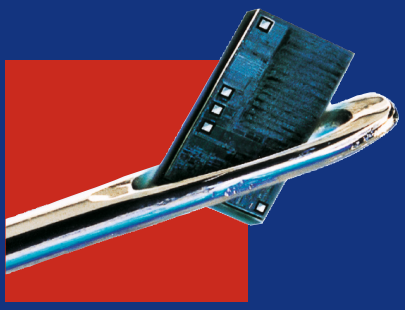
JUBILÄUM
25 Jahre
RFID-Handbuch

8. Auflage



Klaus FINKENZELLER

RFID HANDBUCH

Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC

»Hier bleibt keine technische Frage unbeantwortet.« c't

HANSER

Finkenzeller

RFID-Handbuch

Klaus Finkenzeller

RFID-Handbuch

Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC

unter Mitarbeit von Michael Gebhart, Florian Peters, Josef Preishuber-Pflügl, Peter Raggam, Erich Reisenhofer und Michael E. Wernle

8., aktualisierte Auflage

HANSER

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Brigitte Bauer-Schiewek
Copy editing: Petra Kienle, Fürstenfeldbruck
Schlusslayout: III-satz, Kiel
Coverkonzept: Marc Müller-Bremer, www.rebranding.de, München, unter Verwendung des Photos „MIFARE smartcard IC“ der Firma Philips Semiconductors, Gratkorn, Österreich
Coverrealisation: Max Kostopoulos
Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Gottingen
Printed in Germany

Print-ISBN: 978-3-446-44885-8
E-Book-ISBN: 978-3-446-47972-2

Inhaltsverzeichnis

Vorwort zur 8. Auflage

Dieses Buch richtet sich an die verschiedensten Leser. Zunächst an Ingenieure und Studenten, die zum ersten Mal mit der RFID-Technologie konfrontiert werden. Für sie gibt es einige grundlegende Kapitel über die Funktionsweise und die physikalischen sowie datentechnischen Grundlagen der RFID-Technik. Darüber hinaus richtet sich das Buch an den Praktiker, der sich als Anwender möglichst umfassend und konzentriert einen Überblick über die verschiedensten RFID-Technologien, die gesetzlichen Randbedingungen oder die Einsatzmöglichkeiten verschaffen möchte bzw. muss.

Zwar existiert eine schier unüberschaubare Fülle von Einzelbeiträgen in der Literatur zu diesem Themenbereich, aber alle diese „verteilten" Informationen im Bedarfsfalle zusammenzutragen, ist sehr mühsam und zeitaufwendig, wie auch die Recherchen zu jeder Auflage dieses Buchs aufs Neue beweisen. Dieses Buch soll daher auch eine Lücke im Literaturangebot über RFID-Systeme schließen. Wie groß der Bedarf an technisch fundierter Literatur in diesem Fachbereich tatsächlich ist, zeigt die erfreuliche Tatsache, dass das vorliegende Buch mittlerweile in sieben Sprachen[1] erschienen ist.

Anhand der vielen Bilder und Zeichnungen will dieses Buch eine im wahrsten Sinn des Wortes anschauliche Darstellung der RFID-Technologie geben. Einen besonderen Schwerpunkt stellen dabei die physikalischen Grundlagen dar, welche aus diesem Grunde auch das mit Abstand umfangreichste Kapitel bilden. Besonderer Wert wurde aber auch auf das Verständnis der grundlegenden Konzepte der Datenträger und Lesegeräte sowie der relevanten Normen und funktechnischen Regulierungsvorschriften gelegt. In den letzten Jahren rückt auch die Sicherheit von RFID-Systemen immer mehr in den Vordergrund. Angriffsmöglichkeiten und Abwehrmaßnahmen nehmen daher auch in diesem Buch einen immer größeren Platz ein.

Dieses Buch erschien zum ersten Mal im März 1998, also vor über 25 Jahren. Zum damaligen Zeitpunkt waren der RFID-Hype, den wir in den Jahren nach 2000 erlebt haben, aber auch die technologische Entwicklung auf dem Gebiet der RFID-Technologie in den folgenden 25 Jahren nicht ansatzweise absehbar. Mittlerweile ist die RFID-Technologie gut ausgereift und Innovationen finden sich vor allem in neuen Anwendungen oder einer Vernetzung der Lesegeräte und Transponder im Internet der Dinge. Erfreulich dabei ist es, dass die zugrunde liegenden Konzepte und physikalischen Grundlagen all diese Jahre erhalten geblieben und sind eine gute Voraussetzung für das Verständnis der neueren Entwicklungen waren und sind.

Ein ganz besonderes Ereignis war für mich die Verleihung des Fraunhofer Smart-Card-Preises 2008, der jährlich für besondere Verdienste in der Chipkartentechnologie vergeben wird und damals sowohl an das ebenso bekannte Chipkartenhandbuch meiner beiden Kollegen Rankl und Effing als auch an das RFID-Handbuch ging. Die Preisverleihung fand anlässlich

[1] Derzeit ist das Buch in folgenden Sprachen erhältlich: Deutsch, Englisch, Japanisch, Chinesisch, Koreanisch, Russisch und in chinesischer Langschrift (für Taiwan).

des 18. Smart-Card-Workshops des Fraunhofer Instituts für Sichere Informationstechnologien (SIT) am 5. Februar 2008 in Darmstadt statt. Zu diesem Zeitpunkt war das RFID-Handbuch bereits zehn Jahre erfolgreich etabliert.

Die 1998 in deutscher Sprache erschienene erste Auflage hatte einen Umfang von gerade mal 280 Seiten. War RFID damals noch eine Nischentechnologie und in der Öffentlichkeit kaum näher bekannt, so hat sich dieses Bild mittlerweile sehr gewandelt. RFID und das darauf basierende NFC sind zu einem festen Begriff geworden und durch Anwendungen wie den elektronischen Reisepass, den kontaktlosen Kredit- und EC-Karten oder den elektronischen Produktcode (EPC) sind RFID und NFC heute der breiten Öffentlichkeit als Technologien bekannt.

Auf Grund der komplexen Vielfalt der RFID-Systeme sowie der immer schnelleren technischen Weiterentwicklung dieser Systeme wurde es im Laufe der Jahre immer schwieriger, das Thema als Einzelautor in der notwendigen Tiefe zu bearbeiten. Um auch in Zukunft die RFID-Technologie möglichst umfassend und kompetent in einem Buch zusammenfassen zu können, wurde ab der 6. Auflage ein neuer Weg eingeschlagen. Einige der Kapitel wurden von Co-Autoren übernommen und über mehrere Auflagen weitergeführt. An der vorliegenden Auflage haben Michael E. Wernle (Meshed Systems, München) und Josef Preishuber-Pflügl (innobir e. U., Klagenfurt), aktiv mitgearbeitet.

An dieser Stelle möchte ich mich auch noch bei allen Firmen bedanken, die mit zahlreichen technischen Datenblättern, Vortragsmanuskripten, Zeichnungen und Fotografien zum Gelingen des Werkes beigetragen haben.

München, im Sommer 2023 *Klaus Finkenzeller*

Verwendete Abkürzungen

µP	Mikroprozessor
µs	Mikrosekunde (10^{-6} Sekunden)
ACM	Access Configuration Matrix
ABS	Acrylnitrilbutadienstyrol
AFC	Automatic Fare Collection
AFI	Application Family Identifier (siehe 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 (Amplitudentastung)
ATR	Answer to Reset
ATQ	Answer to Request (ATQA, ATQB: siehe ISO 14443-3)
AVI	Automatic Vehicle Identification (for Railways)
AWG	Arbitrary Waveform Generator (Arbiträrsignalgenerator)
BAC	Basic Access Control (ePass)
BAPT	Bundesamt für Post und Telekommunikation (jetzt Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen)
Bd	Baud, Übertragungsgeschwindigkeit in bit/s
BGT	Block Guard Time
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung (ehemals BMFT)
BMI	Bundesministerium des Inneren
BP	Bandpass(-filter)
BSI	Bundesamt für Sicherheit in der Informationstechnik
C	Capacity (Kapazität eines Kondensators)
CC	Country Code (Tieridentifikation)
CCG	Centrale für Coorganisation GmbH (Zentrale Vergabestelle für EAN-Codes in Deutschland)
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CEN	Comité Européen de Normalisation
CEPT	Conférence Européenne des Postes et Télécommunications
CERP	Comité Européen de Règlementation Postale
CICC	Close Coupling Integrated Circuit Chip Card
CIU	Contactless Interface Unit (Sende-/Empfangsbaustein für kontaktlose Mikroprozessorschnittstellen)

CLK	Clock (Taktsignal)
CRC	Cyclic Redundancy Checksum
DAC	Digital Analogue Converter (Digital Analog Wandler)
dBm	Logarithmisches Leistungsmaß, bezogen auf 1 mW HF-Leistung (0 dBm = 1 mW, 30 dBm = 1W)
DBP	Differential Bi-Phase encoding
DFT	Diskrete Fourier Transformation
DIN	Deutsche Industrienorm
DoD	Department of Defense (Verteidigungsministerium der USA)
DS	Discovery Services (EPC)
DUT	Device under Test (Prüfling, Prüfobjekt)
DWD	Deutscher Wetterdienst
EAN	European Article Number (Strichcode auf Lebensmitteln und Waren)
EAS	Electronic Article Surveillance (elektronische Diebstahlsicherung)
EC	Eurocheque bzw. 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
EMD	Electromagnetic Distortion
EMV	Elektro-Magnetische Verträglichkeit (engl. EMC)
EMV	Europay-MasterCard-Visa (Kreditkartenspezifikation)
EOF	End of Frame
EPC	Electronic Product Code (elektronische Produktkennzeichnung)
EPCIS	EPC Information Services
ERC	European Radiocommunications Committee
ERM	Electromagnetic Compatibility and Radio Spectrum Matters
ERO	European Radiocommunications Office
ERP	Equivalent Radiated Power (effektiv abgestrahlte Sendeleistung)
ESB	Ersatzschaltbild
ETCS	European Train Control System
ETS	European Telecommunication Standard
ETSI	European Telecommunication Standards Institute
EVC	European Vital Computer (Bestandteil der ETCS)
EVU	Energieversorgungsunternehmen
FCC	Federal Commission of Communication
FDX	Full-Duplex

FHSS	Frequency Hopping Spread Spectrum
FM	Frequenzmodulation
FRAM	Ferroelectric Random Access Memory
FSK	Frequency Shift Keying (Frequenzumtastung)
GIAI	Global Individual Asset Identifier (EPC)
GID	General Identifier (EPC)
GRAI	Global Returnable Asset Identifier (EPC)
GSM	Global System for Mobile Communication (ehem. Groupe Spécial Mobile)
GTAG	Global-Tag (RFID Initiative der EAN und des UCC)
HCE	Host Based Card Emulation (NFC)
HDX	Half-Duplex
HF	High Frequency (3 ... 30 MHz)
I2C	Inter-IC-Bus
ICAR	International Committee for Animal Recording
ICC	Integrated Chip Card
ICAO	International Civil Aviation Organization (internationale Zivilluftfahrtbehörde)
ID	Identifikation
ISM	Industrial Scientifical Medical (-Frequenzbereich)
ISO	International Standardization Organization
ITU	International Telecommunication Union (internationale Fernmeldeunion)
L	Loop (Induktivität einer Spule)
LAN	Local Area Network (Lokales Computer-Netzwerk)
LBT	Listen Before Talk
LF	Low Frequency (30 ... 300 kHz)
LLCP	Logical-Link-Control-Protokoll
LPD	Low Power Device (Funkanlage kleiner Leistung zur Übertragung von Daten oder Sprache über einige hundert Meter)
LRC	Longitudinal Redundancy Check
LSB	Least Significant Bit
MAD	MIFARE® Application Directory
MC	Manufacturer Code (Tieridentifikation)
MRZ	Machine readable zone (ePass)
MSB	Most Significant Bit
NAD	Node Address
NDEF	NFC Data Exchange Format
NFC	Near Field Communication

nömL	Nicht-öffentlicher mobiler Landfunk (Industriefunk, Transportunternehmen, Taxifunk etc.)
NRZ	Non-Return to Zero Encoding
NTC	Negative Temperature Coefficient (Heißleitender Widerstand)
NTWC	New Technologies Working Group (ICAO)
NVB	Number of valid bits (siehe ISO 14443-3)
OCR	Optical Character Recognition (Erkennung von Klarschrift)
OEM	Original Equipment Manufacturer
OFW	Oberflächenwellen
ONS	Object Naming Server (EPC)
ÖPNV	Öffentlicher Personennahverkehr
OSDP	Open Supervised Device Protocol
OSS	Open Security Standards
OSS-SO	OSS-Standard Offline
OTA	Over the Air (Möglichkeit zur Programmierung einer SIM-Karte oder eines Secure-Elements über die Datenschnittstellen GPRS/UMTS eines Mobiltelefons)
OTP	One Time Programmable
PC	Personal Computer
PCD	Proximity Card Device (siehe ISO 14443)
PIN	Personal Identification Number (Persönliche Geheimzahl)
PICC	Proximity Integrated Chip Card (siehe ISO 14443)
PKI	Public Key Infrastructure
PM	Phase Modulation (Phasenmodulation)
PMU	Power Management Unit
POS	Point of Sale
PP	Plasticpackage
PPS	Polyphenylensulfid
PSK	Phase Shift Keying
PUPI	Pseudo Unique PICC Identifier (siehe ISO 14443-3)
PVC	Polyvinylchlorid
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 (Rückstrahlquerschnitt, Rückstreuquerschnitt)
REQ	Request (REQA, siehe ISO/IEC 14443)
RFID	Radio Frequency Identification
RFU	Reserved for Future Use (Reserviert für zukünftige Anwendung)
RTC	Real Time Clock

RTD	Record Type Definition (NFC)
RTI	Returnable Trade Items
RTI	Road Transport Information System
RTTT	Road Transport & Traffic Telematics
RWD	Read Write Device (Schreib- und Lesestation)
SAM	Security Authentication Module
SCL	Serial Clock (I2C-Bus Interface)
SDA	Serial Data Address Input Output (I2C-Bus Interface)
SEQ	Sequentielles System
SGLN	Serialized Global Location Number (EPC)
SMD	Surface Mounted Devices
SNEP	Simple NDEF Exchange Protocol
SNR	Serial Number (Seriennummer) oder Signal Noise Ratio (Signal-Rausch-Abstand)
SOF	Start of Frame
SRAM	Static Random Access Memory
SRD	Short Range Devices (Funkanlagen kleiner Leistung zur Übertragung von Daten oder Sprache über kleine Entfernungen, in der Regel einige hundert Meter)
SSCC	Serial Shipping Container Code (EPC)
SWP	Single Wire Protocol (NFC)
TR	Technische Richtlinie (Technical Regulation)
UART	Universal Asynchronous Receiver Transmitter (Sende-/Empfangsbaustein für Computerschnittstellen)
UCC	Universal Code Council (Amerikanischer Standard für Strichcode auf Lebensmitteln und Waren)
UHF	Ultra High Frequency (300 MHz ... 3 GHz)
UN	United Nations (Vereinte Nationen)
UPC	Universal Product Code
UPU	Universal Postal Union
VCD	Vicinity Card Device (siehe ISO 15693)
VDE	Verein Deutscher Elektrotechniker
VHF	Very High Frequency (30 MHz ... 300 MHz)
VICC	Vicinity Integrated Contactless Chip Card (siehe ISO 15693)
VSWR	Voltage Standing Wave Ratio
XOR	eXclusive-OR (Exclusive-OR-Verknüpfung)
ZV	Zulassungsvorschrift

Warenzeichen

HITAG®, i•Code® und MIFARE®
sind eingetragene Warenzeichen von Philips Electronics N.V.

LEGIC® ist ein eingetragenes Warenzeichen von Kaba Security Locking Systems AG.

MICROLOG®
ist ein eingetragenes Warenzeichen von Idesco.

TagIt® und TIRIS®
sind eingetragene Warenzeichen von Texas Instruments.

TROVAN® ist ein eingetragenes Warenzeichen von Trovan, Ltd.

1 Einführung

In vielen Dienstleistungsbereichen, in der Beschaffungs- und Distributionslogik, im Handel, in Produktionsbetrieben und Materialflusssystemen haben automatische Identifikationsverfahren (Auto-ID) eine große Verbreitung gefunden. Aufgabe und Ziel der Auto-ID ist die Bereitstellung von Informationen zu Personen, Tieren, Gütern und Waren.

Die weit verbreiteten Barcode-Etiketten, die schon vor vielen Jahren eine Revolution bei Identifikationssystemen auslösten, sind heute in zunehmenden Fällen nicht mehr ausreichend. Zwar sind Barcodes äußerst billig, ihr Engpass ist jedoch die Unmöglichkeit der Umprogrammierung[2], sowie die notwendige Sichtverbindung zum Ablesen und die relativ geringe Lesegeschwindigkeit.

Eine technisch optimale Lösung ist die Speicherung der Daten in einem Siliziumchip. Aus dem täglichen Leben ist hierzu die Chipkarte mit Kontaktfeld (SIM-Karte, Bankenkarte) die bekannteste Bauform eines elektronischen Datenträgers. Die mechanische Kontaktierung wie bei der Chipkarte ist jedoch in vielen Fällen unzweckmäßig. Weitaus flexibler ist eine kontaktlose Übertragung der Daten zwischen dem Datenträger und einem zugehörigen Lesegerät. Idealerweise wird auch die zum Betrieb des elektronischen Datenträgers benötigte Energie durch das Lesegerät kontaktlos übertragen. Entsprechend den eingesetzten Energie- und Datenübertragungsverfahren werden kontaktlose ID-Systeme als *RFID-Systeme* (Radio Frequency Identification) bezeichnet.

Die Anzahl der Firmen, welche sich aktiv mit der Entwicklung und der Vermarktung von RFID-Systemen befassen, zeigt, dass sich die RFID-Technologie mittlerweile zu einem Milliarden schweren Markt entwickelt hat. Bis 2030 wird mit einem gesamten Marktvolumen zwischen 35 [penow] und über 40 Milliarden US$ [dhapte] gerechnet, worin Datenträger (Tags), Lesegeräte und Software enthalten sind.

Darüber hinaus hat sich die kontaktlose Identifikation in den letzten 35 Jahren zu einem eigenständigen interdisziplinären Fachgebiet entwickelt, das in keine der klassischen Schubladen mehr passt. Es fließen hier Elemente aus den verschiedensten Branchen zusammen: HF-Technik und EMV, Halbleitertechnik, Datenschutz und Kryptographie, Telekommunikation, Fertigungstechnik und viele verwandte Fachgebiete.

Zur Einführung gibt das folgende Kapitel einen Überblick über verschiedene Auto-ID-Systeme, die als verwandte oder benachbarte Systeme zur RFID angesehen werden können.

---

[2] Sofern die Barcodes auf Papier ausgedruckt werden. Mittlerweile werden Barcodes aber auch auf Displays oder Smartphones eingesetzt.

1.1 Automatische Identifikationssysteme

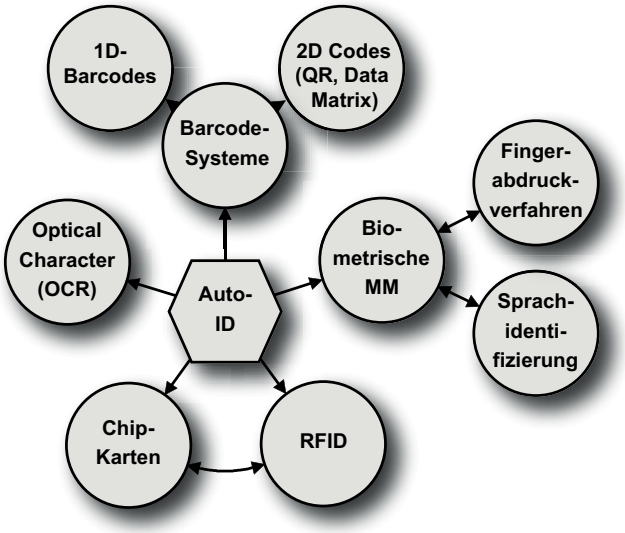


Abb. 1.1 Zusammenfassende Übersicht der wichtigsten Auto-ID-Verfahren.

1.1.1 Barcode-Systeme

Der *Barcode* (Strichcode) ist ein Binärcode aus einem Feld von parallel angeordneten Strichen (engl. bars) und Trennlücken. Diese sind nach einem vorbestimmten Bild angeordnet und stellen Elemente von Daten dar, die auf ein zugehöriges Zeichen verweisen. Die Sequenz aus breiten und schmalen Strichen bzw. Lücken kann numerisch oder alphanumerisch interpretiert werden. Die Ablesung geschieht durch optische Laserabtastung, d.h. durch die unterschiedliche Reflexion eines Laserstrahles an den schwarzen Strichen und weißen Lücken [ident 1].

Die Geschichte des Barcodes begann im Jahr 1948, als Norman Joseph Woodland und Bernhard Siver von einem Supermarktbetreiber erfuhren, der auf der Suche nach einem System zur automatischen Abfrage von Produktdaten für seine Kassen war. Vom Morsecode inspiriert, entwickelten die beiden US-Amerikaner einen Strichcode, auf den 1952 ein Patent erteilt wurde.

Trotz Weiterentwicklung der Technologie dauerte es bis in die 1970er-Jahre, als mit Ein-führung des *UPC* (Universal Product Code) der Durchbruch gelang. So wurde 1974 zum ersten Mal ein Artikel mit Hilfe der Barcode-Technologie an einer Supermarktkasse erfasst. Nur wenig später wurden 1976 mit dem EAN-Code auch in Europa Barcode-Systeme eingeführt.

Heute dürfte der mit Abstand am weitesten verbreitete Barcode eben dieser *EAN-Code* (European Article Number) sein. Der EAN-Code ist eine Weiterentwicklung des US-amerikanischen UPC , welcher heute eine Untermenge des EAN-Codes darstellt. Der UPC ist daher mit dem EAN-Code kompatibel [virnich]. Der EAN-Code ist international standardisiert

und verwendet Nummernkreise die international nur einmalig vergeben werden. Die ersten drei Ziffern stehen für das Land (400 bis 440 für Deutschland). Danach folgen eine Betriebsnummer (Unternehmensnummer) sowie 3 bis 5 Ziffern als Artikelnummer. Insgesamt werden 13 Ziffern dargestellt (EAN-13).

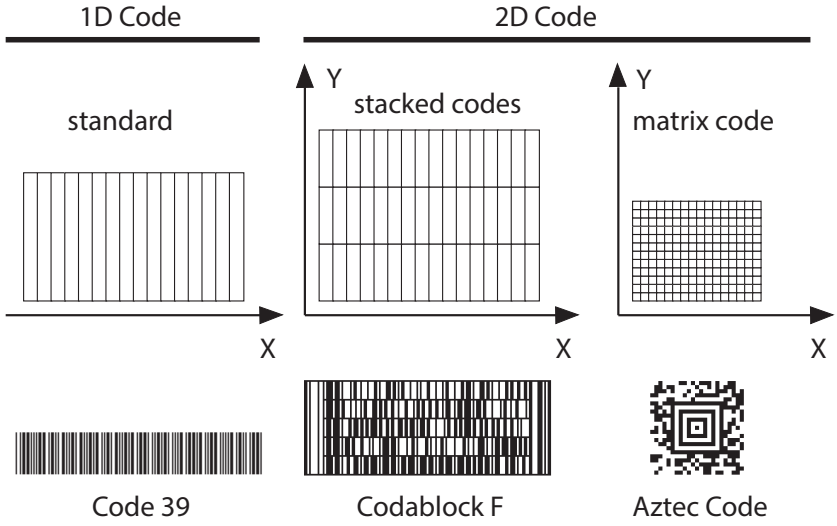


Abb. 1.2 Die Weiterentwicklung vom 1D- zum 2D-Barcode durch Einführung verschiedener Informationsebenen der optischen Darstellung. [logitogo]

Bereits in den 1980er-Jahren wurden die „klassischen" 1D-Barcodes zu einer flächigen Darstellung weiterentwickelt. Dies war die Entstehung der 2D-Barcodes. Deren ältester und bekanntester Vertreter ist der DataMatrix-Code, der seit Ende der 1980er-Jahre in vielen Bereichen eingesetzt wird. Mit dem DataMatrix-Code 144x144 ECC 200 lassen sich bis zu 1556 Bytes oder 2335 ASCII-Zeichen (bei 7 Bit pro Zeichen) kodieren.

Der QR-Code (Quick Response Code) wurde im Jahr 1994 von der Firma Denso Wave entwickelt, mit dem Ziel, Baugruppen und Komponenten eines Automobilkonzerns über die gesamte Logistik hinweg identifizieren zu können. Der QR-Code ist ein quadratischer Matrixcode mit drei Eckmarkierungen, der je nach Fehlerkorrektur-Level sogar noch bei einer Zerstörung von bis zu 30% vollständig gelesen werden kann.

Mit dem Aufkommen von Smartphones wurde es möglich, Barcodes mit der eingebauten Kamera zu fotografieren und mit einer geeigneten App auf dem Smartphone zu detektieren. Dadurch ist der QR-Code heute vor allem auch außerhalb der Produktionslogistik weit verbreitet und wird für verschiedenste Einsatzbereiche genutzt. Viele Plakate, Anzeigen, Poster und sogar Visitenkarten werden mit QR-Codes versehen, die Text enthalten oder auf eine Website verweisen. Umgekehrt kann der QR-Code aber auch auf dem Display eines Smartphones mit hohem Kontrast dargestellt werden. Dies wird bereits seit einiger Zeit von Fluggesellschaften eingesetzt, um Boardkarten auf Smartphones zu übertragen.

Mit dem QR-Code (177x177 Elemente, Fehlerkorrekturlevel „L") lassen sich bis zu 2953 Byte oder 4296 ASCII-Zeichen (bei 7 Bit pro Zeichen) kodieren.

Die Entwicklung der Barcodes ist dabei keineswegs abgeschlossen. So wurde von Microsoft mit dem HCCB (High Capacity Color Barcode) ein 3D-Barcode entwickelt. Durch den Einsatz verschiedener Farben kann der HCCB gegenüber dem klassischen 2D-Barcode in etwa die doppelte Datenmenge auf gleichem Raum darstellen. Mit der Darstellung zeitlich veränderlicher Barcodes auf einem Display wurde mittlerweile sogar die Epoche der 4D-Barcodes eingeläutet. Auch der Einsatz von Smartphones als Barcode-Lesegerät oder -Display wird, zusammen mit ihrer Vernetzung im Internet, sicher noch die eine oder andere sehr interessante Anwendungsmöglichkeit von Barcodes hervorbringen.

Abb. 1.3 Verschiedene Beispiele für 1D- und 2D-Barcodes.

Barcode-Systeme konkurrieren unmittelbar mit den RFID-Systemen. Häufig werden RFID-Systeme auch als elektronischer Barcode bezeichnet, was aber weder den Barcode- noch den RFID-Systemen ganz gerecht wird, da die beiden Systeme auf unterschiedlichen physikalischen Prinzipien beruhen und daher unterschiedliche Vor- und Nachteile aufweisen.

1.1.2 Optical Character Recognition

Der Einsatz von *Klarschriftlesern* (optical character recognition = OCR) begann schon in den 1960er-Jahren. Hierfür wurden spezielle Schrifttypen entwickelt, die durch ihre Stilisierung nicht nur von Menschen, sondern auch automatisch von Maschinen gelesen werden können. OCR-A wurde 1968 als erste optisch maschinenlesbare Schrift entwickelt und ist nach ANSI INCITS 17-1981 spezifiziert. Bereits wenige Jahre später wurde von Adrian Frutiger die Schrift OCR-B entwickelt und in ISO 1073-2 weltweit standardisiert.

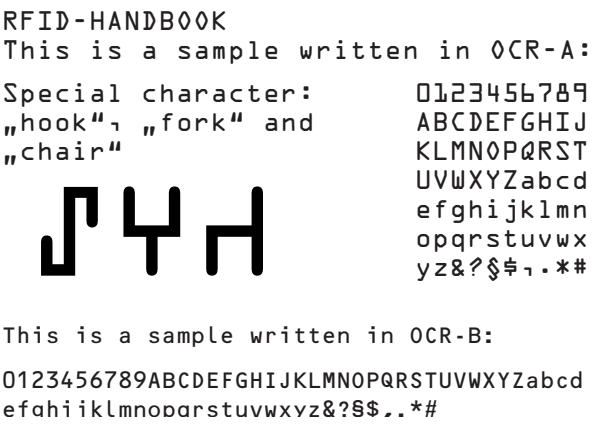


Abb. 1.4 Beispiel für die OCR-Schriften OCR-A und OCR-B.

Die wichtigsten Vorteile der *OCR-Systeme* sind die hohe Informationsdichte sowie die Möglichkeit, im Notfall (oder einfach zur Kontrolle) die Daten auch visuell erfassen zu können [virnich]. OCR-Schriften werden vor allem für Formulare und andere Dokumente verwendet, die maschinell erfasst werden sollen. Die Einsatzgebiete für OCR sind heute in der Produktion, in Dienstleistungs- und Verwaltungsbereichen sowie bei Banken, zur Registrierung von Schecks[3] und von Kreditkarten (siehe auch Abbildung 1.6 auf Seite 7). Die flächendeckende Verbreitung von OCR-Systemen wird jedoch durch die im Vergleich zu anderen ID-Verfahren komplizierten Lesegeräte behindert.

1.1.3 Biometrische Verfahren

Biometrie ist laut Duden-Fremdwörterbuch „die Wissenschaft von der Zählung und (Körper-)Messung an Lebewesen“. Im Zusammenhang mit Identifikationssystemen ist Biometrie der Oberbegriff für alle Verfahren, die Personen durch den Vergleich von unverwechselbaren und individuellen Körpermerkmalen identifizieren. In der Praxis sind dies Fingerabdruck- und Handabdruckverfahren, Sprachidentifizierung und seltener die Augen-Netzhaut- (bzw. auch Iris-) Identifizierung.

1.1.3.1 Sprachidentifizierung

Zur Identifikation einzelner Personen werden in neuerer Zeit spezielle Systeme zur Sprecherverifikation (Sprechererkennung) angeboten. Hierbei spricht der Benutzer in ein Mikrofon, das mit einem Computer verbunden ist. Dieser wandelt die gesprochenen Worte in digitale Signale um, die von der Identifizierungs-Software ausgewertet werden.

Ziel der Sprecherverifikation ist es, die angebliche Identität einer Person anhand ihrer Stimme zu überprüfen. Dabei werden die Sprachmerkmale der sprechenden Person mit einem

[3] In der untersten Zeile von Schecks findet man persönliche Daten (Name, Kontonummer) als OCR-Schrift aufgedruckt.

vorliegenden Referenzmuster überprüft. Bei Übereinstimmung kann dann eine Reaktion ausgelöst werden (z. B. „Tür öffnen“).

1.1.3.2 Fingerabdruckverfahren (Daktyloskopie)

In der Kriminalistik ging man bei der Identifizierung von Straftätern bereits um die vorige Jahrhundertwende zu Fingerabdruckverfahren über. Hierbei geht es um den Vergleich der Papillaren und Hautleisten der Fingerspitzen bzw. Fingerkuppen, die man nicht nur vom Finger selbst, sondern auch von berührten Gegenständen abnehmen kann.

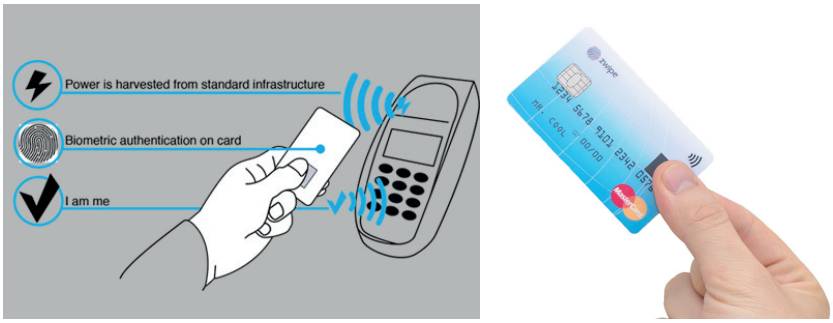


Abb. 1.5 Beispiel für eine kontaktlose Kreditkarte mit integriertem Fingerprintsensor, die Zwipe Mastercard. [zwipe2014] (Grafik und Foto: Zwipe AS Norway)

Bei der Personenidentifikation mittels Fingerabdruckverfahren, meist für eine Zutrittskontrolle, wird die Fingerkuppe auf ein spezielles Lesegerät gelegt. Das System berechnet aus dem eingelesenen Muster einen Datensatz und vergleicht diesen mit einem gespeicherten Referenzmuster. Moderne Fingerabdruck-ID-Systeme benötigen weniger als eine halbe Sekunde zur Erkennung und Prüfung eines Fingerabdrucks. Um gewalttätigen Betrugsversuchen vorzubeugen, wurden sogar Fingerabdruck-ID-Systeme entwickelt, welche erkennen können, ob ein lebender Finger vorgelegt wird [schmidhäusler].

Die fortschreitende Entwicklung in der Halbleitertechnologie ermöglicht heute sogar ein Zusammenwachsen von Fingerabdruck- und RFID-Technologien. Eine kontaktlose Kreditkarte mit eingebautem Fingerabdruck-Scanner soll Kartenzahlungen bequemer und unabhängig von einer PIN-Eingabe oder einer Unterschrift machen. Die Fingerabdruckdaten des Karteninhabers werden auf der Karte selbst sicher gespeichert. Vor der ersten Zahlung wird hierzu vom Karteninhaber ein Referenzscan erstellt. Anschließend lassen sich Zahlungen einfach betätigen, indem der Daumen auf den Sensor gehalten wird, während die Karte in einigen Zentimetern Abstand an ein kontaktloses Terminal geführt wird. Die vom Terminal übertragene Energie reicht dabei auch aus, um den Sensor mit Energie zu versorgen, so dass keine Batterie in der Karte benötigt wird [zwipe2014].

1.1.4 Chipkarten

Als *Chipkarte* bezeichnet man einen elektronischen Datenspeicher, gegebenenfalls mit zusätzlicher Rechnerleistung (Mikroprozessorkarte), welcher – der besseren Handhabung we-

gen – in eine Plastikkarte im Kreditkartenformat eingebaut ist. Erste Chipkarten wurden in Europa bereits um 1984 als vorbezahlte Telefonchipkarten eingesetzt. Zum Betrieb werden Chipkarten in ein Lesegerät eingesteckt, das mit Kontaktfedern eine galvanische Verbindung zu den Kontaktflächen der Chipkarte herstellt. Über die Kontaktflächen wird die Chipkarte aus dem Lesegerät mit Energie und einem Takt versorgt. Die Datenübertragung zwischen dem Lesegerät und der Karte wird auf einer bidirektionalen seriellen Schnittstelle (I/O-Port) abgewickelt. Nach dem Innenleben der Chipkarten unterscheidet man zwischen zwei Grundtypen: Speicherkarte und Mikroprozessorkarte.

Abb. 1.6 Vorderseite einer Kreditkarte im ID-1-Format, mit Chip. (Foto: Giesecke & Devrient, München)

Die mechanischen Abmessungen einer Chipkarte sind in ISO/IEC 7816 standardisiert. Die beiden wichtigsten Bauformen sind dabei ID-1 und ID-000. ID-1 ist mit 85,60 mm x 53,98 mm das größte Format und wird bei allen Banken- und Kreditkarten, dem EU-Führerschein oder den Krankenversicherungskarten eingesetzt. ID-000, das mit 25 mm x 15 mm kleinste der ISO-Formate, kommt überwiegend bei SIM-Karten zum Einsatz. Die Dicke der Karten ist für alle Größen einheitlich und beträgt 0,762 mm (0,03 Zoll).

Einer der wichtigsten Vorteile der Chipkarte liegt darin, dass die in ihr gespeicherten Daten gegen unerwünschten (Lese-) Zugriff und Manipulation geschützt werden können. Chipkarten machen fast alle Dienstleistungen, die mit Informations- oder Geldtransaktionen verbunden sind, einfacher, sicherer und billiger.

Im Jahre 1992 wurden weltweit 200 Millionen Chipkarten ausgegeben (davon 20% alleine in Deutschland!). 20 Jahre später, 2012, wurde die unvorstellbare Menge von knapp 7 Milliarden Chipkarten weltweit verkauft.

Ein Nachteil der kontaktbehafteten Chipkarten ist die Anfälligkeit der Kontakte für Abnutzung, Korrosion und Verschmutzung. Vor allem häufig benutzte Lesegeräte verursachen hohe Kosten durch Ausfall. Zudem können frei zugängliche Lesegeräte (Fahrkartenautomaten) nicht gegen Sabotage geschützt werden. Seit dem Jahr 2000 werden daher zunehmend Chipkarten in den Markt gebracht, die neben den Kontakten zusätzlich über ein kontaktloses RFID-Interface verfügen (siehe dazu Kapitel 10.2.1 „Dual-Interface Karte“, S. 481). Werden die Kontakte vollständig weggelassen, ergibt sich eine kontaktlose Chipkarte und damit ein RFID-Transponder.

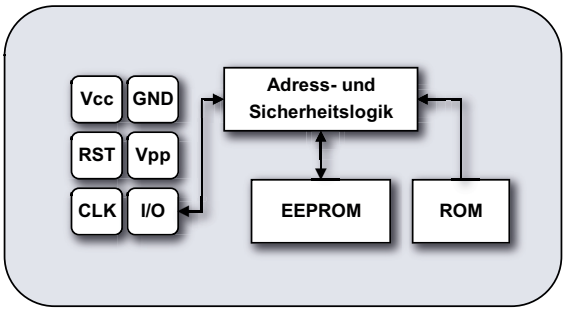


Abb. 1.7 Typische Architektur einer Speicherkarte mit Sicherheitslogik.

1.1.4.1 Speicherkarten

Bei *Speicherkarten* wird über eine sequenzielle Logik (State-Machine) auf den Speicher – meist ein EEPROM – zugegriffen. Hierbei sind auch einfache Sicherheitsalgorithmen, z. B. Stromverschlüsselung (Streamcipher) realisierbar. Die Funktionalität von Speicherkarten ist meist auf eine sehr spezielle Anwendung optimiert. Die Flexibilität der Anwendung ist hierfür zwar stark eingeschränkt, dafür sind Speicherkarten jedoch besonders preisgünstig. Speicherkarten werden deshalb vor allem in preissensitiven Massenanwendungen eingesetzt [rankl].

Beispiele für Speicherkarten sind die vorbezahlten (Debit-)Telefonchipkarten für öffentliche Fernsprecher, die in Europa in den 1990er-Jahren sehr verbreitet waren, sowie die Versichertenkarte der gesetzlichen Krankenkassen in Deutschland [lemme], die erst 2011 durch eine Mikroprozessorkarte abgelöst wurde.

1.1.4.2 Mikroprozessorkarten

Mikroprozessorkarten enthalten – wie schon die Bezeichnung zum Ausdruck bringt – einen Mikroprozessor, der mit einem segmentierten Speicher (ROM-, RAM- und EEPROM-Segment) verbunden ist.

Das maskenprogrammierte ROM enthält ein *Betriebssystem* (übergeordneter Programmcode) für den Mikroprozessor und wird während der Chipfabrikation aufgebracht. Der Inhalt des ROM ist herstellungsbedingt für alle Mikrochips des gleichen Produktionsloses identisch und kann auch nicht mehr überschrieben werden.

Im EEPROM des Chips befinden sich Applikationsdaten und applikationsspezifischer Programmcode. Dieser Speicherbereich kann jedoch nur unter Kontrolle des Betriebssystems beschrieben oder gelesen werden.

Das RAM ist der temporäre Arbeitsspeicher des Mikroprozessors. Die gespeicherten Daten gehen nach Abschalten der Versorgungsspannung verloren.

Mikroprozessorkarten sind sehr flexibel. Moderne Chipkartenbetriebssysteme ermöglichen es auch, unterschiedliche Anwendungen in einer einzigen Karte zu integrieren (Multiappli-

kation). Die applikationsspezifischen Programmteile werden dazu erst nach der Kartenproduktion in das EEPROM geladen und können über das Betriebssystem gestartet werden.

Mikroprozessorkarten werden vor allem in sicherheitssensitiven Anwendungen eingesetzt. Ein Beispiel hierfür sind die SIM-Karten für GSM-Handys oder die von Banken ausgegebenen EC-Karten (electronic cash). Die Programmiermöglichkeit der Mikroprozessorkarten ermöglicht außerdem die schnelle Anpassung an neue Applikationen [rankl].

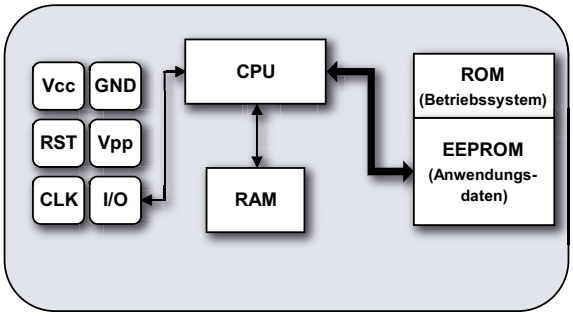


Abb. 1.8 Typische Architektur einer Mikroprozessorkarte.

1.1.5 RFID-Systeme

RFID-Systeme sind den oben beschriebenen Chipkarten eng verwandt. Auch hier werden die Daten auf einem elektronischen Datenträger – dem Transponder – gespeichert. Die Energieversorgung des Datenträgers sowie der Datenaustausch zwischen Datenträger und Lesegerät erfolgen jedoch nicht durch galvanisches Kontaktieren, sondern unter Verwendung magnetischer oder elektromagnetischer Felder. Die technischen Verfahren hierzu wurden aus der Funk- und Radartechnik übernommen. Die Bezeichnung RFID steht deshalb für Radio-Frequency-Identification, also Identifikation durch Radiowellen.

Aufgrund zahlreicher Vorteile der RFID-Systeme gegenüber den anderen Identifikationssystemen erobern RFID-Systeme zunehmend neue Massenmärkte. Beispiele hierfür sind der Einsatz kontaktloser Chipkarten als Ticket für den öffentlichen Nahverkehr, Kreditkarten mit kontaktlosem Interface oder der Einsatz von RFID in der Waren- und Güterlogistik.

1.2 Vergleich verschiedener ID-Systeme

Ein Vergleich (siehe Tabelle 1.1 auf Seite 10) zwischen den oben aufgeführten Identifikationssystemen zeigt die Schwächen und Stärken von RFID zu anderen Systemen. Auch hier zeigt sich die enge Verwandtschaft zwischen kontaktbehafteter Chipkarte und RFID-Syste-

men, doch werden bei Letzteren alle Nachteile im Zusammenhang mit der störanfälligen Kontaktierung (Sabotage, Verschmutzung, nur eine Steckrichtung, zeitaufwendiges Einstecken usw.) vermieden.

Tabelle 1.1: Der Vergleich verschiedener RFID-Systeme zeigt deren Vor- und Nachteile.

Parameter	1D-/2D-Barcode	OCR	Sprecher-erkennung	Biometrie	Chipkarte	RFID-Systeme
Typische Datenmenge/Byte:	1 ~ 100 10~5k	1 ~ 100	–	–	16 ~ 512k	16 ~ 512k
Datendichte	mittel	gering	hoch	hoch	sehr hoch	sehr hoch
Maschinenlesbarkeit	gut	gut	aufwendig	aufwendig	gut	gut
Lesbarkeit durch Personen	bedingt	einfach	einfach	schwer	unmöglich	unmöglich
Einfluss von Schmutz/Nässe	stark	sehr stark	–	–	möglich (Kontakte)	kein Einfluss
Einfluss von (opt.) Abdeckung	totaler Ausfall	totaler Ausfall	–	möglich	–	kein Einfluss
Einfluss von Richtung und Lage	gering	gering	–	–	eine Steckrichtung	kein Einfluss
Abnutzung, Verschleiß	bedingt	bedingt	–	–	Kontakte	kein Einfluss
Anschaffungs-kosten Elektronik	sehr gering	mittel	sehr hoch	sehr hoch	gering	mittel
Betriebskosten (z. B. Drucker)	sehr gering	gering	keine	keine	mittel (Kontakte)	keine
unbefugtes Kopieren/Ändern	leicht	leicht	möglich[a] (Tonband)	unmöglich	unmöglich	unmöglich
Lesegeschwindigkeit (incl. Handhabung des Datenträgers)	gering ~ 4 s	gering ~ 3 s	sehr gering > 5 s	sehr gering > 5 ... 10 s	gering ~ 4 s	sehr schnell ~ 0,5 s
Maximale Entfernung zwischen Datenträger und Lesegerät	0 ... 50 cm	< 1 cm (Scanner)	0 ... 50 cm	direkter Kontakt[b]	direkter Kontakt	HF: 0 ... 1 m, UHF: 0 ... 12 m

[a] Die Gefahr des „Replay“ kann durch Auswahl eines zu sprechenden Textes mit einem Zufallsgenerator verringert werden, da nicht mehr im Voraus bekannt ist, welcher Text gesprochen werden muss.

[b] Dies gilt nur für Fingerabdruck-ID. Bei Augen-Netzhaut- oder Iris-Auswertung ist ein direkter Kontakt nicht nötig bzw. möglich.

1.3 Bestandteile eines RFID-Systems

Ein *RFID-System* besteht immer aus zwei Komponenten:

- dem *Transponder*, der an den zu identifizierenden Objekten angebracht wird;
- dem Erfassungs- oder *Lesegerät*[4], das je nach Ausführung und eingesetzter Technologie als Lese- oder Schreib/Lese-Einheit erhältlich ist.

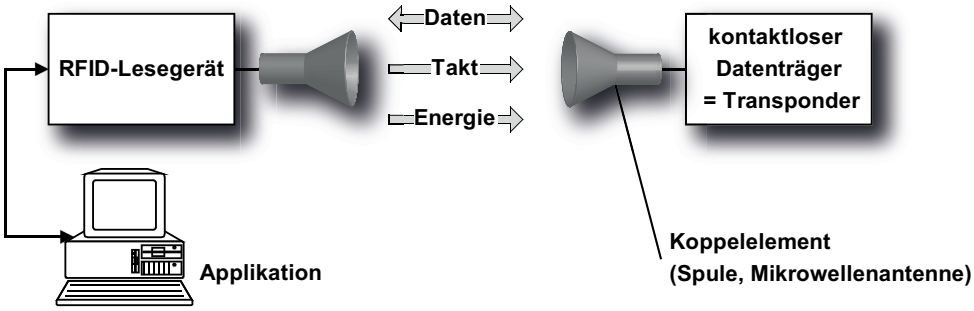


Abb. 1.9 Lesegerät und Transponder sind die Grundbestandteile jedes RFID-Systems.

Ein Lesegerät beinhaltet typischerweise ein Hochfrequenzmodul (Sender und Empfänger), eine Kontrolleinheit sowie ein Koppelelement (Antenne) zum Transponder. Daneben sind viele Lesegeräte mit einer zusätzlichen Schnittstelle (USB, LAN, RS 232, ...) ausgestattet, um die erhaltenen Daten an ein anderes System (PC, Automatensteuerung, ...) weiterzuleiten.

Der Transponder, der den eigentlichen *Datenträger* eines RFID-Systems darstellt, besteht üblicherweise aus einem *Koppelelement* sowie einem elektronischen *Mikrochip*. Außerhalb des Ansprechbereichs eines Lesegeräts verhält sich der Transponder, der in der Regel keine eigene Spannungsversorgung (Batterie) besitzt, vollkommen passiv. Erst innerhalb des Ansprechbereichs eines Lesegeräts wird der Transponder aktiviert. Die zum Betrieb des Transponders benötigte Energie wird ebenso wie Takt und Daten durch die Koppeleinheit (kontaktlos) zum Transponder übertragen.

[4] In diesem Buch wird das Erfassungsgerät – der üblichen umgangssprachlichen Verwendung entsprechend – immer als Lesegerät bezeichnet, unabhängig davon, ob Daten damit nur gelesen oder auch geschrieben werden.

Abb. 1.10 Beispiel für ein RFID-Lesegerät mit kontaktlosem Datenträger (Transponder), im praktischen Einsatz in einem Zutrittskontrollsystem.
(Foto: primion ADR Zutrittskontrollleser, primion Technology GmbH, Stetten a.k.M.)

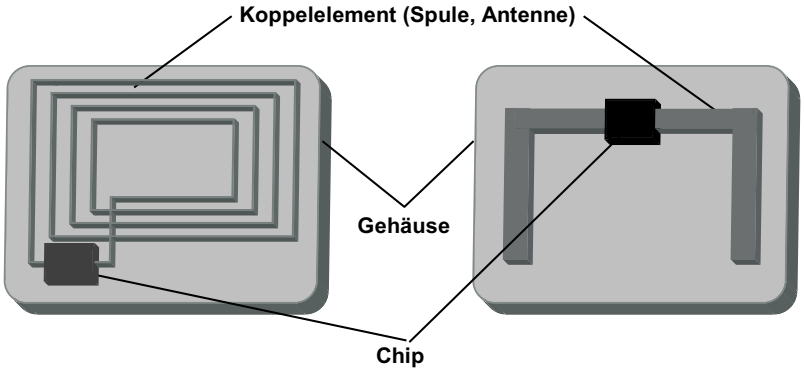


Abb. 1.11 Prinzipieller Aufbau des RFID-Datenträgers, des Transponders. *Links*: induktiv gekoppelter Transponder mit Antennenspule, *rechts*: Mikrowellen-Transponder mit Dipolantenne.

2 Unterscheidungsmerkmale von RFID-Systemen

2.1 Grundsätzliche Unterscheidungsmerkmale

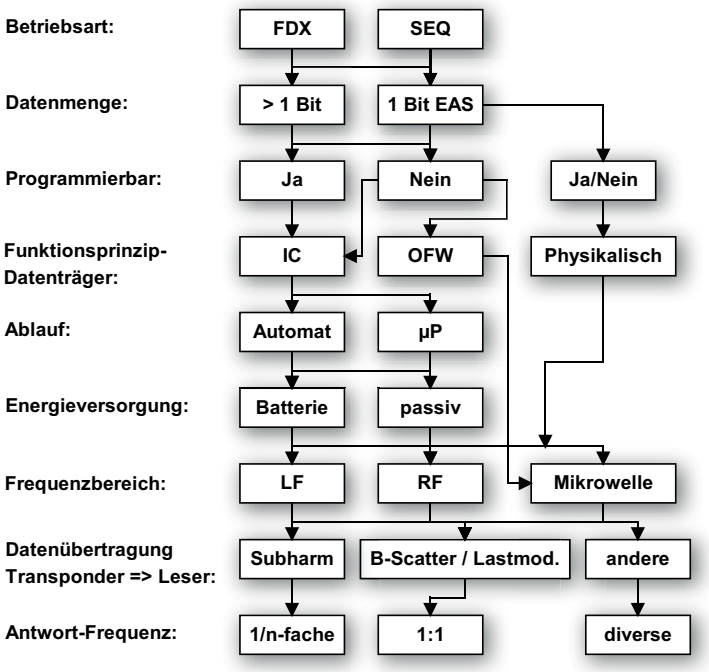


Abb. 2.1 Verschiedene Unterscheidungsmerkmale von RFID-Systemen. [isd]

RFID-Systeme existieren in unzähligen Varianten, von fast ebenso vielen verschiedenen Herstellern. Um den Überblick über RFID-Systeme zu behalten, ist es notwendig, Unterscheidungsmerkmale zu finden, nach denen verschiedenste RFID-Systeme voneinander unterschieden werden können.

Bei der Betriebsart von RFID-Systemen sind zwei grundsätzliche Verfahren zu unterscheiden: Voll- (full-duplex, FDX) und Halbduplex-Systeme (half-duplex, HDX) sowie sequentielle Systeme (SEQ).

Beim *Voll-* und *Halbduplexverfahren* wird die Antwort des Transponders bei eingeschaltetem HF-Feld des Lesegeräts übertragen. Da das Signal des Transponders an der Empfangsantenne, verglichen mit dem Signal des Lesegeräts selbst, extrem schwach sein kann, müssen geeignete Übertragungsverfahren angewendet werden, um die Signale des Transponders von denen des Lesegeräts zu unterscheiden. In der Praxis verwendet man zur Datenübertragung vom Transponder zum Lesegerät Lastmodulation, Lastmodulation mit Hilfsträger, aber auch (Sub-)Harmonische der Sendefrequenz des Lesegeräts.

Bei *sequentiellen Verfahren* hingegen wird das Feld des Lesegeräts periodisch für kurze Zeit abgeschaltet. Diese Lücken werden vom Transponder erkannt und zur Datenübertragung vom Transponder zum Lesegerät benutzt. Nachteil des sequentiellen Verfahrens ist der Ausfall der Energieversorgung des Transponders während der Sendepausen des Lesegeräts, was durch den Einbau ausreichender Stützkondensatoren oder Stützbatterien ausgeglichen werden muss.

Die Datenmenge von RFID-Transpondern reicht üblicherweise von wenigen Bytes bis zu mehreren KBytes. Eine Ausnahme stellen die sogenannten 1-bit-Transponder dar: Eine Datenmenge von genau 1 Bit reicht gerade dazu aus, um dem Lesegerät zwei Zustände zu signalisieren: „Transponder im Feld“ oder „kein Transponder im Feld“. Dies ist jedoch vollkommen ausreichend, um einfache Überwachungs- oder Signalisierungsaufgaben zu erfüllen. Da zur Realisierung eines 1-bit-Transponders kein elektronischer Chip benötigt wird, können diese Transponder für Bruchteile eines Cents hergestellt werden. Aus diesem Grunde werden 1-bit-Transponder in großen Stückzahlen zur *Diebstahlsicherung* (EAS) von Waren in Kaufhäusern und Geschäften eingesetzt. Beim Verlassen des Kaufhauses mit unbezahlter Ware wird das am Ausgang installierte Lesegerät dann den Zustand „Transponder im Feld“ erkennen und entsprechende Reaktionen auslösen. Bei einer ordnungsgemäß bezahlten Ware würde der 1-bit-Transponder an der Kasse entfernt oder deaktiviert werden.

Eine weitere Unterscheidungsmöglichkeit von RFID-Systemen ist die Beschreibbarkeit des Transponders mit Daten. Bei sehr einfachen Systemen wird der Datensatz des Transponders, meist eine einfache (Serien-) Nummer, schon zum Zeitpunkt der Chipherstellung aufgebracht und kann dann nicht mehr verändert werden. Im Gegensatz dazu können beschreibbare Transponder durch das Lesegerät mit Daten beschrieben werden. Zur Speicherung der Daten werden vor allem drei Verfahren eingesetzt: Bei induktiv gekoppelten RFID-Systemen sind EEPROMs (electrically erasable programmable read only memory) das dominierende Verfahren, jedoch mit dem Nachteil einer hohen Leistungsaufnahme während des Schreibvorgangs sowie einer Lebensdauer von maximal 100.000 Schreibvorgängen. In jüngster Zeit werden vereinzelt auch sogenannte FRAMs (ferromagnetic random access memory) eingesetzt. Im Vergleich zu EEPROMs ist die Leistungsaufnahme zum Beschreiben von FRAMs etwa um den Faktor 100, die Schreibzeit sogar um den Faktor 1000 geringer. Probleme in der Herstellung der FRAMs haben deren breite Markteinführung bisher jedoch verhindert.

Vor allem bei den Mikrowellen-Systemen werden auch Statische RAMs (static random access memory, SRAM) zur Datenspeicherung eingesetzt, welche sehr schnelle Schreibzyklen ermöglichen. Zum Datenerhalt wird jedoch eine unterbrechungsfreie Spannungsversorgung aus einer Stützbatterie benötigt.

Bei den programmierbaren Systemen müssen der Schreib- und Lesezugriff auf den Speicher sowie die eventuelle Abfrage einer Schreib- und Leseberechtigung durch eine „innere Logik“ des Datenträgers gesteuert werden. Im einfachsten Falle kann dies durch einen Zustandsautomaten realisiert werden (Weiteres dazu in Kapitel 10 „Architektur elektronischer Datenträger“, S. 457). Mit *Zustandsautomaten* können durchaus sehr komplexe Abläufe re-

alisiert werden. Der Nachteil von Zustandsautomaten ist jedoch die Inflexibilität gegenüber Änderungen der programmierten Funktionen, da hierzu Schaltungsänderungen auf dem Siliziumchip nötig sind. Dies bedeutet in der Praxis eine kostspielige Neuentwicklung des Chiplayouts.

Eine wesentliche Verbesserung ergibt sich durch die Verwendung eines Mikroprozessors. Ein eigenes Betriebssystem zur Verwaltung der Applikationsdaten wird bei der Chipherstellung durch eine Maske in den Prozessor gebracht. Änderungen lassen sich auf diese Weise kostengünstig einbringen, außerdem kann die Software an unterschiedlichste Applikationen spezifisch angepasst werden. Im Zusammenhang mit kontaktlosen Chipkarten spricht man bei beschreibbaren Datenträgern mit Zustandsautomaten auch von „Speicherkarten“, im Gegensatz zu „Prozessorkarten“.

In diesem Zusammenhang müssen auch Transponder erwähnt werden, die Daten aufgrund physikalischer Effekte speichern können. Hierunter fallen die Read-only-Oberflächenwellen-Transponder sowie 1-bit-Transponder, die meist deaktiviert („Beschreiben“ mit „0“), seltener auch wieder reaktiviert („Beschreiben“ mit „1“) werden können.

Ein sehr wichtiges Merkmal von RFID-Systemen ist die *Energieversorgung* der Transponder. *Passive Transponder* beinhalten keine eigene Energieversorgung, die gesamte Energie zum Betrieb passiver Transponder muss deshalb dem (elektrischen / magnetischen) Feld des Lesegeräts entnommen werden. Im Gegensatz dazu enthalten *aktive Transponder* eine Batterie, welche die Energie zum Betrieb des Mikrochips ganz oder zumindest teilweise („Stützbatterie“) zur Verfügung stellt.

Eines der wichtigsten Merkmale von RFID-Systemen ist die Betriebsfrequenz und die daraus resultierende Reichweite des Systems. Als Betriebsfrequenz eines RFID-Systems wird dabei die Frequenz bezeichnet, auf der das Lesegerät sendet. Die Sendefrequenz des Transponders wird nicht berücksichtigt. In den meisten Fällen entspricht sie der *Sendefrequenz* des Lesegeräts (Lastmodulation, Backscatter). Die „Sendeleistung“ des Transponders kann jedoch in jedem Fall um mehrere Zehnerpotenzen niedriger angesetzt werden als die des Lesegeräts.

Grundsätzlich werden die verschiedenen Sendefrequenzen den drei Bereichen LF (low frequency, 30 kHz ... 300 kHz), HF (high frequency) bzw. RF (radio frequency, 3 MHz ... 30 MHz) und UHF (ultra high frequency, 300 MHz ... 3 GHz) bzw. Mikrowelle (> 3 GHz) zugeordnet. Eine zusätzliche Einteilung der RFID-Systeme nach Reichweite ermöglicht die Unterscheidung zwischen Close coupling (< 1 cm), Remote coupling (0 ... 1 m), und long-range Systemen (> 1 m).

Die verschiedenen Verfahren der Datenübertragung, vom Transponder zurück zum Lesegerät, lassen sich in drei Gruppen einteilen. Die Anwendung von Reflexion bzw. Backscatter (die Frequenz der reflektierten Welle entspricht der Sendefrequenz des Lesegeräts: Frequenzverhältnis 1:1) oder Lastmodulation (das Feld des Lesegeräts wird durch den Transponder beeinflusst: Frequenzverhältnis 1:1), die Anwendung von Subharmonischen (1/n-fache) sowie die Erzeugung von Oberwellen (n-fache) im Transponder.

2.2 Bauformen von Transpondern

2.2.1 Disks und Münzen

Häufigste Bauform sind die sogenannten *Disks* (Münzen), Transponder in einem runden (ABS-)Spritzgussgehäuse, mit Durchmessern von wenigen Millimetern bis zu 10 cm. In der Mitte befindet sich meistens eine Bohrung zur Aufnahme einer Befestigungsschraube. Alternativ zu (ABS-)Spritzguss wird auch gerne Polystyrol oder sogar Epoxydharz für einen erweiterten Temperaturbereich verwendet.

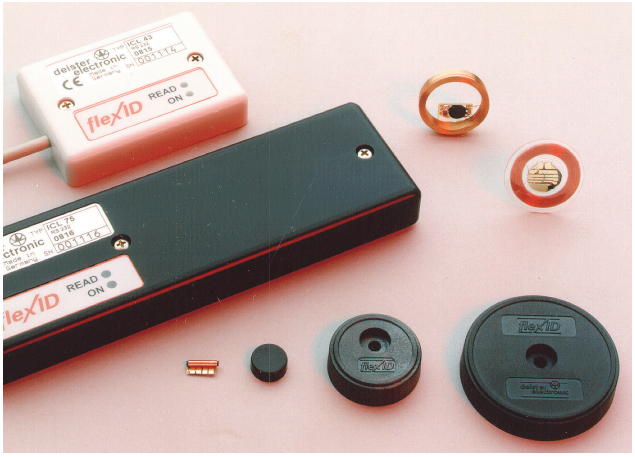


Abb. 2.2 Verschiedene Bauformen von Disk-Transpondern. (Foto: Deister Electronic, Barsinghausen)
rechts: Transponderspule und Chip vor dem Einbau in ein Gehäuse.
links: unterschiedliche Bauformen von Leseantennen.

2.2.2 Glasgehäuse

Für die Identifizierung von Tieren wurden die *Glastransponder* entwickelt, die unter die Haut des Tieres injiziert werden können (siehe hierzu Kapitel 14 „Anwendungsbeispiele“, S. 655).

In dem lediglich 12 bis 32 mm langen Glasröhrchen befinden sich ein auf einem Träger (PCB) montierter Mikrochip sowie ein Chipkondensator zur Glättung der gewonnenen Versorgungsspannung. Die Transponderspule wird aus nur 0,03 mm dickem Draht auf einen Ferritkern gewickelt. Für die mechanische Stabilität sind die inneren Komponenten in einem Weichkleber eingebettet.

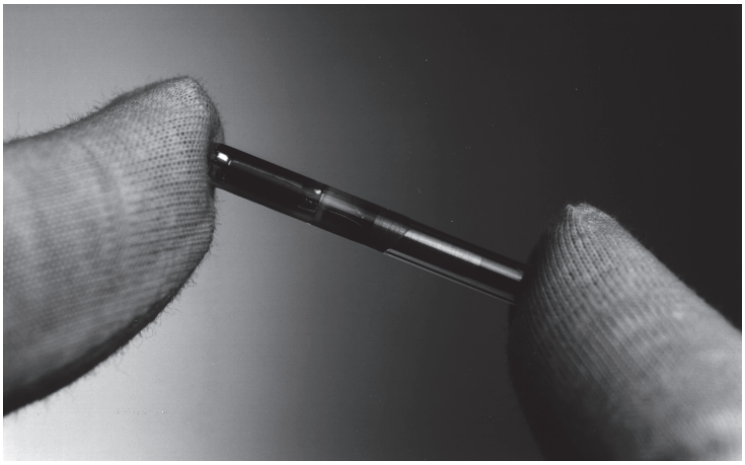


Abb. 2.3 Großaufnahme eines 32-mm-Glastransponders zur Identifikation von Tieren oder zur Weiterverarbeitung zu anderen Bauformen. (Foto: Texas Instruments, Freising)

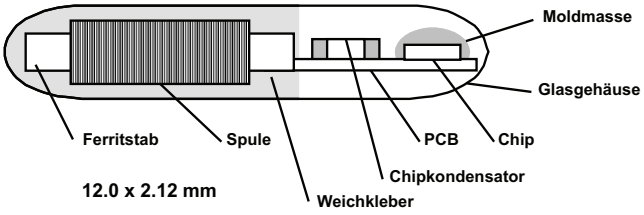


Abb. 2.4 Mechanischer Aufbau eines Glastransponders.

2.2.3 Plastikgehäuse

Für Anwendungen mit besonders hohen mechanischen Anforderungen wurde das *Plastikgehäuse* (*Plasticpackage*, PP) entwickelt. Dieses Gehäuse wird auch gerne in andere Bauformen integriert, so etwa in *Autoschlüssel* für elektronische Wegfahrsperren.

Abb. 2.5 Transponder im Plastikgehäuse. (Foto: Philips Semiconductors, Hamburg)

Der aus Moldmasse (IC-Vergussmasse) bestehende abgeschrägte Quader beinhaltet nahezu die gleichen Komponenten wie der Glastransponder, hat aber durch die längere Spule eine größere Funktionsreichweite. Weitere Vorteile sind die Aufnahmefähigkeit von größeren Mikrochips sowie die hohe Belastungsfähigkeit gegenüber mechanischen Vibrationen, wie

es z. B. von der Automobilindustrie gefordert wird. Auch andere Qualitätsanforderungen, wie Temperatur-Zyklen oder Falltest, erfüllen die PP-Transponder zur vollsten Zufriedenheit [bruhnke].

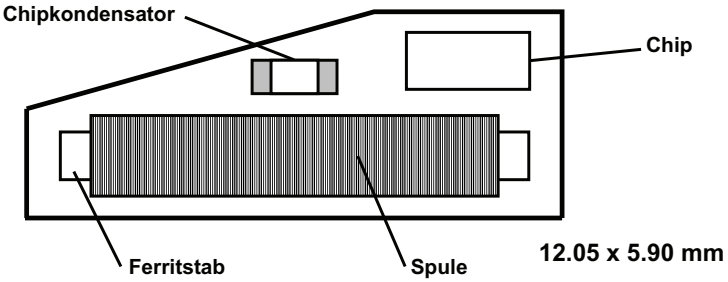


Abb. 2.6 Mechanischer Aufbau eines Transponders im Plastikgehäuse. Die Dicke des Gehäuses beträgt gerade 3 mm.

2.2.4 Werkzeug- und Gasflaschenidentifikation

Für den Einbau induktiv gekoppelter Transponder in *Metalloberflächen* wurden spezielle Bauformen entwickelt. Hierbei wird die Transponderspule in einen Ferritschalenkern gewickelt. Der Transponderchip wird auf der Rückseite des *Ferritschalenkerns* montiert und mit der Transponderspule kontaktiert. Um ausreichend mechanische Stabilität, Vibrations- und Hitzebeständigkeit zu erlangen, werden Transponderchip und Ferritschalenkern mit Epoxydharz in einer Halbschale aus PPS vergossen [link].

Abb. 2.7 Transponder in der nach DIN/ISO 69873 genormten Bauform, zum Einbau in einen Anzugsbolzen eines CNC-Werkzeugs. (Foto: Leitz GmbH & Co, Oberkochen)

Für den Einbau in einen Anzugsbolzen oder Steilkegelschaft zur Werkzeugidentifikation wurden die Außenabmessungen des Transponders sowie dessen Einbauraum in *DIN/ISO 69873* genormt. Zur Gasflaschenidentifikation kommen auch davon abweichende Bauformen zum Einsatz.

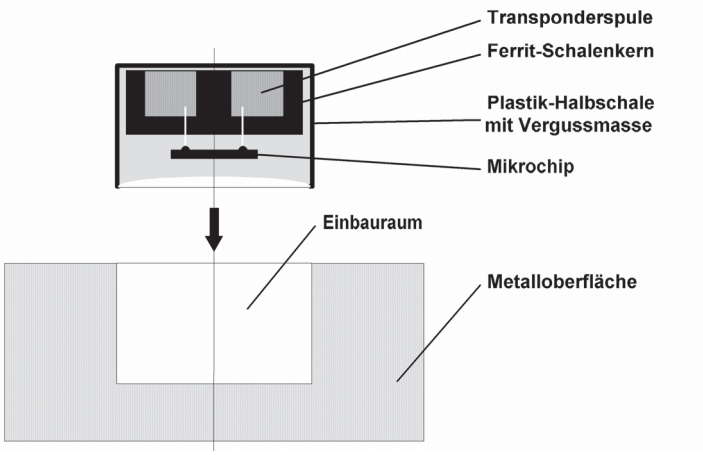


Abb. 2.8 Mechanischer Aufbau eines Transponders zum Einbau in Metalloberflächen. Die Transponderspule wird auf einen Ferrit-U-Kern gewickelt und dann in einer Plastik-Halbschale vergossen. Der Einbau erfolgt mit der Öffnung des U-Kerns nach oben.

2.2.5 Schlüssel und Schlüsselanhänger

Für Anwendungen der Wegfahrsperre oder für Türschließsysteme mit besonders großen Sicherheitsanforderungen werden Transponder auch in mechanische Schlüssel integriert. Als Ausgangsbasis dient hier in der Regel ein Transponder im Plasticpackage, welcher dann in den Schlüsselknauf eingegossen bzw. eingespritzt wird.

Für Zutrittssysteme zu Büro- und Arbeitsräumen hat sich auch eine Transponderbauform als Schlüsselanhänger als sehr beliebt erwiesen.

Abb. 2.9 Schlüsselanhänger-Transponder für ein Zutrittssystem.
(Foto: Philips Semiconductors Gratkorn, A-Gratkorn)

2.2.6 Uhren

Diese Bauform wurde schon Anfang der 90er-Jahre von der österreichischen Firma Ski-Data entwickelt und zunächst als Skipass eingesetzt. Darüber hinaus konnten sich die „*kontaktlosen Uhren*“ vor allem auch bei Zutrittskontrollsystemen durchsetzen. Die Uhr enthält eine auf eine dünne Leiterplatte aufgedruckte Rahmenantenne mit wenigen Windungen, welche möglichst dicht am Uhrengehäuse entlanggeführt werden, um die von der Antennenspule umfasste Fläche – und damit die Reichweite – zu optimieren.

Abb. 2.10
Uhr mit integriertem Transponder als kontaktlose Zutrittsberechtigung. (Foto: Junghans Uhren GmbH, Schramberg)

2.2.7 Bauform ID-1, kontaktlose Chipkarten

Der von Kredit- und Telefonkarten bekannten Bauform ID-1 (85,72 mm x 54,03 mm x 0,76 mm ± Toleranzen) dieser kleinen Plastikkärtchen kommt auch bei RFID-Systemen eine immer größer werdende Bedeutung als *kontaktlose Chipkarte* zu. Ein Vorteil dieser Bauform für induktiv gekoppelte RFID-Systeme besteht in der großen Spulenfläche, wodurch sich bei den Chipkarten hohe Reichweiten ergeben.

Kontaktlose Chipkarten entstehen durch das Einlaminieren eines Transponders zwischen vier PVC-Folien. Dabei werden die Einzelfolien bei hohem Druck und Temperaturen über 100 °C zu einer unlösbaren Einheit verbacken (die Herstellung von kontaktlosen Chipkarten ist in Kapitel 13 „Herstellung von Transpondern und kontaktlosen Chipkarten“, S. 601, ausführlich beschrieben).

front view

Abb. 2.11 Aufbau einer kontaktlosen Chipkarte: Kartenkörper mit Transpondermodul und Antenne.

Abb. 2.12 Halbtransparente kontaktlose Chipkarte. Deutlich zu erkennen die Transponderantenne entlang des Kartenrands. (Foto: Giesecke & Devrient, München)

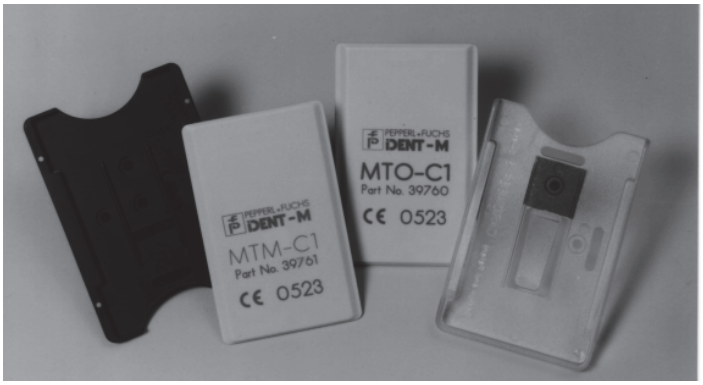


Abb. 2.13 Mikrowellen-Transponder im Kunststoff-Halbschalengehäuse. (Foto: Pepperl & Fuchs, Mannheim)

Kontaktlose Chipkarten in der Bauform ID-1 eignen sich hervorragend als Werbeträger und werden, wie auch Telefonchipkarten, mit künstlerisch gestalteten Aufdrucken versehen.

Nicht immer ist jedoch die in ISO 7810 für ID-1-Karten geforderte maximale Dicke von 0,8 mm einzuhalten. Vor allem Mikrowellentransponder benötigen eine dickere Bauform, weshalb der Transponder hier meist zwischen zwei PVC-Halbschalengehäuse verklebt oder im (ABS-)Spritzgussverfahren verpackt wird.

Abb. 2.14 Smart Label Transponder sind dünn und flexibel genug, um sie als Selbstklebelabel am Fluggepäck anzubringen. (Foto: i-code-Transponder, Philips Semiconductors, A-Gratkorn)

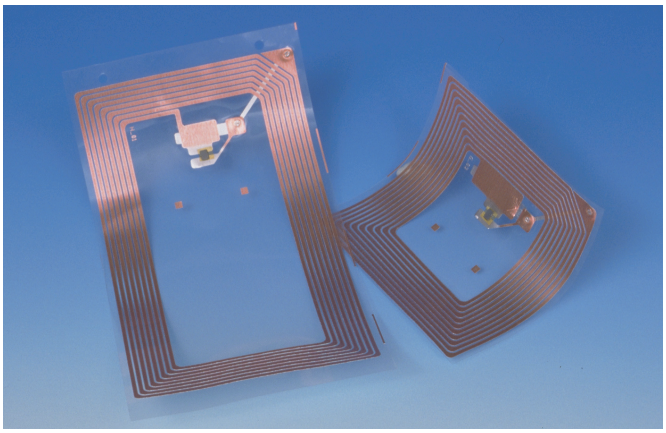


Abb. 2.15 Ein Smart-Label besteht im Wesentlichen aus einer dünnen Papier- oder Plastikfolie, auf die die Transponderspule und der Transponderchip aufgebracht werden.
(Foto: Tag-It Transponder, Texas Instruments, Freising)

2.2.8 Smart Label

Unter „*Smart Label*“ versteht man eine papierdünne Transponderbauform. Hierbei wird die Transponderspule durch *Siebdruck* oder *Ätztechnik* auf eine nur 0,1 mm dicke Plastikfolie

aufgebracht. Diese Folie wird häufig mit einer Papierschicht laminiert und auf der Rückseite mit einem Kleber beschichtet. Die Transponder werden als Selbstklebeetiketten auf einer Endlosrolle geliefert und sind dünn und flexibel genug, um sie auf Gepäckstücke, Pakete und Waren aller Art aufzukleben. Da die *Klebeetiketten* leicht nachträglich bedruckt werden können, ist die Verknüpfung der gespeicherten Daten mit einem zusätzlichen Barcode auf der Vorderseite des *Labels* leicht möglich.

2.2.9 Coil-on-Chip

Bei den bisher vorgestellten Bauformen werden die Transponder aus einer separaten Transponderspule, die als Antenne funktioniert, und einem Transponderchip hergestellt (hybride Technologie). Die Transponderspule wird dabei auf konventionelle Weise an den Transponderchip gebondet.

Abb. 2.16 Durch die Coil-on-chip-Technologie wird eine extreme Miniaturisierung von Transpondern möglich. (Foto: Micro Sensys, Erfurt)

Im Wege der Miniaturisierung liegt es nahe, auch die Spulen auf dem Chip zu integrieren („*coil-on-chip*“). Möglich wird dies durch einen speziellen Mikrogalvanikprozess, der auf einem nomalen CMOS-Wafer stattfinden kann. Die Spule wird hier als planare (einlagige) Spiralanordnung unmittelbar auf dem Isolator des Siliziumchips platziert und durch konventionelle Öffnungen in der Passivierungsschicht mit der darunterliegenden Schaltung kontaktiert [jurisch-95, jurisch-98]. Die erreichten Leiterbahnbreiten liegen im Bereich von 5 bis 10 µm, bei einer Schichtdicke von 15 bis 30 µm. Um die mechanische Belastbarkeit des kontaktlosen Speicherbausteins in Coil-on-chip-Technologie zu gewährleisten, wird eine Abschlusspassivierung auf Polyamidbasis durchgeführt.

Die Größe des Siliziumchips und damit des gesamten Transponders beträgt gerade einmal 3 x 3 mm^2. Zur besseren Handhabung werden die Transponder häufig noch in einen Kunst-

stoffkörper eingebettet und gehören mit Ø 6mm x 1,5 mm zu den kleinsten auf dem Markt verfügbaren RFID-Transpondern.

2.2.10 Weitere Bauformen

Neben diesen wichtigsten Bauformen werden noch eine Menge anwendungsspezifischer Sonderbauformen hergestellt. Beispiele hierfür sind etwa die „Brieftaubentransponder“ oder der „Champion-Chip“ für sportliche Zeitmessungen. Transponder können wohl in jede vom Kunden gewünschte Bauform gebracht werden. Bevorzugt werden dabei Glas- oder PP-Transponder zu weiteren Bauformen verarbeitet.

2.3 Frequenz, Reichweite und Kopplung

Die wichtigsten Unterscheidungskriterien für RFID-Systeme sind die Betriebsfrequenz des Lesegeräts, das physikalische Kopplungsverfahren und die Reichweite des Systems. RFID-Systeme werden auf unterschiedlichsten Frequenzen von Langwelle 135 kHz bis in den Mikrowellenbereich bei 5,8 GHz betrieben. Bei der physikalischen Kopplung kommen *elektrische*, *magnetische* und *elektromagnetische Felder* zum Einsatz. Schließlich variiert die erzielbare Reichweite der Systeme von wenigen mm bis hin zu 15 m und darüber.

RFID-Systeme mit sehr kleinen Reichweiten, im Bereich bis zu typischerweise 1 cm, werden als *Close-coupling-Systeme* bezeichnet. Die Transponder müssen zum Betrieb entweder in ein Lesegerät eingesteckt oder auf einer dafür vorgesehenen Oberfläche positioniert werden. Close-coupling-Systeme verwenden sowohl elektrische als auch magnetische Felder zur Kopplung und können theoretisch auf beliebigen Frequenzen zwischen DC und 30 MHz betrieben werden, da zum Betrieb der Transponder keine Felder abgestrahlt werden müssen. Dies ermöglicht die Bereitstellung größerer Energiemengen, so etwa auch für den Betrieb eines in der Stromaufnahme nicht optimierten Mikroprozessors. Close-coupling-Systeme wurden bis zur Jahrtausendwende vor allem in Applikationen eingesetzt, an die große Sicherheitsanforderungen gestellt wurden, die jedoch keine großen Reichweiten erforderten. Dies waren zum Beispiel elektronische Türschließanlagen oder kontaktlose Chipkartensysteme mit Zahlungsfunktionen. Close-coupling-Transponder wurden ausschließlich als *kontaktlose Chipkarte* im ID1-Format (ISO/IEC 10536) eingesetzt. Heute werden Close-coupling-Chipkarten jedoch nicht mehr verwendet.

RFID-Systeme mit Schreib- und Lesereichweiten bis zu etwa 1 m werden mit dem Überbegriff *Remote-coupling-Systeme* bezeichnet. Fast allen diesen Systemen ist eine *induktive* (magnetische) *Kopplung* gemeinsam, weshalb sie auch als *induktive Funkanlagen* bezeichnet werden. Daneben existieren noch einige wenige Systeme mit *kapazitiver* (elektrischer) *Kopplung* [bistatix]. Mindestens 90% aller verkauften RFID-Systeme gehören derzeit zu den induktiv gekoppelten Systemen. Aus diesem Grunde ist mittlerweile eine fast unüberschaubare Anzahl dieser Systeme auf dem Markt verfügbar. Für verschiedene Standardanwendungen wie kontaktlose Chipkarten, Tieridentifikation oder Industrieautomation existieren darüber hinaus eine Reihe von Normen, welche die technischen Parameter der

Transponder und Lesegeräte spezifizieren. Hierunter fallen auch die *Proximity-coupling*-(ISO 14443, kontaktlose Chipkarten) und *Vicinity-coupling-Systeme* (ISO 15693, *Smart Label* und kontaktlose Chipkarten). Als Sendefrequenzen werden Frequenzen unter 135 kHz oder 13,56 MHz verwendet. Einige Sonderanwendungen (siehe Eurobalise) werden auch noch auf 27,125 MHz betrieben.

RFID-Systeme mit Reichweiten deutlich über 1 m werden als *Long-range-Systeme* bezeichnet. Alle Long-range-Systeme arbeiten mit elektromagnetischen Wellen im *UHF*- und *Mikrowellenbereich*. Die überwiegende Mehrheit dieser Systeme wird nach ihrem physikalischen Funktionsprinzip als *Backscatter-System* bezeichnet. Daneben gibt es im Mikrowellenbereich noch Long-range-Systeme mit *Oberflächenwellen-Transpondern*. Alle diese Systeme werden auf den UHF-Frequenzen 868 MHz (Europa) und 915 MHz (USA) sowie auf den Mikrowellenfrequenzen 2,5 GHz und 5,8 GHz betrieben. Mit passiven (batterielosen) Backscatter-Transpondern können heute Reichweiten von typischerweise 3 m, mit aktiven (batteriegestützten) Backscatter-Transpondern sogar Reichweiten von 15 m und mehr erzielt werden. Die Batterie aktiver Transponder stellt jedoch in keinem Fall die Energie zur Datenübertragung zwischen Transponder und Lesegerät zur Verfügung, sondern dient ausschließlich der Versorgung des Mikrochips und dem Erhalt der gespeicherten Daten. Zur Datenübertragung zwischen Transponder und Lesegerät wird ausschließlich die Energie des elektromagnetischen Feldes eingesetzt, welches vom Lesegerät empfangen wird.

Um den Bezug zu einer möglicherweise irreführenden Reichweitenangabe zu vermeiden, verwendet dieses Buch zur Klassifizierung der physikalischen Eigenschaften im Weiteren ausschließlich die Begriffe „induktiv bzw. kapazitiv gekoppelte Systeme“ und *Mikrowellen-System* oder *Backscatter-System.*

2.4 Aktive und passive Transponder

Ein wichtiges Unterscheidungsmerkmal von RFID-Systemen ist die Art der Energieversorgung des Transponders. Wir unterscheiden dabei zwischen *passiven* und *aktiven Transpondern*.

Passive Transponder verfügen über keinerlei eigene Energieversorgung. Die gesamte zum Betrieb des Transponders benötigte Energie wird durch die Antenne des Transponders dem magnetischen oder elektromagnetischen Feld des Lesegeräts entnommen. Zur Datenübertragung vom Transponder an das Lesegerät kann das Feld des Lesegeräts beeinflusst werden (zum Beispiel durch Lastmodulation oder modulierte Rückstreuung, siehe hierzu Kapitel 3.2 „Voll- und Halbduplexverfahren“, S. 45) oder kurzzeitig Energie aus dem Feld des Lesegeräts im Transponder zwischengespeichert werden (siehe Kapitel 3.3 „Sequentielle Verfahren“, S. 67). Die vom Lesegerät abgestrahlte Energie dient also zur Datenübertragung sowohl vom Lesegerät zum Transponder als auch von diesem zurück an das Lesegerät. Befindet sich der Transponder außerhalb der *Reichweite* eines Lesegeräts, so ist dieser vollkommen ohne elektrische Energie und daher auch niemals in der Lage, irgendein Signal auszusenden.

Aktive Transponder verfügen über eine eigene Energieversorgung, zum Beispiel in Form einer *Batterie* oder einer Solarzelle. Die Energieversorgung wird hierbei zur Spannungsversorgung des Chips eingesetzt. Das vom Lesegerät empfangene magnetische oder elektromagnetische Feld wird also nicht mehr zur Energieversorgung des Chips benötigt, weshalb auch ein deutlich schwächeres Feld als zum Betrieb eines passiven Transponders benötigt wird. Dieser Umstand kann zu einer deutlichen Erhöhung der *Kommunikationsreichweite* beitragen, falls der Transponder in der Lage ist, die entsprechend schwächeren Signale des Lesegeräts zu detektieren. Auch ein aktiver RFID-Transponder ist jedoch nicht in der Lage, ein eigenes Hochfrequenzsignal zu erzeugen, sondern beeinflusst zur Datenübertragung vom Transponder an das Lesegerät das Feld des Lesegeräts, so wie dies bei den passiven Transpondern der Fall ist. Die Energie aus der eigenen Energieversorgung des Transponders leistet also keinen Beitrag zur Datenübertragung vom Transponder zum Lesegerät! In der Literatur wird dieser Typ des Transponders häufig auch als *„semi-passiver" Transponder* bezeichnet [Kleist-2004], was andeuten soll, dass der Transponder kein eigenes Hochfrequenzsignal erzeugen kann.

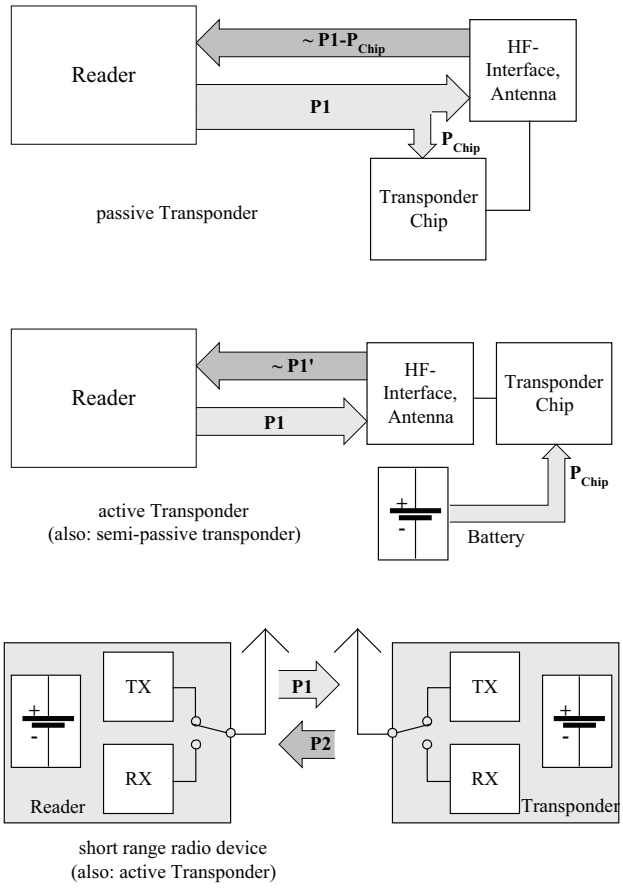


Abb. 2.17 Vergleich zwischen passiven und aktiven Transpondern.

Da sowohl passive als auch aktive (semi-passive) RFID-Transponder das magnetische oder elektromagnetische Feld eines Lesegeräts zur Datenübertragung benötigen, sind die damit erzielbaren Lesereichweiten durch physikalische Grenzen stark limitiert. Unter Berücksichtigung der zugelassenen Sendeleistungen für RFID-Lesegeräte lassen sich damit je nach Frequenzbereich Reichweiten von maximal etwa 15 m erreichen.

Eine weitere Klasse von aktiven Transpondern entspricht in der Schaltungstechnik eher einem klassischen Funkgerät. Diese Transponder verfügen über einen aktiven Sender (TX) sowie häufig auch über einen qualitativ hochwertigen Empfänger (RX). Um Daten an ein Lesegerät zu übertragen, wird der Sender eingeschaltet und von der Antenne ein hochfrequentes elektromagnetisches Feld abgestrahlt. Die Energieversorgung des Transponders erfolgt dabei aus einer lokalen Energiequelle, z. B. einer Batterie.

Diese Transponder senden also selbst ein hochfrequentes elektromagnetisches Feld aus, statt das Feld eines Lesegeräts zu beeinflussen. Aus rein technischer Sicht handelt es sich bei diesen Transpondern daher auch um keine echten „RFID"-Transponder, sondern um *Kurzstreckenfunkgeräte* (*Telemetriesender* oder *short range device*, *SRD*), wie sie zum Beispiel schon seit Jahrzehnten zur Messdatenübertragung von entfernten Punkten eingesetzt werden. Auf Grund der anderen physikalischen Mechanismen können unter Berücksichtigung der zugelassenen Sendeleistung für short range devices Reichweiten von bis zu einigen 100 m erzielt werden. Bei größeren Sendeleistungen sind auch entsprechend größere Reichweiten möglich, als dies mit herkömmlichen Funkanlagen möglich ist.

Um von dem anhaltenden RFID-Boom profitieren zu können, werden Telemetriesender seit einiger Zeit als RFID-Systeme verkauft. Aus Marketingsicht ist dagegen sicher nichts einzuwenden, der Techniker sollte sich jedoch immer im Klaren sein, worin die Unterschiede zwischen RFID-Systemen und Telemetriesendern bestehen und wodurch die hohen Reichweiten der Letzteren begründet sind.

Telemetriesender werden im RFID-Handbuch nicht weiter behandelt, da hierzu bereits eine Menge an Literatur existiert. Als gute Einführung sei [bensky] empfohlen.

2.5 Informationsverarbeitung im Transponder

Ordnet man RFID-Systeme nach dem Funktionsumfang der Transponder hinsichtlich der Informations- und Datenverarbeitung sowie der Größe des im Transponder verfügbaren Datenspeichers, so erhält man ein breites Spektrum an Varianten, dessen Enden durch die Low-end- und High-end-Systeme gebildet wird.

- Das untere Ende der *Low-end-Systeme* wird durch die *EAS-Systeme* (elektronische *Artikelsicherungssysteme*, siehe Kapitel 3.1 „1-bit-Transponder", S. 34) abgedeckt. Diese Systeme überprüfen und überwachen unter Verwendung einfacher physikalischer Effekte die mögliche Anwesenheit eines Transponders im Ansprechbereich eines Detektionsgeräts. Auch *Read-only-Transponder*, die bereits mit einem Mikrochip ausgestattet sind, gehören noch zu den Low-end-Systemen. Diese Transponder verfügen über einen fest kodierten Datensatz, der in der Regel nur aus einer eindeutigen, mehrere Bytes langen *Se-*

riennummer („*unique number*“) besteht. Wird ein Read-only-Transponder in das HF-Feld eines Lesegeräts gebracht, so beginnt er damit, fortlaufend seine ihm eigene Seriennummer auszusenden. Eine Möglichkeit, einen Read-only-Transponder durch das Lesegerät anzusprechen, besteht nicht, es findet also nur ein unidirektionaler Datenfluss vom Transponder zum Lesegerät statt. Im praktischen Betrieb solcher Systeme muss daher darauf geachtet werden, dass sich immer nur ein Transponder im Ansprechbereich des Lesegeräts befindet, da es sonst durch zwei oder mehrere gleichzeitig sendende Transponder unweigerlich zu Datenkollisionen käme, die eine Detektion der Transponder durch ein Lesegerät unmöglich machen. Trotz dieser Einschränkungen sind Read-only-Transponder für viele Anwendungen, in denen das Auslesen einer eindeutigen Nummer genügt, hervorragend geeignet. Aufgrund der einfachen Funktionen eines Read-only-Transponders kann die Fläche der Chips sehr klein gehalten werden, was einerseits zu einer geringen Leistungsaufnahme der Chips, aber andererseits auch zu niedrigen Preisen in der Herstellung führt. Read-only-Systeme werden auf allen Frequenzen betrieben, die für RFID-Systeme zur Verfügung stehen. Die erzielbaren Reichweiten sind dank der geringen Leistungsaufnahme des Mikrochips in der Regel sehr hoch.
Read-only-Systeme werden dort eingesetzt, wo nur wenig Daten benötigt werden oder Strichcodesysteme in der Funktionalität ersetzt werden können, also zum Beispiel in der Steuerung von Warenflüssen, bei der Identifikation von Paletten, Containern, Gasflaschen (ISO 18000), aber auch bei der Identifikation von Tieren (ISO 11785).

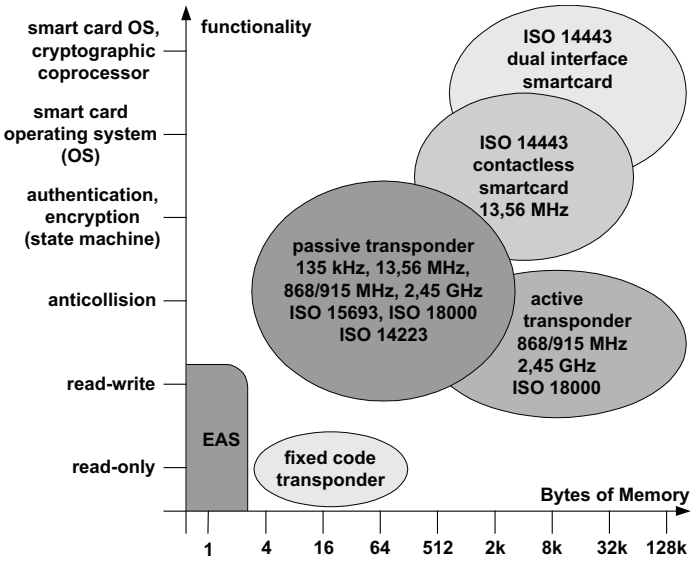


Abb. 2.18 RFID-Systeme können nach ihrer Funktionalität auch in Low-end- und High-end-Systeme eingeteilt werden.

- Das Mittelfeld wird durch eine Vielzahl von Systemen mit beschreibbarem Datenspeicher gebildet, sodass in diesem Bereich die Typenvielfalt mit Abstand am größten ist. Die Speichergrößen variieren von wenigen Bytes bis über 100 kByte EEPROM (passive Transponder) oder auch SRAM (aktive, d.h. batteriegestützte Transponder). Diese Transponder

sind in der Lage, in einer fest codierten *State-Machine* einfache Kommandos des Lesegeräts zum selektiven Lesen und Schreiben des Datenspeichers abzuarbeiten. In der Regel unterstützen die Transponder auch *Antikollisionsverfahren*, wodurch sich mehrere Transponder, die sich zur selben Zeit im Ansprechbereich des Lesegeräts befinden, gegenseitig nicht mehr beeinflussen und durch das Lesegerät selektiv angesprochen werden können (siehe Kapitel 7.2 „Vielfachzugriffsverfahren – Antikollision“, S. 250).
Auch kryptologische Verfahren, also eine *Authentifizierung* zwischen Transponder und Lesegerät, sowie eine Datenstromverschlüsselung (siehe Kapitel 8 „Sicherheit von RFID-Systemen“, S. 273) sind bei diesen Systemen bereits häufig anzutreffen. Diese Systeme werden auf allen Frequenzen betrieben, die für RFID-Systeme zur Verfügung stehen.

- Kontaktlose Chipkarten mit einem Mikroprozessor und einem Chipkarten Betriebssystem (smart-card OS) stellen den unteren Bereich der *High-end-Systeme* dar. Durch den Einsatz von Mikroprozessoren lassen sich wesentlich komplexere Algorithmen zur Verschlüsselung und Authentifizierung verwirklichen, als dies mit einer „festverdrahteten“ State-Machine möglich wäre. Am oberen Ende der High-end-Systeme schließlich befinden sich moderne *Dual-Interface-Chipkarten* (siehe Kapitel 10.2.1 „Dual-Interface Karte“, S. 481), welche mit einem kryptografischen *Coprozessor* ausgestattet sind. Der Einsatz eines Coprozessors ermöglicht durch die damit verbundene enorme Verkürzung von Rechenzeiten den Einsatz kontaktloser Chipkarten auch in Anwendungen, die hohe Anforderungen an die sichere Verschlüsselung der Datenübertragung stellen, wie etwa elektronische Börsensysteme oder Ticketingsysteme für den Nahverkehr.
  High-end-Systeme werden fast ausschließlich auf der Frequenz 13,56 MHz betrieben. Die Datenübertragung zwischen Transponder und entsprechendem Lesegerät wird in der Norm ISO 14443 beschrieben.

2.6 Auswahlkriterien für RFID-Systeme

RFID-Systeme sind mittlerweile allgegenwärtig. Die Entwickler von RFID-Systemen haben dieser Entwicklung Rechnung getragen, sodass unzählige unterschiedliche Systeme auf dem Markt erhältlich sind, deren technische Parameter für unterschiedlichste Anwendungsgebiete – *Ticketing*, *Tieridentifikation*, *Industrieautomation* oder *Zutrittskontrolle* – optimiert sind. Häufig überschneiden sich diese Anwendungsgebiete in ihren technischen Anforderungen, sodass eine klare Zuordnung geeigneter Systeme nicht einfach ist. Die Produktpalette der heute angebotenen RFID-Systeme kann selbst vom Fachmann kaum noch überblickt werden. Für den Anwender ist es deshalb nicht immer einfach, das für ihn am besten geeignete System auszuwählen.

Im Folgenden einige Anregungen, unter welchen Gesichtspunkten RFID-Systeme bei der Auswahl betrachtet werden können.

2.6.1 Arbeitsfrequenz

RFID-Systeme von ca. 100 kHz bis etwa 30 MHz arbeiten mit induktiver Kopplung. Im Gegensatz dazu verwenden UHF- und Mikrowellen-Systeme im Frequenzbereich 868 oder 915 MHz, 2,45 oder 5,8 GHz elektromagnetische Felder zur Kopplung.

Die spezifische *Absorptionsrate* (Dämpfung) bei 100 kHz ist für Wasser oder nichtleitende Stoffe etwa um den Faktor 100 000 niedriger als bei 1 GHz. Damit findet praktisch keine Absorption oder Dämpfung statt. Niederfrequente LF-Systeme werden hauptsächlich wegen der besseren Durchdringung von Objekten benutzt [schürmann-94]. Ein Beispiel hierfür ist der Bolus, ein Transponder, der im Vormagen (Pansen) von Rindern platziert wird und von außen mit einer Ansprechfrequenz von < 135 kHz ausgelesen werden kann.

UHF- und Mikrowellen-Systeme weisen gegenüber induktiven Systemen eine deutlich höhere *Reichweite* von typischerweise 2 ... 15 Metern auf. Die Transonder reagieren jedoch empfindlich Glas, Kunsstoffe, Wasser und Metall in unmittelbarer Nachbarschaft.

Ein wichtiger Faktor ist auch die Empfindlichkeit gegenüber *elektromagnetischen Störfeldern*, wie sie etwa von Schweißrobotern oder starken Elektromotoren erzeugt werden. Induktive Transponder sind hier eindeutig im Nachteil. Insbesondere in Fertigungslinien und Lackieranlagen der Automobilindustrie haben sich deshalb UHF- und Mikrowellen-Systeme etabliert. Hinzu kommt die hohe Speicherkapazität und die hohe Temperaturfestigkeit (bis 250 °C) der Mikrowellen-Systeme [bachthaler].

2.6.2 Reichweite

Die benötigte Reichweite einer Anwendung hängt von mehreren Faktoren ab:

- Positioniergenauigkeit des Transponders
- Minimaler Abstand mehrerer Transponder im praktischen Einsatz
- Geschwindigkeit des Transponders im Ansprechbereich des Lesegeräts

So ist beispielsweise bei kontaktlosen Zahlungsanwendungen – etwa Tickets für ÖPNV – die Positioniergeschwindigkeit sehr klein, da die Transponder von Hand an das Lesegerät geführt werden. Der minimale Abstand mehrerer Transponder entspricht hier dem Abstand zweier Fahrgäste beim Betreten eines Fahrzeuges. Für diese Systeme ergibt sich eine optimale Reichweite von 5 ... 10 cm. Eine größere Reichweite könnte hier nur zu Problemen führen, da womöglich die Tickets mehrerer Fahrgäste gleichzeitig vom Lesegerät erfasst würden. Eine sichere Zuordnung zwischen Ticket und Fahrgast wäre damit nicht mehr möglich.

Auf einer Montagelinie in der Automobilindustrie werden oft gleichzeitig verschiedene Fahrzeugmodelle mit unterschiedlichen Abmessungen gebaut. Damit sind starke Schwankungen des Abstands zwischen dem Transponder am Fahrzeug und dem Lesegerät vorprogrammiert [Bachthaler]. Der Schreib-/Leseabstand des eingesetzten RFID-Systems muss deshalb für die maximal benötigte Reichweite ausgelegt sein. Der Abstand zwischen den Transpondern muss so eingerichtet sein, dass sich immer nur ein einziger Transponder im Ansprechbereich des Lesegeräts befindet. Hier bieten Mikrowellen-Systeme mit einer „*gerichteten Keule*“ des Feldes deutliche Vorteile gegenüber den breiten, ungerichteten Feldern induktiv gekoppelter Systeme.

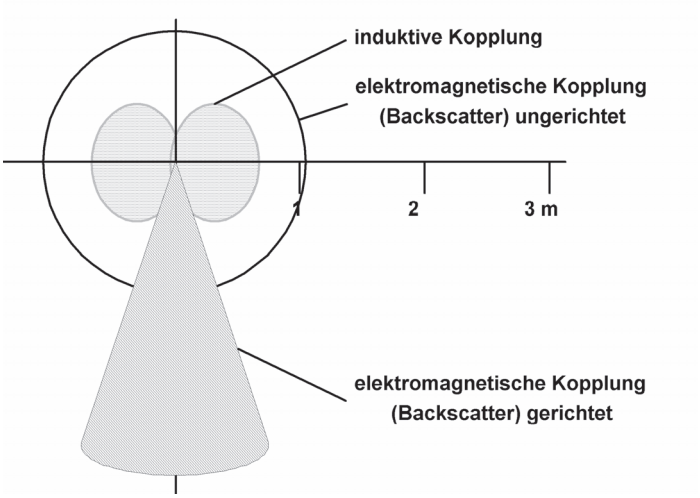


Abb. 2.19 Vergleich der relativen Ansprechbereiche verschiedener Systeme.

Die Geschwindigkeit des Transponders, relativ zum Lesegerät, bestimmt zusammen mit dem maximalen Schreib-/Leseabstand die Aufenthaltsdauer im Ansprechbereich des Lesegeräts. Bei der Identifikation von Fahrzeugen wird die benötigte Reichweite des RFID-Systems so ausgelegt, dass bei maximaler Fahrzeuggeschwindigkeit die Aufenthaltsdauer im Ansprechbereich zur Übertragung der vorgesehenen Daten ausreichend ist.

2.6.3 Sicherheitsanforderungen

Sicherheitsanforderungen, welche an eine geplante RFID-Anwendung zu stellen sind, also *Verschlüsselung* und *Authentifizierung*, sollten sehr genau abgeschätzt werden, um böse Überraschungen in der Einsatzphase von vornherein auszuschließen. Zu diesem Zweck ist zu beurteilen, welchen Anreiz das System einem potenziellen Eindringling bietet, sich durch eine Manipulation Vorteile hinsichtlich Geld- oder Sachwerten zu verschaffen. Um diese Anreize abschätzen zu können, teilen wir die Anwendungen in zwei Gruppen:

- industrielle oder geschlossene Anwendungen;
- öffentliche Anwendungen in Verbindung mit Geld- und Sachwerten.

Hierzu zwei gegensätzliche Anwendungsbeispiele:

Ein typisches Beispiel für eine industrielle oder geschlossene Anwendung wäre auch hier wieder eine Montagelinie in der Automobilindustrie. Zunächst einmal ist dieses RFID-System nur zutrittsberechtigten Personen zugänglich, sodass der Kreis potenzieller Angreifer überschaubar bleibt. Ein mutwilliger *Angriff* auf dieses System durch Verändern oder Verfälschen der Daten auf einem Transponder könnte zwar eine empfindliche Störung des Betriebsablaufs bewirken, doch würde dem Angreifer keinerlei persönlicher Nutzen entstehen. Die Wahrscheinlichkeit eines Angriffs kann also gleich null gesetzt werden, womit auch ein preisgünstiges Low-end-System ohne Sicherheitslogik eingesetzt werden kann.

Als zweites Beispiel dient uns ein Ticketing-System für den Einsatz im ÖPNV. Ein solches System, vor allem die Datenträger in Form kontaktloser Chipkarten, ist für jedermann zugänglich. Der Kreis potenzieller Angreifer ist somit unüberschaubar. Ein erfolgreicher Angriff auf ein derartiges System könnte für das angegriffene ÖPNV-Unternehmen einen großen finanziellen Schaden bedeuten, etwa bei organisiertem Vertrieb gefälschter Fahrausweise, vom Imageverlust für das Unternehmen einmal ganz abgesehen. Für solche Anwendungen ist ein High-end-Transponder mit Authentifizierungs- und Verschlüsselungsverfahren unverzichtbar. Für Anwendungen mit höchsten Sicherheitsanforderungen, beispielsweise Bankenanwendungen mit Kleingeldbörse, sollten ausschließlich Transponder mit Mikroprozessor eingesetzt werden.

2.6.4 Speicherkapazität

Die Chipgröße des Datenträgers – und damit die Preisklasse – wird hauptsächlich durch dessen *Speicherkapazität* bestimmt. Für preissensitive Massenanwendungen mit geringem Informationsbedarf vor Ort werden deshalb festcodierte Read-only-Datenträger eingesetzt. Damit kann jedoch nur die Identität eines Objekts definiert werden. Weitere Daten werden auf der zentralen Datenbank eines Leitrechners gespeichert. Sollen anfallende Daten auf den Transponder zurückgeschrieben werden, benötigt man Transponder mit EEPROM- oder RAM-Speichertechnologie.

EEPROM-Speicher sind vor allem bei UHF- und induktiv gekoppelten Systemen zu finden. Es werden Speicherkapazitäten von 16 Byte bis 64 kByte angeboten.

Batteriegepufferte SRAM-Speicher sind dagegen überwiegend bei Mikrowellen-Systemen anzutreffen. Die angebotenen Speicherkapazitäten reichen von 256 Byte bis zu 64 kByte.

3 Grundlegende Funktionsweise

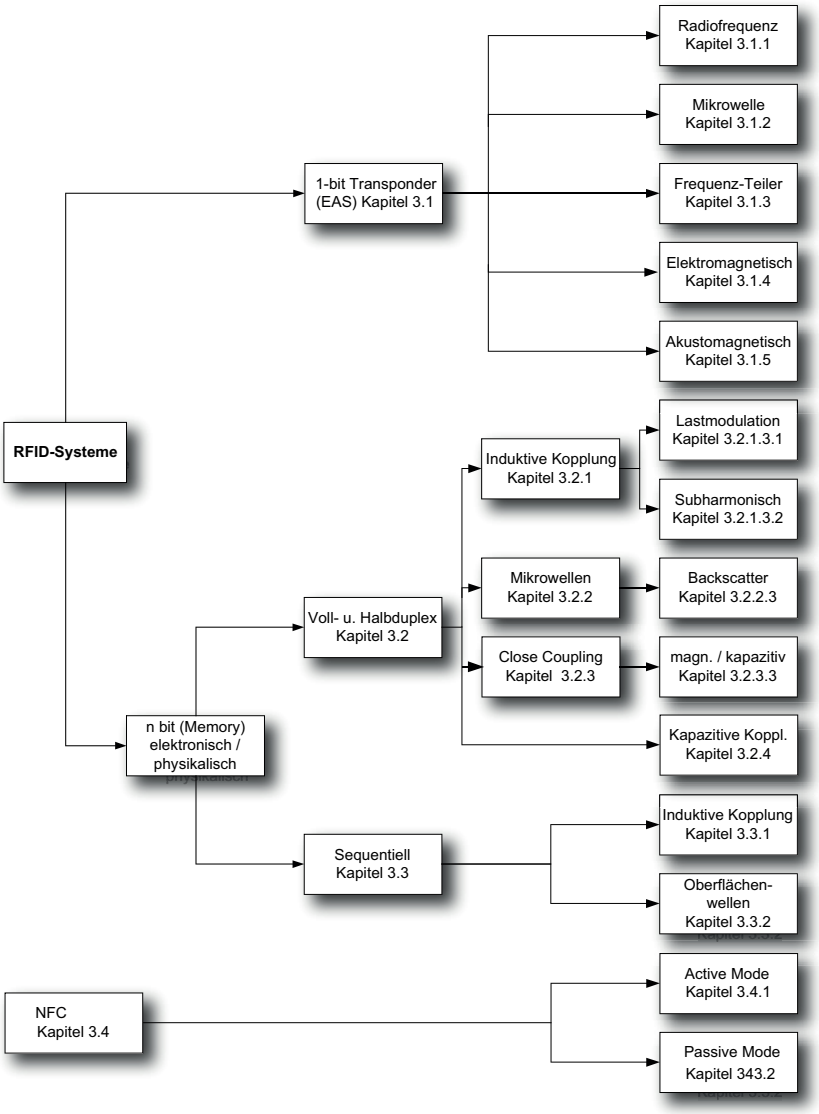


Abb. 3.1 Die Aufteilung der verschiedenen Funktionsweisen von RFID-Systemen in den Kapiteln.

Dieses Kapitel beschreibt das grundsätzliche Zusammenwirken zwischen dem Transponder und einem Lesegerät, insbesondere die Spannungsversorgung des Transponders und die Datenübertragung vom Transponder zum Lesegerät. Eine tiefergehende Beschreibung der physikalischen Zusammenhänge sowie mathematische Modelle für induktive Kopplung oder Backscatter-Systeme sind dem Kapitel 4 „Physikalische Grundlagen für RFID-Systeme“, S. 77 zu entnehmen.

3.1 1-bit-Transponder

Ein Bit stellt die kleinste darstellbare Informationseinheit dar und kennt nur zwei Zustände: „1“ oder „0“. Für Systeme mit *1-bit-Transponder* bedeutet dies, dass nur zwei Systemzustände darstellbar sind: „Transponder im Ansprechbereich“ oder „**kein** Transponder im Ansprechbereich“. Trotz dieser Einschränkung sind 1-bit-Transponder sehr weit verbreitet – ihr Haupteinsatzgebiet sind elektronische *Diebstahlsicherungen* im Warenhaus (*EAS* – electronic article surveillance; elektronische Artikelsicherung).

Eine elektronische Artikelsicherung besteht aus folgenden Komponenten: den Antennen eines „Lesegeräts“ bzw. Detektors, dem *Sicherungsmittel* oder *Etikett*, sowie optional einem *Deaktivator* zur Entschärfung nach dem Bezahlen. Bei modernen Systemen erfolgt die Entwertung gleichzeitig mit der Registrierung des Preiscodes an der Kasse. Manche Systeme verfügen auch noch über einen *Aktivator*, mit dem ein Sicherungsmittel nach Entschärfung wieder reaktiviert werden kann [gillert]. Wesentliches Leistungsmerkmal aller Systeme ist die Erkennungs- oder *Detektionsrate* in Abhängigkeit von der Durchgangsbreite (maximaler Abstand zwischen Transponder und Detektorantenne).

Die Vorgehensweise bei der Abnahme und Überprüfung installierter Artikelsicherungssysteme ist in der Richtlinie *VDI 4470* mit dem Titel „Warensicherungssysteme – Kundenabnahmerichtlinie für Schleusensysteme“ festgelegt. Diese Richtlinie enthält Definitionen und Testverfahren zur Ermittlung von Detektionsrate und Fehlalarmquote. Sie kann dem Einzelhandel als Grundlage für Kaufverträge oder zur laufenden Leistungskontrolle installierter Systeme dienen. Für den Produkthersteller stellt die Kundenabnahmerichtlinie ein wirkungsvolles Kontrollinstrument bei der Entwicklung und Optimierung von Integrationslösungen für Sicherungsprojekte dar [nach VDI 4470].

3.1.1 Radiofrequenz

Das *Radiofrequenz (RF)-Verfahren* arbeitet mit L-C-Schwingkreisen als Sicherungsmittel, welche auf eine definierte Resonanzfrequenz f_R abgeglichen sind. Ursprünglich wurden dazu Induktivitäten aus gewickeltem Kupferlackdraht mit angelötetem Kondensator im Kunststoffgehäuse (*Hartetikette*) verwendet. Heute benutzt man dazu zwischen Folie geätzte Spulen als Aufklebeschildchen. Damit der Dämpfungswiderstand nicht zu groß und damit die Güte der Schwingkreise nicht zu klein wird, muss die Dicke der Aluminium-Leiterbahnen auf den 25µm starken *Polyethylen-Folie* wenigstens 50µm betragen [jörn]. Zur Herstellung der Kondensatorplatten werden 10µm dicke Zwischenfolien verwendet.

Durch das Lesegerät (Detektionsgerät) wird ein magnetisches Wechselfeld im Radiofrequenzbereich erzeugt (siehe Abbildung 3.2). Nähert man den L-C-Schwingkreis dem magnetischem Wechselfeld, so wird über die Spule des Schwingkreises Energie aus dem Wechselfeld in den Schwingkreis eingekoppelt (Induktionsgesetz). Entspricht nun die Frequenz f_G des Wechselfeldes der Resonanzfrequenz f_R des L-C-Schwingkreises, so wird der Schwingkreis zu einer *Resonanzschwingung* angeregt. Der dadurch im Schwingkreis fließende Strom wirkt seiner Ursache, also dem von außen einwirkenden magnetischem Wech-

selfeld entgegen (siehe Kapitel 4.1.10.1 „Transformierte Transponderimpedanz ZT'“, S. 105). Dieser Effekt macht sich in einer kleinen Änderung des Spannungsabfalls über der Generatorspule des Transmitters bemerkbar und führt letztendlich zu einer Abschwächung der messbaren magnetischen Feldstärke. Auch in einer optionalen Sensorspule ist eine Änderung der induzierten Spannung messbar, sobald ein resonanter Schwingkreis in das magnetische Feld der Generatorspule eingebracht wird.

Die relative Stärke dieser Änderung ist abhängig vom Abstand der beiden Spulen zueinander (*Generatorspule* – Sicherungsmittel, Sicherungsmittel – *Sensorspule*) sowie der Güte Q des angeregten Schwingkreises (im Sicherungsmittel).

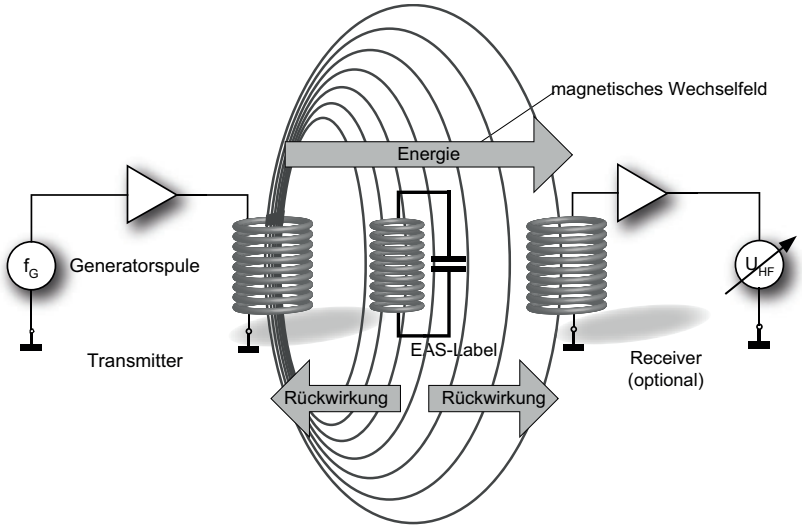


Abb. 3.2 Funktionsprinzip des EAS-Radiofrequenzverfahrens.

Die relative Stärke der Spannungsänderungen an Generator- und Sensorspule ist in der Regel sehr gering und damit schwierig zu erkennen. Um eine sichere Erkennung der Sicherungsmittel zu erreichen, ist es aber notwendig, ein möglichst ausgeprägtes Signal zu erhalten. Dies wird durch einen kleinen Trick erreicht: Die Frequenz des erzeugten Magnetfeldes ist nicht konstant, sondern wird „gewobbelt“. Dabei überstreicht die Generatorfrequenz fortlaufend den Bereich zwischen zwei Eckfrequenzen. Als Frequenzbereich steht den gewobbelten Systemen dazu der Bereich 8,2 MHz ±10% zur Verfügung [jörn].

Immer dann, wenn die gewobbelte Generatorfrequenz genau die Resonanzfrequenz des Schwingkreises (im Transponder) trifft, beginnt dieser einzuschwingen und erzeugt dadurch einen ausgeprägten Dip der Spannungen an der Generator- sowie der Sensorspule. Auch Frequenztoleranzen der Sicherungsmittel, bedingt durch Fertigungstoleranzen oder metallische Umgebung, spielen durch das „Abtasten“ eines ganzen Frequenzbereichs keine Rolle mehr.

Da die Etiketten an der Kasse nicht abgelöst werden, müssen sie so verändert werden, dass ein Ansprechen der Diebstahlsicherung ausgeschlossen ist. Hierzu werden die gesicherten Produkte von der Kassiererin auf ein Gerät gelegt – den *Deaktivator* –, das ein ausreichend

starkes Magnetfeld erzeugt, um mit der induzierten Spannung den Folienkondensator des Transponders zu zerstören. Die Kondensatoren besitzen dazu eigens eingebaute Sollkurzschlussstellen, sogenannte *Dimples*. Das Durchschlagen der Kondensatoren ist irreversibel und verstimmt den Schwingkreis so stark, dass dieser durch das *Wobbelsignal* nicht mehr angeregt werden kann.

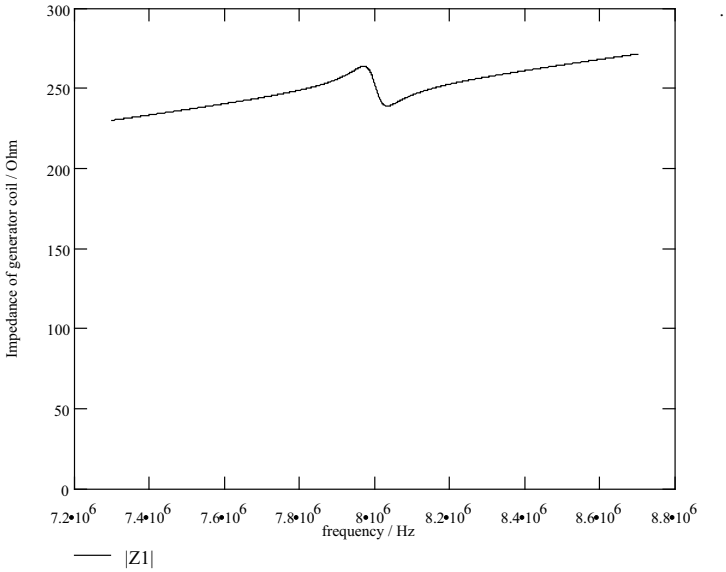


Abb. 3.3 Auftreten eines Impedanz-„Dip“ an der Generatorspule an der Resonanzfrequenz des Sicherungsmittels (Q = 90, k = 1%). Die Frequenz f_G des Generators wird kontinuierlich zwischen zwei Eckfrequenzen gewobbelt. Ein RF-Etikett im Feld des Generators erzeugt auf seiner Resonanzfrequenz f_R einen ausgeprägten Dip.

Zur Erzeugung des benötigten magnetischen Wechselfeldes im Detektionsbereich der Sicherungsanlage werden großflächige *Rahmenantennen* eingesetzt. Die in Säulen integrierten Rahmenantennen werden zu Durchgangsschleusen kombiniert. Die klassische Bauform, bekannt aus jedem größeren Kaufhaus, ist in Abbildung 3.4 dargestellt. Mit dem RF-Verfahren werden Schleusenbreiten von bis zu 2 m erreicht. Bei der relativ niedrigen Detektionsrate von ca. 70% [gillert] zeigt sich ein relativ starker Einfluss von bestimmten Produktmaterialien. Vor allem Metalle (z. B. Konservendosen) beeinflussen die Resonanzfrequenz der Etiketten sowie die Kopplung zur Detektorspule und beeinflussen damit die Detektionsrate negativ. Um die genannte Schleusenbreite und Detektionsrate zu erreichen, müssen Etiketten von 50 x 50 mm zum Einsatz kommen.

Tabelle 3.1: Typische Systemparameter für RF-Systeme [VDI 4471].

Gütefaktor Q der Sicherungsmittel	> 60 .. 80
Minimale Deaktivierungsfeldstärke H_D	1,5 A/m
Maximale Feldstärke im Detektionsbereich	0,9 A/m

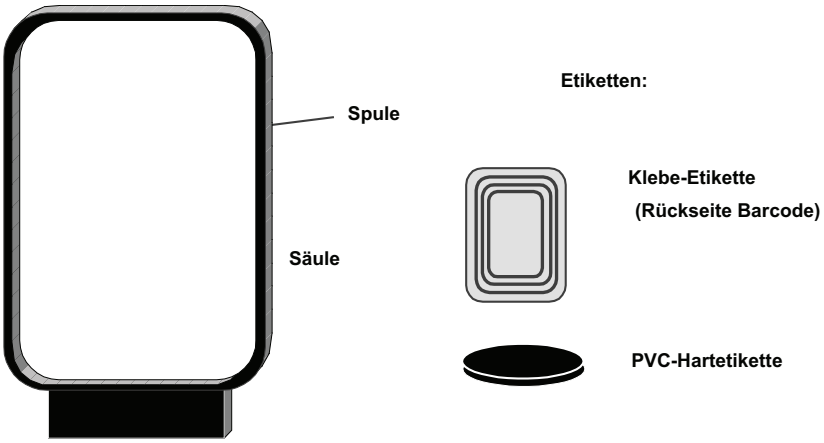


Abb. 3.4 *links:* Typische Rahmenantenne eines RF-Systems (Höhe 1,20 .. 1,60 m);
rechts: Bauformen von Etiketten.

Eine große Herausforderung für die Systemhersteller besteht in der Eigenschaft verschiedener Produkte, ebenfalls Resonanzfrequenzen aufzuweisen (z. B. Kabeltrommeln). Liegen diese Resonanzfrequenzen innerhalb des Wobbelbereichs 8,2 MHz ±10%, werden unweigerlich Fehlalarme ausgelöst.

Tabelle 3.2: Frequenzbereiche unterschiedlicher RF-Sicherungsanalgen [plotzke].

	Anlage 1	Anlage 2	Anlage 3	Anlage 4
Frequenz/MHz:	1,86 – 2,18	7,44 – 8,73	7,30 – 8,70	7,40 – 8,60
Wobbelfrequenz/Hz:	141	141	85	85

3.1.2 Mikrowelle

EAS-Systeme im *Mikrowellenbereich* nutzen die Entstehung von Harmonischen, an Bauteilen mit nichtlinearer Kennlinie (z. B. Dioden). Unter der *Harmonischen* einer sinusförmigen Spannung A mit definierter Frequenz f_A versteht man eine sinusförmige Spannung B, deren Frequenz fB ein ganzzahliges Vielfaches der Frequenz f_A darstellt. Die Subharmonischen der Frequenz f_A sind also die Frequenzen $2f_A$, $3f_A$, $4f_A$ usw. Die N-fache der Ausgangsfrequenz wird in der Funktechnik als Nte Harmonische (Nte Oberwelle) bezeichnet, die Ausgangsfrequenz selbst wird als Grundwelle oder erste Harmonische bezeichnet.

Prinzipiell erzeugt jeder Zweipol mit nichtlinearer Charakteristik Harmonische zur Grundschwingung. Bei *nichtlinearen Widerständen* wird aber Energie verbraucht, sodass nur ein geringer Teil der Grundwellenleistung in die Oberschwingung umgesetzt wird. Unter günstigsten Bedingungen ist bei der Vervielfachung von f auf n·f der Wirkungsgrad $\eta = 1/n^2$. Benutzt man zur Vervielfachung hingegen nichtlineare Energiespeicher, hat man im Idealfall keine Verluste [fleckner].

Zur Frequenzvervielfachung eignen sich *Kapazitätsdioden* als nichtlineare Energiespeicher besonders gut. Anzahl und Stärke der entstehenden Harmonischen werden durch das *Dotierungsprofil* bzw. die Steilheit der Kennlinie der Kapazitätsdiode bestimmt. Ein Maß für die Steilheit (= Kapazitäts-Spannungs-Kennlinie) ist der Exponent n (auch γ). Dieser beträgt für einfach diffundierte Dioden 0,33 (z. B. BA110), für legierte Dioden 0,5 und für Tuner Dioden mit hyperabruptem PN-Übergang etwa 0,75 (z. B. BB 141) [itt75].

Legierte Kapazitätsdioden weisen einen quadratischen Verlauf der Kapazitäts-Spannungs-Kennlinie auf und eignen sich deshalb vor allem zum Verdoppeln von Frequenzen. Mit einfach diffundierten Kapazitätsdioden lassen sich sehr gut höhere Harmonische erzeugen [fleckner].

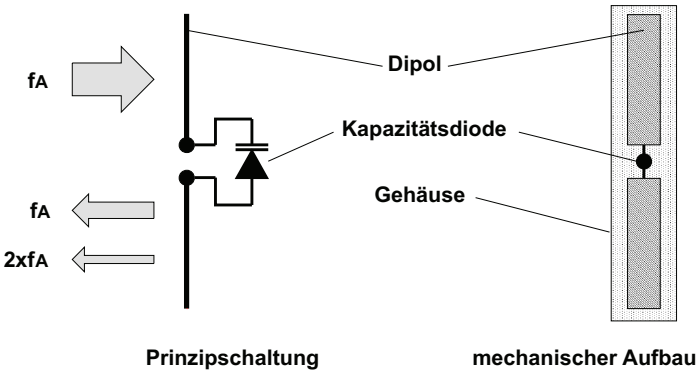


Abb. 3.5 Prinzipschaltbild und typische Bauform eines Mikrowellen-Etiketts.

Der Aufbau eines 1-bit-Transponders zur Erzeugung von Harmonischen ist ausgesprochen einfach: An den Fußpunkt eines auf die Grundwelle abgeglichenen *Dipols* wird eine Kapazitätsdiode geschaltet. Bei einer Grundwellenfrequenz von 2,45 GHz ergibt sich für den Dipol eine Gesamtlänge von 6 cm. Als Grundwellenfrequenz werden 915 MHz (außerhalb Europa), 2,45 GHz oder 5,6 GHz verwendet. Befindet sich der Transponder in der Strahlungskeule des Senders, so werden durch den Stromfluss in der Diode Harmonische der Grundwelle erzeugt und wieder abgestrahlt. Besonders ausgeprägte Signale erhält man je nach verwendetem Diodentyp auf der 2-fachen oder 3-fachen der Grundwelle.

In Kunststoff vergossene Transponder dieser Bauart (Hartetiketten) werden vor allem zur Sicherung von Textilien eingesetzt. An der Kasse werden die Etiketten beim Bezahlen abgenommen und wiederverwendet.

In Abbildung 3.6 wird ein Transponder in die Strahlungskeule eines Mikrowellensenders mit 2,45 GHz gebracht. Die an der Diodenkennlinie des Transponders erzeugte zweite Harmonische von 4,90 GHz wird wieder abgestrahlt und von einem Empfänger detektiert, der auf genau diese Frequenz abgeglichen wurde. Das Eintreffen eines Signals auf Frequenz der zweiten Harmonischen kann dann zum Beispiel das Auslösen einer Alarmanlage bewirken.

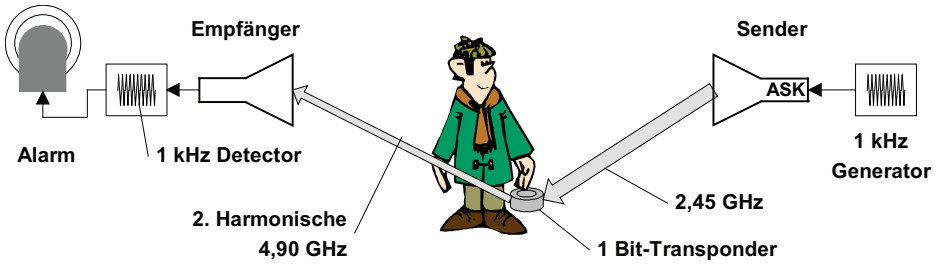


Abb. 3.6 Mikrowellen-Etikett im Ansprechbereich eines Detektors.

Wird die Grundwelle in ihrer Amplitude oder Frequenz moduliert (ASK, FSK), so ist dieselbe Modulation auch in allen Harmonischen enthalten. Dies kann zur Unterscheidung von „Stör"- und „Nutz"-Signalen eingesetzt werden, womit sich Fehlalarme durch Fremdsignale weitestgehend ausschließen lassen. In obigem Beispiel modulieren wir die Amplitude der Grundwelle mit einem Signal von 1 kHz (100% ASK). Auch die am Transponder entstandene 2. Oberwelle ist mit 1 kHz ASK moduliert. Im Empfänger wird das Empfangssignal demoduliert und einem 1-kHz-Detektor zugeführt. Zufällig auftretende Störsignale auf der Empfangsfrequenz 4,90 GHz können dann keinen Fehlalarm auslösen, da diese in der Regel nicht oder anders moduliert sind.

3.1.3 Frequenzteiler

Dieses Verfahren arbeitet im Langwellenbereich bei 100 ... 135,5 kHz. Die Sicherungsetiketten enthalten eine *Halbleiterschaltung* (*Mikrochip*) sowie eine *Schwingkreisspule* aus gewickeltem Kupferlack. Mit einer angelöteten Kapazität wird der Schwingkreis auf der Arbeitsfrequenz des EAS-Systems in Resonanz gebracht. Diese Transponder sind als *Hartetiketten* (Kunststoff) erhältlich und werden beim Kauf von der Ware entfernt.

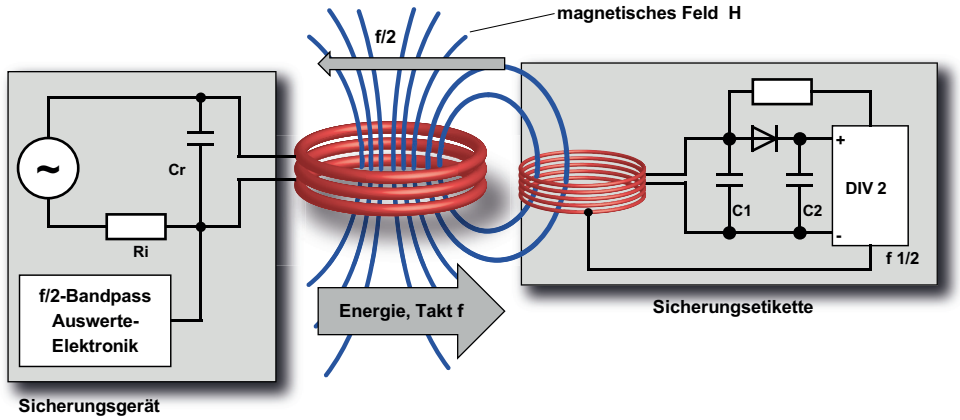


Abb. 3.7 Prinzipschaltbild des EAS-Frequenzteiler-Verfahrens: Sicherungsetikette (Transponder) und Detektor (Auswertegerät).

Der Mikrochip des Transponders wird durch die aus dem magnetischen Feld des Sicherungsgeräts ausgekoppelte Energie mit Betriebsspannung versorgt (siehe Kapitel 3.2.1.1 „Energieversorgung passiver Transponder“, S. 47). Die an der Schwingkreisspule anliegende Frequenz wird vom Mikrochip durch 2 geteilt und zum Sicherungsgerät zurückgesendet. Die Einspeisung des frequenzhalbierten Signals erfolgt an einer Anzapfung der Schwingkreisspule.

Um die Auswertequote zu verbessern, wird das magnetische Feld des Sicherungsgeräts mit niedriger Frequenz gepulst (ASK-moduliert). Wie bei der Erzeugung von Harmonischen, so bleibt auch bei der halbierten Frequenz (*Subharmonische*) die Modulation der Grundwelle (ASK oder FSK) erhalten. Dies wird zur Unterscheidung von „Stör“- und „Nutz“-Signalen eingesetzt. Fehlalarme treten bei diesen Systemen daher kaum auf.

Als Sensor-Antennen werden Rahmenantennen eingesetzt, wie sie von den RF-Systemen her bereits bekannt sind.

Tabelle 3.3: Typische Systemparameter [plotzke].

Frequenz:	130 kHz
Modulationsart:	100% ASK
Modulationsfrequenz/-signal:	12,5 Hz oder 25 Hz, Rechteck 50%

3.1.4 Elektro-Magnetisch

Elektro-magnetische Verfahren arbeiten mit starken magnetischen Feldern im *NF-Bereich* von 10 Hz bis etwa 20 kHz. In den Sicherungsmitteln befindet sich ein weichmagnetischer *amorpher Metallstreifen* mit einer steilflankigen *Hysteresekurve* (siehe hierzu Kapitel 4.1.12 „Magnetische Werkstoffe“, S. 132). In einem starken magnetischen Wechselfeld wird dieser Streifen periodisch ummagnetisiert und bis in die magnetische Sättigung geführt. Das stark unlineare Verhältnis zwischen angelegter Feldstärke H und magnetischer Flussdichte B nahe der Sättigung (siehe hierzu Abbildung 4.56 auf Seite 132) sowie der sprunghafte Wechsel der Flussdichte B nahe dem Nulldurchgang der angelegten Feldstärke H erzeugen Harmonische der Grundfrequenz des Sicherungsgeräts, die von diesem empfangen und ausgewertet werden können.

Eine Optimierung des elektro-magnetischen Verfahrens besteht darin, dem Hauptsignal zusätzlich Signalanteile mit höherer Frequenz zu überlagern. Durch die starke Unlinearität der Hysteresekurve im Streifen entstehen dadurch, zusätzlich zu den Harmonischen, Signalanteile mit Summen- und Differenzfrequenzen der eingespeisten Signale. Bei einem Hauptsignal der Frequenz f_H=20 Hz und den Zusatzsignalen f_1=3,5 und f_2=5,3 kHz entstehen folgende Signale (1. Ordnung):

$f_1+f_2 = f_{1+2} = 8{,}80$ kHz
$f_1-f_2 = f_{1-2} = 1{,}80$ kHz
$f_H+f_1 = f_{H+1} = 3{,}52$ kHz und so weiter ...

Das Sicherungsgerät reagiert hier nicht auf die Harmonischen der Grundfrequenz, sondern auf die Summen- oder Differenzfrequenz der Zusatzsignale.

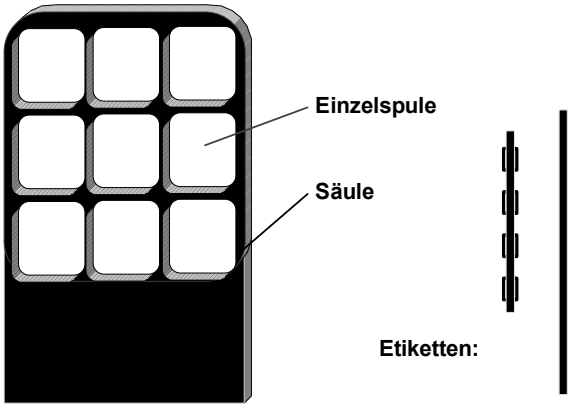


Abb. 3.8 *links:* Typische Antennenbauform der Sicherungsanlage (Höhe ca 1,40 m); *rechts:* Mögliche Bauformen von Etiketten.

Die Sicherungsmittel sind als Etiketten in Form selbstklebender Streifen von einigen cm bis 20 cm Länge erhältlich. Aufgrund der extrem niedrigen Arbeitsfrequenzen eignen sich elektro-magnetische Systeme als einzige für metallhaltige Waren. Nachteilig wirkt sich jedoch die Lageabhängigkeit der Etiketten aus: Für eine sichere Detektion müssen die magnetischen Feldlinien des Sicherungsgeräts senkrecht durch den amorphen Metallstreifen laufen.

Abb. 3.9 Elektro-magnetische Etiketten im Einsatz. (Foto: Schreiner Codedruck, München)

Zur Deaktivierung sind die Etiketten mit einer hartmagnetischen Metallschicht umgeben oder partiell mit hartmagnetischen Plättchen bedeckt. An der Kasse werden die Sicherungsmittel deaktiviert, indem die Kassiererin mit einem starken *Permanentmagneten* den Metall-

streifen entlangfährt [plotzke]. Hierdurch werden die hartmagnetischen Metallplättchen magnetisch. Dabei sind die Metallstreifen so ausgelegt, dass die Remanenzfeldstärke (siehe hierzu Kapitel 4.1.12 „Magnetische Werkstoffe“, S. 132) der Metallplättchen ausreicht, um den amorphen Metallstreifen in der Sättigung zu halten, sodass das magnetische Wechselfeld der Sicherungsanlage nicht mehr wirksam werden kann.

Durch Entmagnetisierung können die Etiketten jederzeit wieder reaktiviert werden. Der Prozess der De- und Reaktivierung ist beliebig oft durchführbar. Aus diesem Grunde lag das Haupteinsatzgebiet der elektro-magnetischen Warensicherung ursprünglich bei Leihbibliotheken. Wegen der kleinen (mind. 32 mm kurze Streifen) und preiswerten Etiketten werden diese Systeme zunehmend auch im Lebensmitteleinzelhandel eingesetzt.

Um die erforderlichen Feldstärken zur Ummagnetisierung der Permalloy-Streifen zu erreichen, wird das Feld von zwei Spulensystemen in den Säulen zu beiden Seiten des schmalen Durchgangs erzeugt. In den beiden Säulen sind mehrere Einzelspulen, typischerweise 9 bis 12, die in der Mitte schwächere und außen stärkere Magnetfelder generieren [plotzke]. Damit sind heute Schleusenbreiten bis zu 1,50 m realisierbar, wobei noch Detektionsraten von 70% erreicht werden [gillert].

Abb. 3.10 Praktische Ausführung einer Antenne für Artikelsicherungssysteme. (Foto: METO EAS-System 2200, Esselte Meto, Hirschborn)

Tabelle 3.4: Typische Systemparameter [plotzke].

Frequenz	70 Hz
optionale Mischfrequenzen verschiedener Anlagen	21 Hz, 215 Hz, 3,3 kHz, 5 kHz
Feldstärke H_{eff} im Detektionsbereich	25 .. 120 A/m
minimale Feldstärke zur Deaktivierung	16000 A/m

3.1.5 Akustomagnetisch

Die Sicherungsmittel akustomagnetischer Systeme bestehen aus kleinen Kunststoffboxen, die etwa 40 mm lang, je nach Ausführung etwa 8 bis 14 mm breit und einen knappen Millimeter hoch sind. In dieser Box befinden sich zwei Metallstreifen, ein *hartmagnetischer Metallstreifen*, der fest mit der Plastikbox verbunden ist, sowie ein Streifen aus *amorphem Metall*, der so gelagert wird, dass er mechanisch frei schwingen kann [zechbauer].

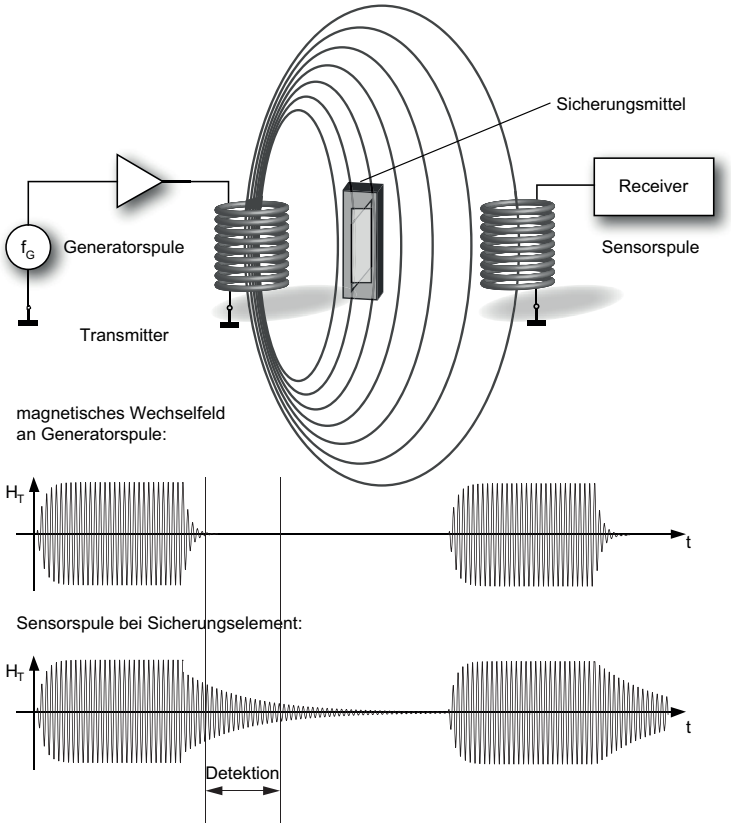


Abb. 3.11 Akustomagnetisches System bestehend aus Sender und Detektionsgerät (Receiver). Befindet sich ein Sicherungsmittel im Feld der Generatorspule, so schwingt dieses nach den Pulsen der Generatorspule wie eine Stimmgabel aus. Das Ausschwingverhalten kann von einem Auswertegerät detektiert werden.

Ferromagnetische Metalle (Nickel, Eisen, usw.) verändern in einem magnetischen Feld unter dem Einfluss der Feldstärke H ihre Länge in einem geringen Maße. Dieser Effekt wird als *Magnetostriktion* bezeichnet und ergibt sich aus einer geringfügigen Änderung des Atomabstandes durch die Magnetisierung. In einem magnetischen Wechselfeld schwingt ein magnetostriktiver Metallstreifen longitudinal mit der Frequenz des Feldes. Entspricht die Frequenz des magnetischen Wechselfeldes der (akustischen) Resonanzfrequenz des Metallstreifens, so wird die Amplitude der Schwingung besonders groß. Bei amorphen Metallen ist dieser Effekt besonders ausgeprägt.

Entscheidend ist nun, dass der magnetostriktive Effekt auch umkehrbar ist. Dies bedeutet, dass von einem schwingenden magnetostriktiven Metallstreifen ein magnetisches Wechselfeld ausgesendet wird. *Akustomagnetische Sicherungssysteme* sind nun so ausgelegt, dass die Frequenz des erzeugten magnetischen Wechselfeldes mit den Resonanzfrequenzen der Metallstreifen in den Sicherungsmitteln exakt übereinstimmt. Der amorphe Metallstreifen beginnt unter dem Einfluss des angelegten Magnetfeldes zu schwingen. Wird das magnetische Wechselfeld nach einiger Zeit abgeschaltet, so schwingt der angeregte Metallstreifen wie eine Stimmgabel noch eine gewisse Zeit weiter und erzeugt dabei selbst ein magnetisches Wechselfeld, das von der Sicherungsanlage leicht detektiert werden kann.

Tabelle 3.5: Typische Betriebsparameter akustomagnetischer Systeme [VDI4471].

Parameter	typischer Wert
Resonanzfrequenz f_0	58 kHz
Frequenztoleranz	± 0,52%
Gütefaktor Q	> 150
minimale Feldstärke zur H_A zur Aktivierung	> 16.000 A/m
Einschaltdauer des Feldes	2 ms
Feldpause (Ausschaltdauer)	20 ms
Ausschwingvorgang des Sicherungsmittels	5 ms

Der große Vorteil dieses Verfahrens besteht darin, dass die Sicherungsanlage während der Zeit, in der das Sicherungsmittel antwortet, selbst nicht sendet und die Detektionsempfänger somit entsprechend empfindlich ausgelegt werden können.

Im aktivierten Zustand sind akustomagnetische Sicherungsmittel magnetisiert, d. h., der eingangs erwähnte hartmagnetische Metallstreifen weist eine hohe Remanenzfeldstärke auf und bildet somit einen Dauermagneten. Um das Sicherungsmittel zu deaktivieren, muss der hartmagnetische Metallstreifen entmagnetisiert werden. Dies verstimmt die Resonanzfrequenz des amorphen Metallstreifens, sodass dieser durch die Ansprechfrequenz der Sicherungsanlage nicht mehr angeregt werden kann. Das Entmagnetisieren des hartmagnetischen Metallstreifens kann nur durch ein in der Feldstärke langsam abklingendes, starkes magnetisches Wechselfeld erfolgen. Die Manipulation der Sicherungsmittel durch vom Kunden mitgebrachte Dauermagneten ist somit sicher ausgeschlossen.

3.2 Voll- und Halbduplexverfahren

Im Gegensatz zu den 1-bit-Transpondern, welche meist durch die Anwendung einfacher physikalischer Effekte (Anschwingvorgänge, Anregung von harmonischen Verfahren mit Hilfe der unlinearen Kennlinien von Dioden oder an der unlinearen Hysteresekurve von Metallen) realisiert werden, verwenden die in diesem und dem folgenden Kapitel beschriebenen Transponder einen elektronischen Mikrochip als Datenträger. Auf diesem Datenträger können Datenmengen von wenigen Bytes bis hin zu einigen MByte gespeichert werden. Um die Datenträger auszulesen oder zu beschreiben, müssen Daten vom Lesegerät an den Transponder und auch zurück vom Transponder an das Lesegerät übertragen werden können. Hierbei kommen zwei grundsätzlich unterschiedliche Verfahren zum Einsatz: Voll- und Halbduplexverfahren, die in diesem Kapitel beschrieben sind, sowie sequentielle Systeme, die im nachfolgenden Kapitel beschrieben werden.

Findet die Datenübertragung von Transponder in Richtung Lesegerät zeitversetzt mit der Datenübertragung vom Lesegerät zum Transponder statt, so bezeichnet man dies als *Halbduplexverfahren* (HDX). Bei Frequenzen unter 30 MHz wird zur Datenübertragung vom Transponder zum Lesegerät am häufigsten das Verfahren der Lastmodulation mit und ohne Hilfsträger eingesetzt, welches auch schaltungs-technisch sehr einfach zu realisieren ist. Damit eng verwandt ist das aus der Radartechnik bekannte Verfahren des modulierten Rückstrahlquerschnitts, welches auf Frequenzen über 100 MHz zum Einsatz kommt. Lastmodulation und modulierter Rückstrahlquerschnitt beeinflussen unmittelbar das durch das Lesegerät erzeugte magnetische oder elektromagnetische Feld, und werden deshalb auch zu den „*harmonischen*“ Verfahren gezählt.

Findet die Datenübertragung vom Transponder in Richtung Lesegerät (Uplink) zeitgleich mit der Datenübertragung vom Lesegerät zum Transponder (Downlink) statt, so bezeichnet man dies als *Vollduplexverfahren* (FDX). Dabei kommen Verfahren zum Einsatz, bei denen die Daten des Transponders auf Teilfrequenzen des Lesegeräts, also einer *subharmonischen*, oder auf einer davon völlig unabhängigen, also *anharmonischen* Frequenz zum Lesegerät übertragen werden.

Zur Datenübertragung vom Lesegerät zum Transponder (Downlink) werden bei Voll- und Halbduplexsystemen unabhängig von der Arbeitsfrequenz oder dem Kopplungsverfahren alle bekannten Verfahren der digitalen Modulation eingesetzt. Man unterscheidet zwischen drei grundsätzlichen Verfahren:

- *ASK*: Amplitude Shift Keying
- *FSK*: Frequency Shift Keying
- *PSK*: Phase Shift Keying

Wegen der einfachen Demodulationsmöglichkeit und der damit verbundenen einfacheren Schaltungstechnik im Transponder, verwendet die überwiegende Mehrheit der Systeme eine ASK-Modulation zur Datenübertragung an den Transponder.

FSK ist theoretisch möglich, dem Autor ist derzeit jedoch kein RFID-System bekannt, bei welchem FSK auf der Downlink kommerziell eingesetzt würde.

Auch PSK gewinnt erst in jüngster Zeit an Bedeutung. So wurde in der Standardisierung für *ISO/IEC 14443* in 2011 ein Projekt gestartet, um mit PSK-Modulationsverfahren in Zukunft Bitraten von 10 MBit/s und höher auf dem Downlinkkanal zu ermöglichen. ASK wird bei ISO/IEC 14443 für Bitraten von 106 kBit/s bis hin zu 6,78 MBit/s eingesetzt.

Das wichtigste gemeinsame Merkmal der Voll- und Halbduplexsysteme besteht darin, dass die Energieübertragung vom Lesegerät zum Transponder kontinuierlich, also unabhängig von der Datenübertragungsrichtung stattfindet. Im Gegensatz dazu findet bei den sequentiellen Systemen (SEQ) die Energieübertragung vom Transponder zum Lesegerät immer nur für eine begrenzte Zeitspanne statt (Pulsbetrieb → *gepulste Systeme*). Die Datenübertragung vom Transponder zum Lesegerät wird in den Pausen zwischen der Energieversorgung des Transponders durchgeführt.

Leider konnte man sich in der Literatur über RFID-Systeme nie auf eine einheitliche Nomenklatur für diese Systemvarianten einigen. Vielmehr ist eine verwirrende und uneinheitliche Zuordnung einzelner Systeme zu Voll- und Halbduplexsystemen üblich. So werden gepulste Systeme häufig als Halbduplexsysteme bezeichnet – dies ist aus Sicht der Datenübertragung zunächst richtig –, alle ungepulsten Systeme werden aber gleichzeitig fälschlicherweise den Vollduplexsystemen zugeordnet. In diesem Buch werden deshalb gepulste Systeme – zur Unterscheidung von anderen Verfahren und entgegen der üblichen RFID-Literatur(!) – als sequentielle Systeme (SEQ) bezeichnet.

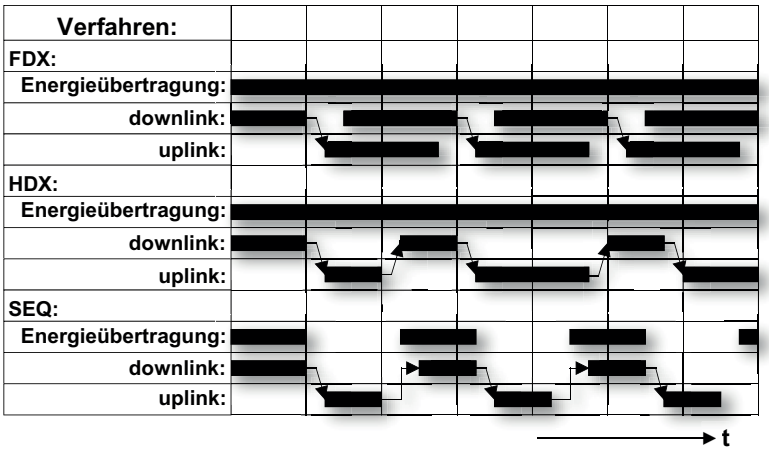


Abb. 3.12 Darstellung der zeitlichen Abläufe bei Voll-, Halbduplex- und sequentiellen Systemen. Die Datenübertragung vom Lesegerät zum Transponder wird in der Abbildung als downlink, die Datenübertragung vom Transponder zum Lesegerät als uplink bezeichnet.

3.2.1 Induktive Kopplung

3.2.1.1 Energieversorgung passiver Transponder

Ein induktiv gekoppelter Transponder besteht aus einem elektronischen Datenträger, meist einem einzelnen Mikrochip, sowie einer großflächigen Spule oder Leiterschleife, welche als Antenne dient.

Induktiv gekoppelte Transponder werden fast ausschließlich passiv betrieben. Dies bedeutet, dass die gesamte zum Betrieb des Mikrochips notwendige Energie durch das Lesegerät zur Verfügung gestellt werden muss. Von der Antennenspule des Lesegeräts wird dazu ein starkes hochfrequentes, elektromagnetisches Feld erzeugt, welches den Querschnitt der Spulenfläche und den Raum um die Spule durchdringt. Da die Wellenlänge der verwendeten Frequenzbereiche (< 135 kHz: 2400 m, 13,56 MHz: 22,1 m) um ein Vielfaches größer ist als die Entfernung zwischen Leser-Antenne und Transponder, darf das elektromagnetische Feld im Abstand des Transponders zur Antenne mathematisch noch als einfaches magnetisches Wechselfeld behandelt werden (Weiteres dazu kann dem Kapitel 4.2.1.1 „Übergang vom Nah- zum Fernfeld bei Leiterschleifen“, S. 138 entnommen werden).

Ein geringer Teil des von der Antenne des Lesegeräts erzeugten magnetisches Feldes durchdringt dabei auch die Antennenspule des Transponders, der sich in einiger Entfernung zur Spule des Lesegeräts befindet. Durch Induktion wird dadurch an der Antennenspule des Transponders eine Spannung U_i erzeugt. Die induzierte Spannung wird gleichgerichtet und dient der Energieversorgung des Datenträgers (Mikrochip).

Der Antennenspule des Lesegeräts wird ein Kondensator C_r parallelgeschaltet, dessen Kapazität so gewählt wird, dass zusammen mit der Spuleninduktivität der Antennenspule ein Parallelschwingkreis gebildet wird, dessen Resonanzfrequenz der Sendefrequenz des Lesegeräts entspricht. Durch den Effekt der Resonanzüberhöhung im Parallelschwingkreis können in der Antennenspule des Lesegeräts sehr hohe Ströme erreicht werden, womit die notwendigen Feldstärken auch zum Betrieb entfernter Transponder erzeugt werden können.

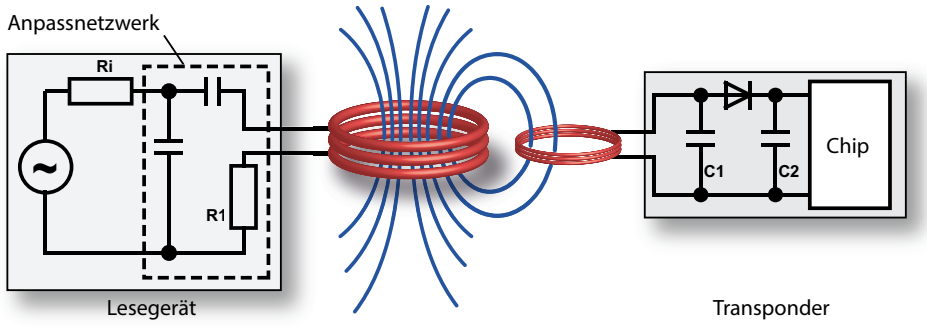


Abb. 3.13 Spannungsversorgung eines induktiv gekoppelten Transponders aus der Energie des magnetischen Wechselfeldes, das vom Lesegerät erzeugt wird.

Die Antennenspule des Transponders bildet zusammen mit dem Kondensator C1 ebenfalls einen Schwingkreis, welcher in etwa auf die Sendefrequenz des Lesegeräts abgestimmt wird. Durch Resonanzüberhöhung im Parallelschwingkreis erreicht die Spannung U_i an der Transponderspule ein Maximum.

Die Anordnung der beiden Spulen kann auch als Transformator interpretiert werden (*transformatorische Kopplung*), wobei zwischen den beiden Windungen nur eine sehr schwache Kopplung besteht. Der Wirkungsgrad der Leistungsübertragung zwischen der Antennenspule des Lesegeräts und dem Transponder ist proportional der Arbeitsfrequenz f, der Windungszahl n der Transponderspule, der umschlossenen Fläche A der Transponderspule, dem Winkel der beiden Spulen zueinander sowie der Entfernung zwischen den beiden Spulen.

Abb. 3.14 Verschiedene Bauformen induktiv gekoppelter Transponder. Dargestellt sind Transponder-Halbzeuge, also Transponder vor dem Einspritzen in ein Kunststoffgehäuse.
(Foto: AmaTech GmbH & Co. KG, Pfronten)

Mit zunehmender Frequenz f nimmt die benötigte Spuleninduktivität der Transponderspule und damit auch die Windungszahl „n“ ab (135 kHz: typisch 100 ... 1000 Windungen, 13,56 MHz: typisch 3 ... 10 Windungen). Da die im Transponder induzierte Spannung jedoch proportional der Frequenz f ist (siehe hierzu Kapitel 4.1.7 „Resonanz“, S. 90), wirkt sich die geringere Windungszahl bei höheren Frequenzen in der Praxis auf den Wirkungsgrad der Leistungsübertragung kaum aus.

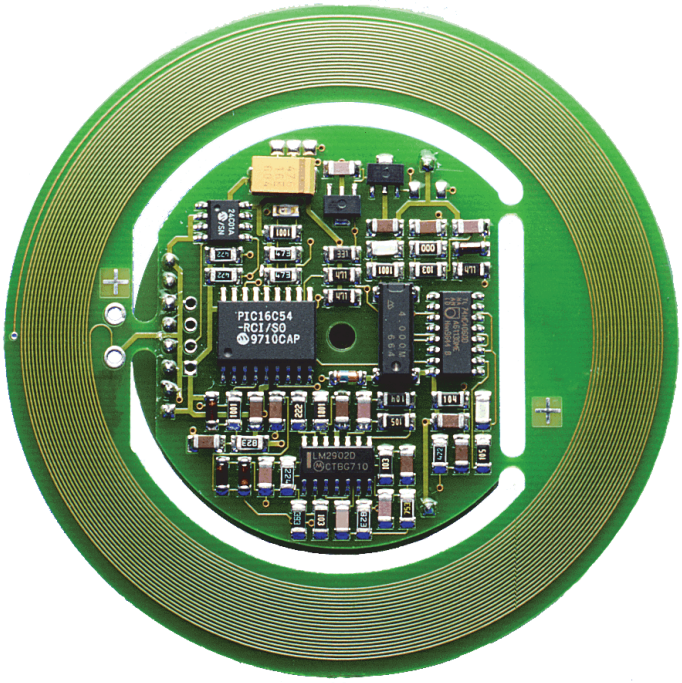


Abb. 3.15 Lesegerät für induktiv gekoppelte Transponder im Frequenzbereich < 135 kHz mit integrierter Antenne. (Foto: easy-key System, micron, Halbergmoos)

3.2.1.2 Datenübertragung Transponder > Lesegerät

3.2.1.2.1 Lastmodulation

Wie bereits gezeigt, besteht bei induktiv gekoppelten Systemen eine *transformatorische Kopplung* zwischen der primären Spule im Lesegerät und der sekundären Spule im Transponder. Dies gilt, solange der Abstand zwischen den Spulen nicht größer als $(\lambda/2\pi)$ 0,16 λ wird, sodass sich der Transponder im *Nahfeld* der Sendeantenne befindet (eine nähere Erklärung zur Definition des Nah- und Fernfeldes siehe Kapitel 4.2.1.1 „Übergang vom Nah- zum Fernfeld bei Leiterschleifen“, S. 138).

Wird ein resonanter Transponder (d. h. die Eigenresonanzfrequenz des Transponders entspricht der Sendefrequenz des Lesegeräts) in das magnetische Wechselfeld der Antenne des Lesegeräts gebracht, so entzieht dieser dem magnetischen Feld Energie. Die dadurch hervorgerufene Rückwirkung des Transponders auf die Antenne des Lesegeräts kann als *transformierte Impedanz* Z_T in der Antennenspule des Lesegeräts dargestellt werden. Das Ein- und Ausschalten eines *Lastwiderstands* an der Antenne des Transponders bewirkt eine Veränderung der Impedanz Z_T und damit Spannungsänderungen an der Antenne des Lesegeräts (siehe Kapitel 4.1.10.3 „Lastmodulation“, S. 115). Dies entspricht in der Wirkung einer Amplitudenmodulation der Spannung U_L an der Antennenspule des Lesegeräts durch den entfernten Transponder. Steuert man das An- und Ausschalten des Lastwiderstands durch

Daten, so können diese Daten vom Transponder zum Lesegerät übertragen werden. Diese Form der Datenübertragung wird als *Lastmodulation* bezeichnet.

In der Praxis zeigt sich, dass der Phasenwinkel der transformierten Impedanz vom Phasenwinkel des Stromes in der Transponderantenne, und damit von der genauen Resonanzfrequenz des Transponderschwingkreises abhängt. Je nach Phasenwinkel der transformierten Impedanz kann eine Lastmodulation eine „positive“ oder „negative“ Amplitudenmodulation, eine reine Phasenmodulation, oder eine Mischung davon, an der Antennenspule des Lesegeräts erzeugen. Hinzu kommt, dass vereinzelt auch kapazitive Lastmodulation, also die Umschaltung der Resonanzfrequenz des Transponders, verwendet wird.

Zur Rückgewinnung der Daten im Lesegerät wird eine an der Antenne des Lesegeräts abgegriffene Spannung gleichgerichtet. Dies entspricht der Demodulation eines amplitudenmodulierten Signals. Ein Schaltungsbeispiel hierfür kann dem Kapitel 11.3.1 „Integriertes HF-Interface“, S. 527 entnommen werden.

Verlässt der Transponder das Nahfeld, also den Bereich $< \lambda/2\pi$ (0,16 λ), so geht mit dem Übergang in das Fernfeld auch die transformatorische Kopplung zwischen der Antenne des Lesegeräts und der Antenne des Transponders verloren. Eine Lastmodulation ist im Fernfeld daher nicht mehr möglich. Dies bedeutet jedoch nicht, dass eine Datenübertragung vom Transponder zum Lesegerät grundsätzlich nicht mehr möglich wäre. Mit dem Übergang ins Fernfeld beginnt der Mechanismus der Backscatter-Kopplung (siehe Kapitel 3.2.2 „Elektromagnetische Backscatter-Kopplung“, S. 58) wirksam zu werden. In der Praxis scheitert eine Datenübertragung zum Lesegerät jedoch in der Regel an dem kleinen Wirkungsgrad der Transponderantennen (d. h. dem geringen Antennengewinn) im Fernfeld.

3.2.1.2.2 Lastmodulation mit Hilfsträger

Auf Grund der geringen Kopplung zwischen Leseantenne und Transponder-Antenne sind die das Nutzsignal darstellenden Spannungsschwankungen an der Antenne des Lesegeräts um Größenordnungen kleiner als die Ausgangsspannung des Lesegeräts. Bei einem 13,56 MHz-System kann in der Praxis, bei einer Antennenspannung von ca. 100V (Spannungsüberhöhung durch Resonanz!) mit einem Nutzsignal von etwa 10 mV gerechnet werden (= 80 dB Nutz/„Störsignal“-Verhältnis). Da diese geringen Spannungsänderungen nur mit einem sehr großen schaltungstechnischen Aufwand zu detektieren sind, macht man sich die durch die Amplitudenmodulation der Antennenspannung entstehenden Modulationsseitenbänder zunutze:

Wird nämlich der zusätzliche Lastwiderstand im Transponder mit sehr hoher Taktfrequenz f_H ein- und ausgeschaltet, so entstehen zwei Spektrallinien im Abstand $\pm f_H$ um die Sendefrequenz des Lesegeräts, die nun leicht detektiert werden können (es muss jedoch $f_H < f_{LESER}$ sein). Im Sprachgebrauch der Funktechnik wird die zusätzlich eingeführte Taktfrequenz als *Hilfsträger* (*Subcarrier*) bezeichnet.

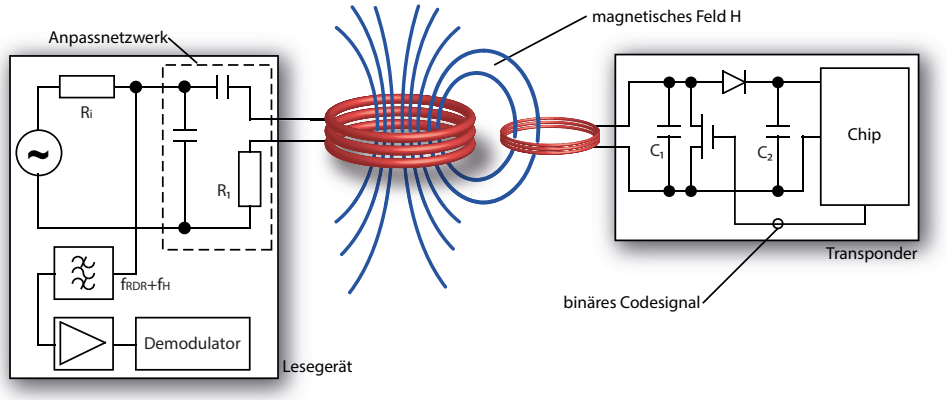


Abb. 3.16 Erzeugung der Lastmodulation im Transponder durch Umschalten des Drain-Source-Widerstandes eines FET auf dem Chip. Das abgebildete Lesegerät ist für die Detektion eines Hilfsträgers ausgelegt.

Um nun Daten an das Lesegerät zu übertragen, wird der *Hilfsträger* selbst im Takt des Datenflusses moduliert. Der Lastwiderstand im *Lastmodulator* wird nun im Takt des modulierten Hilfsträgers ein- und ausgeschaltet. Als Modulationsverfahren für den Hilfsträger werden ASK- (z. B. ISO/IEC 14443 Typ A: On-Off keying), FSK- (z. B. ISO/IEC 15693: Umtastung zwischen den beiden Hilfsträgerfrequenzen 424 kHz und 485 kHz) oder PSK-Modulation (z. B. ISO/IEC 14443 Typ B: 2-PSK oder BPSK) eingesetzt.

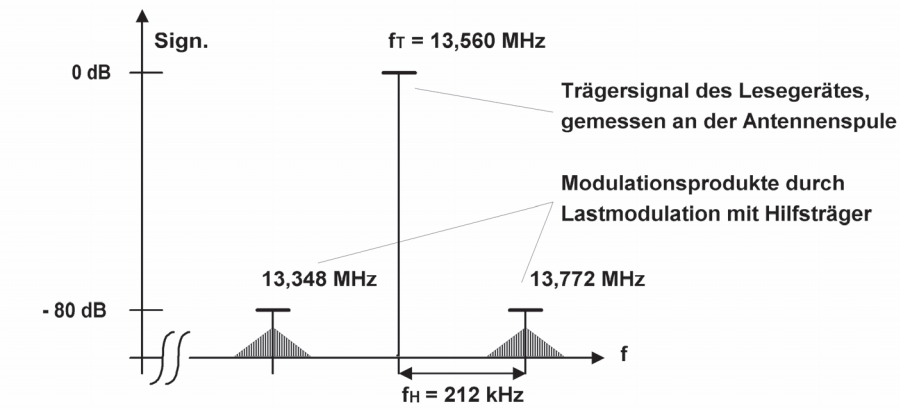


Abb. 3.17 Durch Lastmodulation mit Hilfsträger entstehen zwei Seitenbänder im Abstand der Hilfsträgerfrequenz f_H um die Sendefrequenz des Lesegeräts. Die eigentliche Information steckt in den Seitenbändern der beiden Hilfsträgerseitenbänder, welche durch die Modulation des Hilfsträgers selbst entstehen.

Durch Lastmodulation mit Hilfsträger entstehen an der Antenne des Lesegeräts zwei Modulationsseitenbänder im Abstand der Hilfsträgerfrequenz um die Arbeitsfrequenz f_{LESER}. Diese Modulationsseitenbänder können durch eine Bandpassfilterung auf einer der beiden Frequenzen $f_{LESER} \pm f_H$ vom wesentlich stärkeren Signal des Lesegeräts getrennt werden.

Nach anschließender Verstärkung ist das Hilfsträgersignal dann sehr einfach zu demodulieren.

Lastmodulation mit Hilfsträger wird fast ausschließlich im Frequenzbereich 13,56 MHz eingesetzt. Typische Hilfsträgerfrequenzen sind 212 kHz, 424 kHz (z.B. ISO/IEC 15693) und 848 kHz (z.B. ISO/IEC 14443).

3.2.1.2.3 Schaltungsbeispiel – Lastmodulation mit Hilfsträger

Ein Beispiel für die schaltungstechnische Realisierung eines Transponders mit Lastmodulation mit Hilfsträger ist in Abbildung 3.18 gezeigt. Die Schaltung ist für eine Arbeitsfrequenz von 13,56 MHz ausgelegt und erzeugt einen Hilfsträger von 106 kHz.

Die an der Antennenspule L_1 durch das magnetische Wechselfeld des Lesegeräts induzierte Spannung wird mit dem Brückengleichrichter (D_1 ... D_4) gleichgerichtet und steht nach zusätzlicher Glättung (C_1) der Schaltung als Versorgungsspannung zur Verfügung. Mit dem Parallelregler (ZD 5V6) wird das unbegrenzte Ansteigen der Versorgungsspannung bei Annäherung des Transponders an die Leserantenne verhindert.

Über den Vorwiderstand (R_1) gelangt ein Teil der hochfrequenten Antennenspannung (13,56 MHz) an den Takteingang (CLK) des Frequenzteilers (IC1) und dient dem Transponder als Basis zur Erzeugung eines internen Taktsignals. Nach einer Teilung durch 2^7 (=128) steht an Ausgang Q7 ein Hilfsträger-Taktsignal von 106 kHz zur Verfügung. Das Hilfsträger-Taktsignal wird, gesteuert durch einen seriellen Datenfluss am Dateneingang (DATA), auf den Schalter (T_1) gegeben. Liegt am Dateneingang (DATA) ein logisches HIGH-Signal, so wird das Hilfsträger-Taktsignal auf den Schalter (T_1) gegeben. Der Lastwiderstand (R_2) wird dann im Takt der Hilfsträgerfrequenz an- und abgeschaltet.

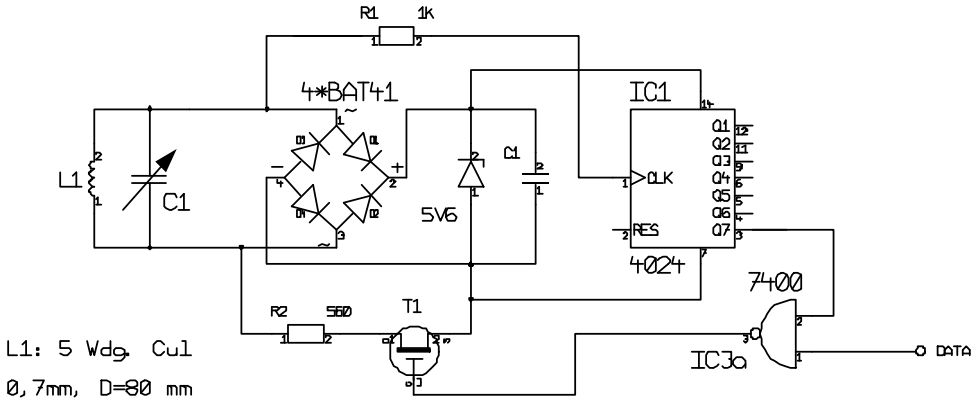


Abb. 3.18 Schaltungsbeispiel für die Erzeugung einer Lastmodulation mit Hilfsträger in einem induktiv gekoppelten Transponder.

Durch die Beschaltung des UND-Gatters (IC3) mit einem beliebigen anderen Ausgang (Q1 .. Q6) des Teilers kann auch eine höhere Hilfsträgerfrequenz (Q6: 212 kHz, Q5: 484 kHz, Q4: 848 kHz, .. Q2: 6,78 MHz) gewählt werden.

Optional lässt sich bei der abgebildeten Schaltung der Transponderschwingkreis mit der Kapazität C_1 auf 13,56 MHz in Resonanz bringen. Die Reichweite dieses „Minimaltransponders“ kann damit deutlich vergrößert werden.

3.2.1.2.4 Aktive Lastmodulation

Die begrenzenden Faktoren eines induktiv gekoppelten RFID-Systems hinsichtlich der *Kommunikationsreichweite* liegen einerseits in der *Energiereichweite* des Lesegeräts, also der Fähigkeit, einen Transponder im Leseabstand mit ausreichend Energie zum Betrieb zu versorgen, sowie anderseits in der Fähigkeit, Daten per Lastmodulation vom Transponder an das Lesegerät zurückzusenden. In beiden Fällen wird eine ausreichend große magnetische Gegenkopplung (mutual magnetic coupling M) zwischen der Antenne des Lesegeräts und der Antenne des Transponders benötigt.

Die physikalischen Parameter eines induktiv gekoppelten RFID-Systems sind zum Beispiel in *ISO/IEC 14443* so definiert, dass sich bei hohen Bitraten (106 .. 868 kBit/s), hohemEnergieverbrauch des Transponderchips (Mikroprozessor mit Smart Card-Betriebssystem) und der Chipkarten-Bauform ID1 eine typische Lesereichweite von 10 cm oder weniger ergibt.

Werden an Stelle der Chipkarten-Bauform ID1 sehr kleine Transponder mit Antennen im Formfaktor einer *SIM-Karte* oder einer *micro-SD Karte* eingesetzt, so sinkt die magnetische Gegenkopplung, und damit die erreichbare Lesereichweite drastisch ab. Soll ein solch kleiner Transponder beispielsweise in ein Mobiltelefon oder in ein PDA eingesetzt werden, um diese mit einem kontaktlosen Interface auszustatten, so führt die kleine Lesereichweite von evtl. nur wenigen Zentimetern schnell zu einem Problem, insbesondere wenn der Transponder bei zusätzlich auftretender Abschirmung (z.B. durch den Akku) schließlich nicht mehr in der Lage ist, die Reichweite zu einem außerhalb befindlichen Lesegerät zu überbrücken.

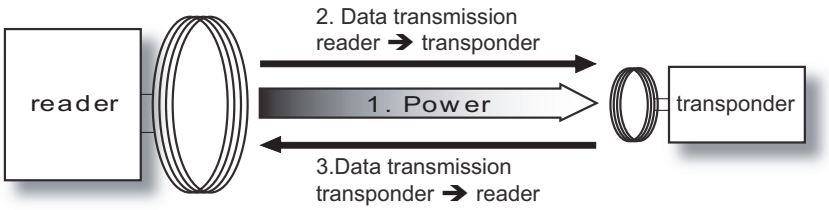


Abb. 3.19 Die die Kommunikationsreichweite begrenzenden Faktoren eines passiven, induktiv gekopplten RFID-Systems.

Um auch mit Transpondern mit sehr kleiner Antennengeometrie akzeptable Lesereichweiten zu erzielen, müssen die eben beschriebenen begrenzenden Faktoren beseitigt werden. Im Falle der Energiereichweite ist das Problem einer zu geringen magnetischen Gegenkopplung einfach zu lösen. Hierzu ist es lediglich notwendig, den Transponder aus einer lokalen Energiequelle (Batterie) mit Strom zu versorgen. Wird der Tansponder in der Bauform einer SIM-Karte oder einer micro-SD Karte in einem Mobiltelefon betrieben, so kann die Energie über einen Anschlusspin direkt im Mobiltelefon zur Verfügung gestellt werden.

Um einen passiven Transponderchip mit Energie zu versorgen, müsste eine Spannung von wenigstens 3 V in der Transponderantenne induziert werden. Bei einem *batteriegestützten Transponder* hingegen wird die in der Antenne induzierte Spannung nicht mehr zur Energieversorgung des Transponderchips verwendet, sondern nur noch dazu, Daten und Kommandos vom Lesegerät zu übertragen. Hierzu reicht aber bereits eine Spannung mit erheblich geringerem Pegel von wenigstens einigen mV aus, da diese einfach verstärkt werden kann. Auf diese Weise kann das Signal des Lesegeräts auch mit kleinsten Transponderantennen und Metallabschirmung auf deutlich größere Entfernung detektiert werden.

Etwas komplexer ist die Optimierung der Datenübertragung vom Transponder zurück zu einem Lesegerät. Die üblicherweise verwendete (passive) Lastmodulation scheidet auch bei einem Transponder mit externer Energieversorgung (aktiver Transponder) aus, da sich ohne eine Verbesserung der magnetischen Kopplung nur eine unwesentliche Verbesserung gegenüber einem passiven (batterielosen) Transponder ergibt. Eine Vergrößerung der magnetischen Kopplung ist aber nur durch die Verringerung des Abstands zwischen den Antennen oder durch eine Vergrößerung der Antennenfläche des Transponders möglich.

Eine Alternative besteht darin, auf anderem Wege ein Signal zu erzeugen, welches im Frequenzspektrum dem Signal einer *passiven Lastmodulation* gleicht, und dieses aktiv (d.h. unter Aufwendung von eigener Energie) an das Lesegerät zu senden. Ein solches Verfahren wird als *aktive Lastmodulation* (active load modulation) bezeichnet. Betrachten wir das durch eine (passive) Lastmodulation an der Antenne des Lesegeräts auftretende Frequenzspektrum, so sind zum Beispiel bei ISO/IEC 14443 neben dem Trägersignal (13,56 MHz) im Abstand der *Hilfsträgerfrequenz* (848 kHz) zwei weitere Spektrallinien (14,408 MHz und 12,712 MHz) zu erkennen, um die sich jeweils zwei Modulationsseitenbänder ausbilden. Die Nutzdaten sind dabei ausschließlich in den Modulationsseitenbändern um die Hilfsträgerlinien enthalten.

Um Daten von einem aktiven Transponder an ein Lesegerät zu senden, würde es ausreichen, die beiden Hilfsträger-Spektrallinien mit den datentragenden Seitenbändern zu erzeugen und an ein Lesegerät zu senden. Das Trägersignal muss dabei nicht übertragen werden; dieses wird vom Lesegerät ohnehin permanent ausgesendet. Ein solches Signal wird als *Zweiseitenband-* oder „*Dual-Side-Band*“ (*DSB*)-Modulation bezeichnet.

Eine Grundschaltung der Nachrichtentechnik, mit der eine solche DSB-Modulation erzeugt werden kann, ist der *Ringmodulator*. Der Ringmodulator wird mit einer Referenzfrequenz fc = 13,56 MHz und dem modulierten Hilfsträger gespeist. Das Ausgangssignal des Ringmodulators ist dann bereits das benötigte DSB-Signal. Dieses wird in einem Verstärker im Pegel angehoben und über die Antenne abgestrahlt.