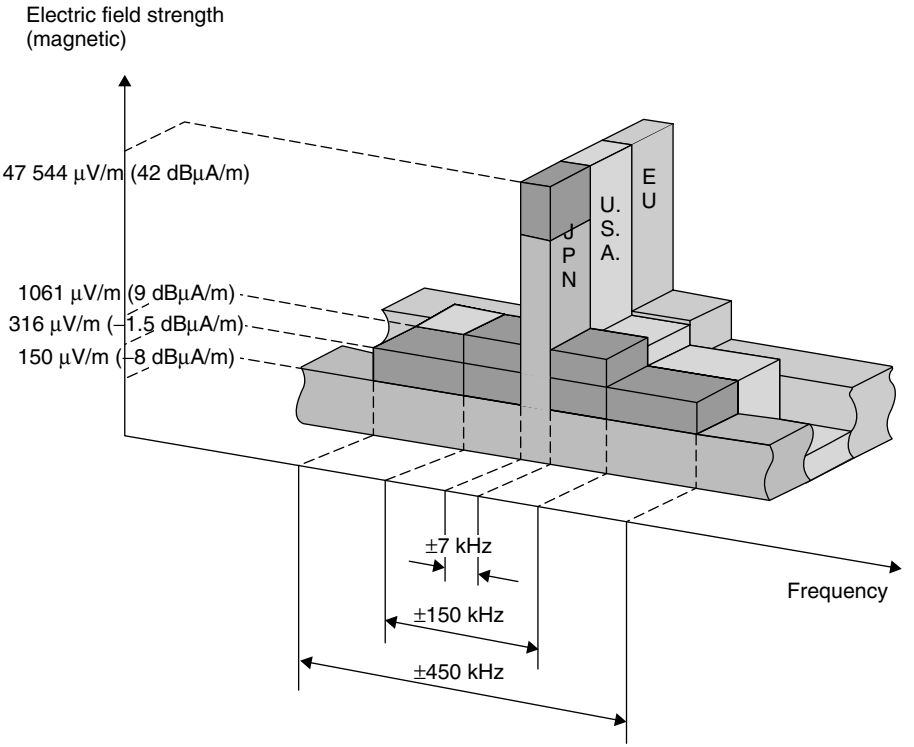


Figure 5.7 Comparison of the permitted magnetic field strengths of the planned regulations for 13.56 MHz RFID systems in the USA, Japan and Europe (reproduced by permission of Takeshi Iga[2], SOFEL, Tokyo)

any of the planned regulations, so at this point it is not possible to deal with these regulations in more detail. See Figure 5.7.

[2] Takeshi Iga: Publisher and translator of the Japanese edition of the RFID handbook. See also http://RFID-handbook.com/japanese

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

6
Coding and Modulation

The block diagram in Figure 6.1 describes a digital *communication system*. Similarly, *data transfer* between reader and transponder in an RFID system requires three main functional blocks. From the reader to the transponder — the direction of data transfer — these are: *signal coding* (*signal processing*) and the *modulator* (*carrier circuit*) in the *reader* (*transmitter*), the *transmission medium* (*channel*), and the *demodulator* (*carrier circuit*) and *signal decoding* (*signal processing*) in the *transponder* (*receiver*).

A signal coding system takes the message to be transmitted and its *signal representation* and matches it optimally to the characteristics of the *transmission channel*. This process involves providing the message with some degree of protection against interference or collision and against intentional modification of certain signal characteristics (Herter and Lörcher, 1987). Signal coding should not be confused with modulation, and therefore it is referred to as *coding in the baseband*.

Modulation is the process of altering the signal parameters of a high frequency carrier, i.e. its amplitude, frequency or phase, in relation to a modulated signal, the baseband signal.

The transmission medium transmits the message over a predetermined distance. The only transmission media used in RFID systems are magnetic fields (inductive coupling) and electromagnetic waves (microwaves).

Demodulation is an additional modulation procedure to reclaim the signal in the baseband. As there is often an *information source* (input) in both the transponder and the reader, and information is thus transmitted alternately in both directions, these components contain both a *modulator* and a *demodulator*. This is therefore known as a *modem* (**Mo**dulator — **Dem**odulator), a term that describes the normal configuration (Herter and Lörcher, 1987).

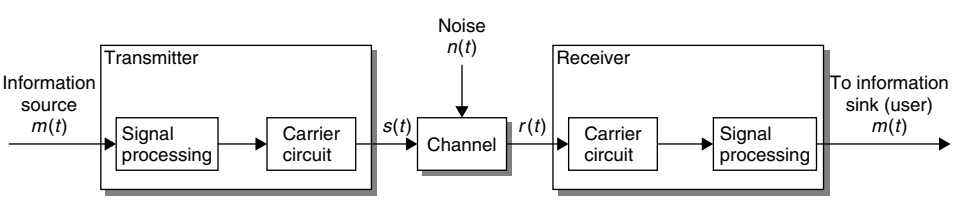


Figure 6.1 Signal and data flow in a digital communications system (Couch, 1997)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The task of signal decoding is to reconstruct the original message from the baseband coded *received signal* and to recognise any *transmission errors* and flag them as such.

6.1 Coding in the Baseband

Binary ones and zeros can be represented in various *line codes*. RFID systems normally use one of the following coding procedures: NRZ, Manchester, Unipolar RZ, DBP (differential bi-phase), Miller, differential coding on PP coding (Figure 6.2).

NRZ code A binary 1 is represented by a 'high' signal and a binary 0 is represented by a 'low' signal. The NRZ code is used almost exclusively with FSK or PSK modulation.

Manchester code A binary 1 is represented by a negative transition in the half bit period and a binary 0 is represented by a positive transition. The Manchester code is therefore also known as *split-phase coding* (Couch, 1997).

The Manchester code is often used for data transmission from the transponder to the reader based upon load modulation using a subcarrier.

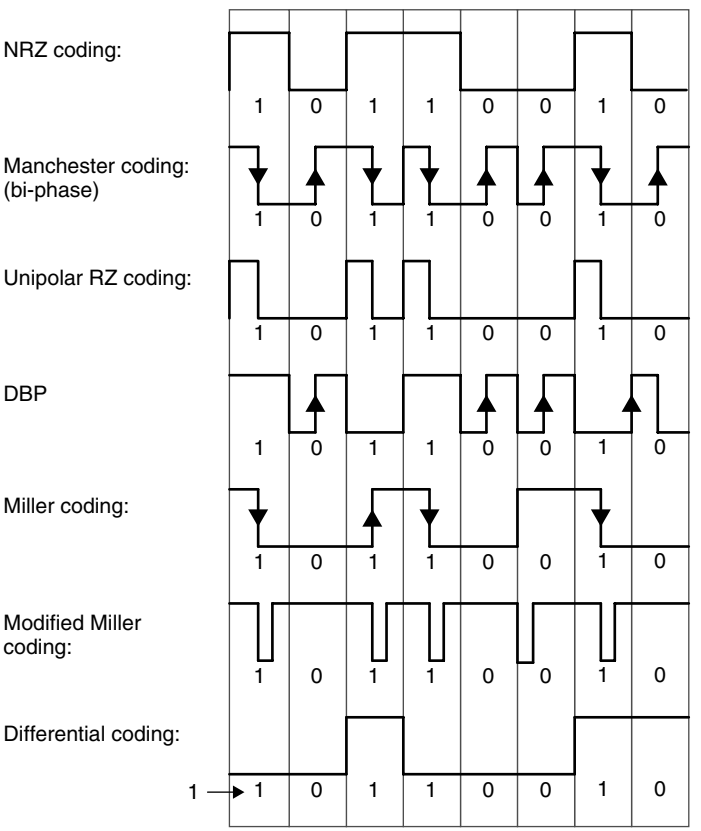


Figure 6.2 Signal coding by frequently changing line codes in RFID systems

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Unipolar RZ code A binary 1 is represented by a 'high' signal during the first half bit period, a binary 0 is represented by a 'low' signal lasting for the entire duration of the bit.

DBP code A binary 0 is coded by a transition of either type in the half bit period, a binary 1 is coded by the lack of a transition. Furthermore, the level is inverted at the start of every bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).

Miller code A binary 1 is represented by a transition of either type in the half bit period, a binary 0 is represented by the continuance of the 1 level over the next bit period. A sequence of zeros creates a transition at the start of a bit period, so that the bit pulse can be more easily reconstructed in the receiver (if necessary).

Modified Miller code In this variant of the Miller code each transition is replaced by a 'negative' pulse. The modified Miller code is highly suitable for use in inductively coupled RFID systems for data transfer from the reader to the transponder.

Due to the very short pulse durations ($t_{\text{pulse}} \ll T_{\text{bit}}$) it is possible to ensure a continuous power supply to the transponder from the HF field of the reader even during data transfer.

Differential coding In 'differential coding' every binary 1 to be transmitted causes a change (toggle) in the signal level, whereas the signal level remains unchanged for a binary zero. Differential coding can be generated very simply from an NRZ signal by using an XOR gate and a D flip-flop. Figure 6.3 shows a circuit to achieve this.

Pulse-pause coding In pulse-pause coding (PPC) a binary 1 is represented by a pause of duration t before the next pulse; a binary 0 is represented by a pause of duration $2t$ before the next pulse (Figure 6.4). This coding procedure is popular in inductively coupled RFID systems for data transfer from the reader to the transponder. Due to the very short pulse durations ($t_{\text{pulse}} \ll T_{\text{bit}}$) it is possible to ensure a continuous power supply to the transponder from the HF field of the reader even during data transfer.

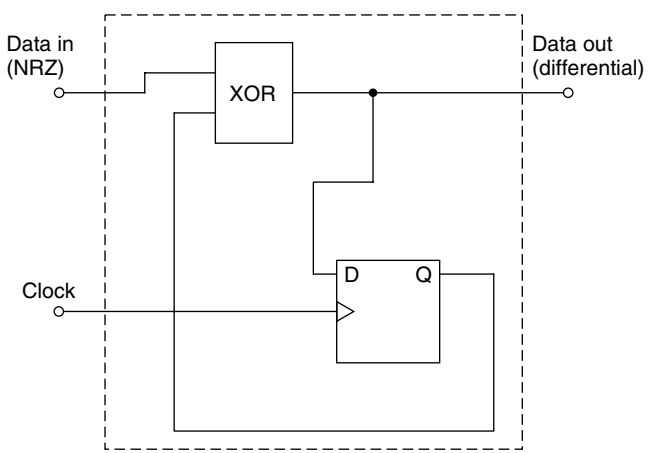


Figure 6.3 Generating differential coding from NRZ coding

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

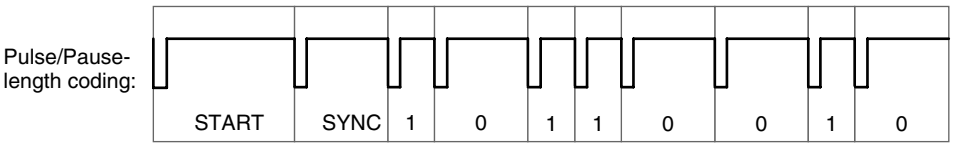


Figure 6.4 Possible signal path in pulse-pause coding

Various boundary conditions should be taken into consideration when selecting a suitable signal coding system for an RFID system. The most important consideration is the signal spectrum after modulation (Couch, 1997; Mäusl, 1985) and susceptibility to transmission errors. Furthermore, in the case of passive transponders (the transponder's power supply is drawn from the HF field of the reader) the power supply must not be interrupted by an inappropriate combination of signal coding and modulation procedures.

6.2 Digital Modulation Procedures

Energy is radiated from an antenna into the surrounding area in the form of electromagnetic waves. By carefully influencing one of three signal parameters — power, frequency, phase position — of an electromagnetic wave, messages can be coded and transmitted to any point within the area. The procedure of influencing an electromagnetic wave by messages (data) is called *modulation*, and an unmodulated electromagnetic wave is called a *carrier*.

By analysing the characteristics of an electromagnetic wave at any point in the area, we can reconstruct the message by measuring the change in reception power, frequency or phase position of the wave. This procedure is known as *demodulation*.

Classical radio technology is largely concerned with analogue modulation procedures. We can differentiate between *amplitude modulation*, *frequency modulation* and *phase modulation*, these being the three main variables of an electromagnetic wave. All other modulation procedures are derived from one of these three types. The procedures used in RFID systems are the digital modulation procedures *ASK* (amplitude shift keying), *FSK* (frequency shift keying) and *PSK* (phase shift keying) (Figure 6.5).

In every modulation procedure symmetric *modulation products* — so-called *sidebands* — are generated around the carrier. The spectrum and amplitude of the sidebands are influenced by the spectrum of the code signal in the baseband and by the modulation procedure. We differentiate between the upper and lower sideband.

6.2.1 Amplitude shift keying (ASK)

In *amplitude shift keying* the amplitude of a *carrier oscillation* is switched between two states u_0 and u_1 (keying) by a binary code signal. U_1 can take on values between u_0 and 0. The ratio of u_0 to u_1 is known as the *duty factor* m.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

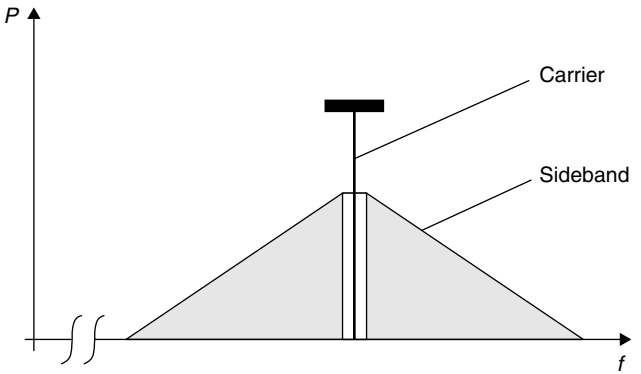


Figure 6.5 Each modulation of a sinusoidal signal — the carrier — generates so-called (modulation) sidebands

To find the duty factor m we calculate the arithmetic mean of the keyed and unkeyed amplitude of the carrier signal:

$$\hat{u}_{\mathrm{m}} = \frac{\hat{u}_0 + \hat{u}_1}{2} \tag{6.1}$$

The duty factor is now calculated from the ratio of amplitude change $\hat{u}_0 - \hat{u}_{\mathrm{m}}$ to the mean value $\hat{u}_{\mathrm{m}}$:

$$m = \frac{\Delta\hat{u}_{\mathrm{m}}}{\hat{u}_{\mathrm{m}}} = \frac{\hat{u}_0 - \hat{u}_{\mathrm{m}}}{\hat{u}_{\mathrm{m}}} = \frac{\hat{u}_0 - \hat{u}_1}{\hat{u}_0 + \hat{u}_1} \tag{6.2}$$

In 100% ASK the amplitude of the carrier oscillation is switched between the carrier amplitude values $2\hat{u}_{\mathrm{m}}$ and 0 (*On-Off keying*; Figure 6.6). In amplitude modulation using an analogue signal (sinusoidal oscillation) this would also correspond with a modulation factor of $m = 1$ (or 100%) (Mäusl, 1985).

The procedure described for calculating the duty factor is thus the same as that for the calculation of the modulation factor for amplitude modulation using analogue

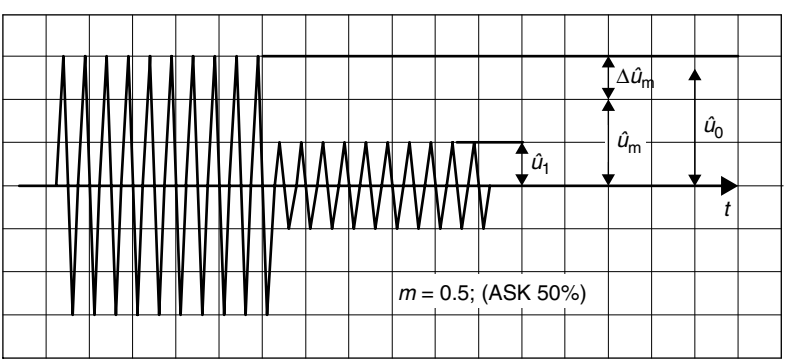


Figure 6.6 In ASK modulation the amplitude of the carrier is switched between two states by a binary code signal

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

signals (sinusoidal oscillation). However, there is one significant difference between keying and analogue modulation. In keying, a carrier takes on the amplitude $\hat{u}_0$ in the unmodulated state, whereas in analogue modulation the carrier signal takes on the amplitude $\hat{u}_m$ in the unmodulated state.

In the literature the duty factor is sometimes referred to as the percentage carrier reduction m' during keying:

$$m' = 1 - \frac{\hat{u}_1}{\hat{u}_0} \tag{6.3}$$

For the example in Figure 6.7 the duty factor would be $m' = 0.66$ ($= 66\%$). In the case of duty factors $<15\%$ and duty factors $>85\%$ the differences between the two calculation methods can be disregarded.

The binary code signal consists of a sequence of 1 and 0 states, with a period duration T and a bit duration τ. From a mathematical point of view, ASK modulation is achieved by multiplying this code signal $u_{code}(t)$ by the carrier oscillation $u_{Cr}(t)$. For duty factors $m < 1$ we introduce an additional constant $(1 - m)$, so for this case we can still multiply $u_{HF}(t)$ by 1 in the unkeyed state:

$$U_{ASK}(t) = (m \cdot u_{code}(t) + 1 - m) \cdot u_{HF}(t) \tag{6.4}$$

The spectrum of ASK signals is therefore found by the convolution of the code signal spectrum with the carrier frequency f_{Cr} or by multiplication of the Fourier expansion of the code signal by the carrier oscillation. It contains the spectrum of the code signal in the upper and lower sideband, symmetric to the carrier (Mäusl, 1985).

A regular, pulse-shaped signal of period duration T and bit duration τ yields the spectrum of Table 6.1 (see also Figure 6.8).

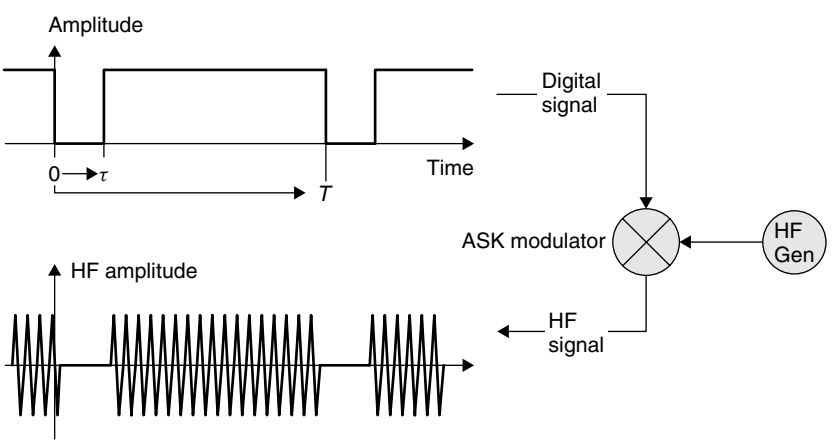


Figure 6.7 The generation of 100% ASK modulation by the keying of the sinusoidal carrier signal from a HF generator into an ASK modulator using a binary code signal

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 6.1 Spectral lines for a pulse-shaped modulated carrier oscillation

Designation	Frequency	Amplitude
Carrier oscillation	f_{CR}	$u_{HF} \cdot (1 - m) \cdot (T - \tau)/T$
1st spectral line	$f_{CR} \pm 1/T$	$u_{HF} \cdot m \cdot \sin(\pi \cdot \tau/T)$
2nd spectral line	$f_{CR} \pm 2/T$	$u_{HF} \cdot m \cdot \sin(2\pi \cdot \tau/T)$
3rd spectral line	$f_{CR} \pm 3/T$	$u_{HF} \cdot m \cdot \sin(3\pi \cdot \tau/T)$
nth spectral line	$f_{CR} \pm n/T$	$u_{HF} \cdot m \cdot \sin(n\pi \cdot \tau/T)$

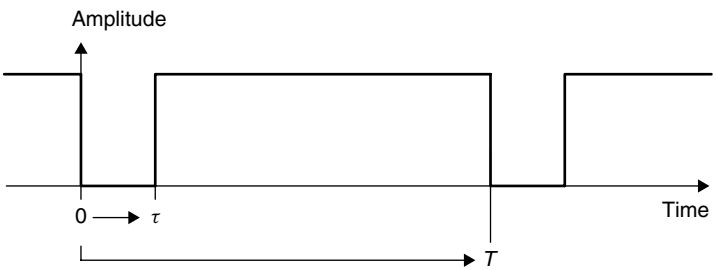


Figure 6.8 Representation of the period duration T and the bit duration τ of a binary code signal

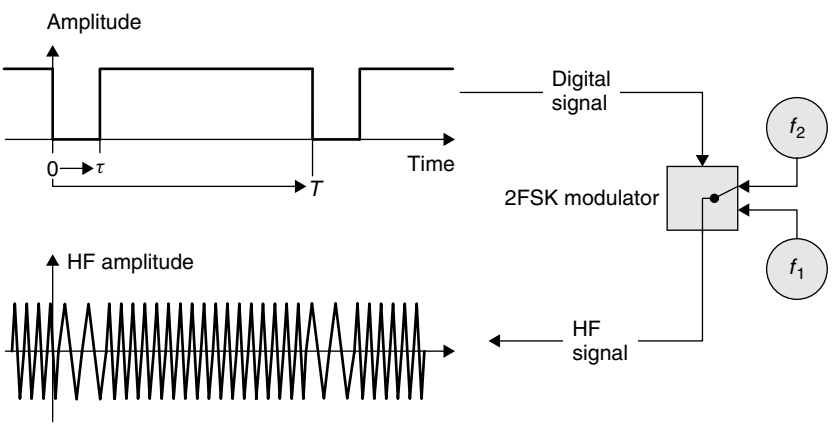


Figure 6.9 The generation of 2 FSK modulation by switching between two frequencies f_1 and f_2 in time with a binary code signal

6.2.2 2 FSK

In *2 frequency shift keying* the frequency of a carrier oscillation is switched between two frequencies f_1 and f_2 by a binary code signal (Figure 6.9).

The carrier frequency f_{CR} is defined as the arithmetic mean of the two characteristic frequencies f_1 and f_2. The difference between the carrier frequency and the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

characteristic frequencies is termed the frequency deviation Δf_{CR}:

$$f_{CR} = \frac{f_1 + f_2}{2} \quad \Delta f_{CR} = \frac{|f_1 + f_2|}{2} \tag{6.5}$$

From the point of view of the time function, the *2 FSK* signal can be considered as the composition of two amplitude shift keyed signals of frequencies f_1 and f_2. The spectrum of a 2 FSK signal is therefore obtained by superimposing the spectra of the two amplitude shift keyed oscillations (Figure 6.10). The baseband coding used in RFID systems produces an asymmetric frequency shift keying:

$$\tau \neq \frac{T}{2} \tag{6.6}$$

In these cases there is also an asymmetric distribution of spectra in relation to the mid-frequency Δf_{CR} (Mäusl, 1985).

6.2.3 2 PSK

In *phase shift keying* the binary states '0' and '1' of a code signal are converted into corresponding phase states of the carrier oscillation, in relation to a reference phase. In 2 PSK the signal is switched between the phase states 0° and 180°.

Mathematically speaking, the shift keying of the phase position between 0° and 180° corresponds with the multiplication of the carrier oscillation by 1 and −1.

The power spectrum of a 2 PSK can be calculated as follows for a mark-space ratio τ/T of 50% (Mansukhani, 1996):

$$P(f) = \left(\frac{P \cdot T_s}{2}\right) \cdot [\sin c^2 \pi (f - f_0) T_s + \sin c^2 \pi (f + f_0) T_s] \tag{6.7}$$

where P is transmitter power, T_s is bit duration ($= \tau$), f_0 is centre frequency, and $\sin c(x) = (\sin(x)/x)$.

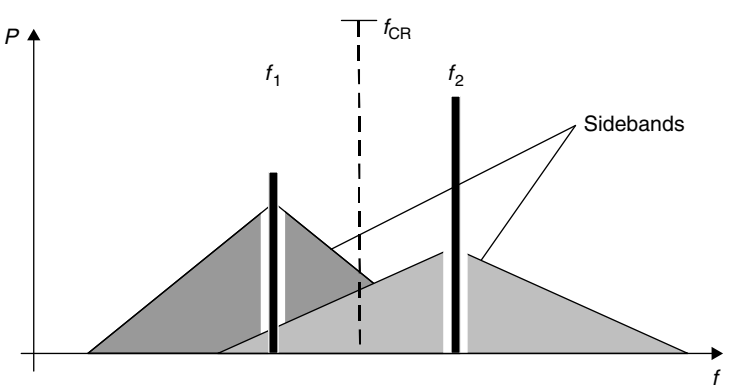


Figure 6.10 The spectrum of a 2 FSK modulation is obtained by the addition of the individual spectra of two amplitude shift keyed oscillations of frequencies f_1 and f_2

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

The envelope of the two sidebands around the carrier frequency f_0 follows the function $(\sin(x)/x)^2$. This yields zero positions at the frequencies $f_0 \pm 1/T_s$, $f_0 \pm 2/T_S$, $f_0 \pm n/T_S$. In the frequency range $f_0 \pm 1/T_S$, 90% of the transmitter power is transmitted. See Figure 6.11.

6.2.4 Modulation procedures with subcarrier

The use of a modulated *subcarrier* is widespread in radio technology. In VHF broadcasting, a stereo subcarrier with a frequency of 38 kHz is transmitted along with the baseband tone channel. The baseband contains only the monotone signal. The differential 'L−R' signal required to obtain the 'L' and 'R' tone channels can be transmitted 'silently' by the modulation of the stereo subcarrier. The use of a subcarrier therefore represents a *multilevel modulation*. Thus, in our example, the subcarrier is first modulated with the differential signal, in order to finally modulate the VHF transmitter once again with the modulated subcarrier signal (Figure 6.12).

In RFID systems, modulation procedures using a subcarrier are primarily used in inductively coupled systems in the frequency ranges 6.78 MHz, 13.56 MHz or 27.125 MHz and in load modulation for data transfer from the transponder to the reader. The load modulation of an inductively coupled RFID system has a similar effect to ASK modulation of HF voltage at the antenna of the reader. Instead of switching the *load resistance* on and off in time with a baseband coded signal, a low frequency subcarrier is first modulated by the baseband coded data signal. ASK, FSK or PSK modulation may be selected as the modulation procedure for the subcarrier. The *subcarrier frequency* itself is normally obtained by the binary division of the operating frequency. For 13.56 MHz systems, the subcarrier frequencies 847 kHz (13.56 MHz ÷ 16), 424 kHz (13.56 Mhz ÷ 32) or 212 kHz (13.56 MHz ÷ 64) are usually used. The modulated subcarrier signal is now used to switch the load resistor on and off.

The great advantage of using a subcarrier only becomes clear when we consider the frequency spectrum generated. Load modulation with a subcarrier initially generates

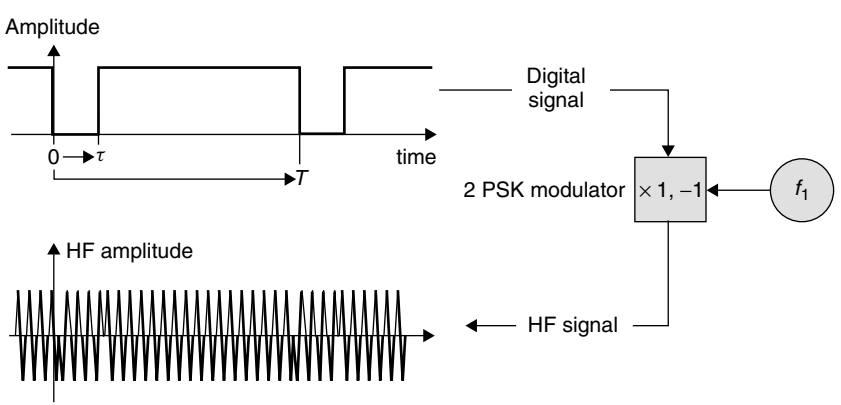


Figure 6.11 Generation of the 2 PSK modulation by the inversion of a sinusoidal carrier signal in time with a binary code signal

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

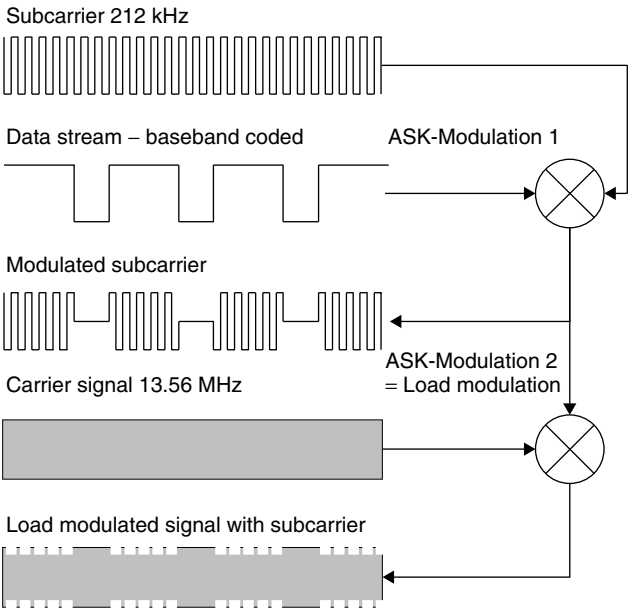


Figure 6.12 Step-by-step generation of a multiple modulation, by load modulation with ASK modulated subcarrier

two spectral lines at a distance ± the subcarrier frequency f_H around the operating frequency (Figure 6.12). The actual information is now transmitted in the sidebands of the two subcarrier lines, depending upon the modulation of the subcarrier with the baseband coded data stream. If load modulation in the baseband were used, on the other hand, the sidebands of the data stream would lie directly next to the carrier signal at the operating frequency.

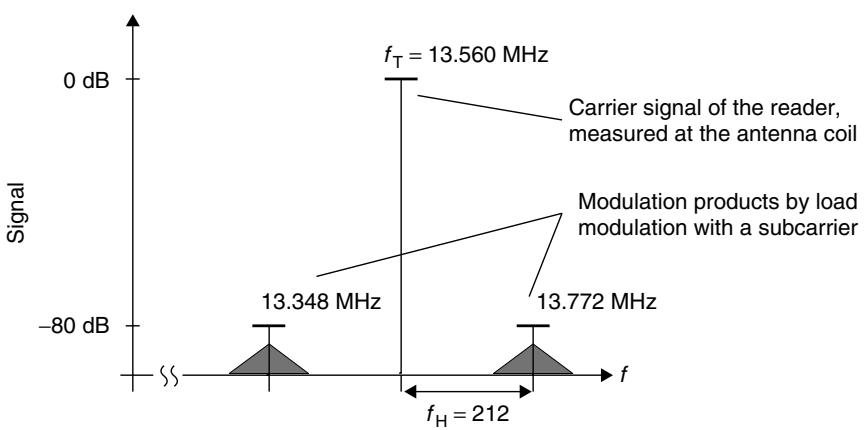


Figure 6.13 Modulation products using load modulation with a subcarrier

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

In very loosely coupled transponder systems the difference between the carrier signal of the reader f_T and the received modulation sidebands of the load modulation varies within the range 80–90 dB (Figure 6.13). One of the two subcarrier modulation products can be filtered out and demodulated by shifting the frequency of the modulation sidebands of the data stream. It is irrelevant here whether the frequencies $f_T + f_H$ or $f_T - f_H$ are used, because the information is contained in all sidebands.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

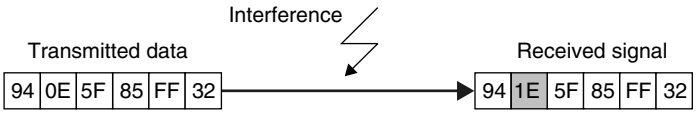


Figure 7.1 Interference during transmission can lead to errors in the data

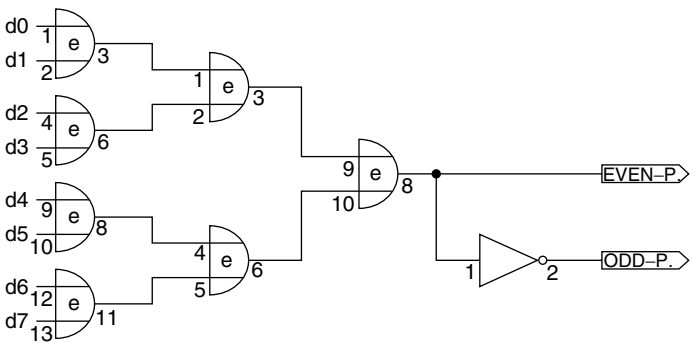


Figure 7.2 The parity of a byte can be determined by performing multiple exclusive-OR logic gating operations on the individual bits

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

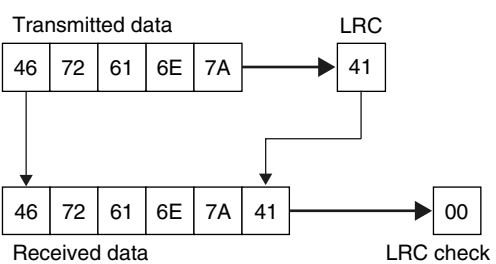


Figure 7.3 If the LCR is appended to the transmitted data, then a new LRC calculation incorporating all received data yields the checksum 00h. This permits a rapid verification of data integrity without the necessity of knowing the actual LRC sum

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.'

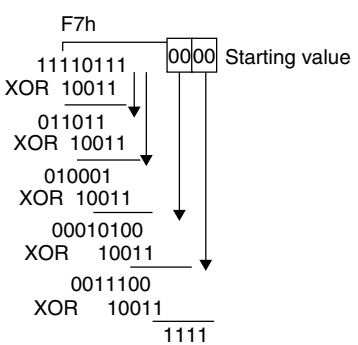


Figure 7.4 Step-by-step calculation of a CRC checksum

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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: $x^{16} + x^{12} + x^5 + 1$

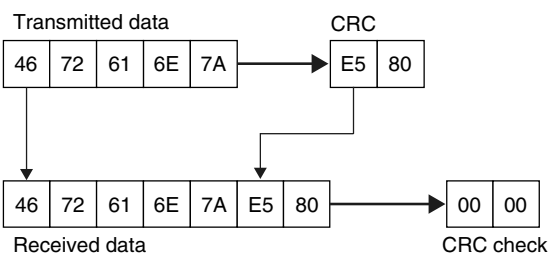


Figure 7.5 If the CRC is appended to the transmitted data a repeated CRC calculation of all received data yields the checksum 0000h. This facilitates the rapid checking of data integrity without knowing the CRC total

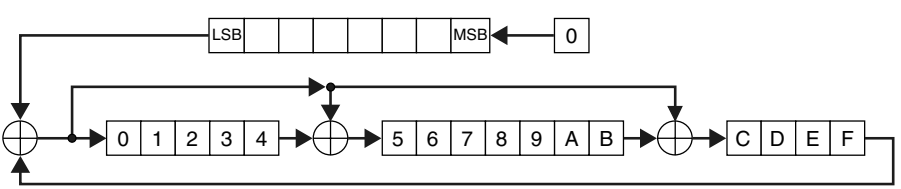


Figure 7.6 Operating principle for the generation of a CRC-16/CCITT by shift registers

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

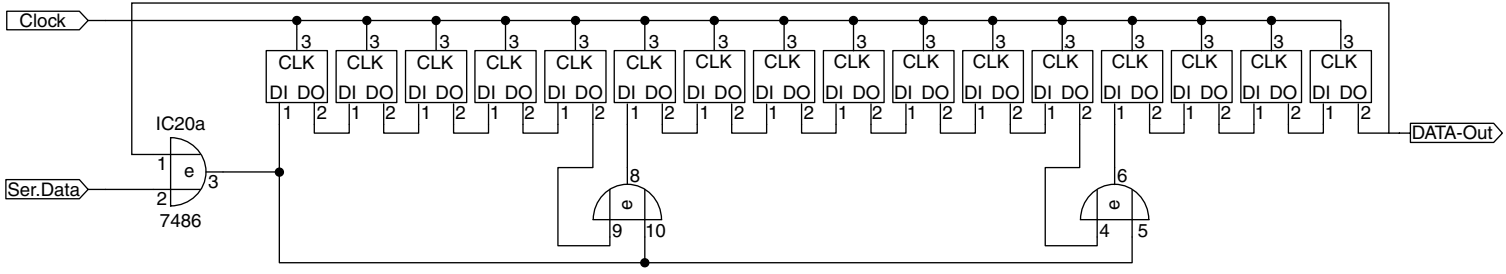


Figure 7.7 The circuit for the shift register configuration outlined in the text for the calculation of a CRC 16/CCITTT

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

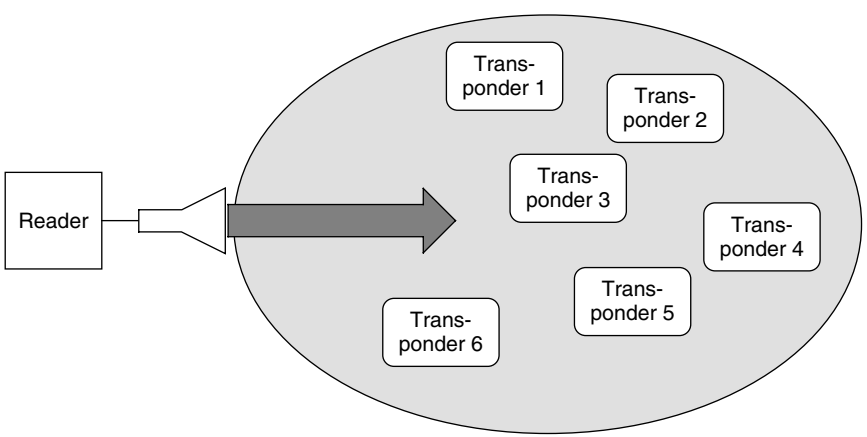


Figure 7.8 Broadcast mode: the data stream transmitted by a reader is received simultaneously by all transponders in the reader's interrogation zone

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

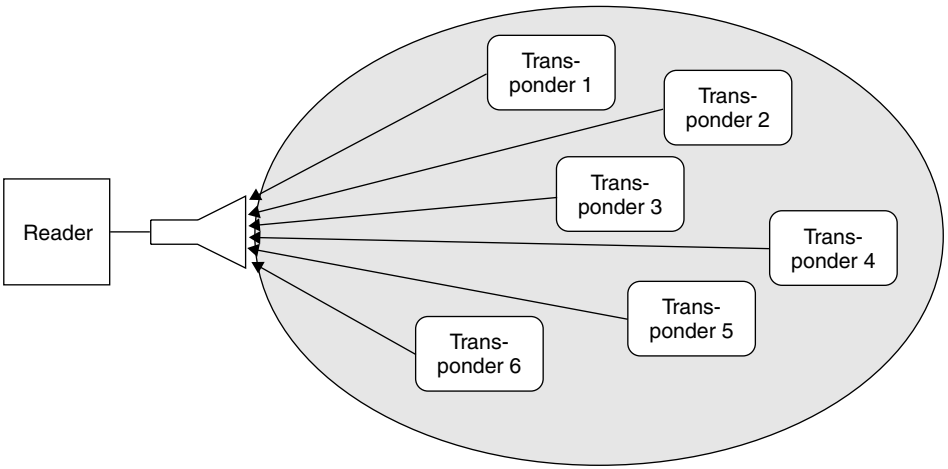


Figure 7.9 Multi-access to a reader: numerous transponders attempt to transfer data to the reader simultaneously

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

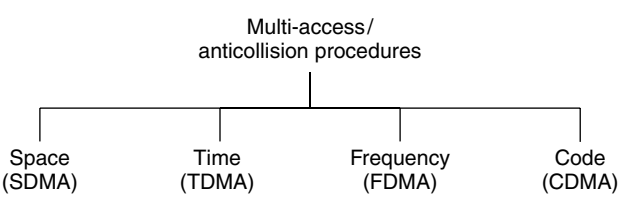


Figure 7.10 Multi-access and anticollision procedures are classified on the basis of four basic procedures

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

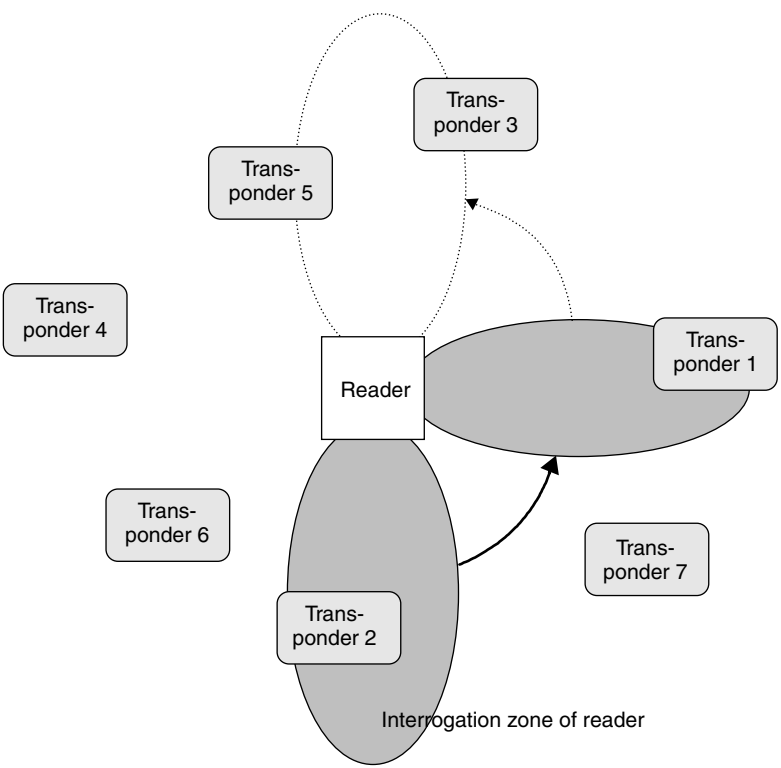


Figure 7.11 Adaptive SDMA with an electronically controlled directional antenna. The directional beam is pointed at the various transponders one after the other

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

7.2.2 Frequency domain multiple access (FDMA)

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

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

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

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

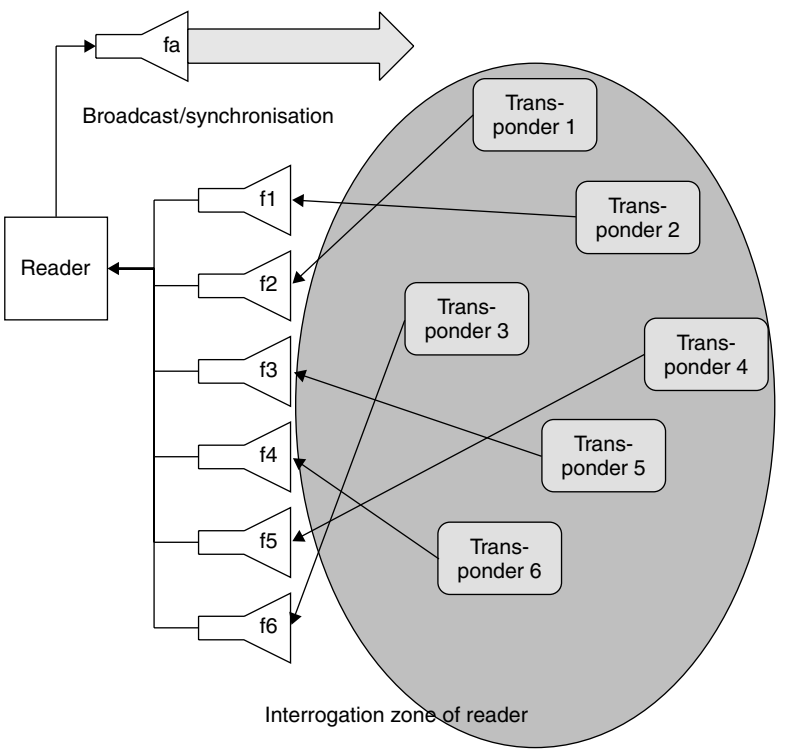


Figure 7.12 In an FDMA procedure several frequency channels are available for the data transfer from the transponders to the reader

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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:

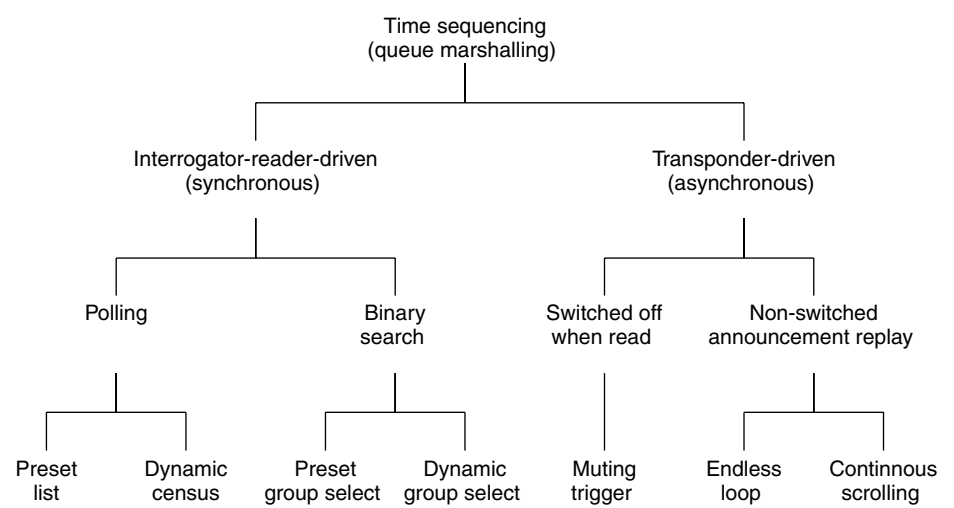


Figure 7.13 Classification of time domain anticollision procedures according to Hawkes (1997).

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

7.2.4 Examples of anticollision procedures

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

7.2.4.1 ALOHA procedure

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

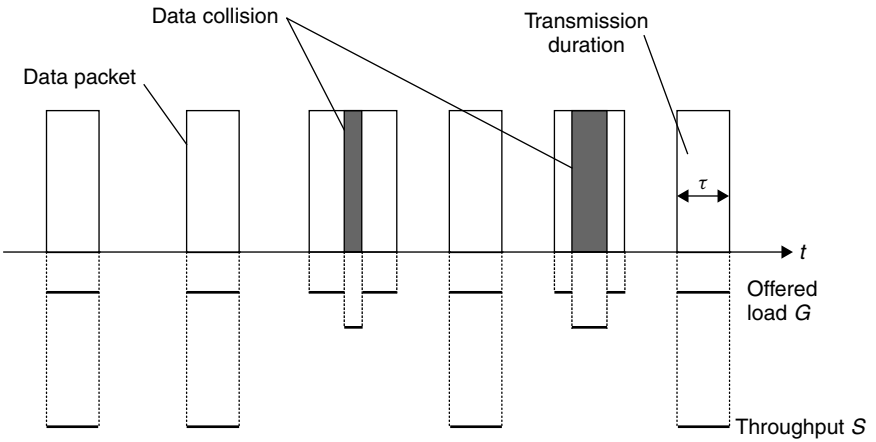


Figure 7.14 Definition of the offered load G and throughput S of an ALOHA system: several transponders send their data packets at random points in time. Now and then this causes data collisions, as a result of which the (data) throughput S falls to zero for the data packets that have collided

where $n = 1, 2, 3, \ldots$ is the number of transponders in the system and $r_n = 0, 1, 2, \ldots$ 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).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 τ of a data packet and the average offered load G. The probability $p(k)$ is a Poisson's distribution[2] with the mean value G/τ:

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

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 τ) 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).

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

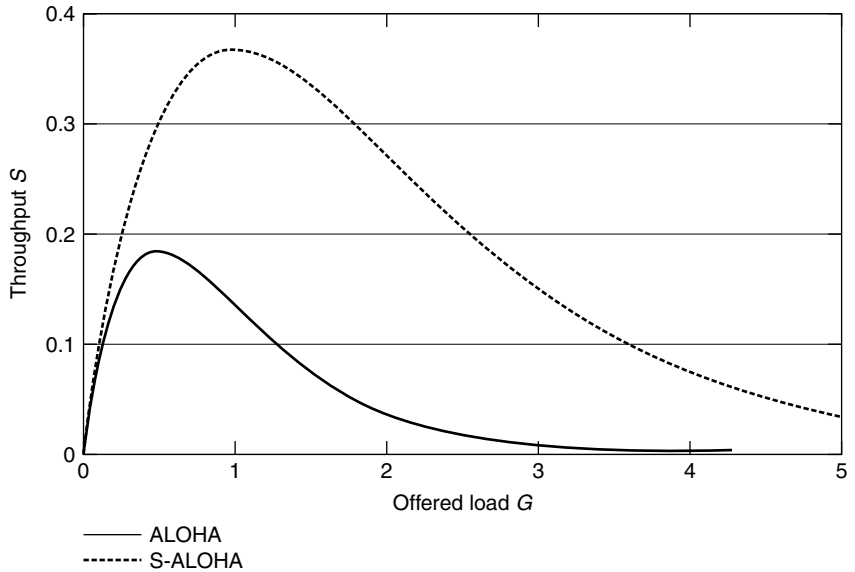


Figure 7.15 Comparison of the throughput curves of ALOHA and S-ALOHA. In both procedures the throughput tends towards zero as soon as the maximum has been exceeded

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

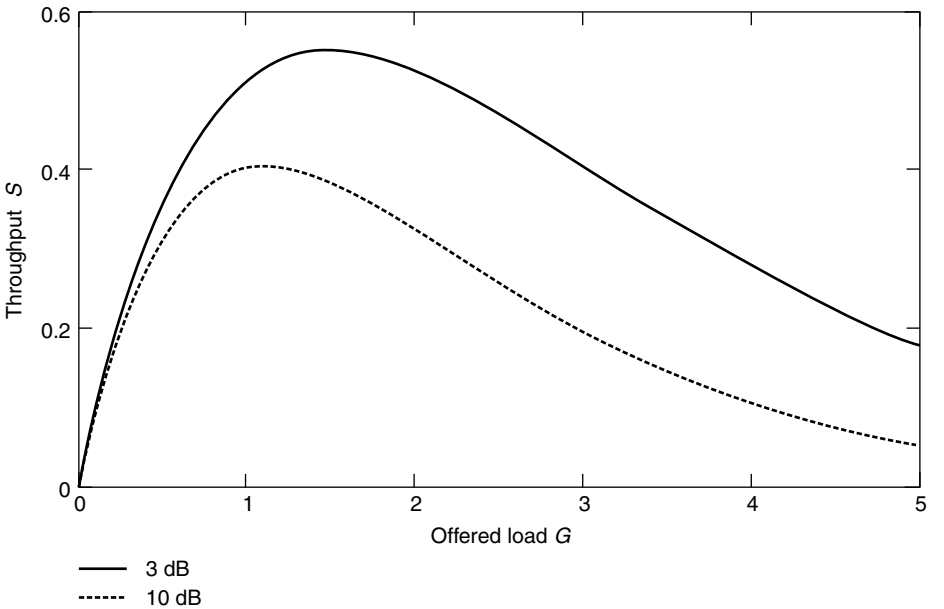


Figure 7.16 Throughput behaviour taking into account the capture effect with thresholds of 3 dB and 10 dB

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

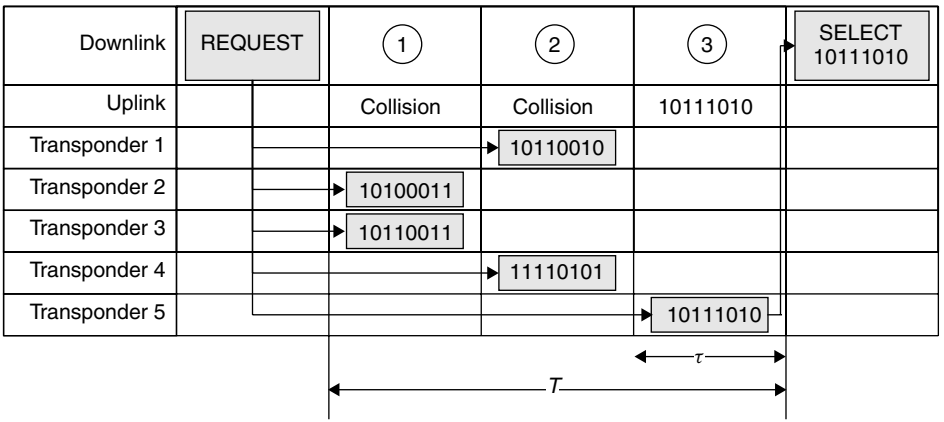


Figure 7.17 Transponder system with slotted ALOHA anticollision procedure

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).

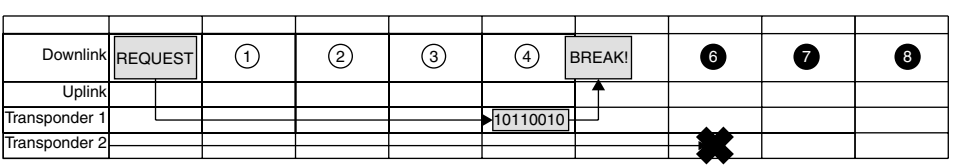


Figure 7.18 Dynamic S-ALOHA procedure with BREAK command. After the serial number of transponder 1 has been recognised without errors, the response of any further transponders is suppressed by the transmission of a BREAK command

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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_{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_{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

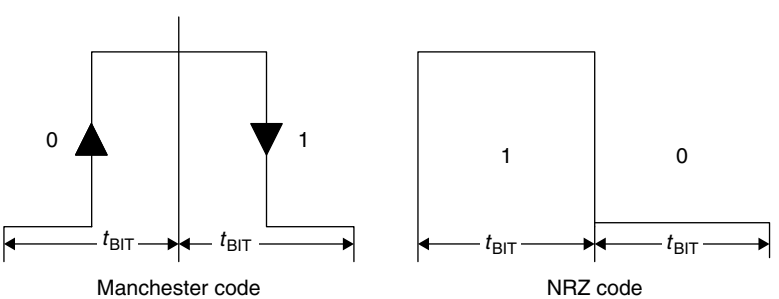


Figure 7.19 Bit coding using Manchester and NRZ code

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

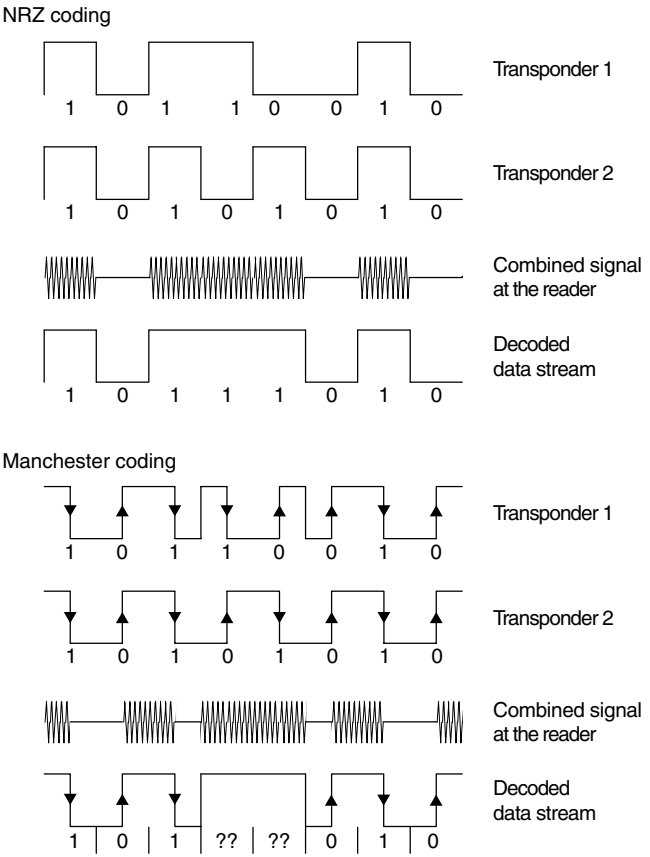


Figure 7.20 Collision behaviour for NRZ and Manchester code. The Manchester code makes it possible to trace a collision to an individual bit

are to guarantee the uniqueness of the addresses (serial numbers) a maximum of 256 transponders can be issued.

The use of the commands defined in Table 7.3 in a binary search algorithm will now be demonstrated based upon a procedure with four transponders in the interrogation zone of the reader. The transponders in our example possess unique serial numbers in the range 00–FFh (= 0 – 255 dec. or 00000000 – 11111111 bin.) (Table 7.4).

The first iteration of the algorithm begins with the transmission of the command **REQUEST (≤11111111)** by the reader. The serial number 11111111b is the highest possible in our example system using 8-bit serial numbers. The serial numbers of all transponders in the interrogation zone of the reader must therefore be less than or equal to 11111111b, so this command is answered by all transponders in the interrogation zone of the reader (see Figure 7.21).

The precise synchronisation of all transponders, so that they begin to transmit their serial numbers at exactly the same time, is decisive for the reliable function of the *binary tree search algorithm*. Only in this manner is the determination of the precise bit position of a collision possible.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 **less than** (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 SNR $\geq$ 1**1**000000b and also in SNR $\leq$ 1**0**111111b.[3] 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$10111111b. 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.

[3] 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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

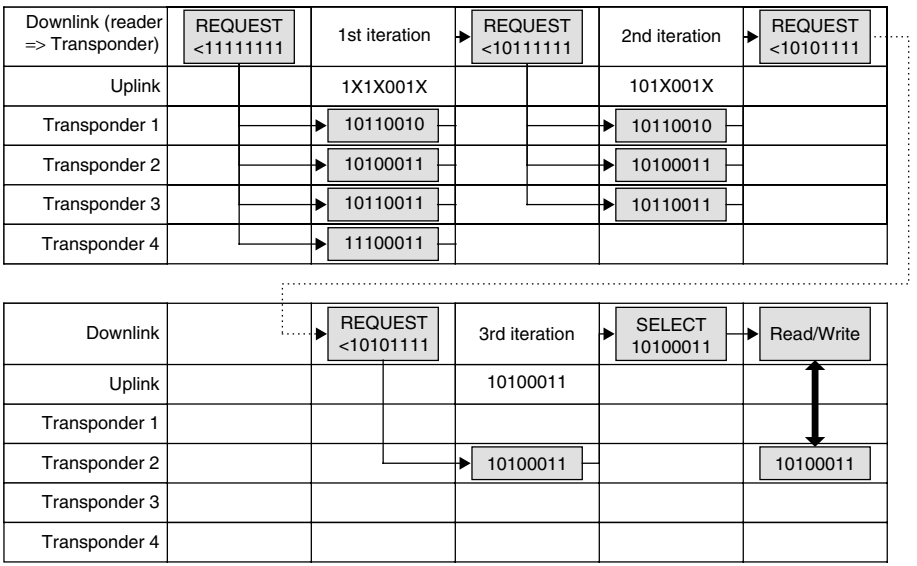


Figure 7.21 The different serial numbers that are sent back from the transponders to the reader in response to the REQUEST command lead to a collision. By the selective restriction of the preselected address range in further iterations, a situation can finally be reached in which only a single transponder 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**	001	**X**
Possible serial number A	1	**0**	1	**0**	001	**0**
Possible serial number B*	1	**0**	1	**0**	001	**1**
Possible serial number C*	1	**0**	1	**1**	001	**0**
Possible serial number D*	1	**0**	1	**1**	001	**1**
Possible serial number E	1	**1**	1	**0**	001	**0**
Possible serial number F*	1	**1**	1	**0**	001	**1**
Possible serial number G	1	**1**	1	**1**	001	**0**
Possible serial number H	1	**1**	1	**1**	001	**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 101**X**001**X** still permits four options for the serial numbers that remain to be detected (Table 7.7).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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	*n*th iteration range =
REQUEST ≥ Range	0	Bit(X) = 1, Bit(0 to X − 1) = 0
REQUEST ≤ Range	SNRmax	Bit(X) = 0, Bit(0 to X − 1) = 1

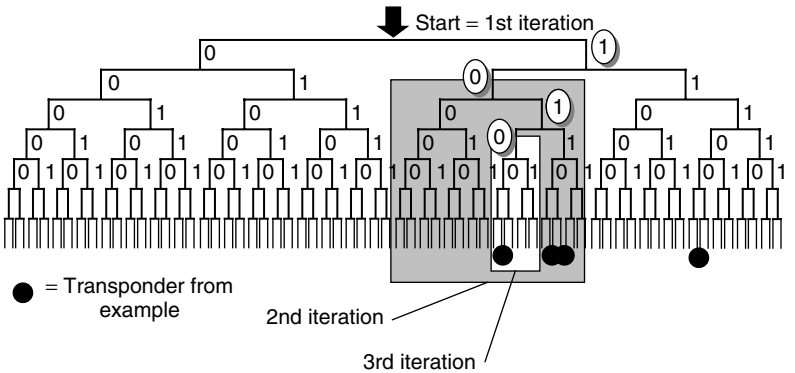


Figure 7.22 Binary search tree. An individual transponder can finally be selected by a successive reduction of the range

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:	765	4	321	0
Received data at reader	101	**X**	001	**X**
Possible serial number A	101	**0**	001	**0**
Possible serial number B*	101	**0**	001	**1**
Possible serial number C*	101	**1**	001	**0**
Possible serial number D*	101	**1**	001	**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 ≤10101111. The reader now transmits to the transponders the command REQUEST (≤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.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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:

$$L(N) = ld(N) + 1 = \frac{\log(N)}{\log(2)} + 1 \tag{7.7}$$

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:

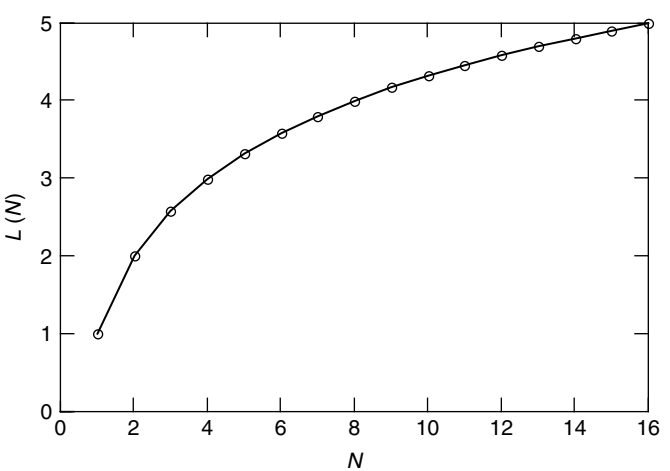


Figure 7.23 The average number of iterations needed to determine the transponder address (serial number) of a single transponder as a function of the number of transponders in the interrogation zone of the reader. When there are 32 transponders in the interrogation zone an average of six iterations are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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

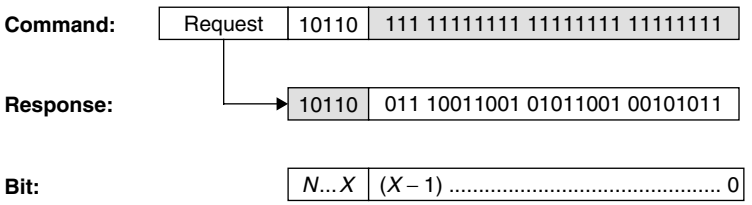


Figure 7.24 Reader's command (*n*th iteration) and transponder's response when a 4-byte serial number has been determined. A large part of the transmitted data in the command and response is redundant (shown in grey). X is used to denote the highest value bit position at which a bit collision occurred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

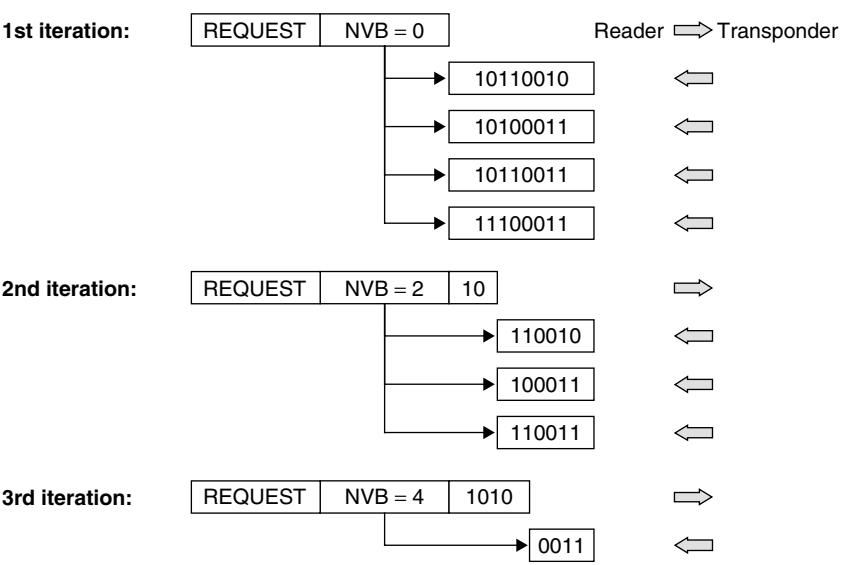


Figure 7.25 The dynamic binary search procedure avoids the transmission of redundant parts of the serial number. The data transmission time is thereby noticeably reduced

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

$((X - 1) - 0)$ 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%.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

8
Data Security

RFID systems are increasingly being used in high security applications, such as access systems and systems for making payments or issuing tickets. However, the use of RFID systems in these applications necessitates the use of security measures to protect against *attempted attacks*, in which people try to trick the RFID system in order to gain unauthorised access to buildings or avail themselves of services (tickets) without paying. This is nothing new — we only have to look to myths and fairy stories to find examples of attempts to outsmart *security systems*. For example, *Ali Baba* was able to gain access to the supposedly secure hideout of the 40 thieves by discovering the secret password.

Modern *authentication protocols* also work by checking knowledge of a secret (i.e. a cryptographic key). However, suitable algorithms can be employed to prevent the secret key being cracked. High security RFID systems must have a defence against the following individual attacks:

- Unauthorised reading of a data carrier in order to duplicate and/or modify data.
- The placing of a foreign data carrier within the interrogation zone of a reader with the intention of gaining unauthorised access to a building or receiving services without payment.
- Eavesdropping into radio communications and replaying the data, in order to imitate a genuine data carrier ('replay and fraud').

When selecting a suitable RFID system, consideration should be given to cryptological functions. Applications that do not require a security function (e.g. industrial automation, tool recognition) would be made unnecessarily expensive by the incorporation of cryptological procedures. On the other hand, in high security applications (e.g. ticketing, payment systems) the omission of cryptological procedures can be a very expensive oversight if manipulated transponders are used to gain access to services without authorisation.

8.1 Mutual Symmetrical Authentication

Mutual authentication between reader and transponder is based upon the principle of three-pass mutual authentication in accordance with *ISO 9798-2*, in which both

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

participants in the communication check the other party's knowledge of a secret (secret cryptological key).

In this procedure, all the transponders and receivers that form part of an application are in possession of the same secret *cryptological key* K ($\rightarrow$ symmetrical procedure). When a transponder first enters the interrogation zone of a reader it cannot be assumed that the two participants in the communication belong to the same application. From the point of view of the reader, there is a need to protect the application from *manipulation* using falsified data. Likewise, on the part of the transponder there is a need to protect the stored data from unauthorised reading or overwriting.

The mutual authentication procedure begins with the reader sending a GET_CHALLENGE command to the transponder. A *random number* R_A is then generated in the transponder and sent back to the reader (response $\rightarrow$ challenge–response procedure). The reader now generates a random number R_B. Using the common secret key K and a common key algorithm e_k, the reader calculates an encrypted data block (token 1), which contains both random numbers and additional control data, and sends this data block to the transponder.

$$\text{Token 1} = e_K(R_B \| R_A \| ID_A \| \text{Text1})$$

The received token 1 is decrypted in the transponder and the random number R'_A contained in the plain text is compared to the previously transmitted R_A. If the two figures correspond, then the transponder has confirmed that the two common keys correspond. Another random number R_{A2} is generated in the transponder and this is used to calculate an encrypted data block (token 2), which also contains R_B and control data. Token 2 is sent from the transponder to the reader.

$$\text{Token 2} = e_K(R_{A2} \| R_B \| \text{Text2})$$

The reader decrypts token 2 and checks whether R_B, which was sent previously, corresponds with R'_B, which has just been received. If the two figures correspond, then the reader is satisfied that the common key has been proven. Transponder and reader have thus ascertained that they belong to the same system and further communication between the two parties is thus legitimised (Figure 8.1).

To sum up, the mutual authentication procedure has the following advantages:

- The secret keys are never transmitted over the airwaves, only encrypted random numbers are transmitted.

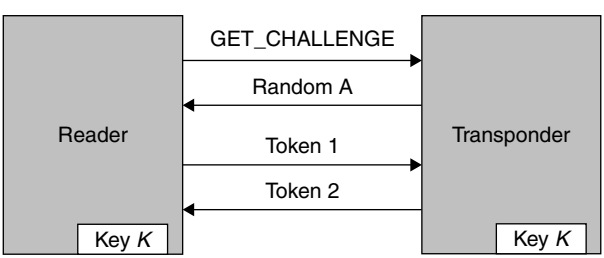


Figure 8.1 Mutual authentication procedure between transponder and reader

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

- Two random numbers are always encrypted simultaneously. This rules out the possibility of performing an inverse transformation using R_A to obtain token 1, with the aim of calculating the secret key.
- The token can be encrypted using any algorithm.
- The strict use of random numbers from two independent sources (transponder, reader) means that recording an authentication sequence for playback at a later date (replay attack) would fail.
- A random key (session key) can be calculated from the random numbers generated, in order to cryptologically secure the subsequent data transmission.

8.2 Authentication Using Derived Keys

One disadvantage of the authentication procedure described in Section 8.1 is that all transponders belonging to an application are secured using an identical cryptological key K. For applications that involve vast quantities of transponders (e.g. the ticketing system for the public transport network, which uses several million transponders) this represents a potential source of danger. Because such transponders are accessible to everyone in uncontrolled numbers, the small probability that the key for a transponder will be discovered must be taken into account. If this occurred, the procedure described above would be totally open to manipulation.

A significant improvement on the authentication procedure described can be achieved by securing each transponder with a different cryptological key. To achieve this, the serial number of each transponder is read out during its production. A key K_X is calculated ($\rightarrow$ derived) using a cryptological algorithm and a *master key* K_M, and the transponder is thus initialised. Each transponder thus receives a key linked to its own ID number and the master key K_M.

The mutual authentication begins by the reader requesting the ID number of the transponder (Figure 8.2). In a special security module in the reader, the *SAM* (security authentication module), the transponder's specific key is calculated using the master key K_M, so that this can be used to initiate the authentication procedure. The SAM

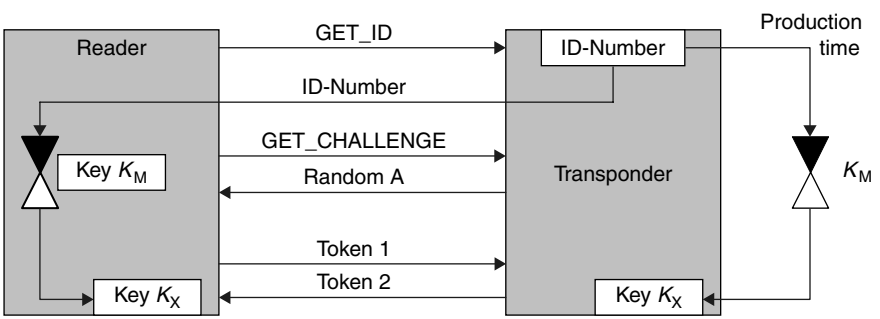


Figure 8.2 In an authentication procedure based upon derived keys, a key unique to the transponder is first calculated in the reader from the serial number (ID number) of the transponder. This key must then be used for authentication

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

normally takes the form of a smart card with contacts incorporating a cryptoprocessor, which means that the stored master key can never be read.

8.3 Encrypted Data Transfer

Chapter 7 described methods of dealing with interference caused by physical effects during data transmission. Let us now extend this model to a potential attacker. We can differentiate between two basic types of attack. Attacker 1 behaves passively and tries to eavesdrop into the transmission to discover confidential information for wrongful purposes. Attacker 2, on the other hand, behaves actively to manipulate the transmitted data and alter it to his benefit. See Figure 8.3.

Cryptological procedures are used to protect against both passive and active attacks. To achieve this, the transmitted data (plain text) can be altered (encrypted) prior to transmission so that a potential attacker can no longer draw conclusions about the actual content of the message (plain text).

Encrypted data transmission always takes place according to the same pattern. The transmission data (plain text) is transformed into cipher data (cipher text) (→ *encryption*, *ciphering*) using a secret *key* K and a secret algorithm. Without knowing the encryption algorithm and the secret key K a potential attacker is unable to interpret the recorded data. It is not possible to recreate the transmission data from the cipher data.

The cipher data is transformed back to its original form in the receiver using the secret key K' and the secret algorithm (→ *decryption*, *deciphering*). See Figure 8.4.

If the keys K for ciphering and K' for deciphering are identical ($K = K'$) or in a direct relationship to each other, the procedure is a *symmetrical key procedure*. If knowledge of the key K is irrelevant to the deciphering process, the procedure is an *asymmetrical key procedure*. RFID systems have for a long time used only symmetrical procedures, therefore we will not describe other procedures in further detail here.

If each character is individually encrypted prior to transmission, the procedure is known as *sequential ciphering* (or *stream ciphering*). If, on the other hand, several characters are incorporated into a block then we talk of a block cipher. Because block

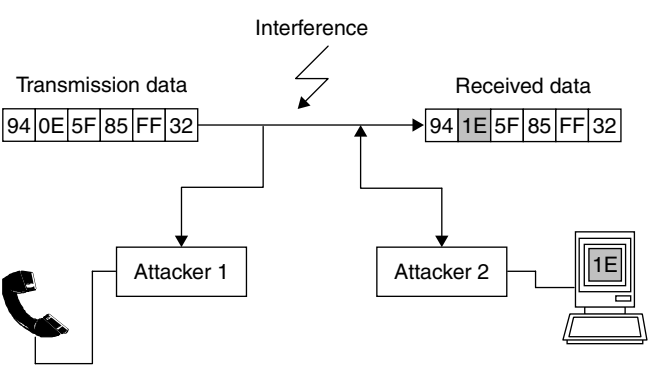


Figure 8.3 Attempted attacks on a data transmission. Attacker 1 attempts to eavesdrop, whereas attacker 2 maliciously alters the data

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

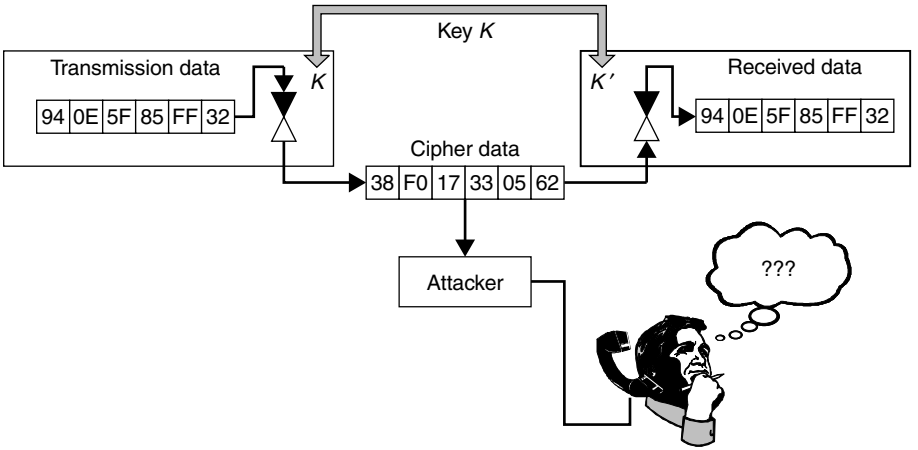


Figure 8.4 By encrypting the data to be transmitted, this data can be effectively protected from eavesdropping or modification

ciphers are generally very calculation intensive, they play a less important role in RFID systems. Therefore the emphasis is placed on sequential ciphers in what follows.

A fundamental problem of all cryptological procedures is the secure distribution of the secret key K, which must be known by the authorised communication participants prior to the start of the data transfer procedure.

8.3.1 Stream cipher

Sequential ciphers or stream ciphers are encryption algorithms in which the sequence of plain text characters is encrypted sequentially using a different function for every step (Fumy, 1994). The ideal realisation of a stream cipher is the so-called *one-time pad*, also known as the *Vernam cipher* after its discoverer (Longo, 1993).

In this procedure a random key K is generated, for example using dice, prior to the transmission of encrypted data, and this key is made available to both parties (Figure 8.5). The key sequence is linked with the plain text sequence by the addition of characters or using XOR gating. The random sequence used as a key must be at least as long as the message to be encrypted, because periodic repetitions of a typically short key in relation to the plain text would permit cryptoanalysis and thus an attack on the transmission. Furthermore, the key may only be used once, which means that an extremely high level of security is required for the secure distribution of keys. Stream ciphering in this form is completely impractical for RFID systems.

To overcome the problem of key generation and distribution, systems have been created based upon the principle of the one-time pad stream cipher, that use a so-called *pseudorandom sequence* instead of an actual random sequence. Pseudorandom sequences are generated using so-called pseudorandom generators.

Figure 8.6 shows the fundamental principle of a sequential cipher using a pseudo-random generator: because the encryption function of a sequential cipher can change (at random) with every character, the function must be dependent not only upon the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

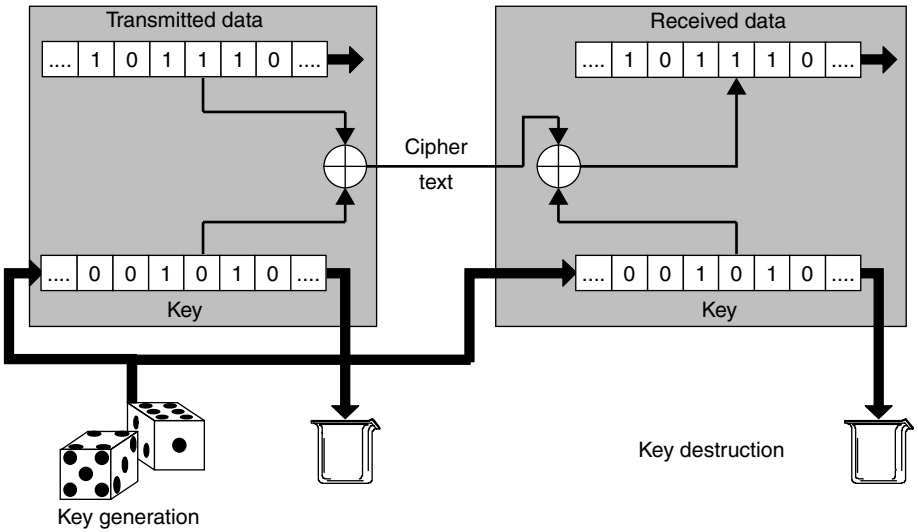


Figure 8.5 In the one-time pad, keys generated from random numbers (dice) are used only once and then destroyed (wastepaper basket). The problem here is the secure transmission of the key between sender and recipient

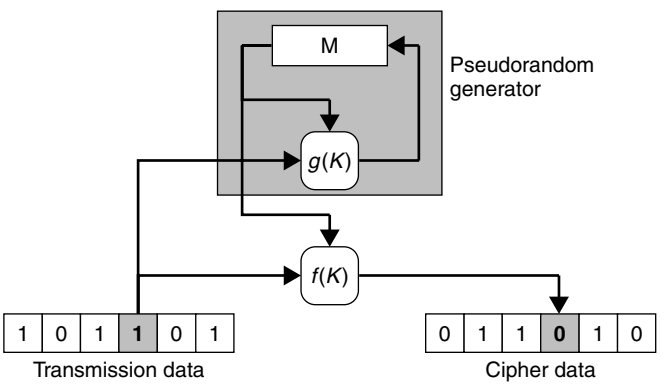


Figure 8.6 The principle underlying the generation of a secure key by a pseudorandom generator

current input character but also upon an additional feature, the internal state M. This internal state M is changed after every encryption step by the state transformation function $g(K)$. The pseudorandom generator is made up of the components M and $g(K)$. The security of the cipher depends principally upon the number of internal states M and the complexity of the transformation function $g(K)$. The study of sequential ciphers is thus primarily concerned with the analysis of pseudorandom generators.

The *encryption function* $f(K)$ itself, on the other hand, is generally very simple and can only comprise an addition or XOR logic gating (Fumy, 1994; Glogau, 1994).

From a circuitry point of view, pseudorandom generators are realised by state machines. These consist of binary storage cells, so-called flip-flops. If a state machine

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

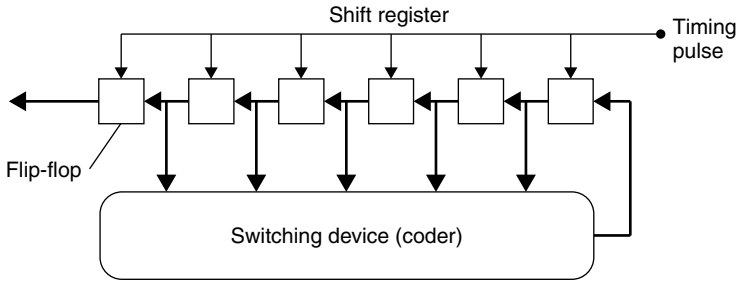


Figure 8.7 Basic circuit of a pseudorandom generator incorporating a linear feedback shift register (LFSR)

has n storage cells then it can take on 2^n different internal M states. The state transformation function $g(K)$ is represented by combinatorial logic (a more detailed explanation of the functionality of state machines can be found in Chapter 10). The implementation and development of pseudorandom generators can be greatly simplified if we restrict ourselves to the use of linear feedback shift registers (Figure 8.7).

A shift register is realised by the serial connection of flip-flops ($output_n$ is connected with $input_{n+1}$) and the parallel connection of all timing inputs. The content of the flip-flop cell is shifted forwards by one position with every timing pulse. The content of the last flip-flop is output (Golomb, 1982; Rueppel, 1986).

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 kHz ± 1.8 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

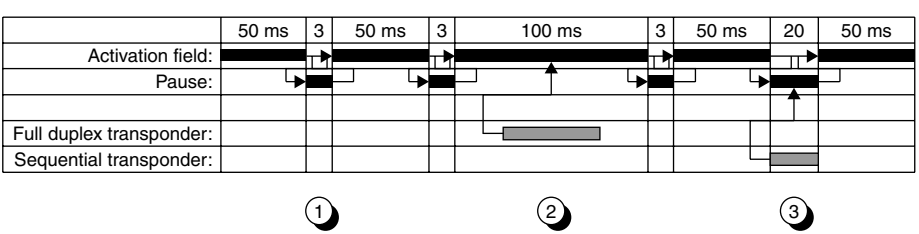


Figure 9.1 Path of the activation field of a reader over time: ① no transponder in interrogation zone, ② full/half duplex (= load modulated) transponder in interrogation zone, ③ sequential transponder in the interrogation zone of the reader

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

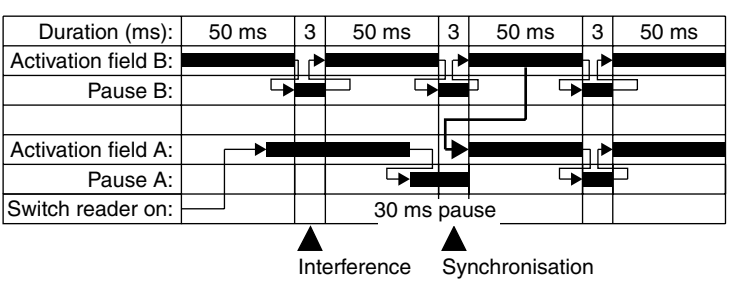


Figure 9.2 Automatic synchronisation sequence between readers A and B. Reader A inserts an extended pause of a maximum of 30 ms after the first transmission pulse following activation so that it can listen for other readers. In the diagram, the signal of reader B is detected during this pause. The reactivation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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 00000000001. 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.

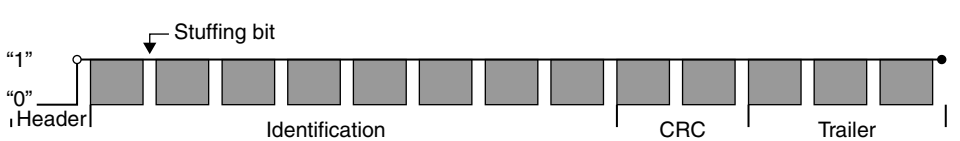


Figure 9.3 Structure of the load modulation data telegram comprising of starting sequence (header), ID code, checksum and trailer

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

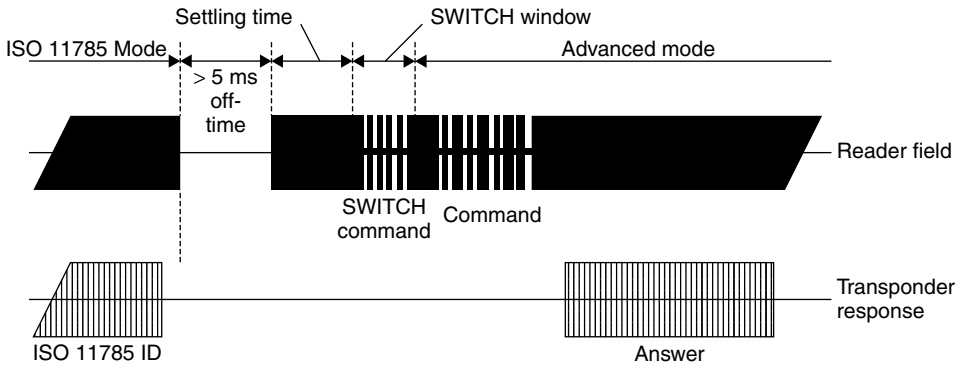


Figure 9.4 Signal path at the antenna of a reader

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/fc = 2.33 ms SWITCH window: 232.5/fc = 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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

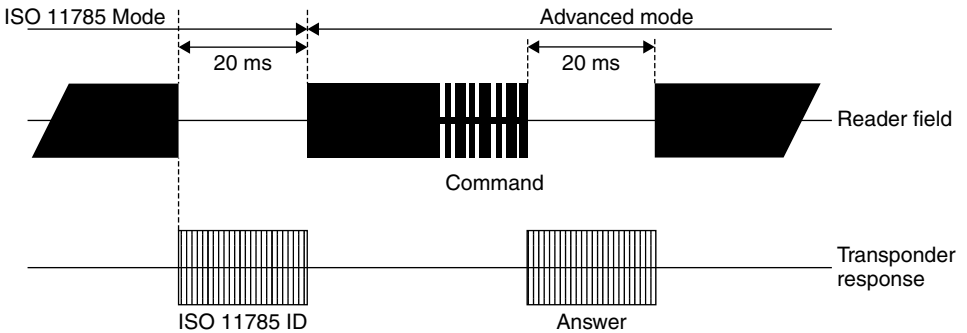


Figure 9.5 A sequential advanced transponder is switched into advanced mode by the transmission of any desired command

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

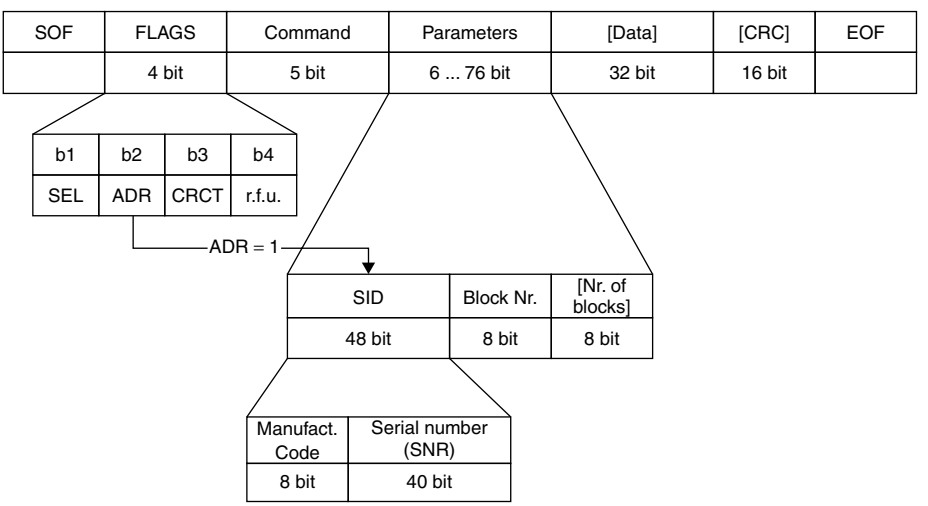


Figure 9.6 Structure of an ISO 14223 command frame for the transmission of data from reader to transponder

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

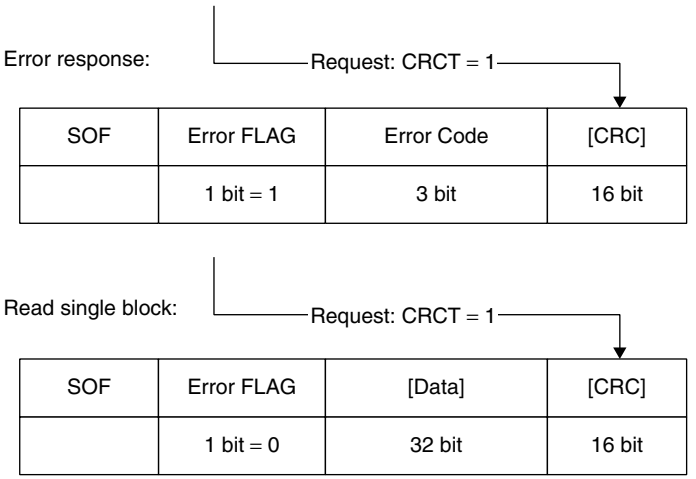


Figure 9.7 Structure of an ISO 14223 response frame for the transmission of data from transponder to the reader

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).[1] 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[2] and the small advantages in comparison to contact smart cards,[3]

[1] 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.
[2] The cards consist of a complex structure consisting of up to four inductive coupling elements and the same number of capacitive coupling elements.
[3] Close coupling smart cards also need to be inserted into a reader for operation, or at least precisely positioned on a stand.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

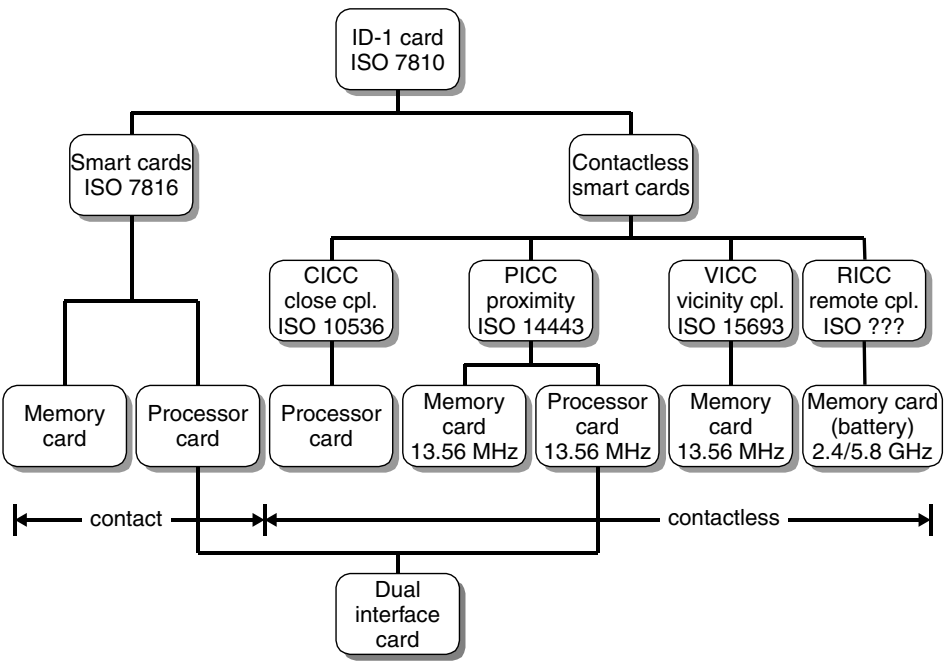


Figure 9.8 Family of (contactless and contact) smart cards, with the applicable standards

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)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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° 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° *PSK*. The reader is designed such that a load change

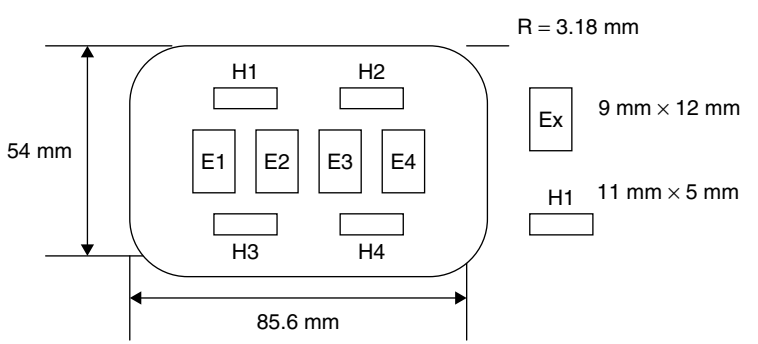


Figure 9.9 Position of capacitive (E1–E4) and inductive coupling elements (H1–H4) in a close coupling smart card

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

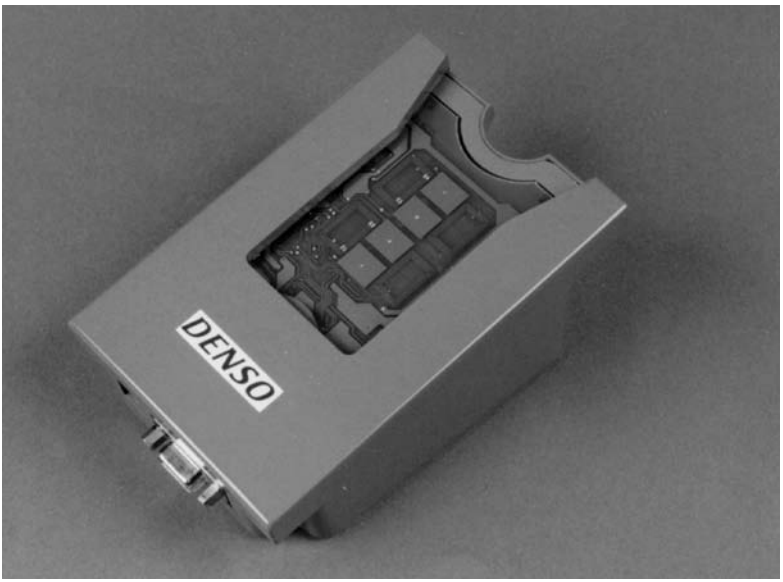


Figure 9.10 Half opened reader for close coupling smart cards in accordance with ISO 10536. In the centre of the insertion slot four capacitive coupling areas can be seen, surrounded by four inductive coupling elements (coils) (reproduced by permission of Denso Corporation, Japan — Aichi-ken)

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 $U_{\text{diff}} = U_{\text{E1}} - U_{\text{E2}}$ 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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

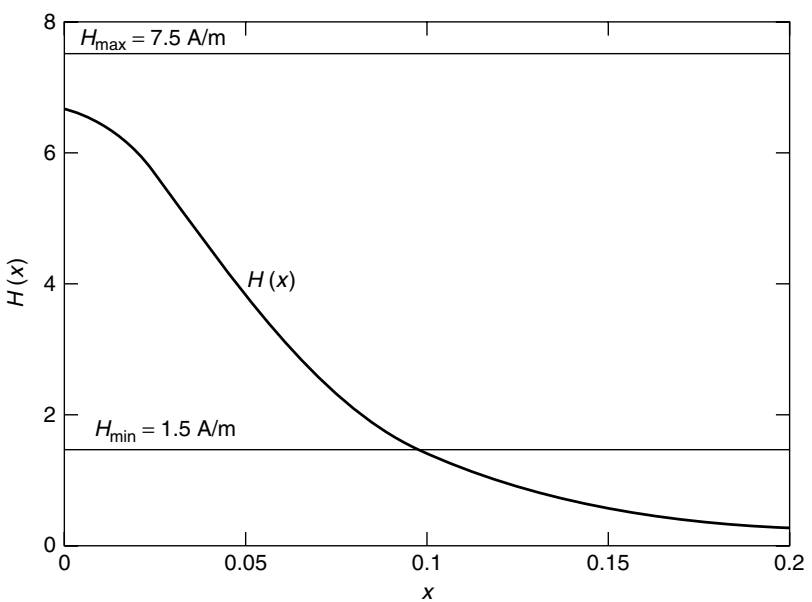


Figure 9.11 Typical field strength curve of a reader for proximity coupling smart cards (antenna current $i_1 = 1\text{A}$, antenna diameter $D = 15\,\text{cm}$, number of windings $N = 1$)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

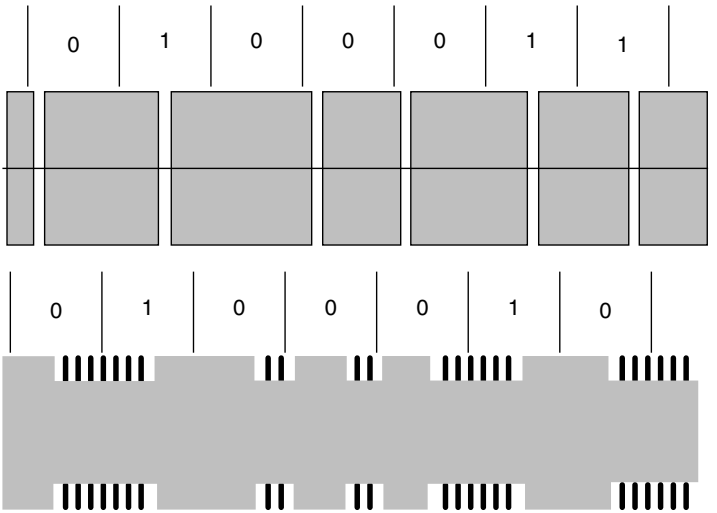


Figure 9.12 Modulation procedure for proximity coupling smart cards in accordance with ISO 14443 — Type A: Top: Downlink — ASK 100% with modified Miller coding (voltage path at the reader antenna). Bottom: Uplink — load modulation with ASK modulated 847 kHz subcarrier in Manchester coding (voltage path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

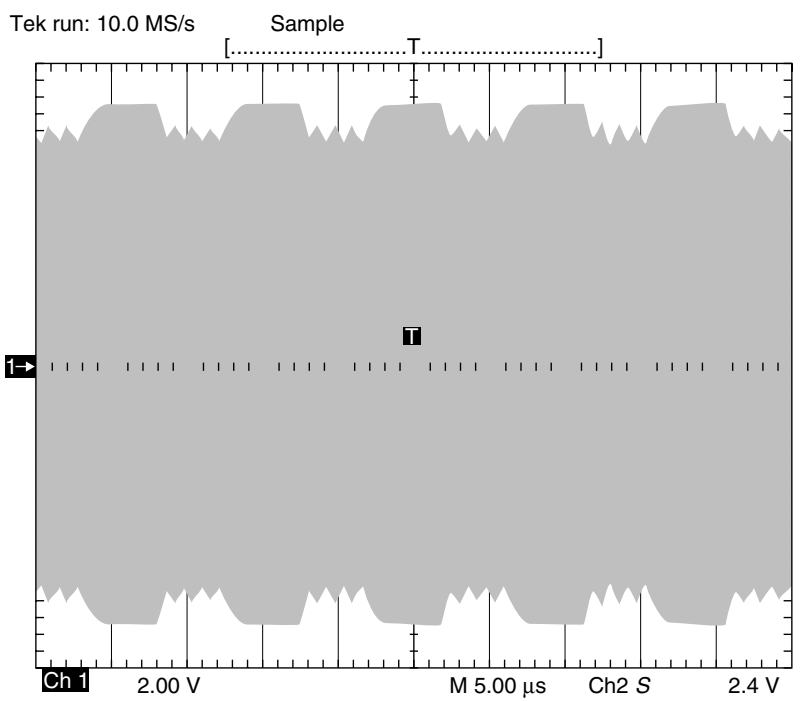


Figure 9.13 The oscillogram of a signal generated at the reader antenna by a Type A card using load modulation with an ASK modulated subcarrier

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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).

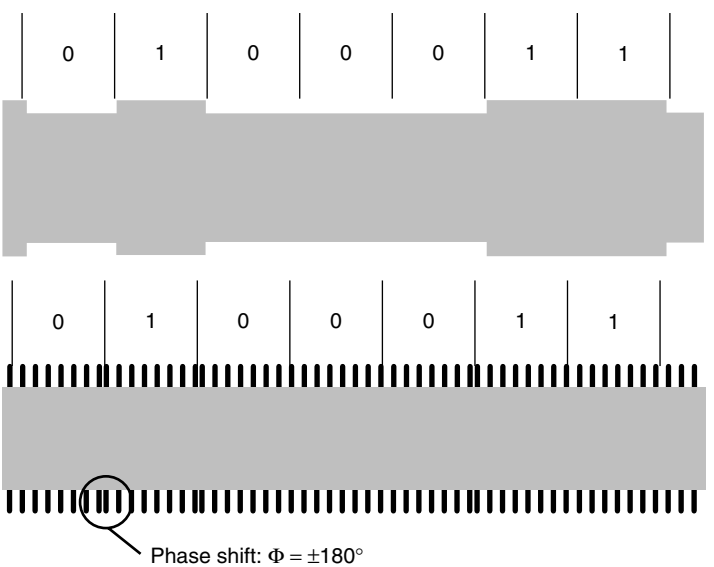


Figure 9.14 Modulation procedure for proximity coupling smart cards in accordance with ISO 14443 — Type B. Top: Downlink — ASK 10% with NRZ coding (voltage path at the reader antenna). Bottom: Uplink — load modulation with BPSK modulated 847 kHz subcarrier in NRZ coding (voltage path at the transponder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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

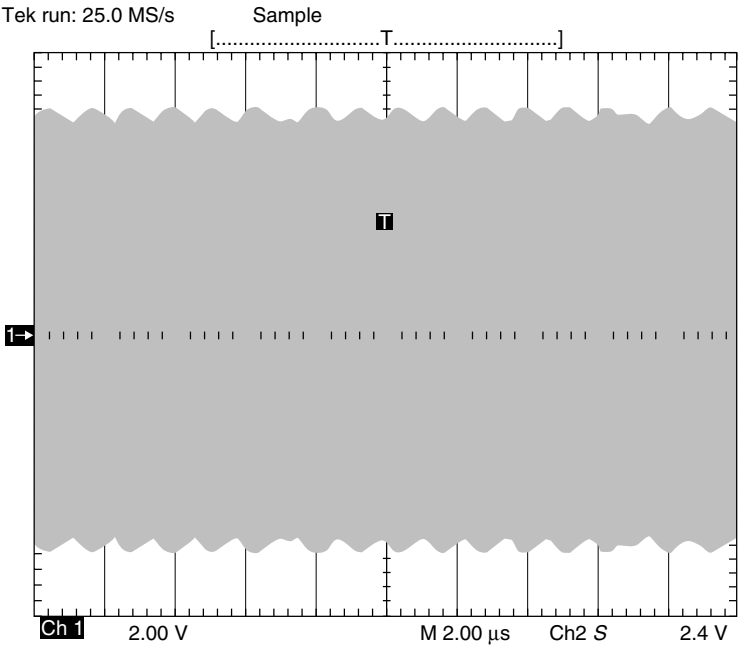


Figure 9.15 The oscillogram of a signal generated at the reader antenna by a Type B card using load modulation with BPSK modulated subcarrier

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

9.2.2.3 Part 3 – Initialisation and anticollision

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

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

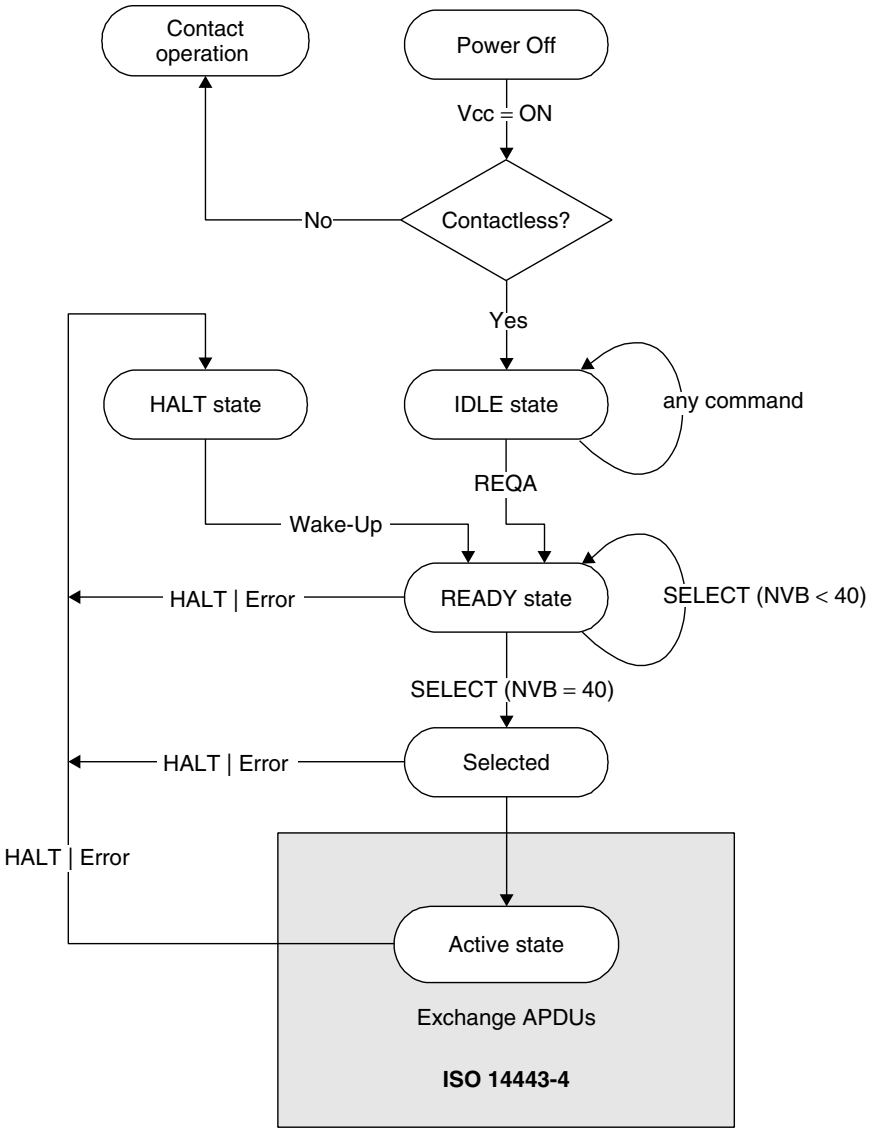


Figure 9.16 State diagram of a Type A smart card in accordance with ISO 14443 (Berger, 1998)

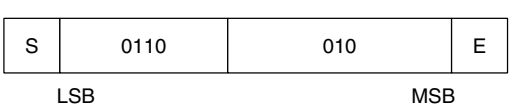


Figure 9.17 The reader's **Request command** for Type A cards (REQA) is made up of only 7 data bits. This reliably rules out the misinterpretation of useful data destined for another card as a REQUEST command (S = start of frame, E = end of frame)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

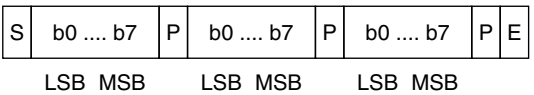


Figure 9.18 With the exception of the REQA command and data transmitted during the anti-collision routine, all data sent between reader and card (i.e. command, response and useful data) is transferred in the form of standard frames. This always begins with a start-of-frame signal (S), followed by any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

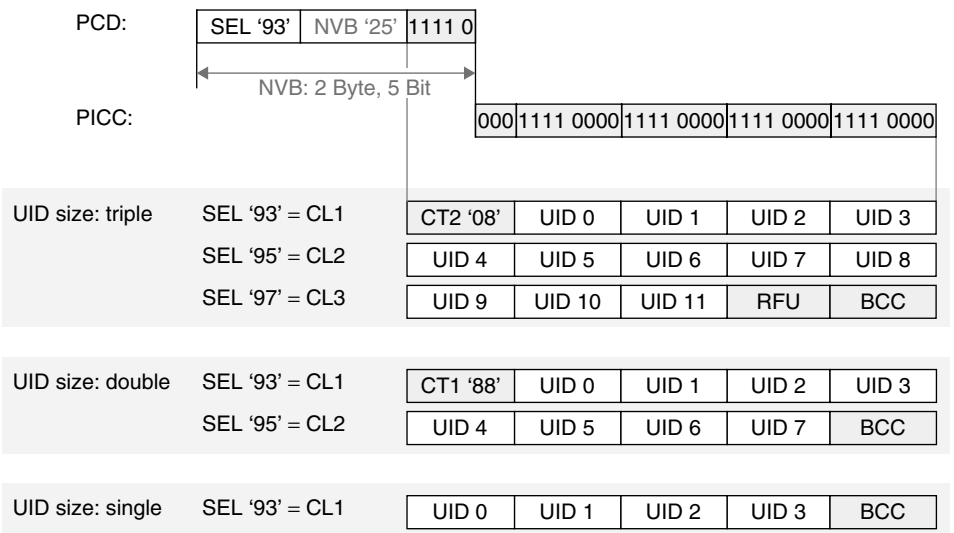


Figure 9.19 A dynamic binary search tree algorithm is used for the determination of the serial number of a card. The serial numbers can be 4, 7 or 10 bytes long, so the algorithm has to be run several times at different cascade levels (CL)

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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

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

Table 9.9 Required time grid for the transponder response during anticollision

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

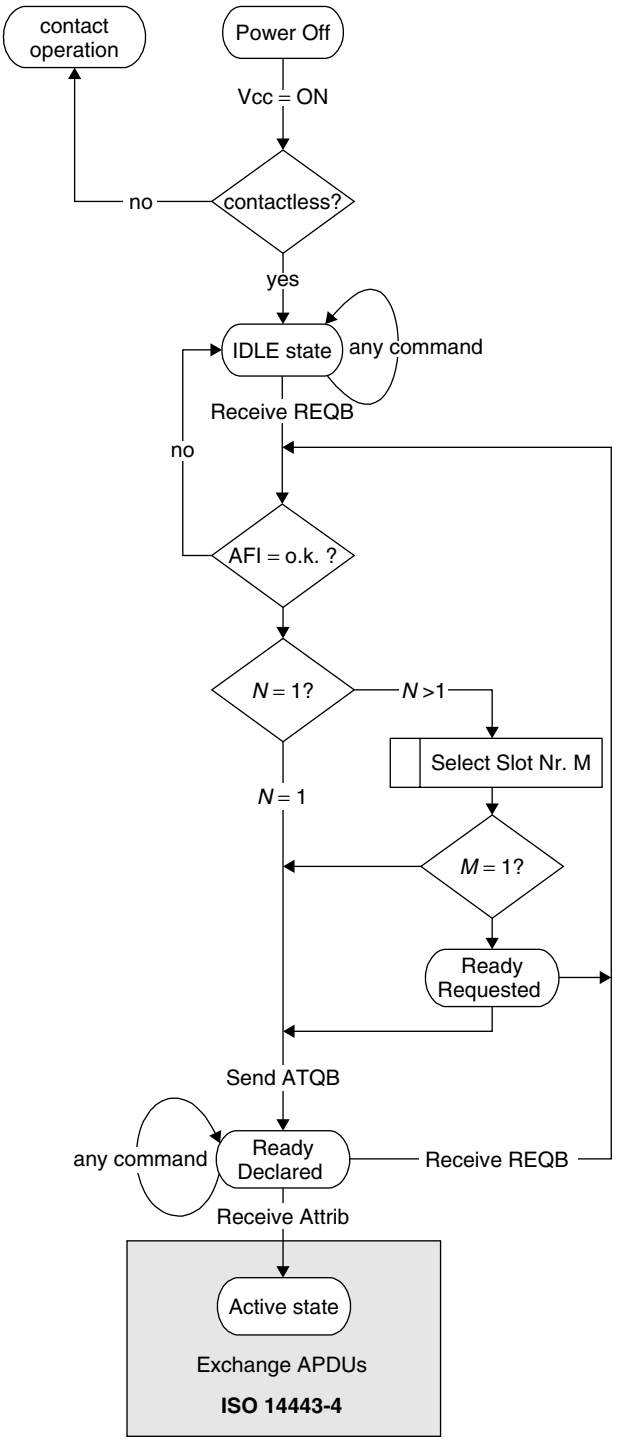


Figure 9.20 State diagram of a Type B smart card in accordance with ISO 14443.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

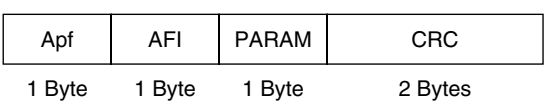


Figure 9.21 Structure of an REQB command. In order to reliably rule out errors the anticollision prefix (Apf) possess a reserved value (05h), which may not be used in the NAD parameter of a different command

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

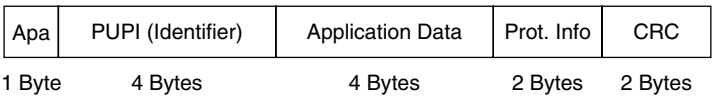


Figure 9.22 Structure of an ATQB (Answer To Request B)

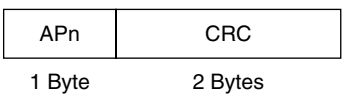


Figure 9.23 Structure of a slot marker. The sequential number of the following slot is coded in the parameter APn: APn = 'nnnn 0101b' = 'n5h'; n = slot marker 1–15

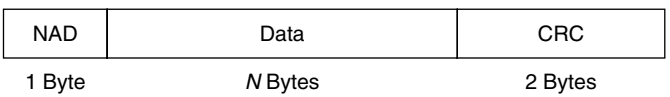


Figure 9.24 Structure of a standard frame for the transmission of application data in both directions between the reader and a Type B card. The value x5h (05h, 15h, 25h, ... E5h, F5h) of the NAD (node address) are subject to anticollision commands, in order to reliably rule out confusion with application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

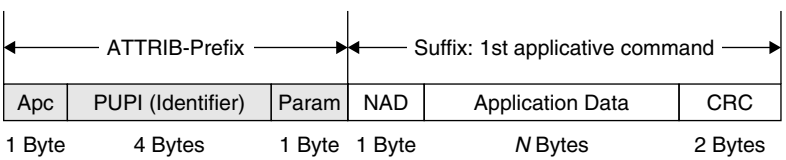


Figure 9.25 A card is selected by the sending of an application command preceded by the ATTRIB prefix, if the identifier of the card corresponds with the identifier (PUPI) of the prefix

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

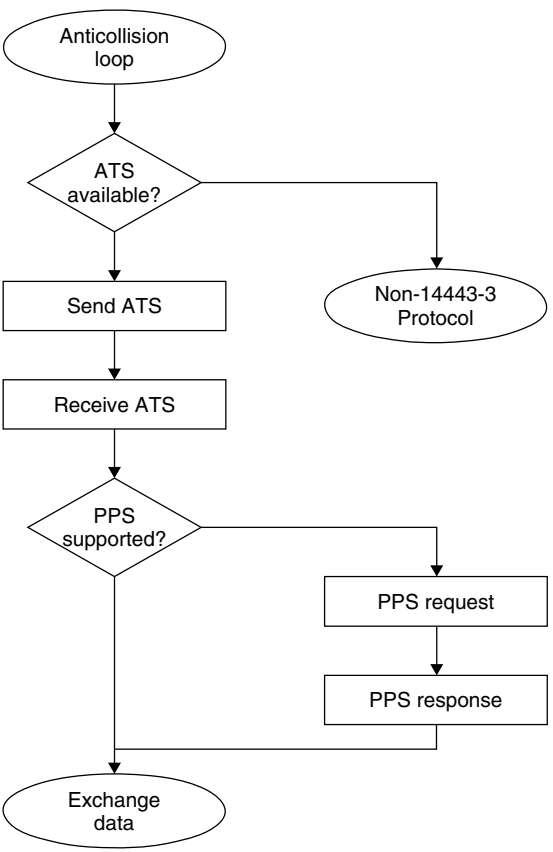


Figure 9.26 After anticollision the ATS of the card is requested

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

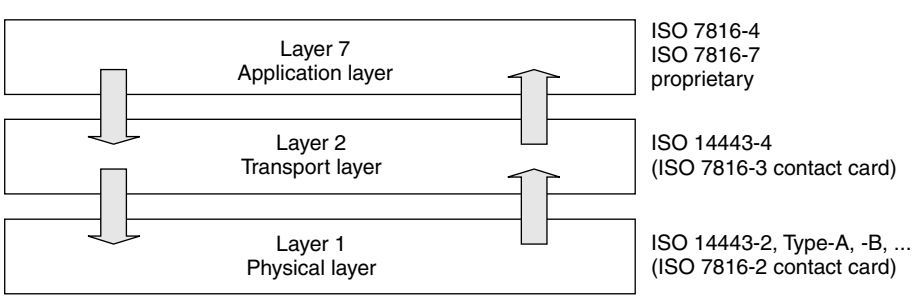


Figure 9.27 The ISO/OSI layer model in a smart card

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

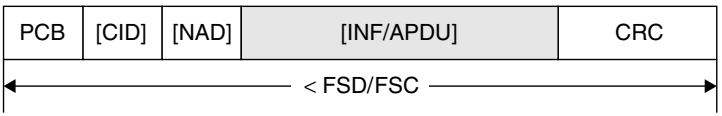


Figure 9.28 Structure of the frame in ISO 14443. The data of the application layer, Layer 7 (grey), are packed into the protocol frame of the transport layer (white)

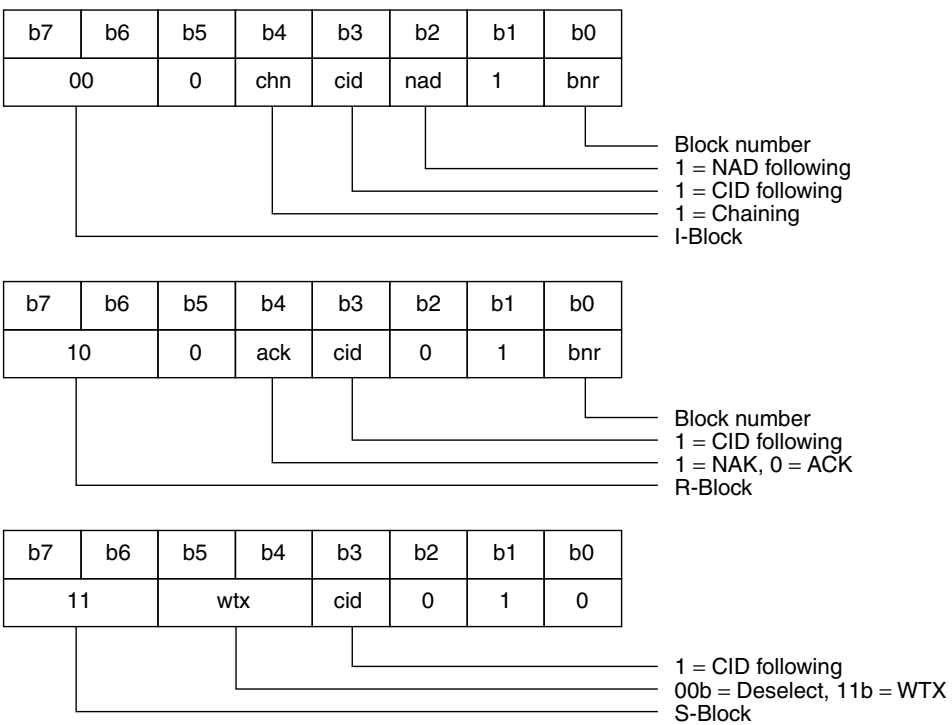


Figure 9.29 Coding of the PCB byte in a frame. The entire transmission behaviour is controlled by the PCB (protocol control byte) in the protocol

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.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

card (see FCC 15 Part 3: the permissible magnetic field strength of the modulation side bands lies 50 dB below the maximum field strength of the carrier signal of 42 dBμA/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 μs. 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:

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

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 μs long modulation pulses separated by a time slot of 56.65 μs (9.44 μs × 4) (Figure 9.32).

The EOF signal consists of a single modulation pulse lasting 9.44 μs, 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 MHz ± 7 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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

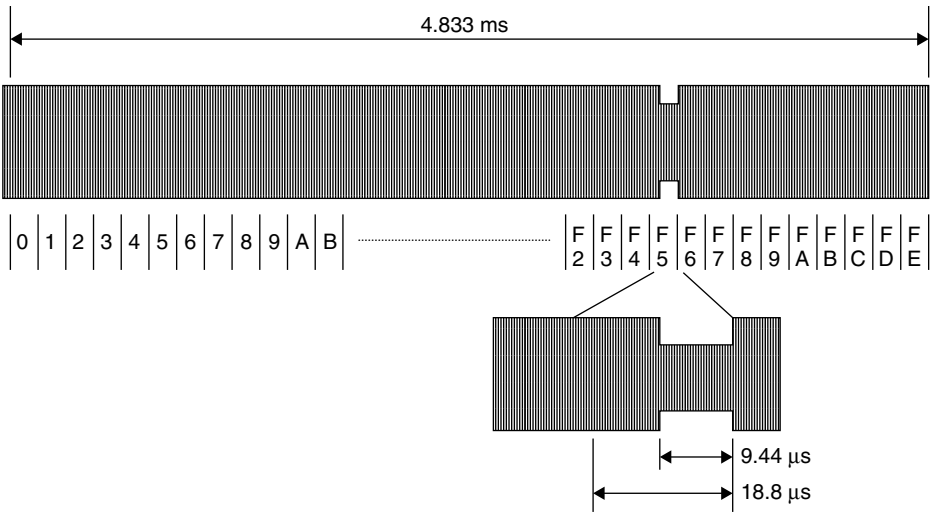


Figure 9.30 The '1 of 256' coding is generated by the combination of 512 time slots of 9.44 µs length. The value of the digit to be transferred in the value range 0–255 can be determined from the position in time of a modulation pulse. A modulation pulse can only occur at an uneven time slot (1, 3, 5,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

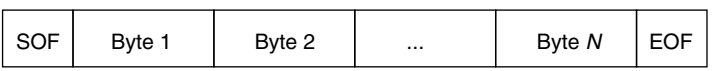


Figure 9.31 Structure of a message block (framing) made up of frame start signal (SOF), data and frame end signal (EOF)

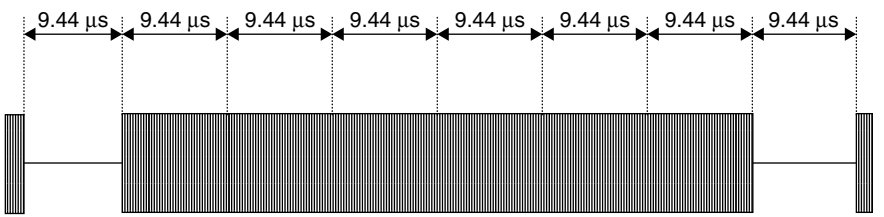


Figure 9.32 Coding of the SOF signal at the beginning of a data transmission using '1 of 256' coding

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

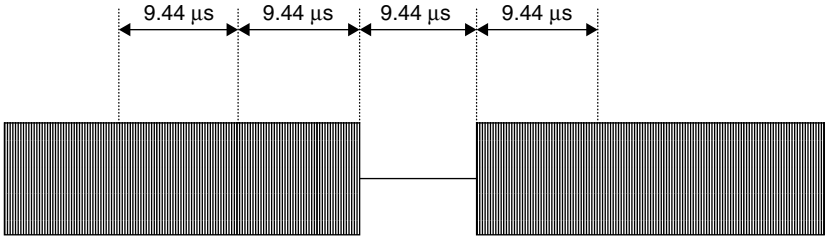


Figure 9.33 The EOF signal consists of a modulation pulse at an even time slot ($t = 2$) and thus is clearly differentiated from useful data

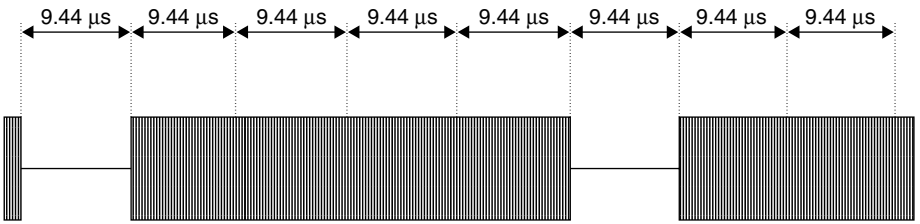


Figure 9.34 The SOF signal of '1 of 4' coding consists of two 9.44 µs long modulation pulses separated by an interval of 18.88 µs

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	$f_c/32$	$f_c/32$; $f_c/28$

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

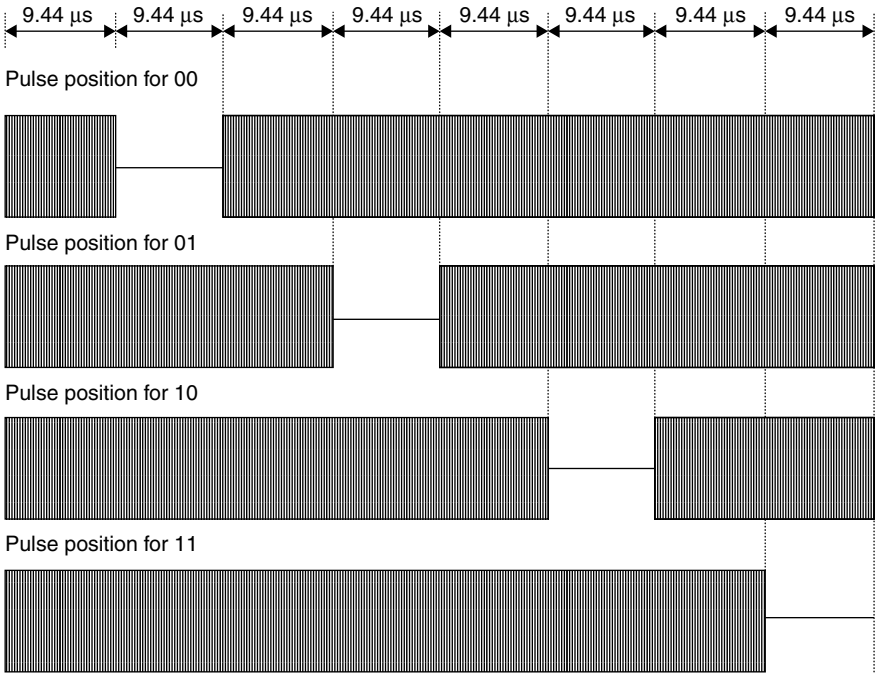


Figure 9.35 '1 of 4' coding arises from the combination of eight time slots of 9.44 µs length. The value of the digit to be transmitted in the value range 0–3 can be determined from the time position of a modulation pulse

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

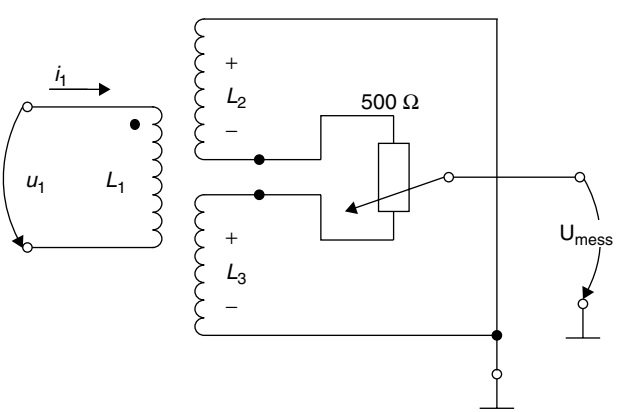


Figure 9.36 Measuring bridge circuit for measuring the load modulation of a contactless smart card in accordance with ISO 14443

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

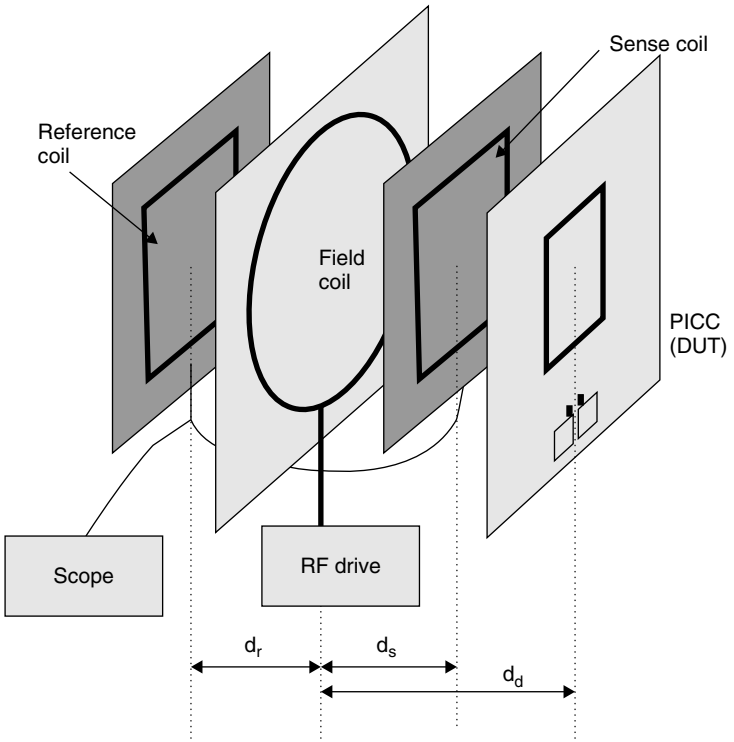


Figure 9.37 Mechanical structure of the measurement bridge, consisting of the field generator coil (field coil), the two sensor coils (sense and reference coil) and a smart card (PICC) as test object (DUT) (reproduced by permission of Philips Semiconductors, Hamburg)

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 Ω 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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

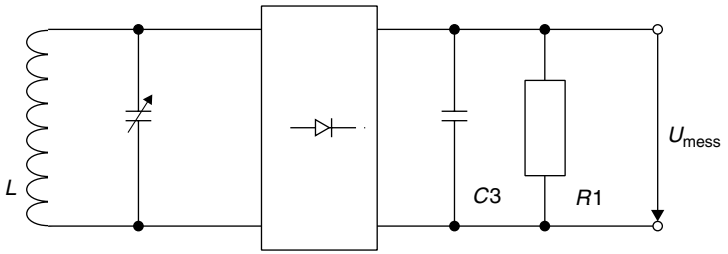


Figure 9.38 Circuit of a reference card for testing the power supply of a contactless smart card from the magnetic HF field of a reader

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_{meas} of the reference card is now measured at defined resonant frequencies ($f_{res} = 13–19\,MHz$) 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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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).

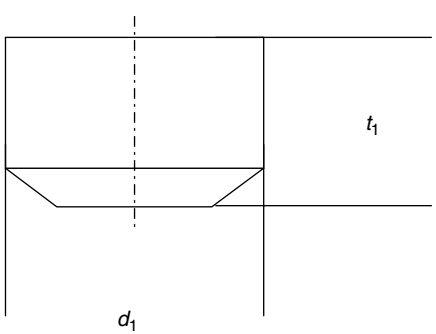


Figure 9.39 Format of a data carrier for tools and cutters

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

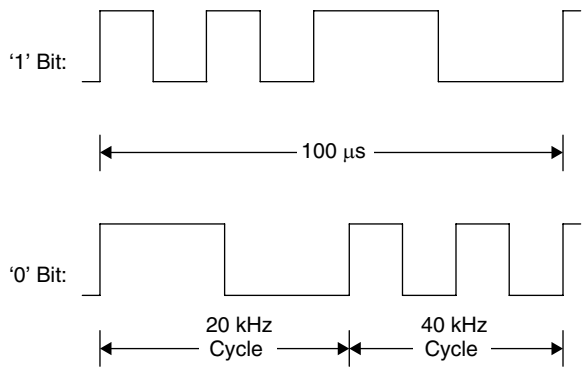


Figure 9.40 Coding of data bits using the modified FSK subcarrier procedure

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. this

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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'

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

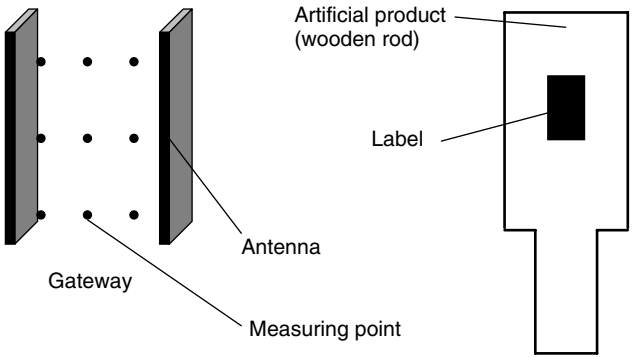


Figure 9.42 Left, measuring points in a gateway for inspection using artificial products; right, artificial product

- 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*

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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



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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 Radiocommunications 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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 $' 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	$>0.005\,m^2$

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

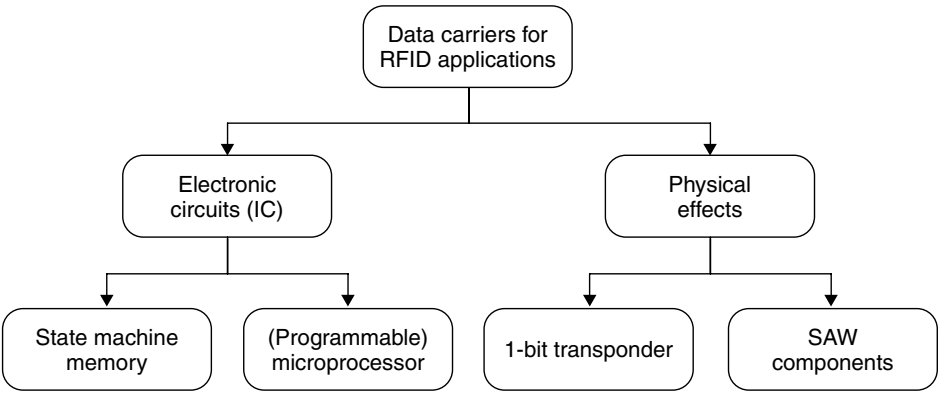


Figure 10.1 Overview of the different operating principles used in RFID data carriers

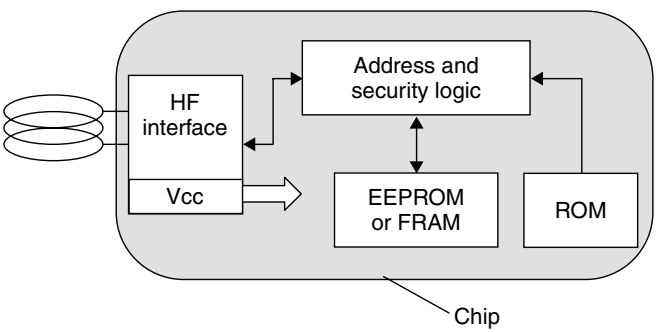


Figure 10.2 Block diagram of an RFID data carrier with a memory function

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.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

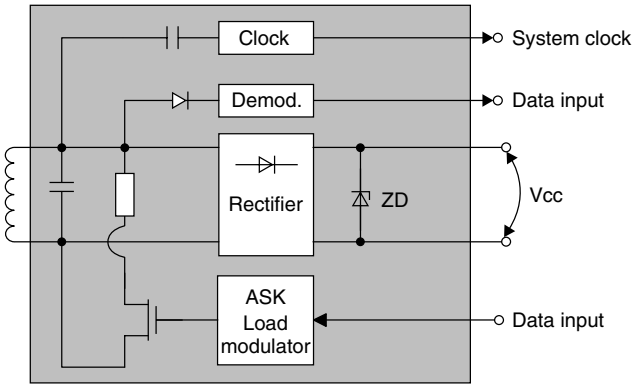


Figure 10.3 Block diagram of the HF interface of an inductively coupled transponder with a load modulator

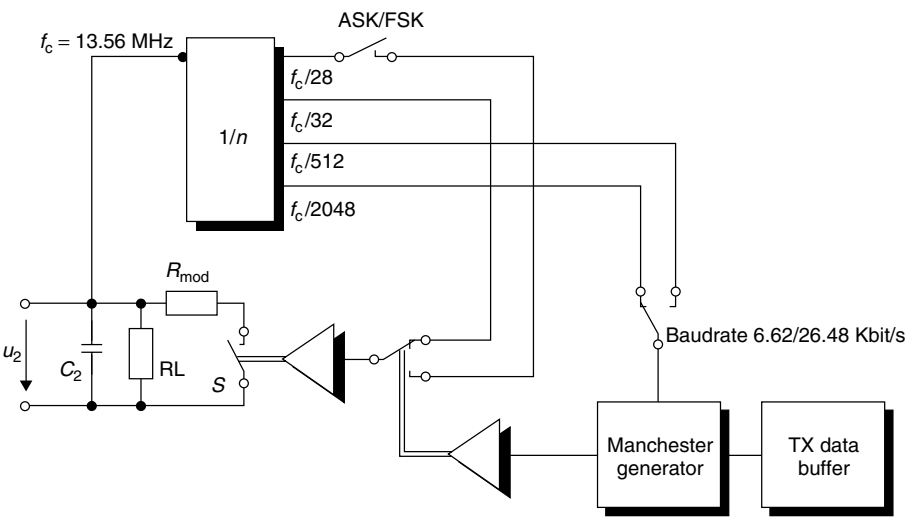


Figure 10.4 Generation of a load modulation with modulated subcarrier: the subcarrier frequency is generated by a binary division of the carrier frequency of the RFID system. The subcarrier signal itself is initially ASK or FSK modulated (switch position ASK/FSK) by the Manchester coded data stream, 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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

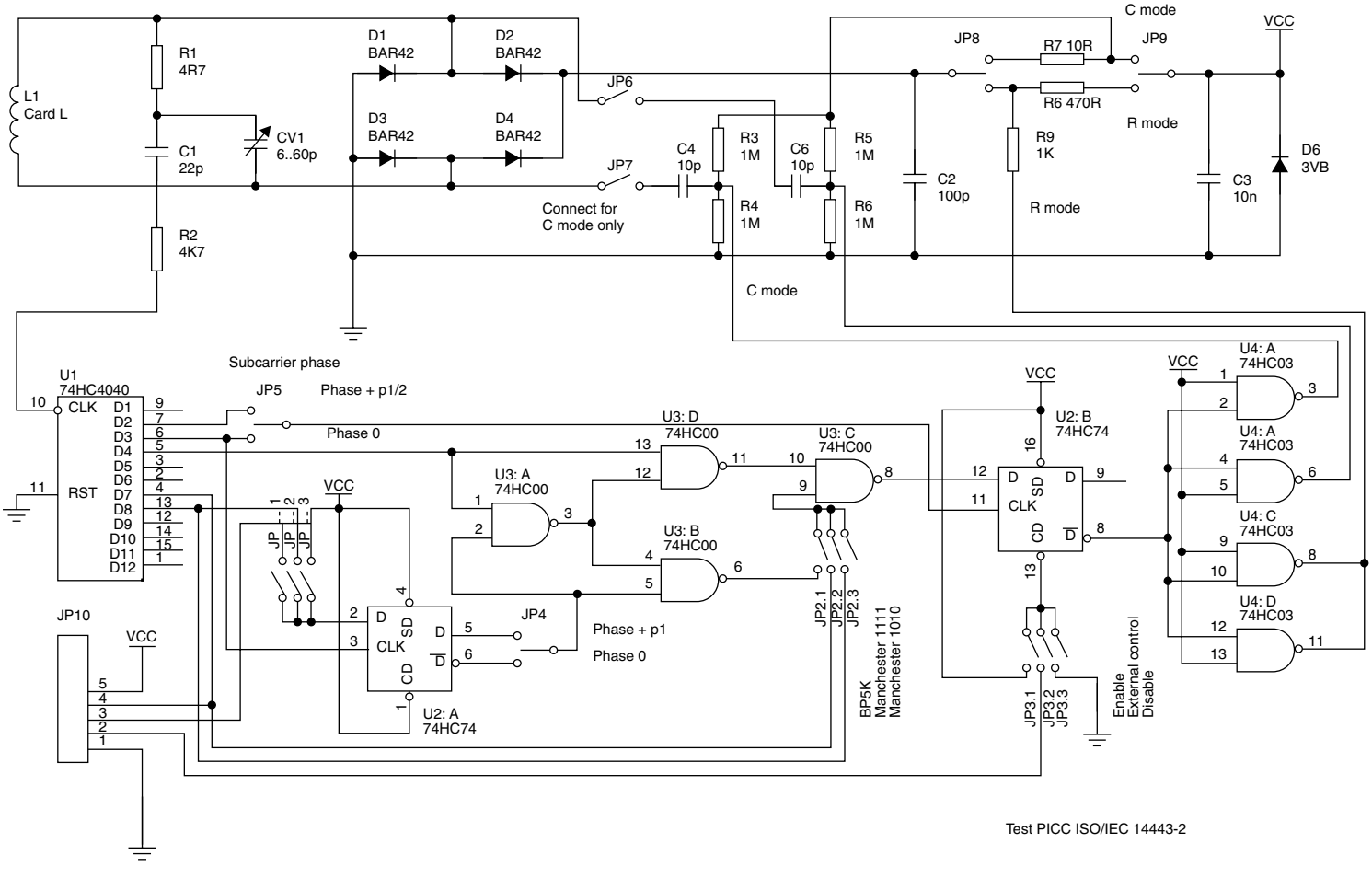


Figure 10.5 Example circuit of a HF interface in accordance with ISO 14443

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

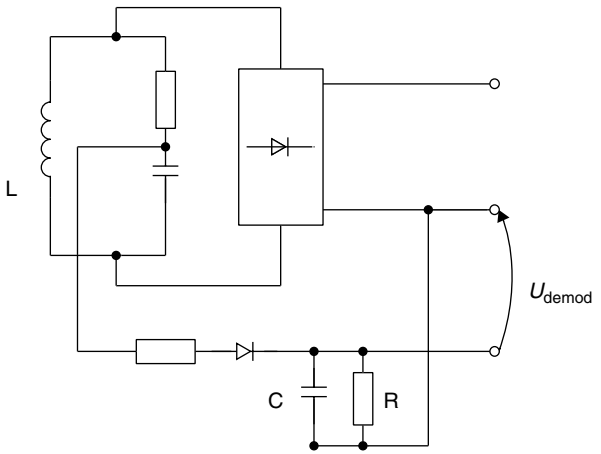


Figure 10.6 A 100% ASK modulation can be simply demodulated by an additional diode

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.

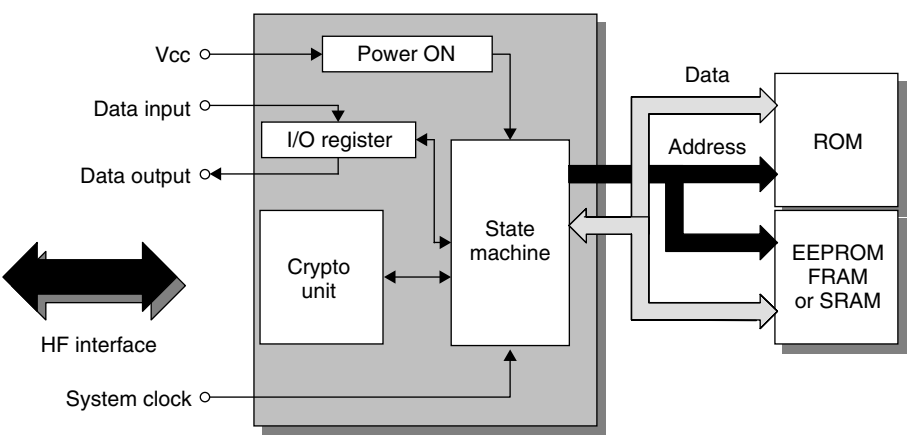


Figure 10.7 Block diagram of address and security logic module

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

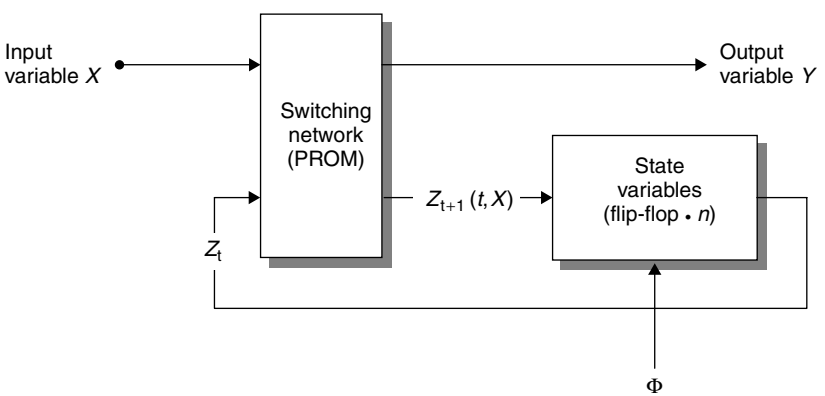


Figure 10.8 Block diagram of a state machine, consisting of the state memory and a backcoupled switching network

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

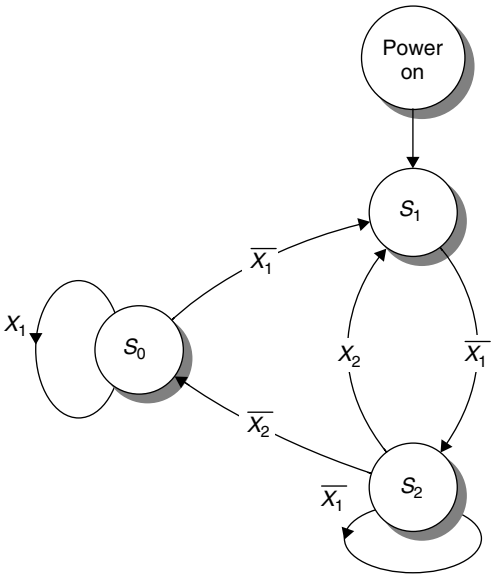


Figure 10.9 Example of a simple state diagram to describe a state machine

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

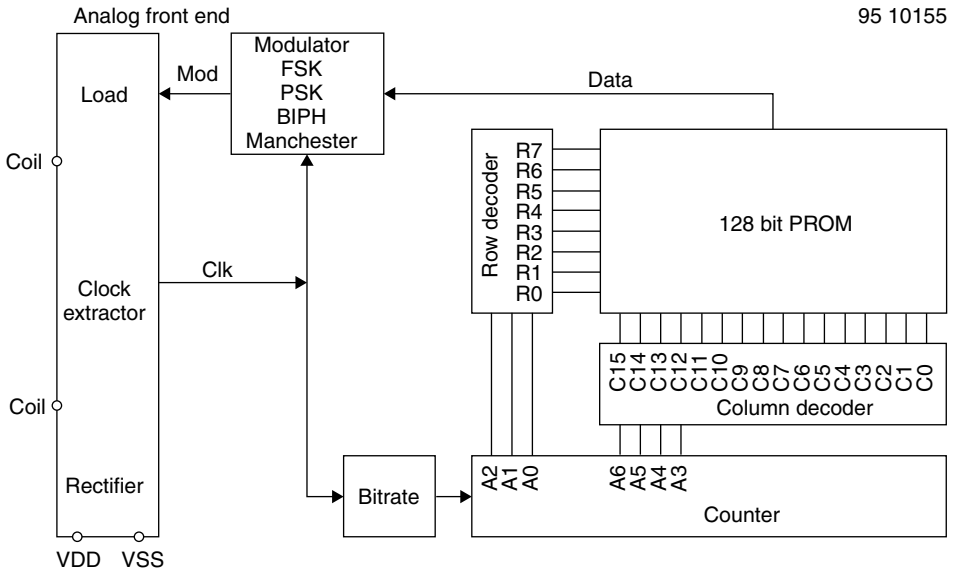


Figure 10.10 Block diagram of a read-only transponder. When the transponder enters the interrogation zone of a reader a counter begins to interrogate all addresses of the internal memory (PROM) sequentially. The data output of the memory is connected to a load modulator which is set to the baseband code 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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

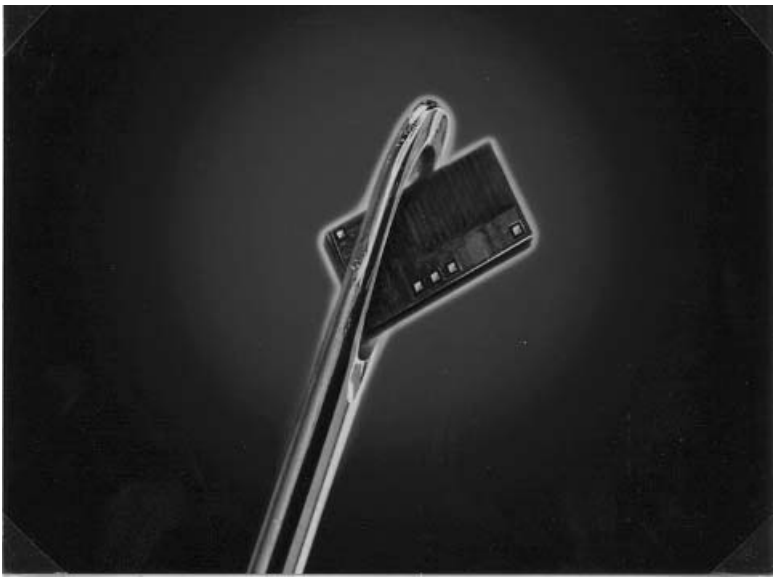


Figure 10.11 Size comparison: low-cost transponder chip in the eye of a needle (reproduced by permission of Philips Electronics N.V.)

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

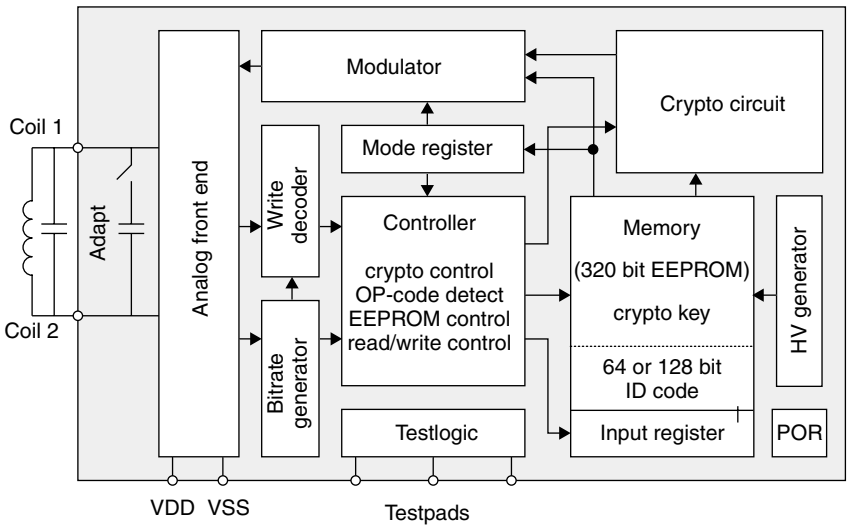


Figure 10.12 Block diagram of a writable transponder with a cryptological function to perform authentication between transponder and reader (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

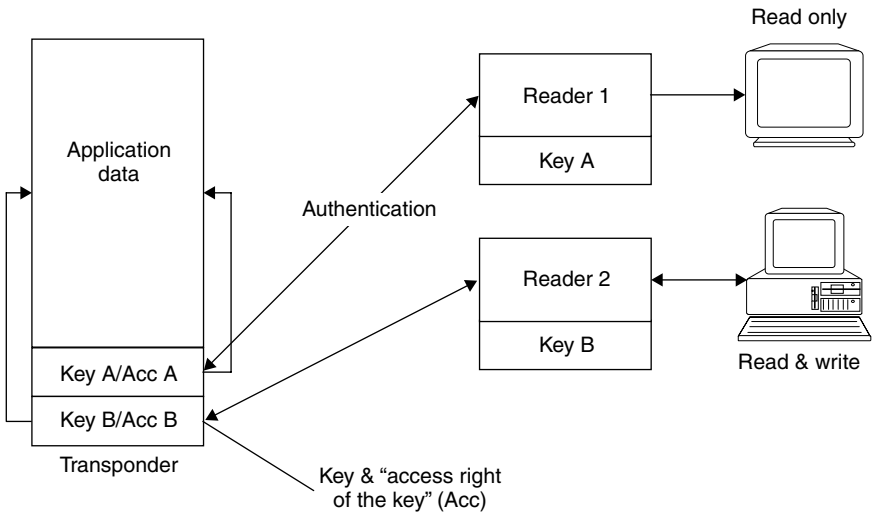


Figure 10.13 A transponder with two key memories facilitates the hierarchical allocation of access rights, in connection with the authentication keys used

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

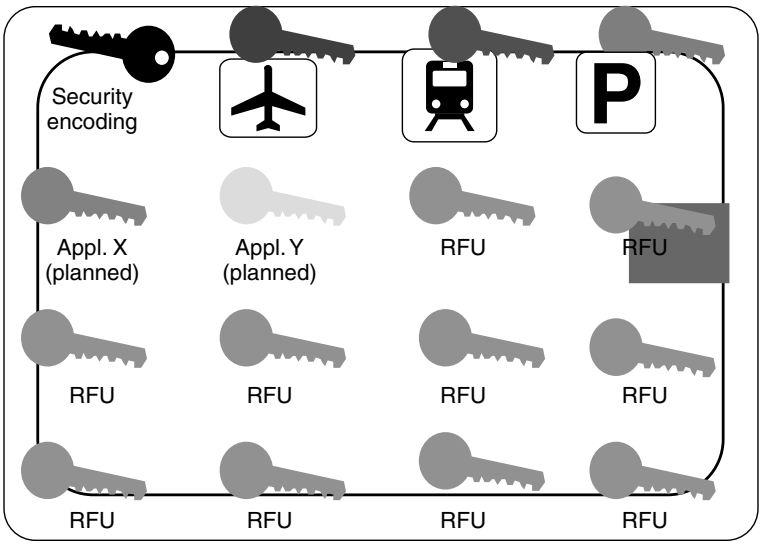


Figure 10.14 Several applications on one transponder — each protected by its own secret key

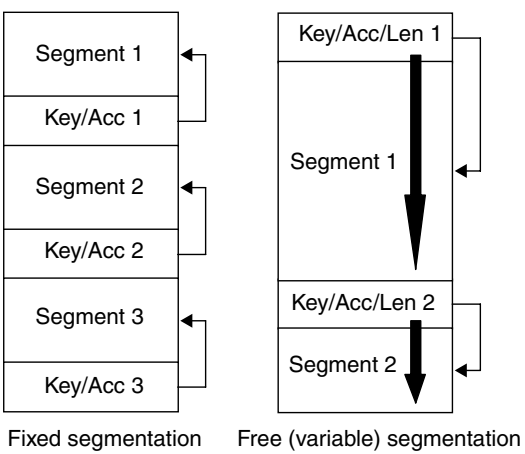


Figure 10.15 Differentiation between fixed segmentation and free segmentation

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

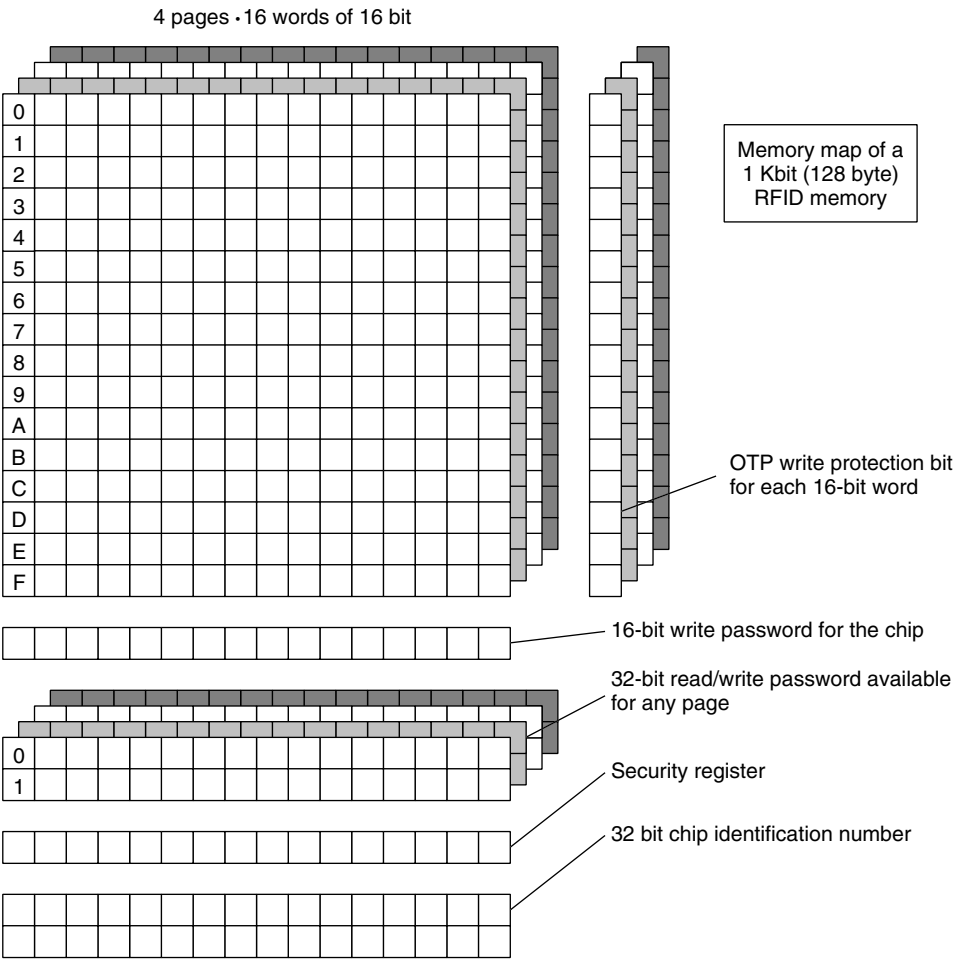


Figure 10.16 Example of a transponder with fixed segmentation of the memory (IDESCO MICROLOG®) The four 'pages' can be protected against unauthorised reading or writing using different passwords (IDESCO, n.d.)

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

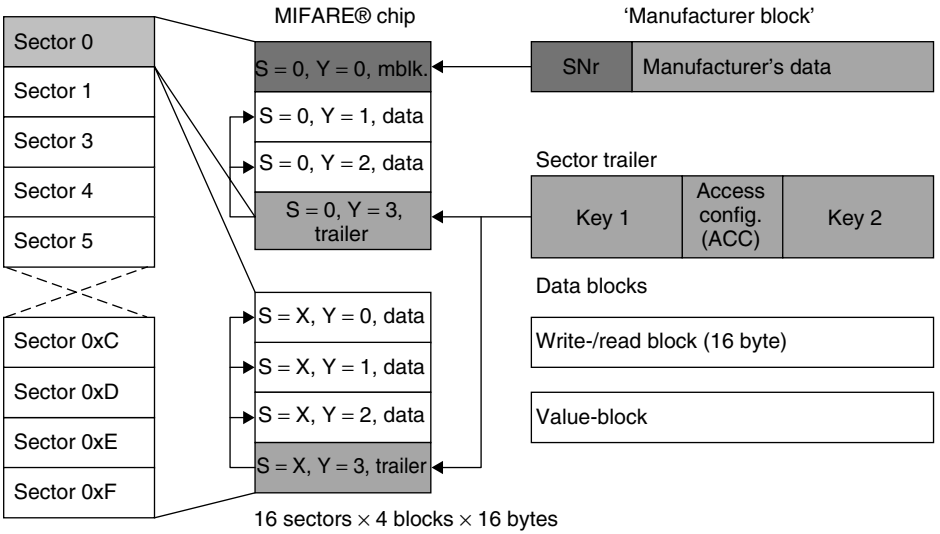


Figure 10.17 Memory configuration of a MIFARE® data carrier. The entire memory is divided into 16 independent sectors. Thus a maximum of separate 16 applications can be loaded onto a MIFARE® card

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 00 h, then this is an *administration code* for the management of free or reserved sectors.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

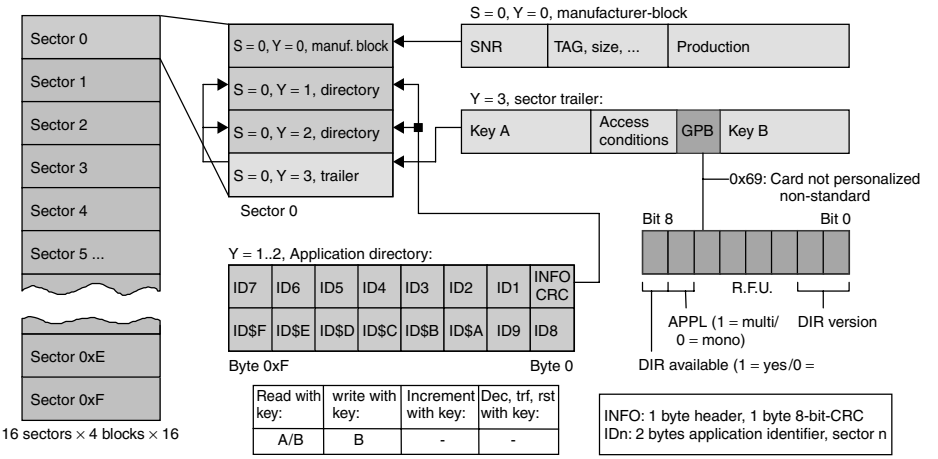


Figure 10.18 The data structure of the MIFARE® application directory consists of an arrangement of 15 pointers (ID1 to ID$F), which point to the subsequent sectors

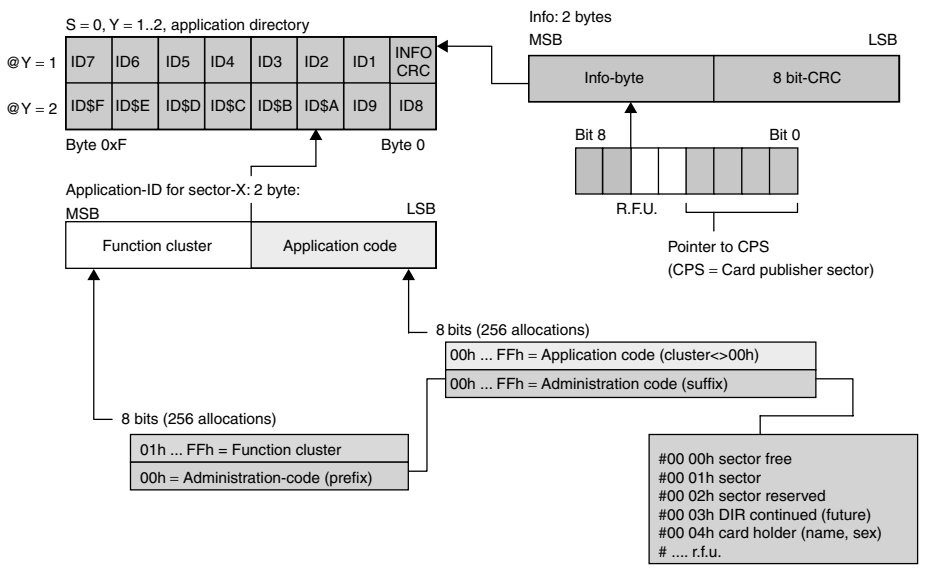


Figure 10.19 Data structure of the MIFARE® application directory: it is possible to find out what applications are located in each sector from the contents of the 15 pointers (ID1 to ID$F)

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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^2C (IIC) bus* interface established themselves years ago, particularly in consumer electronics. I^2C 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^2C 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^2C 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.

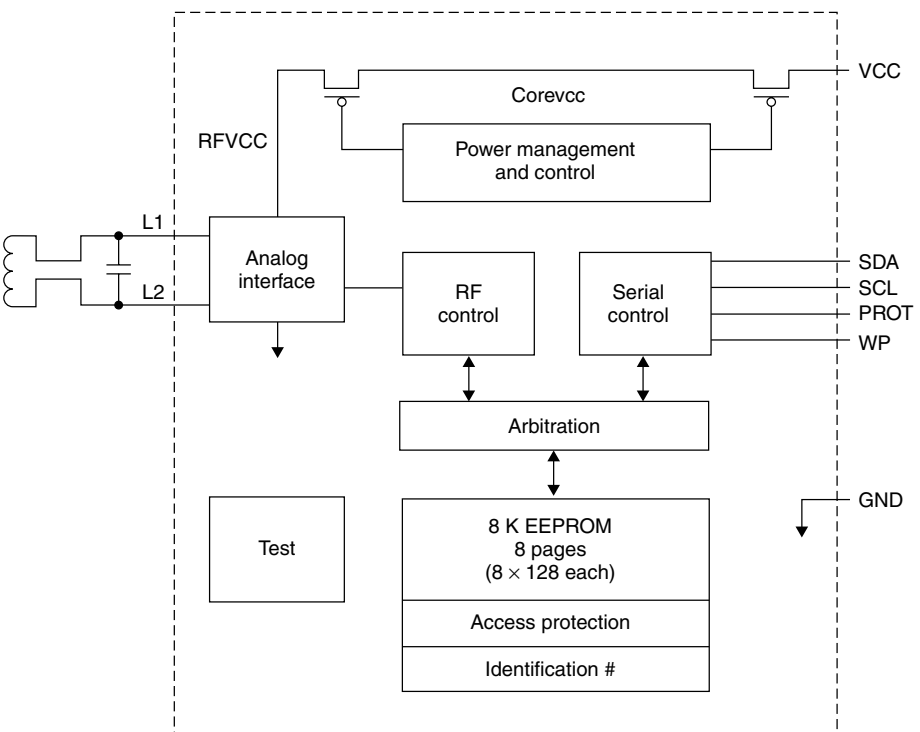


Figure 10.20 Block diagram of a dual port EEPROM. The memory can be addressed either via the contactless HF interface or an IIC bus interface (reproduced by permission of Atmel Corporation, San Jose, USA)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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^2C bus and the HF interface. However, read and write access to the access protection page itself is only possible via the I^2C 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^2C 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 WP7–WP0 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^2C 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^2C bus.

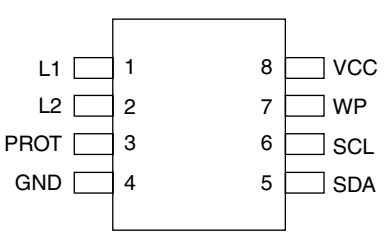


Figure 10.21 Pin assignment of a dual port EEPROM. The transponder coil is contacted to pins L_1 and L_2. All other pins of the module are reserved for connection to the I^2C bus and for the power supply in 'contact mode' (reproduced by permission of Atmel Corporation, San Jose, USA)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

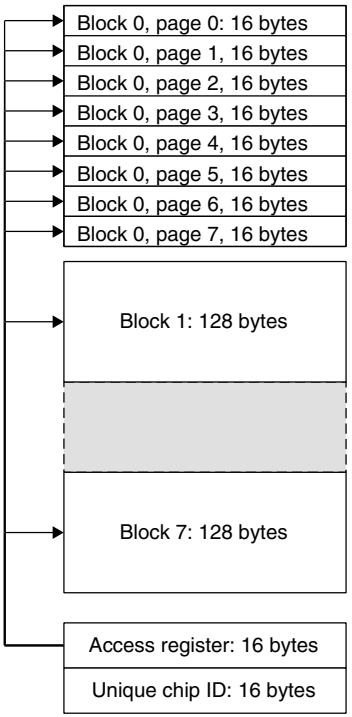


Figure 10.22 Memory configuration of the AT24RF08. The available memory of 1 Kbyte is split into 16 segments (blocks 0–7) of 128 bytes each. An additional memory of 32 bytes contains the access protection page and the unique serial numbers. The access protection page permits different access rights to be set in the memory for the HF and I^2C 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
SB_{AP}						PB_{AP}		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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

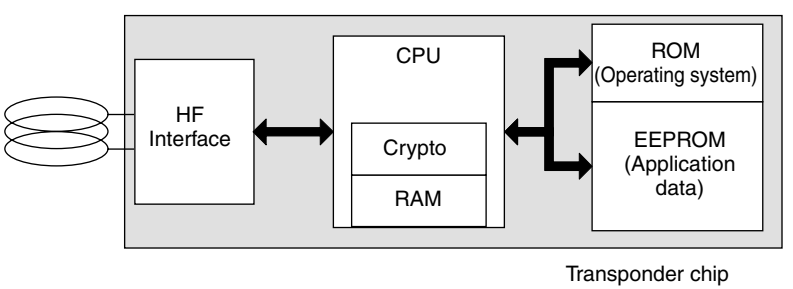


Figure 10.24 Block diagram of a transponder with a microprocessor. The microprocessor contains a coprocessor (cryptological unit) for the rapid calculation of the cryptological algorithms required for authentication or data encryption

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

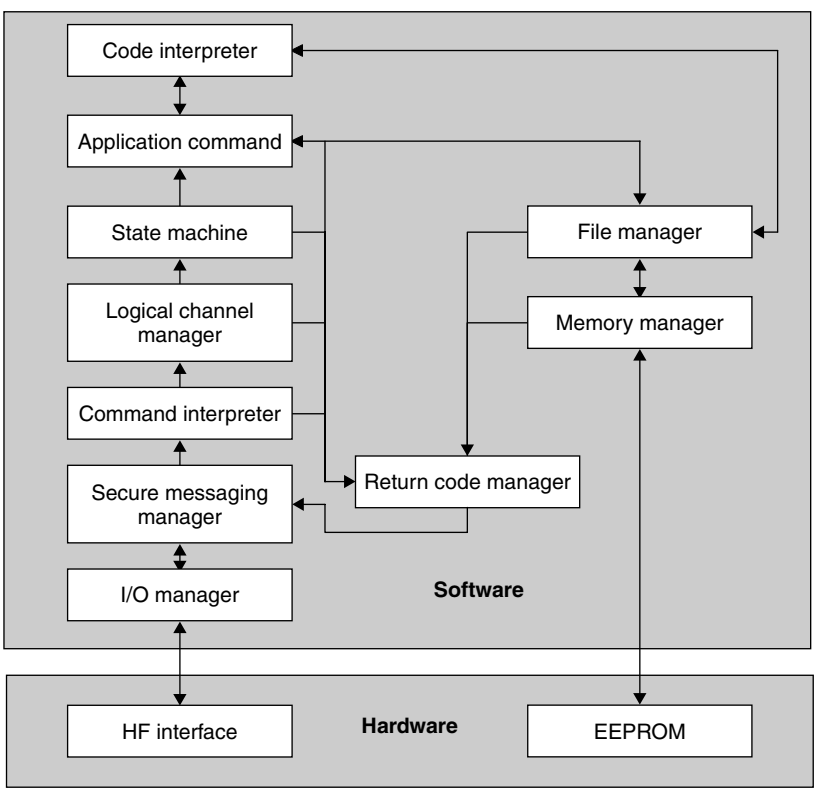


Figure 10.25 Command processing sequence within a smart card operating system (Rankl and Effing, 1996)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 ($H_{\min} = 1.5$ 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,

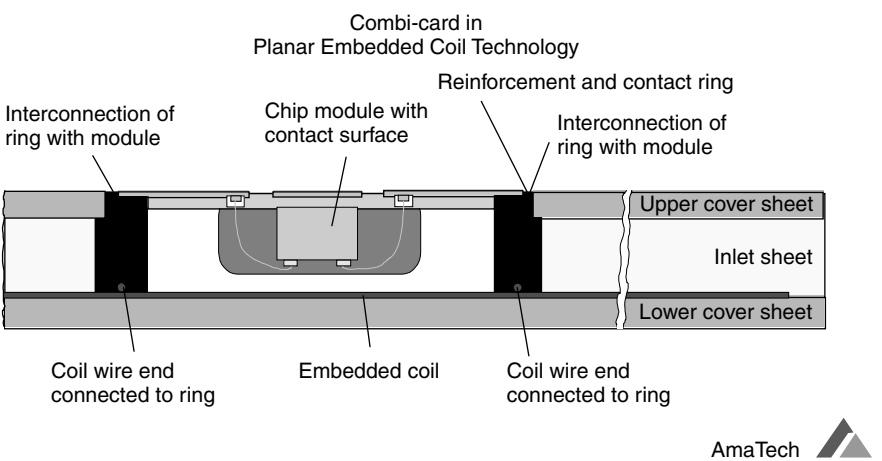


Figure 10.26 Possible layout of a dual interface smart card. The chip module is connected to both contact surfaces (like a telephone smart card) and a transponder coil (reproduced by permission of Amatech GmbH & Co. KG, Pfronten)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

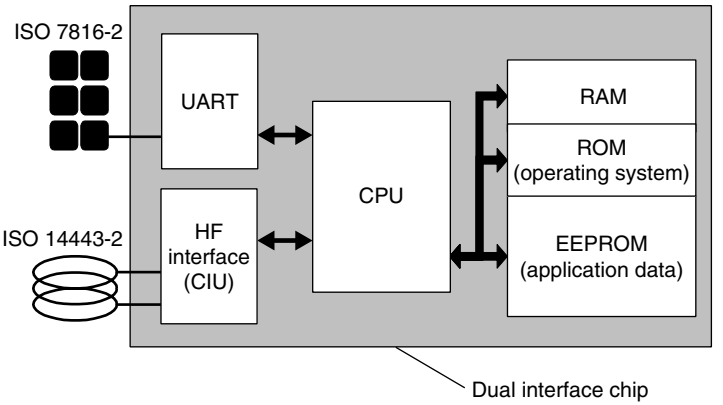


Figure 10.27 Block diagram of a dual interface card. Both smart card interfaces can be addressed independently of one another

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.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

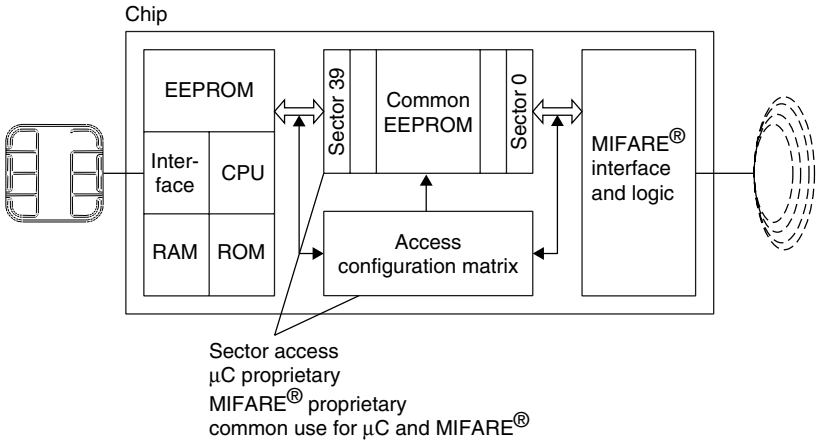


Figure 10.28 Block diagram of the MIFARE®-plus 'dual interface card' chip. In contactless operating mode the common EEPROM is accessed via a MIFARE®-compatible state machine. When operating via the contact interface a microprocessor with its own operating system accesses the same memory (reproduced by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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

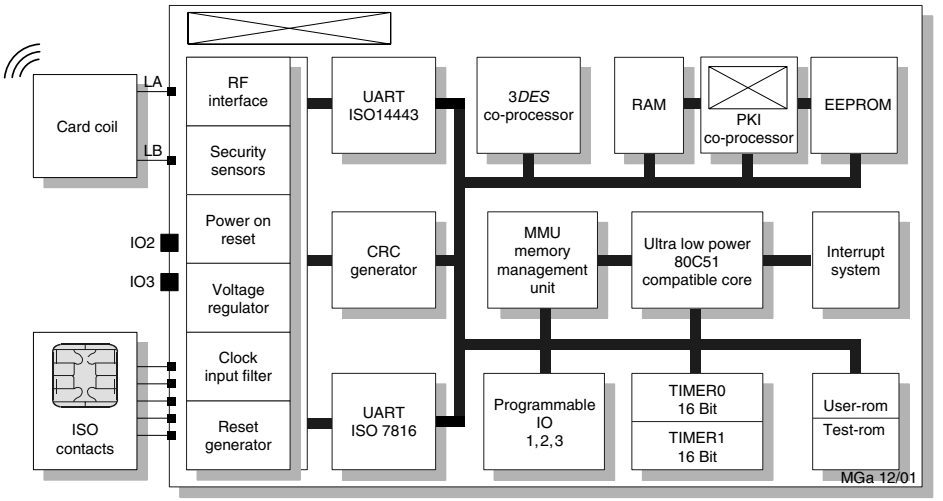


Figure 10.29 Block diagram of the dual interface card chip 'MIFARE ProX' (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

(*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*

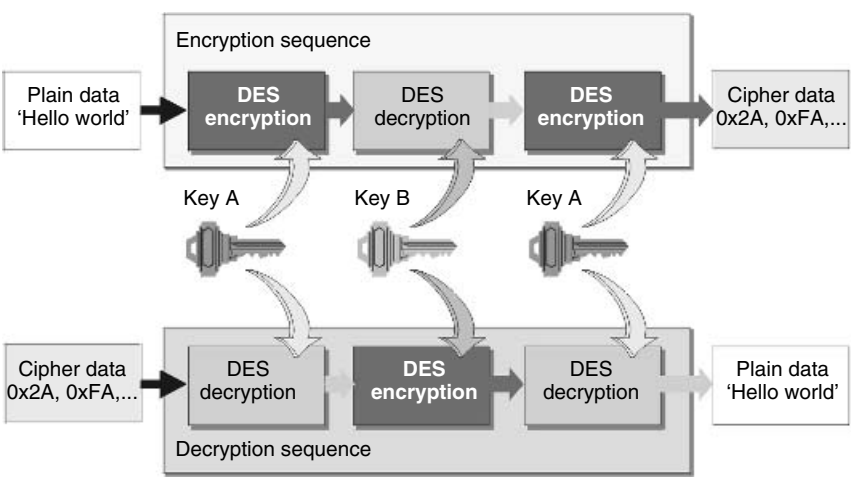


Figure 10.30 Calculation of the 3DES (triple DES). Encryption (above) and decryption (below) of a data block (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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.

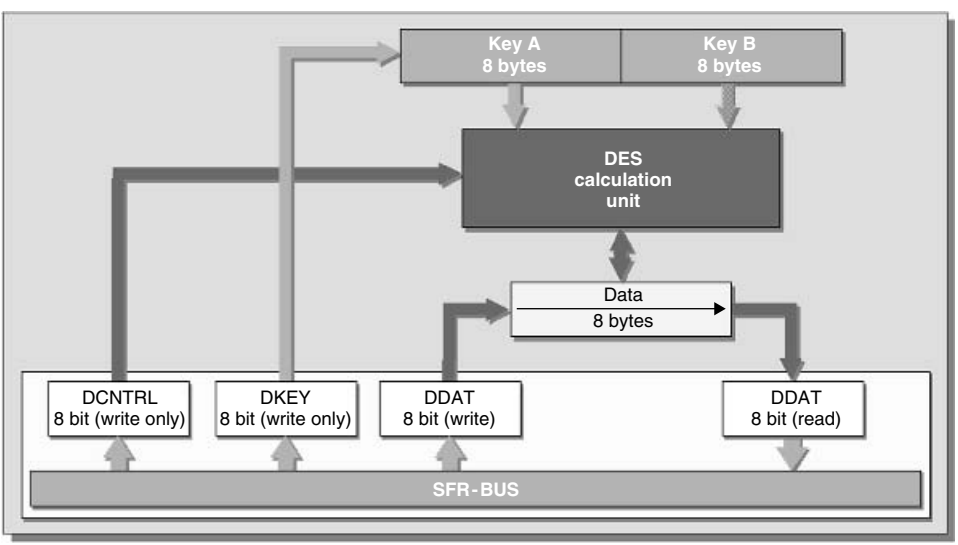


Figure 10.31 Block diagram of a DES coprocessor. The CPU key and data can be transferred to the coprocessor by means of its own SFR (special function register) (reproduced by permission of Philips Semiconductors Gratkorn, A-Gratkorn)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

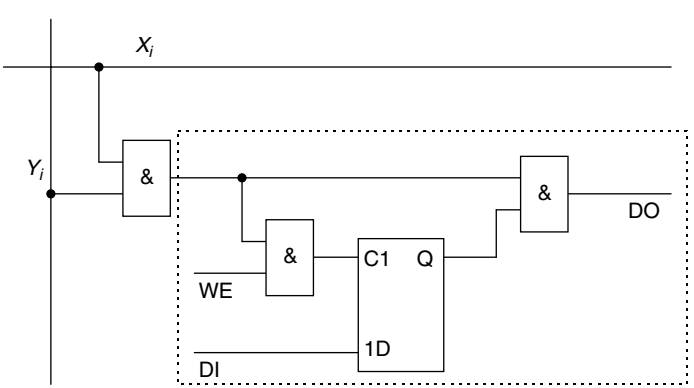


Figure 10.32 Simplified functional block diagram of a (S)RAM cell

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

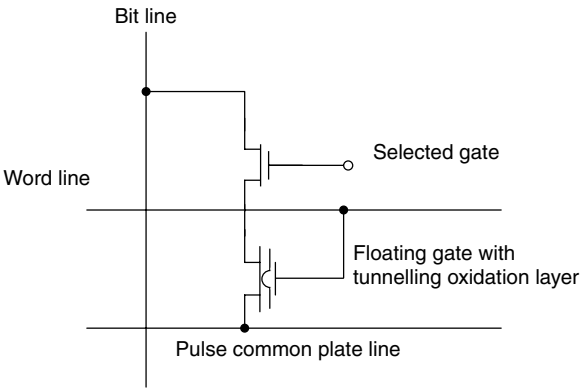


Figure 10.33 The EEPROM cell consists of a modified field effect transistor with an additional floating gate

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.

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

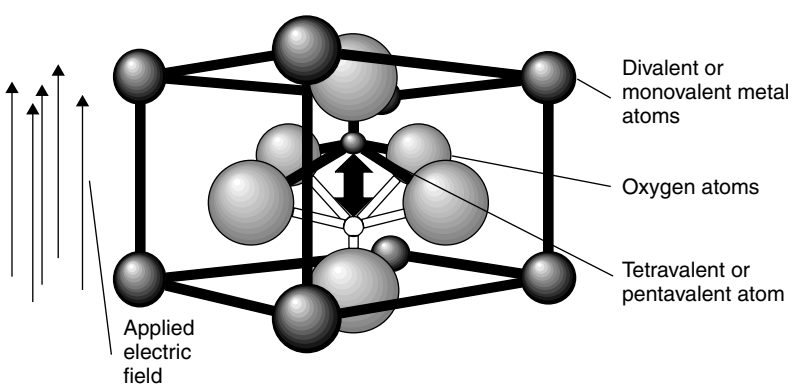


Figure 10.34 Basic configuration of a ferroelectric crystal lattice: an electric field steers the inner atom between two stable states

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

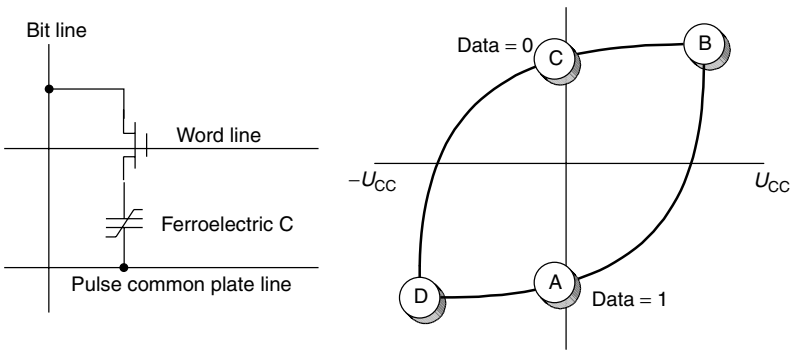


Figure 10.35 FRAM cell structure (1 bit) and hysteresis loop of the ferroelectric capacitor

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

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

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 μs. 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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

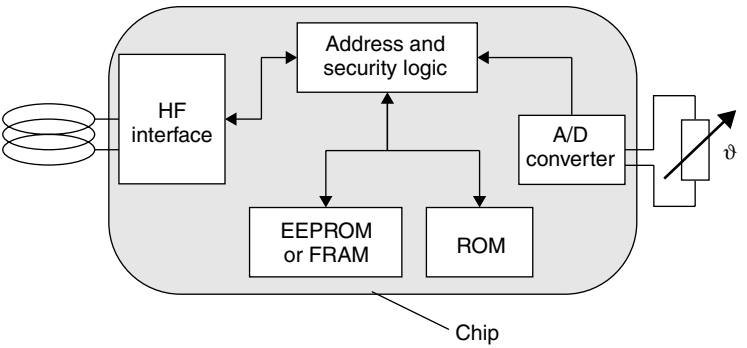


Figure 10.36 Inductively coupled transponder with additional temperature sensor

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).

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

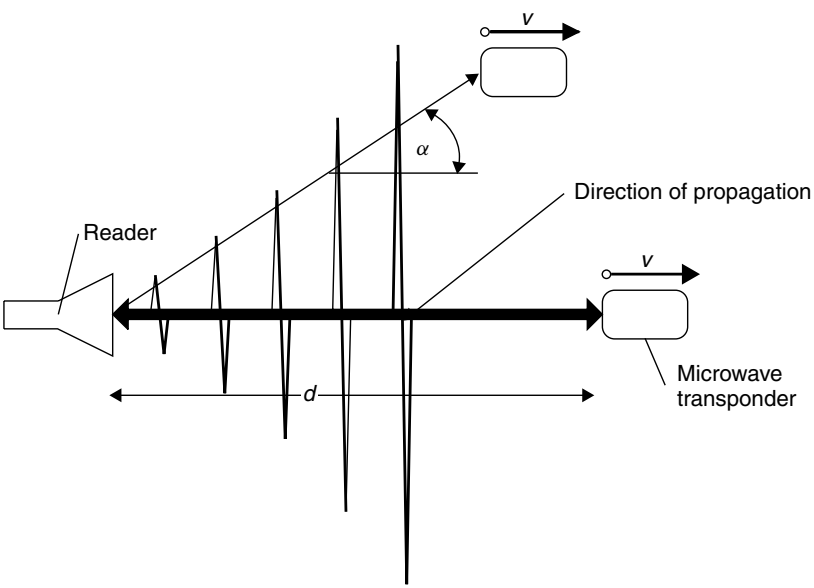


Figure 10.37 Distance and speed measurements can be performed by exploiting the Doppler effect and signal travelling times

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 α between the direction of propagation of the microwaves.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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:

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

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

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, 3×10^8 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 4.5.4.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

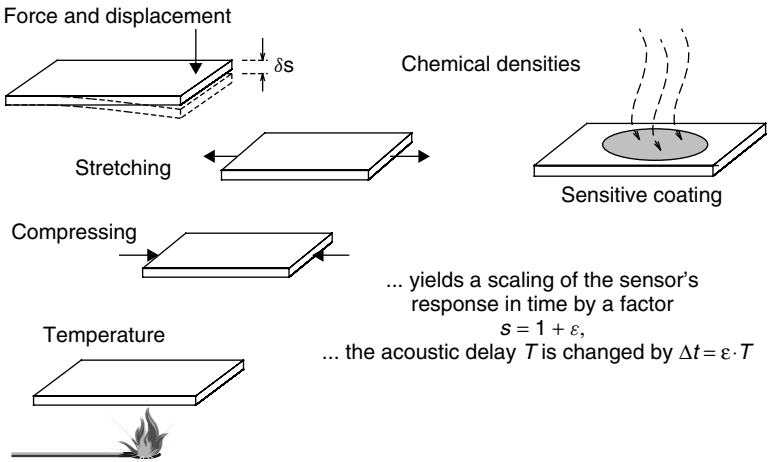


Figure 10.38 Influence of quantities on the velocity v of the surface wave in piezocrystal are shear, tension, compression and temperature. Even chemical quantities can be detected if the surface of the crystal is suitably coated (reproduced by permission of Technische Universität Wien, Institut für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

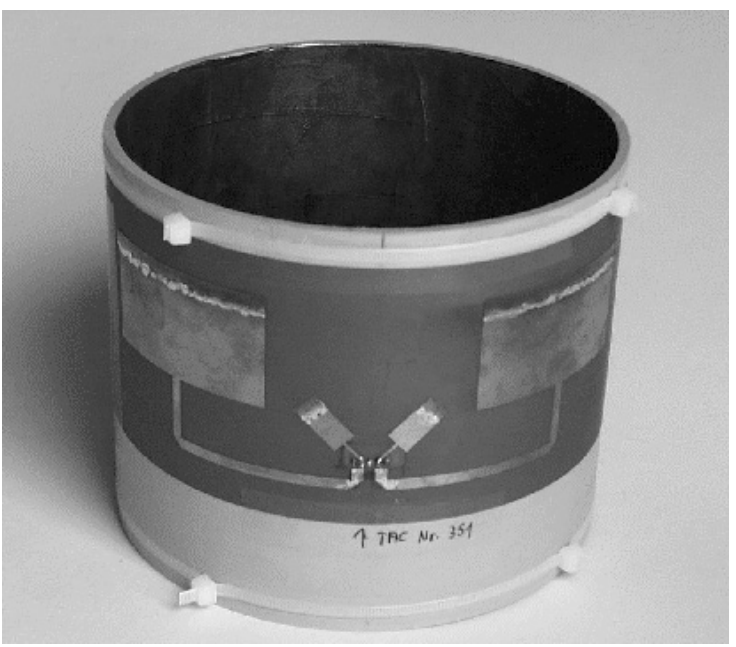


Figure 10.39 Arrangement for measuring the temperature and torque of a drive shaft using surface wave transponders. The antenna of the transponder for the frequency range 2.45 GHz is visible on the picture (reproduced by permission of Siemens AG, ZT KM, Munich)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

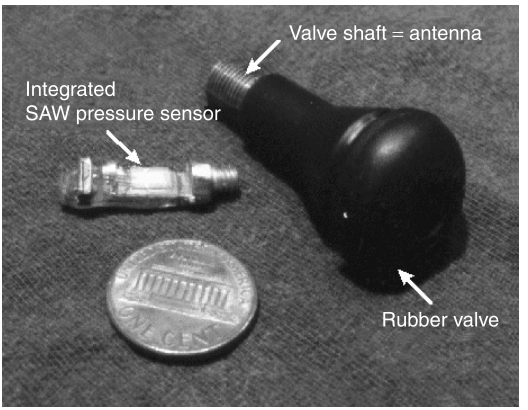


Figure 10.40 A surface wave transponder is used as a pressure sensor in the valve shaft of a car tyre valve for the wireless measurement of tyre pressure in a moving vehicle (reproduced by permission of Siemens AG, ZT KM, Munich

The working range of surface wave transponders extends to low temperatures of $-196\,^{\circ}\mathrm{C}$ (liquid nitrogen) and in a vacuum it even extends to very low temperatures.[1]

The normal surface wave crystals have only limited suitability for high temperatures. For example, in lithium niobate segregation occurs at a temperature of just $300\,^{\circ}\mathrm{C}$; in quartz there is a phase transition at $573\,^{\circ}\mathrm{C}$. Moreover, at temperatures above $400\,^{\circ}\mathrm{C}$ 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 $1000\,^{\circ}\mathrm{C}$ can be used (Reindl *et al.*, 1998b).

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

[1] At very low temperatures, however, the sensitivity S of a SAW transponder ultimately tends towards zero.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

11
Readers

11.1 Data Flow in an Application

A *software application* that is designed to read data from a contactless data carrier (transponder) or write data to a contactless data carrier, requires a contactless *reader* as an interface. From the point of view of the application software, access to the data carrier should be as transparent as possible. In other words, the read and write operations should differ as little as possible from the process of accessing comparable data carriers (smart card with contacts, serial EEPROM).

Write and read operations involving a contactless data carrier are performed on the basis of the *master–slave principle* (Figure 11.1). This means that all reader and transponder activities are initiated by the application software. In a hierarchical system structure the application software represents the master, while the reader, as the slave, is only activated when write/read commands are received from the application software.

To execute a command from the application software, the reader first enters into communication with a transponder. The reader now plays the role of the master in relation to the transponder. The transponder therefore only responds to commands from the reader and is never active independently (except for the simplest read-only transponders. See Chapter 10).

A simple read command from the application software to the reader can initiate a series of communication steps between the reader and a transponder. In the example in Table 11.1, a read command first leads to the activation of a transponder, followed by the execution of the authentication sequence and finally the transmission of the requested data.

The reader's main functions are therefore to activate the data carrier (transponder), structure the communication sequence with the data carrier, and transfer data between the application software and a contactless data carrier. All features of the contactless communication, i.e. making the connection, and performing anticollision and authentication procedures, are handled entirely by the reader.

11.2 Components of a Reader

A number of contactless transmission procedures have already been described in the preceding chapters. Despite the fundamental differences in the type of coupling

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

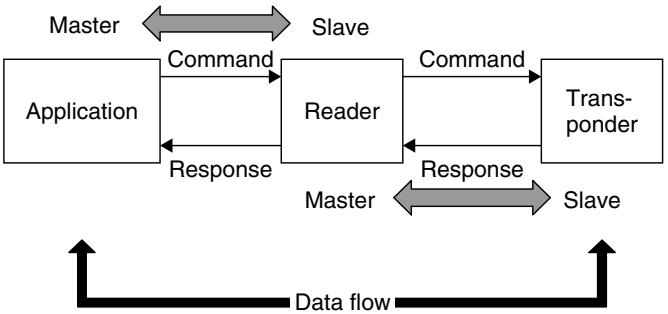


Figure 11.1 Master–slave principle between application software (application), reader and transponder

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

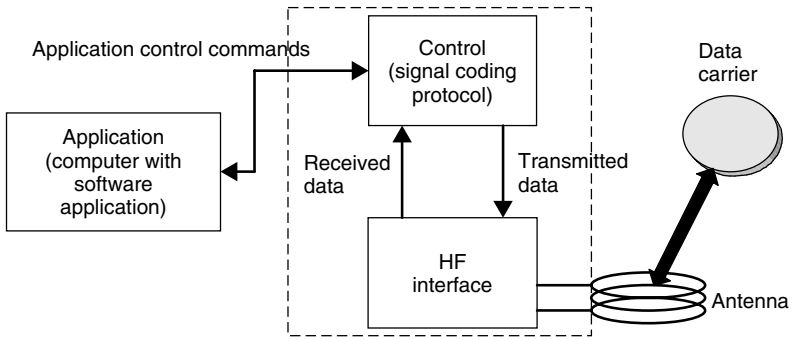


Figure 11.2 Block diagram of a reader consisting of control system and HF interface. The entire system is controlled by an external application via control commands

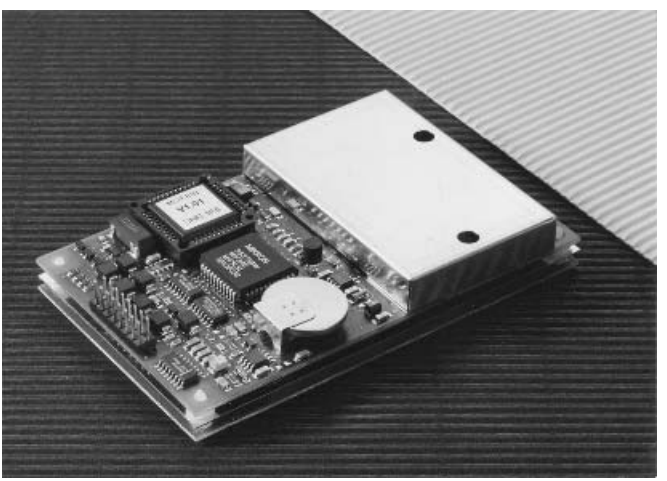


Figure 11.3 Example of a reader. The two functional blocks, HF interface and control system, can be clearly differentiated (MIFARE® reader, reproduced by permission of Philips Electronics N.V.)

11.2.1 HF interface

The reader's HF interface performs the following functions:

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

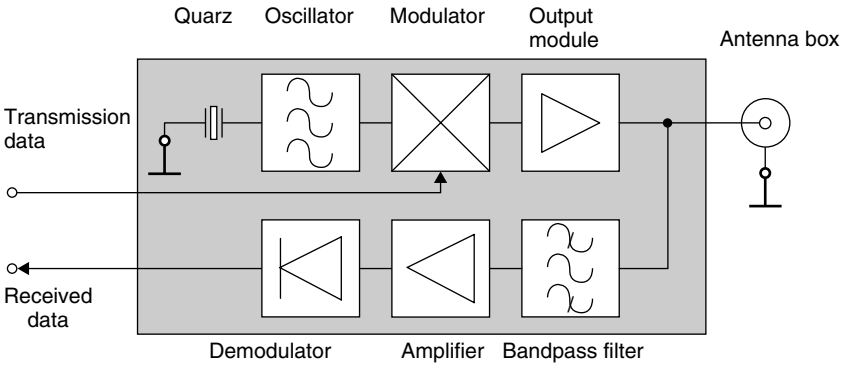


Figure 11.4 Block diagram of an HF interface for an inductively coupled RFID system

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

11.2.1.1 Inductively coupled system, FDX/HDX

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

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

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

11.2.1.2 Microwave systems – half duplex

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

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

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

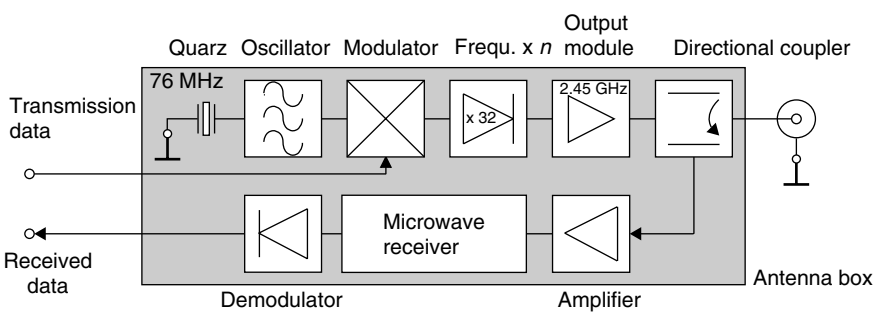


Figure 11.5 Block diagram of an HF interface for microwave systems

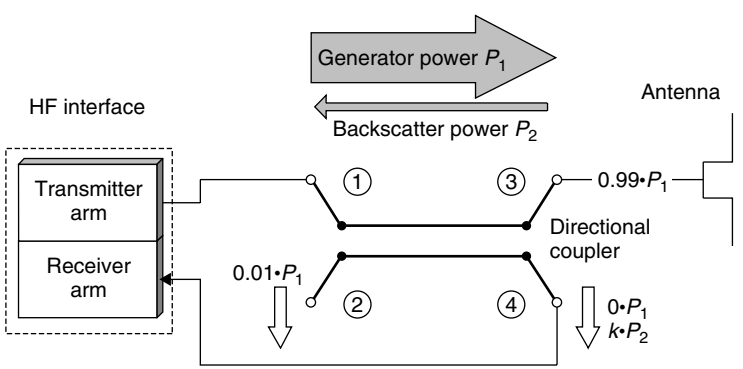


Figure 11.6 Layout and operating principle of a directional coupler for a backscatter RFID system

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

and *directivity*:

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

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

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

11.2.1.3 Sequential systems – SEQ

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

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

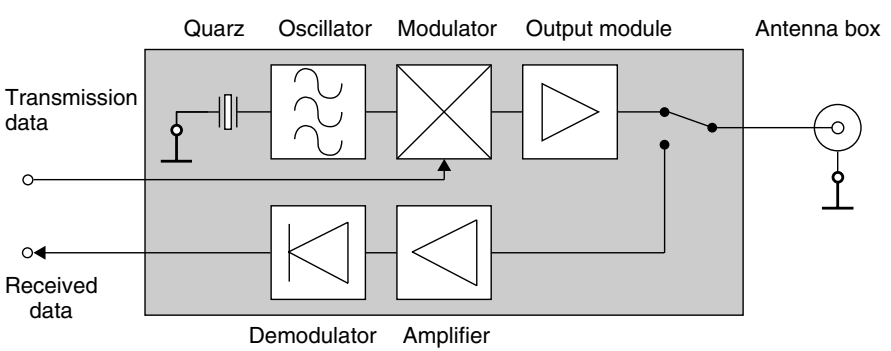


Figure 11.7 HF interface for a sequential reader system

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

11.2.1.4 Microwave system for SAW transponders

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

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

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

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

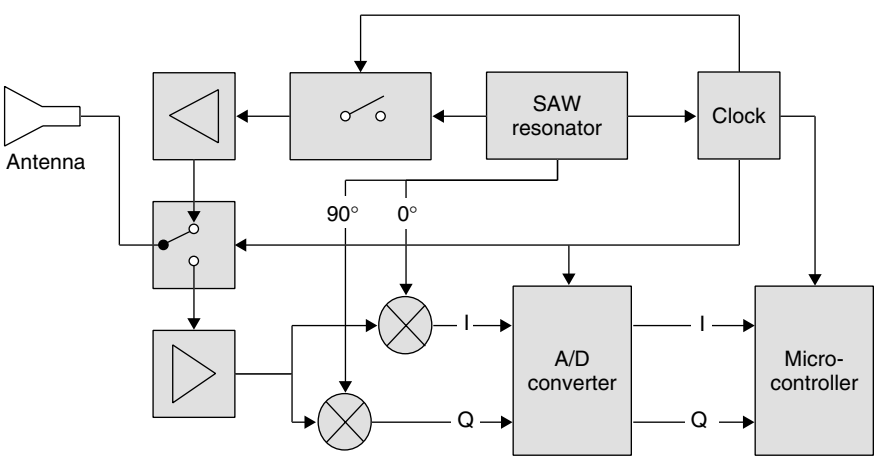


Figure 11.8 Block diagram of a reader for a surface wave transponder

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

11.2.2 Control unit

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

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

In more complex systems the following additional functions are available:

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

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

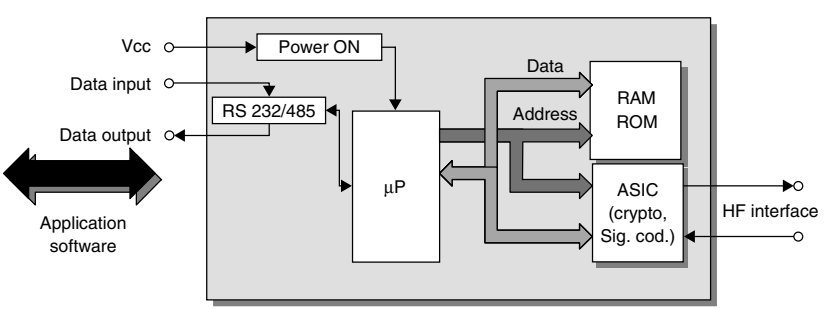


Figure 11.9 Block diagram of the control unit of a reader. There is a serial interface for communication with the higher application software

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

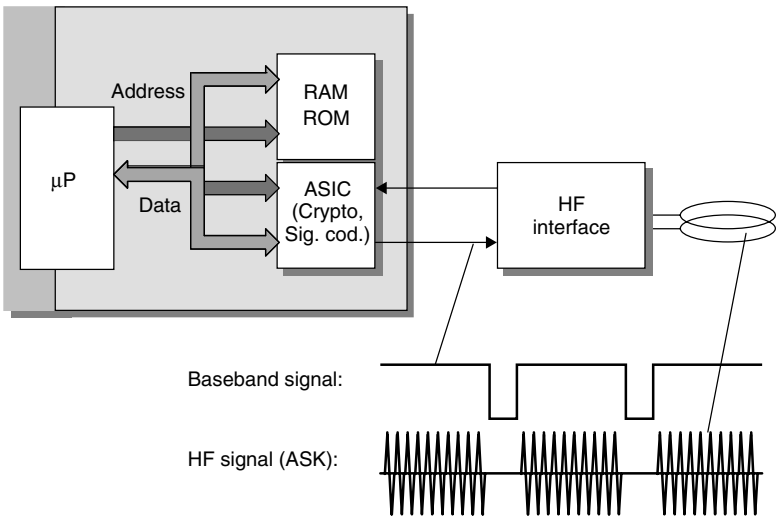


Figure 11.10 Signal coding and decoding is also performed by the control unit in the reader

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

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

11.3 Low Cost Configuration – Reader IC U2270B

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

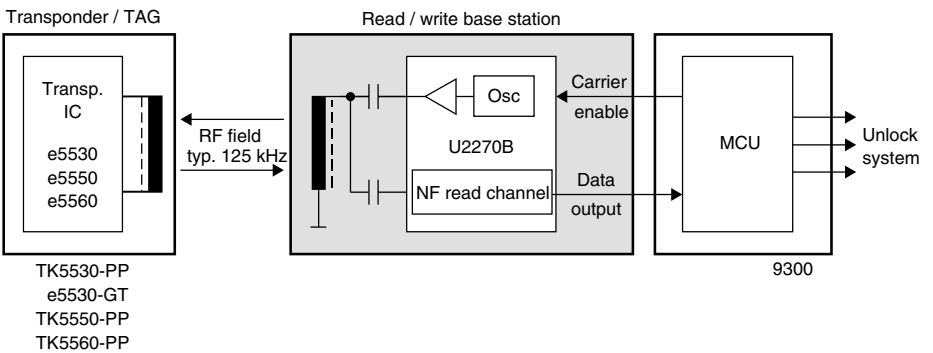


Figure 11.11 The low-cost reader IC U2270B represents a highly integrated HF interface. The control unit is realised in an external microprocessor (MCU) (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

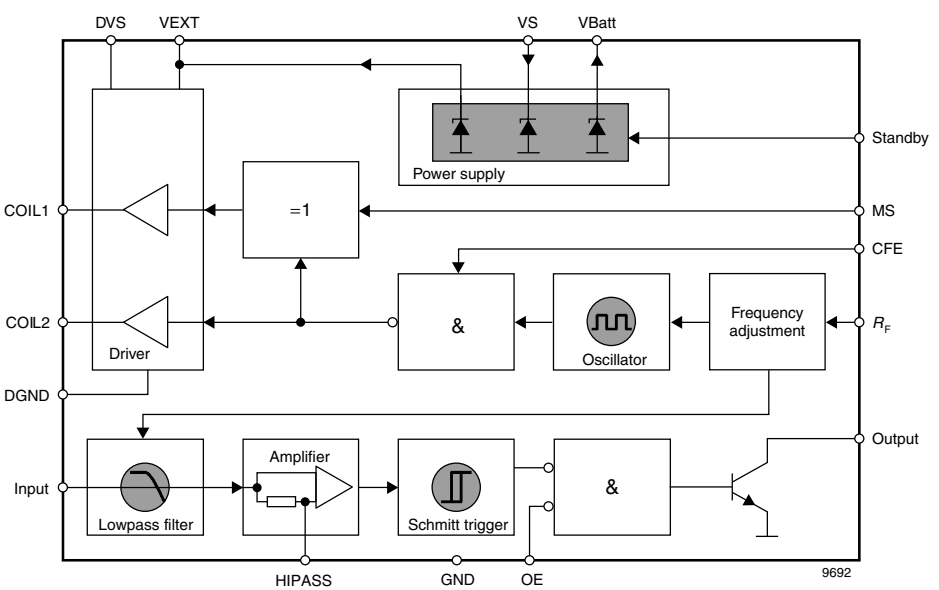


Figure 11.12 Block diagram of the reader IC U2270B. The transmitter arm consists of an oscillator and driver to supply the antenna coil. The receiver arm consists of filter, amplifier and a Schmitt trigger (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

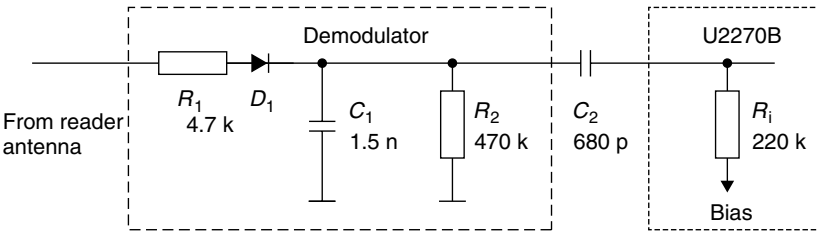


Figure 11.13 Rectification of the amplitude modulated voltage at the antenna coil of the reader (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

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

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

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

11.4 Connection of Antennas for Inductive Systems

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

11.4.1 Connection using current matching

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

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

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

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

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

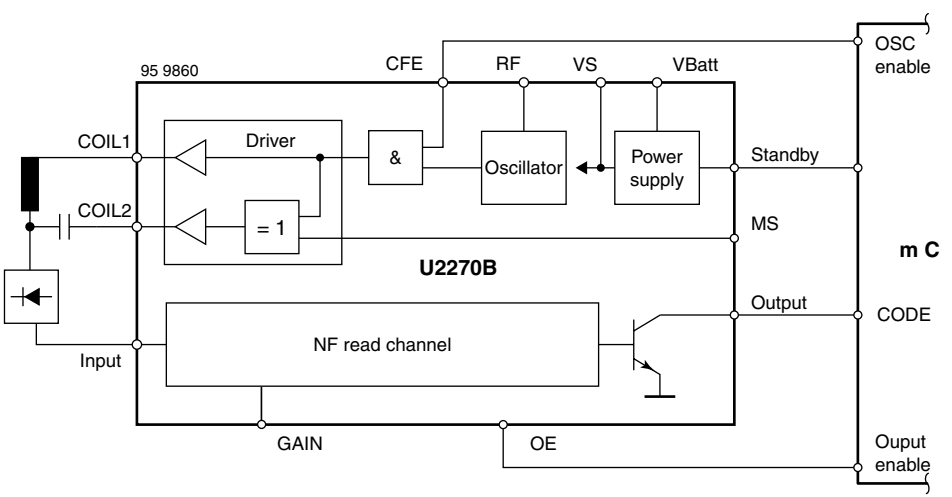


Figure 11.14 Block diagram for the reader IC U2270B with connected antenna coil at the push–pull output (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

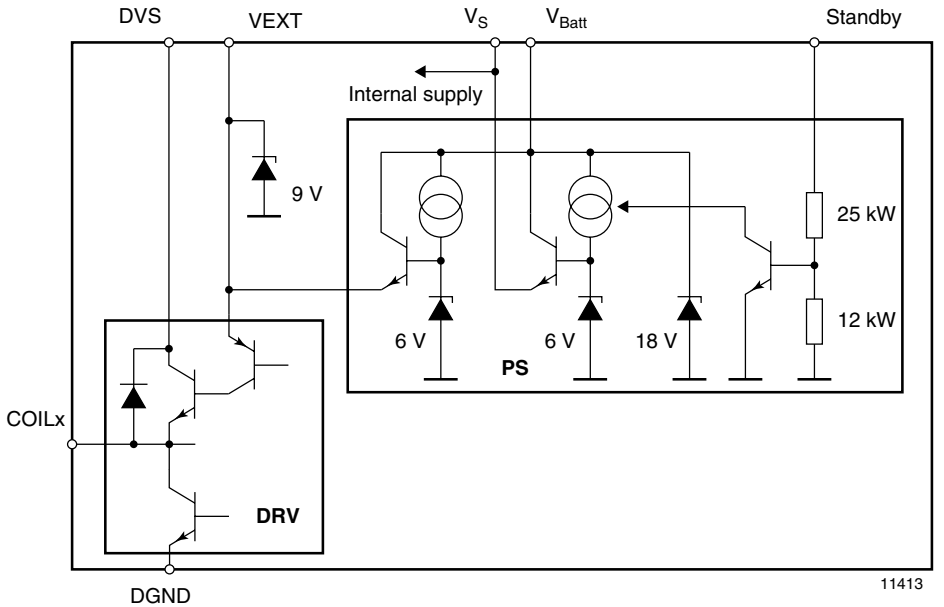


Figure 11.15 Driver circuit in the reader IC UU2270B (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

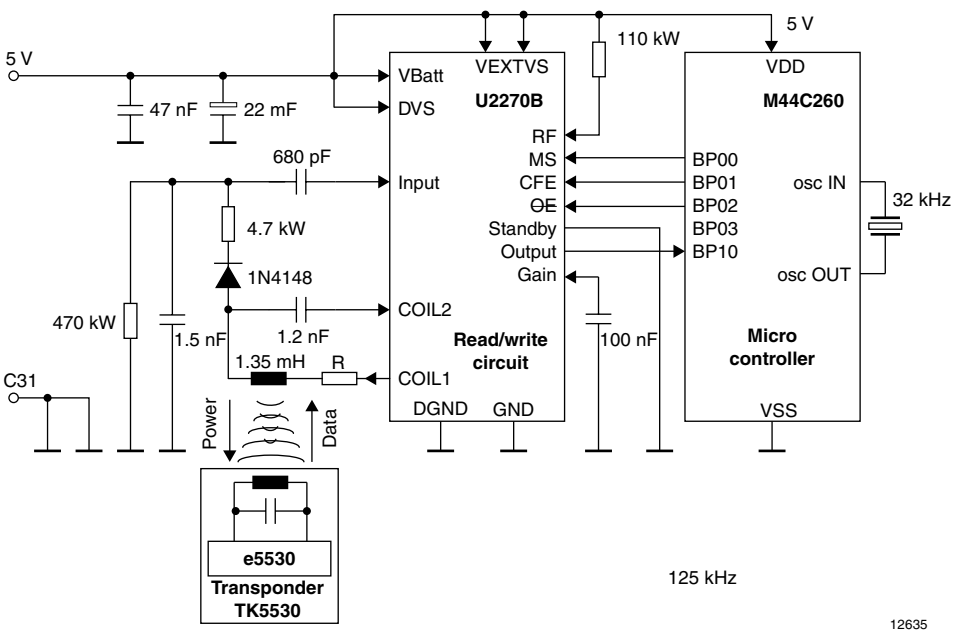


Figure 11.16 Complete example application for the low cost reader IC U2270B (reproduced by permission of TEMIC Semiconductor GmbH, Heilbronn)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

11.4.2 Supply via coaxial cable

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

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

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

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

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

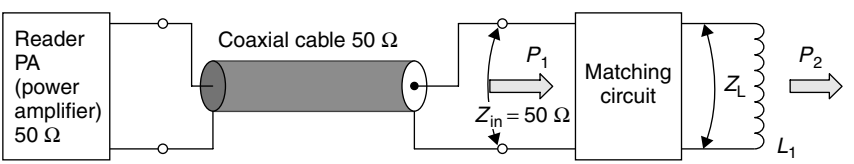


Figure 11.17 Connection of an antenna coil using 50 Ω technology

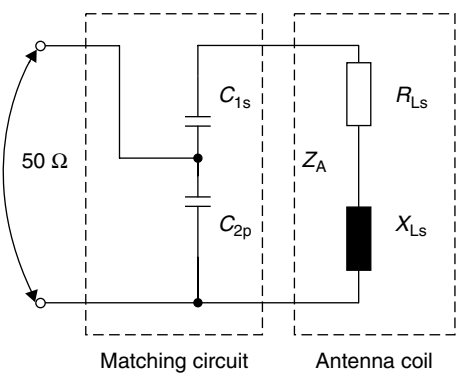


Figure 11.18 Simple matching circuit for an antenna coil

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

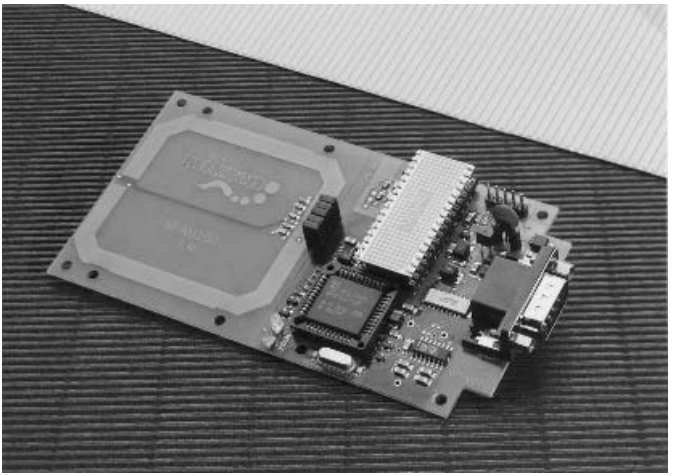


Figure 11.19 Reader with integral antenna and matching circuit (MIFARE®-reader, reproduced by permission of Philips Electronics N.V.)

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

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

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

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

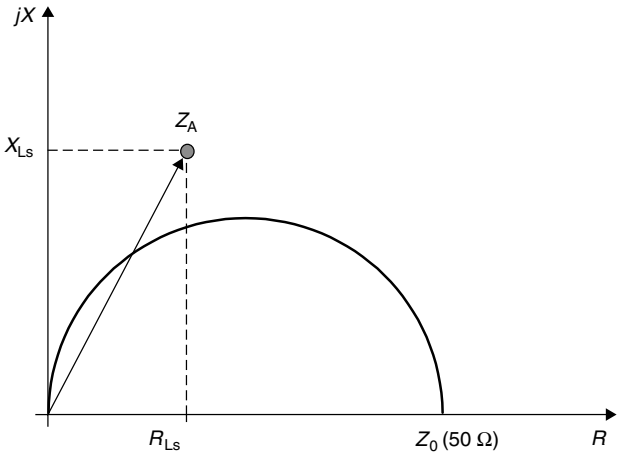


Figure 11.20 Representation of Z_A in the impedance level (Z plane)

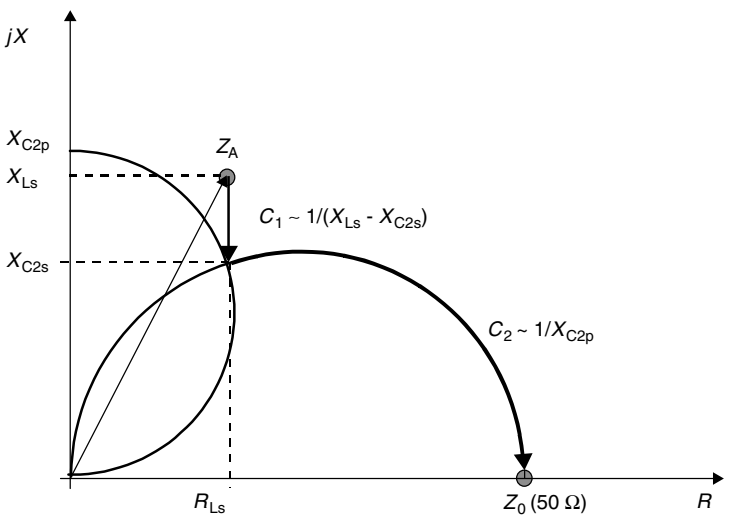


Figure 11.21 Transformation path with C_{ls} and C_{2p}

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

We further find for C_{ls}:

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

11.4.3 The influence of the Q factor

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

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

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

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

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

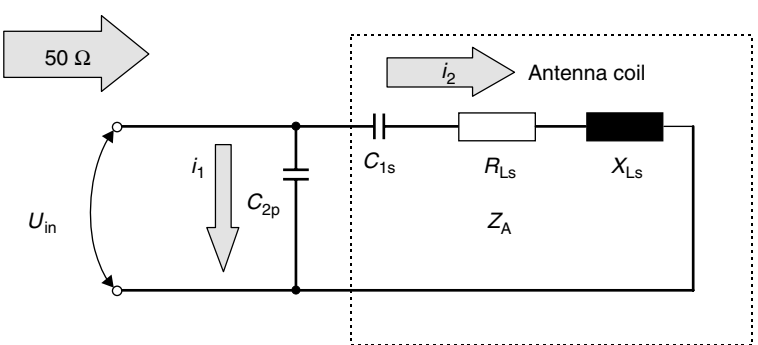


Figure 11.22 The matching circuit represented as a current divider

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

11.5 Reader Designs

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

11.5.1 OEM readers

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

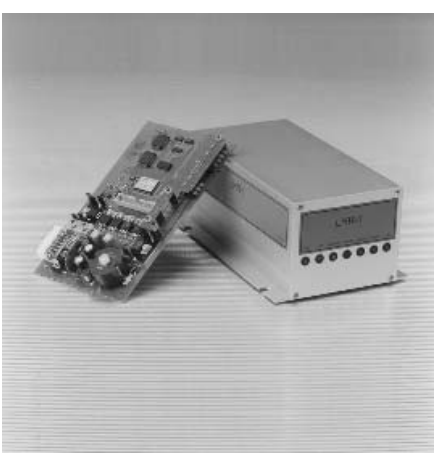


Figure 11.23 Example of an OEM reader for use in terminals or robots (photo: Long-Range/High-Speed Reader LHRI, reproduced by permission of SCEMTEC Transponder Technology GmbH, Reichshof-Wehnrath)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 11.2 Typical technical data

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

Table 11.3 Typical technical data

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

Table 11.4 Typical technical data

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



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

11.5.2 Readers for industrial use

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

11.5.3 Portable readers

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

12

The Manufacture of Transponders and Contactless Smart Cards

12.1 Glass and Plastic Transponders

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

12.1.1 Module manufacture

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

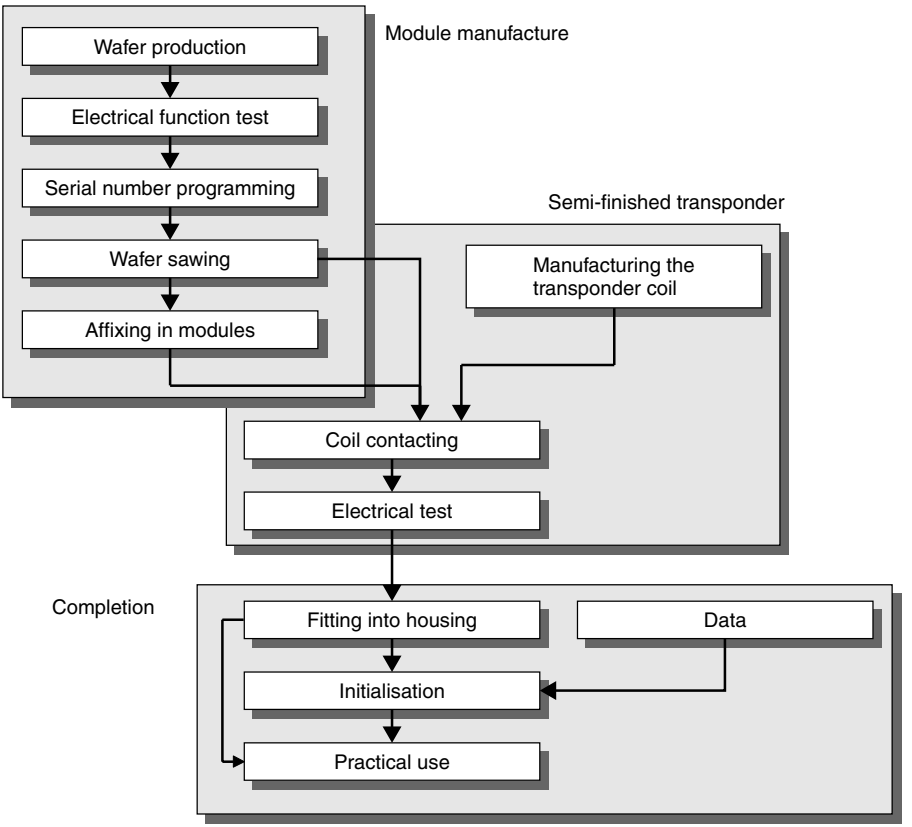


Figure 12.1 Transponder manufacture

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

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

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

12.1.2 Semi-finished transponder

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

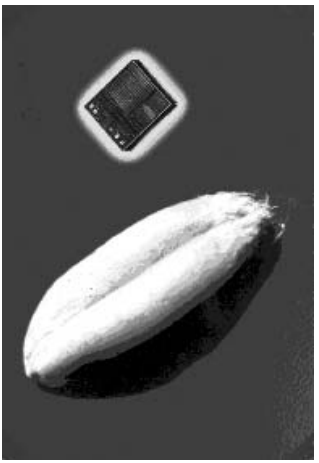


Figure 12.2 Size comparison of a sawn die with a cereal grain. The size of a transponder chip varies between 1 mm^2 and 15 mm^2 depending upon its function (photo: HITAG® Multimode-Chip, reproduced by permission of Philips Electronics N.V.)

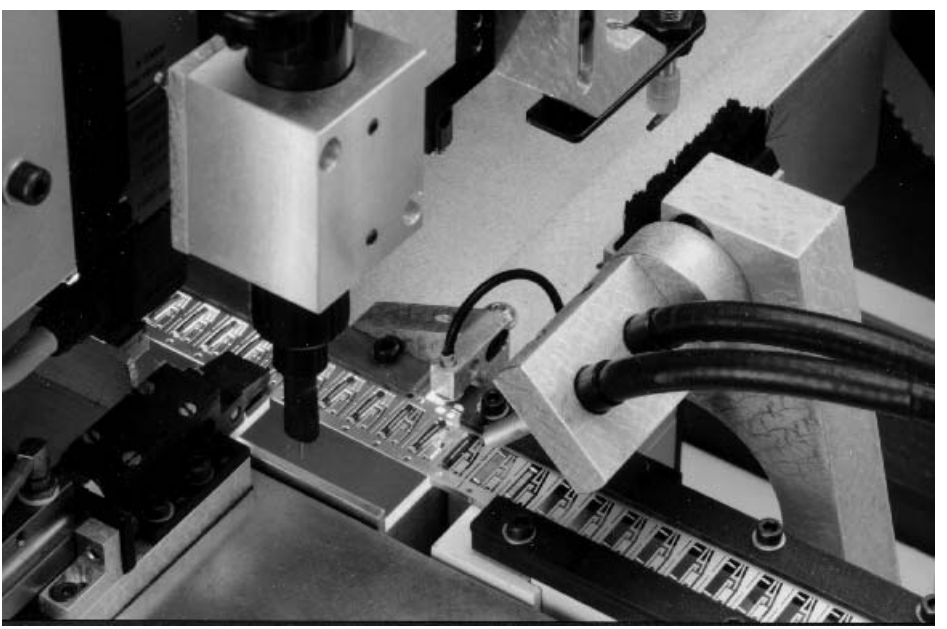


Figure 12.3 Manufacture of plastic transponders. In the figure an endless belt is fitted with transponder coils wound onto a ferrite core. After the transponder chip has been fitted and contacted, the transponder on the belt is sprayed with plastic (reproduced by permission of AmaTech GmbH & Co. KG,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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

12.1.3 Completion

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

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

12.2 Contactless Smart Cards

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

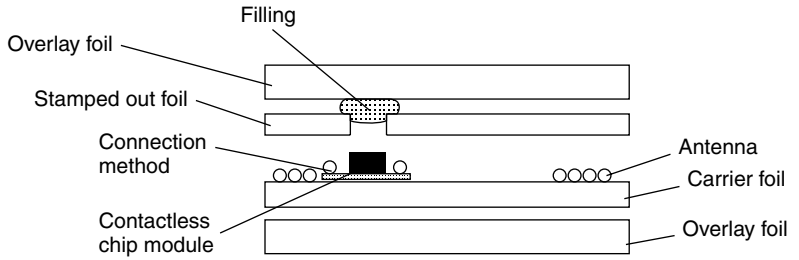


Figure 12.4 Foil structure of a contactless smart card

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

12.2.1 Coil manufacture

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

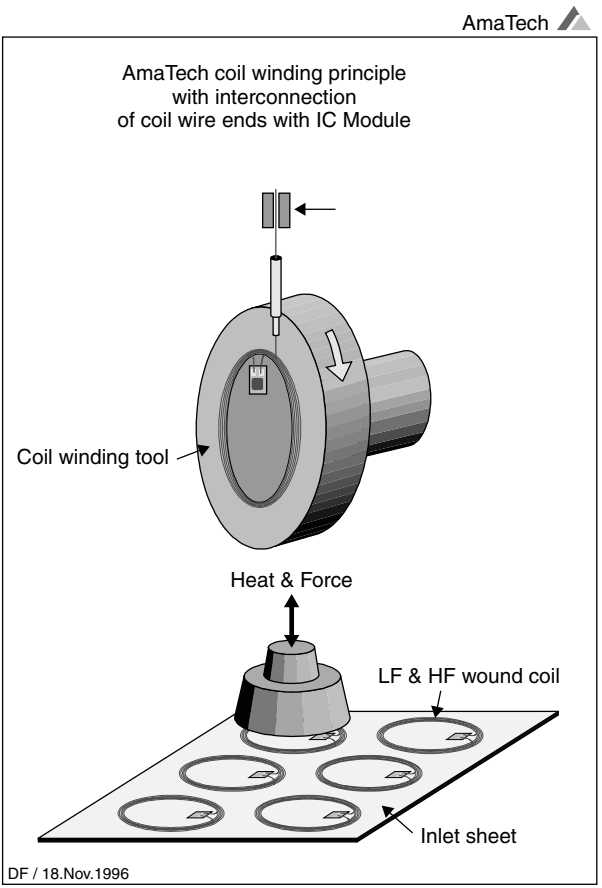


Figure 12.5 Production of a semi-finished transponder by winding and placing the semi-finished transponder on an inlet sheet (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

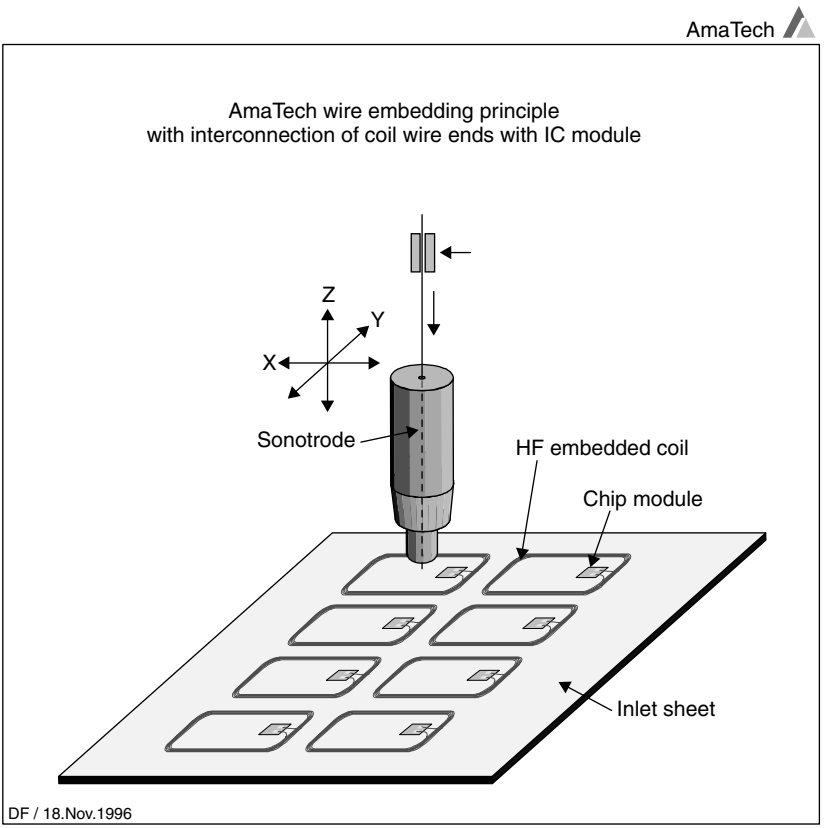


Figure 12.6 Manufacture of an inlet sheet using the embedding principle (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

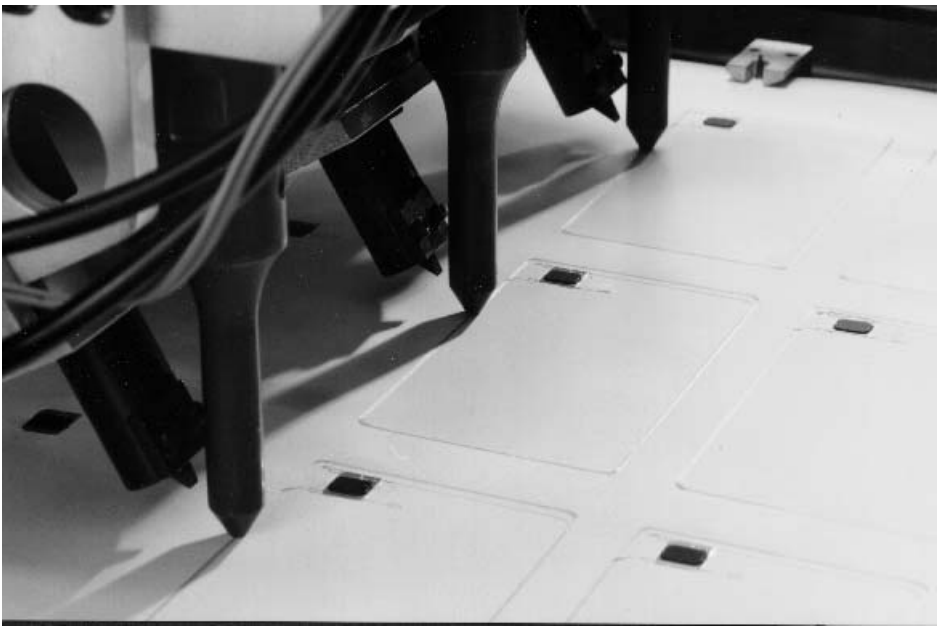


Figure 12.7 Manufacture of a smart card coil using the embedding technique on an inlet foil. The sonotrodes, the welding electrodes (to the left of the sonotrodes) for contacting the coils, and some finished transponder coils are visible (reproduced by permission of AmaTech GmbH & Co. KG, Pfronten)



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

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

12.2.2 Connection technique

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

Conductor	Surface resistance
Silver (Ag)	5–20 mΩ/□
Copper (Cu)	30–120 mΩ/□
Graphite (carbon)	20 000–100 000 mΩ/□

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

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

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

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

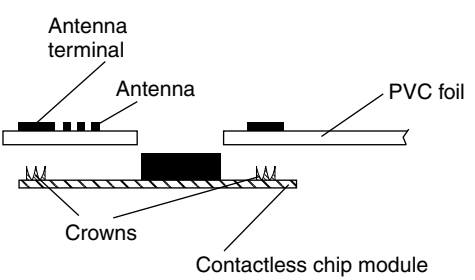


Figure 12.9 Contacting of a chip module to a printed or etched antenna by means of cut clamp technology

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

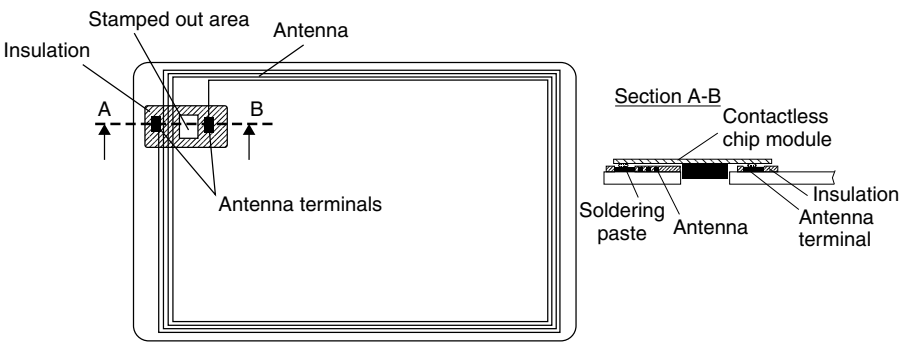


Figure 12.10 Soldered connection between the chip module and an etched antenna

12.2.3 Lamination

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

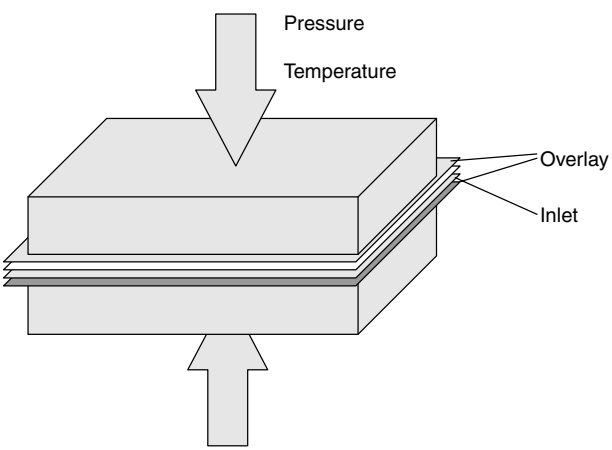


Figure 12.11 During the lamination procedure the PVC sheets are melted at high pressure and temperatures up to 150 °C

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

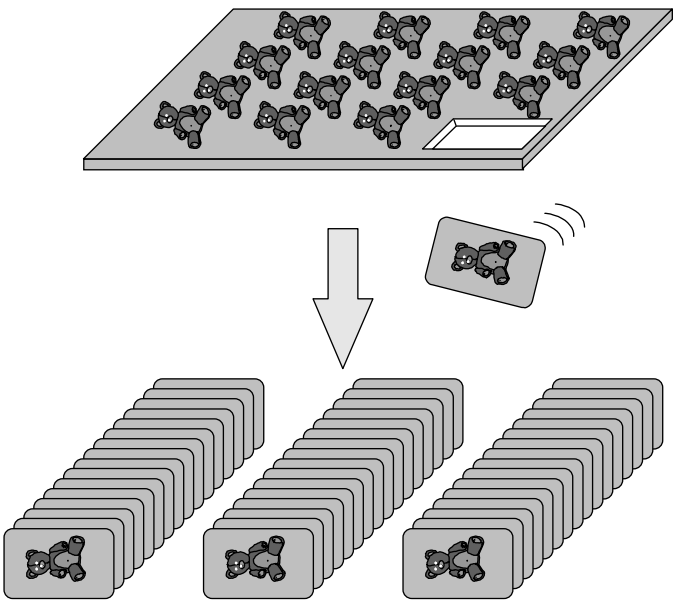


Figure 12.12 After the cooling of the PVC sheets the individual cards are stamped out of the multi-purpose sheets

of heat, the foils are brought into a soft elastic state at high pressure (approximately 100–150 °C). This 'bakes' the four sheets to create a permanent bond (Figure 12.11).

After the *lamination* and cooling of the laminated PVC foils, the individual smart cards are stamped out of the multi-purpose sheet (Figure 12.12). A subsequent functional test ensures the quality of the cards before these can be sent to the customer.

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

13
Example Applications

13.1 Contactless Smart Cards

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

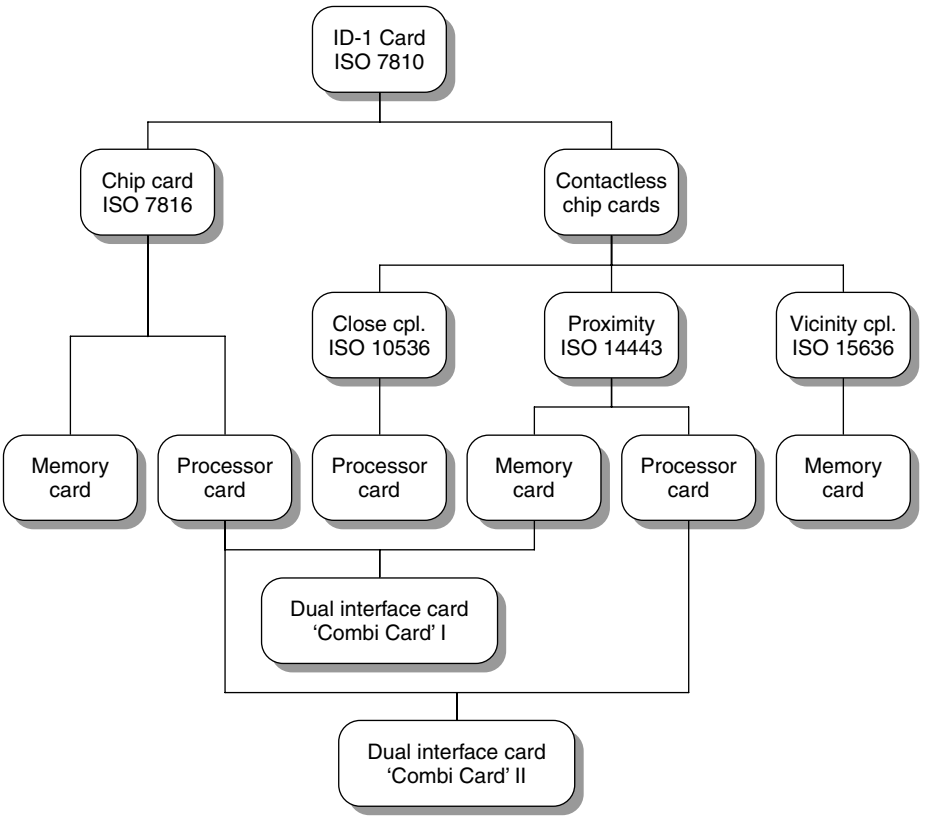


Figure 13.1 The large 'family' of smart cards, including the relevant ISO standard

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

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

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

13.2 Public Transport

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

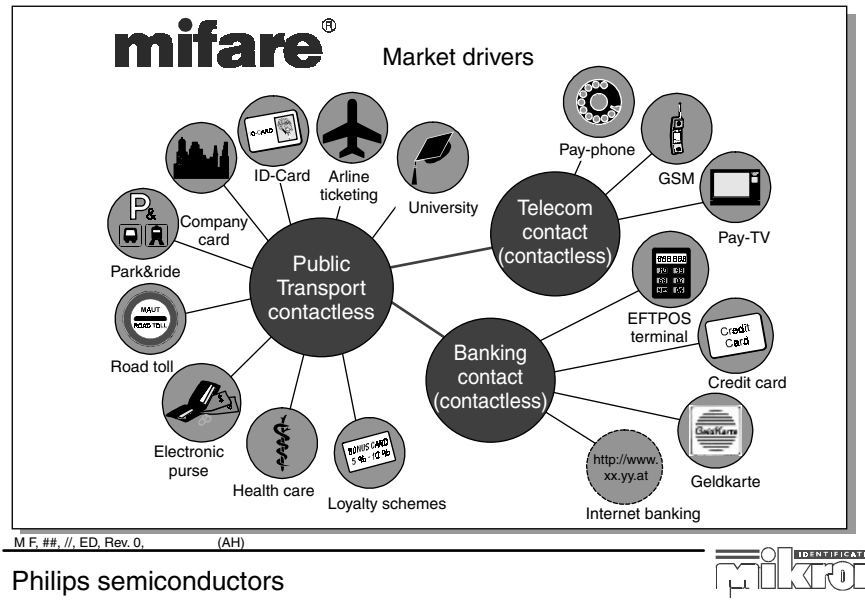


Figure 13.2 The main fields of application for contactless smart cards are public transport and change systems for telephone boxes or consumer goods (groceries, cigarettes) (reproduced by permission of Philips Electronics N.V.)

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

13.2.1 The starting point

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

13.2.2 Requirements

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

13.2.2.1 Transaction time

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

13.2.2.2 Resistance to degradation, lifetime, convenience

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

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

13.2.3 Benefits of RFID systems

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

Benefits for passengers

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

Benefits for the driver

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

Benefits for the transport company

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

Benefits for the transport association

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

Benefits for the treasury

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

13.2.4 Fare systems using electronic payment

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

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

13.2.5 Market potential

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 13.2 Different fare systems for payment with contactless smart card

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

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

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

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

13.2.6 Example projects

13.2.6.1 Korea – Seoul

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

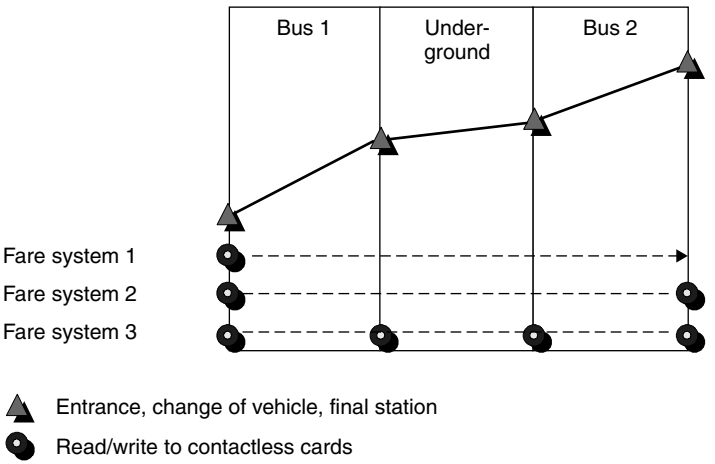


Figure 13.4 Use of the different tariff systems in a journey by public transport. The journey shown involves two changes between the underground and bus network. The number of times the smart card is read depends upon the fare system used



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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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



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

13.2.6.2 Germany – Lüneburg, Oldenburg

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

13.2.6.3 EU Projects – ICARE and CALYPSO

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

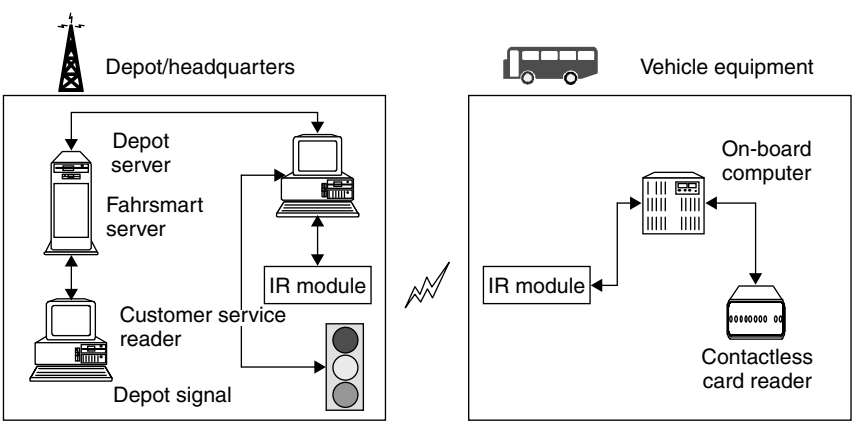


Figure 13.8 System components of the Fahrsmart system. The vehicle equipment consists of a reader for contactless smart cards, which is linked to the on-board computer. Upon entry into the station, the record data is transferred from the on-board computer to a depot server via an infrared link

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

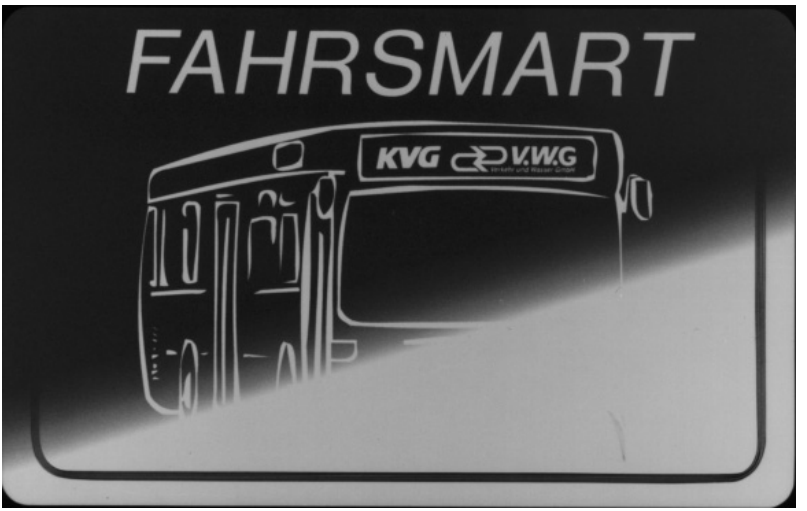


Figure 13.9 Fahrsmart II contactless smart card, partially cut away. The transponder coil is clearly visible at the lower right-hand edge of the picture (reproduced by permission of Giesecke & Devrient, Munich)

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

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

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

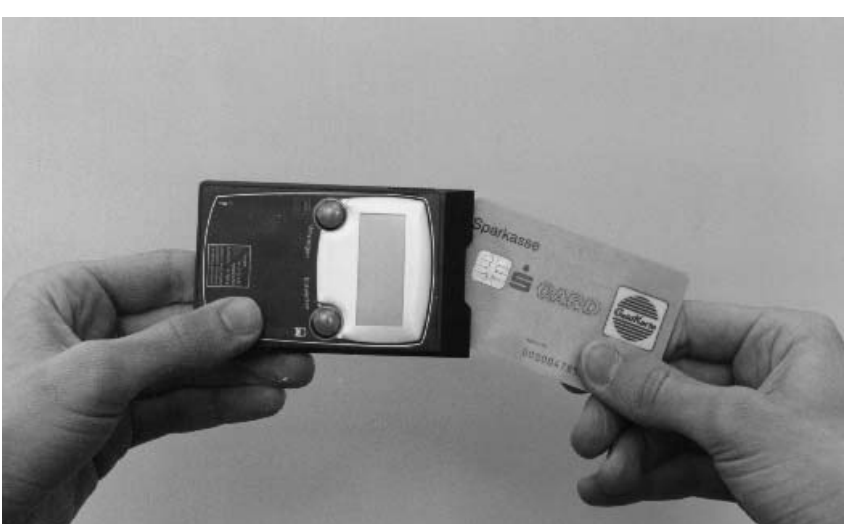


Figure 13.10 The contactless FlexPass of the district of Constance showing the GeldKarte and envelope (reproduced by permission of TCAC GmbH, Dresden)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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



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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

13.3 Ticketing

13.3.1 Lufthansa miles & more card

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

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

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

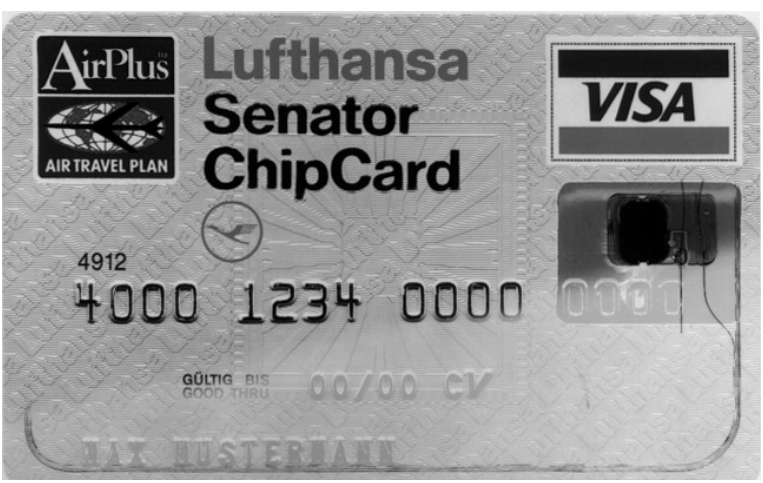


Figure 13.12 Miles & More — Senator ChipCard, partially cut away. The transponder module and antenna are clearly visible at the right-hand edge of the picture underneath the hologram (reproduced by permission of Giesecke & Devrient, Munich)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

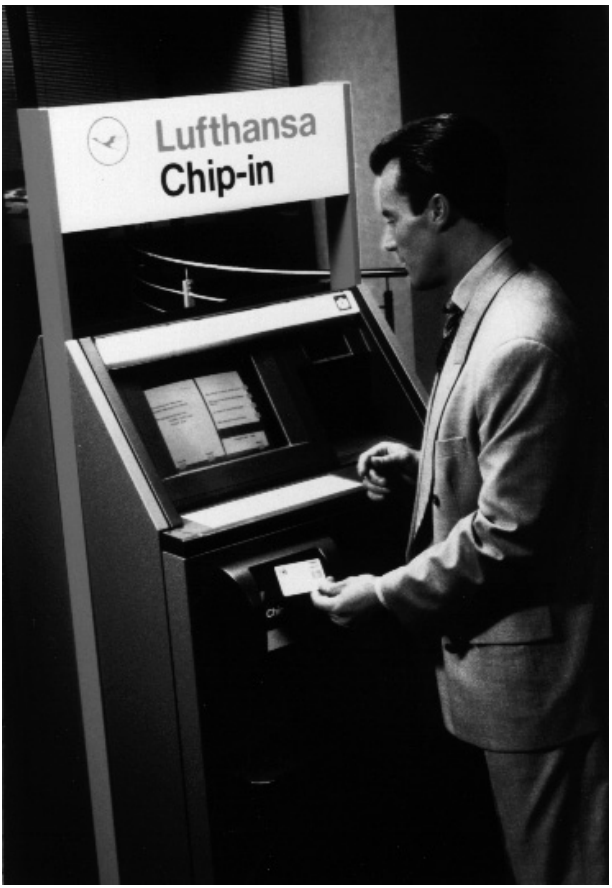


Figure 13.13 Passenger checking in using the contactless Miles & More Frequent Flyer Card (reproduced by permission of Lufthansa)

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

13.3.2 Ski tickets

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

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

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

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

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



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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

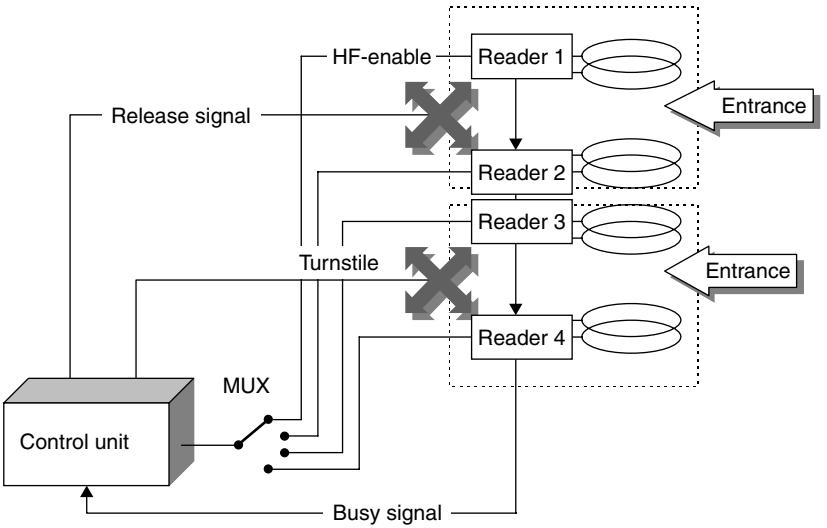


Figure 13.15 To achieve mutual decoupling the readers are switched alternately in time-division multiplex operation

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

13.4 Access Control

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

13.4.1 Online systems

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

13.4.2 Offline systems

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

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



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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

13.4.3 Transponders

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

13.5 Transport Systems

13.5.1 Eurobalise S21

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

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

The ETCS comprises four main systems:

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

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

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

Four different balise types have been developed by Siemens:

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

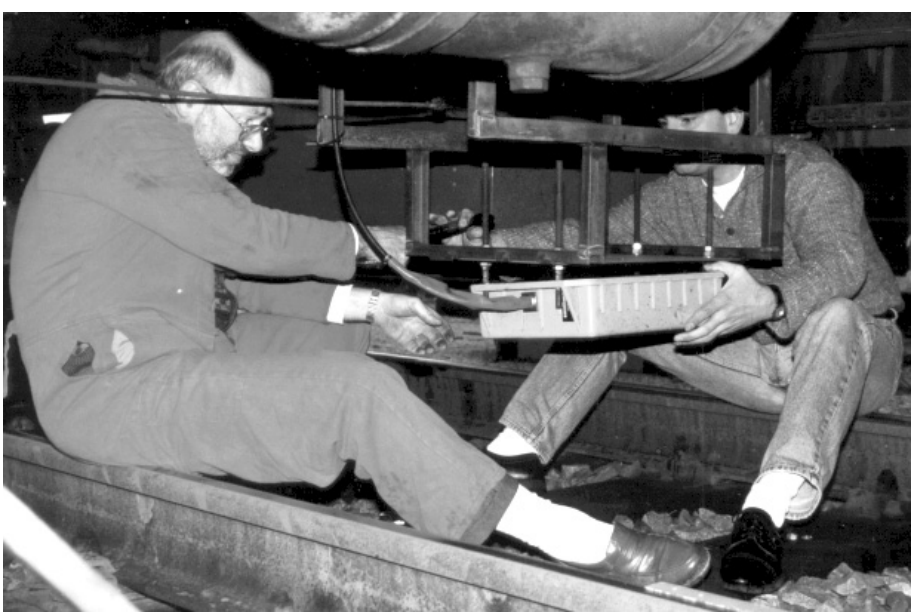


Figure 13.20 Fitting a read antenna for the Euro balise onto a tractive unit (reproduced by permission of Siemens Verkehrstechnik, Braunschweig)

HANSHOW-EX. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Table 13.3 Basic data for the Eurobalise

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

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

13.5.2 International container transport

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

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

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

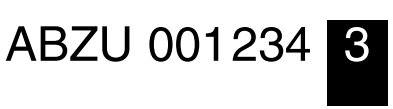


Figure 13.21 Container identification mark, consisting of owner's code, serial number and a test digit

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

13.6 Animal Identification

13.6.1 Stock keeping

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

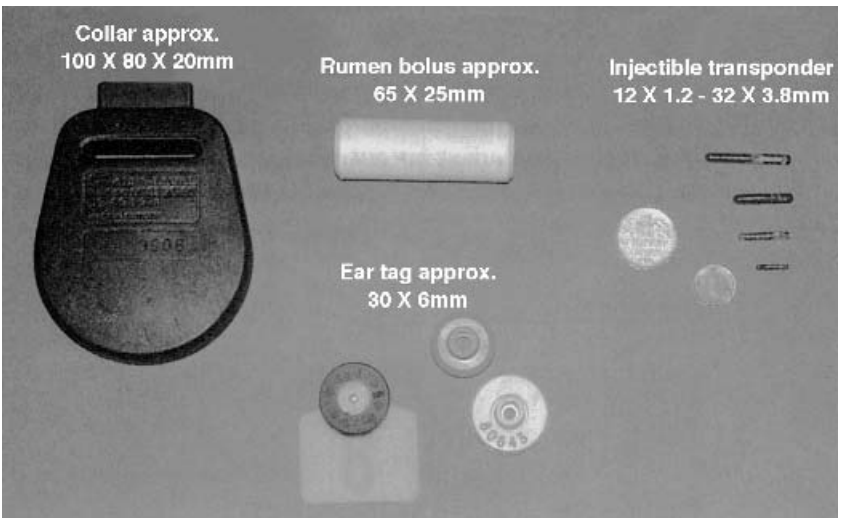


Figure 13.22 Size comparison of different variants of electronic animal identification transponders: collar transponder, rumen bolus, ear tags with transponder, injectible transponder (reproduced by permission of Dr Michael Klindtworth, Bayrische Landesanstalt für Landtechnik, Freising)

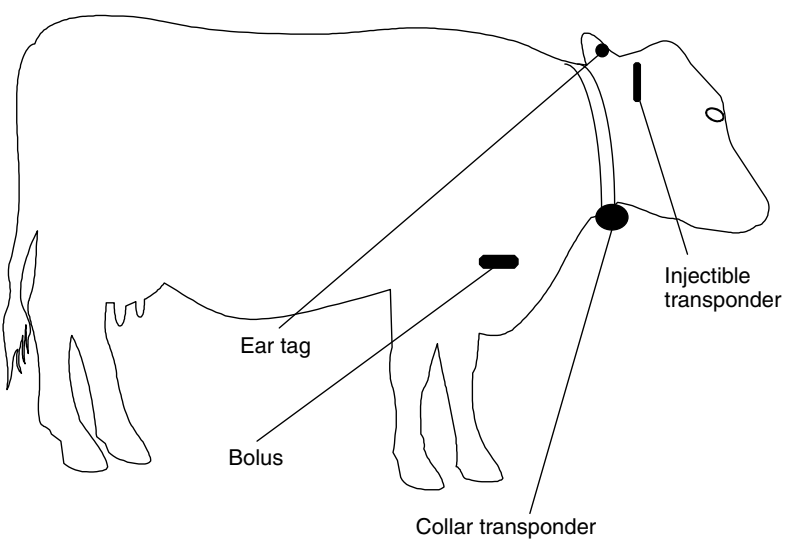


Figure 13.23 The options for attaching the transponder to a cow

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

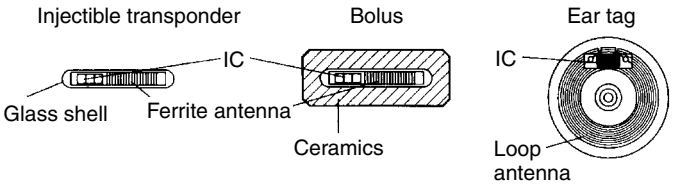


Figure 13.24 Cross-sections of various transponder designs for animal identification (reproduced by permission of Dr Georg Wendl, Landtechnischer Verein in Bayern e.V., Freising)

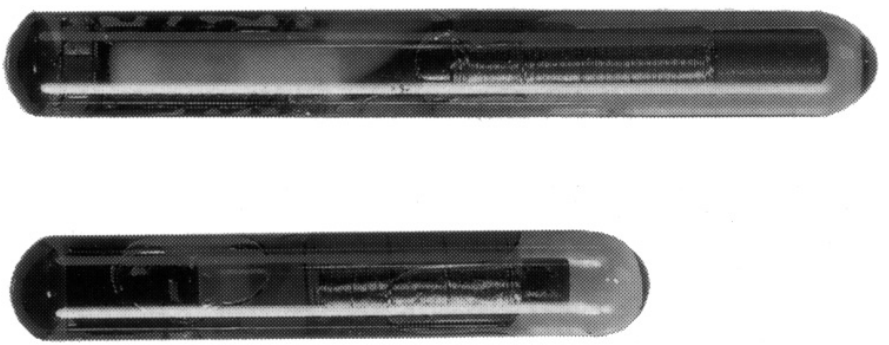


Figure 13.25 Enlargement of different types of glass transponder (reproduced by permission of Texas Instruments)

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

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

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

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

13.6.2 Carrier pigeon races

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

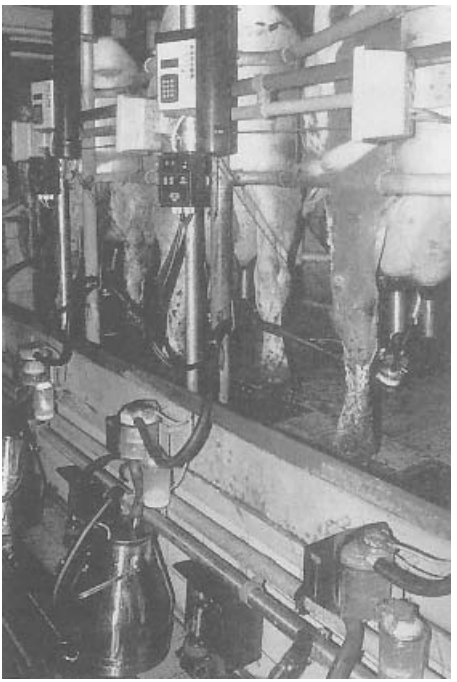


Figure 13.27 Automatic identification and calculation of milk production in the milking booth (reproduced by permission of Dr Georg Wendl, Landtechnischer Verein in Bayern e.V., Freising)



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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

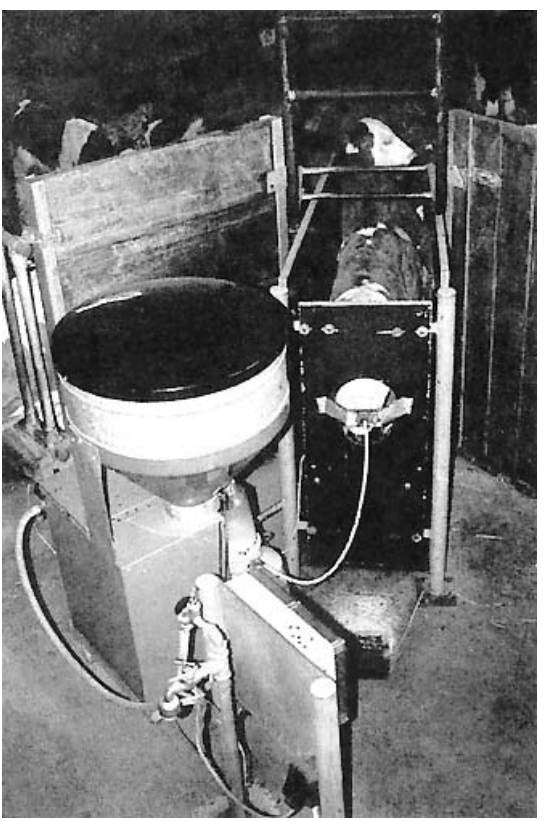


Figure 13.30 Example of automated animal recognition in practice: grouping calves properly for feeding often requires much time and effort. Here a machine takes on this task: the animals can receive an individually adjustable amount of milk in several small portions (reproduced by permission of Dr Michael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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

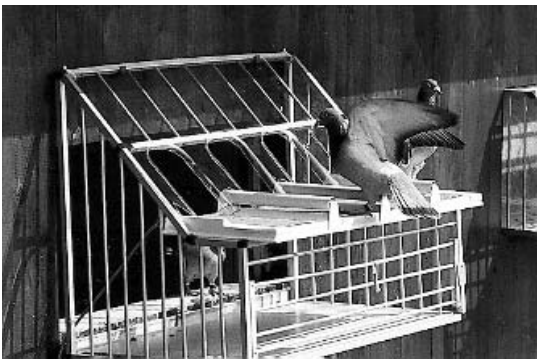


Figure 13.31 Pigeon upon arrival at its own pigeonry. Upon the pigeon's entry, the transponder in the ring is read (reproduced by permission of Legic Identsystems, CH-Wetzikon)

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

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

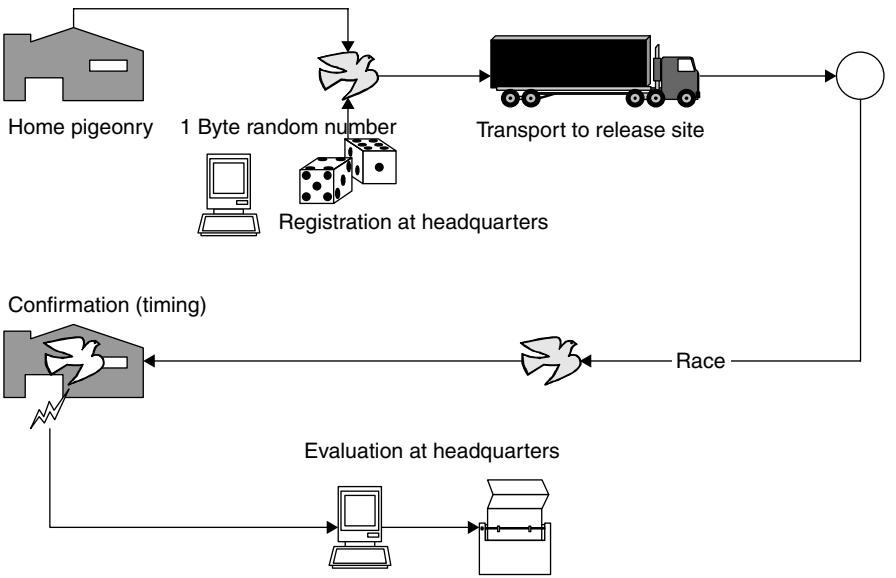


Figure 13.32 The generation of a random number which is written to the transponder before the start protects against attempted fraud

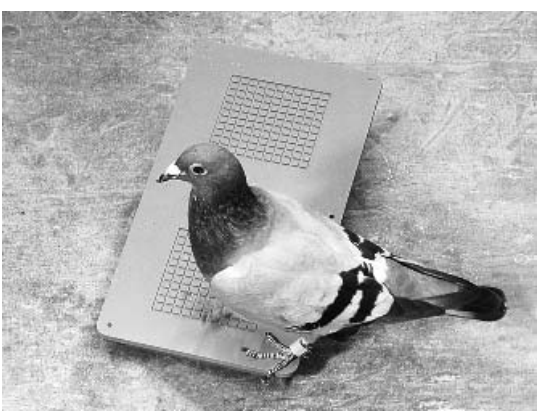


Figure 13.33 Typical antenna of an electronic confirmation system. The transponder on the pigeon's left leg is also clearly visible (reproduced by permission of Deister Electronik, Barsinghausen)

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

13.7 Electronic Immobilisation

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

13.7.1 The functionality of an immobilisation system

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

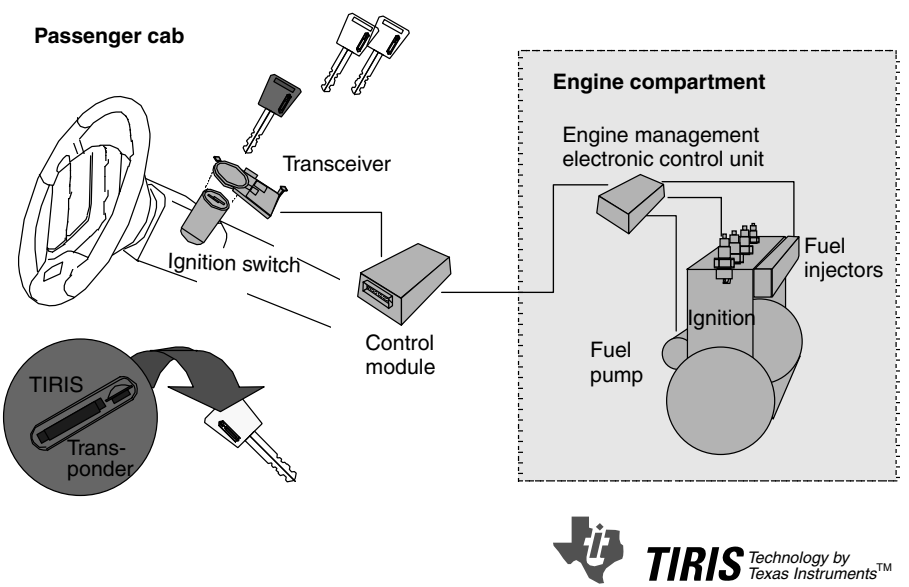


Figure 13.36 Functional group of an electronic immobilisation system. The RFID reader authenticates itself with regard to the motor electronics to prevent the manipulation of the reader. The motor electronics control the ignition, fuel and starter and thus can block all the crucial functions of the vehicle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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

13.7.2 Brief success story

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

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

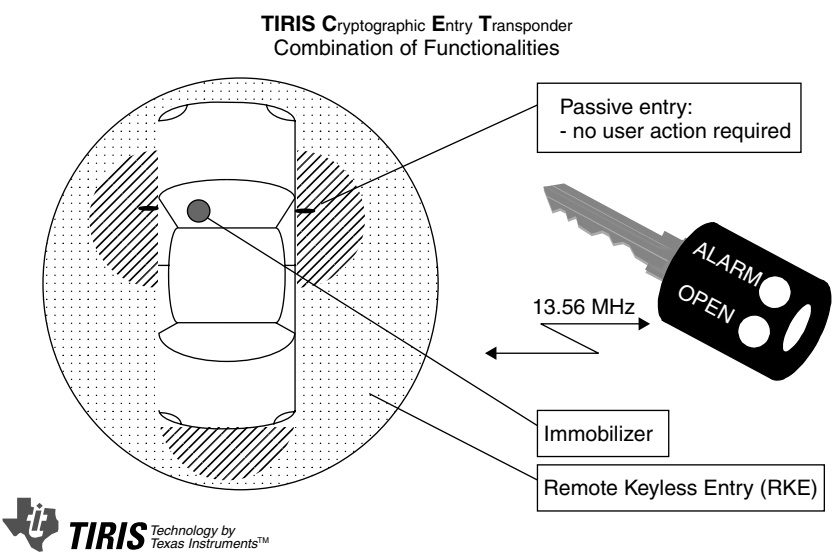


Figure 13.37 Electronic immobiliser and door locking system are integrated into a transponder in the ignition key. In the ignition lock and in the vicinity of the doors (passive entry) the transponder is supplied with power by inductive coupling. At greater distances (remote keyless entry) the transponder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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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

13.7.3 Predictions

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

13.8 Container Identification

13.8.1 Gas bottles and chemical containers

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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



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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

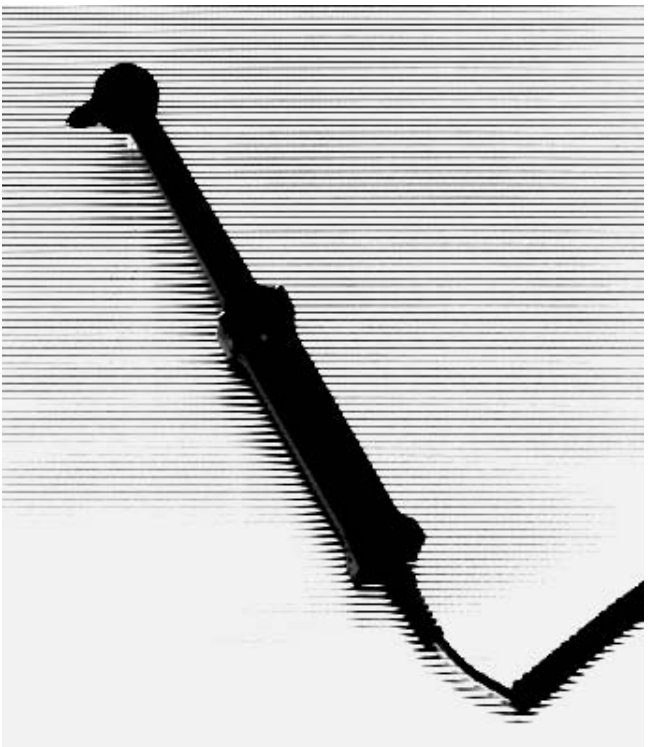


Figure 13.39 Portable antenna for reading inductively coupled transponders mounted on gas bottles or other containers (reproduced by permission of SCEMTEC Transponder Technology GmbH, Reichshof-Wehnrath)

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

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

13.8.2 Waste disposal

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

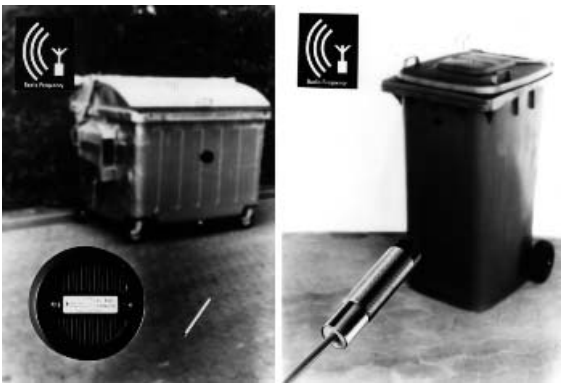


Figure 13.40 Left, dustbin transponder for fitting onto metal surfaces; right, reader antenna for installation in the dustcart. A plastic dustbin fitted with a transponder is shown in the background (reproduced by permission of Deister Electronic, Barsinghausen)

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

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

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

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

13.9 Sporting Events

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

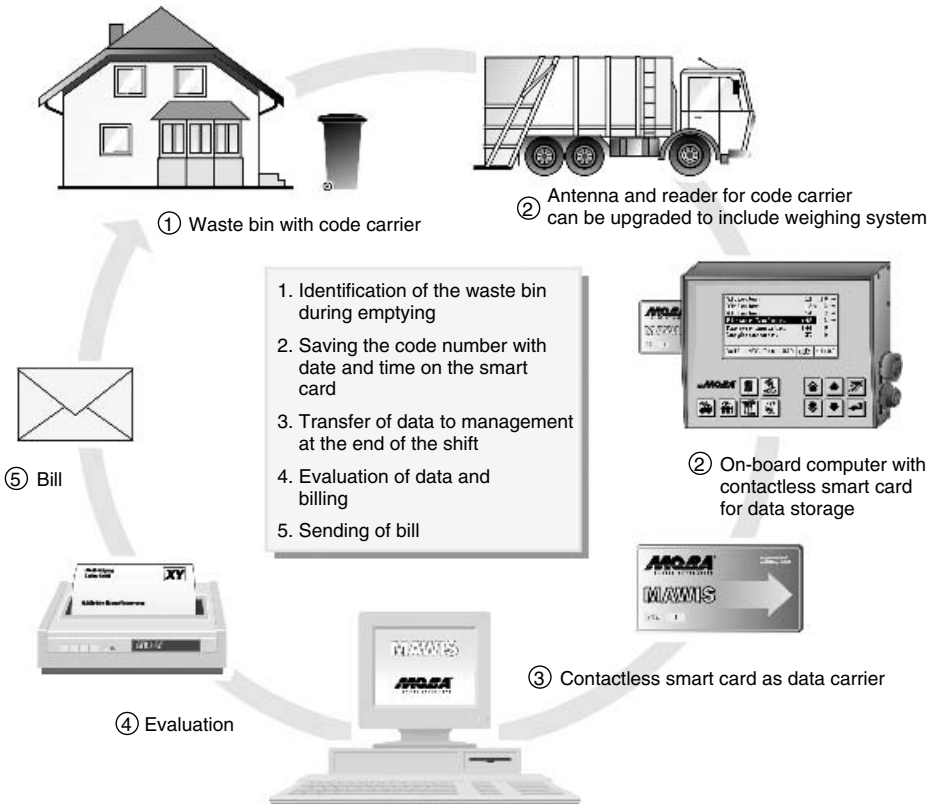


Figure 13.41 Waste generation cycle including billing (reproduced by permission of MOBA Mobile Automation GmbH, Elz)

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

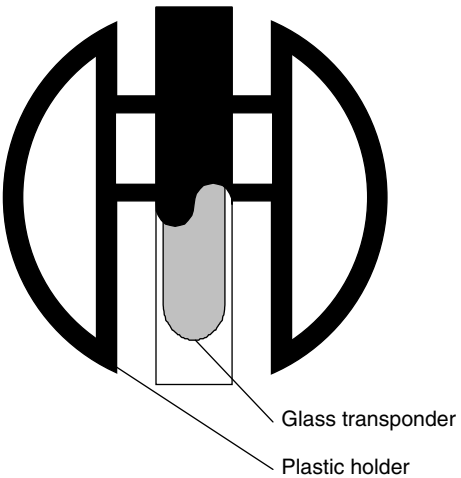


Figure 13.42 The transponder consists of a glass transponder, which is injected into a plastic housing that is shaped according to its function. The diagram shows the partially cut away plastic housing



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

13.10 Industrial Automation

13.10.1 Tool identification

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

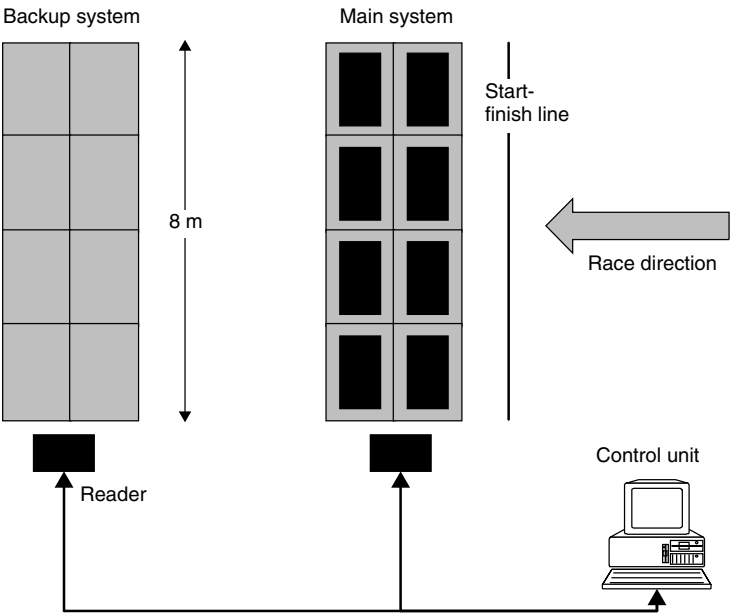


Figure 13.44 A control station consists of a main system and a reserve system. The systems are made up of arrays of antennas in mats



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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

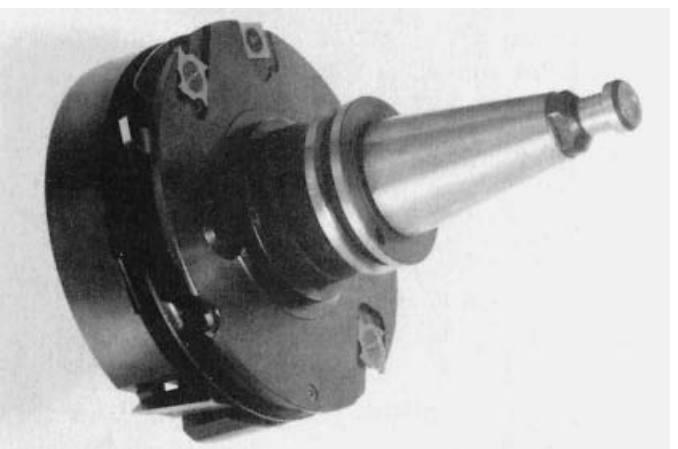


Figure 13.46 CNC milling tool with transponder in the retention bolts (reproduced by permission of Leitz GmbH & Co., Oberkochen)

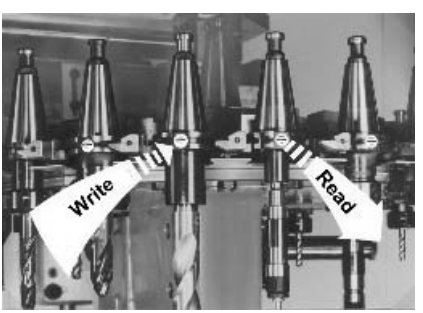


Figure 13.47 Various woodworking tools with transponder data carrier in the taper shaft (reproduced by permission of EUCHNER & Co., Leinfelden-Echterdingen)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

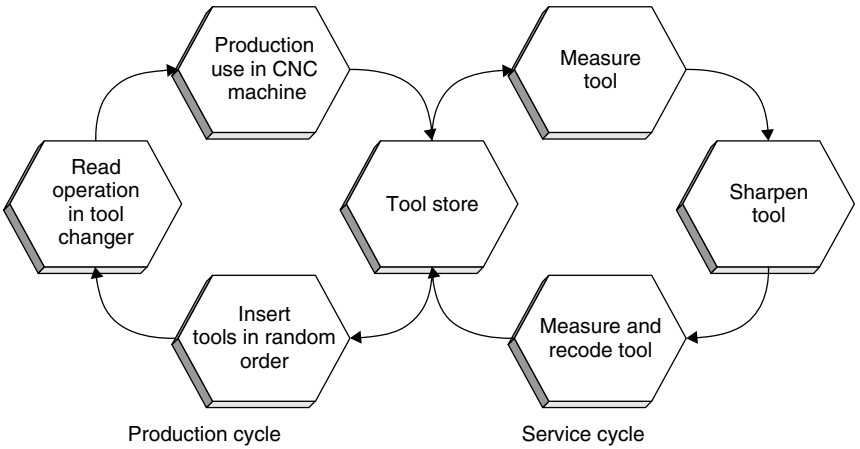


Figure 13.48 Representation of the tool cycle when using transponder coded CNC tools

Table 13.4 Example of a data record for a tool transponder

Customer	**Furniture Production Plant XY**
LEITZ ID no.	130004711 D25x60
Manufacturing ref.	Y21
Place of manufacture	UHE
Rotation direction	3
Max. rotation speed	24 000
Min. rotation speed	18 000
Ideal rotation speed	20 000
Radius correction	25 011
Longitudinal correction	145 893
Greatest radius	25 500
Greatest length	145 893
Maximum travel	3000
Current travel	875
Tool number	14
Tool type	1
Number of sharpenings	2
Angle of clearance	20
Cutting rake	15
Free text	Finishing cutter HM Z = 3

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

13.10.2 Industrial production

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

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

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

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

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

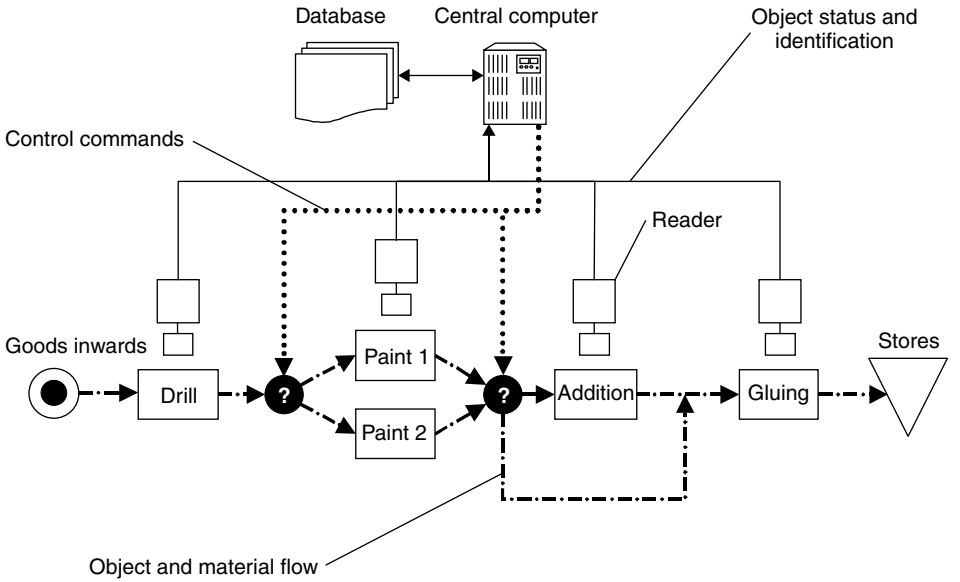


Figure 13.49 The object and data flow in a central control system is performed using completely separate routes. The central computer has a powerful database in which all process data is stored

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

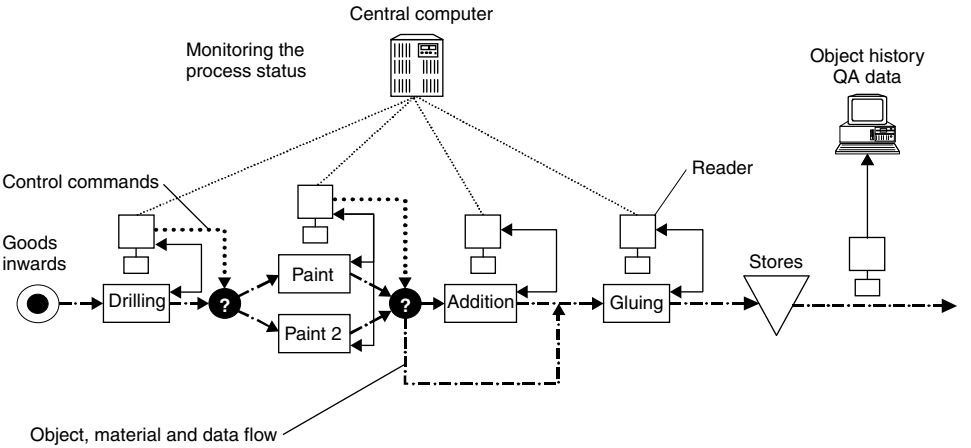


Figure 13.50 In a decentralised system the data is carried along with the objects

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

13.10.2.1 Benefits from the use of RFID systems

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

13.10.2.2 The selection of a suitable RFID system

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

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

Table 13.5 Comparison between the two memory technologies for transponders

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

13.10.2.3 Example projects

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

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



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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

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

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

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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



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

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

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

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

13.11 Medical Applications

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

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

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

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

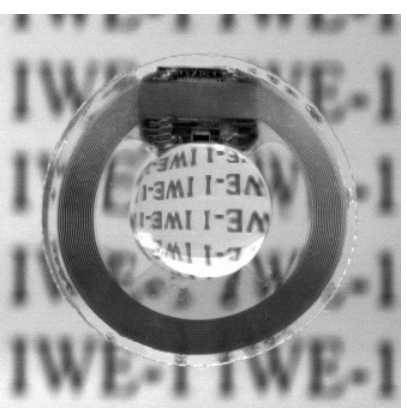


Figure 13.53 Transponder unit after casting into an artificial intraocular lens made of silicon. (reproduced by permission of IWE1, RWTH Aachen, D-52074 Aachen)

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

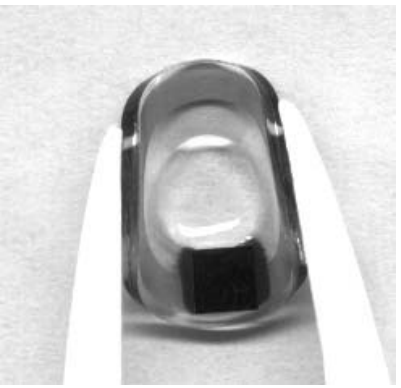


Figure 13.54 Cast transponder unit deformed by a pair of tweezers (reproduced by permission of IWE1, RWTH Aachen, D-52074 Aachen)

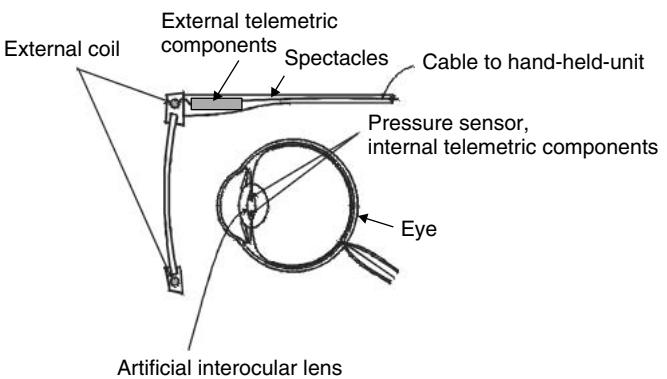


Figure 13.55 An implanted transponder with a pressure sensor, and an antenna coil integrated into the frame of a pair of glasses make up the system for the continuous measurement of interocular pressure (reproduced by permission of IWE1, RWTH Aachen, D-52074 Aachen)

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

14
Appendix

14.1 Contact Addresses, Associations and Technical Periodicals

The author himself can be contacted by post at the address of the publishing company:

Klaus Finkenzeller
c/o Carl Hanser GmbH & Co
Fachbuchlektorat
Kolbergerstr. 22
D-81679 Munich
Germany
and on the internet:
Homepage: http://RFID-handbook.de
http://RFID-handbook.com
Email: klaus.finkenzeller@web.de
or: dl5mcc@qsl.net

14.1.1 Industrial associations

AIM is the global trade association of providers and users of components, networks, systems, and services that manage the collection and integration of data with information management systems. AIM strives to stimulate the understanding, adoption, and use of technology and member company products and services through setting standards, marketing and education, market research, advocacy, and information technology industry relations.

Many manufacturers of RFID systems are members of the Industrieverband für Automatische Identifikation und Betriebsdatenerfassung (AIM). A list of members can be obtained from the following address:



AIM Argentina
Av. Alicia M. De Justo 740
4th Floor, Office #17



AIM Japan
ONO Roppongi Bldg.,
3-1-28, Roppongi, Minato-ku,

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Puerto Madero, C1107 AAR Bs. As.
Argentina
Tel: +54 11 4334 0033
Fax: +54 11 4342 9741
Email: rmtaylor@multiscan-corp.com
Web: http://www.aimarg.org.ar
Contact: Mr. Roberto Martinez Taylor



AIM Belgium
Diamant Building
No. 80 Boulevard A. Reyers
B-1030 Brussels
Belgium
Phone: +32 2 706 8000
Fax: +32 2 706 8009
Email: herman.looghe@agoria.be
Web: http://www.aimbel.be
Contact: Mr. Herman Looghe



AIM Brasil
Associacao Brasileira das
Empresas de Coleta de Dados
R. Bela Cintra, 746 - cj. 152 15 and.
CEP: 0145-902
Sao Paulo, Brasil
Tel: +55 11 3151 4572
Fax: +55 11 3258 0495
Email: aimbrasil@aim.org.br
Web: http://www.aim.org.br
Contact: Ms. Claudia Reis



AIM China
Unit 406, Suntrans Plaza,
No. 3 Beisanhuanzhong Road
Xicheng District,
Beijing China 100029
Tel: +86 10 62371516
Fax: +86 10 62371516
E-mail: scanchina@263.net
Web: http://www.aimchina.org.cn/



AIM Denmark
c/o Logisys A/S
Skagensgade 35
2630 Hoje Taastrup
Denmark
Tel: +45 43 52 67 11
Fax: +45 43 52 61 32
Email: info@aimdenmark.dk
Web: http://www.aimdenmark.dk
Contact: Mr. Arne Rask

Tokyo 106-0032
Japan
Tel: +81-3-5575-6231
Fax: +81-3-3586-3132
Email: benkoike@aimjapan.or.jp
Web: http://www.aimjapan.or.jp
Contact: Mr Ben Koike



AIM Mexico
Asturias No 31
Col. Alamos
03400 Mexico, D F
Mexico
Tel: +52 5 519 1553
Fax: +52 5 530 5482
Email: info@aim-mexico.com
Web: http://www.aim-mexico.com
Contact: Mr. Oscar Marquez



AIM Netherlands
Gevart van Doernestraat 34
5751 ML Deurne
The Netherlands
Tel: +31 493 351 867
Fax: +31 493 317 099
Email: aim@aim-ned.nl
Web: http://www.aim-ned.nl
Contact: Ing. Carl G Vermelis



AIM Russia
P.O. Box 4
Moscow 119415
Russia
Tel: +7 095 431 3007
Fax: +7 095 785 2748
Email: info@aim.ru
Web: http://www.aim.ru
Contact: Mr. Grigory Slusarenko



AIM Sweden
Neglinge Centre
S 133 33 Saltsjobaden
Sweden
Tel: +46 8 717 6148
Fax: +46 8 717 6098
Email: kansliet@aimsweden.se
Web: http://www.aimsweden.se
Contact: Ms. Kristina Leth

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189



AIM Finland
c/o Oy Maxicon AB
Riilahdentie 5 F 27
02360 Espoo
Finland
Tel: +358 9 802 4518
Fax: +358 9 802 4518
Email: info@aimfinland.fi
Web: http://www.aimfinland.fi
Contact: Mr. Toivo Solatie



AIM Germany
Akazienweg 26
D-68623 Lampertheim-Neuschloß
Germany
Tel: +49 6206 13177
Fax: +49 6206 13173
Email: aim-d-@t-online.de
Web: http://www.aim-d.de
Contact: Mr. Erwin Kretz



AIM Italia
c/o Consorzio Tecnoimprese
Via Console Flaminio 19
1-20134 Milan
Italy
Tel: +39 02 210 111 247
Fax: +39 02 210 111 222
Email: f.musiari@tecnoimprese.it
Web: www.aim.tecnoimprese.it/
Contact: Mr. Franco Musiari



AIM United Kingdom
The Old Vicarage
Haley Hill
Halifax HX3 6DR
West Yorkshire, England
United Kingdom
Tel: +44 1422 368368
Fax: +44 1422 355604
Email: ian@aimglobal.org
Web: http://www.aim-uk.org.uk
Contact: Mr. Ian G. Smith



Coming in 2003: **AIM USA**

Regional Support Centres

AIM currently has three regional support centres worldwide:

North, South, Central America Region	634 Alpha Drive Pittsburgh, Pennsylvania 15238 USA Phone: +1 412 963 8588 Fax: +1 412 963 8753 Email: info@aimglobal.org
Europe, Middle East, and Africa Regions	Avenue des Gaulois, 7 B-1040 Brussels, Belgium Phone: +32 2 7434420 Fax: +32 2 7431550 Email: emea@aimglobal.org Contact: Mr. Raimondo Bussi

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Asia Pacific Region

Room 1002, Taurus Building
21A Granville Road, Tsimshatsui
Kowloon, Hong Kong
Phone: +852 27783368
Fax: +852 27783383
Email: mailto:wing@aimglobal.org

Contactless smart cards can be used as electronic tickets, helping to improve speed and convenience and aiding the realisation of new public transport products and flexible strategies. The *KONTIKI* working group aims to analyse technological and application-related developments, to develop practical application options for public transport, and to use these as the basis for recommendations to transport companies and associations. The idea is that users, manufacturers, consultants, associations and organisations work together to create interdisciplinary solutions. The working group is now active across Europe.

Work is carried out in subgroups, and the results are presented centrally. The working group also acts as a point of contact and consulting body to potential users of future smart card projects. Contact address:

Arbeitskreis kontiki
c/o Weber Marketing
Wiesbadener Weg 6
65812 Bad Soden
Germany
Telephone: +49 6196 766 66 50
Fax: +49 6196 766 66 51
Homepage: http://www.kontiki.net
Email: weber@kontiki.net

A further group of companies, the Low Power Radio Association (LPRA), is concerned with low power radio systems. The LPRA was established in 1990 in the United Kingdom as the voice of the 'low power radio' industry. Now some 200 companies from around the world belong to LPRA. In addition to RFID, the association also deals with other radio services such as telemetry, cordless audio, Bluetooth, etc.

Low Power Radio Association
Brearley Hall
Luddenden Foot
Halifax
West Yorkshine HX2 6HS
UK
Homepage: http://www.LPRA.org

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

14.1.2 Technical journals

One German-language technical journal that deals with the subjects of barcodes, auto-ID and RFID is:

ident, Das Forum für Automatische Datenerfassung
Umschau Zeitschriftenverlag — Breidenstein GmbH
Stuttgarter Str. 18–24
D-60329 Frankfurt am Main
Germany
Homepage: http://www.ident.de

The following are English-language technical journals on the same subject:

Supply Chain Systems
(ID-Systems)
174 Concord St.
Peterborough, NH 03458
USA
Homepage: http://www.idsystems.com
RFID corner: http://www.idsystems.com/reader/RFID_Edge/index.htm

Frontline-Solutions
c/o Frontline Today
7500 Old Oak Blvd.
Cleveland, OH 44130
USA
Homepage: http://www.frontlinetoday.com

Automatic I. D. News
Tower House
Sovereign Park
Lathkill Street
Market Harborough
Leicestershire, LE 16 9EF
UK
Homepage: http://www.idnewseurope.com

Global ID-Magazine
Giroday & Partners
Piazza Duca D'Aosta, 10
20124 Milano
Italy
Homepage: http://www.global-id-magazine.com

Business Solutions
Corry Publishing
2840 West 21st Street

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Erie, PA 16506
USA
Homepage: http://www.businesssolutionsmag.com

RF-innovations
The Old Vicarage
Haley Hill
Halifax,
West Yorkshine HX3 6DR
UK

Smart Labels Analyst
The IDTechEx Web Journal
IDTechEx Limited
Downing Park Innovation Centre
Swaffham Bulbeck
Cambridge CB5 0NB
UK
Homepage: http://www.idtechex.com

14.1.3 RFID on the internet

A collection of links to RFID companies and further interesting pages on this subject is available at the following internet addresses:

http://rfid-handbook.de/links
http://members.surfbest.net/eaglesnest/rfidweb.htm
http://home.att.net/~randall.j.jackson/rfidlinks.htm

A good overview of the current state of standardisation, the work of AIM, and a comprehensive overview of companies is provided by the RFID homepage of AIM:

http://www.aimglobal.org/technologies/rfid

The monthly *RFID Newsletter* of AIM, which is sent out by email free of charge, is also recommended. Old editions are available on the following page:

http://www.aimglobal.org/technologies/rfid/newsletter/RFID_Newsletter_Issues.htm

Technical specifications and information on the current state of standardisation of auto-ID systems of all types (barcode, RFID, etc.) are available on the official *Auto-ID homepage*:

http://www.autoid.org

Current information about new developments and products in the field of RFID and EAS, a summary of the most important RFID patents, and an introduction to the

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

technical principles of the most important RFID procedures can be found in *Transponder News*:

http://rapidttp.co.za/transponder
http://rapidttp.com/transponder

A collection of press releases and articles on all RFID subjects can be found on the following homepage:

http://rfidjournal.com

The *RFID Bulletin Board* is available as a discussion forum on the internet. The purpose of the RFID Bulletin Board is to serve as a neutral forum for the free exchange of information between RFID users, developers and all those interested in the subject of RFID. Questions, contributions and discussions on technical and commercial topics relating to RFID, event notices, questions on applications, standardisation of RFID, etc. are permitted and welcomed:

http://rfid-handbook.de/forum

RFID is also being discussed in numerous usenet news groups. A quick overview can be obtained by using the usenet search function at google.com (enter 'rfid OR contactless' as the search expression):

http://groups.google.com

14.2 Relevant Standards and Regulations

26. BImSchV: 'Sechsundzwanzigste Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes — Verordnung über elektromagnetische Felder', with explanatory section, in Wolfgang Kemmer, '*Die neue Elektrosmog-Verordnung*', H. Hoffmann GmbH Verlag, Berlin, 1997, ISBN 3-87344-103-9.

CEPT T/R 60-01: *Low-power radiolocation equipment for detecting movement and for alert* (EAS). Technical Recommendation. http://www.ero.dk

CEPT T/R 22-04: *Harmonisation of frequency bands for Road Transport Information Systems (RTI) (toll systems, freight identification)*. Technical Recommendation. http://www.ero.dk

EN 50061: *Safety of implantable cardiac pacemakers*. Regulations for protecting against malfunctions due to electromagnetic interference (corresponds with VDE 0750). http://www.etsi.org

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

EN 300 220: *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1000 MHz frequency range with power levels ranging up to 500 mW*. http://www.etsi.org

Part 1: Technical characteristics and test methods
Part 2: Supplementary parameters not intended for conformity purposes.
Part 3: Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive.

EN 300 330: *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment in the frequency range 9 kHz to 25 MHz and inductive loop systems in the frequency range 9 kHz to 30 MHz*. http://www.etsi.org

Part 1: Technical characteristics and test methods.
Part 2: Harmonized EN under article 3.2 of the R&TTE Directive.

EN 300 440: *Radio Equipment and Systems (RES); Short range devices, Technical characteristics and test methods for radio equipment to be used in the 1 GHz to 25 GHz frequency range with power levels ranging up to 500 mW*. http://www.etsi.org

ETS 300 683: *Radio Equipment and Systems (RES); ElectroMagnetic Compatibility (EMC) standard for Short Range Devices (SRD) operating on frequencies between 9 kHz and 25 GHz*. http://www.etsi.org

EN 300 761: *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Automatic Vehicle Identification (AVI) for railways operating in the 2.45 GHz frequency range*. http:// www.etsi.org

Part 1: Technical characteristics and methods of measurement.
Part 2: Harmonized standard covering essential requirements under article 3.2 of the R&TTE Directive

EN 300 674: *Electromagnetic compatibility and radio spectrum matters (ERM); Road Transport and Traffic Telematics (RTTT); Technical characteristics and test methods for Dedicated Short Range Communications (DSRC) transmission equipment (500 kbit/s / 250 kbit/s) operating in the 5.8 GHz Industrial, Scientific and Medical (ISM) band*. http:// www.etsi.org

EN 301 489: *Electromagnetic compatibility and radio spectrum matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services*. http://www.etsi.org

Part 1: Common technical requirements
Part 2: Specific requirements for radio paging equipment

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Part 3: Specific requirements for Short-Range Devices (SRD) operating on frequencies between 9 kHz and 25 GHz
Part 4: Specific requirements for fixed radio links and ancillary equipment and services
Part 5: Specific requirements for Private land Mobile Radio (PMR) and ancillary equipment (speech and non-speech)
Part 6: Specific conditions for Digital Enhanced Cordless Telecommunications (DECT) equipment
Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)
Part 8: Specific requirements for GSM base stations
Part 9: Specific conditions for wireless microphones and similar Radio Frequency (RF) audio link equipment
Part 10: Specific conditions for First (CT1 and CT1+) and Second Generation Cordless Telephone (CT2) equipment
Part 11: Specific conditions for FM broadcasting transmitters
Part 12: Specific conditions for Earth Stations operated in the frequency ranges between 4 GHz and 30 GHz in the Fixed Satellite Service (FSS)
Part 13: Specific conditions for Citizens' Band (CB) radio and ancillary equipment (speech and non-speech)
Part 15: Specific conditions for commercially available amateur radio equipment
Part 16: Specific conditions for analogue cellular radio communications equipment, mobile and portable
Part 17: Specific requirements for Wideband data and HIPERLAN
Part 18: Specific requirements for Terrestrial Trunked Radio (TETRA)
Part 19: Specific conditions for Receive Only Mobile Earth Stations (ROMES) operating in the 1.5 GHz band providing data communications
Part 20: Specific conditions for Mobile Earth Stations (MES) used in the Mobile Satellite Services (MSS)
Part 22: Specific requirements for VHF aeronautical mobile and fixed radios

ERC/DEC 92-02: *CEPT/ERC Decision on the frequency bands to be designated for the coordinated introduction of Road Transport Telematic Systems*. http://www.ero.dk

ERC/DEC 97-10: *CEPT/ERC Decision on the mutual recognition of conformity assessment procedures including marking of radio equipment and radio terminal equipment*. http://www.ero.dk

ERC/DEC 01-01: *CEPT/ERC Decision: Non-specific short range devices in 6765–6795 kHz and 13.552–13.567 MHz*. http://www.ero.dk

ERC/DEC 01–02: *CEPT/ERC Decision: Non-specific short range devices in 26.957–27.283 MHz*. http://www.ero.dk

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

ERC/DEC 01–03: *CEPT/ERC Decision: Non-specific short range devices in 40.660–40.700 MHz.* http://www.ero.dk

ERC/DEC 01–04: *CEPT/ERC Decision: Non-specific short range devices in 868.0–868.6 MHz, 868.7–869.2 MHz, 869.4–869.65 MHz, 869.7–870.0 MHz.* http://www.ero.dk

ERC/DEC 01–05: *CEPT/ERC Decision: Non-specific short range devices in 2400–2483.5 MHz.* http://www.ero.dk

ERC/DEC 01–13: *CEPT/ERC Decision: Short range devices for inductive applications in 9–59,750 kHz, 59.750–60.250 kHz, 60.250–70 kHz, 70–119 kHz and 119–135 kHz.* http://www.ero.dk

ERC/DEC 01–14: *CEPT/ERC Decision: Short range devices for inductive applications in 6765–6795 kHz, 13.553–13.567 MHz.* http://www.ero.dk

ERC/DEC 01–15: *CEPT/ERC Decision: Short range devices for inductive applications in 7400–8800 kHz.* http://www.ero.dk

ERC/DEC 01–16: *CEPT/ERC Decision: Short range devices for inductive applications in 26.957–27.283 MHz.* http://www.ero.dk

ERC/REC 01–06: *CEPT/ERC Recommendation: Procedure for mutual recognition of type testing and type-approval for radio equipment.* http://www.ero.dk

ERC/REC 70-03: *CEPT/ERC Recommendation 70-03 relating to the use of Short Range Devices (SRD).* http://www.ero.dk

ISO 7810: *Identification cards — Physical characteristics.*

ISO 7816: *Identification cards — Integrated circuit(s) cards with contacts*:

- Part 1: Physical characteristics
- Part 2: Dimensions and location of the contacts
- Part 3: Electronic signals and transmission protocols
- Part 4: Interindustry commands for interchange
- Part 5: Registration system for applications in IC Cards
- Part 6: Interindustry Data elements
- Part 7: Interindustry commands for Structured Card Query Language (SCQL)
- Part 8: Security architecture and related interindustry commands
- Part 9: Enhanced interindustry commands
- Part 10: Electronic signals and answer to reset for synchronous cards
- Part 11: Card structure and enhanced functions for multi-application use

ISO 9798: *Information technology — Security techniques — Entity authentication.* Principles and description of authentication procedures.

ISO 10373: *Identification Cards — Test methods.* Test methods for 'plastic cards' for testing the card body and the fitted card element

HANSHOW Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

(magnetic strip, semiconductor chip). The standard consists of the following parts:

Part 1: General
Part 2: Magnetic strip technologies
Part 3: Integrated circuit cards (contact smart cards)
Part 4: Contactless integrated circuit cards (close-coupling)
Part 5: Optical memory cards
Part 6: Proximity cards (contactless smart cards in accordance with DIN/ISO 14443)
Part 7: Vicinity cards (contactless smart cards in accordance with DIN/ISO 15693)

ISO 10374: *Container — Automatische Identifizierung* (*Freight containers — Automatic identification*). Automatic identification of freight containers by a 2.45 GHz transponder system.

ISO 10536: *Identification cards — Contactless integrated circuit(s) cards*. Contactless smart cards in close coupling technology. The standard consists of the following parts:

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

ISO 11784: *Radio-frequency identification of animals — code structure*. Identification of animals by RFID systems. Description of the data structure.

ISO 11785: *Radio-frequency identification of animals — technical concept*. Identification of animals by RFID systems. Description of the RF transmission procedure.

ISO 14223: *Radio-frequency identification of animals — Advanced Transponders*:

Part 1: Air interface
Part 2: Code and command structure

ISO 14443: *Identification cards — Proximity integrated circuit(s) cards*:

Part 1: Physical characteristics
Part 2: Radio frequency interface
Part 3: Initialization and anticollision
Part 4: Transmission protocols

ISO 15693: *Identification cards — contactless integrated circuit(s) cards — Vicinity Cards*:

Part 1: Physical characteristics
Part 2: Air interface and initialisation
Part 3: Protocols
Part 4: Registration of Applications/issuers

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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 (868/915 MHz)
ISO 69873:	*Tools and clamping devices with data carriers — Dimensions for data carriers and their fitting space*
S-918-00:	AAR Manual of Standards and Recommended Practices Railway Electronics, S-918: *Standard for Automatic Equipment Identification*. Adopted: 1991; Revised: 1995, 2000
VDE 0848:	*Safety in electromagnetic fields (Part 2 — Protection of people in the frequency range 30 kHz to 300 GHz, Part 4A2 — Protection of people in the frequency range 0 Hz — 30 kHz.*
VDE 0750:	See EN 50061.
VDI 4470 — Teil 1:	*Warensicherungssysteme — Kundenabnahmerichtlinie für Schleusensysteme* Ermittlung der Erkennungsrate und Detektionsrate bei der Inbetriebnahme von EAS-Systemen vor Ort.
VDI 4470 — Teil 2:	*Warensicherungssysteme — Kundenabnahmerichtlinie für Deaktivierungsanlagen*. Prüfung von Deaktivierungsanlagen für EAS-Systeme.

14.2.1 Sources for standards and regulations

DIN, ISO, VDE, VDI and other standards can be purchased in Germany from:

Beuth Verlag GmbH,
Burggrafenstr. 3

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

D-10772 Berlin
Germany

Telecommunications standards (EN, I-ETS) can be downloaded free of charge from:
European Telecommunications Standards Institute (ETSI)
650 Route des Lucioles
F-06921 Sophia Antipolis
CEDEX-France
Homepage: http://www.etsi.org

German national legislation and the *Amtsblatt* (Official Journal) can be obtained from:
Regulierungsbehörde für Telekommunikation und Post (RegTP)
Canisiusstrasse 21
D-55122 Mainz
Germany
Homepage: http://www.regtp.de

An overview of regulation in the 44 member states of CEPT, plus all documents of the European Radiocommunication Committee (ERC), can be downloaded free of charge from:
European Radiocommunications Office (ERO)
Peblingehus
Nansensgade 19
DK-1366 Copenhagen
Homepage: http://www.ero.dk

General notes on *CE marking* in the EC internal market, plus notes on the *R&TTE Directive* (1999/5/EC) for radio and telecommunications terminal equipment can be found at the following websites:
http://europa.eu.int/comm/enterprise/newapproach/legislation/guide/legislation.htm
http://europa.eu.int/comm/enterprise/rtte

14.3 References

Abramson, Norman (n.d.) *Multiple access in wireless digital networks*, ALOHA Networks Inc., San Francisco, CA, http://www.alohanet.com/ sama/samatppr.html

Agilent Technologies (n.d.) Technical Data Sheet, *Surface Mount Microwave Schottky Detector Diodes — HSMS-286x Series*

Ampélas, André (1998) *Towards a city pass, ICARE-CALYPSO, two European projects for ticketing, electronic money and city services*

Anderson, Russel (1998) The use of polymer thick film for printing of contactless smartcard coils, DuPont Photopolymer and Electronic Materials, in: *Smart Card Technologies and Applications — Second Workshop on Smart Card Technologies and Applications*, IEEE Tagungsband, Berlin, 16 November

Anselm, Dieter (n.d.) *Diebstahl von Kraftfahrzeugen mit Wegfahrsperren*, Allianz-Zentrum für Technik, Munich

Anselm, Dieter (1996) *Voller Erfolg der elektronischen Wegfahrsperre*, Allianz-Zentrum für Technik, Munich, 21 March

Atmel Corporation (1994) RFID-ASIC Fact Sheet, March

Atmel Corporation (1998) *Asset Identification EEPROM, AT24RF08*, San Jose, CA, http://www.atmel.com

Bachthaler, Reiner (1997) Auswahlkriterien für elektronische Datenspeicher, *ident*, 3

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Baddeley, David and Ruiz, Christian (1985) *Test PICC — Type B Proximity Cards, Technical Contribution — ISO/IEC JTC1/SC17/WG8/TF2 N242*, Motorola, Genf 01/1998

Baur, Erwin (1985) *Einführung in die Radartechnik*, Teubner Studienskripten, Stuttgart, ISBN 3-519-00106-3

Berger, Dominik (1998) Contactless smart card standards and new test methods, in: *Smart Card Technologies and Applications — Second Workshop on Smart Card Technologies and Applications*, IEEE Tagungsband, Berlin, 16 November

Bögel, Gerd vom and Niederholz, Michael (2001) Transpondersystem zur Messung des Augeninnedrucks, *Electronic Embedded Systeme*, **5**, http://www.systeme-online.de

Bögel, Gerd vom, Scherer, Klaus and Bollerott, Michael (1998) Transponder für Ident- und Telemetrie-Anwendungen, in: *Automatische Identifikation: Kommunikation in der Logistikkette, basierend auf Tagungsbeitragen der SMAID '98* (Spring Meeting on Auto-ID), Umschau Zeitschriftenverlag, Frankfurt am Main, ISBN 3-930007-95-9

Borgonovo, Flaminio and Zorzi, Michele (1997) Slotted ALOHA and CDPA: A comparison of channel access performance in cellular systems, *Wireless Networks*, **3**

Bosse, Georg (1969) *Grundlagen der Elektrotechnik — Das elektrostatische Feld und der Gleichstrom*, B.I.-Hochschultaschenbücher Band 182, Mannheim

Braunkohle, Elektronische Kennzeichnung von Gefahrstoffen (1997) **2** (March/April)

Bruhnke, Michael (1996) *Kontaktlose Chipkartentechnologie in der Automobilindustrie (Immobilizer)*, Lecture script for ChipCard 96, Eching

Bulst, W.-E., Fischerauer, G. and Reindl, L. (1998) State of the art in wireless sensing with surface acoustic waves, in: *Proceedings of the 24th Annual Conference of the IEEE Industrial Electronics Society IECON*, pp. 2391–6, ISBN 0-8194-2459-5

Bührlen, Martin (1995) Mikron-Chip macht Gasflaschen intelligent, *Card-Forum*, **11**

Caspers, Friedrich (1997) *Aktuelle Themen der Kfz-Versicherung*, Allianz Versicherungs-AG, Munich, 25 March

ChampionChip (n.d.) *Real-Time ChampionChip — Das Zeitmeß- und Identifikationssystem für den aktiven Sport*, Sport Team, Drebber

Couch II, Leon W. (1997) *Digital and Analog Communication Systems*, Prentice-Hall, London, ISBN 0-13-599028-9

Czako, Josef (1997) *Neue Innovationsplattform für Verkehrsunternehmen*, Tagungsband — OMNICARD 1997, in *Time*, Berlin

Doerfler, M. (1994) Mikroelektronische Authentifizierungssysteme für die Serienausstattung von Kfz, in: *Identifikationssysteme und kontaktlose Chipkarten*, GME-Fachbericht 13, VDE-Verlag, Berlin 1994

Droschl, Georg (1997) *Der Markt für kontaktlose Chipkarten: Von der Vision zur Realität*, Tagungsband — OMNICARD 1997, in *Time*, Berlin

Dziggel, Klaus Peter (1997) *The SOFIS Auto-ID Identification System*, lecture script for SMAID '97, Dortmund

EC (1995) *The Radio Equipment and Telecommunications Terminal Equipment Directive (1999/5/EC)*, http://europa.eu.int/comm/enterprise/rtte

EAN.UCC (1999) *EAN.UCC White Paper on Radio Frequency Identification*, EAN International & UCC Inc., November, http://www.ean-int.org

EAN.UCC (2000) *RFID and the EAN.UCC System, GTAG Project Team*, EAN International & UCC Inc., http://www.ean-int.org

ERC (2000) *CEPT marking and the R&TTE Directive*, ERC Report 84, European Radiocommunications Committee (ERC), Lisbon, June, http:// www.ero.dk

ERC (2002) *ERC recommendation 70-03 (Tromso 1997 and subsequent amendments) relating to the use of short range devices (SRD)*, Recommendation Adopted by the Frequency Management, Radio Regulatory and Spectrum Engineering Working Groups, European Radiocommunications Committee (ERC), February, http://www.ero.dk

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Ernst, Horst (1996) EURO-Balise S21 — Meilenstein für das ETCS, *ETR — Eisenbahntechnische Rundschau*, **45**, October

Escort Memory Systems (1998a) *RFID Application — Case Study, Automotive Engine Manufacturer, General Motors*, Escort Memory Systems, Scotts Valley, California

Escort Memory Systems (1998b) *RFID Application — Case Study, Agricultural Equipment Manufacturer, John Deere Company*, Escort Memory Systems, Scotts Valley, California

Escort Memory Systems (1998c) *RFID Application — Case Study, Meat Processor, J. M. Schneider Meats*, Escort Memory Systems, Scotts Valley, California

EURO ID (n.d.) Datasheet: *Anwendungsbeispiele für das trovan® RF-Identifikationssystem — Dienstleistungen — Abfall — Logistik*, EURO I.D. Identifikationssysteme GmbH & Co. KG, Weilerswist

Fleckner, Harald (1987) Dioden und ihre Anwendung in Frequenzvervielfachern für den Mikrowellenbereich, *UKW-Berichte*, **1**, Verlag UKW-Berichte, Baiersdorf

Fliege, Norbert (1996) *Digitale Mobilfunksysteme*, B. G. Teubner, Stuttgart, ISBN 3-519-06181-3

Fricke, Hans, Lamberts, Kurt and Patzelt, Ernst (1979) *Grundlagen der elektrischen Nachrichtenübertragung*, B. G. Teubner, Stuttgart, ISBN 3-519-06416-2

Friedrich, Ulrich and Annala, Anu-Leena, *Palomar — a European answer for passive UHF RFID applications*, RFID Innovations 2001 conference, http://vicarage-publications.co.uk

Fries, Matthias and Kossel, Marcel (n.d.) *Aperture Coupled Patch Antennas for an RFID-System using Circular Polarization Modulation*, ETH Zürich, http://www.ifh.ee.ethz.ch/~kossel/publikationen.html

Fumy, Walter (1994) *Kryptographie*, R. Oldenburg Verlag, Munich

Geers, R., Puers, B., Goedseels, V. and Wouters, P. (1997) *Electronic Identification, Monitoring and Tracking of Animals*, CAB International, Wallingford, ISBN 0-85199-123-8

Giesecke & Devrient (1997) Datasheet, *Referenzprojekte — kontaktlose Chipkarte RM8k-MIFARE®*, Munich

Gillert, Frank (1997) Quellensicherung auf Basis von EAS-Technologien, *ident*, **3**

Glogau, Ralf (1994) Geheimsache, *DOS*, **12**, DMV Verlag

Golomb, W. Solomon (1982) *Shift Register Sequences*, Aegean Park Press, Laguna Hills, CA, ISBN 0-89412-048-4

GTAG (2001) *Minimum protocol and performance requirement — part 1: resolution process*, GTAGprN0150drMPPR, Version 1.3, EAN-International & UCC Inc., http://www.ean-int.org

Haberland, Marc (1996) Gedächtnis ohne Ladungsträger, Ferroelektrische RAMs — die Speicher der Zukunft, *Elektronik*, **25**

Haghiri, Y. and Tarantino, T. (1999) *Vom Plastik zur Chipkarte*, Carl Hanser Verlag, Munich

Hamann, Ulrich (1997) *Optimierte Halbleiter-Chips für kontaktlose Chipkarten-Applikationen*, Tagungsband — OMNICARD 1997, *Time*, Berlin

Hanex (n.d.) Sales presentation, *Hanex RFID-System for Metal*, HXID-System, Hanex Co. Ltd., Japan

Hawkes, Peter (1997) *Singing in Concert — Some of the possible methods of orchestrating the operation of multiple RFID-Tags enabling fast, efficient reading without singulation*, Amsterdam, 19 February

Herter, E. and Lörcher, W. (1996) *Nachrichtentechnik — Übertragung, Vermittlung und Verarbeitung*, 4th edn, Carl Hanser Verlag, Munich, ISBN 3-446-14593-1

Hewlett-Packard, Application Note 956-4, *Schottky Diode Voltage Doubler*

Hewlett-Packard, Application Note 986, *Square Law and Linear Detection*

Hewlett-Packard, Application Note 988, *All Schottky Diodes are Zero Bias Detectors*

Hewlett-Packard, Application Note 1088, *Designing the Virtual Battery*

Hewlett-Packard, Application Note 1089, *Designing Detectors for RFID Tags*

Homburg, Dietrich (1996) Barcodeleser in der Automobilindustrie, *ident*, **1**, Umschau Zeitschriftenverlag, Frankfurt am Main

ident, (1996) **1**, Umschau Zeitschriftenverlag, Frankfurt am Main

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

IDESCO (n.d.) Technical Information, *IDESCO MICROLOG® 1k Memory*, Idesco, Oulu, Finland

Integrated Silicon Design Pty Ltd (ISD) (1996) *Training Manual*, Adelaide, Australia

Intermetall Semiconductors ITT (1975) *Kapazitätsdioden, Schalterdioden, PIN-Dioden — Grundlagen und Anwendungen*, Freiburg

Jörn, Fritz (1994) WIE — Elektronische Diebstahlsicherung, FAZ

Jurianto, Joe and Chia, Michael Y.W. (n.d.a) *Voltage, Efficiency Calculation and Measurement of Low Power Rectenna Rectifying Circuit*, Singapore Science Park, Centre for Wireless Communications, http://leonis.nus.edu.sg

Jurianto, Joe and Chia, Michael Y.W. (n.d.b) *Zero Bias Schottky Diode Model For Low Power, Moderate Current Rectenna*, Singapore Science Park, Centre for Wireless Communications, http://leonis.nus.edu.sg

Jurisch, Reinhard (1994) *Coil on Chip — monolithisch integrierte Spulen für Identifikationssysteme*, GME technical report *Identifikationssysteme und kontaktlose Chipkarten*, vde-Verlag, Berlin

Jurisch, Reinhard (1995) mic3: Die neue kontaktlose Chipkartentechnologie, *Card Forum*, **3**

Jurisch, Reinhard (1998) Transponder mit integrierter Sensorik, *Elektronik*, **18**

Kern, Christian (1994) *Injektate zur elektronischen Tieridentifizierung*, working paper 205, published by the Kuratorium für Technik und Bauwesen in der Landwirtschaft e. V. (KTBL), Darmstadt, March (KTBL-Schriften-Vertrieb im Landwirtschaftsverlag GmbH, Münster-Hiltrup)

Kern, Christian J. (1997) *Technische Leistungsfähigkeit und Nutzung von injizierbaren Transpondern in der Rinderhaltung*, Forschungsbericht Agrartechnik — No. 316, Dissertation, Landtechnik Weihenstephan, 1997, ISSN 0931–6264 (source: Institut für Landtechnik Weihenstephan, Vöttinger Strasse 36, D-85354 Freising)

Kern, Ch. and Wendl G. (1997) Tierkennzeichnung — Einsatz elektronischer Kennzeichnungssysteme in der intensiven und extensiven Rinderhaltung am Beispiel von Deutschland und Australien, *Landtechnik*, **3**

Klindtworth, Michael (1998) *Untersuchung zur automatisierten Identifizierung von Rindern bei der Qualitätsfleischerzeugung mit Hilfe injizierbarer Transponder*, Forschungsbericht Agrartechnik — No. 319, Dissertation, Technische Universität München, ISSN 0931–6264 (source: Technische Universität München, Institut und Bayerische Landesanstalt für Landtechnik, Vöttinger Strasse 36, D-85254 Freising)

Koch, Dieter and Gahr, Peter (1998) Elektronische Schliesssysteme, *Baumeister — Zeitschrift für Architektur*, **3**, Callwey Verlag, Munich

Kossel, Marcel and Benedicter, Hansruedi (n.d.) *Circular Polarized Aperture Coupled Patch Antennas for an RFID System in the 2.4 GHz ISM Band*, ETH Zürich, http://www.ifh.ee.ethz.ch/~kossel/publikationen.html

Kraus, John D. (1988) *Antennas*, 2nd edn, McGraw-Hill, New York, ISBN 0-07-100482-3

Kraus, Gunthard (DG8GB) (2000) Moderner Entwurf von Patch-Antennen, Part 1: *UKW-Berichte*, **3**; Part 2: *UKW-Berichte* **4**, http://www.ukw-berichte.de

Krebs, D. (n.d.) Unpublished manuscripts, Venture Development Corp., http://www.vdc-corp.com

Krug, Friedrich (DJ3RV) (1985) Mikrostreifenleitungs-Antennen, *UKW-Berichte*, **2**, http://www.ukw-berichte.de

Kuchling, Horst (1985) *Taschenbuch der Physik*, Verlag Hari Deutsch, Thun und Frankfurt/Main, ISBN 3-87144-097-3

Lee, Youbok (1999) *Antenna circuit design*, AN710, application note, microID 13.56 MHz — RFID system design guide, Microchip, http://www.microchip.com

Lehmann, Ulrich (1996) Aktivitäten von Siemens zur Einführung der EURO-Balise S21, *SIGNAL + DRAHLT* **88**(12)

Leitz (n.d.) *Intelligente Werkzeuge für mehr Sicherheit und Komfort*, Fa. Leitz, Oberkochen

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Lemme, Helmut (1993) *Der Mikrorechner in der Brieftasche*, *Elektronik*, 20, 22, 26, Franzis-Verlag, Munich

Link, Walter (1996, 1997) Identifikation mit induktiven Systemen, *ident*, 2, 1

Longo, G. (1993) *Secure digital communications*, Springer-Verlag, New York

Lorenz, Helge (1998a) *Kontaktlose Anwendung elektronischer Geldbörsen im Verkehrswesen*, in: *Die Chipkarte auf dem Weg zu Akzeptanz und Nutzung*, conference documentation, OMNICARD 1998, Berlin

Lorenz, Helge (1998b) *Der INTER-MOBIL-PASS: Multifunktionale Nutzung der Geldkarte für kontaktlose Anwendungen im Verkehrs- und Dienstleistungsbereich*, conference documentation, Verkehrswissenschaftliche Tage

Lorenz, Helge (1998c) FlexPass: Kontaktloses Medium für Bus und Bahn, *B. BI.*, **4**

Mäusl, Rudolf (1985) *Digitale Modulationsverfahren*, Hüthig Verlag, Heidelberg, ISBN 3-7785-0913-6

Mansukhani, Arun (1996) Wireless Digital Modulation, *Applied Microwave & Wireless*, November/December

Mathcad (n.d.) File: *har-lep.mcd*: Vo vs. Pin calculator, based upon Harrison & Polozec (1994) Nonsquarelaw behavior of diode detectors analyzed by the Ritz–Galerkin Method, *IEEE Trans MTT*, **42**(5), May, http://rfglobalnet.com

Meinke, H. and Gundlach, F. W. (1992) *Taschenbuch der Hochfrequenztechnik*, 5th edn, Springer-Verlag, Berlin/Heidelberg, ISBN 3-540-54717-7

Miehling, Martin, Die Transpondertechnik in der Praxis — Hightech für die Sicherheit, *W&S*, **10**, Hüthig GmbH, Heidelberg

Motorola Inc. (1999) *BiStatix™ Technology, A Whitepaper, Version 4.1*, March

Mühlberger, Andreas (2001) *High speed public encryption on contactless smart cards*, Philips Semiconductors Gratkorn GmbH, A-Gratkorn, http://www.semiconductors.philips.com/identification

Nührmann, Dieter (1994) *Professionelle Schaltungstechnik*, Franzis Verlag, Munich, ISBN 3-7723-6715-1

Osborne, Andrew (n.d.) *The EAN.UCC GTAG (TM) Project*, EAN-International & UCC Inc., http://www.ean-int.org/gtag.htm

Palomar (18000) ISO (WD)18000-6 Mode 3, Annex 4 — *Delta RCS definition*, PALOMAR submission

Panasonic (n.d.) Technical Data Sheet — *Features of ferroelectric nonvolatile memory*

Paul, Reinhold (1993) *Elektrotechnik 1–Felder und einfache Stromkreise*, 3rd edn, Springer-Verlag, Berlin/Heidelberg, ISBN 3-540-55753-9

Pein, Rüdiger (1996) Hilfe bei Prüfungsfragen — Prüfsummenverfahren, *DOS*, **2**

Pepperl & Fuchs (1998) Mikrowellen-Identsystem rationalisiert Montage, *Konstruktion & Engineering*, 1, January

Pepperl & Fuchs (n.d.a) *Mikrowellen-Identifikationssysteme in der Fertigung bei BMW*, Pepperl & Fuchs, Mannheim

Pepperl & Fuchs (n.d.b) *Fabrikautomation, Produktübersicht Identifikationssysteme*, Pepperl & Fuchs, Mannheim

Philipp, Stefan (2001) *CISC vs. RISC and a plea for peace. Enhanced Microcontroller Architecture for Smart Card ICs*, Philips Semiconductors, D-Hamburg, http://www.semiconductors.philips.com/identification

Philips Components (1994) Datasheet, *Ferrite roof antennas for RF-identification transponders*, August

Plotzke, O., Stenzel, E. and Frohn, O. (1994) *Elektromagnetische Exposition an elektronischen Artikelsicherungsanlagen*, Forschungsgemeinschaft für Energie und Umwelttechnologie — FGEU mbH commissioned by the Bundesanstalt für Arbeitsmedizin, Berlin

Prawitz, Ursula (1996) *Ident-Systeme in der Müllentsorgung: Kostensenkung für Bürger und Kommunen*, *Ident*, **1**

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Rankl, W. and Effing, W. (1996) *Handbuch der Chipkarten*, 2nd edn, Carl Hanser Verlag, Munich ISBN 3-446-18893-2

REGTP (2000a) Verfügung 61/2000, *Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für induktive Funkanlagen des nichtöffentlichen mobilen Landfunks (nömL)*, Amtsblatt 12, Regulierungsbehörde für Telekommunikation und Post, Bonn, 28th June, ISSN 1434–8128, http://www.regtp.de

REGTP (2000b) Verfügung 73/2000, *Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für Funkanlagen geringer Leistung des nichtöffentlichen mobilen Landfunks (nömL) in ISM Frequenzbereichen; SRD (Short Range Devices)*, Amtsblatt 18, Regulierungsbehörde für Telekommunikation und Post, Bonn, 20th September, ISSN 1434–8128, http://www.regtp.de

Reichel, Karl (1980) *Praktikum der Magnettechnik*, Franzis Verlag, Munich, ISBN 3-7723-6661-9

Reindl, L. and Mágori, V. (1995) *Funksensorik mit passiven Oberflächenwellen-Komponenten (OFW)*, VDI-Reihe 8: Mess-, Steuerungs- und Regeltechnik (Nr. 515), pp. 62–79

Reindl, L., Scholl, G., Ostertag, T., Schmidt, F., Pohl, A. (1998a) Funksensorik und Identifikation mit OFW-Sensoren, *Sensortagung Bad Nauheim, ITG/GMA Fachbericht* 148 — *Sensoren und Messtechnik*, pp. 77–86, VDE Verlag, ISBN 3-8007-2330-1

Reindl, L., Scholl, G., Ostertag, T., Seisenberger, C., Hornsteiner, J. and Pohl, A. (1998b) *Berührungslose Messung der Temperatur mit passiven OFW-Sensoren*, appeared in: Tagungsband VDI/GMA — Temperatur, VDI Report No. 1379, pp. 93–8

Reindl, L., Scholl, G., Ostertag, T., Scherr, H., Wolff, U. and Schmidt, F. (1998c) Theory and application of passive SAW radio transponders as sensors, *IEEE Transaction on Ultrasonics, Ferroelectrics and Frequency Control*, **45**(5), pp. 1281–92, ISSN 0885–3010

Rothammel, Karl (1981) *Antennenbuch*, 7th edn, Franckh'sche Verlagsbuchhandlung, W. Keller & Co., Stuttgart, ISBN 3-440-04791-1

Roz, Thierry and Fuentes, Vincent (n.d.) *Using low power transponders and tags for RFID applications*, Firmenschrift, EM Microelectronic Marin, CH-Marin

Rueppel, Rainer A. (1986) *Analysis and Design of Stream Ciphers*, Springer-Verlag, Heidelberg, ISBN 3-540-16870-2

Ruppert, Helmut (1994) Identifizierungssysteme mit zusätzlichen Sensorfunktionen, *GME-Fachbericht Nr. 13–Identifikationssysteme und kontaktlose Chipkarten*, vde-Verlag, Berlin

Sander, R. and Mollik, H. (1997) Ein guter Partner — RF-Identifikation in der Logistik löst Kundenprobleme, *ident*, **3**, Umschau Zeitschriftenverlag, Frankfurt

Schenk, C. (1997) Identifikationssysteme in der Automobilindustrie, *ident*, **2**, Umschau Zeitschriftenverlag, Frankfurt

Schmidhäusler, Fritz (1995) *Zutrittskontrolle richtig planen — Techniken, Verfahren, Organisation*, Hüthig Verlag, Heidelberg, ISBN 3-7785-2415-1

Schürmann, Josef (1993) TIRIS — Leader in Radio Frequency Identification Technology, *Texas Instruments Technical Journal*, November/December

Schürmann, Josef (1994) Einführung in die Hochfrequenz Identifikations Technologie, *GME Technical Report*, No. 13, *Identifikationssysteme und kontaktlose Chipkarte*, vde-Verlag, Berlin

Seidelmann, Christoph (1997) Funkwellen für Container — Automatische Identifizierung im kombinierten Verkehr, *ident*, **4**, Umschau Zeitschriftenverlag, Frankfurt

Sickert, Klaus (1994) Kontaktlose Identifikation — eine Übersicht, *GME-Fachbericht No. 13*, *Identifikationssysteme und kontaktlose Chipkarte*, vde-Verlag, Berlin

Siebel, Wolf (1983) *KW-Spezial-Frequenzliste*, Siebel Verlag Wachtberg-Pech

Siemens AG (n.d.) Data sheet *SOFIS — das sichere Ortungs- und Auto-ID System für Verkehrsunternehmen*, Siemens A. G., Bereich Verkehrstechnik, Berlin

Suckrow, Stefan (1997) Das Smith-Diagramm, *Funkschau*, **10**, Franzis Verlag, Munich

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

TagMaster (1997) Datasheet: *Mark Tag™ S1255, multiple access read-only-card*, TagMaster AB, S-Kista

Tanneberger, Volkmar (1995) *Informationsübertragung im Strassenverkehr mit passiven, batterielosen Mikrowellen-Transpondern*, Verlag Shaker, Braunschweig, ISBN 3-8265-0788-6

TEMIC (1977) Telefunken microelektronic GmbH, *Remote Control and Identification Systems*, Design Guide, D-Heilbronn, August

Texas Instruments Deutschland GmbH (1996) *Standard Transponder Specifications*, 06/1996

Tietze, U. and Schenk, Ch. (1985), *Halbleiter Schaltungstechnik*, 7th edn, Springer-Verlag, Berlin, ISBN 3-540-12488-6

Töppel, Matthias (1996) Zehn Milliarden Zugriffszyklen — Prozeßgesteuerte Identifikationssysteme, *elektro AUTOMATION*, **4**, Konradin Verlag, Leinfelden-Echterdingen

Ullerich, Stella (2001) *Herstellung und Charakterisierung ein- und mehrlagiger flexibler Mikrospulen für medizinische Telemetrieanwendungen*, Rheinisch-Westfälische Technische Hochschule (RWTH) Aachen, December, http://opac.bib.rwth-aachen.de/

Ullerich, S., Mokwa, G., Bögle, G. vom and Schnakenberg, U. (2000) Mico coils for an advanced system for measuring intraocular pressure, *Technical Digest 1st annual International IEEE-EMBS Special Topic Conference on Microelectronics in Medicine and Biology*, Lyon, France, 12–14 October, pp. 470–4

Ullerich, S., Mokwa, G., Bögle, G. vom and Schnakenberg, U. (2001a) A foldable artificial lens with an integrated transponder system for measuring intraocular pressure, *Technical Digest 11th International Congress on solid-state sensors and actuators Transducers '01 and Eurosensors XV*, Munich, Germany, 10–14 June, pp. 1224–7

Ullerich, S., Mokwa, G., Bögle, G. vom and Schnakenberg, U. (2001b) Foldable micro coils for a transponder system measuring intraocular pressure, *Proceedings of Sensors 2001*, 8–10 May, Nuremberg, Germany, vol. 1, pp. 319–342

Vcd, Krebs D., Unpublished manuscripts, Venture Development Corp., http://www.vdc-corp.com

Virnich, M. and Posten, K. (1992) *Handbuch der codierten Datenträger*, Verlag TÜV Rheinland GmbH, Cologne, ISBN 3-8249-0044-0

Vogt (1990) *Vogt Elektronik, Components Handbook — 1990*, Passau

Weisshaupt, Bruno and Gubler, Gerda (1992) *Identifikations- und Kommunikationssysteme, Datenträger verändern die Automation*, Die Bibliothek der Technik, Band 61, verlag moderne industrie AG & Co., Landsberg/ Lech, ISBN 3-478-93071-5

Wolff, Hartmuth (1994) Optimaler Kfz-Diebstahlschutz durch elektronische Wegfahrsperren, *GME Technical Report*, No. 13, *Identifikations-systeme und kontaktlose Chipkarten*, vde-Verlag, Berlin

Zechbauer, Ulrike (1999) Mit amorphen Metallen auf der Jagd nach Ladendieben, *Forschung und Innovation*, **1**, Siemens AG, Munich, http://www.forschung-innovation.de

Zorzi, Michele (1995) Mobile radio slotted ALOHA with capture and diversity, *Wireless Networks*, **1**

14.4 Printed Circuit Board Layouts

14.4.1 Test card in accordance with ISO 14443

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

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

14.4.2 Field generator coil

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

Table 14.1 Jumper position for setting the supported modulation procedures

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

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

Table 14.2 Parts list for test chip card

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

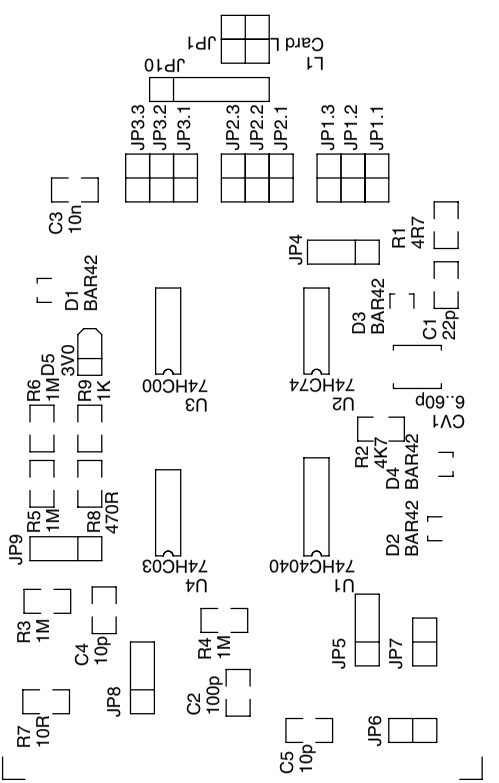


Figure 14.1 Component mounting diagram of the ISO 14443 test card. The transponder's antenna is in the upper half of the printed circuit board

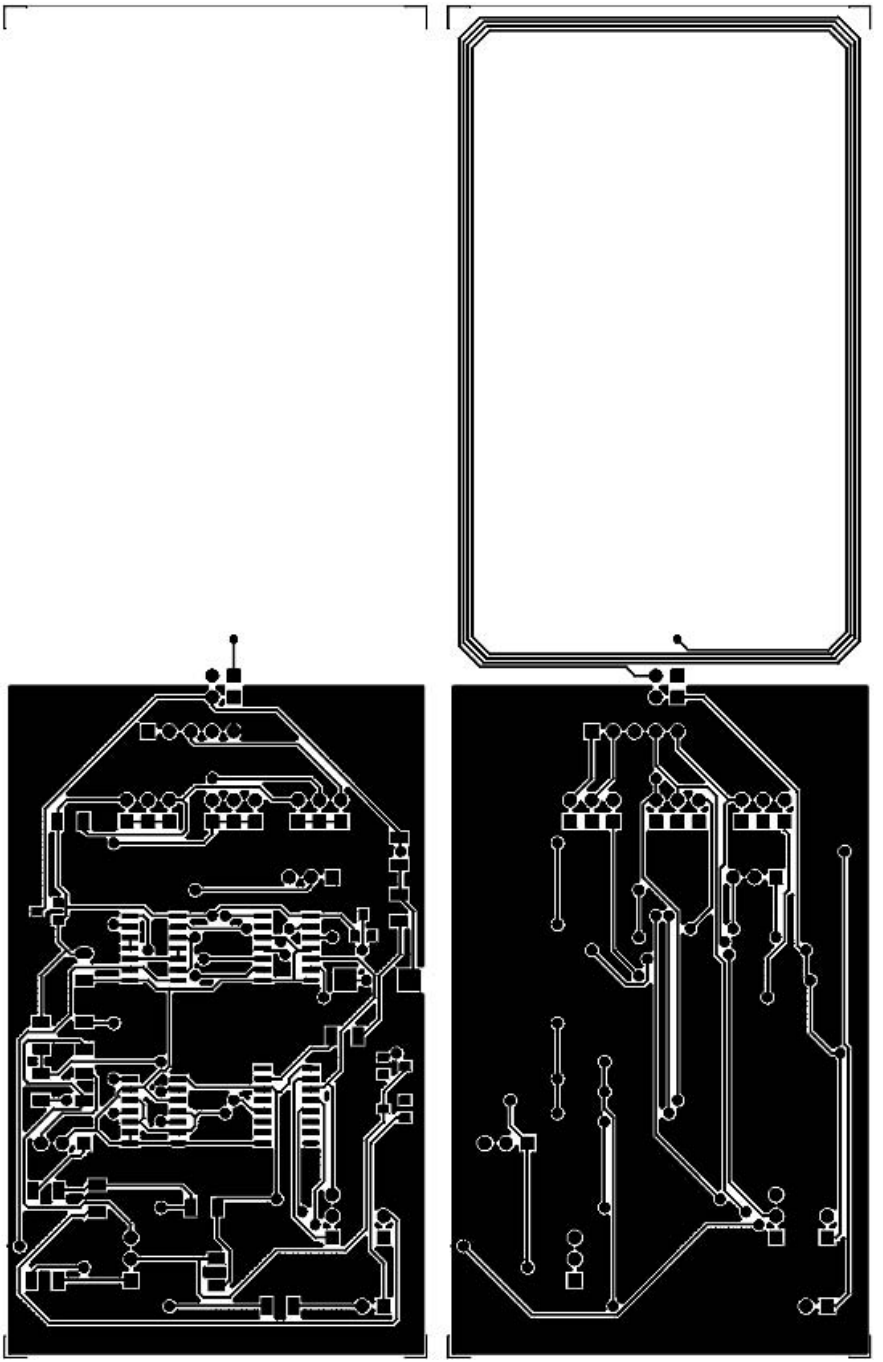


Figure 14.2 Printed circuit board layout of the test card, front and back

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

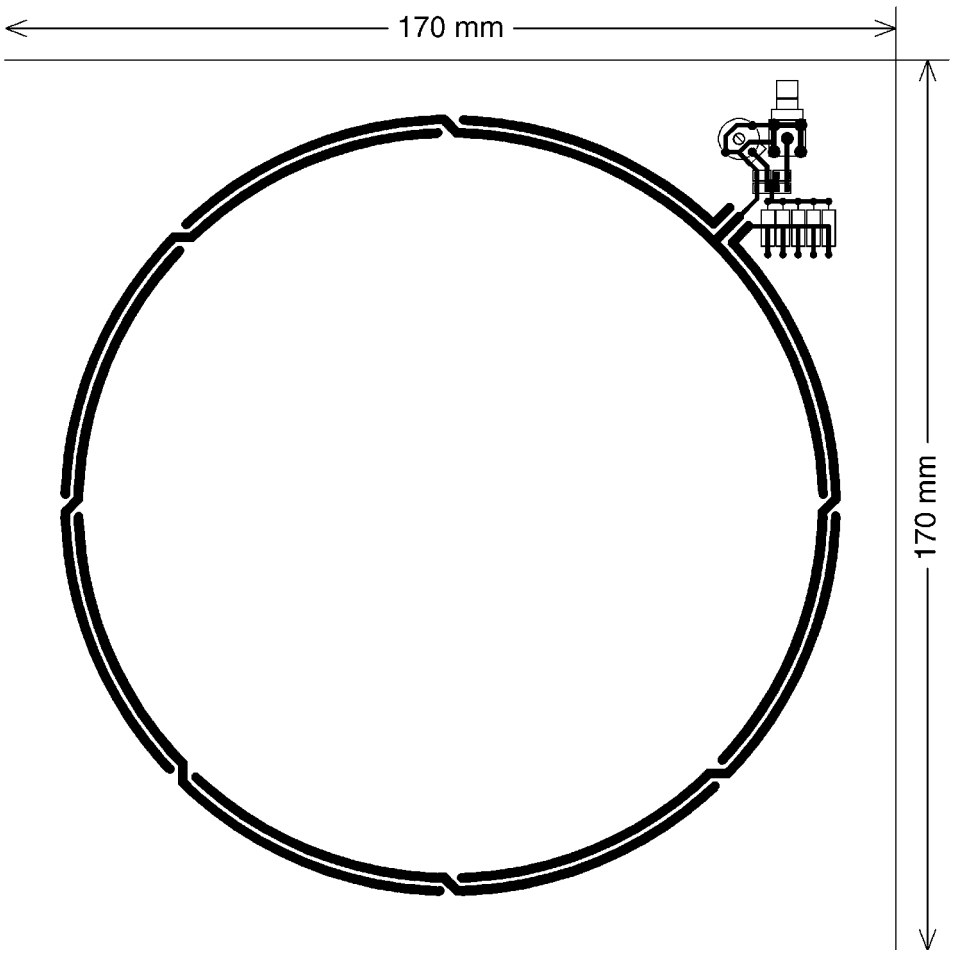


Figure 14.3 Layout of the field generator coil — front (reproduced by permission of Philips Semiconductors, Hamburg)

Table 14.3 Parts list of the interface circuit

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

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

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

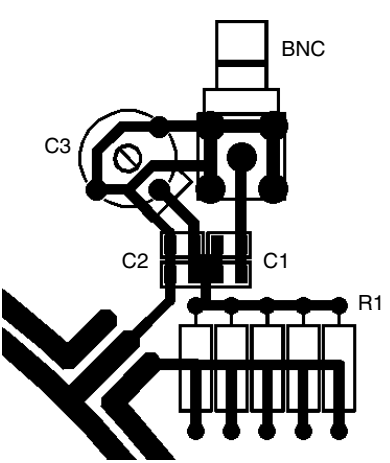


Figure 14.5 Interface circuit of the field generator coil — component mounting diagram

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

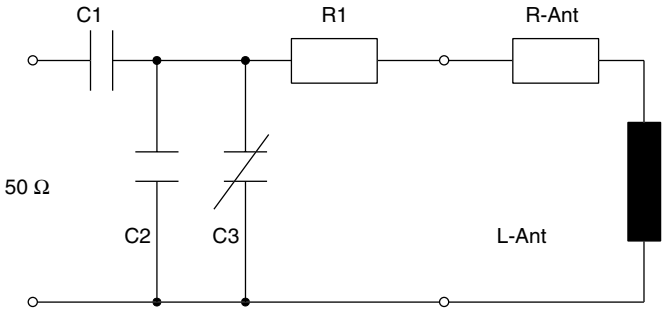


Figure 14.6 Interface circuit of the field generator coil — circuit

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Index

1-bit transponder 29
199/5/EG 170, 177, 405
2 frequency shift keying 189
2 FSK 189
  modulation 57
2-wire folded dipole 125

A/D converter 303
Absorption rate 26, 169
Acceleration measurement 305
Access authorisation 357
Access control 25, 360
Access protection page 290
Access register 282
Access rights 283
Acoustomagnetic security system 37
Activation field 230
Activator 29
Active transponder 13, 78
Address logic 278
Administration code 287
Advanced mode 233
Advanced transponder 233
AFC 343
AIM 394, 399
Air gap 49
Ali Baba 221
ALOHA procedure 205, 206
Amorphous metal 36, 38, 111
Amplitude 183
Amplitude modulation 98, 186
Anharmonic 40
Animal identification 25, 230, 404
  dipole 57
Antenna 119
Antenna coil 319
Antenna current 87
Antenna radius 65
Anti-collision algorithm 102
Anti-collision procedure 25
Anti-collision system 202
Anti-theft devices 29
APDU 253
Application 286
Application code (MAD) 287
Application directory 287
  MAD 287
Application identifier 270
Application layer 270
Application software 310, 317
Artificial interocular lens 392
ASK modulation 186, 243, 244, 312
Asymmetric key procedure 224
ATQB 248
ATS 253
Attack 27
Attempted attack 221
Authentication 25, 27, 221, 282, 373
Authentication protocol 221
Auto-ID Homepage 399
Automatic fare collection 343
Automatic I.D. News 398
Automatic Vehicle Identification 401
Automotive industry 389

Backscatter 49
  modulated 143
Backscatter modulator 274
Backscatter system 23, 117, 131, 166
Backscatter transponder 176
Baked enamel 330
Bandwidth 167
Barcode 2, 270
Baseband signal 183, 312
Battery 140
Bending measurement 305
Binary search procedure 205
Binary search tree algorithm 213, 245
Biometry 4
Bit coding 212

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Block structure 281
Bolus 367
Broadcast 200
Bulletin board 400
Business Solutions 398
Busy signal 357

Calibration coil 261
CALYPSO 353
Cancellation 141
Capacitance diode 34
Capacitive coupling 23, 51
Capacitive coupling element 238
Capacitive load modulation 98
Capture effect 209
Car keys 14
Cardiac pacemaker 400
Carrier 183, 186
Carrier circuit 183
Carrier oscillation 186
CDMA 201
CE mark 170, 177
  documentation 406
CEPT 169, 177
Channel 183
Channel spacing 170
Characteristic wave impedance 115
Charging capacitor 54
Checksum 195
Chip 6
CID 254
Cipher
  one-time-pad 225
  sequential 225
  Vernam 225
Ciphering 224
Circuit damping 76
Circular polarisation 116, 129
Clamping device identification 265
Close coupling 340
Close coupling system 22, 50
Close-coupling smart card 236, 261
CNC technology 381
Coaxial cable 322
Code
  EAN 3
Code division multiple access 201
Coding in the baseband 183
Coil resistance 73
Coil-on-chip 20
Collar transponder 364
Collision interval 208
Communication system 183
Compression measurement 305
Conductor loop 86, 112
Conductor loop antenna 87
Configuration register 282
Contact smart card 293
Contacting 337
Contactless clock 18
Contactless interface unit 296
Contactless smart card 18, 22, 332
Container identification 265, 377
Coprocessor 25
Coupling
  capacitive 23, 51
  electric 23, 51
  inductive 22, 61, 113
  magnetic 22
Coupling coefficient 70, 92
Coupling element 7
  inductive 238
  capacitive 238
Coupling loss 314
CRC 197, 236, 255, 296
Cryptographic co-processor 294, 297
Cryptography 294
Cryptological key 222
Cryptological unit 278
Crystal lattice 148
Current matching 55

Data block 254
Data carrier 6
Data transfer 183
Data transmission 97
DBP code 185
Deactivation device 268
Deactivation rate 268
Deactivator 29
Deciphering 224
Decryption 224, 298
Demodulation 183, 186, 273, 276
Demodulator 183
DES 297
Detection rate 29, 266
Dice 330
Die 330
Dielectric gap 111
Differential bi-phase code 184
Differential code 185
Dimple 32
DIN 405

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Diode
Schottky 49
Dipole antenna 34, 57, 111, 119, 125
Direction of maximum radiation 127
Directional antenna 127
Directional beam 26
Directional coupler 49
Directional coupling 313
Director 127
Disk transponder 13
Dopant profile 34
Doppler effect 303
Driver 318
Dual interface card 25, 293, 351
Dual port EEPROM 289
Duty factor 186

EAN 270
EAN code 3
EAN/UCC-128 271
Ear tag 364
EAS 11, 29, 172
EAS system 23
Eddy 112
Eddy current 72
Eddy current losses 110
EEPROM 388
lifetime 300
write time 302
Effective aperture 121
Effective height 125
Effective length 125
EIRP 119
Electric coupling 23, 51
Electric field 22, 111
Electric rotational field 71
Electrical field 51
Electrode 51
Electromagnetic field 22
Electromagnetic interference field 26
Electromagnetic procedure 36
Electromagnetic wave 113, 117, 322
creation of 112
Electronic Article Surveillance 11, 23, 29, 172, 173
electromagnetic procedure 36
frequency divider procedure 35
microwave systems 33
RF procedure 29
Electronic data carrier 273
Electronic immobilisation 371
Electronic immobilisation system 14
Elektrosmog-Verordnung 400
Embedding technique 333
EN 300 220 176
EN 300 330 167, 173
EN 300 440 176
Encrypted data transmission 224
Encryption 27, 224, 297
Encryption function 226
End-of-burst detector 56
Energy range 82, 315
Equivalent circuit
Schottky diode 134
ERC recommendation 70–03 169
ERO 170, 177
Address 406
ERP 120
Etching 19
Etching technique 335
ETCS 361
ETSI 173
Address 406
Eurobalise 171, 361
European Radio Office 170
Exchange system 350

Fahrsmart 349
False alarm rate 266
Far field 112, 167
FCC Part 15 179
FCC regulation 179
FDMA 201, 204
FDX 11, 40
FDX-B transponder 233
Ferrite 15
Ferrite antenna 108
Ferrite pot core 15
Ferrite rod 110
Ferromagnetic metal 38
Field
electric 51
magnetic 61
Field generator coil 262, 414
interface circuit 417
Field line
magnetic 84
Field strength 142
magnetic 61
maximum 65
path of 64
Floating gate 299
FRAM 300
write time 302

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Frame 254
Frame antenna 32
Free space attenuation 114
Free space path loss 47
Freight containers ID 404
Frequency 183
  anharmonic 40
  harmonic 33, 40
  percentual distribution 162
  subharmonic 36, 40
  transmission 13
Frequency band 170
Frequency domain multiple access 201, 204
Frequency modulation 186
Frequency range 161
  2.45 GHz 117, 166
  5.8 GHz 166
  135 kHz 162
  6.78 MHz 163
  13.56 MHz 163
  27.125 MHz 163
  433.920 MHz 164
  868 MHz 166
  915 MHz 117, 166
Frequency selection 167
Frequency shift keying 186
Frontline-Solutions 398
FSDI 253
FSK 186
FSK modulation 312
Full duplex procedure 11, 40
Function cluster 287
Functional testing 261

Generator coil 31
Generator polynomial 197
Glass transponder 14, 110
Glaucoma 392
Global ID magazine 398
Graphite coating 53
Ground antenna 379
Group antenna 129
GTAG 269

H-field 173
Half duplex procedure 11, 40
Half-wave dipole 125
Hard magnetic metal 37
Hard tag 30, 34
Harmonic 33
Harmonic frequency 40
HDX 11, 40
HF interface 273, 310
High-end system 25
High-end transponder 273
Human medicine 392
Hybrid card 351
Hysteresis curve 36, 107

I block 254
ICARE 350
ident 398
Identification codes for animals 230
Identification of animals 229
Identification system 385
IDLE mode 245
Ignition lock 372
IIC bus 189
Immobilisation system 317
Impedance matching 134, 139
Induced voltage 72
Inductance 67
  mutual 68, 72
Inductance law 72
Inductive coupling 22, 61, 113, 167
Inductive coupling element 238
Inductive radio system 22, 172, 173
Industrial automation 25
Injectible transponder 364
Information source 183
Injection needle 366
Inlet foil 332
Input capacitor 131
Input impedance
  antenna 121
  transponder 131
Input voltage
  HF 80
Interdigital transducer 57, 149
Interface circuit
  component mounting diagram 417
Interference reflection 152
Internet links 399
Interrogation field strength 66, 80, 142, 241
Interrogation pulse 151
Interrogation zone 84, 131
ISM frequency ranges 161
ISO 405
ISO 10374 265
ISO 10536 51, 237
ISO 11784
  identification code 233
ISO 6346 265
ISO 69871 265

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

ISO 69872 265
ISO 69873 16, 265
ISO 9798-2 221
ISO container 265
Isotropic emitter 115, 199
Item management 268, 405

Key 224
  application specific 284
  application's own 284
  hierarchical 283
  master 223
  secret 282
Key memory 282
KONTIKI 397

Label 20
Lamination 339
Langasite 307
Lead frame 337
Licensing regulations 173
Line code 184
Linear detection 134
Lines of magnetic flux 62
Lithium niobate 57, 148
Lithium tantalate 57, 148
Load modulation 44, 53, 97, 232, 238, 319
  capacitive 98
  ohmic 98
  real 98
Load modulator 102, 274
Load resistance 95, 191
Load resistor 44, 131
Long-range system 23, 47
Longitudinal redundancy check 196
Longwave 161
Loop antenna 174
Low-barrier Schottky diode 49
Low-cost transponder 168
Low-end system 23
LPRA 397
LRC 196
Lufthansa 354

MAD 287
  application code 287
  function cluster 287
Magnetic alternating field 62
Magnetic coupling 22
Magnetic field 22, 61, 111
Magnetic field lines 84
Magnetic field strength 61
Magnetic flux 66
Magnetisation characteristic 107
Magnetostriction 38
Main radiation direction 119
Manchester code 184, 212
Manipulation 222
Market for smart cards 5
Mass production 385
Master key 223
Master-slave principle 310
Mat 380
Matching 139
  current 55
  power 55
  voltage 55
Matching circuit 322
Material flow 385
Measurement
  acceleration 304, 305
  compression 305
  distance 303
  flow 304
  gases 304
  light 304
  moisture 304
  PH value 304
  physical quantities 307
  speed 303
  temperature 305
Memory
  segmented 285
Memory block 236
Memory capacity 28
Memory card 5
Memory segmentation
  variable 285
Metal
  amorphous 36, 38
  hard magnetic 37
Metal foil 53
Metal lid 110
Metal surface 15, 72, 110, 377, 282
  radar cross-section 118
Metallic surface 109
Microchip 7, 35, 73, 329
  operating voltage 78
  power consumption 95
  power supply 73
Microcoil 392
Microprocessor 292
  operating system 292
  smart card 6, 296

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Microstrip antenna 128
Microwave 33
Microwave frequency 47
Microwave range 23
Microwave system 313
MIFARE 295
MIFARE transponder 286
Miller code 185, 243
  modified 185
Mobile telephone 293
Modem 183
Modified miller code 185
Modulated backscatter 49, 143
Modulated radar cross-section 117
Modulation 146, 183, 186
  2-FSK 57
  ASK 312
  FSK 312
  PSK 312
Modulation capacitor 100
Modulation index 146
Modulation product 186
Modulation resistor 98, 276
Modulator 183
Motor electronics 373
MP&PR specification 271
Multi-access 200
Multilevel modulation 191
Multiplexer 357
Mutual authentication 221
Mutual authorisation 282
Mutual inductance 68, 72, 88, 68–69

National legislative regulations 177
Near field 43, 112, 167
NF range 36
Noise 145
Non-linear resistance 33
NRZ code 184, 212, 239, 243
NTC 303

Occipital bone 367
OCR reader 3
OCR system 3
OEM reader 326
Offered load 206
On-chip oscillator 318
On-chip trimming capacitor 54
On-off keying 187
One-port resonator 155
One-time-pad 225
Operating frequency 86
Operating system 6, 292
  smart card 296
Operating voltage 78
Order processing 391
Oscillator 145, 312
  on-chip 318
OSI layer model 254
Overlay foil 332

Parallel regulator 79
Parallel resonant circuit 73
Parity bit 195
Parity test 195
Passive transponder 13, 41, 78, 274
Password 282
Patch antenna 128
Payment 293
PCB 255
PCD 240, 256
Peak value rectification 134
Penetration depth 169
Permanent magnet 37
Permeability 106
Phase 183
Phase modulation 100, 186
Phase noise 145
Phase position 305
Phase shift keying 186
PICC 240
Piezoeffect 148
Piezoelectric crystal 148
Piezoelectrical effect 57
Pigeon ring 370
Planar antenna 128
Plastic housing 14
Plastic package (PP) 14
Polarisation 116
  circular 116
  horizontal 116
  linear 116
  vertical 116
Polarisation direction 142
Polarisation loss 116
Polling procedure 205
Polyethylene foil 31
Polymer thick film paste 334
Power consumption 95
Power level 170
Power management unit 295
Power matching 55
Power on logic 278
Power saving mode 297

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Power supply 13, 73, 133, 273
shunt regulator 80
Power-down mode 296
Poynting radiation vector S 115
PPM 257
Press reports on the internet 400
Production process 385
Programming station 358
Protocol
T = 1 253
T = CL 253
Proximity card 240
Proximity coupling smart card 261
Pseudorandom sequence 225
PSK 186, 238
Public transport 340
Pulse pause coding 185
Pulse position modulation 257
Pulse radar 316
Pulsed system 41

Q factor 76, 96, 102, 156, 325
Quality features 260
Quartz 148

R block 254
R&TTE Directive 170, 177, 406
R&TTE homepage 177
Radar cross-section 117
RADAR technology 49, 117
Radiation density 115, 117
Radiation pattern 119
Radiation resistance 121, 125, 128, 140
Radio service 161
Radio system 161
Rail traffic 171
Random number 222, 370
Range 26, 47, 53, 65, 85, 152, 168, 202
Range limit 114
RATS 252
Rayleigh wave 148
RCS 118
Read range 53, 65, 82, 85
Read-only transponder 23, 273, 280
Reader 7, 86, 183, 310, 326–8
for OCR 3
REC 70-03 169
Received power 122
Received signal 184
Received signal conditioning 318
Receiver 183
Receiver arm 312
Receiver sensitivity 145
Reference card 261, 263, 264
Reflection 141
Reflection characteristics 49
Reflection cross-section 49
Reflective delay line 152
Reflective properties 117
Reflector 57, 127, 150
RegTP 406
Regulation 170
Regulations
reference sources 405
Release taper shaft 265
Remote coupling system 22
REQB command 248
REQUEST command 206, 209
Resistance
nonlinear 33
Resonant circuit coil 35
Resonant frequency 31, 73, 89
Resonator 156
Response pulse
phase angle 152
phase position 305
Retention bolts 383
Retention knob 265
RF innovations 399
RF procedure 30
RFID market 2
RFID newsletter 399
RFID system 1, 7, 25
Road toll systems 172
Robots 391
RSA 298
RTI 400

S block 254
SAK 252
SAM 223
SAW 57
Saw on foil 330
Scanning pulse 57
Scatter aperture 118, 122, 143
Schottky detector 134, 142
Schottky diode 49, 134
junction capacitance 134
junction resistance 134
Screen printing 19
Screen printing technique 333
Scutulum 367
SDMA 201, 202
Security element 29

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Security logic 278
Security requirements 27
  smart card 294
Security system 221
Security tag 29
Segmented transponder 284
SELECT command 210
Self-inductance 72
Semiconductor circuit 35
Sensor coil 31
Sensor data 302
Seoul 347
SEQ 54
Sequential cipher 225
Sequential procedure 11, 54
Sequential transponder 11
Serial number 23, 209, 213, 280, 298, 329, 372
Series resonant circuit 86, 320
Shift register 200
Short range device 170
Shortening factor 126
Shortwave frequency 163
Shunt regulator 79, 102
Shunt resistor 78
Sideband 146, 186
Sigma modulation 143
Signal coding 183
Signal decoding 183
Signal processing 183
Signal representation 183
Signal travelling times 303
Silver conductive paste 53
Ski lift 356
Slot 208
Slotted ALOHA procedure 208, 248
Smart card 5
  close-coupling 236
  with microprocessor 6
Smart card market 5
Smart card operating system 296
Smart label 19, 21
Smart Labels Analyst 399
Software application 310
Sonotrode 333
Space division multiple access 201, 202
Speed of light 112
Spherical emitter 115
Split-phase encoding 184
Spread spectrum 201, 271
Spurious emissions 175
Square law detection 135
SRAM 389
SRD 170, 173, 401, 403
Standards
  reference sources 405
State diagram 279
State machine 12, 25, 273, 279, 295
Sticky labels 19
Storekeeping 391
Stream cipher 224
Stretching measurement 305
Subcarrier 44, 191, 238, 274, 312
Subcarrier frequency 191
  307.2 kHz 238
  847 kHz 243
Subharmonic 36, 40
Superposition 141
Supply chain systems 398
Surface acoustic wave 57, 148
Surface acoustic wave device 57
Surface acoustic wave transponder 23, 315
Surface resistance 334
Swept signal 31
Symmetrical key procedure 224
Synchronisation
  cable 231
  of several readers 231
System clock 279

T/R 22-04 176
T/R 60-01 176
Tag 29
Taper shaft 383
TDMA 201, 205
Telemetry transmitter 173, 302
Temperature measurement 305
Temperature sensor 155, 303
Test mode 329
Three pass mutual authentication 221
Ticketing 26
Time domain multiple access 201, 205
Tool holder 381
Tool identification 265
Touch & go 49
Traffic telematics 172
Transaction time 294
Transformed impedance 44
Transformed transponder impedance 88, 97
Transformer coupling 113
Transformer-type coupling 42
Transmission channel 183
Transmission error 184

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189

Transmission frequency 13, 91
Transmission medium 183
Transmission protocol
ISO 14223 234
Transmitter 183
Transmitter arm 312
Transmitter output power 176
Transponder 7, 183
1-bit 29
active 13
disk 13
glass 14
passive 13, 41, 78, 274
Transponder antenna 143
Transponder coil 330
Transponder impedance
transformed 88
Transponder News 400
Transponder resonant circuit 97, 102, 276
Transponder resonant frequency 105
Transport container 270
Transport layer 270
Trimming capacitor
on-chip 54

U2270B 318
UCC 270
UHF frequency range 47, 165, 270
UHF range 23
Unipolar code 185
Unique number 23, 298, 372

VDE 406
VDI 406
VDI 4470 29, 267
Vehicle identification 171
Vehicle theft 371
Vernam cipher 225
VHF range 164
VICC 256
Vicinity coupling 340
smart card 256
system 23
VISA 352
Voltage divider
capacitive 53
Voltage doubler 135
Voltage matching 55

Wafer 329
Warensicherungssysteme
Kundenabnahmerichtlinie 405
Waste disposal 378
Wavelength 112
Winding technique 333
Write time 302

Yagi-Uda antenna 127

ZKA 352

HANSHOW-Ex. 1029
Hanshow Am. Inc. v. SES-Imagotag Inc.
IPR2024-00189