RFID HANDBOOK

FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS, RADIO FREQUENCY IDENTIFICATION AND NEAR-FIELD COMMUNICATION, THIRD EDITION

Klaus Finkenzeller
Giesecke & Devrient GmbH, Munich, Germany

Translated by Dörte Müller
Powerwording.com

WILEY
A John Wiley and Sons, Ltd., Publication

RFID HANDBOOK
THIRD EDITION

RFID HANDBOOK

FUNDAMENTALS AND APPLICATIONS IN CONTACTLESS SMART CARDS, RADIO FREQUENCY IDENTIFICATION AND NEAR-FIELD COMMUNICATION, THIRD EDITION

Klaus Finkenzeller
Giesecke & Devrient GmbH, Munich, Germany

Translated by Dörte Müller
Powerwording.com

WILEY
A John Wiley and Sons, Ltd., Publication

This edition first published 2010

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

Library of Congress Cataloging-in-Publication Data

Finkenzeller, Klaus.
[RFID Handbuch. English]
Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition / Klaus Finkenzeller ; translated by Dörte Müller. – 3rd ed.
p. cm.
Includes index.
ISBN 978-0-470-69506-7 (cloth)
1. Inventory control–Automation. 2. Radio frequency identification systems. 3. Smart cards. I. Title.
TS160.F5513 2010
658.7′87 – dc22

2010008338

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

ISBN: 978-0-470-69506-7

Typeset in 9/11 Times by Laserwords Private Limited, Chennai, India
Printed and bound in Great Britain by CPI Antony Rowe, Chippenham, Wiltshire, UK

Contents

Preface to the Third Edition **xi**

List of Abbreviations **xiii**

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
1.1.4 Smart Cards 4
1.1.5 RFID Systems 6
1.2 A Comparison of Different ID Systems 6
1.3 Components of an RFID System 6

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 13
2.2.3 Plastic Housing 13
2.2.4 Tool and Gas Bottle Identification 15
2.2.5 Keys and Key Fobs 15
2.2.6 Clocks 17
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 21
2.4 Active and Passive Transponders 22
2.5 Information Processing in the Transponder 24
2.6 Selection Criteria for RFID Systems 25
2.6.1 Operating Frequency 26
2.6.2 Range 26
2.6.3 Security Requirements 27
2.6.4 Memory Capacity 28

3	**Fundamental Operating Principles**		**29**
3.1	1-Bit Transponder		29
	3.1.1	*Radio Frequency*	29
	3.1.2	*Microwaves*	33
	3.1.3	*Frequency Divider*	34
	3.1.4	*Electromagnetic Types*	35
	3.1.5	*Acoustomagnetic*	38
3.2	Full- and Half-Duplex Procedure		39
	3.2.1	*Inductive Coupling*	40
	3.2.2	*Electromagnetic Backscatter Coupling*	45
	3.2.3	*Close-Coupling*	48
	3.2.4	*Data Transfer Reader → Transponder*	49
	3.2.5	*Electrical Coupling*	50
3.3	Sequential Procedures		52
	3.3.1	*Inductive Coupling*	52
	3.3.2	*Surface Acoustic Wave Transponder*	55
3.4	Near-Field Communication (NFC)		57
	3.4.1	*Active Mode*	57
	3.4.2	*Passive Mode*	59
4	**Physical Principles of RFID Systems**		**61**
4.1	Magnetic Field		61
	4.1.1	*Magnetic Field Strength H*	61
	4.1.2	*Magnetic Flux and Magnetic Flux Density*	66
	4.1.3	*Inductance L*	66
	4.1.4	*Mutual Inductance M*	67
	4.1.5	*Coupling Coefficient k*	68
	4.1.6	*Faraday's Law*	70
	4.1.7	*Resonance*	72
	4.1.8	*Practical Operation of the Transponder*	76
	4.1.9	*Interrogation Field Strength H_{min}*	77
	4.1.10	*Total Transponder–Reader System*	84
	4.1.11	*Measurement of System Parameters*	100
	4.1.12	*Magnetic Materials*	106
4.2	Electromagnetic Waves		110
	4.2.1	*The Generation of Electromagnetic Waves*	110
	4.2.2	*Radiation Density S*	112
	4.2.3	*Characteristic Wave Impedance and Field Strength E*	112
	4.2.4	*Polarisation of Electromagnetic Waves*	114
	4.2.5	*Antennas*	116
	4.2.6	*Practical Operation of Microwave Transponders*	127
4.3	Surface Waves		144
	4.3.1	*The Creation of a Surface Wave*	144
	4.3.2	*Reflection of a Surface Wave*	146
	4.3.3	*Functional Diagram of SAW Transponders*	147
	4.3.4	*The Sensor Effect*	149
	4.3.5	*Switched Sensors*	154
5	**Frequency Ranges and Radio Licensing Regulations**		**155**
5.1	Frequency Ranges Used		155

	5.1.1	*Frequency Range 9–135 kHz*	157
	5.1.2	*Frequency Range 6.78 MHz (ISM)*	158
	5.1.3	*Frequency Range 13.56 MHz (ISM, SRD)*	159
	5.1.4	*Frequency Range 27.125 MHz (ISM)*	159
	5.1.5	*Frequency Range 40.680 MHz (ISM)*	160
	5.1.6	*Frequency Range 433.920 MHz (ISM)*	160
	5.1.7	*UHF Frequency Range*	160
	5.1.8	*Frequency Range 2.45 GHz (ISM, SRD)*	161
	5.1.9	*Frequency Range 5.8 GHz (ISM, SRD)*	161
	5.1.10	*Frequency Range 24.125 GHz*	161
	5.1.11	*Selection of a Suitable Frequency for Inductively Coupled RFID Systems*	162
5.2	The International Telecommunication Union (ITU)		164
5.3	European Licensing Regulations		165
	5.3.1	*CEPT/ERC REC 70-03*	166
	5.3.2	*Standardised Measuring Procedures*	170
5.4	National Licensing Regulations in Europe		172
	5.4.1	*Germany*	172
5.5	National Licensing Regulations		175
	5.5.1	*USA*	175
5.6	Comparison of National Regulations		176
	5.6.1	*Conversion at 13.56 MHz*	176
	5.6.2	*Conversion on UHF*	178
6	**Coding and Modulation**		**179**
6.1	Coding in the Baseband		179
6.2	Digital Modulation Procedures		180
	6.2.1	*Amplitude Shift Keying (ASK)*	182
	6.2.2	*2 FSK*	185
	6.2.3	*2 PSK*	185
	6.2.4	*Modulation Procedures with Subcarrier*	187
7	**Data Integrity**		**189**
7.1	The Checksum Procedure		189
	7.1.1	*Parity Checking*	189
	7.1.2	*LRC Procedure*	190
	7.1.3	*CRC Procedure*	191
7.2	Multi-Access Procedures – Anticollision		194
	7.2.1	*Space Division Multiple Access (SDMA)*	196
	7.2.2	*Frequency Domain Multiple Access (FDMA)*	197
	7.2.3	*Time Domain Multiple Access (TDMA)*	197
	7.2.4	*Examples of Anticollision Procedures*	199
8	**Security of RFID Systems**		**213**
8.1	Attacks on RFID Systems		214
	8.1.1	*Attacks on the Transponder*	215
	8.1.2	*Attacks on the RF Interface*	216
8.2	Protection by Cryptographic Measures		226
	8.2.1	*Mutual Symmetrical Authentication*	227
	8.2.2	*Authentication using Derived Keys*	228
	8.2.3	*Encrypted Data Transfer*	228

9	**Standardisation**		**233**
9.1	Animal Identification		233
	9.1.1	*ISO/IEC 11784 – Code Structure*	233
	9.1.2	*ISO/IEC 11785 – Technical Concept*	234
	9.1.3	*ISO/IEC 14223 – Advanced Transponders*	236
9.2	Contactless Smart Cards		240
	9.2.1	*ISO/IEC 10536 – Close-Coupling Smart Cards*	241
	9.2.2	*ISO/IEC 14443 – Proximity-Coupling Smart Cards*	243
	9.2.3	*ISO/IEC 15693 – Vicinity-Coupling Smart Cards*	258
	9.2.4	*ISO/IEC 10373 – Test Methods for Smart Cards*	263
9.3	ISO/IEC 69873 – Data Carriers for Tools and Clamping Devices		267
9.4	ISO/IEC 10374 – Container Identification		267
9.5	VDI 4470 – Anti-theft Systems for Goods		267
	9.5.1	*Part 1 – Detection Gates – Inspection Guidelines for Customers*	267
	9.5.2	*Part 2 – Deactivation Devices – Inspection Guidelines for Customers*	270
9.6	Item Management		270
	9.6.1	*ISO/IEC 18000 Series*	270
	9.6.2	*GTAG Initiative*	273
	9.6.3	*EPCglobal Network*	274
10	**The Architecture of Electronic Data Carriers**		**283**
10.1	Transponder with Memory Function		283
	10.1.1	*RF Interface*	283
	10.1.2	*Address and Security Logic*	286
	10.1.3	*Memory Architecture*	289
10.2	Microprocessors		300
	10.2.1	*Dual Interface Card*	303
10.3	Memory Technology		307
	10.3.1	*RAM*	307
	10.3.2	*EEPROM*	308
	10.3.3	*FRAM*	309
	10.3.4	*Performance Comparison FRAM – EEPROM*	310
10.4	Measuring Physical Variables		311
	10.4.1	*Transponder with Sensor Functions*	311
	10.4.2	*Measurements Using Microwave Transponders*	312
	10.4.3	*Sensor Effect in Surface Wave Transponders*	315
11	**Readers**		**317**
11.1	Data Flow in an Application		317
11.2	Components of a Reader		317
	11.2.1	*RF Interface*	318
	11.2.2	*Control Unit*	323
11.3	Integrated Reader ICs		324
	11.3.1	*Integrated RF Interface*	325
	11.3.2	*Single-Chip Reader IC*	327
11.4	Connection of Antennas for Inductive Systems		331
	11.4.1	*Connection Using Current Matching*	333
	11.4.2	*Supply via Coaxial Cable*	333
	11.4.3	*The Influence of the Q Factor*	338
11.5	Reader Designs		338

11.5.1 OEM Readers 338
11.5.2 Readers for Industrial Use 338
11.5.3 Portable Readers 338
11.6 Near-Field Communication 339
11.6.1 Secure NFC 341

12 The Manufacture of Transponders and Contactless Smart Cards 347
12.1 Glass and Plastic Transponders 347
12.1.1 Chip Manufacture 347
12.1.2 Glass Transponders 348
12.1.3 Plastic Transponders 351
12.2 Contactless Smart Cards 352
12.2.1 Coil Manufacture 352
12.2.2 Connection Technique 356
12.2.3 Lamination 359

13 Example Applications 361
13.1 Contactless Smart Cards 361
13.2 Public Transport 362
13.2.1 The Starting Point 362
13.2.2 Requirements 363
13.2.3 Benefits of RFID Systems 363
13.2.4 Fare Systems using Electronic Payment 365
13.2.5 Market Potential 366
13.2.6 Example Projects 366
13.3 Contactless Payment Systems 372
13.3.1 MasterCard® 374
13.3.2 ExpressPay by American Express® 374
13.3.3 Visa® Contactless 374
13.3.4 ExxonMobil Speedpass 375
13.4 NFC Applications 375
13.5 Electronic Passport 380
13.6 Ski Tickets 383
13.7 Access Control 385
13.7.1 Online Systems 385
13.7.2 Offline Systems 385
13.7.3 Transponders 387
13.8 Transport Systems 388
13.8.1 Eurobalise S21 388
13.8.2 International Container Transport 390
13.9 Animal Identification 391
13.9.1 Stock Keeping 391
13.9.2 Carrier Pigeon Races 395
13.10 Electronic Immobilisation 398
13.10.1 The Functionality of an Immobilisation System 399
13.10.2 Brief Success Story 401
13.10.3 Predictions 402
13.11 Container Identification 403
13.11.1 Gas Bottles and Chemical Containers 403
13.11.2 Waste Disposal 404

13.12 Sporting Events 405
13.13 Industrial Automation 409
13.13.1 Tool Identification 409
13.13.2 Industrial Production 410
13.14 Medical Applications 417

14 Appendix 419
14.1 Contact Addresses, Associations and Technical Periodicals 419
14.1.1 Industrial Associations 419
14.1.2 Technical Journals 421
14.1.3 RFID on the Internet 422
14.2 Relevant Standards and Regulations 423
14.2.1 Standardisation Bodies 423
14.2.2 List of Standards 423
14.2.3 Sources for Standards and Regulations 428
14.3 Printed Circuit Board Layouts 429
14.3.1 Test Card in Accordance with ISO 14443 429
14.3.2 Field Generator Coil 435
14.3.3 Reader for 13.56 MHz 435

References 441

Index 449

Preface to the Third Edition

This book is aimed at an extremely wide range of readers. First and foremost it is intended for engineers and students 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 each new edition of this book proves. 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 already appeared in five languages. Editions in two further languages are currently being prepared. 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, great importance is also assigned to providing an understanding of the basic concepts, data carrier and reader, as well as of the relevant standards and radio-technology regulations.

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. With the widespread use of RFID technology, it becomes also increasingly difficult not to lose track of applications. In ever-shorter intervals, the media provides information on new applications for RFID systems. 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.

A new addition to this third edition is Near-Field Communication (NFC) which has been introduced to several different chapters. Chapter 3 now includes the fundamentals of NFC; and Chapter 13 presents NFC interface components and describes the extension from NFC to secure-NFC.

Another addition is a complete wiring diagram and proposed circuit for an RFID reader according to ISO/IEC 14443. A layout and complete component kit of this wiring diagram and circuit is also available on the Internet.

It was a very special occasion when the Fraunhofer Smart Card Prize 2008 – which annually honors special contributions to smart-card technology - was awarded to the known smart-card

handbook of my two colleagues Rankl and Effing as well as to this RFID handbook. The prize-giving ceremony took place on the occasion of the 18th Smart-Card Workshop of the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt on 5 February 2008.

In March 2008, we were able to look back on ten successful years of the RFID Handbook. The first German-language edition was published in March 1998 and comprised 280 pages. At that time, RFID was still a niche technology and hardly known to the public; this has completely changed. Today, RFID has become an established term; and due to applications such as the electronic passport and electronic product code (EPC), a broad public has become aware of this technology.

At this point I would also like to express my thanks to all 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, Autumn 2008

List of Abbreviations

µP	Microprocessor
µs	Microsecond (10^{-6}s)
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
ASCII	American Standard Code for Information Interchange
ASIC	Application specific integrated circuit
ASK	Amplitude shift keying
ATQ	Answer to request (ATQA, ATQB: see ISO 14443-3)
ATR	Answer to reset
AVI	Automatic vehicle identification (for railways)
BAC	Basic access control (ePassport)
BAPT	Bundesamt für Post und Telekommunikation (now the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway)
Bd	Baud, transmission speed in bit/s
BGT	Block guard time
BKA	Germany's Federal Criminal Police Office
BMBF	Bundesministerium für Bildung und Forschung (Ministry for Education and Research, was BMFT)
BMI	German Federal Ministry of the Interior
BP	Bandpass filter
BSI	German Federal Office for Information Security
C	Capacitance (of a capacitor)
CCG	Centrale für Coorganisation GmbH (central allocation point for EAN codes in Germany)
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CEN	Comité Européen de Normalisation
CEPT	Conférence Européene des Postes et Télécommunications
CERP	Comité Européen de Règlementation Postale
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

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)
DoD	Department of Defense (USA)
DS	Discovery services (EPC)
DWD	German Weather Service
EAN	European Article Number (barcode on groceries and goods)
EAS	Electronic article surveillance
EC	Eurocheque or electronic cash
ECC	European Communications Committee
ECTRA	European Committee for Regulatory Telecommunications Affairs
EDI	Electronic document interchange
EEPROM	Electric erasable and programmable read-only memory
EIRP	Equivalent isotropic radiated power
EMC	Electromagnetic compatibility
EOF	End of frame
EPC	Electronic product code
EPCIS	EPC Information Services
ERC	European Radiocommunications Committee
ERM	Electromagnetic compatibility and radio spectrum matters
ERO	European Radiocommunications Office
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
GIAI	Global individual asset identifier (EPC)
GID	General identifier (EPC)
GRAI	Global returnable asset identifier (EPC)
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
ICAO	International Civil Aviation Organization
ICC	Integrated chip card
ID	Identification
ISM	Industrial scientific medical (frequency range)
ISO	International Organization for Standardization
ITU	International Telecommunication Union
L	Loop (inductance of a coil)
LAN	Local area network

LBT	Listen before talk
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
MRZ	Machine readable zone (ePassport)
MSB	Most significant bit
NAD	Node address
NFC	Near field communication
nomL	Nonpublic mobile land radio (industrial radio, transport companies, taxi radio, etc.)
NRZ	Non-return-to-zero encoding
NTC	Negative temperature coefficient (thermal resistor)
NTWC	New Technologies Working Group (ICAO)
NVB	Number of valid bits (see ISO 14443-3)
OCR	Optical character recognition
OEM	Original equipment manufacturer
ONS	Object naming server (EPC)
OTA	Over the air (possibility to program a SIM card or a secure element via the GPRS/UMTS interface of a mobile phone)
OTP	One time programmable
PC	Personal computer
PCD	Proximity card device (see ISO 14443)
PICC	Proximity integrated contactless chip card (see ISO 14443)
PIN	Personal identification number
PKI	Public key infrastructure
PMU	Power management unit
POS	Point of sale
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 and 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
SGLN	Serialised global location number (EPC)
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)
SSCC	Serial shipping container code (EPC)
TR	Technical Regulation
UART	Universal asynchronous receiver–transmitter (transmission/receiving module for computer interfaces)
UCC	Universal Code Council (American standard for barcodes on groceries and goods)
UHF	Ultra-high frequency (300 Mhz to 3 GHz)
UN	United Nations
UPC	Universal Product Code
UPU	Universal Postal Union
VCD	Vicinity card device (see ISO 15693)
VDE	Verein Deutscher Elektrotechniker (German Association of Electrical Engineers)
VHE	Very high frequency (30 MHz to 300 MHz)
VICC	Vicinity integrated contactless chip card (see ISO 15693)
VSWR	Voltage standing wave ratio
XOR	Exclusive OR
ZV	Zulassungsvorschrift (Licensing Regulation)

Trademarks

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 devices 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 pigeonholes. It brings together elements from extremely varied fields: RF 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).

RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition. Klaus Finkenzeller

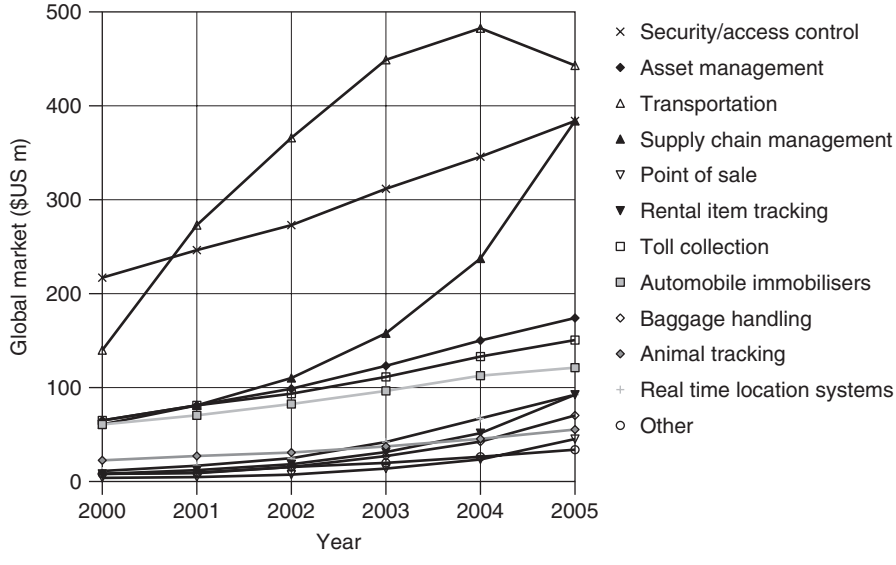

Figure 1.1 The estimated growth of the global market for RFID systems between 2000 and 2005 in million $US, classified by application (Krebs, n.d.)

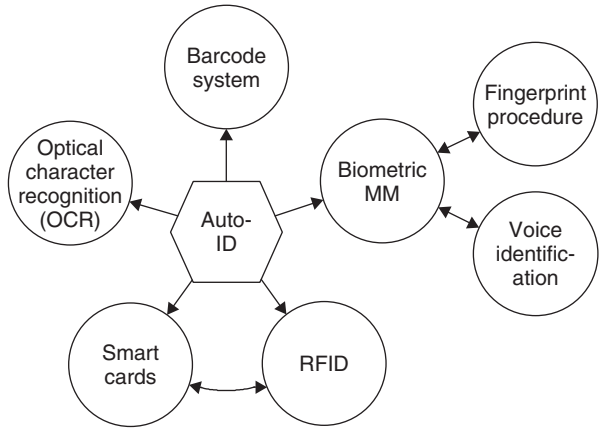

Figure 1.2 Overview of the most important auto-ID procedures

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).

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

Table 1.1 Common barcodes with typical applications

Code	Typical application
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

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.

In addition to the EAN code, the barcodes shown in Table 1.1 are popular in other industrial fields.

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 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).

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.

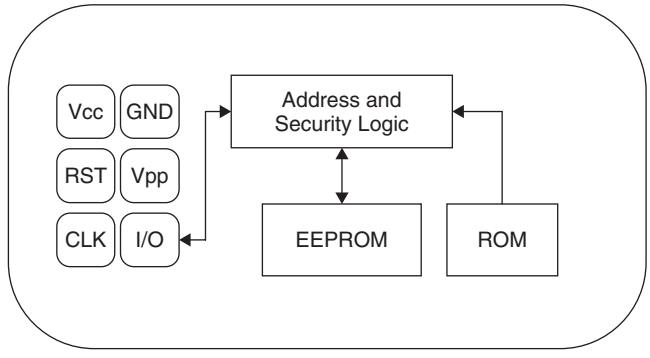

Figure 1.4 Typical architecture of a memory card with security logic

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

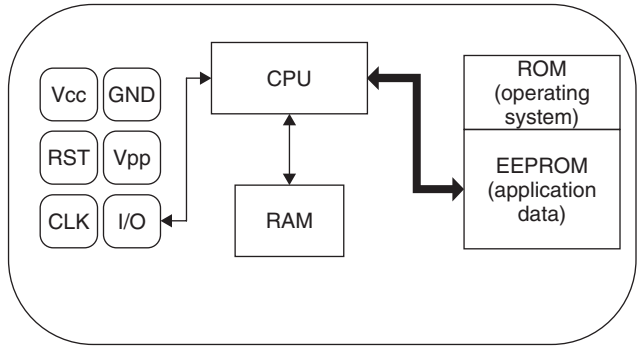

Figure 1.5 Typical architecture of a microprocessor card

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 program 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 program 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.

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 program 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 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 1.2). Here too, there is a close relationship between contact-based smart cards and RFID systems; however, the latter circumvent 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 1.6):

- 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).

Table 1.2 Comparison of different RFID systems showing their advantages and disadvantages

System parameters	Barcode	OCR	Voice recognition	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 (optical) 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.

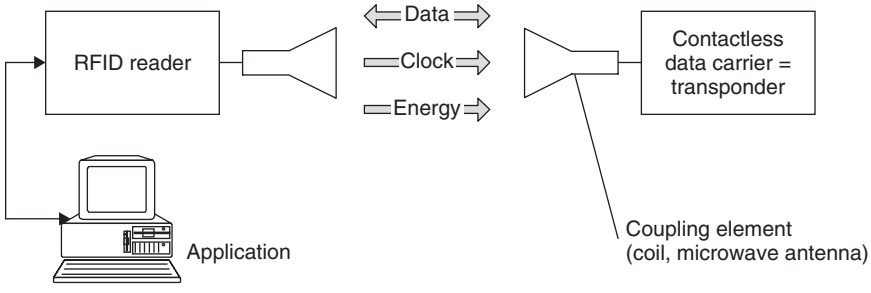

Figure 1.6 The reader and transponder are the main components of every RFID system

Figure 1.7 RFID reader and contactless smart card in practical use (reproduced by permission of Kaba Benzing GmbH)

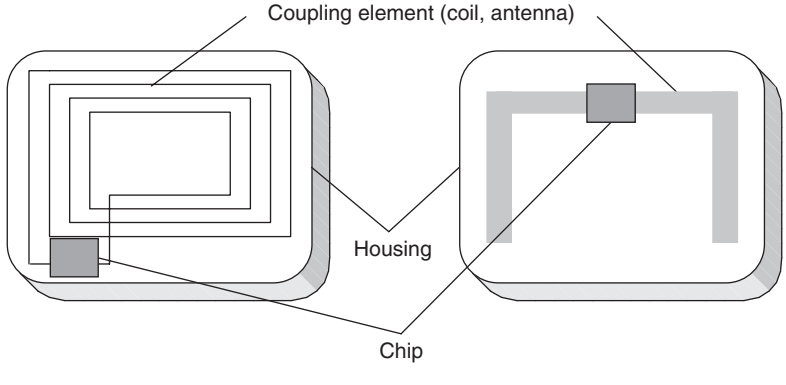

Figure 1.8 Basic layout of the RFID data-carrying device, the transponder. Left, inductively coupled transponder with antenna coil; right, microwave transponder with dipolar antenna

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*. 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.

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-duplex* 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, and 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.

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)

RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication, Third Edition. Klaus Finkenzeller

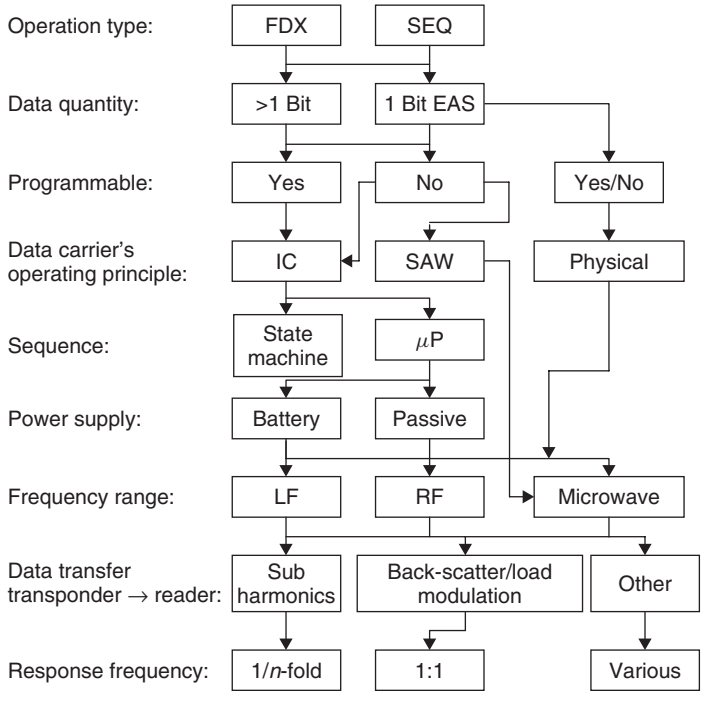

Figure 2.1 The various features of RFID systems (reproduced by permission of Integrated Silicon Design Pty, Ltd)

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 100 000–1000 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 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.