

Bachelor Wahlpflicht

Technische Informatik,
Telekommunikation



Einführung in Technik und Anwendung von RFID

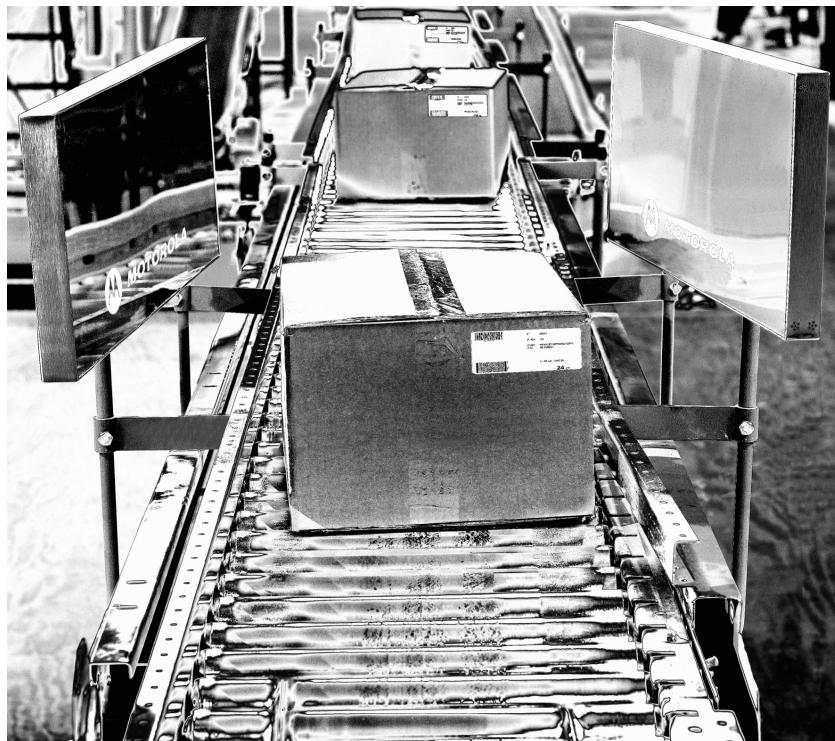


Foto: Motorola, grafische Bearbeitung: R. S. Mayer

Skript zur Vorlesung

Alle Rechte bei ZFH 2008 und R. S. Mayer 2014

nur zum persönlichen Gebrauch – keine Veröffentlichung ohne schriftliche Genehmigung

Ralf S. Mayer

Hochschule Darmstadt h_da – University of Applied Sciences

5. Oktober 2015

Einleitung

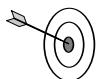
Diese Dokumentation ist die Vorabversion des Skripts¹ für den Bachelor Studiengang am Fachbereich Informatik der Hochschule Darmstadt **h_da** für das Modul

Einführung in die Technik und Anwendung von RFID

gültig ab dem SS 2009.

Im vorliegenden Text werden die folgenden Symbole verwendet:

Die Lernziele einer Einheit werden meist zu Beginn eines Kapitels oder Absatzes hervorgehoben mit mit dem Symbol einer Zielscheibe kenntlich gemacht.



Definition bestimmter Begriffe und Größen werden im Text hervorgehoben und am Rand mit dem in der Mathematik üblichen Symbol versehen.



Wichtige Fakten und Erkenntnisse sind im Text hervorgehoben um sich diese **zu merken**. Wie das Symbol nahelegt, macht es Sinn sich diese zur Wiederholung noch einmal zu notieren.



Hinweis auf beispielsweise Besonderheiten.



Um das Augenmerk auf gewisse Tatsachen zu lenken, werden diese gesondert hervorgehoben und mit dem Symbol für **Achtung** oder **Beachte** kenntlich gemacht. Es sind dies häufig Dinge, welche leicht verwechselt werden können, oder ein besonderer Hinweis im gegebenen Zusammenhang.



¹Diese Skript wurde mit L^AT_EX erstellt. Siehe z.B [ST05, Kop05, MGB⁺⁰⁵]



Beispiel 0.1. Zur Vertiefung eines Sachverhalts werden **Beispiele** gegeben. Auch können mit Beispielen aus anderen Bereichen Querbezüge aufgezeigt werden, welche die Bedeutung erläutern und Wissen und Verständnis festigen.



Zusammenfassung der Fakten, meist am Ende eines Kapitels.



Übung 0.1. **Übungen** sind sowohl im Text zur Vertiefung eines Themas plaziert, als auch zur Wiederholung am Ende eines Kapitels. Übungen sollten stets schriftlich durchgeführt werden. Sie sind Voraussetzung für das Lernen und Behalten des Stoffes und dienen der Selbstkontrolle. Die einzelnen Übungen sind nach Kapitel nummeriert. Die Lösungen zu den einzelnen Aufgaben stehen in einer erweiterten Ausgabe des Werks zur Verfügung.



Experiment 0.1. Experiment Versuch beispielsweise zur Messung von Eigenschaften oder Verhalten eines Bauteils oder Systems



Laborversuch 0.2. Laborversuch Typischer Versuch im Rahmen eines Praktikums, bei dem systematisch Eigenschaften und/oder Verhalten eines Bauteils oder Systems gemessen, ausgewertet, dokumentiert und diskutiert werden sollen.

Für das Dezimaltrennzeichen wird – wie in der Informatik und der englischsprachigen Literatur üblich – statt des **Kommas** der **Dezimalpunkt** verwendet.

Dieses Werk ist ausschließlich für den persönlichen Gebrauch bestimmt.
Kopieren, Vervielfältigen, zugänglich machen für andere als Mitglieder des Fachbereichs Informatik der Hochschule Darmstadt – auch auszugsweise – bedarf der ausdrücklichen schriftlichen Zustimmung des Herausgebers und Autors R. S. Mayer.

Hinweise, Kritik und Anregungen senden Sie bitte an <mailto:r.mayer@fbi.h-da.de>. Der Autor ist Ihnen dafür stets dankbar.

Darmstadt, 5. Oktober 2015

Lernziele

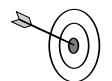
Ziel dieser Vorlesung mit Praktika ist die Einführung in die Technologie der Radiofrequenz-Identifikation (RFID). Dabei sollen die Kenntnisse über die Grundlagen und Funktionsweisen dieses Verfahrens vermittelt werden. Als Schüsseltechnologie bei Logistik- und Warenwirtschaft und zunehmend auch in der Automatisierungstechnik erlangt RFID schnell wachsende Bedeutung in vielen Branchen.

In dieser Lehreinheit soll die Fähigkeit vermittelt werden, die einzelnen RFID-Standards für deren Eignung in unterschiedlichen Anwendungsfällen bewerten und auswählen zu können. Weiterhin werden praktische Aspekte bei der Einbindung von RFID in bestehende informationstechnische Umgebungen wie Softwareanwendungen und Datenbanken in Unternehmen angesprochen. Dabei spielt Kompatibilität, Wartung und Erweiterbarkeit sowie Zukunftssicherheit aus Unternehmenssicht eine wichtige Rolle.

Da Akzeptanz eine entscheidende Rolle spielt, zielt diese Kurseinheit auch auf die Fähigkeit ab, Chancen und Risiken beim Einsatz von RFID unter den verschiedensten Gesichtspunkten objektiv bewerten zu können.

Nach dem Studium dieser Kurseinheit sollen Sie

- *die Grundlagen der drahtlosen Kommunikation über magnetische Felder und elektromagnetische Wellen verstehen*
- *die grundsätzliche Funktionsweise von RFID-Lesegeräten und RFID-Transpondern erläutern können,*
- *Vor- und Nachteile der eingesetzten Frequenzbereiche beschreiben und anhand typischer Anwendungszenarien zuordnen können,*
- *ein Design für eine typische Anwendung in Automatisierung, Logistik oder Warenwirtschaft entwerfen und grundlegende Prozesse skizzieren können,*
- *Aspekte des Datenschutzes, der Sicherheit bezüglich Fälschung und ungewollten Zugriff auf Informationen benennen und bewerten können.*



Lernziele

Inhaltsverzeichnis

Einleitung	i
Lernziele	v
1. Einführung in automatische Identifikationssysteme	1
1.1. Warum Identifikationssysteme	1
1.2. Gängige Identifikationssysteme	3
1.2.1. Barcode	3
1.2.2. Optical Character Recognition	4
1.2.3. Biometrie	4
1.2.4. Chipkarten	4
1.2.5. RFID-Systeme	5
1.2.6. Vergleich einiger Auto-ID-Verfahren	5
1.3. Prinzip von RFID	6
1.4. Transponder oder Tags	7
1.4.1. Passive Tags	7
1.4.2. Aktive Tags	7
1.4.3. Definition passiv – semi-passiv – aktiv	8
1.5. Frequenzbereiche	9
1.6. Typische Anwendungen	9
1.7. Zusammenfassung	10
1.8. Übungen	10
2. Grundlagen	11
2.1. Grundbegriffe Elektrotechnik	11
2.1.1. Spannung, Strom und Felder	11
2.1.2. Leistung	12
2.1.3. Widerstand	13
2.2. Schwingkreis	14
2.3. Maxwell und die Folgen	17
2.4. Induktive oder magnetische Kopplung	18
2.5. Resonanz	20
2.5.1. Resonanzkurve	21
2.5.2. Dämpfung und Gütefaktor	23

2.5.3. Dezibel	24
2.6. Elektromagnetische Wellen	25
2.6.1. Der geöffnete Schwingkreis	25
2.6.2. Lichtgeschwindigkeit, Frequenz und Wellenlänge	27
2.7. Antennen	29
2.7.1. Antennenformen	29
2.7.2. Charakteristik der Abstrahlung	30
2.7.3. Sendeleistung und Gewinn	30
2.7.4. Polarisation	30
2.8. Modulation	32
2.9. Reichweite	33
2.9.1. Reichweite von Feldern und Wellen	34
2.9.2. Absorption	35
2.9.3. Reflexion	35
2.9.4. Echoreichweite	36
2.10. Elektromagnetische Kopplung	37
2.11. RFID-Frequenzen und Eigenschaften	38
2.11.1. Eigenschaften der Frequenzen	38
2.11.2. Frequenzbänder	39
2.12. Zusammenfassung	41
2.13. Übungen	41
3. RFID-Systeme	43
3.1. Normen und Spezifikationen	44
3.1.1. Langwelle LF 125-134 kHz	44
3.1.2. Hochfrequenz HF 13.56 MHz	44
3.1.3. UHF 868 - 915 MHz	46
3.1.4. Elektronischer Produktcode	47
3.1.5. Sensoren	48
3.2. Voll- und Halbduplex-Übertragung	48
3.3. Datenintegrität	49
3.4. Codierung	50
3.5. Zugriffsverfahren - Antikollision	51
3.5.1. Räumliche Trennung	51
3.5.2. Zeitliche Trennung	52
3.5.3. Frequenzmultiplex	53
3.5.4. Codemultiplex	53
3.6. Kollisionserkennung	53
3.7. Antikollisions-Verfahren	54
3.7.1. Reader- und transpondergetriebene Verfahren	55
3.7.2. ALOHA- und Slotted-ALOHA-Verfahren	55

3.7.3. Binäre Suche	56
3.8. Statistische Betrachtung von ALOHA und Slotted-ALOHA	56
3.8.1. Poisson-Statistik	57
3.8.2. ALOHA	58
3.8.3. Slotted-ALOHA	60
3.8.4. Dynamisches Slotted-ALOHA	62
3.9. Zusammenfassung	62
3.10. Übungen	62
4. Anwendungen von RFID	65
4.1. Verbreitete Anwendungen mit RFID	65
4.1.1. Artikel-Diebstahlsicherung	65
4.1.2. Fahrzeug Wegfahrsperrre	66
4.1.3. Tier-Identifikation	66
4.1.4. Personen-Identifikation	67
4.1.5. Geschlossene Systeme	67
4.1.6. Offene Systeme	68
4.1.7. Elektronische Ausweisdokumente	68
4.1.8. Identifikation von Büchern und Akten	69
4.2. RFID in der Automatisierung	69
4.3. Logistikanwendungen	70
4.4. Produktsicherheit und Verbraucherschutz	70
4.5. Mobile Computing und NFC	71
4.5.1. Übersicht	71
4.5.2. Einführung	72
4.5.3. Geschichte	72
4.5.4. Verbreitung von Smartphones	72
4.5.5. Smartphone Betriebssysteme	74
4.5.6. Technologie	75
4.5.7. Anwendungen	75
4.5.8. NFC-Architektur und Spezifikationen	78
4.6. Oberflächenwellen-Transponder	78
4.7. Medizinische Anwendungen mit RFID	79
4.8. Szenario Anwendungsbereiche	80
4.9. Geschäftsmodelle	80
4.10. Zusammenfassung	82
4.11. Übungen	82
5. Systemarchitektur	83
5.1. RFID-Hardware	83
5.1.1. Lesegeräte	83

Inhaltsverzeichnis

5.1.2. Hand-Lesegeräte	84
5.1.3. Stationäre Systeme	84
5.1.4. Tag-Bauformen	84
5.1.5. Netzwerk und Rechner	86
5.2. Architektur	86
5.2.1. Systemarchitektur mit RFID	86
5.2.2. Transponder und RFID-Leser	87
5.2.3. Software Infrastruktur	87
5.3. Zusammenfassung	90
5.4. Übungen	90
6. Kontaktlose Chipkarten	91
6.1. MIFARE classic	91
7. Sicherheit und Datenschutz	93
7.1. Technische Maßnahmen	93
7.1.1. Kryptografie - Kryptologie	94
7.1.2. Authentifizierung	94
7.1.3. Verschlüsselte Datenübertragung	95
7.1.4. Begrenzung der Reichweite	95
7.2. EMV und Gesundheit	95
7.2.1. Thermische Effekte	95
7.2.2. Nicht-thermische Effekte	96
7.2.3. Vorsichtsmaßnahmen bei aktiven medizinischen Implantaten	96
7.2.4. Grenzwerte	96
7.3. Öffentliche Akzeptanz von RFID	96
7.4. Gesetzliche Rahmenbedingungen	97
7.5. Zusammenfassung	98
7.6. Übungen	98
A. Anhang: Lösungen und Hinweise zu Aufgaben	99
A.1. Kapitel 1	99
A.2. Kapitel 2	99
A.3. Kapitel 3	100
A.4. Kapitel 4	100
A.5. Kapitel 5	100
A.6. Kapitel 7	100
Glossar	101
Literatur	107

Literaturempfehlungen **113**

Stichwortverzeichnis **115**

Inhaltsverzeichnis

Tabellenverzeichnis

1.1. Vergleich Auto-ID-Verfahren	6
2.1. RFID-Frequenzen, Wellenlängen und Eigenschaften	28
3.1. ISO/IEC-Standards	45
3.2. EPC globale Standards	46
3.3. EPC Code Typ 1 - Klasse 1	47
4.1. Funktionsweise gängiger RFID-Anwendungen	65
4.2. Worldwide Mobile Device Sales to End Users by Vendor in 3Q12	73
4.3. Worldwide Mobile Device Sales to End Users by Vendor in 2Q15	74
4.4. Worldwide Mobile Device Sales to End Users by Operating System in 3Q12	74
4.5. Worldwide Smartphone OS Market Share	75
4.6. Worldwide Mobile Device Sales to End Users by Operating System in 2Q15	75

Tabellenverzeichnis

Abbildungsverzeichnis

1.1. Kosten von Medienbrüchen	2
1.2. 1- und 2-dimensionale Barcodes	4
1.3. Funktionsweise von RFID	6
2.1. Schwingkreis	14
2.2. Induktive Kopplung	19
2.3. Ersatzschaltbild Transponder mit magnetischer Kopplung	20
2.4. Resonanzkurve für Schwingkreis	22
2.5. Schwingkreis mit Antenne	26
2.6. Magnetische und elektrische Feldstärke einer ebenen Welle	27
2.7. Lineare Polarisation einer elektromagnetischen Welle	31
2.8. Zirkulare Polarisation elektromagnetischer Wellen	31
2.9. Digitale Modulation	32
2.10. Kopplung über elektromagnetisches Feld	37
2.11. Frequenzbereiche und relevante Eigenschaften für RFID	39
2.12. Verfügbare Frequenzbereiche für RFID	40
3.1. Zeitliche Abläufe bei Voll- und Halbduplex und sequenziellen Systemen	48
3.2. Beispiele Signalcodierung bei RFID	50
3.3. Kollision mit NRZ- und Manchester-Codierung	54
3.4. Zufälliges Eintreffen der Datenpakete bei ALOHA	58
3.5. Durchsatz bei ALOHA und Slotted-ALOHA	60
3.6. Zeitschlitzte für das Senden von Datenpaketen bei S-ALOHA	61
4.1. Elektronische Ausweisdokumente	68
4.2. RFID Symbol	69
4.3. Wireless und NFC	71
4.4. NFC-Logo	72
4.5. World Shipments of NFC-enabled Cellular Handsets	73
4.6. NFC Anwendungen	76
4.7. Zahlteller mit NFC	77
4.8. Architektur der NFC-Kommunikation	78
4.9. Spezifikationen für die NFC-Kommunikation	79
4.10. RFID Anwendungsszenarien in Deutschland	80

Abbildungsverzeichnis

4.11. Klassifizierung von E-Business nach Geschäftspartnern	81
4.12. Erweiterung der Klassifizierung von E-Business	81
5.1. Handlesegerät, Reader und Antenne	83
5.2. Aufbau von Tags	84
5.3. Tag-Bauformen	85

1. Einführung in automatische Identifikationssysteme

In vielen Bereichen finden **automatische Identifikationsverfahren – Auto-ID** genannt – weite Verbreitung. In Logistik, Handel und Produktion (Warenwirtschaft) werden damit Informationen zu Personen, Tieren, Gütern und Waren bereitgestellt.

Am weitesten verbreitet sind Strichcode-Etiketten (engl. Barcode), die zwar äußerst preiswert sind, jedoch auch einige Nachteile aufweisen, siehe Abschnitt 1.2. Die allgemeine Lösung ist die Speicherung von Daten auf Silizium-Chips, welche der überwiegende Teil der neueren Verfahren nutzt.

Aus all diesen Techniken ragt RFID (Radio Frequency Identification) heraus, dem beispielsweise für die folgende Jahre ein jährliches durchschnittliches Wachstum von etwa 47 % in Europa, und weltweit etwa 60 % vorausgesagt wird [Deu, EH09].

1.1. Warum Identifikationssysteme

In vielen Bereichen des öffentlichen Lebens, der Logistik und der Warenwirtschaft müssen Identitäten von Objekten und/oder Personen erfasst werden. Mit Identität kann in diesem Zusammenhang auch nur das Vorhandensein eines bestimmten Merkmals oder einer Eigenschaft gemeint sein wie das Vorhandensein einer Briefmarke oder eines gültigen Tickets für Kino oder Straßenbahn. Informationen, welche auf einem Medium vorhanden sind, sollen zur Verarbeitung oder Kontrolle auf ein anderes Medium oder System übertragen werden. Damit liegt ein **Medienbruch**, den wir wie folgt beschreiben¹ vor.

*Informationen sind an Medien gebunden. Informationen werden per Sprache, per Fax, per E-Mail, auf Papier, als Video oder elektronische Datei gespeichert und übermittelt. Ist bei der Verarbeitung der Information ein **Übergang auf ein anderes Medium** erforderlich, dann bedeutet dies einen **Medienbruch**.*

:=

¹vergl. [ITW].

1. Einführung in automatische Identifikationssysteme



Beispiel 1.1. Wird als beispielsweise ein empfangenes Fax in einen Computer als Textdatei eingegeben, so findet in diesem Fall ein Medienbruch statt.



Ein Medienbruch führt in den meisten Fällen zu zusätzlichen **Fehlern, Verzögerungen und Kosten**.

Am höchsten sind die Medienbruch-Kosten bei Eingabe per Hand, gefolgt von Spracheingabe und Scannen von Barcode, wie Bild 1.1 zeigt. RFID ist diesbezüglich, außer der direkte Vernetzung von eingebetteten Systemen (embedded systems), die beste Lösung, welche im Idealfall keine menschliche Intervention mehr erfordert, vergl. [FM05].

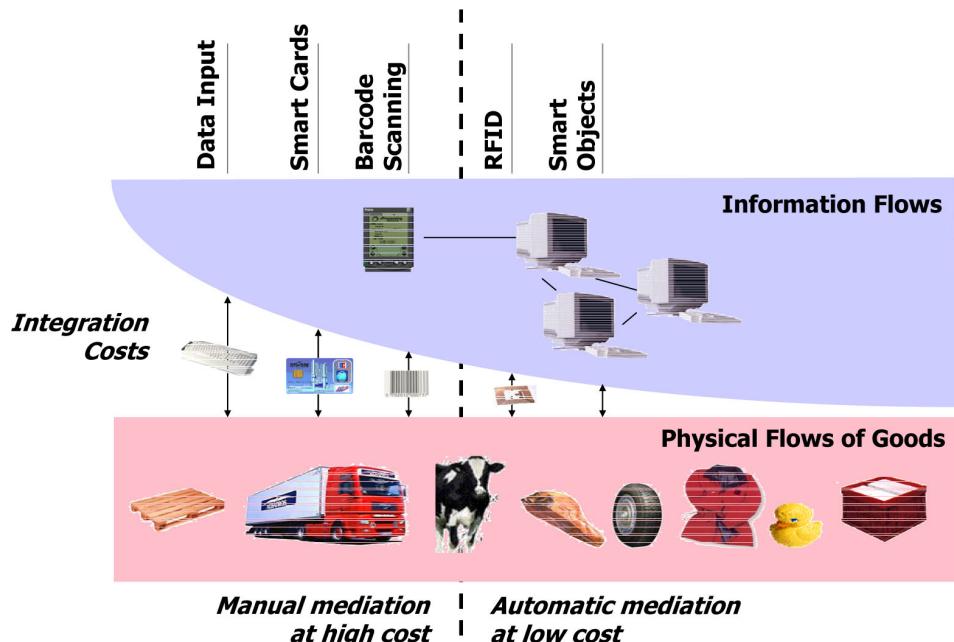
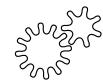


Bild 1.1.: Kosten von Medienbrüchen, vergl. [FM05]

Beispiel 1.2. Als Beispiel seien Kosten im ÖPNV aufgeführt. Der Verkauf in Zürich kostet allein 16% des Ticketpreises durch die Bereitstellung von Automaten, Versorgung mit fälschungssicherem Papier, Wartung und Reparatur. Ferner gehen in deutschen Großstädten etwa weitere 25% durch Schwarzfahrer verloren. Interne Abrechnungen im Verkehrsverbund können nur auf der ungenauen Basis aufwändiger Stichprobenzählungen erfolgen. Transaktionszeiten für Verkauf und Kontrolle im Fahrzeug und damit Wartezeiten sind erheblich, siehe [Fin06]



Barcodes zur automatisierten Erkennung von Produkten sind seit mehr als 20 Jahren im Einsatz. Zur **Diebstahlsicherung** in Kaufhäusern tragen auf sogenannten „Funketiketten“² die 1-bit Information, ob die Ware bezahlt wurde oder nicht.

1.2. Gängige Identifikationssysteme

Bevor wir auf die Radiofrequenz-Identifikation (RFID) eingehen, werden im Folgenden einige gängige Identifikationsverfahren kurz besprochen. In Abschnitt 1.2.6 folgt eine kurze Gegenüberstellung der Vor- und Nachteile der einzelnen Verfahren.

1.2.1. Barcode

Der **Barcode** – auch **Strichcode** genannt – ist ein Binärkode aus einem Feld von parallel angeordneten Strichen³ und Lücken, welche direkt auf das zu markierende Objekt aufgedruckt oder mittels eines bedruckten Etiketts angebracht wird, siehe Bild 1.2a als Beispiel für eine Produktnummer in EAN-Codierung.

Eindimensionale **Strichcodes** (1D) werden zur Codierung von bis zu 128 Zeichen verwendet. Bild 1.2b zeigt einen 2-dimensionalen Code (2D, Data Matrixcode), mit dem bis etwa 2300 ASCII-Zeichen dargestellt werden können, und der beispielsweise als Freimachungsvermerk bei Postsendungen verwendet wird.

Übung 1.1. Versuchen Sie die beiden Barcodes in Bild 1.2 zu entschlüsseln. Suchen Sie dazu im Internet nach geeigneten (kostenlosen) Links und Software.



²für diese ungenaue Bezeichnung wird im Folgenden nur noch die Bezeichnung *Transponder* oder *Tag*, siehe Abschnitt 1.4, verwendet.

³engl. **bar** = Strich



(a) EAN128B



(b) Datamatrix (2D)

Bild 1.2.: 1- und 2-dimensionale Barcodes

1.2.2. Optical Character Recognition

Klarschriftleser ermöglichen das Erkennen von geschriebenem Text, **OCR** genannt. Es findet Anwendung im Dienstleistungsbereich, wie das Registrieren von Bankformularen und Schecks sowie bei der Briefsortierung.



Übung 1.2. Falls Sie Zugang zu einem Scanner und Software für Schrifterkennung haben, untersuchen Sie die Erkennbarkeit von Schriften unterschiedlicher Größe und Schriftarten (Fonts) sowie handgeschriebenen Text (Druckbuchstaben). (Siehe Experiment ?? auf Seite ??.)

1.2.3. Biometrie

Biometrie fasst die Erkennung biologischer Merkmale zusammen. Bekannte Verfahren sind die Erkennung des Fingerabdrucks, Auges (Iris), der Gesichtsform, Stimmmerkmalen und des Erbguts DeoxyriboNucleic Acid (**DNA**). Letzteres ist für die schnelle Identifikation aufgrund der aufwändigen Analyse und der damit verbundenen Kosten nicht geeignet. Für die übrigen existierenden Geräte und Software.

1.2.4. Chipkarten

Chipkarten werden auch als **Smartcards**⁴ oder **Integrated Circuit Card (ICC)** bezeichnet und sind elektronische Datenspeicher mit eigenem Mikroprozessor und müssen in der Version mit Kontaktfeldern mit dem Lesegerät galvanisch⁵ in Verbindung gebracht werden. Man bezeichnet sie als *kontaktbehaftet*.

⁴engl. *smart* = clever, schlau, gewitzt, raffiniert

⁵galvanische Kopplung: Herstellung eines geschlossenen Stromkreises

Bei den Chipkarten gibt es sehr unterschiedliche Ausführungen von der *Speicherplatte* mit einfacher Logik bis zur Karte mit *Prozessor* und **Betriebssystem** und Sicherheitsmerkmalen wie *Kryptografie*, siehe Kapitel 7.1.1.

Beispiel 1.3. Chipkarten oder **Smartcards** sind beispielsweise Telefonkarten, EC- oder Geldkarten, Krankenversicherungskarten oder die **SIM-Karten** in Mobiltelefonen.



Bisweilen wird auch von *kontaktlosen* Smartcards gesprochen. Es handelt sich hierbei in der Regel um **RFID-Systeme** oder sie können diesen in der Funktionsweise zugeordnet werden, wie wir im Folgenden sehen werden.

1.2.5. RFID-Systeme

RFID-Systeme sind ähnlich der Chipkarten, jedoch erfolgt die Kopplung nicht über den direkten elektrischen Kontakt, sondern **kontaktlos** über **magnetische** oder **elektromagnetische** Felder, also mit Hilfe von Funk- oder Radar-Wellen.



RFID-Etiketten müssen folglich mit dem Lesegerät nicht in Berührung, sondern nur in die Nähe gebracht werden. Der Leseabstand kann dabei – je nach Verfahren – einige Millimeter bis einige Meter betragen.

Bei **RFID** handelt es sich um eine Technologie, um Dinge kontaktlos aus einem gewissen Abstand zu identifizieren.

1.2.6. Vergleich einiger Auto-ID-Verfahren

Tabelle 1.1 vergleicht einige Auto-ID-Verfahren. Die angegebenen Preise sind nur ungefähr, da insbesondere bei RFID – abhängig vom Frequenzbereich und dem Speichervolumen – in Zukunft mit zunehmend günstigeren Herstellungsverfahren zu rechnen ist.

1. Einführung in automatische Identifikationssysteme

Tabelle 1.1.: Vergleich Auto-ID-Verfahren, vergl. [Fin06]. \oplus : gut, \odot : mittel, \ominus : schlecht

Eigenschaft/ Verhalten bei	Barcode	OCR	Biometrie	Chipkarte	RFID
Anschaffungskosten	$\oplus\oplus$	\odot	\ominus	\oplus	\odot
Preis	$\oplus\oplus$			$\ominus\ominus$	\odot^6
Datenmenge	\ominus	\ominus		\oplus	\oplus
Schmutz/Nässe	$\ominus\ominus$	$\ominus\ominus$		\odot	$\oplus\oplus$
Optische Abdeckung	$\ominus\ominus$	$\ominus\ominus$			$\oplus\oplus$
Abnutzung	\ominus	\ominus		\odot	$\oplus\oplus$
Unbefugtes Kopieren	$\ominus\ominus$	$\ominus\ominus$	$\oplus\oplus$	$\oplus\oplus$	$\oplus - \oplus\oplus$
Lesegeschwindigkeit	\ominus	\ominus	$\ominus\ominus$	\ominus	$\oplus\oplus$
Leseentfernung	\odot	\ominus	$\ominus\ominus$	$\ominus\ominus$	$\oplus\oplus$

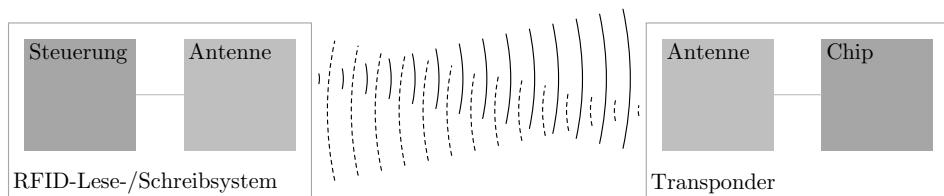


Bild 1.3.: Funktionsweise von RFID

1.3. Prinzip von RFID



Ein RFID-System besteht aus mindestens zwei Komponenten:

Lesegerät als Lese- oder bisweilen Schreib-/Leseeinheit

Transponder ist am zu identifizierenden Objekt angebracht

Das Lesegerät kann eine eigenständige Einheit darstellen oder mit einem Computersystem verbunden sein.

Der **Transponder**⁷ ist der eigentliche Datenträger im RFID-System und besteht im Wesent-

⁶Preise hängen stark von Stückzahlen ab und unterliegen dem üblichen raschen Wandel bei Elektronikkomponenten. Preise bei Auflagen bis zehntausend: 0.50-1.00 €, ab einer Mia. Stück: 0.05-0.10 €, vergl. [RFI]. Derzeit noch ≥ 10 cent.

⁷Kurzform aus Transmitter-Responder

lichen aus einer Antenne und einer elektronischen Schaltung auf einem Mikrochip. Der Transponder enthält in der Regel keine Batterie. Er wird über die elektromagnetischen Wellen des Lesegeräts mit Energie versorgt, und sendet seine Kennung, ggf. auch weitere Daten an das Lesegerät zurück, siehe Abschnitt 1.4.

Transponder

Die Übertragung zwischen Lesegerät und Transponder erfolgt über den freien Raum, die sogenannte **Luftschnittstelle**.

Luftschnittstelle

Für RFID werden sehr unterschiedlichen Frequenzbereiche, siehe Absatz 1.5, verwendet. Diese bestimmen die grundsätzlichen Eigenschaften wie Reichweite, Lesegeschwindigkeit und übertragbare Datenmenge. Die Reichweite – also der mögliche Abstand zwischen Lesegerät und Transponder – ist durch die Energie begrenzt, welche für die Energie- und Signalübertragung zur Verfügung steht.

1.4. Transponder oder Tags

1.4.1. Passive Tags

Ein RFID-Transponder wird üblicherweise auch als **Tag**⁸ bezeichnet.

Tag

Passive Transponder verfügen über keine eigene **Energieversorgung**. Die für den Betrieb benötigte Energie wird durch die Antenne des Transponders dem magnetischen oder elektromagnetischen Feld des Lesegerätes entnommen. Die Datenübertragung vom Transponder zum Lesegerät kann auf unterschiedliche Art erfolgen: zum einen durch Beeinflussung der vom Lesegerät ausgesendeten Wellen, beispielsweise durch Lastmodulation, siehe Kapitel 2.4, oder - im Bereich höherer Frequenzen - durch Veränderung der rückgestreuten Welle (modulierte Rückstreuung), siehe Kapitel 2.9.4.

passive Transponder

Energie

1.4.2. Aktive Tags

Aktive Transponder verfügen über eine eigene Energieversorgung, z.B. eine Batterien oder Solarzelle. Diese dient nur der Spannungsversorgung für den Chip. Dies kann notwendig sein um darauf flüchtige Daten zu speichern oder zu erfassen. Sie wird jedoch nicht dazu benutzt ein eigenes Hochfrequenzsignal zu erzeugen. Diese Definition wird in der Literatur jedoch leider widersprüchlich benutzt, siehe Abschnitt 1.4.3. Indirekt kann dies zu einer deutlichen Erhöhung der Kommunikationsreichweite beitragen, weil der Transponder dadurch in der Lage ist noch schwächere Signale des Lesegeräts zu detektieren.

aktive Transponder

Geräte, welche selbstständig senden können, zählen nicht mehr zur RFID-Technologien, sondern zu den Kurzstreckenfunkgeräten (Telemetriesender, **SRD**), siehe auch [Fin06]

Telemetrie

⁸engl. tag = Markierung, Kennzeichen, Marke

1.4.3. Definition passiv – semi-passiv – aktiv

In der Literatur werden die Definitionen über RFID-Transponder teilweise widersprüchlich verwendet.



Um die Übersicht zu behalten wollen wir noch einmal die Begriffe aufzählen und erläutern:

Passive RFID-Transponder benutzen ausschließlich die Energie aus dem vom Lesegerät erzeugten Felds, sowohl für die Aktivierung des Mikrochips, als auch zum Senden der Daten

:=

Semi-passive oder semi-aktive RFID-Transponder werden gleichbedeutend bezeichnet, siehe beispielsweise [Fin06, FM05]. Sie besitzen eine interne Batterie zur Versorgung des Chip. Zum Senden von Daten wird ausschließlich die Energie aus dem Feld des Lesegeräts bezogen

Aktive RFID-Transponder Beispielsweise nach [FM05] besitzen diese eine Batterie, deren Energie sowohl für die Versorgung des Chip, als auch zum Senden verwendet wird. [Fin06] klassifiziert diese Bauart als **Telemetriesender** und nicht als echten RFID-Transponder. Es soll hier der Vorschlag einer Abgrenzung durch die Festlegung gemacht werden, dass ein RFID-Transponder – auch ein aktiver – stets nur Leseanfragen beantwortet und niemals selbstständig sendet.

Die Definition der passiven RFID-Transponder wird in der Literatur einheitlich verwendet. Semi-passive oder semi-aktive RFID-Transponder werden bei [Fin06] als aktive Transponder bezeichnet.

Der Begriff aktiver Transponder ist widersprüchlich:



- beim einen Autor, siehe [Fin06], dient die Batterie nur zur Pufferung des Chips, nicht zum Senden
- beim anderen, siehe [FM05], dient die Batterie für die Versorgung des Chip und zum Senden.

Bei dem anhaltenden RFID-Boom ist davon auszugehen, dass RFID- und Telemetriesysteme in den vielfältigen Anwendungen zunehmend vermischt werden. Die hohen Reichweiten, von

denen zuweilen die Rede ist, sind in der Verwendung von Sendern mit eigener Energiequelle begründet.

Diese Aspekte werden wir auch bei den Grundlagen in Kapitel 2 im Zusammenhang mit Datenschutz besprechen.

1.5. Frequenzbereiche

RFID-Systeme werden in unterschiedlichen Frequenzbereichen genutzt, derzeit hauptsächlich in den Bereichen um 125 kHz (**LF**), 13.56 MHz (**HF**) und zwischen 868 bis 915 MHz (**UHF**), siehe Kapitel 2.11 und Tabelle 2.1.

Jedes System, welches elektromagnetische Wellen erzeugt oder abstrahlt, wird rechtlich als Funkanlage betrachtet. Keinesfalls darf ein RFID-System anderer Funkdienste wie Rundfunk, Fernsehen oder Zeitzeichensender sowie Mobilfunkdienste wie Polizei, Sicherheitsdienste und Flugsicherung beeinträchtigen. Daher sind Frequenzbereiche weltweit reguliert. Funkanlagen (ein RFID-System ist ein solches) müssen entweder aufwändig einzeln zugelassen werden oder in einem dafür zugelassenen Frequenzbereich nach festen Regeln operieren.

Für die Identifikation mit Radiofrequenz (RFID) können die **ISM-Frequenzen (Industry, Scientific, Medical)** genutzt werden. Diese Bereiche stehen für Hochfrequenznutzungen in Industrie, Wissenschaft und Medizin zur Verfügung. Beispiele hierfür sind Babyphone, Funkfernbedienungen, Mikrowellenherde oder Kurzwellenbestrahlung in der Medizin.

Frequenzbereiche

ISM

Leider sind diese Bereiche international **nicht** immer **einheitlich** geregelt, was den weltumspannenden Einsatz von RFID behindert. Dies betrifft oft nicht nur die verwendete Frequenz, sondern auch die zulässige Sendeleistung. Beispiel hierfür ist der Bereich Ultra High Frequency (**UHF**), welcher in Europa um 868 MHz, in den USA um 915 MHz liegt. Mehr dazu in den Kapiteln 2 und 3.

1.6. Typische Anwendungen

RFID-Systeme finden überall dort Anwendung, wo folgende Rahmenbedingungen und Eigenschaften für das zu identifizierende Objekt und die Leseeinheit(en) in Frage kommen:

- kein direkter Sichtkontakt, Lesewinkel nicht definiert
- Unempfindlichkeit gegenüber rauen oder schwierige Umgebungsbedingungen wie Feuchtigkeit, Schmutz, Temperatur oder grelles Licht (Barcodes) ...
- schnelle und sichere Erfassung
- größere Lesedistanzen, als mit einfachen optischen Systemen (Barcode-Scanner) möglich
- Pulkerfassung, Erkennen mehrerer Objekte gleichzeitig

1. Einführung in automatische Identifikationssysteme

- gesicherte Übertragung und Passwortschutz
- Erschwerung oder Verhinderung der Fälschung von Tags und den damit gekennzeichneten Objekten
- Individualisierung des Objekts, Schreiben/Verändern von Information

Diese Eigenschaften müssen nicht alle gleichzeitig zutreffen und hängen von den Anforderungen und der Auswahl der sehr unterschiedlichen RFID-Systeme ab, wie in den folgenden Kapiteln vertieft werden wird.



RFID umspannt heute einfachste Systeme wie Warensicherung durch elektronische Überwachung ([EAS](#)) über Zugangskontrolle, Artikel- und Tieridentifikation bis hin zu komplexen Anwendungen wie dem elektronischen Reisepass.

1.7. Zusammenfassung

In der Automatisierung spielt die Identifikation von Objekten eine entscheidende Rolle. Das Kapitel zählt die wichtigsten Verfahren der automatischen Identifikation (Auto-ID) auf und vergleicht die wichtigsten Eigenschaften. RFID ist etabliert für Diebstahlsicherung und Wegfahrsperren und weist gegenüber dem Barcode viele Vorteile auf. Jedoch wirken derzeit der Preis für Tags und teilweise international uneinheitliche Standards der breiten Anwendung noch entgegen.



1.8. Übungen

Übung 1.3. Vergleichen Sie an Hand der Informationen aus diesem Kapitel Barcode und RFID und zeigen Sie einige Vor- und Nachteile des jeweiligen Prinzips auf.

Übung 1.4. Welche Funk-Frequenzbereiche dürfen unter bestimmten Voraussetzungen ohne eine individuelle Genehmigung für Anwendungen wie beispielsweise RFID genutzt werden?

Übung 1.5. Zählen Sie alle Ihnen bekannten existierende RFID-Anwendungen auf?

Übung 1.6. Wie können Transponder oder Tags grundsätzlich klassifiziert werden?

2. Grundlagen

Für das Verständnis der Funktionsweise von RFID, Anwendungen und technische Grenzen werden im Folgenden einige Grundlagen erläutert. Dabei geht es um elektrische Schwingkreise, Kopplung über Spulen und Antennen, elektromagnetische Wellen und deren Ausbreitung.

Es werden an dieser Stelle vorwiegend qualitative Zusammenhänge locker erläutert und Grundkenntnisse kurz wiederholt; eine Vertiefung und Details bieten Fachgebiete wie Elektro- und Hochfrequenztechnik oder allgemein die Physik. Die Fußnoten sollen dazu Hinweise bieten, sind aber für das Verständnis der allgemeinen Zusammenhänge nicht unbedingt erforderlich.

2.1. Grundbegriffe Elektrotechnik

2.1.1. Spannung, Strom und Felder

Bei jeder elektronischen Anwendung werden **elektrische Ladungen** bewegt. Die Kraft, welche diese Ladungen bewegt, ist die **Spannung**.

Für die folgenden Betrachtungen können wir uns die Ladungen als die frei beweglichen Elektronen in einem metallischen Leiter vorstellen.

*Die Menge an Ladung Q , welche in einem Zeitintervall t einen Leitungsquerschnitt passiert, wird als **Strom** I bezeichnet, also*

$$I = \frac{Q}{t} \quad (2.1)$$

*Strom wird in der Einheit **A**, gesprochen **Ampère**, gemessen.*

:=

*Die Kraft, welche elektrische Ladungen bewegt, ist die **Spannung**. Die Spannung U wird in der Einheit **V**, gesprochen **Volt**, angegeben.*

:=

An dieser Stelle führen wir kurz den Begriff **Feld** ein.

2. Grundlagen



Ein Feld beschreibt die Abhangigkeit einer physikalischen Groe in Abhangigkeit vom raumlichen Ort.

Allgegenwartiges Beispiel ist das Schwerefeld der Erde. Sein Wert in unserem Badezimmer erzeugt aus der Masse unseres Korpers den (ortsabhangigen) Wert, welchen wir morgens von der Waage ablesen – er hangt also vom **Potenzial** an dieser Stelle ab. In vielen Fallen interessiert nur die **Potenzialdifferenz** zwischen zwei raumlichen Orten. So macht es einen groen Unterschied, ob wir uns einen Hammer aus 10 cm oder 2 m Hohe auf den Fu fallen lassen. Im zweiten Fall ist die Potenzialdifferenz und damit die Wirkung entsprechend groer.

Ebenso konnen wir uns im Raum ein **elektrisches Feld** E vorstellen. Es wird beschrieben durch das Spannungspotenzial am jeweiligen Ort. Die Spannung zwischen zwei Punkten im Raum ist also die Potenzialdifferenz zwischen diesen Punkten. Dass diese erheblich sein kann, wird beispielsweise bei einem Gewitter deutlich.

Die Starke eines Feldes ist die anderung des Potenzial von einem Punkt zu einem benachbarten Punkt. Im Fall des elektrischen Feldes wird die Feldstarke E in $[V/m]$, also in *Volt/Meter* angegeben. Uberschreitet die elektrische Feldstarke einen gewissen Wert, entsteht ein Funke wie beispielsweise bei einer Zundkerze oder bei Gewitter.

Auch das **magnetische Feld** ist von Bedeutung und wird weiter unten besprochen.

2.1.2. Leistung

Alle technischen Anwendungen benotigen **Energie** fur ihre Funktion. Zusammen mit der **Leistung** werden beide Begriffe im Folgenden kurz erlautert.



In der Elektrotechnik kann die Leistung P vereinfacht als Produkt aus Spannung U und Strom I dargestellt werden:

$$P = U \cdot I \quad (2.2)$$

oder falls Strom und Spannung zeitabhangig sind:

$$P(t) = U(t) \cdot I(t) \quad (2.3)$$

Die Einheit fur die Leistung ist das **Watt**, mit $[W] = [VA]$.

Die **Energie**, oder auch **Arbeit** W genannt, ist die über ein Zeitintervall $\Delta t = t_2 - t_1$ summierte Leistung. Falls die Leistung zeitabhängig ist, wird die Energie als Integral über das Zeitintervall t_1, t_2 dargestellt,

$$W = \int_{t_1}^{t_2} P(t) dt \quad (2.4)$$



bei konstanter Leistung über ein Zeitintervall δt vereinfacht sich Gleichung 2.4 zu

$$W = P \cdot \Delta t \quad (2.5)$$

Das Formelzeichen W für die Energie darf nicht mit der **SI-Einheit für Leistung – Watt –** verwechselt werden



Mit der Einheit s – Sekunde – ergibt sich aus den Gleichungen 2.2 und 2.5 für die Energie die Maßeinheit $[Ws] = [VAs]$. Die Wattsekunde ist gleichbedeutend mit der Einheit J , dem Joule.

2.1.3. Widerstand

Als **elektrischer Widerstand** R ist der Quotient aus Spannung und Strom definiert und wird in der Einheit **Ohm**, Symbol Ω , gemessen. Beim einfachsten Fall einer linearen Abhängigkeit bezeichnet man R als **ohmschen Widerstand**, der sich mit der folgenden Gleichung beschreiben lässt:

$\therefore =$

$$R = \frac{U}{I} \quad (2.6)$$

Viele Systeme verhalten sich bei Wechselspannungen- und strömen nicht linear wie ein ohmscher Widerstand. Deren Widerstand wird dann als **komplexer Widerstand** oder **Impedanz Z** bezeichnet. Diesbezüglich werden in diesem Werk jedoch keine weiteren Betrachtungen durchgeführt, so dass Interessierte hier auf weiterführende Literatur wie [KSW06] hingewiesen seien.

Impedanz Z

2.2. Schwingkreis

Das Prinzip der Identifikation mit Radiowellen, RFID, beruht auf der Übertragung von Energie und Information durch den freien Raum – und damit auf elektromagnetischen Feldern und Wellen.

Zuerst soll betrachtet werden, wie überhaupt elektrische Schwingungen zustande kommen. In Bild 2.1 ist ein einfacher Schwingkreis dargestellt. Das linke Symbol aus Kreis und einer Welle ist eine Wechselspannungsquelle, welche über einen Widerstand R den eigentlichen Schwingkreis aus einer Kapazität (Kondensator) C und der Induktivität (Spule) L mit Energie versorgt.

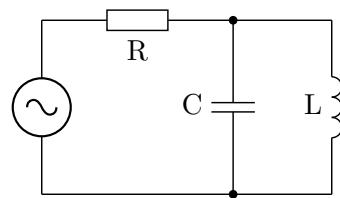


Bild 2.1.: Schwingkreis

Kapazität C



Hierbei spielen die Eigenschaften von **Kapazität C** und **Induktivität L** als sich gegenseitig ergänzende Energiespeicher eine entscheidende Rolle.

Ein Kondensator ist in der Lage, Ladung zu speichern – abhängig von der an ihm anliegenden Spannung U .

:=

Das Verhältnis aus Ladung Q und Spannung U ist für einen gegebenen Kondensator konstant und wird als Kapazität C bezeichnet und in F – Farad – gemessen.

$$C = \frac{Q}{U} \quad (2.7)$$



Beispiel 2.1. Bei einem Fahrradreifen beispielsweise hängt die gespeicherte Luftmenge vom Druck ab und natürlich auch umgekehrt. Ein Lkw-Reifen hat eine entsprechend größere Kapazität.

Das Symbol des Kondensators sind zwei parallele Platten. Ist der Kondensator geladen, trägt die eine Platte positive, die gegenüberliegende negative Ladung. Dabei ist die **Energie** im elek-

trischen Feld gespeichert.

Eine Induktivität L verhält sich ähnlich einer trägen Masse in der Mechanik, die jeder Änderung ihrer Geschwindigkeit eine Kraft entgegengesetzt. Eine Induktivität setzt jeder Änderung des Stroms I , der durch sie fließt, eine Spannung entgegen, welche als Induktionsspannung bezeichnet wird. In einer Formel lässt sich dies wie folgt ausdrücken:



$$U = L \cdot \frac{dI}{dt} \quad (2.8)$$

Die Induktivität L wird in H – Henry – gemessen. Auch eine Spule speichert Energie im **magnetischen Feld**, welches durch den Strom in der Spule erzeugt wird.

Mit den vorangegangenen Beschreibungen von C und L betrachten wir jetzt, wie in Bild 2.1 eine elektrische Schwingung entstehen kann. Zuerst betrachten wir die sich aus dieser Tatsache ergebende Gleichung, bevor wir uns den Sachverhalt mit einem einfachen Beispiel anschaulich machen. Zu jedem Zeitpunkt t liegen am Kondensator C und der Spule L immer die gleiche Spannung an, weil diese miteinander verbunden sind – also $U_C(t) = U_L(t)$.

Wir stellen Gleichung 2.7 zeitabhängig dar $U_C(t) = Q(t)/C$ und setzen diese dann mit Gleichung 2.8 gleich:

$$\begin{aligned} U_C(t) &= U_L(t) \\ \frac{1}{C} \cdot Q(t) &= L \cdot \frac{dI(t)}{dt} \end{aligned} \quad (2.9)$$

In Abschnitt 2.1.1 hatten wir gesehen, dass der Strom I die Änderung der Ladung mit der Zeit ist, also

$$I(t) = \frac{dQ}{dt} \quad (2.10)$$

Leiten wir Gleichung 2.9 nach der Zeit ab, erhalten wir die Differenzialgleichung

$$\frac{1}{C} \cdot I(t) = L \cdot \frac{d^2I(t)}{dt^2} \quad (2.11)$$

welche beispielsweise durch die Funktion

$$I(t) = I_0 \cdot \sin(\omega t) \quad (2.12)$$

2. Grundlagen

Kreisfrequenz also einen sinusförmigen Strom, gelöst wird.¹ Eine volle Periode für eine sinus- oder cosinusförmige Schwingung entspricht 2π , daher ergibt sich der Zusammenhang zwischen Frequenz f und der **Kreisfrequenz** ω zu²

$$\omega = 2\pi \cdot f \quad (2.13)$$

Einsetzen von Gleichung 2.12 in 2.11 ergibt^{3,4}

$$\left| \frac{1}{C} \cdot I_0 \cdot \sin(\omega t) \right| = \left| L \cdot \omega^2 \cdot I_0 \cdot \sin(\omega t) \right| \quad (2.14)$$

Resonanzfrequenz Damit ergibt sich die Kreisfrequenz ω_r für die Resonanz

$$\omega_r = \frac{1}{\sqrt{LC}} \quad (2.15)$$

und die **Resonanzfrequenz** f_r mit Gleichung 2.13

$$f_r = \frac{1}{2\pi} \frac{1}{\sqrt{LC}} \quad (2.16)$$

Phasenverschiebung

Der Ansatz $I(t) = I_0 \sin(\omega t)$, Gleichung 2.12, stellt also eine gültige Lösung dar. Setzten wir diese Lösung beispielsweise in Gleichung 2.8 ein, erhalten wir für die Zeitabhängigkeit der Spannung die Cosinus-Funktion. Im Resonanzfall für Kapazität C und Induktivität L eilt die Spannung $U(t)$ dem Strom $I(t)$ um $\varphi = 90^\circ = \pi/2$ voraus. Diese **Phasenverschiebung** φ ist ein wesentliches Kennzeichen schwingender und resonanter Systeme.

Bevor wir die gewonnenen Erkenntnisse weiter diskutieren, betrachten wir zuerst das anschauliche Beispiel.



Beispiel 2.2. Ein schwingendes Pendel kennen wir von der **Kinderschaukel**. Nur wenn wir genau die Resonanzfrequenz treffen, werden große Ausschläge erreicht. Dabei bleibt, sobald das System richtig schwingt, die notwendige Anregung – ein leichtes Anstoßen im Takt – relativ klein und muss nur den Verlust durch den Reibungswiderstand ausgleichen. In der Resonanz werden die Schwingungsamplituden unter Umständen sehr groß. Liegt man außerhalb der Resonanzfrequenz, bleiben die Ausschläge klein.

¹In Mathematik, Technik und Naturwissenschaften ist es üblich, das Argument von Winkelfunktionen wie sin, cos usw. in **Bogenmaß**, also Längen auf dem Einheitskreis (mit Radius 1) anzugeben. Ein Winkel von 360° entspricht also den vollen Kreisumfang 2π

²griech. Buchstabe ω : omega

³wegen $d \sin(ax)/dx = a \cos(ax)$ und $d \cos(ax)/dx = -a \sin(ax)$

⁴eigentlich ergibt die zweite Differenziation, siehe Fußnote 3, auf der rechten Seite der Gleichung ein negatives Vorzeichen, wie dies auch der Knotenregel (1. Satz des Kirchhoff-Gesetz) entspricht. Der Betrag der Ströme ist gleich: $|I_C(t)| = |I_L(t)|$

Die Resonanzkurve eines elektrischen Systems ist in Bild 2.4 gezeigt.

Betrachten wir nun das Beispiel 2.2 von der Seite der Energie her, so finden wir dort zwei Energieformen vertreten: Das eine ist die potentielle Energie, wenn das schaukelnde Kind zur einen oder anderen Seite ausgelenkt, und damit gegenüber den niedrigsten Punkt in der Mitte angehoben ist. Die (potenzielle) Energie liegt dann in der erhöhten Position. Schwingt die Schaukel genau durch die Mitte – den niedrigsten Punkt – liegt die Energie in der maximalen Geschwindigkeit, der so genannten kinetischen Energie. Es gibt also im Verlauf der periodischen Bewegung stets Punkte, bei denen die eine Energieform gleich Null, die andere maximal ist. Eine Schwingung wandelt also ständig die eine Energieform in die andere um. Weiterhin sind deren Maxima um 90° zueinander phasenverschoben.

Genau diese Situation finden wir auch beim elektrischen Schwingkreis. Einmal ist die **Spannung maximal** – die Energie ist im **elektrischen Feld** des Kondensators gespeichert, eine viertel Periode später ist der **Strom maximal** – die Energie ist im **magnetischen Feld** der Spule gespeichert. Dazwischen finden wir die Mischung beider Energieformen. In Bild 2.1 ist die Situation wiedergegeben. Die Anregung durch die Wechselspannung wird über den Widerstand R mehr oder minder schwach eingekoppelt, C und L speichern abwechselnd die Energie.

2.3. Maxwell und die Folgen

Nun zeigt sich in der Elektrodynamik, dass **elektrische** und **magnetische** Felder direkt voneinander abhängen, auch ohne Komponenten wie Kondensatoren, Spulen und Drähte.

Jede bewegte Ladung und damit jeder Strom ist mit einem **Magnetfeld** verbunden. Ein stromdurchflossener, gerader Leiter wird von kreisförmigen, geschlossenen Feldlinien umgeben. Dieses **H-Feld** ist proportional zum Strom I und unabhängig vom Material, welches den Leiter umgibt. Seine Stärke nimmt mit dem Abstand vom Leiter ab⁵. Biegt man den Leiter zu einer Schleife oderwickelt ihn zu einer Spule mit mehreren Windungen, entsteht ein H-Feld, wie es in Bild 2.2 angedeutet ist. Die Feldlinien reichen dabei unendlich weit, werden jedoch mit dem Abstand immer schwächer.

Maxwell⁶ stellte bereits 1862 eine Reihe von Gesetzen auf, von denen zwei hier von besonderer Bedeutung sind.

⁵Mathematisch ausgedrückt ist das Umlaufintegral über die Feldstärke H entlang einer geschlossenen Kurve gleich der Summe der von der Kurve eingeschlossenen Ströme:

$$\sum I = \oint \vec{H} d\vec{s}$$

⁶James Clark Maxwell, *1831 †1879, schottischer Physiker

2. Grundlagen



Durchflutungsgesetz von Maxwell: Jedes zeitlich veränderte elektrische Feld erzeugt ein magnetisches Feld.



Induktionsgesetz von Maxwell: Jedes zeitlich veränderte magnetische Feld erzeugt ein elektrisches Feld.

In beiden Fällen handelt es sich in diesem Zusammenhang um ein Wirbelfeld, das heißt ein Feld mit geschlossenen Feldlinien.

Mit diesen und weiteren Gesetzen begründete Maxwell die theoretischen Grundlagen für Entstehung und Ausbreitung **elektromagnetischer Wellen**, und damit technischer Anwendungen wie RFID.

2.4. Induktive oder magnetische Kopplung

Betrachten wir Bild 2.2, erkennen wir auf der linken Seite wieder einen Schwingkreis wie in Bild 2.1. Dabei ist die Induktivität L_1 als eine flache Spule ausgelegt. Die magnetischen Feldlinien erfüllen den Raum um die Spule. Da der Kreis aus C_1 und L_1 schwingt, ändern die Feldlinien ständig ihre Stärke.

Wird nun eine weitere Spule L_2 in den Bereich des **magnetischen Wechselfelds** gebracht, wird in dieser nach dem **Induktionsgesetz** eine **Wechselspannung** induziert. Sind C_2 und L_2 nach Gleichung 2.16 abgestimmt, entsteht eine rezonante Schwingung.



Beispiel 2.3. Die Spulen L_1 und L_2 in Bild 2.2 sind über das H-Feld magnetisch gekoppelt, Energie wird von L_1 auf L_2 übertragen, ohne dass beide elektrisch miteinander verbunden sind. Diese Art der Kopplung wird bei jedem **Transformator** verwendet, wobei Eisen zwischen den Spulen die Kopplung sehr stark verbessert, weil darin die Feldlinien gebündelt und verstärkt werden.

Da bei rezonanter Abstimmung von L_2 und C_2 große Schwingungsamplituden und Spannungen entstehen, kann die Diode D die Wechselspannung gleichrichten und den Kondensator C_3 mit einer Gleichspannung aufladen. Mit dieser Spannung wird der Chip mit Energie versorgt.

Die durch den rechten Teil der Schaltung entzogene Energie schwächt natürlich das magnetische Feld von L_1 und damit die Amplitude der Schwingung in L_1 und C_1 . Mit einer einfachen Ergänzung der elektronischen Schaltung im linken Teil – dem **Lesegerät** – kann diese Abschwächung nachgewiesen werden.

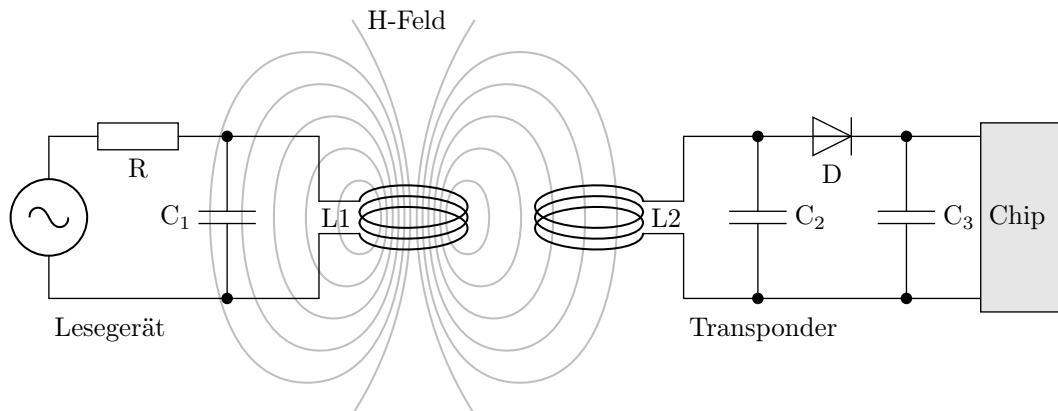


Bild 2.2.: Induktive Kopplung

Beispiel 2.4. Elektronische Diebstahlsicherungen (EAS) verwenden einfachste und besonders preiswerte **Transponder**, welche im rechten Teil der Schaltung nur aus einem Schwingkreis aus Spule und Kondensator bestehen und bei der Resonanzfrequenz dem magnetischen Wechselfeld ein wenig Energie entziehen. Die Spulen L1 des Lesegeräts sind bei vielen Kaufhäusern und Märkten groß und sichtbar an den Ausgängen plaziert.



Neben dem Verfahren aus Beispiel 2.4 existieren noch weitere Verfahren für die Überwachung von Artikeln und werden in Abschnitt 4.1.1 noch behandelt.

*Da bei der Artikelüberwachung nur das Vorhandensein eines Transponders überprüft wird – also ja oder nein – bezeichnet man diese Transponder auch als **1-Bit-Transponder**.*



Betrachten wir noch einmal den Transponder in Bild 2.2 und stellen uns vor, der Chip entzieht seinem Schwingkreis in einer bestimmten zeitlichen Abfolge durch eine zusätzliche Last mehr oder weniger Energie. Dann wird auch durch die magnetische Rückwirkung der Schwingkreis des Lesegeräts beeinflusst, dessen Schwingungsamplitude dann im gleichen Rhythmus schwankt. Das ursprünglich gleichmäßige Feld des Lesegeräts wird also durch Last moduliert, weshalb man bei diesem Verfahren von **Lastmodulation** spricht. Auf diese Weise kann der Transponder **Information** zum Lesegerät übertragen.

Lastmodulation

Mit dieser Darstellung haben wir bereits die grundlegende Funktionsweise der Informationsübertragung bei RFID-Systemen im Frequenzbereich von etwa 100 kHz bis ca 27 MHz erklärt.

2.5. Resonanz

Im Abschnitt 2.2 wurde der elektrische Schwingkreis aus Induktivität und Kapazität qualitativ vorgestellt.

Es folgen nun einige Betrachtungen am Beispiel eines Transponders für den Frequenzbereich 13.56 MHz. Wir werden dabei die Eigenschaften der Resonanz und den Begriff des Gütefaktors an Hand eines konkreten Systems kennen lernen.



Auch hier werden wir nur die prinzipielle Vorgehensweise bei den zu Grunde liegenden Überlegungen aufzeigen; um Unterstützung bei Wunsch nach Vertiefung einzelner Themen zu geben, werden Ansätze aufgezeigt und Hinweise auf weiterführende Literatur gegeben.

Bild 2.3 zeigt das Ersatzschaltbild für ein RFID-System aus der Sicht des Transponders. Das Lesegerät ist auf die Sendespule L_1 reduziert. Die magnetische Kopplung, auch induktive Kopplung genannt, über die Luftschnittstelle ist mit M angedeutet, bei dem ein Strom i_1 in der Spule des Lesegeräts einen Strom i_2 in der Antennenspule des Transponders induziert.

Während Bild 2.2 einen Idealzustand darstellt, der in der Praxis so nicht möglich ist, kommt das Schaltbild 2.3 näher an die Realität.

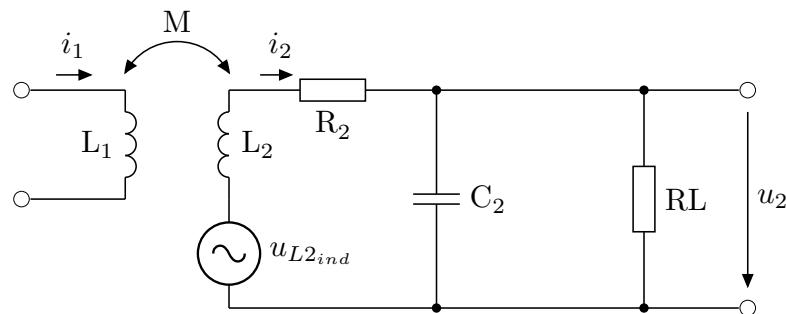


Bild 2.3.: Ersatzschaltbild Transponder mit magnetischer Kopplung, vergl. [Fin06]

Jede reale Schaltung hat einen nicht verschwindenden Widerstand, da Leitungen, Bauteile und Spulendrähte keine idealen Leiter darstellen. Dieser ohmsche Widerstand ist in R_2 abgebildet. Der Einfachheit halber sind parasitäre Kapazitäten mit in C_2 eingerechnet. Unter parasitärer Kapazität versteht man die Tatsachen, dass sich beispielsweise Leiterbahnen auf Schaltungen oder Wicklungen auf Spulen ebenso wie Elektroden eines Kondensators verhalten.

Serienschwingkreis

Zur vereinfachten Betrachtung wird die durch das Magnetfeld in der Spule L_2 induzierte Spannung u_{L2ind} als separate Spannungsquelle dargestellt. Die Spannungsquelle u_{L2ind} , die Induktivität L_2 , die Kapazität C_2 und der Widerstand R_2 bilden einen **Serienschwingkreis**⁷

⁷Der RLC-Serienschwingkreis (oft auch *Reihenschwingkreis* genannt) wird als Standardproblem in der Literatur

Der Serienschwingkreis 2.1 ist im Ersatzschaltbild 2.3 lediglich durch einen Lastwiderstand R_L erweitert, welcher parallel zu C_2 geschaltet ist. Dieses Bild ist realistisch, weil eine Transponderschaltung über die Spannung an C_2 mit Energie versorgt werden kann, wie beispielsweise in Bild 2.2 der Chip. Hierbei interessiert der mögliche Betrag der Spannung u_2 an R_L beziehungsweise C_2 .

Die Berechnung des Ersatzschaltbilds wird an dieser Stelle nicht ausgeführt; es wird lediglich das Ergebnis und Hinweise zum Ansatz und Lösungsweg angegeben.

Für jedes elektrische Netzwerk gelten die **Kirchhoffschen Regeln**⁸, auch für **zeitabhängige** Ströme und Spannungen. Beim Ansatz muss auf Grund der Wechselspannung- beziehungsweise -ströme und den dadurch bedingten Phasenverschiebungen in Induktivität und Kapazität der **Wechselstromwiderstand**⁹ der Komponenten eingesetzt werden.

Bei der Berechnung interessiert uns die Spannung u_2 in Abhängigkeit von der in Spule L_2 induzierten Spannung u_{L2ind} und der Frequenz f . Der Ansatz mit komplexen Widerständen¹⁰ führt zu einer komplexen Gleichung¹¹. Da uns an dieser Stelle nur die Beträge der Spannungen und Ströme, und nicht die Phasenlage interessieren, bestimmen wir – ohne Herleitung – über die **frequenzabhängige Impedanz**¹² Z , welche auch **Scheinwiderstand** genannt wird, die Spannung u_2

$$|u_2| = \left| \frac{u_{L2ind}}{\sqrt{\left(1 - \omega^2 L_2 C_2 + \frac{R_2}{R_L}\right)^2 + \left(\frac{\omega L_2}{R_L} + \omega R_2 L_2\right)^2}} \right| \quad (2.18)$$

2.5.1. Resonanzkurve

Für einen Schwingkreis nach Bild 2.3, bei dem die Werte für L_2 und C_2 auf die Resonanzfrequenz 13.56 MHz abgestimmt sind, wird für unterschiedliche Werte von R_2 im Diagramm 2.4 das Spannungsverhältnis $|u_2|/|u_{L2ind}|$ nach Gleichung 2.18 aufgetragen.

beispielsweise bei [KSW06, Col04] ausführlich beschrieben und berechnet.

⁸Knotenregel: $\sum I = 0$ und Maschenregel: $\sum U = 0$

⁹Wechselstromwiderstände können elegant als *komplexer Widerstand* Z angesetzt werden. Dabei werden die Anteile in *Real-* und *Imaginärteil* aufgespalten und die *Periodizität* von Strom oder Spannung mit dem *exponentiellen Ansatz* $e^{i\omega t} = \sin(\omega t) + i \cdot \cos(\omega t)$ beschreiben, vergl. [KSW06]

¹⁰siehe Fußnote 9, komplexer Widerstand für Induktivität: $Z_L = j\omega L$, für Kapazität:

¹¹ $Z_C = -j/\omega C$ und für ohmsche Widerstände: $Z_R = R$ (nur Realteil). Für die Rechnung mit j gilt: $j \cdot j = -1$.

$$u_2 = \frac{u_{L2ind}}{1 + (j\omega L_2 + R_2) \cdot \left(\frac{1}{R_L} + j\omega C_2\right)} \quad (2.17)$$

¹²Der komplexe Widerstand Z besteht aus einem *Realteil* R und einem *Imaginärteil* jX , siehe Fußnote 9: $Z = R + jX$. Die Impedanz Z bestimmt sich geometrisch aus der Länge, welche von R und X aufgespannt werden. $Z = \sqrt{R^2 + X^2}$

2. Grundlagen

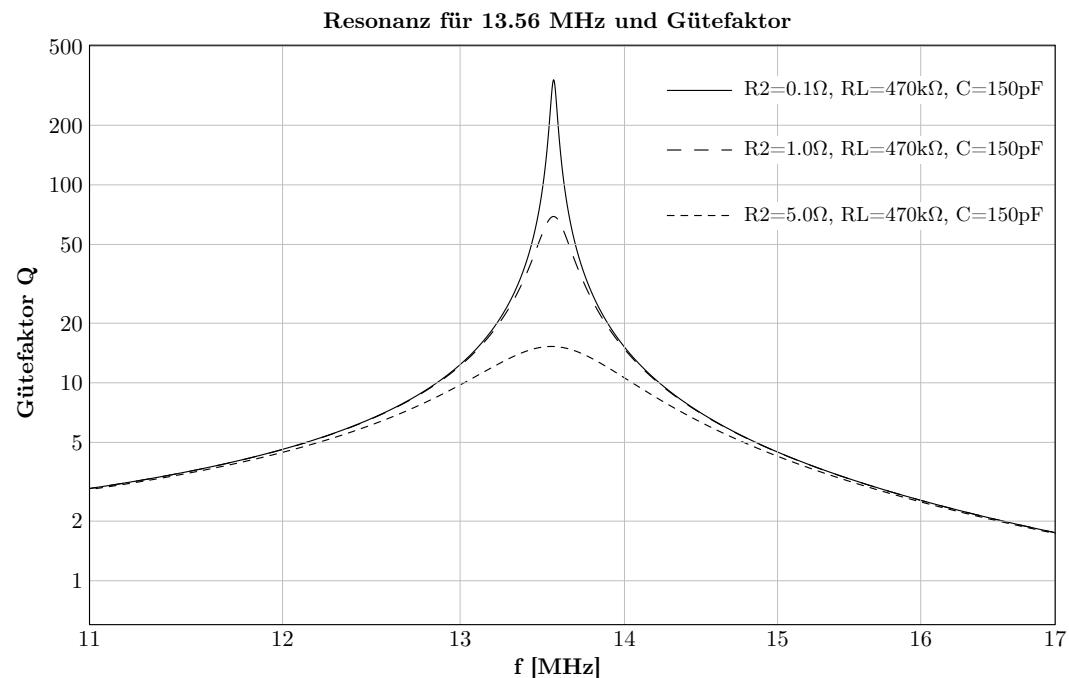


Bild 2.4.: Resonanzkurve für Schwingkreis in Schaltung 2.3 und Gleichung 2.19

Die drei Kurven beschreiben die **Resonanzkurve** bei drei unterschiedlichen Dämpfungen, welche durch den Verlust durch den Widerstand R_2 hervorgerufen werden. Beachten Sie die doppelt logarithmische Darstellung im Diagramm; bei linearer Auftragung wären der Verlauf der Abhängigkeiten nicht sichtbar.

Resonanzkurve

Deutlich ist die **Spannungsüberhöhung** im Bereich der Resonanzfrequenz erkennbar. Aus wenigen Volt an induzierter Spannung in der Spule L_2 werden an Kondensator und Lastwiderstand mühelos das Zehn- bis Hundertfache. **Resonanz** entsteht also, wenn in der Nähe der Eigenfrequenz eines schwingfähigen Systems die Anregung bei jeder Schwingungsperiode dem System Energie zuführen kann, das heißt die Phasenlage der Anregung mit der Schwingung zusammenpasst. Die größte Amplitude ist dann erreicht, wenn die Anregung die Verluste bei jeder Schwingung gerade ausgleicht.

Bekannte Beispiele sind die Kinderschaukel, Beispiel 2.2, oder eine mechanische Uhr, die mit einmaligem Aufziehen tagelang laufen kann, je nach **Güte** oder Qualität des Uhrwerks, weil ja pro Schwingung nur die Reibungsverluste ausgeglichen werden müssen.

Beispiel 2.5. Ein weiteres Beispiel wäre ein in einer kleinen Kuhle festgefahrenes Fahrzeug. Die Kraft einer Person reicht in der Regel nicht, das Hindernis auf ein Mal zu überwinden. Im richtigen Takt zum Hin- und Herschwingen angeregt, genügt eine vergleichsweise kleine Kraft auch große Massen zu bewegen.



2.5.2. Dämpfung und Gütefaktor

Die Höhe der Resonanzkurve ist nur durch die Verluste an R_2 begrenzt und bewirkt die Dämpfung. Die Dämpfung ist der Kehrwert des Gütefaktors.



Bei Dämpfung $\rightarrow 0$, das heißt $R_2 \rightarrow 0$, wachsen die Amplituden ins Unbegrenzte, was zu einstürzenden Brücken bei resonanter Anregung beispielweise durch Wind führen kann und daher **Resonanzkatastrophe** genannt wird.

Güte(faktor) Q

Man charakterisiert ein schwingfähiges System durch seine **Güte** oder den **Gütefaktor** Q . Die Güte Q berechnet sich in unserem Beispiel bei der Resonanzfrequenz aus dem Verhältnis des Betrags der Spannungen an den Komponenten L oder C und der Gesamtspannung.

Der Gütefaktor Q für das Schaltbild 2.3 wird bei [Fin06] direkt aus den Werten der Komponenten angegeben. Dabei wird beim rechten Ausdruck die Resonanzbedingung $C_2 = 1/\omega^2 L_2$ benutzt

$$Q = \frac{1}{R_2 \cdot \sqrt{\frac{C_2}{L_2}} + \frac{1}{R_L} \cdot \sqrt{\frac{L_2}{C_2}}} = \frac{1}{\frac{R_2}{\omega L_2} + \frac{\omega L_2}{R_L}} \quad (2.19)$$

Man erkennt, dass die Güte Q auch mit der Wahl der Induktivität¹³ L_2 für die Transponderspule optimiert werden kann.

Eine gängige Definition des Gütefaktors ergibt sich aus der **Breite** b der Resonanzkurve. Dabei werden oberhalb und unterhalb der Resonanzfrequenz f_r die beiden Frequenzen $f_u < f_r < f_o$ bestimmt, bei denen die maximale **Leistung** des Schwingkreises bei Resonanz f_r auf die **Hälfte** abgefallen ist.

$$Q = \frac{f_r}{f_o - f_u} = \frac{\omega_r}{\omega_o - \omega_u} \quad (2.20)$$

Wegen der Beziehung der Gleichungen 2.6 und 2.2 ist die Leistung proportional zur Spannung zum Quadrat, also $P \sim U^2$. Halbe Leistung bedeutet daher den $1/\sqrt{2}$ -ten Teil der Spannung. Diese Punkte können beispielsweise aus dem Diagramm 2.4 bestimmt werden.

¹³Benötigte Windungszahlen bei Transpondern mit 135 kHz etwa 1000, bei 13.56 MHz etwa 10 [FM05]

2.5.3. Dezibel



In der Technik werden Verhältnisse von Spannungen, Strömen, Leistungen usw. meist **logarithmisch** dargestellt als **Dezibel dB** der entsprechenden Messgröße.

Mit log ist im Folgenden der **dekadische Logarithmus**, also der Logarithmus zur Basis 10 gemeint.

Die Größe **Dezibel dB** ist das Zehnfache des dekadischen Logarithmus vom **Verhältnis A zweier Leistungen P_1 und P_2**

$$A = 10 \cdot \log\left(\frac{P_2}{P_1}\right) \quad (2.21)$$

:=

Für das Verhältnis der mit den Leistungen P verknüpften Spannungen U gilt wegen $P \sim U^2$ das **Verstärkungsmaß**

$$A = 20 \cdot \log\left(\frac{U_2}{U_1}\right) \quad (2.22)$$

Beachte die Beziehung $\log(x^2) = 2 \cdot \log(x)$.

Beispiel 2.6. Als Beispiel für das Leistungsmaß Dezibel formulieren wir die Definition des Gütefaktors Q aus der Resonanzbreite b noch einmal wie folgt:

Gesucht sind die beiden Leistungen P_b , welche die Hälfte der Leistung bei Resonanz betragen, also $P_b/P_r = 0.5$

$$10 \cdot \log\left(\frac{P_b}{P_r}\right) dB = 10 \log(0.5) dB \approx 10 \cdot (-0.3) dB = -3 dB$$

Die gesuchte Leistung ist also **-3 dB** der Leistung bei Resonanz. Für das gesuchten Spannungsverhältnis U_b/U_r benutzen wir das Verstärkungsmaß¹³. Es gilt:

$$\begin{aligned} 20 \cdot \log\left(\frac{U_b}{U_r}\right) dB &= -3 dB \\ \log\left(\frac{U_b}{U_r}\right) &= -\frac{3}{20} && \text{Funktion } 10^x \text{ anwenden } \Rightarrow \\ \frac{U_b}{U_r} &= 10^{-\frac{3}{20}} = 0.707 = \frac{1}{\sqrt{2}} \end{aligned}$$



Auch hier beachte die Definitionen! Für Leistungsmaß gilt Gleichung 2.21, für Verstärkungsmaß die Gleichung 2.22

Das in Dezibel ausgedrückte Verhältnis von Größen wird uns im Folgenden an weiteren Stellen begegnen.

2.6. Elektromagnetische Wellen

Der folgende Abschnitt behandelt die Entstehung und die Eigenschaft elektromagnetischer Wellen. Diese sind die Grundlage jeder Funkanwendung. Auch hier stehen die qualitativen und vereinfachten Betrachtungen für das Verständnis der RFID-Technologie im Vordergrund. Details behandelt das Fachgebiet der Hochfrequenztechnik, beispielsweise [Zim00].

2.6.1. Der geöffnete Schwingkreis

Mit Bild 2.1 in Abschnitt 2.2 haben wir einen Schwingkreis aus Kapazität und Induktivität vorgestellt. Der Aufbau wird dahingehend verändert, dass die Kapazität geöffnet wird, das heißt die beiden Kondensatorplatten stehen einander nicht mehr unmittelbar gegenüber, sondern werden „aufgebogen“, so dass die eine nach oben und die andere nach unten steht. Dazwischen liegt die Induktivität der Spule L .

Diese Anordnung stellt eine **Antenne** in Stabform dar. Die einander gegenüberliegenden Enden der Antennen stellen die Kapazität C dar, der Leiter zwischen den Enden die Induktivität L . Nach wie vor haben wir also einen LC-Schwingkreis vor uns.

Antenne

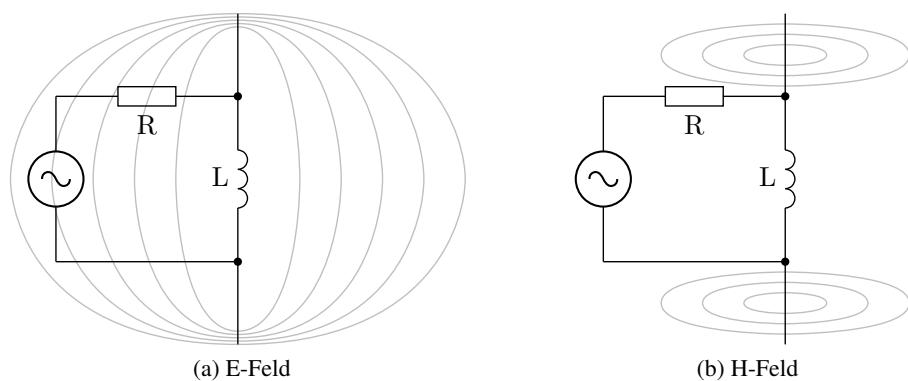


Bild 2.5.: Schwingkreis mit Antenne

Ist die Spannung an L und C auf dem Maximum, sind Ladungen an den Enden konzentriert, am einen Ende die positiven, am anderen die negativen. Dadurch entsteht ein **elektrisches Feld**, welches einen gewissen Bereich um die Antenne füllt, siehe Bild 2.5a

Beginnt sich der Kondensator zu entladen, fließt ein **Strom** durch die Antenne, welcher ein konzentrisches **Magnetfeld** um die Antenne erzeugt. Auch dieses Feld, siehe Bild 2.5b erfüllt den Raum in einem gewissen Abstand um die Antenne.

Da der LC-Kreis schwingt, wechseln sich die Maxima des **elektrischen** und **magnetischen** Feldes periodisch nacheinander ab. Weiterhin können wir erkennen, dass die Feldlinien des E- und des H-Feldes stets **senkrecht** zueinander stehen.

Weiterhin haben wir mit dem **Induktionsgesetz** und dem **Durchflutungsgesetz** in Abschnitt 2.3 gesehen, dass das sich stets ändernde Magnetfeld ein **elektrisches Wirbelfeld** und das sich ändernde elektrische Feld ein **magnetisches Wirbelfeld** erzeugt, beide also im Raum miteinander verknüpft sind.

Magnetische und elektrische Felder können sich nur mit höchstens der **Lichtgeschwindigkeit** im Raum ausbreiten. Ist die Frequenz hoch und erfolgt der Wechsel der maximalen Spannung an den Antennenenden schnell, können sich die elektrischen Feldlinien in Bild 2.5a nur einen gewissen Bereich im Raum ausbreiten, bevor sich an der Antenne Feldlinien der entgegengesetzten Richtung bilden. Die einzelnen Feldpakete lösen sich wie nierenförmige Blasen ab und entfernen sich in den Raum um die Antenne. Das gleiche Bild gilt auch für die magnetischen Feldlinien. Es entsteht eine **elektromagnetische Welle**¹⁴.

Während in der Antenne und in dessen unmittelbarer Nähe – dem **Nahfeld** – das H-Feld und das E-Feld noch einander abwechseln, also 90° phasenverschoben sind, sind ab einem gewissen Abstand – dem **Fernfeld** – elektrisches und magnetisches Feld in Phase, siehe Bild 2.6

Der Übergang vom Nah- zum Fernfeld hängt von der Wellenlänge ab und wird in den Abschnitten 2.6.2 und 2.9.1 näher behandelt.

¹⁴Für die Darstellung der Wellenentstehung und -ausbreitung siehe bspw. [ebe, Her]

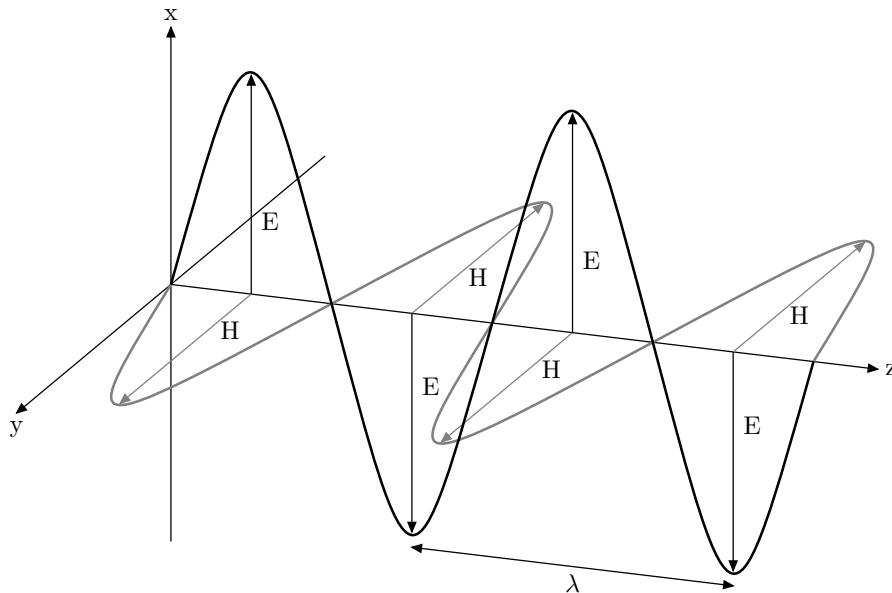


Bild 2.6.: Magnetische und elektrische Feldstärke einer ebenen Welle

2.6.2. Lichtgeschwindigkeit, Frequenz und Wellenlänge

In der Funktechnik spielen die Begriffe Frequenz und Wellenlänge eine wichtige Rolle. Sie sind durch eine Naturkonstante, die Lichtgeschwindigkeit c , miteinander verknüpft. Die **Lichtgeschwindigkeit c** beträgt im Vakuum

$$c = 2.9979 \cdot 10^8 \text{ m/s} \approx 3 \cdot 10^8 \text{ m/s} \quad (2.23)$$

Ein elektrisches oder magnetisches Feld oder eine elektromagnetische Welle kann sich also höchstens mit dieser Geschwindigkeit ausbreiten. In Materie ist diese Geschwindigkeit von 300 000 km/s etwas geringer.

Weiter oben haben wir bereits schwingende Systeme kennen gelernt. Ein solches System benötigt für eine vollständige Schwingung – beispielsweise von Maximum zu Maximum – eine bestimmte Zeit, die **Periodendauer T** genannt wird.

Frequenz f

Die Anzahl der **Schwingungen pro Sekunde**, welches ein System mit der Periodendauer T ausführt, wird die **Frequenz f** genannt und ergibt sich zu

$$f = \frac{1}{T} \quad (2.24)$$

und wird in **Hertz [Hz] = [1/s]** gemessen.

\doteq

2. Grundlagen

Breitet sich eine elektromagnetische Welle der Frequenz f im Raum aus, legt sie pro Sekunde $3 \cdot 10^8 \text{ m}$ zurück. Entlang dieser Strecke liegen also f vollständige Schwingungen. Daraus kann die Länge einer Schwingung berechnet werden, siehe Bild 2.6.

*Diese Länge wird als **Wellenlänge** λ bezeichnet und hängt mit Frequenz f und der Wellenausbreitungsgeschwindigkeit c wie folgt zusammen*

:=

$$\lambda = \frac{c}{f} \quad (2.25)$$

Einen quantitativen Zusammenhang zwischen Frequenz und Wellenlänge¹⁵ zeigt die Beschriftung der x-Achse in Bild 2.12.

Typische Wellenlängen und Eigenschaften bei RFID-Anwendungen sind

Tabelle 2.1.: RFID-Frequenzen, Wellenlängen und Eigenschaften. Daten von [Seg81]. Absorptionsdaten für LF und HF extrapoliert aus Daten von [Seg81]

Bezeichnung	Frequenz	Wellenlänge	Absorptionskoeffizient a in $H_2O [cm^{-1}]$	Absorptionslänge $1/a$
LF	125 - 135 kHz	2220 - 2400 m	$\approx 5 \cdot 10^{-8}$	200 km
HF	13.56 MHz	22.1 m	$\approx 1 \cdot 10^{-5}$	1 km
UHF	868 MHz	34.5 cm	$\approx 6.8 \cdot 10^{-2}$	14.7 cm
UHF	2.45 GHz	12.2 cm	≈ 0.68	1.47 cm
SHF	5.8 GHz	5.2 cm	≈ 2.8	3.6 mm

Auf die Erzeugung und Ausbreitung von Funkwellen und deren Eigenschaften haben Frequenz und Wellenlänge einen entscheidenden Einfluß. Je nach verwendeter Frequenz unterscheiden sich RFID-Systeme erheblich voneinander. Dies hat zum einen Auswirkung auf die Lesereichweite von Tags und der Rate der Datenübertragung und zum anderen auf deren Verwendbarkeit in unterschiedlichen Umgebungen auf Grund der unterschiedlich starken **Absorption** in Materialien, die wir in Abschnitt 2.9.2 besprechen.

¹⁵griech. Buchstabe λ : lambda

2.7. Antennen

Bei Funkanwendungen wie RFID kommen Antennen eine wichtige Bedeutung zu. Sie stellen die Verbindung zwischen Systemen her, welche räumlich voneinander getrennt sind. Das Wissen über Antennen ist ein überaus umfangreiches und lebendiges Fachgebiet der Hochfrequenztechnik und beruht nach wie vor auf sehr viel Erfahrung. Daher werden wir hier nur einige elementare Fakten ansprechen.

Grundsätzlich hängt die Antennengröße immer mit der Wellenlänge λ zusammen. Daher ist bei niedrigen Frequenzen und damit großen Wellenlängen die reine elektromagnetische Kopplung problematisch, da die notwendigen Antennen um effizient zu sein meter bis kilometer lang sein müssten¹⁶, siehe Tabelle 2.1.

Daher wird bei RFID mit niedrigen Frequenzen die magnetische Kopplung über Spulen praktiziert. Diese Spulen können weiter verkleinert werden, indem man sie auf einen Ferritkern¹⁷wickelt, siehe auch Fußnote 16. Diese Antennen nennt man **Ferritantennen**.

2.7.1. Antennenformen

Eine elementare Antennenform ist der **$\lambda/2$ -Dipol**. Die Bezeichnung bezieht sich auf die Wellenlänge der Frequenz, für welche die Antenne verwendet werden soll.

$\lambda/2$ -Dipol

Für technische Beschreibungen wie **Funkzulassungsvorschriften** wird häufig von einem **isotropen Strahler**¹⁸, oder auch **Kugelstrahler** genannt, ausgegangen, welcher die Energie der elektromagnetischen Welle in **alle Raumrichtungen** gleichmäßig abstrahlt, also in seiner Charakteristik **keine** Abhängigkeit von der Richtung aufweist.

isotroper Strahler

Die meisten Antennenformen weisen jedoch eine starke Richtungsabhängigkeit auf, wie es für ihren Anwendungszweck auch gewollt ist. Einen Eindruck von der Vielfalt bekommen sie bei einem bewussten Blick auf Sendeanlagen und Hausdächer.

Neben Dipolantennen werden bei RFID-Transpondern im **Mikrowellenbereich** auch sogenannte **Schlitzantennen** eingesetzt. Dabei befindet sich in einer leitenden Fläche ein Schlitz der Länge $\lambda/2$ und einer Breite $\ll \lambda/2$. Die Signalein beziehungsweise -auskopplung erfolgt an zwei gegenüberliegenden Seiten, vergl. [SS05].

Schlitzantenne

Im UHF-Bereich sind ferner **Patchantennen**¹⁹ im Einsatz. Dabei wird im Abstand h isoliert zu einer leitenden Grundfläche eine runde oder rechteckige Leiterfläche (Patch²⁰) angebracht. Für die Kantenlänge L_P der kurzen Seite gilt $L_P = \lambda/2 - h$. Patchantennen können durch Ätz- oder Klebetechnik leicht und preiswert hergestellt werden. Sie sind bei entsprechender Ein- und

Patchantenne

¹⁶Eine $\lambda/2$ -Antenne in einer Funkuhr für das DCF77-Zeitsignal (77.5 kHz) müsste knapp 2 km lang sein. Man verwendet daher Antennen, bei der die Antennenlänge anteilig auf einen Ferritkern aufgewickelt ist, und empfängt damit den H-Anteil des elektromagnetischen Feldes

¹⁷Aus Pulver gepresstes oder gesintertes magnetisches Material

¹⁸griech.: *isos* = gleich; *tropos* = Drehung, Richtung. Also für alle Richtungen gleich, richtungsunabhängig

¹⁹oder Mikrostrip-Antenne

²⁰engl.: *patch* = Flecken, kleine Stelle

2. Grundlagen

Auskopplung gut für zirkular polarisierte Wellen, siehe Abschnitt 2.7.4, geeignet, vergl. [Fin06, SS05].

Charakteristik sowie Sende- und Empfangseigenschaften werden in den folgenden Abschnitten am Beispiel des $\lambda/2$ -Dipols besprochen.

2.7.2. Charakteristik der Abstrahlung

Ein Dipol, wie wir ihn in Bild 2.5 kennen gelernt haben, kann nach oben und unten, also in der Antennenrichtung, keine Energie abstrahlen. Am stärksten ist hingegen die Wirkung des elektromagnetischen Feldes senkrecht zur Antennenachse.

Der Charakteristik der Energieabstrahlung beim $\lambda/2$ -Dipol entspricht einer Keule²¹ senkrecht zur Antennenachse. Keine Abstrahlung nach oben oder unten, maximale Abstrahlung senkrecht zur Antenne.

2.7.3. Sendeleistung und Gewinn

In Zulassungsvorschriften für Funkanlagen und in der RFID-Literatur stößt man häufig auf zwei Begriffe für **äquivalente Sendeleistung** – ERP und EIRP – welche hier kurz angesprochen werden sollen. Die Sendeleistung, welche ein Kugelstrahler, siehe **isotroper Strahler** in Abschnitt 2.7.1, wird mit **EIRP** bezeichnet.

EIRP
Antennengewinn

Eine Dipolantenne hat eine gewisse **Richtwirkung**, wie in Abschnitt 2.7.2 erläutert. Sie richtet die zur Verfügung stehende Leistung auf ein bestimmtes Raumsegment. Man spricht daher von einem **Antennengewinn** in der bevorzugten Richtung gegenüber einem Kugelstrahler.

ERP

Die äquivalente Sendeleistung **ERP** gibt an, mit welcher Leistung ein Kugelstrahler gespeist werden müsste, um die gleiche Strahlungsleistung abzugeben, wie die betrachtete Antenne in Hauptstrahlungsrichtung. Der Faktor G_i wird **Gewinn** genannt, vergl. [SS05, Fin06].

$$P_{EIRP} = P_{ERP} \cdot G_i \quad (2.26)$$

Für eine $\lambda/2$ -Antenne ist der Gewinn $G_{\lambda/2} = 1.64$.

2.7.4. Polarisation

Ein von einem Dipol erzeugtes elektromagnetisches Feld stellt eine ebene Welle dar. Das elektrische Feld E schwingt parallel zur Antennenachse, siehe Bild 2.7. Schwingt der \vec{E} -Vektor, wie in Bild 2.7a, in der x -Ebene, kann er in einer Empfangsantenne, im rechten Teil des Bilds, im Antennenstab nur Elektronen in dieser Ebene zum Schwingen anregen²².

²¹Wenn Θ der Winkel ist, welchen die Strahlrichtung mit der Antennenspitze bildet, ist beim $\lambda/2$ -Dipol die abgestrahlte Energie $W(\Theta) \sim \sin^2(\Theta)$

²²Die gleiche Überlegung gilt auch für die Strominduktion durch das zum E -Feld senkrecht stehende Magnetfeld H

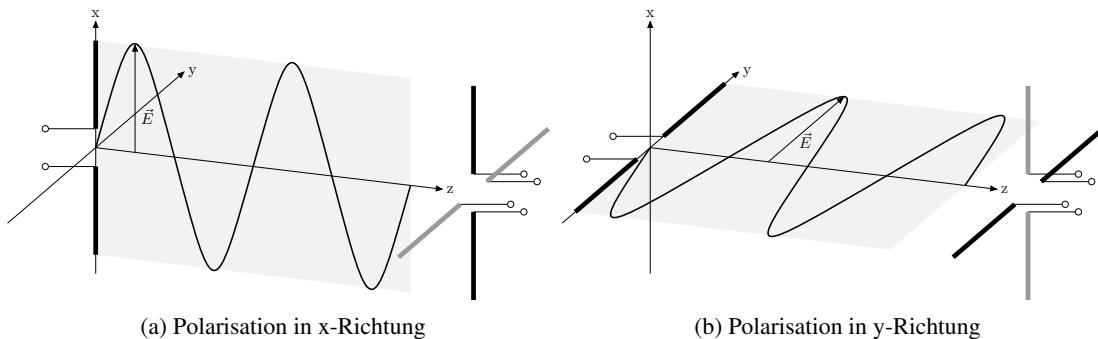


Bild 2.7.: Lineare Polarisation einer elektromagnetischen Welle

Nur wenn der Dipol in dieser Ebene liegt, wird eine Antennenspannung induziert. Die Antenne senkrecht zu dieser Ebene, grau eingefärbt, bleibt stumm. Die Situation in Bild 2.7b ist vergleichbar, nur schwingt die Welle jetzt um 90° gegenüber vorher gedreht in der y-Ebene. Auch hier kann nur die Antenne, welche parallel zur Sendeantenne ausgerichtet ist, empfangen. Man sagt, die Welle ist **linear polarisiert**. Um die Polarisation zu charakterisieren, wird die Ebene angegeben.

lineare Polarisation

Diese scheinbar unbedeutende Tatsache hat erhebliche Auswirkungen auf RFID-Systeme. Während die von einem Lesegerät ausgesandten Wellen linear polarisiert, könnten Tags nur gelesen werden, wenn ihre Antenne auf die Ebene ausgerichtet ist. Jede Drehung um den Winkel Θ der Antenne zur Ebene schwächt das Signal um den Betrag $\cos(\Theta)$. Bei 90° wäre kein Senden und Empfangen möglich²³.

Dieser Nachteil der linearen Polarisation beispielsweise für RFID-Anwendungen kann vermieden werden, in dem man im Sender zwei Dipole kreuzt, siehe Bild 2.8.

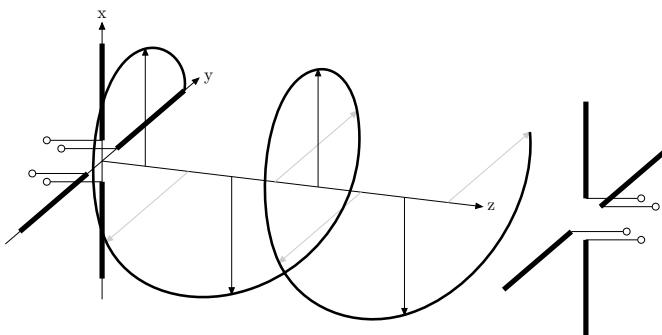


Bild 2.8.: Zirkulare Polarisation elektromagnetischer Wellen

²³Satelliten-Fernsehen beispielsweise verwendet die Polarisation – *horizontal* und *vertikal* – um einen Frequenzbereich doppelt nutzen zu können.

2. Grundlagen

zirkulare Polarisation

Man schickt die Wechselspannung der Sendefrequenz im Bild zum Beispiel auf den Dipol in y-Richtung und das um $90^\circ = \pi/2$ verzögerte Signal auf den Dipol in x-Richtung. Dadurch schwankt der \vec{E} -Vektor des elektrischen Feldes nicht mehr nur in einer Ebene, sondern er dreht sich um die Achse der Ausbreitungsrichtung wie eine Schraube. Man spricht daher von **zirkularer Polarisation**. Damit wird ein Empfänger unabhängig von der Winkelausrichtung des Empfangsdipols. Dieser wird bei einer zirkularen Polarisation immer in voller Stärke angeregt. In Bild 2.8 ist der um die z-Achse in Ausbreitungsrichtung rotierende Verlauf des Feldes bei zirkularpolarisierter Welle skizziert, der durch den Versatz der beiden senkrechten Komponenten x und y um den Phasenwinkel $\varphi = 90^\circ$ entsteht. Ein Empfangsdipol wird, ebenso wie die im Winkel zu ihm stehenden gleich stark angeregt.

Bei RFID-Systemen wird dieser Tatsache Rechnung getragen, indem Antennen eingesetzt werden, welche zirkularpolarisierende Wirkung haben. Auch existieren bereits Transponder mit integrierten Dipolantennen auf dem Markt.

2.8. Modulation

Modulation

Um Informationen mit einer Funkwelle übertragen zu können, muss das Trägersignal verändert – moduliert – werden. Analoge Verfahren der **Modulation** werden bei Rundfunk und Fernsehen verwendet.

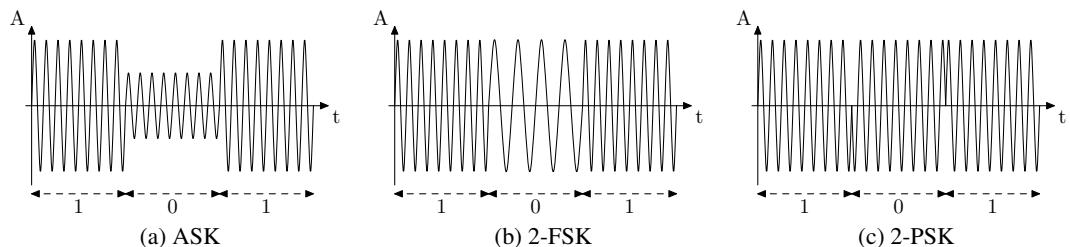


Bild 2.9.: Digitale Modulation

:=

Die **digitale Modulation** von Trägerfrequenzen wird als **Tastung** oder engl. **keying** bezeichnet.

Demodulator

Um das vom **Sender** durch Modulation übertragene Signal wieder zurückzugewinnen, muss vom **Empfänger** ein **Demodulator** eingesetzt werden. Weitere Details können der Fachliteratur, beispielsweise [Fin06] entnommen werden.

Für die Modulation mit digitalen Signalen werden bei RFID im wesentlichen drei in Bild 2.9 dargestellte Verfahren angewandt, vergl. auch [Fin06]:

Amplitudentastung (ASK) Amplitude der Trägerschwingung wird durch ein binäres Codesignal zwischen zwei Werten u_0 und u_1 umgeschaltet, siehe Bild 2.9a.



Zweifrequenzumtastung (2-FSK) Frequenz einer Trägerschwingung wird durch ein binäres Codesignal zwischen zwei Frequenzen f_1 und f_2 umgeschaltet, siehe Bild 2.9b.

Phasenumtastung (PSK) Die Phasenlage einer Trägerschwingung wird durch ein Codesignal zwischen 0° und 180° umgeschaltet, siehe Bild 2.9c.

Die Modulation mit digitalen Signalen wird auch als *Tastung* oder *Umtastung* bezeichnet.

Entscheidend bei jeder Art von Modulation ist die Entstehung von **Seitenbändern**, das heißt Frequenzen unterhalb und oberhalb der Grundfrequenz. Dies ermöglicht dem Lesegerät die im empfangenen Signal immer stark enthaltene Grundfrequenz durch Filter zu unterdrücken und die sehr viel schwächeren Seitenbänder zu detektieren. Der Gütefaktor der beteiligten Schwingkreise darf daher nicht zu hoch sein, damit die Seitenbänder noch satt in der Resonanzüberhöhung liegen, siehe Bild 2.4.

Seitenband

Den Bildern 2.9 können wir qualitativ noch eine weitere Information entnehmen. Die Frequenz der Modulation mit binären Daten und damit der **Datenrate** f_d – in den Bildern durch die Pfeile angedeutet – muss deutlich kleiner sein als die Trägerfrequenz f_T . Die mögliche **maximale Datenrate**, siehe Beispiel 2.7, $f_d \ll f_T$, ist folglich begrenzt durch die Arbeitsfrequenz des RFID-Systems, siehe auch Bild 2.11.

Datenrate

Beispiel 2.7. Die Ton-Qualität beim analogen Rundfunk hängt stark vom Frequenzband und der Modulationsart ab. Langwelle (LW) klingt schlechter als Mittelwelle (MW), beide Amplitudenmodulation. UKW mit höheren Frequenzen und Frequenzmodulation bringt deutlich höhere Qualität.



Die eigentlichen Daten werden meist vor der Modulation noch **kodiert**, um die Fehler bei der Übertragung zu verringern. Siehe hierzu auch Abschnitt 3.4. Zur Erhöhung der Sicherheit und des Datenschutzes wird bei einigen Systemen eine **Verschlüsselung**, also Kryptografie angewandt, siehe Abschnitt 7.1.1.

2.9. Reichweite

Für die Anwendung von RFID-Systemen ist die **Reichweite** von besonderer Bedeutung. Die maximale Reichweite ist im Wesentlichen durch die folgenden Faktoren bestimmt:

2. Grundlagen

- Eigenschaft der Ausbreitung elektromagnetischer Felder und Wellen bei einer gegebenen Frequenz.
- **Energierreichweite**, also der Abstand, bis zu dem der Transponder aus dem Feld des Lesegeräts noch ausreichend mit Energie versorgt werden kann
 - vom Transponder empfangene minimale Signalstärke
 - minimale Stärke des vom Transponder zurückgesendeten Signal, welches vom Lesegerät noch sicher detektiert werden kann.
- Störungen durch die Umgebung, wie andere Funkanwendungen oder Störfelder durch Maschinen und Geräte
- **Kollision**, das heißt Überlagerung durch weitere im Ansprechbereich des Lesegeräts befindliche RFID-Transponder
- räumliche Ausrichtung zwischen Antenne des Lesegeräts und dem Transponder.
- Reflexion oder Absorption durch Material, auf dem der Transponder angebracht ist oder welches sich zwischen Leser und Tag befindet.

2.9.1. Reichweite von Feldern und Wellen

Für den Betrieb von RFID-Anwendungen ist die Feldstärke bei magnetisch arbeitenden Systemen und die Strahlungsleistung bei elektromagnetischen von Interesse, da dies für die **Reichweite** von Bedeutung ist. In beiden Fällen – bei Spule wie beim Dipol – müssen die Verhältnisse nahe der Antenne und die in einem gewissen Abstand unterschieden werden.

Nah- und Fernfeld

Beim elektromagnetischen Feld bei einem Abstand r von der Antenne spricht man von **Nahfeld**²⁴, wenn $\lambda/2 < r < 4\lambda$ ist.

Ab einem Abstand $r > 4\lambda$ spricht man von **Fernfeld**. Beachten Sie dabei den Zusammenhang mit der Wellenlänge, das heißt der Arbeitsfrequenz des RFID-Systems in Tabelle 2.1.

Reichweite bei magnetischer Kopplung

RFID-Systeme von LF (um 125 kHz) und HF (13.56 MHz und 27 MHz) sind magnetisch über Leiterschleifen (Spulen) gekoppelt. Im Nahbereich fällt das magnetische Feld H entlang der Spulenachse als Funktion des Abstands r mit $1/r^3$ ab, was in der Praxis einem starken Abfall entspricht²⁵. Sehr nahe an der Spule und abhängig von Windungszahlen und Durchmesser der

²⁴In der Literatur wird noch zwischen *strahlendem* und *reaktivem* Nahfeld unterschieden, vergl. [SS05]

²⁵Die Energie E_H des magnetischen Feldes ist proportional zur Feldstärke im Quadrat, also $E_H \sim H^2$. Damit sinkt die Leistung mit dem Abstand mit $\sim 1/r^5$

Spulen von Lesegerät und Transponder bleibt die Feldstärke über einen gewissen Abstand r konstant²⁶.

Reichweite elektromagnetischer Strahlung

Bei RFID-Systemen im UHF- (868, 900 MHz) und Mikrowellenbereich (2.45, 5.8 GHz) liegen vergleichsweise kurze Wellenlängen vor. Hier ist das Fernfeld von Interesse, dessen Leistung mit dem Abstand r wie $\sim 1/r^2$ abfällt²⁷, also deutlich langsamer als bei der magnetischen Kopplung.

2.9.2. Absorption

Der **Absorptionskoeffizient**²⁸ a , gibt den exponentiellen Abfall der Intensität einer Strahlung durch **Absorption** im Medium an, siehe Tabelle 2.1.

Die elektromagnetische Strahlung wird beim Durchgang durch Materie geschwächt. Die Länge, bei der die Intensität auf den Faktor $1/e$, etwa 37%, abgefallen ist²⁹, bezeichnet man als **Absorptionslänge**. Sie ist ein sehr anschauliches Maß für die Fähigkeit der Funkwellen, Materie zu durchdringen. Die ungefähren Werte für RFID-Frequenzen sind in Tabelle 2.1 aufgeführt.

Absorptionskoeffizient

Absorptionslänge

Zwar nimmt mit höheren Frequenzen die Funkreichweite prinzipiell zu, jedoch werden bei Frequenzen vom **UHF-** bis **SHF**-Bereich Umwelteinflüsse wie Nebel oder Regen oder beispielsweise auch Feuchtigkeit von Transportpaletten zunehmend spürbar.

2.9.3. Reflexion

Für die Funkübertragung spielt die **Reflexion** eine wichtige Rolle. Darunter versteht man das Zurückwerfen der einfallenden Strahlung durch Objekte und Oberflächen. Reflexion ist erwünscht, wenn die einfallenden Funkwellen eines RFID-Lesegeräts vom Transponder möglichst stark reflektiert werden. Dieser Effekt wird bei den Systemen mit Frequenzen oberhalb 868 MHz ausgenutzt.

Reflexion

Andererseits kann Reflexion an Oberflächen in der Umgebung das Lesen von Transpondern erschweren oder unmöglich machen. Die zurückgeworfenen Wellen von der Leseantenne überdecken dabei das sehr schwache Echo der Transpondersignale.

²⁶Falls in einem konkreten Anwendungsfall Berechnungen notwendig werden, sei auf die Literatur wie [Fin06] verwiesen.

²⁷Umgeben wir eine Antenne, welche eine konstante Leistung P_{ges} in alle Richtungen abstrahlt mit einem kugelförmigen Luftballon. Die Oberfläche des Ballons ist $4\pi r^2$. Durch ein beliebiges Flächenelement F fließt also eine Leistung P_F , die umgekehrt proportional zur Gesamtoberfläche des Ballons ist, also $P_F(r) \sim P_{ges}/4\pi r^2$

²⁸Der Absorptionskoeffizient a gibt nach dem *Lambert-Beerschen Gesetz* die exponentielle Schwächung der Intensität einer Strahlung nach Zurücklegen der Wegstrecke x durch Absorption an. Ist die ursprüngliche Intensität P_0 , dann gilt für die Intensität P nach Zurücklegen der Weglänge x : $P(x) = P_0 \cdot e^{-ax}$. Dabei ist $e = 2.71828$ die *Eulersche Zahl*.

²⁹Die *Absorptionslänge* ist der Kehrwert des Absorptionskoeffizienten, siehe auch Fußnote 28

2. Grundlagen

BackscatterSysteme

Das Verhalten wird von den Abmessungen reflektierender Objekte und der Wellenlänge λ der einfallenden Strahlung bestimmt. Abmessungen, welche kleiner als 0.1λ sind, können in der Praxis völlig vernachlässigt werden, vergl. [Fin06]. Objekte mit Abmessungen vergleichbar mit der Wellenlänge, verhalten sich ähnlich wie Antennen, man spricht daher vom **Resonanzbereich**. Bei RFID-Transpondern wird dieser Bereich in den sogenannten **Backscatter-Systemen**³⁰ ab 868 MHz ausgenutzt, siehe auch Abschnitt 2.10.

Bei großen Objekten verglichen mit der Wellenlänge spielt ausschließlich die Geometrie und der Einfallswinkel der Welle eine Rolle. Die Reflexion gleicht der eines spiegelnden Objekts bei Lichteinfall. Man spricht daher vom **optischen Bereich** der Reflexion.

2.9.4. Echoreichweite

Ohne weitere Herleitungen werden hier die fundamentalen Beziehungen für die Reichweite einer rückgestreuten Welle wiedergegeben, um die grundlegenden Gesetzmäßigkeiten plausibel zu machen, welche die Reichweite von RFID-Systemen nach dem Rückstreuprinzip beschreibt.



Die Rückstreuung elektromagnetischer Strahlung wird in der **RADAR**-Technik verwendet

Rückstreuquerschnitt

Betrachten wir eine Leseantenne als Sender und eine Transponderantenne als rückstreuendes Objekt, welche sich im Abstand r zur Antenne des Lesegeräts befindet, siehe Bild 2.10. Sendet der Leser mit der Leistung P_R über seine Antenne mit Gewinn G , so beschreibt Gleichung 2.27 die am Transponder einfallende Strahlungsdichte S_T . Die Transponderantenne streut nun einen Teil der einfallenden Strahlungsdichte S_T zurück zur Lese-Antenne. Wieviel sie reflektiert, hängt von ihrem **Rückstreuquerschnitt**³¹ σ ab. Gleichung 2.28 gibt die an der Leseantenne empfangene Strahlungsdichte S_B des rückgestreuten Echos an. Die Abhängigkeit mit $1/4\pi r^2$ von der Entfernung r ist in Fußnote 27 erläutert.

$$S_T = \frac{G \cdot P_R}{4\pi \cdot r^2} \quad (2.27)$$

$$S_B = \frac{\sigma \cdot S_T}{4\pi \cdot r^2} \quad (2.28)$$

Modulation

Der Rückstreuquerschnitt σ hängt von Form, Ausrichtung und Eigenschaften des reflektierenden Objekts ab. Seine Abhängigkeit von der Wellenlänge λ der Strahlung wird in der Literatur mit $\sigma \sim 1/\lambda^2$ angegeben, vergl. [Ung88, MG92]. Das bedeutet, dass die Stärke der Rückstreuung mit dem Quadrat der Frequenz anwächst.

Ändern sich die elektrischen Eigenschaften der Antenne und des mit ihr verbundenen Schwingkreises – siehe Bild 2.2 –, ändert sich auch der Rückstreuquerschnitt σ . Modulation im Transpon-

³⁰engl. *backscatter*: Rückstreuung

³¹in der Literatur auch als *Rückstrahlquerschnitt*, *Radarquerschnitt* oder *Echoquerschnitt* bezeichnet

der bewirkt damit eine **Modulation** der rückgestreuten Wellen - auch **modulierte Rückstreuung** genannt. Auf diese Art werden Daten zum Lesegerät übertragen, siehe Abschnitt 2.10.

Hat die Empfangsantenne – also die Antenne des Lesegeräts – eine wirksame Fläche A , erhalten wir aus der Strahlungsdichte S_B des rückgestreuten Signals die empfangene Leistung P_B an der Antenne³²: $P_B = A \cdot S_B$. Mit den Gleichungen 2.27 und 2.28 erhalten wir Gleichung 2.29.

$$P_B \sim \frac{A \cdot G \cdot P_R}{\lambda^2 \cdot (4\pi \cdot r^2)^2} \quad (2.29)$$

$$r_{max} \sim \sqrt[4]{\frac{A \cdot G \cdot P_R}{\lambda^2 \cdot 16\pi^2 \cdot P_{B,min}}} \quad (2.30)$$

Um ein rückgestreutes Signal in einem Empfänger erkennen zu können, ist stets eine Mindestleistung $P_{B,min}$ erforderlich. Setzen wir diese in Gleichung 2.29 ein und lösen nach r auf, erhalten wir die Beziehung für die **maximale Reichweite** r_{max} für ein RFID-System in Gleichung 2.30.

maximale Reichweite

Aus den Abhängigkeiten in hoher Potenz (4-te Wurzel!) in Gleichung 2.30 ergeben sich wesentliche Erkenntnisse für die Reichweite in RFID-Anwendungen:

- Abhängigkeit von effektiver Fläche (Größe) und Gewinn der Antenne des Lesegeräts
- Empfindlichkeit des Empfängers
- Reichweite steigt mit der Wurzel aus der Frequenz ($\sim 1/\lambda$)
- Um die Reichweite zu verdoppeln, wird die 16-fache Sendeleistung P_R benötigt

Damit sind bereits die physikalischen Grenzen des Möglichen aufgezeigt, mit denen wir uns auch noch im Zusammenhang mit **Sicherheit** und **Datenschutz** in Kapitel 7 beschäftigen werden.

2.10. Elektromagnetische Kopplung

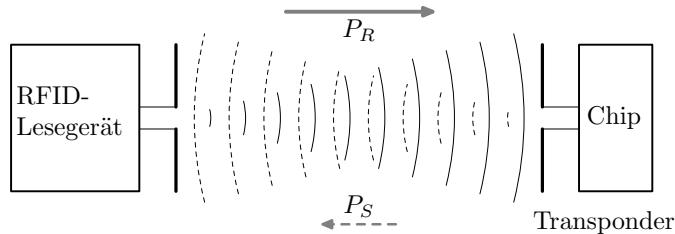


Bild 2.10.: Kopplung über elektromagnetisches Feld

³²weitergehende Zusammenhänge zwischen wirksamer Fläche und Gewinn einer Antenne sind hier nicht weiter berücksichtigt

2. Grundlagen

Diese Art der Kopplung findet in den **Backscatter-Systemen** ab den RFID-Frequenzen von 868 MHz aufwärts Anwendung.

Die Antenne des Lesegeräts erzeugt eine elektromagnetische Welle, welche in der Antenne des Transponders eine Spannung erzeugt. Diese Spannung wird in passiven Transpondern gleichgerichtet und dient der **Energieversorgung** des Mikrochips, wie in Bild 2.2 skizziert. Die vom Lesegerät zum Transponder übertragene Leistung P_R fällt mit dem Quadrat der Entfernung. Daraus ergibt sich eine maximale Entfernung – die **Energierreichweite** –, bei welcher der Chip des Transponders noch ausreichend mit Energie versorgt und der Transponder überhaupt aktiviert werden kann.

Die Transponderantenne streut einen Teil der empfangenen Leistung zurück. Diese rückgestrahlte Leistung P_B fällt ebenfalls mit dem Quadrat der Entfernung r zur Empfangsantenne. Auf diese Abhängigkeit in vierter Potenz zu r sind wir ausführlich in Abschnitt 2.9.4 eingegangen.

Die Übertragung der Daten vom Transponder zum Lesegerät erfolgt durch Variation des Rückstreuquerschnitts und bewirkt damit die **Modulation** der rückgestreuten Leistung P_B , wie in Bild 2.10 der Pfeil andeutet. Man spricht dabei auch vom **modulierten Rückstreuquerschnitt**.

Das Lesegerät demoduliert das empfangene Signal und dekodiert daraus die vom Transponder gesendeten Daten.

2.11. RFID-Frequenzen und Eigenschaften

Die folgenden Abschnitte fassen die Eigenschaften der derzeit verwendeten Frequenzen für RFID-Anwendungen zusammen und geben einen Überblick über Frequenzbereiche.

2.11.1. Eigenschaften der Frequenzen

Die Wahl der Frequenz ist entscheidend für die Funktionssicherheit einer RFID-Anwendung. Dies liegt daran, dass sich die Eigenschaften elektromagnetischer Wellen mit der Frequenz ändern. Diese werden dem sichtbaren Licht^{33,34} immer ähnlicher, je höher die Frequenz ist.

Diagramm 2.12 zeigt qualitativ die Eigenschaften typischer RFID-Frequenzen und fasst die Erkenntnisse aus den Abschnitten 2.9.1, 2.9.2 und 2.9.3 auf einen Blick zusammen.

Mit der Frequenz nimmt die **Reflexion** an Oberflächen von Materialien, insbesondere Metallen, zu. Auch sinkt mit der Frequenz die Fähigkeit elektromagnetischer Wellen, Materie zu durchdringen. Dies liegt an der **Absorption** der Energie, welche dabei in Wärme³⁵ umgewandelt wird. Daher ist der Frequenzbereich $\geq 868 \text{ MHz}$ für die Etikettierung von flüssigen Waren

³³Fernes Infrarot beginnt bei 3 THz, entsprechend $\lambda < 1000 \mu\text{m}$

³⁴Licht wird in der Literatur üblicherweise nicht mehr über die Frequenz, sondern über die *Wellenlänge* spezifiziert, siehe Gl. 2.25, z.B. sichtbares Licht violett bis rot – $380 \text{ nm} < \lambda < 780 \text{ nm}$

³⁵Beispiel hierfür ist die *Mikrowelle* zum Erwärmen von Speisen, oder *Kurzwellenbestrahlung* in der Medizin

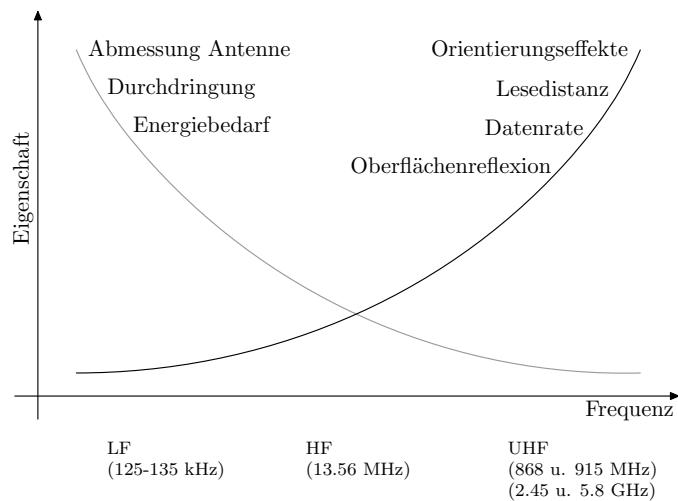


Bild 2.11.: Frequenzbereiche und relevante Eigenschaften für RFID nach [Ker06]

oder für am oder im Körper getragene Identifikations-Transponder wenig geeignet, siehe auch Kapitel 4.

2.11.2. Frequenzbänder

Nach dem derzeitigen Stand benutzt die RFID-Technologie bestimmte Frequenzbereiche, welche unter der Voraussetzung, dass bestimmte Regeln und Vorschriften eingehalten werden, ohne Einzelgenehmigung der Anlage betrieben werden dürfen. Sie nutzen die **ISM**-Frequenzen, siehe Abschnitt 1.5. Diese Frequenzen sind im Diagramm 2.12 zusammen mit einer Auswahl anderer Funkdienste dargestellt. Bei der Darstellung sind auf der x-Achse die Frequenzen, dazugehörigen Wellenlängen und allgemeine Bezeichnung der Frequenzbänder dargestellt. Auf der y-Achse sind die maximal zulässigen **Feldstärken** (bei $f < 30MHz$) beziehungsweise relativen **Sendeleistungen** (bei $f > 30MHz$) aufgetragen. Diese gelten in der Darstellung nur für die RFID-Frequenzbereiche. Beachten Sie, dass beide Achsen logarithmisch dargestellt sind.

Bei der Zulassung der Frequenzbereiche existieren nationale Unterschiede. Ein besonderes Problem stellt RFID im UHF-Bereich dar. In Europa darf hierfür nur der Bereich von 865 bis 868 MHz mit maximal 2 W ERP, siehe **ETSI EN 302-208**, genutzt werden. In den USA gilt der Bereich um 915 MHz mit 4 W [Rob04]. In Europa beispielsweise sind 915 MHz für den Mobilfunk im GSM900-Band reserviert.

Gleiches gilt auch für die maximal zulässige Sendeleistung, welche unter Umständen auch davon abhängt, ob das RFID-System innerhalb oder außerhalb von geschlossenen Gebäuden betrieben wird.

Die jeweiligen Vorschriften sind derzeit noch im Wandel begriffen und sollten bei der Planung einer Anwendung im Zweifelsfall mit den aktuellen Vorgaben der zuständigen Regulierungsbe-

2. Grundlagen

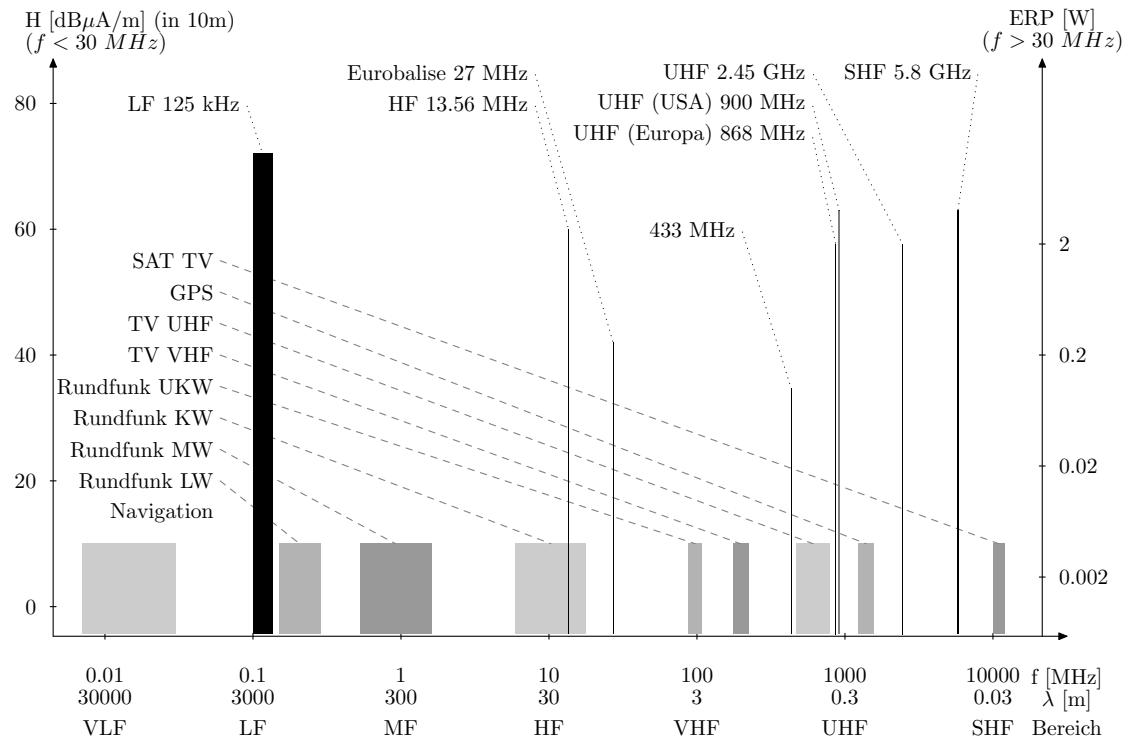


Bild 2.12.: Verfügbare Frequenzbereiche für RFID nach [Fin06, Zim00], Erläuterung siehe Text

hörde³⁶ abgeglichen werden.

³⁶In Deutschland: Bundesnetzagentur ([BNetzA](#))

2.12. Zusammenfassung

- RFID-Lesegerät und -Transponder kommunizieren über den freien Raum (Luftschnittstelle)
- Die Übertragung von Energie und Daten erfolgt über das Magnetfeld bei der induktiven Kopplung oder das elektromagnetische Feld bei Backscattersystemen.
- Lesegerät und Transponder sind auf einen bestimmten Frequenzbereich abgestimmt. In diesem Bereich sind die Schwingkreise der Komponenten in Resonanz.
- Antennen bei induktiver Kopplung sind Spulen, Datenübertragung erfolgt über Lastmodulation.
- Bei elektromagnetischer Kopplung streut der Transponder Strahlung zurück. Die Datenübertragung erfolgt über die Modulation des rückgestreuten Anteils.
- Frequenz, Antennengrößen und Ausrichtung der Komponenten zueinander beeinflussen die Verbindung zwischen Lesegerät und Tag.
- Die mögliche Reichweite hängt von der verwendeten Frequenz ab. Ferner beeinflussen Absorption und Reflexion die Verbindung.
- Für die Modulation mit binären Daten existieren unterschiedliche Verfahren.

2.13. Übungen



Übung 2.1. Zwischen einem Lesegerät und einem Transponder werden Energie und Informationen übertragen. Über welche Schnittstelle erfolgt dieser Austausch?

Übung 2.2. Nennen Sie die zwei wichtigsten Verfahren zur Kopplung zwischen RFID-Lesegerät und Transponder.

Übung 2.3. Welche Faktoren beeinflussen die maximale Distanz, zwischen denen ein Lesegerät und ein RFID-Transponder betrieben werden können?

Übung 2.4. Bei der Kommunikation spielt auch die Ausrichtung des Transponders zum Lesegerät – also räumliche Lage, Winkel – eine wichtige Rolle. Erklären Sie qualitativ, warum das so ist?

Übung 2.5. Transponder und Lesegerät arbeiten in der Regel auf einem bestimmten Frequenzbereich. Welches sind die Gründe dafür?

Übung 2.6. Zu den wichtigsten RFID-Verfahren zählen die Backscatter-Systeme. Durch welche grundlegenden Parameter wird deren Reichweite bestimmt?

3. RFID-Systeme

Nach der Einführung in die physikalischen Grundlagen wollen wir uns mit der Realisierung von RFID-Systemen befassen. Beispiele für Anwendungen folgen in Kapitel 4.

Auch bei RFID unterscheidet man offene und geschlossene Systeme - wir greifen diese Begriffe und Beispiele dazu in Abschnitt 4.1.4 auf.

*Unter einem **geschlossenen** System versteht man ein abgeschlossenes Umfeld, beispielsweise eine Bibliothek, welches jedes entleihbare Objekt mit einer Identifikationsnummer, einer **ID**, versieht. Außerhalb der Anwendung hat diese **ID** keinerlei Bedeutung.*

:=

*In **offenen** Systemen hat beispielsweise die eindeutige Bezeichnung einer Kaugummisorte in Form der Artikelbezeichnung – kodiert als **EAN** oder **UPC** in Barcode oder als RFID-Tag – auch weiterhin eine Bedeutung, wenn der Artikel längst bezahlt und das Geschäft verlassen ist.*

:=

Bei den offenen Systemen knüpfen die Bedenken von einigen Verbraucherschützern an. Die Artikelnummer lässt nämlich einen eindeutigen Bezug zu Hersteller und Produkt und gegebenenfalls ein Kaufverhalten zu.

Beispiel 3.1. Der neue **ePass** und **Personalausweis** sind ein Beispiel für ein offenes System. Auf dem Transponder sind personenbezogene Daten wie der volle Name, Geburtsdatum und weitere Merkmale wie Fingerabdrücke gespeichert.



Durch die schnell wachsende Bedeutung der Technologie wird auch die verbindliche Beschreibung durch **Normen** vorangetrieben, welche die Voraussetzung insbesondere für funktionierende offene Systeme sind. Auch wenn diese längst noch nicht abgeschlossen ist, wollen wir – mehr ist in diesem Rahmen nicht möglich – eine Übersicht mit einigen Referenzen geben¹.

Normen

¹eine Vielzahl weiterer Normen befinden sich derzeit in Vorbereitung oder Überarbeitung. Für die Planung konkreter RFID-Projekte sollte stets der aktuelle Stand abgefragt werden.

3.1. Normen und Spezifikationen

Die verschiedenen **IEC/ISO**-Normen beschreiben die grundlegenden Funktionen eines RFID-Systems. Sie spezifizieren – entsprechend dem **OSI-Referenzmodell** – die einzelnen Schnittstellen zwischen RFID-Lesegerät und Transponder und garantieren so, dass auch Lesegeräte und Transponder verschiedener Hersteller untereinander kommunizieren können. Sie definieren dabei sowohl die physikalische Schicht mit Trägerfrequenzen, Codierung, Timing, Modulationsverfahren und Datenübertragungsraten als auch Vielfachzugriffsverfahren, Befehlsumfang, Reichweiten, und Datensicherheit (Authentifizierung, Verschlüsselung). Auch Aspekte wie mechanische und chemische Beständigkeit und der Umweltverträglichkeit bei der Entsorgung werden erfasst, vergl. [LFH05a, LFH05b].

Einen kleinen Ausschnitt fassen Tabellen 3.1 und 3.2 zusammen. Eine kompakte Übersicht hierzu bieten beispielsweise [Fin06, AIMb, AIMa]

3.1.1. Langwelle LF 125-134 kHz

ISO 18000-2

Den **LF**-Systemen liegt im Wesentlichen der *ISO 18000-2*-Standard zugrunde, welcher die physikalische Schicht der Kommunikation, das Protokoll, die Befehle und die Methoden für Anti-Kollision – siehe Abschnitt 3.5 – behandelt. Es existieren zwei unterschiedliche Typen von Tags.

Typ-A (FDX)

Der **Typ-A**, welcher bei 125 kHz vom Lesegerät ständig mit Leistung versorgt und im **Vollduplex-Modus (FDX)** betrieben wird. Der **Typ-B** wird bei 134.2 kHz im **Halbduplex-Modus (HDX)** betrieben [ISOb].

Die unterschiedlichen Modi werden in Abschnitt 3.2 behandelt.

Typ-B (HDX)

3.1.2. Hochfrequenz HF 13.56 MHz

ISO 15693

Im weltweit standardisierten HF-Frequenzbereich bei 13.56 MHz wurde die *ISO 15693* für kontaktlose Chipkarten veröffentlicht – siehe Tabelle 3.1 – welche Übertragungsraten von 1.6 kbit/s bzw. 6.6 kbit/s bei Reichweiten bis 1 m ermöglicht (**Vicinity-coupling**). Damit können etwa 20 Transponder pro Sekunde erfasst werden [LFH05a, LFH05b].

ISO 14443

Die **proximity-coupling**-Karten der *ISO 14443* unterscheidet sich von der zuvor genannten Norm durch eine höhere Übertragungsrate von 106 kbit/s und eine Reichweite bis maximal 15 cm [LFH05a, LFH05b].



In der ISO 14443 sind jedoch zwei nicht miteinander kompatible Kartentypen beschrieben, den **Typ-A** und den **Typ-B**. Eine RFID-Karte muss dabei nur einen der beiden Typen unterstützen. Jedoch muss ein **kompatibles Lesegerät** beide Kommunikationsarten unterstützen [Fin06].

Typ-A

Bei der Datenübertragung von Lesegerät → Karten vom **Typ-A** wird bei 100%-**ASK**-Modula-

3.1. Normen und Spezifikationen

Tabelle 3.1.: ISO/IEC-Standards (nach [AIMa, Fin06])

Standard	Gruppe	Anwendungsbereich
ISO/IEC 18000-1	Luftschnittstellen	Referenzarchitektur
ISO/IEC 18000-2	Luftschnittstellen	Luftschnittstelle unterh. 135 kHz
ISO/IEC 18000-3	Luftschnittstellen	Luftschnittstelle - 13.56 MHz
ISO/IEC 18000-6	Luftschnittstellen	Luftschnittstelle - 860-960 MHz
ISO/IEC 18046-1	Testmethoden	Leistung von RFID-Systemen
ISO/IEC 18047-2	Testmethoden	Konformität - Luftschnittstelle unterh. 135 kHz
ISO/IEC 15961	Datenprotokoll	Anwendungsinterface
ISO/IEC 15962	Datenprotokoll	Transponderinterface
ISO/IEC 15963	Datenprotokoll	Eindeutige Identifizierung
VDI 4470	Anwendung	Waren sicherungssysteme
VDI 4472-1	Anwendung	Textile Kette - allgemein
ISO/IEC 21007-1	Anwendung	Gaszyylinder - allgemein
ISO/IEC 69873	Anwendung	Datenträger für Werk- und Spanzeuge
ISO/IEC 10373	Kontaktlose Chipkarten	Testmethoden für kontaktlose Chipkarten
ISO/IEC 10374	Anwendung	Containeridentifikation - aktive Mikrowellentransponder
ISO/IEC 11784	Tieridentifikation	Code Struktur
ISO/IEC 11785	Tieridentifikation	Technische Konzepte
ISO/IEC 14223	Tieridentifikation	„advanced transponders“ - Teile -1 bis -3
ISO/IEC 10536	Kontaktlose Chipkarten	„Close coupling“ - Reichweite 0...1 cm
ISO/IEC 14443	Kontaktlose Chipkarten	„Proximity coupling“ - Reichweite 0...10 cm
ISO/IEC 15693	Kontaktlose Chipkarten	„Vicinity coupling“ - Reichweite 0...1 m
ISO/IEC 24753	Sensoren	
ISO/IEC 18092		NFC IP 1
ISO/IEC 21481		NFC IP 2

tion² – Kapitel 2.8, Bild 2.9a – eine modifizierte **Millercodierung** verwendet. Dabei sind die Austastlücken nur 2 – 3 μ s kurz, so dass eine kontinuierliche Energieversorgung erreicht wird.

²siehe Bild 2.9 auf Seite 32

Tabelle 3.2.: EPC globale Standards (nach [AIMa])

Bezeichnung	Anwendungsbereich
UHF Class 0 Version 1	Luftschnittstelle - UHF - Readonly
UHF Class 1 Version 1	Luftschnittstelle - UHF - Write once read many times
HF Class 1 Version 1	Luftschnittstelle - 13.56 MHz - Write once read many times
UHF Generation 2 Version 1.0.9	Luftschnittstelle - UHF - Read/Write
HF Generation 2	Datenprotokoll (mehrere Standards zu Datenablage, Anwendungsinterface, API , Object Naming Service, Reader- steuerung und Codierung)

:=

*Die Richtung der Datenübertragung vom Lesegerät zum Transponder bezeichnet man auch als **Downlink**.*

Hilfsträger

Bei der Datenübertragung von der Chipkarte → Lesegerät wird ein Lastmodulationsverfahren mit **Hilfsträger** eingesetzt. Die Hilfsträgerfrequenz ist f_H beträgt $847 \text{ kHz} = 13.56 \text{ MHz}/16$ und wird im Transponder einfach mit einem Binärteiler aus der Grundfrequenz erzeugt. Der Hilfsträger wird mit dem Datenstrom von der Chipkarte in **Manchester**-Codierung durch Ein-Aus-Tastung moduliert [Fin06].

:=

*Die Datenübertragung vom Transponder zum Lesegerät bezeichnet man als **Uplink**.*

Typ-B

Bei Karten vom **Typ-B** kommt für den Downlink eine 10%-**ASK**-Modulation zum Einsatz. Die Bits werden in **NRZ** kodiert. Für den Uplink vom Transponder zum Lesegerät erfolgt eine Lastmodulation mit dem Hilfsträger $f_H = 847 \text{ kHz}$. Dabei werden die Daten 180° phasenmoduliert – siehe Bild 2.9c. Vergl. [Fin06]

Close coupling-RFID-Chipkarten nach *ISO 10536* bieten gegenüber kontaktbehafteten Karten kaum Vorteile und haben sich auf dem Markt nicht durchgesetzt [Fin06].

3.1.3. UHF 868 - 915 MHz

Gen2

Auch bei den Systemen im UHF-Band existieren unterschiedliche Normen. Mit dem **Gen2-Protokoll** wird ein einheitliches, global gültiges Protokoll mit den folgenden Eigenschaften zur Verfügung gestellt [Fin06]:

- gegenseitige Störung benachbarter Lesegeräte wird durch den **Dense-Reader-Mode** ver-

hindert.

- Aufteilung des Speichers auf dem Transponder in vier unabhängige Sektoren
- mehrerer Transponder dürfen identischen EPC enthalten, womit Transponder wie Barcodes gehandhabt werden können.
- veränderte Bitcodierung auf dem HF-Interface verbessert Detektionsrate

3.1.4. Elektronischer Produktcode

Der **Electronic Product Code (EPC)** erlaubt die eindeutige Identifikation eines Objekts und hat seit 2006 den Status eines Industriestandards erreicht. **EPCglobal Network** bietet über Internet verfügbare Dienste wie den **Object Naming Service (ONS)** und den **Electronic Product Code Information Service (EPCIS)** um Logistikprozesse zu unterstützen, vergl. [Fin06] und Kapitel 4.3.

EPC

Tabelle 3.3.: EPC Code Typ 1 - Klasse 1 (nach [Ker06])

Bezeichnung	Datenlänge	Verwendung
Header	8 bit	Versionsnummer
epc Manager	28 bit	Firma, Hersteller (verantwortlich für Zuteilung <i>Object Class</i> und <i>Serial Number</i>)
Object Class	24 bit	Objektart, Artikelbezeichnung
Serial Number	36 bit	Seriennummer des Einzelobjekts
Item Information	32 bit	Information zum Einzelobjekt

Der EPC-Code besteht heute aus 128 Bit, der sich entsprechend Tabelle 3.3 zusammen setzt. Die Unternehmens- und Artikelbezeichnung (epc Manager, Object Class) entspricht dem in Barcodes verwendeten EAN/UCC-Code.

Eine Vielzahl weiterer Codierungen existieren in **96 bit** und **64 bit**, siehe beispielsweise [Fin06, Flö05b].

Grundsätzlich trägt jeder Transponder eine eindeutige, nicht veränderbare Seriennummer als transpondereigene Kennung aus mehreren Byte. Diese wird bei seiner Herstellung festgelegt und macht ihn einzigartig. Sie wird ein Mal geschrieben und kann beliebig oft gelesen werden (WORM). Diese Transponder-Seriennummer ist unabhängig von den Informationen, die in einem eventuell vorhandenen Datenbereich dem Anwender des Tags zur Verfügung gestellt werden.



Dieser Seriennummer³ kommt bei den Zugriffsverfahren in Abschnitt 3.5 besondere Bedeutung zu.

3.1.5. Sensoren

Sensoren

Ein weiterer interessanter Ansatz ist die Kopplung von **Sensoren** mit aktiver RFID-Technik zur Erfassung und Protokollierung von Parametern wie beispielsweise Temperatur. Hierfür befindet sich die ISO 24753 in Entwicklung [AIMb, RFI06].

Bei den Sensor-Anwendungen spielen auch **Oberflächenwelle-Transponder** eine wichtige Rolle, siehe auch Abschnitt 5.1.4.

3.2. Voll- und Halbduplex-Übertragung

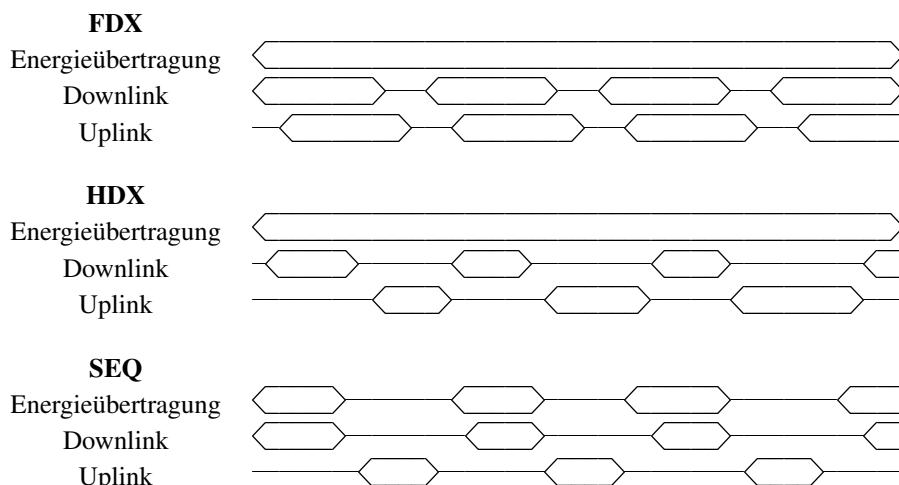


Bild 3.1.: Zeitliche Abläufe bei Voll- und Halbduplex und sequenziellen Systemen (nach [Fin06])

Abgesehen von den 1-bit Transpondern zur Diebstahlsicherung enthalten die meisten Transponder einen Datenspeicher in Form eines Mikrochip, der bis zu einigen kByte an Daten enthalten kann. Um diese Informationen auszulesen, müssen zwischen Lesegerät und Transponder Daten ausgetauscht werden. Dies kann auf zwei unterschiedliche Arten geschehen, dem Vollduplex- und dem Halbduplex-Verfahren, siehe Bild 3.1.

Vollduplex Beim **Vollduplex (FDX)** findet die Datenübertragung vom Lesegerät zum Transponder und vom Transponder zum Lesegerät – also in beide Richtungen – **gleichzeitig** statt. Bei LF- und

³engl. *unique number*

HF-Systemen werden häufig Verfahren angewendet, bei denen die Daten des Transponders auf Frequenzen übertragen, die sich aus der Teilung der Frequenz des Lesegeräts ergeben – also auf **subharmonischen** Frequenzen. Im UHF- und Mikrowellenbereich erfolgt die Übertragung durch den **modulierten Rückstreuquerschnitt**, siehe Kapitel 2.10.

Erfolgt die **Uplink**-Übertragung der Daten vom Transponder **abwechselnd** von der **Downlink**-Übertragung der Daten vom Lesegerät zum Transponder, spricht man von **Halbduplex (HDX)**. Bei LF- und HF-Systemen erfolgt dies durch **Lastmodulation** mit oder ohne Hilfsträger.

Halbduplex

Beiden Verfahren gemeinsam ist die **kontinuierliche Energieübertragung** vom Lesegerät zum Transponder – also unabhängig von der Datenübertragung. Dazu im Gegensatz existieren **sequenzielle Systeme**, bei denen die Energieübertragung vom Lesegerät zum Transponder immer nur während einer begrenzten Zeitspanne erfolgt. Die Datenübertragung vom Transponder zum Lesegerät erfolgt mit der gespeicherten Energie während der Pausen. Man spricht von **Pulsbetrieb** und **gepulsten Systemen**. Gepulste Systeme sind immer Halbduplex-Systeme⁴. Vorteil der sequenziellen Systeme ist, dass die Datenaussendung des Transponders in völliger Ruhe von Signalen des Lesegeräts erfolgt. Dies erleichtert die Detektion der stets vergleichsweise schwachen Transpondersignale.

sequenzielle Systeme

3.3. Datenintegrität

Um Fehler bei der wechselseitigen Übertragung zwischen RFID-Lesegerät und Transponder zu erkennen und gegebenenfalls korrigieren zu können, werden den eigentlichen Daten noch **Prüfbits** angefügt.

Dabei kommen die folgenden Verfahren zum Einsatz, vergl. [Fin06]:

Paritätsprüfung⁵ Den Nutzdaten wird ein weiteres Bit als Prüfbit angefügt. Dieses Bit wird entsprechend der Daten so gesetzt, dass insgesamt eine **gerade Anzahl** von 1-Bits bei **gerader Parität**⁶ entsteht. Bei **ungerader Parität**⁷ wird das Prüfbit auf eine **ungerade Anzahl** von 1-Bits ergänzt. Ein einzelner **Bitfehler** kann zwar **erkannt** aber **nicht korrigiert** werden.

Längssummenprüfung Bei der Längssummenprüfung (**LRC**) werden alle Bytes der zu übertragenden Daten bitweise mit **XOR** verknüpft und ergibt 1 Byte Prüfsumme, welches zusammen mit den Daten übertragen wird. Beim Empfang werden alle Datenbytes und die Prüfsumme wieder nacheinander mit XOR verknüpft. Das Ergebnis muss 0 ergeben, falls die Übertragung korrekt war. Auch **Mehrfehler** können erkannt werden, sofern sie sich nicht gegenseitig aufheben. Eine Fehlerkorrektur ist auf Grund der Vieldeutigkeit nicht möglich.

⁴[Fin06] weist darauf hin, dass in der Literatur bisweilen *gepulste System* mit *Halbduplex* und in Folge fälschlicherweise *ungepulste System* mit *Vollduplex* gleichgesetzt werden.

⁵engl. *parity check*

⁶engl. *even parity*

⁷engl. *odd parity*

Zyklischer Redundanzcheck Mit dem in vielen Bereichen häufig eingesetzten **CRC**-Verfahren können auch größere Datenblöcke mit einer Prüfung versehen werden. Die zu übertragenen Daten werden mathematisch als Polynom betrachtet und werden durch ein bestimmtes Polynom, dem **Generatorpolynom** geteilt, wobei sich ein Rest ergibt. Dieser Rest wird den zu sichernden Daten angefügt. Werden alle Daten wieder durch das Generatorpolynom geteilt, muss das Ergebnis 0 ergeben. **CRC** erlaubt auch die Erkennung **mehrfacher Fehler** und bis zu gewissen Grenzen deren **Korrektur**.

Allen Verfahren gemeinsam ist, dass sie einfach mit logischen Schaltungen in Hardware zu realisieren sind und schnell arbeiten. Für weitergehende Informationen sei auf die Literatur verwiesen.

3.4. Codierung

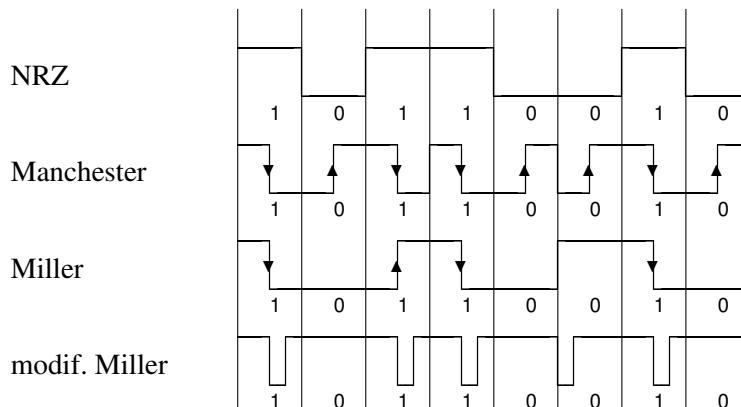


Bild 3.2.: Beispiele Signalcodierung bei RFID

Unter der **Codierung** versteht man an dieser Stelle die Umsetzung einer binären Zeichenfolge in einen elektrischen Pegel oder die Modulation einer Trägerfrequenz.

Bei der **NRZ**-Codierung werden Signale entsprechend ihrem logischen Wert umgesetzt. Beim Übergang von 0 auf 1 oder umgekehrt erfolgen Flankenwechsel genau an der Bitgrenze.

Bei der **Manchester**-Codierung⁸ erfolgt bei jedem Bit ein Flankenwechsel in der Mitte jedes Bit. Bei der 1 wird eine negative Flanke erzeugt, bei der 0 eine positive. Die Manchester-Codierung erlaubt **Kollisionserkennung**, wie wir im Folgenden Abschnitt 3.5 sehen werden.

Weitere Formen der Codierung bei RFID sind die **Miller**- beziehungsweise **modifizierte Miller**-Codierung. Bei der Miller-Codierung erfolgt bei der 1 stets ein Flankenwechsel in der

⁸auch *bi-phase* genannt

3.5. Zugriffsverfahren - Antikollision

Bitmitte. Eine auf eine 1 folgende 0 behält den Pegel, eine weitere 0 erzeugt einen Flankenwechsel bei Beginn des neuen Bit. Der modifizierte Millercode erzeugt statt eines Flankenwechsels einen kurzen Impuls, bei der 1 in der Bitmitte, bei der Null am Anfang des Bit, falls der Millercode dort einen Wechsel erzeugen würde.

Bild 3.2 zeigt nur einen Ausschnitt aus den möglichen Codierungen für RFID.

3.5. Zugriffsverfahren - Antikollision

Für die Kommunikation zwischen einem Transponder und einem Lesegerät ist es erforderlich, dass für die Zeitdauer der Datenübertragung eine ungestörte Verbindung besteht. Dies bedeutet, dass zu einem gegebenen Zeitpunkt immer nur ein Transponder seine Daten zum Lesegerät sendet, und andere im Lesefeld befindliche so lange schweigen. In anderen Worten ausgedrückt darf ein Kommunikationskanal zu einem gegebenen Zeitpunkt in der Regel nur von zwei Kommunikationspartnern benutzt werden und bleibt auch so lange zugeteilt, wie die Verbindung besteht⁹.

immer nur einer

Vielfachzugriffs- und Antikollisionsverfahren sind möglich durch eine Trennung in

Raum (**SDMA**: Space Division Multiple Access) Durch räumliche Trennung ist der Betrieb mehrerer Systeme gleichzeitig möglich



Zeit (**TDMA**: Time Division Multiple Access) Mehrere Systeme an einem selben Ort arbeiten parallel durch zeitliche Einteilung, d.h. einer nach dem anderen.

Frequenz (**FDMA**: Frequency Division Multiple Access) Am selben Ort zur gleichen Zeit können mehrere Partner kommunizieren, wenn sie unterschiedliche Frequenzen benutzen.

Codierung (**CDMA**: Code Division Multiple Access) Unterschiedliche Codierung ermöglicht gleichzeitige Kommunikation

Wir wollen dies kurz an den folgenden Ausführungen erläutern.

3.5.1. Räumliche Trennung



Beispiel 3.2. Wollen sich mehrere Personen gleichzeitig besprechen, suchen sie unterschiedliche Räume auf. Für RFID-Systeme die parallel und gleichzeitig arbeiten sollen, bedeutet dies, dass Lesegeräte und deren Sendeleistung so ausgerichtet sind, dass sich deren Ansprechbereiche nicht berühren oder überschneiden, also quasi **räumlich getrennt** sind.

⁹Telefonleitung während eines Gesprächs

Räumliche Trennung kann auch durch **Begrenzung der Reichweite** und viele Lesegeräte und Antennen erreicht werden.



Beispiel 3.3. Beispiele sind große sportliche Veranstaltungen, bei denen viele Antennen als Matten ausgelegt werden, welche die Läufer – mit Transpondern ausgestattet – zur Zeitmessung passieren.



Ist eine räumliche Trennung oder Begrenzung der Reichweite nicht möglich, zum Beispiel nebeneinanderliegende mit RFID-Antennen ausgestattete Tore bei Lagerhallen, so können die Leser so betrieben werden, dass sie immer nur kurz hintereinander senden und empfangen, also im **Zeitmultiplex** betrieben werden.



3.5.2. Zeitliche Trennung

Beispiel 3.4. Wollen mehrere Personen effizient und mit sicherer Informationsübertragung kommunizieren, so spricht zu einem gegebenen Zeitpunkt immer nur einer. Auch dafür gibt es mehrere Verfahren:

- der Diskussionsleiter als **master**, der Zeitschlüsse zuteilt oder
- ein Kollisionserkennungsverfahren, bei dem man irgendwann beginnt zu sprechen. Beginnen mehrere gleichzeitig, schweigen sofort alle wieder und jeder beginnt nach einer mehr oder weniger zufälligen Wartezeit



Bei mehreren Transponder im Lesebereich einer Antenne kann ein Datentransfer nur erfolgen, wenn diese **zeitversetzt** antworten. Sie müssen sich den verfügbaren Kanal aufteilen. Die Steuerung der zeitlichen Einteilung kann durch die Transponder oder das Lesegerät erfolgen. Letztere kann man als **synchron** betrachten, weil alle Transponder gleichzeitig kontrolliert werden.

Bei den wichtigsten Antikollisionsverfahren bei RFID werden **TDMA**-Verfahren eingesetzt, siehe Abschnitt 3.5.

3.5.3. Frequenzmultiplex

Beispiel 3.5. Innerhalb gewisser Grenzen kann eine Kommunikation in Personengruppen, zum Beispiel Party, trotzdem möglich sein, obwohl mehrere gleichzeitig sprechen. Voraussetzung sind **unterschiedliche Frequenzen** in den Stimmen (Frau/Mann). Diese Fähigkeit des menschlichen Gehörs nimmt beim Erwachsenen mit dem Alter stetig ab; bei dieser Anforderung macht sich die Schwerhörigkeit am stärksten bemerkbar.



Im UHF-Bereich stehen für RFID-Systeme eine Vielzahl von **Frequenzkanälen** zur Verfügung. Dadurch wird in einem begrenzten Umfang ein gleichzeitiger Betrieb auch bei räumlicher Überschneidung möglich. Nach der Norm **ETSI EN 302-208** stehen in Europa 15 Kanäle im Bereich 865...868 MHz im Abstand von 200 kHz zur Verfügung.



Bei der Benutzung durch RFID-Lesegeräte gilt das Prinzip **Lauschen**, ob der Kanal frei ist (-96 dB), bevor gesendet wird, auch mit **Listen Before Talk (LBT)** bezeichnet¹⁰ [Rob04].

Werden in räumlicher Nähe (Reflexionen) mehr als 15 UHF-Lesegeräte betrieben kann ein zusätzliches Zeitmultiplexing der Leser notwendig werden.

Bei aktiven Transpondern im Sinne von Telemetriesendern (Short Range device) kann ein Lesegerät über den Downlink-Kanal einzelne Transponder anweisen, auf einer bestimmten aus den zur Verfügung stehenden Frequenzen $f_1 \dots f_N$ zu senden. Ein Beispiel dafür wäre das **ISM**-Band 433...435 MHz.

3.5.4. Codemultiplex

Da man in realen Anwendungen davon ausgehen kann, dass dicht beieinander liegende RFID-Systeme den gleichen RFID-Standard verwenden, kommt ein Codemultiplex nicht wirklich in Frage. Der Codierung jedoch kommt eine besondere Bedeutung zu, weil bestimmte Codes die Erkennung von Kollisionen möglich macht, siehe Abschnitt 3.6

3.6. Kollisionserkennung

Zu den Gepflogenheiten in einer Gesprächsrunde gehört, siehe Beispiel 3.4, einer sprechenden Person nicht ins Wort zu fallen – also den Kanal abzuhören und erst zu senden, wenn sonst niemand spricht. Wir haben zuvor dieses Prinzip als „Listen Before Talk“ kennen gelernt. Was aber passiert, wenn zwei Personen gleichzeitig zu sprechen beginnen? Normalerweise erkennen

¹⁰Die EN 302-208 ersetzt die EN 300-220 und damit die auf 0.5 W begrenzte Sendeleistung und den duty cycle $\leq 10\%$

3. RFID-Systeme

Kollision

beide diese sogenannte **Kollision** und handeln entsprechend bestimmter Regeln. Diese Kollisionserkennung wollen wir nun etwas genauer betrachten.

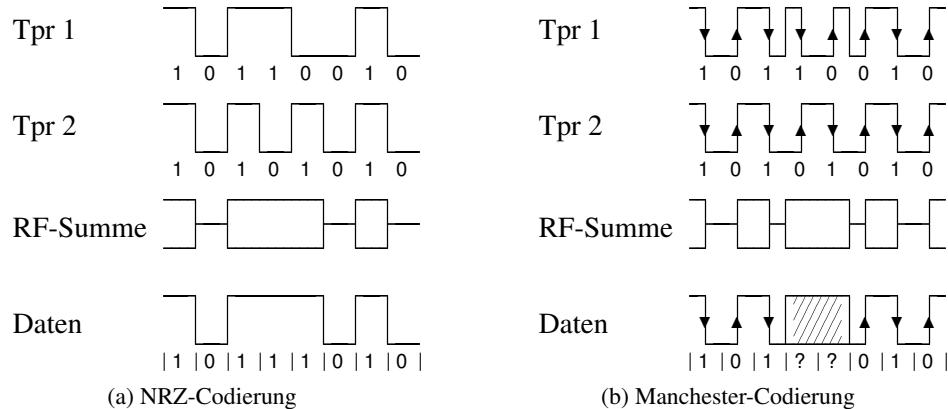


Bild 3.3.: Kollision mit NRZ- und Manchester-Codierung

Senden zwei Transponder (Tpr) gleichzeitig eine unterschiedliche Bitfolge, so entsteht ein Hochfrequenz (RF)-Summensignal, welches sich aus den Signalen beider Transponder zusammen setzt. Decodiert das Lesegerät das empfangene Signal, wird bei der NRZ-Codierung in Bild 3.3a eine falsche Zeichenfolge empfangen. Die **Kollision**, das heißt Überlagerung zweier Signale wird anhand der Daten **nicht unbedingt erkannt!**, siehe Bild 3.3. Lediglich ein Fehler in der Prüfsumme (Parität oder CRC), siehe Abschnitt 3.3, kann auf die Kollision hinweisen.

Auch bei der Manchester-Codierung in Bild 3.3b entsteht aus der Überlagerung beider Transponder ein RF-Summensignal. Jedoch entsteht bei der Decodierung ein **ungültiger** Datenstrom. Damit kann die **Kollision erkannt** werden, weil die Codierung der mit „?“ gekennzeichneten Bits nicht der Manchester-Codierung entspricht.

Bei der Manchester-Kodierung kann nicht nur eine Kollision, sondern auch das kollidierende Bit erkannt werden. Diese Tatsache ist von Bedeutung für **Suchalgorithmen** zur Erkennung, welche Transponder sich gleichzeitig im Ansprechbereich des Lesegeräts befinden.

3.7. Antikollisions-Verfahren

Bei RFID-Systemen muss grundsätzlich zwischen zwei Formen der Kommunikation unterscheiden werden.

Sendet das Lesegerät, wird die Nachricht von allen im Ansprechbereich vorhandenen Transpondern empfangen. Diese Form der Übermittlung entspricht dem **Rundfunk**¹¹

¹¹engl. broadcast

Bei der zweiten Form der Kommunikation übertragen viele einzelne Transponder ihre Daten zum Lesegerät – was man als **Vielfachzugriff**¹² bezeichnet. Da die **Kanalkapazität** beschränkt ist, muss sie den einzelnen Transpondern in geeigneter Form zugeteilt werden, damit keine gegenseitige Störung – **Kollision** – auftritt. Im Folgenden werden kurz zwei Verfahren beschrieben, welche auf **TDMA** beruhen.

Vielfachzugriff

3.7.1. Reader- und transpondergetriebene Verfahren

Bei den Methoden zur *zeitlichen* Kollisionsvermeidung und Mehrfachzugriffs werden **lesergetriebene**¹³ und **transpondergetriebene**¹⁴ Verfahren unterschieden.

Ein lesergetriebenes Verfahren ist **synchron**, ein transpondergetriebenes **asynchron**, vergl. [Fin06, S. 219 f], [Kad95, S. 155 f.], [DB96, S. 276 f.] und [BLSR].

3.7.2. ALOHA- und Slotted-ALOHA-Verfahren

Beim reinen **ALOHA**-Verfahren kann jeder Teilnehmer zu einem beliebigen Zeitpunkt ein Datenpaket fester Länge versenden. Tritt eine **Kollision** mit einem anderen Teilnehmer auf, wartet jeder der betroffenen Teilnehmer eine zufällig lange Zeit und beginnt erneut mit dem Senden. Der Durchsatz hängt stark von der Nutzung des Kanals, **mittleres Verkehrsangebot**¹⁵ G genannt, ab. Das Maximum des Durchsatzes S liegt bei 18% wenn $G \approx 0.5$. Im günstigsten Fall bleiben so mehr als 80% der Kanalkapazität ungenutzt.

ALOHA

Der geringe Durchsatz des **ALOHA**-Verfahrens lässt sich optimieren, indem eine definierte Anzahl Zeitschlüsse – **Slots** – festgelegt werden, in denen ein Transponder senden darf. Auch hier wird angenommen, dass die Übertragungsdauer τ für alle Pakete gleich groß ist. Die Dauer der Zeitschlüsse wird entsprechend kurz gewählt. Der Leser **synchronisiert** für alle Transponder deren Beginn. Dieses Verfahren wird als **slotted ALOHA (S-ALOHA)** bezeichnet. Durch die Verkürzung des Intervalls¹⁶ verringert sich die Wahrscheinlichkeit einer Kollision – der maximal mögliche Durchsatz S steigt auf etwa 37%, vergl. [Fin06].

**slotted ALOHA
(S-ALOHA)**

Weiterhin kann der Durchsatz des **slotted ALOHA**-Verfahrens auf die Anzahl Transponder im Lesebereich verbessert werden, indem die Anzahl verfügbarer Zeitschlüsse vom Lesegerät **dynamisch** angepasst werden kann. Dieses Verfahren wird als **dynamisches slotted-ALOHA** bezeichnet.

**dynamisches
S-ALOHA**

¹²engl. *multiple access*

¹³engl: *interrogator (reader) driven*

¹⁴engl: *transponder driven*

¹⁵in einem Beobachtungszeitraum T , der Übertragungsdauer τ_i für ein Paket und die Häufigkeit r_i der Aussendung eines Teilnehmers i im Zeitraum T sowie und der Anzahl der Teilnehmer $n = 1, 2, \dots$ gilt für das *mittlere Verkehrsangebot*

$$G = \sum_{i=1}^n \frac{\tau_i}{T} \cdot r_i$$

¹⁶siehe Fußnote 15

Da Transponder stets über eine **eindeutige Seriennummer, SNR** verfügen, können mit den folgenden Kommandos die Daten einzelner Transponder gelesen und geschrieben werden, vergl. [Fin06].

REQUEST Synchronisation aller im Ansprechbereich befindlichen Transponder durch das Lesegerät und Aufforderung, in einem der Zeitschlitzte die Seriennummer zu übertragen.

SELECT(SNR) Auswählen (Selektieren) des Transponders mit der zuvor ermittelten Seriennummer (SNR). Alle übrigen Transponder reagieren jetzt nur noch auf das REQUEST-Kommando.

KOMMANDO nur für den zuvor ausgewählten Transponder, zum Beispiel Lesen oder Schreiben von Daten.

3.7.3. Binäre Suche

Die binäre Suche¹⁷ von Transpondern im Ansprechbereich des Lesegeräts ist ein iterativer Algorithmus. Mit dem REQUEST(SNR)-Befehl kann das Lesegerät alle Transponder mit dieser oder einer kleineren Seriennummer veranlassen diese zu senden. Vorausgesetzt, alle angesprochenen Transponder übertragen genau zur gleichen Zeit, kann bei Kollisionen die exakte Position kollidierender Bits ermittelt werden, siehe Abschnitt 3.6. Bei einem kollidierenden Bit befinden sich genau zwei Transponder im Ansprechbereich, welche sich in diesem Bit unterscheiden. Bei zwei Bit sind es bis zu vier, bei drei Bit bis zu acht usw. Die Suche wird in einen **binären Baum**^{18,19} aufgeteilt. In wenigen Schritten kann so ein einzelner Transponder gefunden werden. Interessant dabei ist die Tatsache, dass die Anzahl der notwendigen Iterationen sich nur logarithmisch zur Anzahl der Transponder verhält, also eine Verdopplung der Anzahl den Suchaufwand nur jeweils um eins erhöht. Die für dieses **Antikollisionsverfahren** notwendigen Befehle werden um das Kommando UNSELECT erweitert, der den zuvor mit SELECT(SNR) ausgewählten Transponder – auch für REQUEST – stumm schaltet.

Binärbaum

ALOHA- und binäres Suchverfahren sind auch als Beispiele in [Fin06] ausführlich dargestellt.

3.8. Statistische Betrachtung von ALOHA und Slotted-ALOHA

Es kann jeweils nur ein Tag vom Lesegerät erfasst werden. Sind mehrere Tags im Lesefeld, so beginnen sie mit der Übertragung ihrer ID, sobald sie durch das elektromagnetische Feld des Lesers ausreichend mit Energie versorgt sind. Findet eine zeitliche Überschneidung der Übertragungen von zwei oder mehr Transpondern statt, tritt eine *Kollision* auf – die übermittelten Daten sind unbrauchbar.

¹⁷engl. *binary search*

¹⁸engl. *binary tree*

¹⁹für weitergehende Informationen siehe Literatur

Um diesen Fall einer Kollision – oder besser den Fall *keiner* Kollision – genauer zu betrachten, stellen wir die folgenden Annahmen und Überlegungen an. Sei τ die *Dauer der Einzelübertragung* und sei diese für alle Transponder gleich. Sei p die Wahrscheinlichkeit, dass zwei - oder mehrere - Übertragungen kollidieren, dann ist $q = 1 - p$ die Wahrscheinlichkeit einer ungestörten Übertragung. Es gebe ferner n Transponder, welche unabhängig und zufällig voneinander senden.

Diese Art Fragestellung tritt häufig auf, beispielsweise in einem Geschäft bei zufälliger Ankunft von Kunden und der daraus folgenden Anzahl Bedienungen. Oder die Betrachtung der Wahrscheinlichkeit, dass n Ereignisse - wie zum Beispiel der Ausfall von zwei Speicherplatten - innerhalb eines bestimmten Zeitraums auftreten. Diese Art der Fragestellung wird durch die Poisson-Statistik beschreiben.

3.8.1. Poisson-Statistik

Man kann λ die *Ereignisrate* nennen.

Die Poisson²⁰-Verteilung P_n beschreibt die Wahrscheinlichkeit wie häufig ein Ereignis n , in einem gegebenen Zeitraum τ erfolgt:

Poissonverteilung

$$P_n(\tau) = \frac{(\lambda\tau)^n \cdot e^{-\lambda\tau}}{n!} \quad (3.1)$$

mit

λ	Ereignisrate
τ	Betrachtungszeitraum
n	Anzahl statistisch voneinander unabhängiger Ereignisse
$n! = n \cdot (n - 1) \cdot (n - 2) \cdot \dots \cdot 1$	und $0! = 1$

(3.2)

Beispiel 3.6. Angenommen, ein Gerät falle 2 mal in 1000 Stunden aus. Wie groß ist die Wahrscheinlichkeit, dass dieses Gerät 2 mal in 1 Stunde ausfällt?

$$\lambda = \frac{2}{1000}; n = 2; \tau = 1$$

$$\begin{aligned} P_n(\tau) &= \frac{(\lambda\tau)^n \cdot e^{-\lambda\tau}}{n!} \\ P_2(1) &= \frac{\left(\frac{2}{1000} \cdot 1\right)^2 \cdot e^{-\frac{2}{1000} \cdot 1}}{2!} \\ &= 1.996 \cdot 10^{-6} \end{aligned}$$



²⁰Siméon Denis Poisson, frz. Physiker u. Mathematiker, *21.06.1781, † 25.04.1840

3.8.2. ALOHA

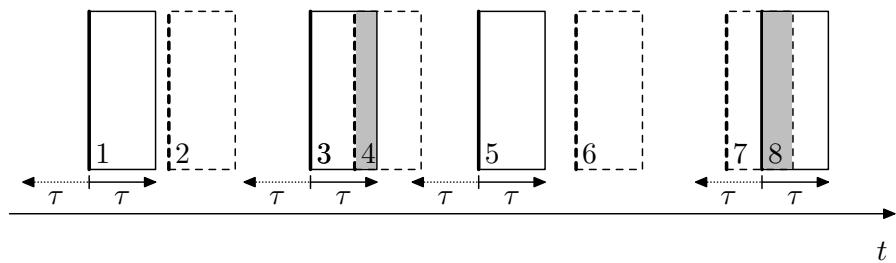


Bild 3.4.: Zufälliges Eintreffen der Datenpakete beim reinen ALOHA. Die Dauer der Übertragung eines Datenpaketes ist τ . Überschneiden sich zwei Pakete, tritt eine Kollision auf (graue Bereiche). Fette Linien markieren den zeitlichen Beginn eines Pakets. Die einzelnen Pakete sind im linken unteren Teil nummeriert. Weitere Erläuterungen siehe im Text.

Bild 3.4 zeigt die Situation des reinen *ALOHA*²¹, bei dem einzelne Datenpakete zufällig eintreffen. Die sendenden Stationen wissen nichts darüber, ob gerade eine Übertragung stattfindet²². Durchgezogene und gestrichelt gezeichnete Pakete dienen der Beschreibung aus statistischer Sicht. Die Übertragungsdauer aller Pakete sei einheitlich τ , der zeitliche Beginn eines Pakets ist mit einer durchgezogenen Linie gekennzeichnet. Wir betrachten die folgenden Überlegungen aus der Sicht der durchgezogenen gezeichneten Pakete. Trifft ein Paket (durchgezogene Linien) ein, dann wird es genau dann *ungestört* übertragen, wenn im Zeitraum τ vor seinem Start *und* im Zeitraum τ nach seinem Start keine Übertragung eines anderen Pakets beginnt (fette gestrichelte Linie). So wird Paket 1 ungestört übertragen, weil keine weitere Übertragung in den Zeitraum von 2τ fällt. So werden auch die Pakete 2, 5 und 6 ungestört übertragen.

Paket 3 wird nicht durch ein zuvor im kritischen Zeitraum τ gesendetes Paket gestört, wohl aber durch Paket 4, welches in den Zeitraum nach Beginn der Übertragung fällt. Paket 3 und 4 werden durch *Kollision* unbrauchbar.

Paket 8 wird durch ein zuvor im kritischen Zeitraum τ gesendetes Paket 7 gestört. Auch hier sind die Pakete 7 und 8 durch *Kollision* zerstört.

Die durchgeföhrten Betrachtungen können wir auch aus der Sicht der gestrichelten Pakete mit gleichem Ergebnis durchführen.

²¹als erstes stochastisches Zugriffsverfahren (random access) 1970 an der Universität Hawaii entwickelt und implementiert, [Kad95]

²²der Kanal wird beim und vor dem Senden nicht überwacht. Daher gibt es kein *listen before talk* und keine Kollisionserkennung - *collision detection* - und schon gar keine Kollisionsvermeidung - *collision avoidance*

Für eine mögliche Kollision beziehungsweise *keine* Kollision folgt daraus die Frage:
Wie groß ist die Wahrscheinlichkeit, dass im Zeitraum 2τ kein weiterer Transponder sendet?
 Das hängt davon ab, wie viel *Verkehr* herrscht. Hierzu können wir eine *Rate* oder *Ereignisrate* definieren - in Beispiel 3.6 war diese $\lambda = 2/1000$.

Im Falle der Benutzung eines Kanals durch mehrere Teilnehmer, bei der alle zufällig und völlig unabhängig voneinander senden, erhalten wir mit Gleichung 3.1 die *Wahrscheinlichkeit*, dass *keine Kollision* zwischen Datenpaketen - also $n = 0$ - auftritt.

$$\begin{aligned} P_0(2\tau) &= \frac{(\lambda \cdot 2\tau)^0 \cdot e^{-\lambda \cdot 2\tau}}{0!} \\ &= e^{-\lambda \cdot 2\tau} \end{aligned} \quad (3.3)$$

Sei T der *Zeitraum für die Beobachtung*, τ_i die *Dauer der Benutzung* durch den Teilnehmer i , n deren Anzahl und r_i die Häufigkeit, mit der Teilnehmer i im Zeitraum T sendet. Die *Ereignisrate* mit der Dimension [*Ereignisse/Zeit*] ist damit

$$\lambda = \frac{1}{T} \cdot \sum_{i=1}^n r_i \quad (3.4)$$

Um die Anforderung an den Kanal zu beschreiben, definiert man das sogenannte *Verkehrsangebot* G . Es beschreibt die *angefragte Sendezzeit* pro *Zeiteinheit* und ist damit dimensionslos.

$$G = \sum_{i=1}^n \frac{\tau_i}{T} \cdot r_i \quad (3.5)$$

Vergleichen wir die Gleichungen 3.4 und 3.5 miteinander, und nehmen wir sinnvollerweise an, dass die individuellen Übertragungszeiten τ_i annähernd gleich sind, also τ erhalten wir²³

$$G = \lambda \cdot \tau \quad (3.6)$$

Gleichung 3.3 wird damit zu

$$\begin{aligned} P_0(G) &= \frac{(2G)^0 \cdot e^{-2G}}{0!} \\ &= e^{-2G} \end{aligned} \quad (3.7)$$

Es leuchtet ein, dass der *Durchsatz* S an Nachrichten einerseits vom *Verkehrsangebot* und andererseits von der Wahrscheinlichkeit abhängt dass eine Nachricht überhaupt ungestört übertragen werden kann. Damit ist der Durchsatz für das reine ALOHA

$$S = G \cdot e^{-2G} \quad (3.8)$$

²³man beachte, dass λ beliebige positive Werte, auch > 1 annehmen kann. In diesem Fall ist das Angebot dann größer als die Kapazität. In einem Geschäft würde sich das dann durch eine Warteschlange äußern.

Bei einem Verkehrsangebot von **0.5** wird bei reinen ALOHA ein Durchsatz von maximal bf 18,4% erzielt, siehe Bild 3.5. Das ALOHA-Verfahren ist sehr einfach zu realisieren, aber nicht besonders effizient. Man beachte, dass ALOHA ein *transpondergesteuertes* Verfahren²⁴ ist: Jeder Transponder sendet - ohne den Kanal vorher abzuhören - nach einer mehr oder minder zufälligen Zeit immer wieder seine Kennung.

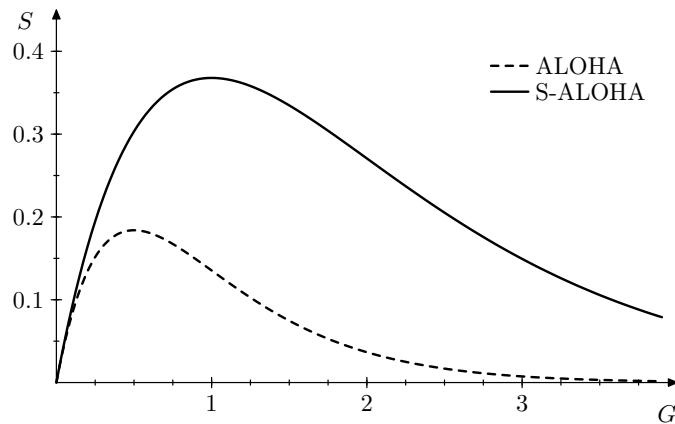


Bild 3.5.: Durchsatz bei ALOHA und Slotted-ALOHA

3.8.3. Slotted-ALOHA

Im vorangegangenen Abschnitt haben wir den begrenzten Durchsatz des ALOHA-Verfahrens kennen gelernt. Liegt in der Zufälligkeit der Aussendung des Pakets jedes einzelnen sendewilligen Transponders. Damit beträgt die Zeitspanne, bei der ein Datenpaket durch Kollision mit einem anderen zerstört werden kann das doppelte der Übertragungsdauer, nämlich 2τ .

Würde man feste Zeitpunkte vorgeben, bei der eine Übertragung beginnen muss, schrumpft diese Zeitspanne für mögliche Kollisionen auf τ , wie aus Bild 3.6 hervorgeht. Die festen Zeitpunkte, *Slot*²⁵ genannt, werden vom Lesegerät vorgegeben²⁶. Das Antikollisionsverfahren ist also *lesergesteuert* und wird als *Slotted-ALOHA* bezeichnet.

Die Wahrscheinlichkeit für eine Kollision in Gleichung 3.3 halbiert sich der *vulnerablen*²⁷ Zeitraum von 2τ auf nur noch τ

$$\begin{aligned} P_0(\tau) &= \frac{(\lambda\tau)^0 \cdot e^{-\lambda\tau}}{0!} \\ &= e^{-\lambda\tau} \end{aligned} \tag{3.9}$$

²⁴engl.: *transponder driven*, asynchrone Übertragung

²⁵engl: *time slot* = Zeitfenster

²⁶engl.: *interrogator (reader) driven*, synchrone Übertragung

²⁷lat: *vulnus* = Wunde, verletzbaren

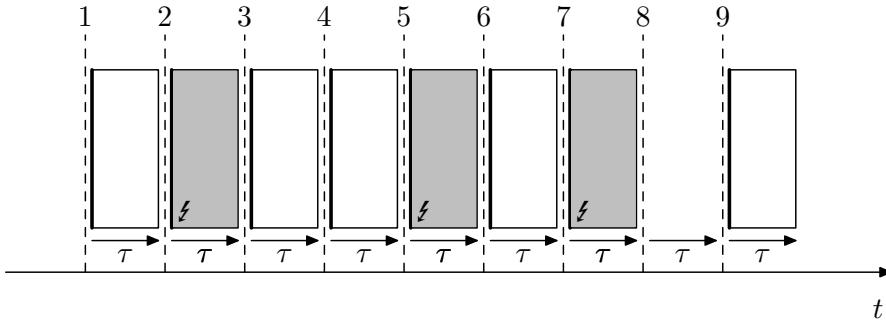


Bild 3.6.: Zeitschlitzte für das Senden von Datenpaketen bei S-ALOHA (Slotted-ALOHA) verhindern das zeitlich zufällige Eintreffen der Datenpakete durch Synchronisation. Die Zeitdauer für mögliche Kollisionen (\cancel{X}) sind auf die Dauer eines Zeitschlitzes (slot) von τ begrenzt, siehe Text. Es kann auch vorkommen, dass in einem Zeitschlitz - wie beispielsweise 8 - keiner der Teilnehmer sendet.

und mit Gleichung 3.6 einen *Durchsatz* S für *Slotted-ALOHA*

$$S = G \cdot e^{-G} \quad (3.10)$$

Slotted (S-ALOHA) erreicht bei einem Verkehrsangebot von **1.0** einen Durchsatz von maximal **36,8%**, siehe Bild 3.5.

Diese Verbesserung des Durchsatzes mag unmittelbar einleuchten, wenn man davon ausgeht, dass im Mittel pro Zeitschlitz ein Datenpaket zur Übermittlung ansteht. Wir müssen uns das Verfahren jedoch etwas genauer betrachten: Das Lesegerät gibt eine Anzahl Zeitschlitzte vor, der Transponder entscheidet per Zufall, welchen er zum Senden seiner Daten wählt.

Bei diesem *lesergesteuerten* Verfahren nutzt das Lesegerät die auf Seite 56 beschriebenen Befehle. Dies ist nur möglich, wenn Transponder stets über eine **eindeutige Seriennummer, SNR** verfügen. Mit den oben beschriebenen Datenpaketen überträgt ein Transponder ausschließlich seine Seriennummer, was sehr schnell erfolgt. Die Dauer τ wird damit klein gehalten. Sobald ein Transponder an Hand seiner Seriennummer erkannt wurde, wird er durch einen *Select*-Befehl ausgewählt, um mit dem nachfolgenden Befehl Daten zu lesen oder zu schreiben, vergl. [Fin06].

REQUEST Synchronisation aller im Ansprechbereich befindlichen Transponder durch das Lesegerät und Aufforderung, in einem der Zeitschlitzte die Seriennummer zu übertragen.

SELECT(SNR) Auswählen (Selektieren) des Transponders mit der zuvor ermittelten Seriennummer (SNR). Alle übrigen Transponder reagieren jetzt nur noch auf das REQUEST-Kommando.

KOMMANDO nur für den zuvor ausgewählten Transponder, zum Beispiel Lesen oder Schreiben von Daten.

3. RFID-Systeme

Beim slotted-Aloha ist die Anzahl der Zeitschlitz fest vorgegeben. Sind wenige Transponder im Feld des Lesegeräts, wird Zeit durch unbenutzte Slots verschenkt, sind viele Transponder im Erfassungsbereich, sinkt durch ein zu hohes Verkehrsangebot in jedem Zeitschlitz der Durchsatz dramatisch. Ideal wäre eine flexible Anpassung der Anzahl zur Verfügung stehender Slots; dies wird im folgenden Abschnitt [3.8.4](#) beschrieben.

3.8.4. Dynamisches Slotted-ALOHA

Das *dynamische Slotted-ALOHA*-Verfahren beruht auf dem S-ALOHA und ist ebenfalls *synchrone* und *lesergesteuert*. Lediglich die Anzahl der zur Verfügung stehenden Zeitschlitz wird *dynamisch* den Gegebenheiten angepasst.

Es gibt zwei Möglichkeiten. Das Lesegerät beginnt den Zyklus mit nur einem oder zwei Zeitschlitz und teilt im *Request* die Anzahl der zur Verfügung stehenden Schlitz mit. Genügt dies nicht für einen gesicherte Ermittlung einer Transponder-ID, wird die Anzahl der *Slots* so lange erhöht ($1, 2, 4, 8, \dots$), bis ein Transponder seine Kennung übermittelte konnte.

Eine andere Möglichkeit ist, von vornherein eine höhere Anzahl Zeitschlitz zur Verfügung zu stellen ($16, 32, 48, 64, \dots$). Mit den *Request*-Kommando fordert das Lesegerät die Transponder zum Senden ihrer **ID** auf und stellt dafür die Anzahl Zeitschlitz zur Verfügung. Sobald eine Transponder-ID gültig übertragen wurde, setzt das Lesegerät einen *Break*-Befehl ab und unterbricht somit weitere Übermittlungen. Danach folgen wie im vorangegangenen Abschnitt [3.8.3](#) die Befehlsabfolge zur Auswahl (*Select*) mit anschließenden Befehlen den Datenspeicher des Transponder betreffend (*Read_Data*, *Write_Data* u.ä.), vergl. [\[Fin06\]](#).

3.9. Zusammenfassung

In diesem Kapitel wurden die folgenden Aspekte behandelt:

- Normen und Standards für RFID-Systeme
- Produktcode und globale Dienste
- Übertragungsverfahren über die Luftschnittstelle
- Datenintegrität und -Codierung
- Antikollisionsverfahren

3.10. Übungen



Übung 3.1. Welche allgemeine Arten des Vielfachzugriffs kennen Sie?

Übung 3.2. Wie kann eine Kollision zwischen zwei Transpondern durch ein Lesegerät erkannt werden?

Übung 3.3. Welches Zugriffsverfahren kann als stochastisch (zufällig) und welches als deterministisch charakterisiert werden?

4. Anwendungen von RFID

4.1. Verbreitete Anwendungen mit RFID

Tabelle 4.1.: Funktionsweise gängiger RFID-Anwendungen

Anwendung	Datenmenge	Funktionsweise	Steuerung	Typ		Frequenz		
				passiv	aktiv	LF	HF	UHF 868-915 MHz
EAS	1 bit	phys.	-	x		<=	x	x
Wegfahrsperre	n Byte		IC	x		x		
Reifendrucksensor	n bit	OFW	-	x				x
Sensoren allg.	n Byte		IC		x		x	x
Container-ID	15 Byte		IC		x			a/a/r ¹
Tier-ID	8-16 Byte		IC	x		x		
Produkt-ID	n Byte		IC	x			x	x
Zugangskontrolle	n Byte		IC	x		x	x	x
Reisepass	n kByte		IC	x			x	
FunktionsKarte	n kByte		IC	x			x	
Nahfeld (NFC)	n kByte		Appl.	x	x		x	

Derzeit verbreitete Anwendungen von **RFID** sind auszugsweise in Tabelle 4.1 dargestellt. Erläuterungen werden an den betreffenden Stellen im Text gegeben. Im folgenden greifen wir einige und typische der vielfältigen Möglichkeiten für den Einsatz von **RFID** auf. Für eine Übersicht, siehe beispielsweise [Ker06].

4.1.1. Artikel-Diebstahlsicherung

Diebstahlsicherung (EAS) in Geschäften sind seit langem durch die großen Antennen an den Ausgängen ein gewohntes Bild. Diese besonders preiswerten Transponder tragen nur 1 Bit an

¹aktivieren, respond - antworten

4. Anwendungen von RFID

Information – Tag im Lesefeld vorhanden oder nicht. Es finden sehr unterschiedliche Frequenzbereiche Anwendung.

EAS-Systeme arbeiten alle nach dem Prinzip des **resonanten Schwingkreises**. Nachgewiesen wird – je nach Verfahren – die **Absorption** von Energie aus dem erregenden Feld (8.2 MHz) oder die Erzeugung von **Oberwellen** aufgrund des nichtlinearen Verhaltens von darin enthaltenem ferromagnetischen Material (10 Hz-20 kHz) oder einer nichtlinearen Kapazitätsdiode (2.45 GHz).

Bei **akustomagnetischen** Systemen wird im Sicherungsmittel ein Metallstreifen durch kurze Impulse (58 kHz) wie eine Stimmgabel zum Schwingen angeregt. Nachgewiesen wird das Ausschwingen. Bei den Hartetiketten (100-135 kHz), welche an der Kasse entfernt werden, erzeugt ein **IC** eine geteilte Frequenz und **Lastmodulation**.

An der Ware verbleibende Transponder werden nach Bezahlung durch ein Magnetfeld deaktiviert, oder ein starkes Wechselfeld zerstört eine Art Sicherung, so dass der Schwingkreis nicht mehr im Überwachungsfeld ansprechen kann. Weitere Details zu diesem Abschnitt, siehe [Fin06]

4.1.2. Fahrzeug Wegfahrsperrre

Eine wahre RFID-Erfolgsgeschichte tragen sehr viele am Schlüsselbund. In allen Zündschlüsseln von Automobilen sind heute **LF-Transponder** eingebaut, die mit einem Lesegerät am **Zündschloß** überprüft werden welches über ein Kontrollmodul mit der Motorsteuerung verbunden ist. Heute werden **kryptografische Verfahren**² angewandt, bei denen sich der Transponder im Zündschlüssel (einseitig) beim Lesegerät **authentifiziert**. Wegfahrsperrren sind ein typische Beispiel für ein **geschlossenes System**, in dem Tags und **IDs** nur innerhalb eine Bedeutung haben.

Die Anzahl der Diebstähle sind seit Einführung drastisch zurückgegangen und nur noch auf Diebstähle des Originalschlüssels oder Abschleppen/Verladen auf Transporter zurückzuführen. Es wurde kein Fall seit 1995 bekannt, bei denen ein Dieb die Wegfahrsperrre überwunden hat [Fin06].

4.1.3. Tier-Identifikation



Der Tieridentifikation kommt eine besondere Bedeutung aus der Sicht der Seuchenprävention zu. Zum Schutz der Verbraucher und der Bestände vor unerlaubter Verwertung oder Verbringung kranker Tiere ist eine **eindeutige** und **fälschungssichere** Kennzeichnung notwendig.

Tieridentifikation mit RFID arbeitet im **LF**-Frequenzbereich, weil die Transponder und Antennen durch Wicklung der Spule auf einen winzigen Ferritkern **sehr klein** hergestellt werden können. Auch ist im Langwellenbereich die **Absorption** im lebenden Gewebe (Wasser) noch **sehr gering** – siehe Kapitel 2.9.2.

²siehe Kapitel 7.1.1 und Fußnoten 4 und 5 auf Seite 94

Die **Kennzeichnung von Tieren** beruht auf der Norm *ISO 11784*, siehe Tabelle 3.1, und beschreibt mit 64 bit (8 Byte) unter anderem einen eindeutigen **Ländercode** nach *ISO 3166* und **einmalige länderspezifische Registriernummer** [Fin06].

ISO 11784

Die Übertragungsverfahren werden in der *ISO 11785* für Halb- und Vollduplex (**HDX** und **FDX**) beschreiben. Hierbei wird den Anforderungen der Massentierhaltung, bei denen häufig mehrere Lesegeräte in Nachbarschaft betreiben werden und gegenseitige Störung zu verhindern ist, Rechnung getragen, vergl. [Fin06].

ISO 14223 beschreibt die **advanced Transponders** welche neben der eindeutigen **ID** einen weiteren, größeren Datenbereich für zusätzliche Informationen bereithält. Dabei ist die **Abwärts-kompatibilität** zu *ISO 14223*-Lesegeräten gewährleistet.

Seit neuestem ist auch die Kennzeichnung von **Heimtieren** wie Hund und Katze mit RFID-Transpondern EU-weit vorgeschrieben. Dabei spritzt der Tierarzt einen Transponders aus Glas oder anderem verträglichen Material von der Größe eines Reiskorns ins subkutane Gewebe³.

Ohrmarke

Bei der Massentierhaltung, beispielsweise Rindern, sind beidseitige **RFID-Ohrmarken** mit Nummernaufdruck üblich. Vorteil ist, dass bei der Anbringung keine zusätzlichen Kosten durch den Tierarzt anfallen. Ohren mit Ohrmarke werden bei der Verarbeitung entfernt und bis zur Kontrolle aufbewahrt. Ein **Implantat** müsste bei der Schlachtung aufwändig entfernt werden, damit es nicht in die Produkte gelangen kann.

Implantat

Weitere Kennzeichnungen wie RFID-Fußring bei Geflügel oder Bolus im Pansen von Rindern haben ihre spezifischen Vor- und Nachteile [Ker06]. Tieridentifikation ist ein **offenes System**, bei dem Registrierungen auch überbetrieblich genutzt werden. Auch eine entlaufene Katze kann über zentrale Verzeichnisse der Tierärzte sofort dem Besitzer zugeordnet werden.

4.1.4. Personen-Identifikation

Ein weites Einsatzgebiet ist die Identifikation von Personen, zum Zweck der **Zugangskontrolle**, **Abrechnung von Dienstleistungen** und bei Ausweispapieren auch zur Erhöhung der **Fälschungssicherheit**. Es können wieder **offene Systeme** und **geschlossene Systeme** unterschieden werden, wie wir sie bereits in Kapitel 3 definiert haben.

Firmenausweis

4.1.5. Geschlossene Systeme

Bei Zugangskontrollen zu Firmengebäuden genügt in der Regel die Vorlage eines **Firmenausweises**. Anhand der **ID** des vorgelegten RFID-Transponders könnte dem Pförtner zu Sicherheit das Foto des Inhabers auf dem Bildschirm angezeigt werden. Zugang zu einzelnen Bereichen kann einfach zentral im Rechnernetz über Rechte dynamisch zugeteilt werden⁴.

Auf diese Art sind **Besuchertickets** auf **Messen**, Schlüssel für **Hotelzimmer** u.v.a.m. realisiert. Bei der **Fußballweltmeisterschaft 2006** wurde der im Ticket eingearbeitete HF-Transponder ge-

Besucherticket

³In der Presse wurde berichtet, dass Diskotheken in Spanien und Holland ihren Gästen den Mitgliedsausweis als **RFID-Implantat** im Oberarm anbieten, vergl. [Hof06]

⁴Flexibilität und Kosteneinsparung gegenüber *konventionellen Schließsystemen* sind beträchtlich

4. Anwendungen von RFID

nutzt, die Kontrolle durch Lesegeräte an den Eingängen zu optimieren und um das Ticket selbst durch die einmalige **ID** auf dem Chip **fälschungssicher** zu machen [Hof06].

Bezahlsysteme

Wird die RFID-Karte auch im Rahmen eines **Bezahlsystems** eingesetzt, so bietet sich die Sicherheit durch **gegenseitige Authentifizierung** von Tag und Leser an. Guthaben und Abbuchungen können dann einfach im **Datenbereich** des Transponders durchgeführt werden.

Weitere Beispiele einer Anwendung dieser Struktur sind **Skipass** oder **Ticket** im **ÖPNV**, welche die Abwicklung deutlich beschleunigen. Dabei interessant der Einbau des Transponders in beispielsweise eine Armbanduhr, welche einfach und schnell vor das Lesegerät gehalten wird.

4.1.6. Offene Systeme

Reisepass

Ein **offenes System** mit hohen Sicherheitsanforderungen sind maschinenlesbare amtliche **Ausweisdokumente** (**MRTD**: Machine Readable Travel Document) mit RFID wie beispielsweise der neu in der EU eingeführte **Reisepass** („**ePass**“) oder den deutschen **Personalausweis** („**ePersonausweis**“), siehe Abschnitt 4.1.7.

4.1.7. Elektronische Ausweisdokumente in Deutschland



(a) Elektronischer Reisepass (ePass)

(b) Elektronischer Personalausweis

Bild 4.1.: Elektronische Ausweisdokumente (Quelle: [BMI])

In Deutschland sind der **elektronische Reisepass**⁵ und der neue **elektronische Personalaus-**

⁵in Deutschland seit 2005 mit elektronischem Passbild, seit 2007 mit Fingerabdruck

weis^{6,7} verfügbar.



Bild 4.2.: RFID Symbol

Nähtere Informationen hierzu sind beispielsweise unter [BMI, BSI, ICA, ePa, Aus] zu finden. Der ePass ist mit dem Symbol in Bild 4.2 eindeutig als elektronisches Dokument gekennzeichnet.

Die Speicherung des **Passbilds** und zukünftig auch von **Fingerabdrücken** im Datenbereich ist verbindlich. **Integrität** und **Authentizität** der auf dem Chip gespeicherten Daten werden über eine **digitale Signatur** abgesichert, vergl. [Fin06]. Damit wird ein hohes Maß an **Fälschungssicherheit** im ePass erreicht.

Fälschungssicherheit

Das kontaktlose HF-Interface der elektronischen Ausweisdokumente entspricht der **ISO 14443**, also einer **maximalen Reichweite** von 10 cm. Ferner wird die für die Antikollision notwendige **Seriенnummer** im Mikrochip des Transponders jedes Mal **zufällig** erzeugt. Somit ist ein **Tracking** anhand der Seriennummer unmöglich.

4.1.8. Identifikation von Büchern und Akten

Als **geschlossene Systeme** lässt RFID sich in **Bibliotheken** einsetzen. Dabei werden Bücher und Medien wie CD/DVD mit beispielsweise HF-Tags versehen. Damit können Ausgabe und Rückgabe nicht nur deutlich vereinfacht, sondern auch automatisiert werden. Auch für die **Inventur** können Regale einfach mit tragbaren Leser- und Erfassungsgeräten abgefahren werden. Auch können die einzelnen Regalfächer mit Antennen⁸ ausgerüstet werden, so dass der Bestand ständig – online – abgeprüft und gesichert werden kann, vergl. [Ker06]. Eine einfache **ID** und Zuordnung in der internen Datenverwaltung ist dabei völlig ausreichend.

Bibliotheksverwaltung

Entsprechend verringern vergleichbare Systeme erheblich den Aufwand und lösen viele Probleme der **Aktenverwaltung** beispielsweise in Anwaltskanzleien. Dort werden Unterlagen häufig bewegt und sind häufig nicht im Haus sondern beispielsweise bei einer Gerichtsverhandlung.

Aktenverwaltung

4.2. RFID in der Automatisierung

Die Erfassung und Verfolgung von Objekten haben wir bereits in den vorangegangenen Abschnitten kennen gelernt. In der Automatisierung können Objekte während ihrer Fertigung zur eindeutigen Identifizierung markiert werden, beispielsweise bei automobilen Fertigungsstraßen und der teilweise sehr individuellen Bearbeitung wie Farben, Sonderausstattung und Motorisierung.

Bei der Fertigung von Produkten aus Holz und Metall spielen **Werkzeugmaschinen** eine herausragende Rolle in der **automatisierten Fertigung**. So unterscheiden sich einzelne **Werk- und Spanzeuge** deutlich in ihrer Beschaffenheit und ihren **Eigenschaften** wie zulässige Drehzahl,

⁶ab November 2010 in Scheckkartenformat mit Biometriemerkmalen

⁷verbindlich mit RFID seit November 2010

⁸RFID book shelf

4. Anwendungen von RFID

Durchmesser und Standfestigkeit. Auch ändern sich Eigenschaften im Laufe des Gebrauchs. Daher liegt es nahe, Daten maschinenlesbar am Werkzeug selbst in einem RFID-Chip unterzubringen.

Werkzeug-
identifikation

Für die **Werkzeugidentifikation** werden LF-Transponder nach **ISO 69873** eingesetzt. Die **induktive Kopplung** ist in metallischer Umgebung gut geeignet. Hersteller programmieren in den Transponder bereits alle **relevanten Werkzeugdaten**. Somit lassen sich sowohl automatisierte Abläufe als auch der **Service** wie Kontrolle, Schärfungen und Radiuskorrekturen durch Dokumentation auf dem Chip selbst optimieren, siehe [Fin06].

Servicedaten

Gepäckmanagement

4.3. Logistikanwendungen

Ein enorme logistische Herausforderung ist das **Gepäckmanagement** an Großflughäfen. Bisher werden meist Barcode-Etiketten verwendet. Deren Erkennungsrate liegt bei etwa 70% pro Leeseinheit [Fra06]. Bei der großen Anzahl Gepäckstücke, den engen Zeitfenstern und drohenden Ersatzleistungen bei Verspätung oder Verlust entstehen hohe Kosten durch manuelle Nachbearbeitung und Rückverfolgung. Einige Flughäfen wie HongKong und LasVegas haben bereits RFID mit UHF-Technologie im Einsatz, andere in Erprobung. Auch bei Pulkerfassung kann von einer individuellen **Erkennungsrate** von über 98% ausgegangen werden [Kiz06].

Container-
identifikation

Frachtcontainer werden mit aktive, batteriegestützten Mikrowellentranspondern ausgestattet. Nach **ISO 10374** werden diese mit einem unmodulierten Trägersignal in UHF, 868-915 MHz oder 2.45 GHz aktiviert, siehe „a“ in Tabelle 4.1, und antworten („r“) mit der Aussendung ihrer Daten auf 2.45 GHz.

In Logistik, Handel und Vertrieb ist der Einsatz von RFID bereits verbreitet. In Kapitel 5 werden diese Anwendungen und deren Architektur näher behandelt.

4.4. Produktsicherheit und Verbraucherschutz

Verbraucherschutz

Eine Reihe von Vorfällen in der Fleischverarbeitung zeigen deutlich die Anforderungen an den **Verbraucherschutz** auf. Mit der RF-Identifikation von **Nutztieren**, Abschnitt 4.1.3 ist eine wichtige Voraussetzung geschaffen, auch Endprodukte von der Quelle bis zum Konsumenten lückenlos und automatisiert mit RFID zu dokumentieren. Neben dem **Produktcode** können Herkunfts-, Verarbeiter- und Transportdaten mit geringem Aufwand im Datenbereich des Tag abgelegt werden. Diese Art der Kennzeichnung des Erzeugers ist als sichtbarer Aufdruck in einigen Ländern der EU bereits üblich.

Kühlkette

Aktive Transponder mit **Sensorfunktion** können beispielsweise **Kühlketten** überwachen und dokumentieren. Eine europäische Untersuchung ergibt, dass *ca. 40% der Eis-Artikel in den Truhen des deutschen Handels leichte sichtbare Mängel aufweisen und bis zu 10% der Eis-Artikel vom Kunden aufgrund der äußerlichen Beschaffenheit als deutlich geschädigt empfunden werden*. Hier bietet die **Überwachung von Umweltparametern** ein enormes **Einsparpotenzial** (20 Mrd.€) [RFI06].

Auch bei **Arzneimitteln** ist durchgängige Kühlung zum Teil sehr wichtig. Bei dieser Produktgruppe spielt auch die **Produktsicherheit** eine herausragende Rolle. Fälschungen dringen zunehmend in den Markt – mit gefährlichen Folgen – ein und verursachen den legitimen Herstellern hohe Verluste. Eindeutige und individuelle Kennzeichnung jeder einzelnen Packung mit RFID wäre ein wirtschaftlich vertretbarer Weg, der auch durch **Rückverfolgbarkeit** beispielsweise kritischer Impfstoffe leichter ermöglicht (Verbraucherschutz). Ferner bietet sich dadurch die Möglichkeit, nicht erlaubte Reimporte und Transfers zu verhindern^{9,10}.

In Ländern wie den USA bedeuten die gesetzlichen Bedingungen zur **Produkthaftung** für Unternehmen ein hohes finanzielles Risiko. Hier können sich Kosten für den Einsatz von RFID zur Verbesserung des Nachweises und der Rückverfolgbarkeit in Produktion und Logistik schnell amortisieren.

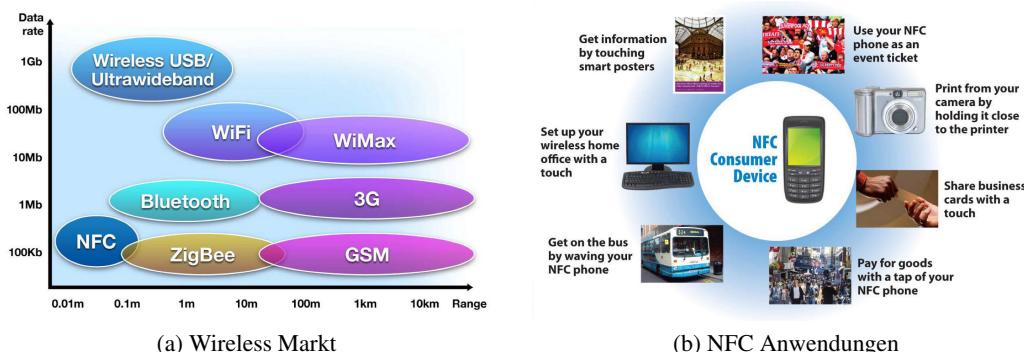
Produktsicherheit

Produkthaftung

4.5. Mobile Computing und Near-Field-Communication (NFC)

Die **NFC**-Technologie hat in den vergangenen Jahren eine rasante Entwicklung erfahren. Inzwischen sind die dazugehörigen Standards stabil und es stehen erste Anwendungen zur Verfügung. Wir beginnen daher mit einer kurzen Übersicht in Abschnitt 4.5.1 um dann im darauf folgenden Abschnitt 4.5.2 in die Technologie einzuführen.

4.5.1. Übersicht



(a) Wireless Markt

(b) NFC Anwendungen

Bild 4.3.: Wireless und NFC-Anwendungen (Quelle: [Mai09])

⁹Weniger wirtschaftsstarken Länder erhalten lebenswichtige Medikamente und Impfstoffe teilweise zu deutlich günstigeren Preisen als Industrienationen.

¹⁰Krankenhäuser erhalten Medikamente bisweilen zu geringeren als dem Apothekenpreis. Derzeit ist schwer nachvollziehbar, ob Händler beim Hersteller für Krankenhäuser einkaufen und zu höheren Margen an Apotheken liefern, vergl. [Swe06]

NFC (Near Field Communication) ist eine neue Technologie zur **drahtlosen Verbindung**, welche existierende Anwendungen der **drahtlosen Kommunikation** und **Identifikation** miteinander verbindet. Dabei schließt NFC eine Lücke im Markt **drahtloser Anwendungen**, siehe Bild 4.3a. Geräte mit NFC vereinfachen für Konsumenten deutlich die Kommunikation untereinander, helfen Informationen zu teilen und machen Bezahlvorgänge sicherer. Bild 4.3b deutet die Vielzahl möglicher Anwendungen an.

NFC: aktiv und passiv

NFC arbeitet bei 13.56 MHz mit Raten bis zu 424 kbit/s. Zur Sicherheit für den Benutzer ist die **Reichweite** auf wenige cm begrenzt [NFCa]. NFC-Schaltungen können sich **aktiv** verhalten, also wie ein preiswertes **RFID-Lesegerät** als auch **passiv** wie einen **Tag**, kompatibel beispielsweise zu den Smart-Cards *ISO 14443 A*¹¹ und *ISO 14443 B*. Eine Vielzahl von Anwendungen ist denkbar und bereits realisiert, hier wenige Beispiele, vergl. [GH06]:

4.5.2. Einführung



Bild 4.4.: NFC-Logo

Eine gute Einführung und Übersicht bietet beispielsweise [Mül09]. NFC wurde im Jahr 2002 von *NXP Semiconductor*® und *Sony*® gemeinsam erfunden. Das *NFC Forum* wurde in 2004 von *NXP*¹², *Sony*® und *Nokia*® eingerichtet. Die ersten kommerziell verfügbaren Telefone gab es 2005 erstmals von *Nokia*. Nach ersten Feldversuchen in 2005 folgten die ersten kommerziellen Anwendungen 2006 in Europa, 2007 weltweit [Mül09].

Bild 4.4 zeigt die offizielle Markierung eines Bereichs, welcher eine NFC-Antenne enthält.

4.5.3. Geschichte

NFC ist eine vergleichsweise neue Technologie und unterliegt derzeit noch weitere Entwicklung. Eine kurze historisch Übersicht der Entstehung von NFC gibt [Mül09]:

2002 NXP und Sony erfinden NFC

2004 NXP, Sony und Nokia rufen das *NFC Forum* ([NFCa]) ins Leben

2005 erstes kommerzielles NFC-fähiges Mobiltelefon verfügbar. Erste Feldversuche.

2006 Produkteinführung in Europa. 100 Mitglieder im *NFC Forum*

2007 weltweite Produkteinführung

2008 150 Mitglieder im NFC Forum

¹¹Beispielsweise *MIFARE*® von *NXP Semiconductors*®, vormals Philips®

¹²eine Übersicht des Herstellers ist beispielsweise unter

[http://www.nxp.com/#/search/params=\[q=NFC,p=1,l=en\]|filters=\[\]](http://www.nxp.com/#/search/params=[q=NFC,p=1,l=en]|filters=[]) und speziell

[http://www.nxp.com/#/pip/pip=\[pfp=50326\]|pp=\[t=pfp,i=50326\]](http://www.nxp.com/#/pip/pip=[pfp=50326]|pp=[t=pfp,i=50326]) zu finden

Tabelle 4.2.: Worldwide Mobile Device Sales to End Users by Vendor in 3Q12 (Thousands of Units). Quelle: Gartner (November 2012)¹³

Vendor	3Q12		3Q11	
	Units ($\cdot 10^3$)	Market Share	Units ($\cdot 10^3$)	Market Share
Samsung	97 956.8	22.9 %	82 612.2	18.7 %
Nokia	82 300.6	19.2 %	105 353.5	23.9 %
Apple	23 550.3	5.5 %	17 295.3	3.9 %
ZTE	16 654.2	3.9 %	14 107.8	3.2 %
LG Electronics	13 968.8	3.3 %	21 014.6	4.8 %
Huawei Device	11 918.9	2.8 %	10 668.2	2.4 %
TCL Communication	9 326.7	2.2 %	9 004.7	2.0 %
Research In Motion	8 946.8	2.1 %	12 701.1	2.9 %
Motorola	8 562.7	2.0 %	11 182.7	2.5 %
HTC	8 428.6	2.0 %	12 099.9	2.7 %
Others	146 115.1	34.2 %	145 462.2	32.9 %
Total	427 729.5	100.0 %	441 502.2	100.0 %

4.5.4. Verbreitung von Smartphones

Man kann davon ausgehen, dass für die Verbreitung der NFC-Technologie und damit Durchsatz am Markt mobile Endgeräte mit ihren hohen Stückzahlen wie PDAs und Smartphones beitragen werden. Tabellen 4.2 und 4.3 geben einen Blick auf die aktuelle Marktentwicklung.

Man kann davon ausgehen, dass das Jahr 2011 für NFC der Beginn der Marktdurchdringung und neuen Anwendungen, auch im Konsumentenbereich sein wird. Darauf verweist die Vorhersage für NFC in Mobilgeräten¹⁵ in Bild 4.5.



Bild 4.5.: World Shipments of NFC-enabled Cellular Handsets (in Millions of Handsets Shipped) IHS Inc. (Feb 2014)¹⁶

¹³Gartner (November 2012): <http://www.gartner.com/newsroom/id/2237315>

¹⁴Gartner (August 2015): <http://www.gartner.com/newsroom/id/3115517>

¹⁵IHS iSuppli: WW forecast of cell phones with integrated NFC capability - 2011: <http://www.isuppli.com/>

4. Anwendungen von RFID

Tabelle 4.3.: Worldwide Mobile Device Sales to End Users by Vendor in 2Q15 (Thousands of Units). Quelle: Gartner (November 2015)¹⁴

Vendor	2Q15		2Q14	
	Units ($\cdot 10^3$)	Market Share	Units ($\cdot 10^3$)	Market Share
Samsung	88 739	19.9 %	97 418	21.9 %
Apple	48 086	10.8 %	35 345	8.0 %
Microsoft	27 690	6.2 %	43 814	9.9 %
Huawei	26 119	5.9 %	18 219	4.1 %
LG Electronics	17 622	4.0 %	18 310	4.1 %
Lenovo & Motorola	16 626	3.7 %	19 266	4.3 %
Xiaomi	16 065	3.6 %	12 541	2.8 %
TCL Communication	15 733	3.5 %	13 923	3.1 %
ZTE	14 560	3.3 %	12 629	2.8 %
Micromax	9 884	2.2 %	8 578	1.9 %
Others	164 634.7	36.9 %	164 148.3	37.0 %
Total	445 758.8	100.0 %	444 190.4	100.0 %

Tabelle 4.4.: Worldwide Mobile Device Sales to End Users by Operating System in 3Q12 (Thousands of Units). Quelle: Gartner (November 2012)¹⁸

Operating System	3Q12		3Q11	
	Units ($\cdot 10^3$)	Market Share	Units ($\cdot 10^3$)	Market Share
Android	122 480.0	72.4 %	60 490.4	52.5 %
iOS	23 550.3	13.9 %	17 295.3	15.0 %
Research In Motion	8 946.8	5.3 %	12 701.1	11.0 %
Bada	5 054.7	3.0 %	2 478.5	2.2 %
Symbian	4 404.9	2.6 %	19 500.1	16.9 %
Microsoft	4 058.2	2.4 %	1 701.9	1.5 %
Others	683.7	0.4 %	1 018.1	0.9 %
Total	169 178.6	100.0 %	115 185.4	100.0 %

Laut dem Marktforschungsunternehmen *GfK*¹⁷ sind im ersten Quartal 2014 bereits 49.9 % der verkauften Smartphones mit NFC ausgestattet. Im März 2012 waren es nur 4.4 %

4.5.5. Smartphone Betriebssysteme

Sehr aufschlussreich ist für die Beurteilung der *NFC*-Technologie ist die Verbreitung der *Betriebssysteme* für Smartphones, siehe Tabelle 4.4. Interessant dabei ist insbesondere *Android*, für das *GOOGLE* eine NFC-Unterstützung anbietet.

¹⁶http://press.ihs.com/sites/ihs.newshq.businesswire.com/files/2014-02-11_NFC.jpg

¹⁷<http://www.cio.de/a/rfid-chip-unterm-fell-total-normal,2958413>

¹⁸Gartner (November 2012), siehe Fußnote 13

¹⁹IDC (2015), <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>

²⁰Gartner (November 2015), siehe Fußnote 14,<http://www.gartner.com/newsroom/id/3115517>

Tabelle 4.5.: Worldwide Smartphone OS Market Share (Share in Unit Shipments. Quelle: International Data Corporation (IDC) (2015)¹⁹

Operating System	Market Share in Period			
	Q1 2012	Q1 2013	Q1 2014	Q1 2015
Android	59.2 %	75.5 %	81.2 %	78.0 %
iOS	22.9 %	16.9 %	15.2 %	18.3 %
Microsoft Phone	2.0 %	3.2 %	2.5 %	2.7 %
BlackBerry OS	6.3 %	2.9 %	0.5 %	0.3 %
Others	9.52 %	1.5 %	0.7 %	0.7 %

Tabelle 4.6.: Worldwide Mobile Device Sales to End Users by Operating System in 2Q15 (Thousands of Units). Quelle: Gartner (August 2015)²⁰

Operating System	2Q15		2Q14	
	Units ($\cdot 10^3$)	Market Share	Units ($\cdot 10^3$)	Market Share
Android	271 010	82.2 %	242 484	83.8 %
iOS	48 086	14.6 %	35 345	12.2 %
Windows	8198	2.5 %	8095	2.8 %
BlackBerry	1153	0.3 %	2044	0.7 %
Others	1229.0	0.4 %	1416.8	0.5 %
Total	329 676.4	100.0 %	290 384.4	100.0 %

4.5.6. Technologie

Der wesentliche Unterschied zwischen dem traditionellen **RFID**- und der **NFC**-Technologie ist die **Aufhebung der strikten Trennung zwischen Lesegerät und Transponder**. Ein NFC-fähiges Gerät kann sich **einerseits wie ein Lesegerät und in einer anderen Rolle wie ein Transponder verhalten**.



Die drei möglichen Grundmuster der Kommunikation eines **NFC**-Geräts sind in Bild 4.6 gezeigt.

NFCAnwendungsarten

4.5.7. Anwendungen

NFC-Anwendungen können in drei Kategorien unterteilt werden, vergl. [Mül09]:

NFCAnwendungsarten

Karten Emulationsmodus²¹ *Transaktions-Modus* wie mobiles Bezahlen, Zugangskontrolle, Ticketing u.v.a.m., siehe Beispiel 4.1

Peer-to-Peer Kommunikation²² *Connectivity* Datenübertragung für schnelle, einfache und be-

²¹ engl. card emulation mode

²² engl. peer-to-peer communication, P2P

4. Anwendungen von RFID

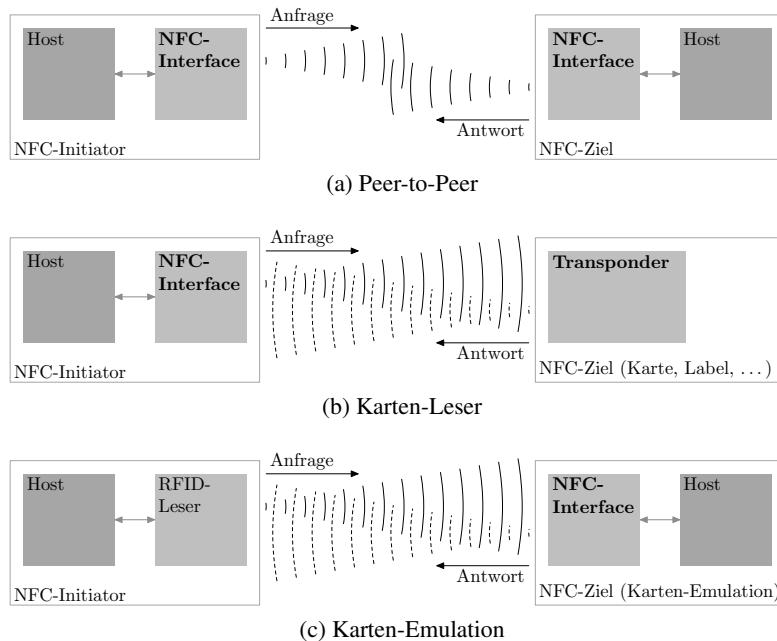


Bild 4.6.: Grundmuster von NFC-Anwendungen:

- (a) Zwei NFC-Geräte kommunizieren miteinander und tauschen Informationen aus. Beide Geräte erzeugen ein HF-Feld und senden aktiv.
- (b) NFC-Gerät fungiert als RFID-Leser für (passive) RFID, Transponder. Die Datenübertragung erfolgt durch Lastmodulation.
- (c) NFC-Gerät emuliert einen passiven RFID-Transponder und überträgt Daten mittels Lastmodulation.

queme Gerätezuordnung, Konfiguration und ähnliches, siehe Beispiele 4.2 und 4.3

Leser-Modus²³ Dienstleistungen wie Zugang zu Diensten, schlanke Werbung²⁴, siehe Beispiele 4.4 und 4.5



Beispiel 4.1. In Wien kann eine **Fahrkarte** mit dem NFC-Handy gekauft werden. An einem Lesegerät baut der Benutzer eine Verbindung mit dem Internet-Portal auf und gibt das Fahrziel ein. Das Ticket, unter Berücksichtigung möglicher Sondertarife kommt sofort auf das Mobiltelefon – zur Bestätigung erhält der Kunde eine kostenlose SMS. Später wird das Ticket mit der Handyrechnung bezahlt. Auch in Deutschland laufen Feldversuche unter anderen in Hanau und München [Kot07].

²³engl. reader mode

²⁴engl. smart advertising

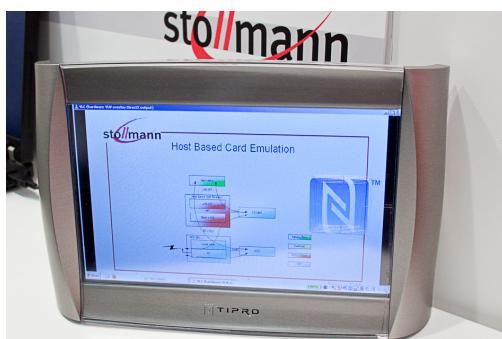
Beispiel 4.2. Fahrpläne für die Rückfahrt aus Paris zum Flughafen können direkt aufs Handy geladen werden, nachdem man auf dem Handy den gewünschten Tag, die Zeit und das Ziel eingegeben hat.



Beispiel 4.3. Austausch von **Informationen** zwischen zwei Handy-Benutzer: Durch Aktivieren der entsprechenden Funktion und Zusammenbringen beider Geräte auf den Abstand von etwa zehn Zentimetern können beispielweise Kontaktdaten schnell und einfach ausgetauscht werden.



Beispiel 4.4. Auf einem mit Bildschirm und NFC-Antenne ausgestatteten **Zahlsteller** beispielsweise in einer Tankstelle läuft kontinuierlich Werbung und Informationen. Interessiert sich der Kunde für nähere Informationen, hält er sein NFC-fähiges Mobiltelefon einfach an die Antenne, und erhält beispielsweise einen Internet-Link auf sein Gerät, siehe Bild 4.7.



(a) Zahlsteller mit Antenne



(b) Mobiltelefon mit NFC

Bild 4.7.: Zahlsteller mit NFC-Anwendung

4. Anwendungen von RFID



Beispiel 4.5. Ein Poster mit RFID-Tag wirbt für ein Konzert. Hält man sein Handy mit NFC über den Tag, liest dieses die Daten, baut direkt eine Telefonverbindung zum Ticket-Center für die Reservierung und Bezahlung auf. Abends dann wird das Handy nur noch vor den Leser am Eingang gehalten und der Einlass erfolgt.

4.5.8. NFC-Architektur und Spezifikationen

Die der NFC-Kommunikation zu Grunde liegende Architektur der Kommunikation zeigt Bild 4.8.

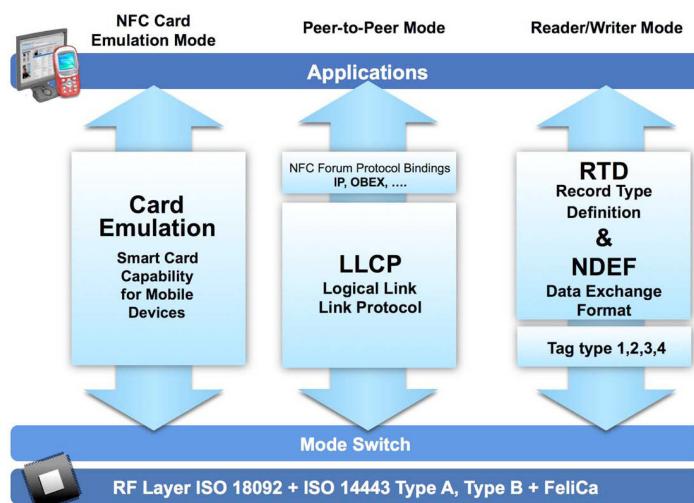


Bild 4.8.: Architektur der NFC-Kommunikation [Mai09]

NFC ist in den folgenden ISO/IEC-, ETSI- und ECMA-Normen beschrieben: *ISO/IEC 18092*, *ISO/IEC 21481*, *ECMA 340, 352, 356*, *ETSI TS 102 190*, [TSI].

Die Definition der Struktur von NFC-Anwendungen und technische Details werden im *NFC Forum*, [NFCa]²⁵, gesammelt, abgestimmt und verwaltet.

4.6. Oberflächenwellen-Transponder

Eine weitere Transponder-Bauart, welche auf rein **physikalischem Prinzip** wie die meisten EAS-Anwendungen in Abschnitt 4.1.1 arbeiten, sind **Oberflächenwellen-Transponder**. Am

²⁵http://www.nfc-forum.org/specs/spec_list

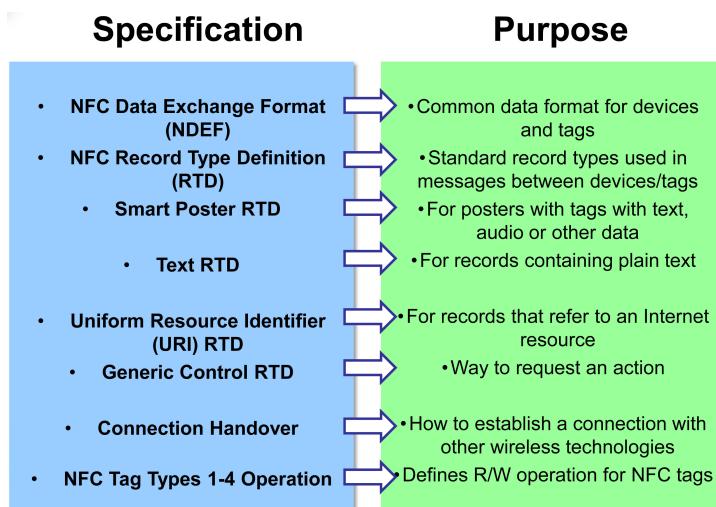


Bild 4.9.: Spezifikationen für die NFC-Kommunikation [Mai09]

Rand eines **piezoelektrischen** Kristalls ist eine Antenne angebracht. Ein kurzer elektromagnetischer Impuls erzeugt in einer Wandlerstruktur (Interdigitalwandler) im Kristall eine mechanische Welle (**OFW**), welche den Kristall entlangläuft. Auf dem Kristall sind in charakteristischen Abständen Streifen aufgebracht, welche die durchlaufende Schallwelle teilweise reflektierenden. Das zurücklaufende Wellenmuster erzeugt im Interdigitalwandler und der Antenne eine Impulsfolge, welche als hochfrequente modulierte Funkwelle zurückgestrahlt wird. Diese Transponder können sehr schnell ausgelesen werden, ca. 100 000 mal pro Sekunde. Der Oberflächenwellen-Transponder kann um passive Sensoren einfach erweitert werden, um auf diese Weise beispielsweise den **Reifendruck** zu messen, vergl. [Fin06]. **OFW**-Transponder sind frei von elektronischen Komponenten und daher für rauen Einsatz auch bei hohen Temperaturen gut geeignet.

Reifendrucksensor

4.7. Medizinische Anwendungen mit RFID

Eine wesentlicher Vorzug passiver RFID-Transponder ist, ohne eine eigene Stromversorgung auszukommen. Damit können sie zuverlässig als **Sensoren** über viele Jahre hinweg, auch im medizinischen Bereich, angewendet werden.



Eine häufige Erkrankung ist das *Glaukom* – der erhöhte Innendruck des Auges kann langfristig zur Erblindung führen. Dieser unterliegt starken Schwankungen. Es scheinen eben die Schwankungen zu sein, welche zur Schädigung führen, weniger der Absolutdruck. Die Messung kann nur beim Augenarzt durchgeführt werden. Um die Krankheit verstehen zu können, wären regel-

4. Anwendungen von RFID

mäßige Messungen im natürlichen Umfeld des Patienten nötig.

Um dies untersuchen zu können, besteht die Möglichkeit eine ohnehin zu ersetzen Augenlinse – beispielsweise beim **grauen Star** – durch eine mit eingebautem Drucksensor und einer passiven RFID-Technologie zu ersetzen. Die Spule des Lesegeräts befindet sich im Gestell einer Brille, vergl. [Fin06, S. 444 ff]. Dies wäre ein Beispiel für eine **Sensoranwendung**.

Weitere Implantate sind die Glastransponder zur Tieridentifikation, siehe Abschnitt 5.1.4. Ein Bolus im Rinderpansen – Abschnitt 4.1.3 – zur Identifikation könnte beispielsweise einfach um einen **Sensor** für die **Körpertemperatur** erweitert werden.

In diesem Bereich können für die nahe Zukunft viele interessante und nutzbringende Anwendungen erwartet werden.

4.8. Szenario Anwendungsbereiche in Deutschland

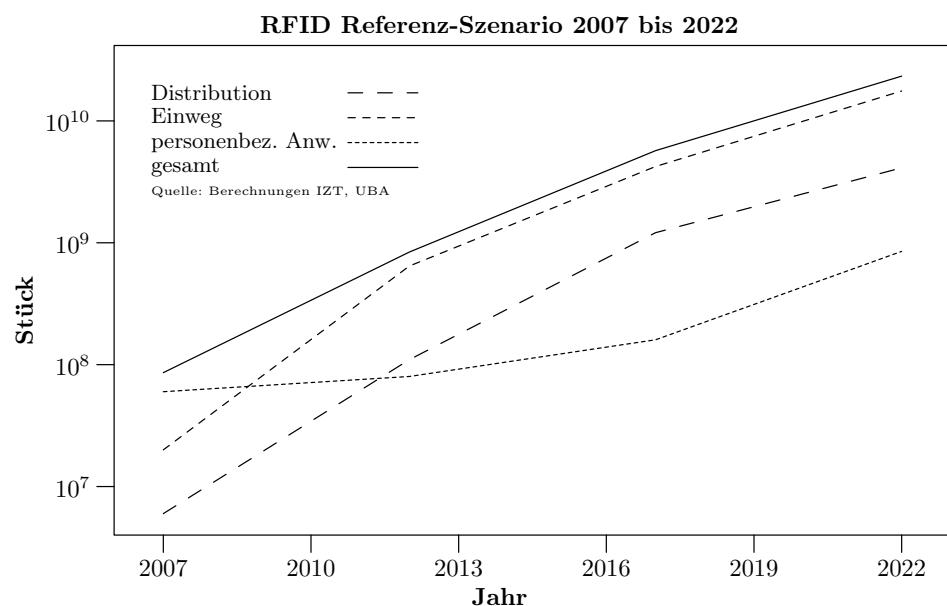


Bild 4.10.: RFID Anwendungsszenarien in Deutschland 2007-2022 [EH09]

4.9. Geschäftsmodelle

In der *Geschäftsmodellen in der digitalen Ökonomie* beschreibt Stähler [Stä02, S. 55] die Klassifizierung von E-Business wie in Bild 4.11.

	A2C	A2B	A2A
	B2C	B2B	B2A
	C2C	C2B	C2A

Nachfrage

Bild 4.11.: Klassifizierung von E-Business nach Geschäftspartnern, Quelle siehe [Stä02, S. 55]. Die Abkürzungen sind wie folgt zu lesen: C: *Customer* (Kunde), B: *Business* (Unternehmen), A: *Administration* (Verwaltung). Bei einem Geschäftsmodell wie B2C (*Business-to-Customer*) richtet sich das Unternehmen an den Endkunden

Dieses Bild gilt es zu erweitern, bietet doch *Auto-ID* neue Opportunitäten der Interaktion, beispielsweise durch mobile Systeme wie *NFC* und maschinenlesbare Ausweise wie den *ePerso* oder *ePass*.

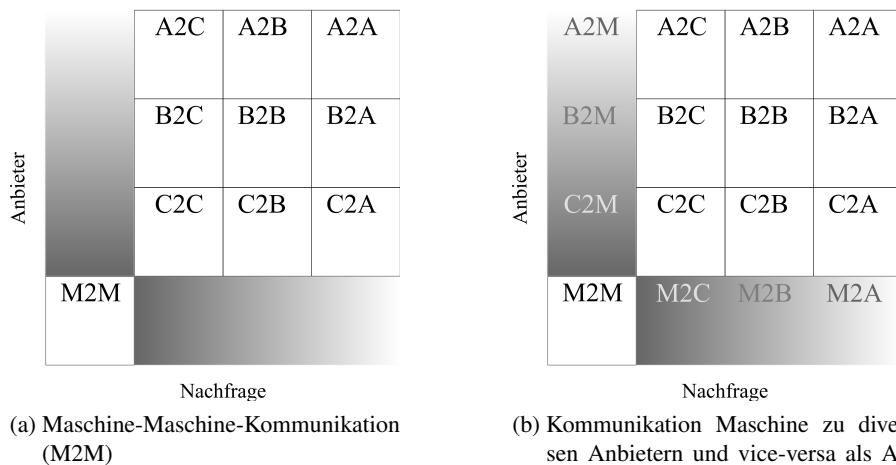


Bild 4.12.: Erweiterung von Bild 4.11 der Klassifizierung von E-Business durch neue Technologien

4.10. Zusammenfassung

Mit einer Auswahl von Anwendungen und genutzten Frequenzbereichen werden in diesem Kapitel RFID-Anwendungen in Logistik und Automatisierung beschrieben. RFID bringt Vorteilen zur Erhöhung der Fälschungssicherheit und des Verbraucherschutzes. Weitere Technologien wie Oberflächenwellentransponder, Containeridentifikation und **NFC** werden angesprochen.



4.11. Übungen

Übung 4.1. Warum wird bei der Identifikation von Tieren der LF-Frequenzbereich genutzt?

Übung 4.2. Warum haben Oberflächentransponder (**OFW**) eine sehr kurze Antwortzeit?

Übung 4.3. Wie kann man den Unterschied zwischen offenen und geschlossenen Systemen beschreiben?

Übung 4.4. Welche Maßnahmen werden beim elektronischen Pass ergriffen, um Fälschung zu verhindern und den Datenschutz zu gewährleisten?

Übung 4.5. Warum ist *RFID*-Technologie für Sensoren als medizinische Implantate so interessant?

5. Systemarchitektur

Dieses Kapitel gibt einen kurzen Überblick über RFID-Systeme, Anwendungen und Realisierung bezüglich Hard- und Software.

5.1. RFID-Hardware

Die an RFID-Systemen beteiligte **Hardware** gliedert sich allgemein in **Schreib-/Lesegeräte**, **Transponder**, **Netzwerk-** und **Rechnerkomponenten**.

5.1.1. Lesegeräte



(a) Handlesegerät

(b) Reader XR480

(c) Antennen

Bild 5.1.: Handlesegerät, Reader und Antenne. Quellen a-c [Psion Teklogix GmbH, Motorola]

Lesegeräte sind meist unscheinbar und häufig in Systeme integriert, wie beispielsweise das Zündschloß im Fahrzeug, Zugangskontrollen für Personen und Fahrzeuge und RFID-Flächen an Automaten.

5.1.2. Hand-Lesegeräte

Handlesegeräte wie Bild 5.1a werden meist **mobil** eingesetzt in der Logistik, wo Ware, Lieferant oder Empfänger sowie Unterschrift registriert und zu einem späteren Zeitpunkt aus dem mobilen Gerät in eine zentrale Datenbank übertragen werden. Hand-Geräte können modular zu **LF-**, **HF-** oder **UHF**-Lesern umgerüstet und mit **Barcode-Scannern** kombiniert werden.

Weiterhin können diese Geräte mit **WLAN** in ein Datennetzwerk eingebunden werden. Für **PDA**s existieren RFID-Erweiterungsmodul; ferner kann man Handys mit **NFC**-Technologie, siehe Kapitel 4.5, dieser Gruppe zurechnen.

5.1.3. Stationäre Systeme

Lesegerät

Stationäre Anlagen bestehen aus **Lesegerät**, Bild 5.1b, und Antenne. Lesegeräte wie im abgebildeten Beispiel können mehrere **Antennen** oder **Antennenpaare** ansteuern. Dabei sind getrennte Antennen für Senden (**TX**) und Empfangen (**RX**) anschließbar, was die Flexibilität und Detektionsrate erhöht. Ferner verfügen diese Lesegeräte über **Schnittstellen** für **Netzwerkanschluss**, und **Konfiguration**.

Antenne

Antennen werden dabei häufig zu **Portalen**, Bild 5.1c angeordnet, um eine Rundumerfassung auch größerer Objekte, beziehungsweise die gleichzeitige Erfassung vieler Objekte zu verbessern.

Portal

5.1.4. Tag-Bauformen

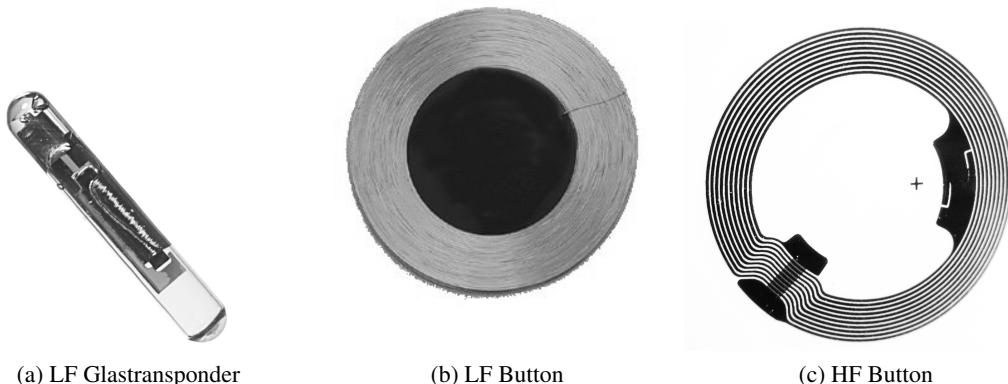


Bild 5.2.: Aufbau von Tags. Quellen a-c [www.virbac.de / www.peterprohn.de, Psion Teklogix GmbH]

Von zentraler Bedeutung bei RFID sind die Transponder. Zum Einen gibt die ihnen zu Grunde liegende Technik die **Reichweite** und Eignung für den Einsatz in unterschiedlichen **Umgebungen**.

gen vor. Zum Anderen bestimmt deren Technologie und Herstellung den **Preis der Tags**, die ja in riesigen Stückzahlen der **Markierung** dienen sollen. Aus dem Frequenzbereich, in dem die Tags arbeiten, ergeben sich erhebliche Unterschiede in der Größe und der Herstellung.

LF- und HF-Transponder arbeiten mit **magnetischer Kopplung**. Für die Antennenspulen sind LF sind bei **124-135 kHz** einige hundert Windungen notwendig. Dabei kann diese, wie bei den **Glastranspondern**, Bild 5.2a, auf einen **Ferritkern** aufgebracht oder als **Luftspule**, Bild 5.2b, realisiert sein. Leitermaterial und Wickeln verursachen entsprechende **Herstellungskosten** im Vergleich zu den höheren Frequenzbereichen.

Im HF-Bereich bei **13.56 MHz** beträgt die notwendige Windungszahl der Antennne nur etwa 5 bis 10. Diese kann direkt als Leiterbahn gedruckt werden wie in Bild 5.2c, was die Herstellungskosten und den Platzbedarf erheblich senkt. Daher sind HF-Tags gute Kandidaten für die Markierung von Produkten und werden beispielsweise im **medizinischen Bereich** eingesetzt.

LF

HF

UHF

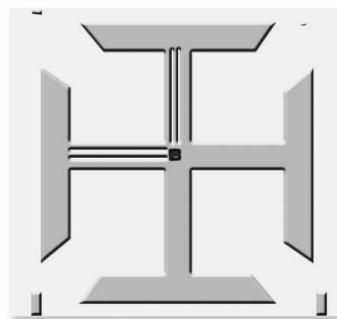
Bauform



(a) Implantat



(b) HF Button



(c) UHF Gen2 (4"×4")

Bild 5.3.: Tag-Bauformen: Quellen a-c [www.virbac.de / www.peterprohn.de, Psion Teklogix GmbH, Motorola]

Im UHF-Bereich bei **868-915 MHz** werden die Antennenstrukturen noch einfacher und reduzieren sich auf **Dipol-Strukturen**, allerdings mit der durch die **Wellenlänge** vorgegebenen Größe, siehe Kapitel 2.6.2. Bild 5.3c zeigt einen Gen2-Tag mit doppeltem Dipol, welcher von der **Polarisation** der einfallenden Welle weitgehend unabhängig ist, allerdings eine Breite von ca. 9.5 cm besitzt. Bei RFID in der Logistik kann ein starker Trend zu UHF beobachtet werden.

Praktische **Bauformen** von RFID-Transpondern sind sehr vielfältig und reichen von Implantaten, Bild 5.3a, über Zündschlüssel für Wegfahrsperrern, Schlüsselanhänger für Zugangskontrollsysteme, **Chipkarten** im üblichen Format von Kreditkarten, in Kunststoff gegossene Formen wie **Knöpfe** (Button), Bild 5.3b, etwa in Münzgrößen, **Stifte**, bis hin zu **Etiketten** im HF- und UHF-Bereich, Bild 5.3c und 5.2c in meist rechteckiger Realisierung.

5.1.5. Netzwerk und Rechner

Die Einbindung von RFID-Komponenten in eine bestehende oder neu zu erstellende Infrastruktur für Verwaltung, Planung, Fertigung und/oder Automatisierung erfolgt über serielle Verbindung mit einzelnen Rechnern, **LAN**-Netze oder Industriebussysteme. Einer geeigneten **Softwarerestruktur** kommt hier eine besondere Bedeutung zu, siehe Abschnitt 5.2.3.

5.2. Architektur

Während ein Barcode-Scanner in der Größenordnung zehn Etiketten pro Sekunde erfassen kann, sind es bei einem RFID-Leser bis zu einigen hundert. Entsprechend leistungsfähig muss ein datenverarbeitendes System ausgelegt sein. Nach einer knappen Darstellung der Hardware betrachten wir im Folgenden die Architektur der Software-Komponenten.

5.2.1. Systemarchitektur mit RFID

Die Struktur einer **Unternehmensanwendung** mit RFID besteht in der Regel aus **verteilten Systemen** und kann folgendermaßen gegliedert werden:

- RFID-Tags
 - kodiert eine eindeutige **ID** und gegebenenfalls zusätzliche Information.
 - eigenständiges Objekt wie Parkchip, Ausweiskarte usw.
 - an Objekten zu deren Identifikation angebracht
- RFID-Leser
 - Lesen/Schreiben von Transponderdaten
 - liefert Rohdaten, die weiter bearbeitet werden müssen
 - benötigt individuelle Konfiguration
- RFID-Middleware
 - Verarbeitung, das heißt Filterung und Aggregation der Rohdaten
 - Transport der Information an die Backend-Systeme
 - Management des RFID-Netzwerks und der Endgeräte.
- Backendsysteme
 - Verarbeitung der Daten für Automatisierung, Logistik oder Prozesssteuerung.
 - Analyse der Daten
 - Persistenz, das heißt Archivierung und Speicherung von Informationen in **Datenbanken**

- Aktionen aufgrund der Informationen
- Interaktion mit anderen Systemen wie **Naming Services (ONS)**, **Produktdatenbanken** wie **EPCIS** oder **Track-and-Trace** (Verfolgung von Objekten in einer Versorgungskette)

5.2.2. Transponder und RFID-Leser

Für RFID-Systeme existieren eine Vielzahl unterschiedlicher Normen, Frequenzbereiche und Anwendungen, siehe Kapitel 3. Ferner gibt es sowohl für Tags, als auch für Leser **unterschiedliche Hersteller** und Ausführungen. Auch mit Blick auf zukünftige Erweiterungen muss von einer sehr **heterogenen Landschaft** ausgegangen werden.

heterogene Landschaft

RFID-Leser müssen auch für die unterschiedlichen Gegebenheiten **konfiguriert** werden, das heißt sie benötigen individuelle **Netzwerk-Adressen** und **-Konfiguration**, Einstellungen der **Frequenzkanäle-** und **Sequenz**, **Sendeleistung**, **Datenrate** und **Codierung** um einige zu nennen [FL05a].

Konfiguration

RFID-Lesegeräte liefern im Betrieb eine **Flut von Daten** und **elementaren Ereignissen**. Erst durch eine geeignete Filterung, Zusammenfassung und Vorverarbeitung in der **Middleware**, siehe Abschnitt 5.2.3, kann die Information in den Unternehmensanwendung sinnvoll genutzt werden.

Datenflut

5.2.3. Software Infrastruktur

Größere Systeme werden meist hierarchisch und modular und die Architektur in mehrerer Schichten¹ konzipiert, um die folgenden grundsätzlichen Forderungen zu erfüllen:

¹engl. *multi-tier* = mehrstufig



Sicherheit und Zuverlässigkeit

Performanz bezüglich Datendurchsatz, Antwortzeiten etc.

Skalierbarkeit Die Leistungsfähigkeit des Systems steht in einem etwa linearen Verhältnis zu den eingesetzten Ressourcen.

Modularität Spezifische Funktionalität ist in (mehr oder minder) unabhängigen Komponenten realisiert. Dadurch wird auch die **Erweiterbarkeit** erleichtert.

Wart- und Testbarkeit

Plattformunabhängigkeit Unter Umständen kann eine gewisse Unabhängigkeit bezüglich der verwendeten **Hardware** und die Möglichkeit des Einsatzes alternativer **Softwarekomponenten und Betriebssysteme** langfristig einen wirtschaftlichen Vorteil darstellen.

Middleware für RFID

Die **RFID-Middleware** stellt die Softwareschicht dar, welche sich zwischen den Lesegeräten und der Unternehmensanwendung befindet. Ihre Aufgabe ist es, siehe auch Abschnitt 5.2.1, RFID-Daten zu empfangen, zu verarbeiten und die gefilterten Daten an die Anwendung weiterzuleiten.



Gelangt ein Transponder in den Bereich eines Lesers, wird ein **Event** – (Ereignis) – erzeugt, welches sich aus **Seriенnummer**, **Daten**, **Zeit** und **Leser-ID** zusammensetzt [AIMb]. Diese Events werden mit der Erfassungsgeschwindigkeit des Lesers so lange gesendet, wie sich der Tag in der Nähe des Lesers befindet. Für die Anwendung ist aber nur von Interesse, wann der Transponder den Lesebereich betreten (entry) und wann er ihn wieder verlassen hat (exit).



Teile einer Anwendung sind meist nur an bestimmten Ereignissen interessiert, möglicherweise zusammen mit weiteren Informationen.

Beispiel 5.1. Beispiel wäre ein Kunde mit Kundennummer – anhand seiner RFID-Kundenkarte – und dem Inhalt seines Einkaufswagens, welcher durch die Tags an den Artikeln erkannt wird.

Filterung
Aggregation

Diese **Vorverarbeitung** durch **Filterung** und **Aggregation (Zusammenfassung)** ist eine der Aufgaben der Middleware. Sie könnte diese Daten beispielsweise an das Kunden-**Abrechnungs-**

system senden, welches sofort den Lieferschein druckt und zu einem späteren Zeitpunkt die Rechnung erstellt.

Physikalisch identische Events von den Leseantennen an einem der Portale der Warenanlieferung sind dagegen für den Teil der Unternehmensanwendung von Bedeutung, welches für den **Warenbestand** und die **Lieferantenbeziehungen** zuständig ist. Üblicherweise sind die Tore für die Warenlieferung meist mit mehreren Antennen/Lesegeräten zur Verbesserung der Erfassung ausgestattet. Damit ist die **räumliche Zuordnung** unterschiedlicher Quellen eine weitere Aufgabe der Middleware.

Die Verarbeitung der RFID-Ereignisse erfolgt in **Echtzeit**, was bedeutet, dass die **Antwort** des Systems **deterministisch** (vorhersagbar) ist und innerhalb eines **vorgegebenen Zeitraums** erfolgt. In der Regel kommunizieren die verteilten Systeme über **Nachrichten**, also **asynchron**, vergl. [Sch05]. Dies wird durch eine oder mehrerer **Event-Queues** realisiert. Eine synchrone Kopplung mit Methodenaufruf und Warten auf die Antwort wäre bei großen und heterogenen Systemen praktisch nicht vorhersagbar.

Die Konfiguration eines wahren Zoos von RFID-Lesegeräten, die Wartung, Aufspielen neuer Firmware und bei Ersatz defekter Geräte von Hand ist nicht nur sehr aufwändig, sondern auch fehleranfällig. Daher ist das **Konfigurationsmanagement** für das RFID-Netzwerk eine weitere wichtige Aufgabe für eine RFID-Middleware.

Wie bei den meisten Technologien existieren bei den verschiedenen Herstellern sehr unterschiedliche Ansätze. Neben den oft proprietäre Ansätzen der klassischen Hersteller etablierter **ERP**-Systeme (Enterprise Resource Planning) existiert ein breites Spektrum weiterer Konzepte [Sch05]. Eine breite Unterstützung unterschiedlichster Hersteller und skalierbaren Ansatz bietet beispielsweise *Sybase* mit *RFIDanywhere[©]* [Syb].

räumliche Zuordnung
Echtzeit
Event-Queue
Konfigurationsmanagement

5.3. Zusammenfassung

Dieses Kapitel beschreibt die unterschiedlichen Arten von Leseeinheiten und Transpondern. Die grundsätzliche Architektur einer Unternehmensanwendung mit RFID wird bezüglich Hard- und Software skizziert. Bei großen Systemen ist eine geeignete Middleware von großer Bedeutung, deren Aufgaben und Eigenschaften beschrieben werden.



5.4. Übungen

Übung 5.1. Beurteilen Sie den Herstellungsaufwand für Transponder der Frequenzbereiche LF, HF und UHF?

Übung 5.2. Welcher RFID-Frequenzbereich wird Ihrer Meinung nach den größten Zuwachs erfahren?

Übung 5.3. Welches RFID-System würden Sie für die Kennzeichnung fester und flüssiger Medikamente empfehlen und warum?

Übung 5.4. Skizzieren Sie die wesentlichen Komponenten einer typischen RFID-Anwendung. Welche Aufgaben haben diese?

Übung 5.5. Man könnte RFID-Leser direkt an existierende Unternehmensanwendungen koppeln. Warum ist der Einsatz einer Middleware sinnvoll?

6. Kontaktlose Chipkarten

In diesem Kapitel sollen Details der Datenhaltung und Zugriffsverfahren unterschiedlicher **RFID**-Karten betrachtet werden. In den Abschnitten [6.1](#) bis ... wenden wir uns den gängigen **HF**-Karten der *ISO 14443* zu.

6.1. MIFARE classic

Die *MIFARE classic* ist eine der ältesten RFID-Karten und implementiert die *ISO 14443 A*. Sie wird in den Größen 1 kB und 4 kB, sowie als *Mini* mit 320 Byte geliefert.

Der Speicher ist in *Blöcken* zu je 16 Byte organisiert. Je vier *Blöcke* (64 Byte) werden zu einem *Sektor* zusammengefasst.

Jeder Sektor lässt sich durch einen *Zugriffsschlüssel* (*key*) schützen. *Zugriffsbits* in jedem Block geben für diesen an, welche Operationen mit welchem der beiden Zugriffsschlüsseln (*keyA* und *keyB*) ausgeführt werden dürfen.

Block 0 in Sektor 0 enthält herstellerspezifische Daten wie die *Seriennummer* (4 Byte) und eine vom Hersteller vergebene eindeutige Kennung (*UID*), siehe [\[LR10\]](#).

6. Kontaktlose Chipkarten

7. Sicherheit und Datenschutz

Dieses abschließende Kapitel behandelt die grundlegenden Aspekte der Sicherheit von RFID-Anwendungen.

Der Begriff **Sicherheit** in der deutschen Sprache umfasst mehrere sehr verschiedene Aspekte, wie die unterschiedlichen englischen Begriffe **safety**¹ und **security**² deutlich aufzeigen. **Datenschutz** und **Schutz der Rechte der Person** sind damit Bestandteil der Sicherheit im erweiterten Sinne.

Sicherheit
Datenschutz

Ein im erweiterten Sinne sicheres RFID-System muss **Schutz** bieten und das Folgende verhindern:

Unberechtigtes Lesen eines Datenträgers, Duplizieren und/oder Verändern der Daten

Fremde Datenträger in den Lesebereich einbringen um unberechtigt Zutritt oder Leistungen zu erhalten.

Abhören der Funkverbindung und Wiedergabe der Daten um eine berechtigte Benutzung vorzutäuschen³.

Unberechtigtes Sammeln von Daten ohne Erlaubnis und Kenntnis des Inhabers des Datenträgers.

Gesundheitliche Schäden durch die Anwendung.

Daraus ergeben sich zwei Ansatzpunkte, **technische Maßnahmen** und **gesetzliche Regelungen** zum Schutz persönlicher Daten.

7.1. Technische Maßnahmen

Zu den technischen Maßnahmen gehört gegenseitige Authentifizierung und die Verschlüsselung der Daten bei der Übertragung, wie in den folgenden Abschnitten näher erläutert wird.

Bei einfachen Anwendungen wie Industrieautomation oder Kennzeichnung eines Werkzeugs sind solche Maßnahmen nicht notwendig und würden nur unnötige Kosten verursachen.

¹safety wird bei [MW04] als Zustand der *Sicherheit vor Verletzung oder Verlust* oder als *Schutz vor unbeabsichtigte oder gefährlichen Betriebszuständen* eines Geräts definiert

²security wird bei [MW04] mit den Begriffen *Freiheit vor Gefahr, Freiheit vor Angst und Furcht, [...] Betrug* sowie *Schutz vor Spionage, Sabotage, Verbrechen, Angriff, ...* belegt

³replay and fraud

7. Sicherheit und Datenschutz

Ferner kann durch die Begrenzung der Reichweite die Gefahr eines Lauschangriffs verringert werden.

7.1.1. Kryptografie - Kryptologie

Kryptografie

Kryptografie⁴ und Kryptologie⁵ können wie folgt definiert werden:

:=

Kryptografie lässt sich als eine öffentliche Wissenschaft und Teildisziplin der Mathematik definieren, in der Vertrauen geschaffen, übertragen und erhalten wird. Kryptografie ist der Entwurf von **Verschlüsselungsverfahren** [BNS10, S. 1, 3].

:=

Viele Autoren bezeichnen **Kryptologie** als Oberbegriff für zwei Teildisziplinen, nämlich die **Kryptografie** und die **Kryptoanalyse**, welche die **Analyse** von Verschlüsselungsverfahren zum Gegenstand hat, vergl [BNS10, S. 3].

7.1.2. Authentifizierung

Bei besonderen Anwendungen wie beispielsweise bargeldlose Zahlsysteme im öffentlichen Nahverkehr (**ÖPNV**) oder Ausweiskarten wie Reisepass muss sichergestellt sein, dass nur berechtigte Anwendungen auf den Datenträger zugreifen können. Umgekehrt benötigt das Lesegerät die Sicherheit, dass der ihr vorgelegte Datenträger nicht gefälscht ist und zu dieser Anwendung gehören.

**symmetrische
Authentifizierung**

Zu den Verfahren gehört die **gegenseite symmetrische Authentifizierung**. Dabei sind beide – Lesegerät und Transponder – im Besitz eines gleichen geheimen Schlüssels. Nach Aufforderung sendet der Transponder eine Zufallszahl R_T an das Lesegerät. Das Lesegerät fügt eine Zufallszahl R_L an und sendet beide verschlüsselt an den Transponder. Dieser entschlüsselt beide Zahlen, vergleicht das Ergebnis mit der von ihm gesendeten Zahl. Der Transponder erzeugt eine zweite Zufallszahl R'_T , verschlüsselt sie zusammen mit R_L und sendet sie an das Lesegerät, welches nach Entschlüsselung die Übereinstimmung mit seiner Zufallszahl überprüft. Nachteil des Verfahrens ist, dass jede Transponderkarte den identischen **geheimen Schlüssel** enthält, was bei massenhaft verteilten Transpondern wie **ÖPNV**-Tickets in einer Großstadt ein gewisses Risiko der Aufdeckung darstellt, vergl. [Fin06].

abgeleiteter Schlüssel

Eine Verbesserung bieten **abgeleitete Schlüssel**. Mit der **ID**-Nummer der einzelnen Karte und einem **Masterschlüssel** wird ein individueller Schlüssel berechnet und auf der Karte gespeichert.

⁴Kryptografie: griech. *kryptós* = verbergen, *gráphein* = schreiben

⁵Kryptologie: griech. *kryptós* = verbergen, *logos* = Lehre

Die Karte verschlüsselt fortan mit diesem Schlüssel, den das Lesegerät aus der **ID**-Nummer des Transponders und dem Masterschlüssel in einem besonderen Sicherheitsmodul des Lesegeräts berechnen kann.

7.1.3. Verschlüsselte Datenübertragung

Nach erfolgreicher gegenseitiger Authentifizierung können die zu übertragenden Daten nach unterschiedlichen Verfahren verschlüsselt werden, auf die hier nicht weiter eingegangen werden kann. Interessierte seien auf die Literatur, beispielsweise [Fin06], verwiesen.

7.1.4. Begrenzung der Reichweite

Ein weitere wichtiger Faktor für die Sicherheit der Daten auf dem Tag ist eine Begrenzung der Reichweite. Diese ist durch physikalische Gegebenheiten, siehe Kapitel 2.9, begrenzt oder bereits in einigen Standards, siehe Kapitel 3.1, vorgegeben.

LF- und HF-Anwendungen haben von Natur aus kürzere Reichweiten. UHF-Anwendungen sind durch Absorption und Reflexion stark beeinflussbar, siehe Kapitel 2.9.1 und 2.9.3 – ein wenig Metallfolie beispielsweise von einer Schokoladenverpackung genügen, den Transponder auch bei kürzester Entfernung unlesbar zu machen.

7.2. EMV und Gesundheit

Die Diskussion um gesundheitliche Gefährdungen durch elektromagnetische Wellen wurde bereits vor mehr als 50 Jahren mit der flächendeckenden Einführung des Rundfunks und neuerdings mit der rasanten Ausbreitung von Mobiltelefonen und Nahbereichsfunk (**WLAN**) aufgeworfen [AIM06].

TODO: !!! neuere Quellen, z.B [MK08] !!!

Die Wechselwirkung elektromagnetischer Strahlung und biologischen Gewebe ist durch zwei Effekte möglich.

7.2.1. Thermische Effekte

In dem für RFID relevanten Frequenzbereich oberhalb 100 kHz werden elektromagnetische Wellen überwiegend absorbiert und führen zu **Erwärmung des Gewebes**. Dieser Effekt wird in Watt/kg Körpergewicht gemessen und als **SAR** angegeben. Eine Wirkung auf den menschlichen Körper sind ab 4 W/kg nachgewiesen worden. Der gesetzlich festgelegte **Grenzwert** liegt für die **Normalbevölkerung** bei **0.08 W/kg**, bei **beruflicher Exposition** bei **0.4 W/kg**, vergl. [AIM06].

Erwärmung

7.2.2. Nicht-thermische Effekte

Bei niedrigeren Frequenzen unterhalb 100 kHz können Wechselfelder **Ströme** im Gewebe induzieren. Dabei kann nicht ausgeschlossen werden, dass diese Effekte auf die **Zellmembranen** haben, vergl. [AIM06].

Diese Frequenzen < 100 kHz kommen bei RFID **nicht** zum Einsatz.

7.2.3. Vorsichtsmaßnahmen bei aktiven medizinischen Implantaten

Sicherheitsabstand Für Träger von **Herzschriftermachern** wird eine **Sicherheitsabstand** von 25 cm zu RFID-Schreib-/Leseeinheiten angeraten.

Bei **Hörgeräten** sind Störungen durch schnurlose Telefone und Mobiltelefonen bei Abständen unter 30 cm beziehungsweise 70 cm bekannt, vergl. [AIM06].

7.2.4. Grenzwerte

Erarbeitung und Überwachung von Grenzwerte für die **Öffentlichkeit** und **Arbeitnehmer** sind auch Gegenstand der **Europäischen Kommission**. Interessanterweise sind derzeit für die **maximale Leistungsflußdichte** W/m^2 für Frequenzen unterhalb 10 GHz **noch keine Grenzwerte** definiert.

Alle Grenzwerte basieren auf der ständigen Beobachtung wissenschaftlicher Erkenntnisse und technischer Entwicklungen. Sie enthalten stets einen **Sicherheitsaufschlag** von mindestens einem Faktor 10, vergl. [AIM06].

7.3. Öffentliche Akzeptanz von RFID

Entscheidend für den Erfolg einer Technologie ist deren Akzeptanz in der Öffentlichkeit und bei den Kunden. Weder Horrorszenarien – von Gegnern spektakulär verbreitet – vom gläsernen Bürger, der mittels in alltäglichen Artikeln verdeckt angebrachten Transpondern mit unrealistisch hohen Lesereichweiten ausspioniert wird, noch Beschwichtigungsversuche und Desinformation seitens Befürworten sind den eigentlichen Zielen dienlich.

Ein erfolgreicher Einsatz der RFID-Technologie bringt in der Zukunft für viele Unternehmen, aber auch für Prozesse im öffentlichen Leben – beispielsweise deutliche Kosteneinsparung und Effizienz im Öffentlichen Personen Nahverkehr – entscheidende Vorteile, teilweise auch im Interesse der Allgemeinheit.

[Thi05] schlägt daher vor, aus den Kernaussagen der Skeptiker die folgenden Ziele auf den entsprechenden Handlungsebenen abzuleiten:

Technologie RFID-Systeme auf technischer Ebene so gestalten, dass Datenmissbrauch unmöglich oder zumindest erheblich erschwert wird.

7.4. Gesetzliche Rahmenbedingungen

Prozesse Erhöhung des Nutzens für den Kunden bei gleichzeitiger Reduktion der Risiken auf ein Minimum durch organisatorische Maßnahmen.

Dialog Den Risikodialog in und mit der Öffentlichkeit, sowie den einzelnen Konsumenten führen um Glaubwürdigkeit zu erhalten und gegebenenfalls wieder zu gewinnen.

Regeln Verbindlichen Festlegung für alle Seiten, welche Anwendungen und Handlungsweisen im Zusammenhang mit der Technologie zulässig sind und welche nicht.

In den Artikeln von [Thi05] und [EIC06] werden diese Aspekte übersichtlich dargestellt.

7.4. Gesetzliche Rahmenbedingungen

Grundlage des Datenschutzes ist das **Bundesdatenschutzgesetz (BDSG)**, [Bun]. Vergleiche für die folgenden Ausführungen [EIC06]. Im Zusammenhang mit RFID findet das Datenschutzrecht Anwendung, wenn

- der RFID-Tag selbst **personenbezogene Daten** speichert
- **nicht personenbezogene Daten** auf dem Tag **natürlichen Personen zugeordnet werden können**

Im Datenschutzrecht in § 3 Abs.1 BDSG werden **personenbezogene Daten** als *Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person* definiert. Es gilt das **Verbotsprinzip**, nach dem *grundsätzlich die Erhebung und Verarbeitung personenbezogener Daten verboten und nur ausnahmsweise gestattet ist, wenn entweder die Einwilligung des Betroffenen oder eine gesetzliche Ermächtigung dazu vorliegt*, siehe § 4 BDSG.

Es gilt ferner der Grundsatz der **Datenvermeidung- und Sparsamkeit**, § 3a BDSG. Es sollen erst **Alternativen** in Betracht gezogen werden, die das gleiche Ziel ohne Erhebung personenbezogener Daten erreichen. Falls solche Daten erforderlich sind, müssen diese **offen** und **transparent** und für den Betroffenen **erkenn-** und **nachvollziehbar** erhoben werden. In der Regel muss der Betroffene **einwilligen**, § 4a BDSG.

Unter den besonderen Voraussetzungen der § 28 - § 31 BDSG ist im **nicht-öffentlichen Bereich** die Datenverarbeitung auch **ohne Einwilligung** des Betroffenen zulässig. Beispielsweise ist in § 28 Abs.1 Nr.1 BDSG die Nutzung personenbezogener Daten im Rahmen der Zweckbestimmung eines **Vertragsverhältnisses** erlaubt. § 28 Abs.1 Nr.2 BDSG wägt die berechtigten Interessen der verantwortlichen Stelle mit den schutzwürdigen Interessen des Betroffenen ab.

[EIC06] sowie [GH06] führen diese Aspekte anhand unterschiedlicher Szenarien aus. Beim Entwurf von Prozessen mit RFID sollte daher immer die **Entfernung** der Tags von der Ware nach Bezahlung oder die Möglichkeit zur **Lösung** oder **Deaktivierung** darauf befindlicher Informationen, auch durch den Kunden selbst, in Erwägung gezogen werden. Kunden sollen stets über Erhebungen **informiert** und auf die Verwendung **hingewiesen** werden.

§§ BDSG

personenbezogene
Daten

Datenvermeidung

Einwilligung

7.5. Zusammenfassung

In diese Kapitel wurden folgende Aspekte behandelt:

- Sicherheit vor Fälschung und unberechtigte Nutzung durch technische Maßnahmen wie Kryptografie und Begrenzung der Reichweite.
- Elektromagnetische Verträglichkeit (**EMV**), Gesundheit und Grenzwerte.
- Akzeptanz von Technologien wie RFID
- Gesetzliche Rahmenbedingungen und Datenschutz, Informations-, Hinweispflicht und Einwilligung.

7.6. Übungen



Übung 7.1. Welche Stellen sind für die Festlegung von Grenzwerten bei elektromagnetischer Strahlung zuständig?

Übung 7.2. Mit welcher möglichen biologischen Wirkung ist bei RFID zu rechnen?

Übung 7.3. Welches ist die gesetzliche Grundlage für die Erhebung, Speicherung- und Verarbeitung personenbezogener Daten?

A. Anhang: Lösungen und Hinweise zu den Aufgaben

A.1. Kapitel 1

Lösung (1.3). Siehe Kapitel 1 und Tabelle 1.1.

Lösung (1.4). Wie nennt man Frequenzbereiche, welche unter bestimmten Voraussetzungen für den allgemeinen Gebrauch zugelassen sind?. Siehe Abschnitt 1.5.

Lösung (1.5). Beispiele im Text und eigene Beobachtungen.

Lösung (1.6). Siehe Abschnitt 1.4.

A.2. Kapitel 2

Lösung (2.3). Die Reichweite hängt davon ab, wie stark Feldern und Wellen bei einem bestimmten Abstand sind.

Lösung (2.4). Zur Kommunikation muss stets eine ausreichend große Spannung im Empfänger induziert werden. Dies hängt auch davon ab, wie die Empfangsspule zu den Feldlinien, beziehungsweise die Antenne zur einfallenden Welle ausgerichtet ist. Betrachten Sie hierzu die Abbildungen und den Text in Kapitel 2, oder in der Literatur beispielsweise [Fin06].

Lösung (2.5). Siehe Abschnitt 2.5.

Lösung (2.6). Siehe Abschnitt 2.9.4.

A.3. Kapitel 3

Lösung (3.1). Siehe Abschnitt 3.5.

Lösung (3.2). Siehe Abschnitt 3.6.

Lösung (3.3). In Abschnitt 3.5 werden zwei Arten von Verfahren beschrieben. Bei der einen senden die Teilnehmer zufällig, bei der anderen wird vom Leser bestimmt, wer senden darf.

A.4. Kapitel 4

Lösung (4.1). Siehe Text in Kapitel 4 und 2.9.2.

Lösung (4.2-4.4). Siehe Text in Kapitel 4.

A.5. Kapitel 5

Lösung (5.1-5.3). Siehe Text in Kapitel 5 und recherchieren Sie gegebenenfalls.

Lösung (5.4-5.5). Siehe Text in Kapitel 5.

A.6. Kapitel 7

Lösung (7.1-7.3). Siehe Text in Kapitel 7

Glossar

A	Ampère SI -Einheit für Strom.
ADC	Analog Digital Converter. Analog-Digital-Wandler.
AIP	Air Interface Protocol.
ALOHA	X.25 Paketnetzwerk auf Hawaii, 1971. Stochastisches Zugriffsprotokoll benannt nach ALOHA, z.B. Grundlage bei Ethernet.
AM	Amplitudenmodulation.
ANSI	American National Standards Institute. Amerikanisches Mitglied der ISO .
API	Application Programming Interface. Programmierschnittstelle.
ARM	Advanced Risc Machine. Mikrocontrollerarchitektur [ARM].
ASCII	American Standard Code for Information Interchange. 7-Bit Zeichencodefestlegung.
ASIC	Application Specific Integrated Circuit. Applikationsspezifischer Chip-Baustein.
ASK	Amplitude Shift Keying. Amplitudenmodulation zur Signalisierung von Daten.
ASN	Advanced Shipping Notification. Lieferavis.
BCD	Binary Coded Decimal. Codierungsweise von Dezimalzahlen, bei der jede Ziffer durch 4 Bit dargestellt wird.
BDSG	Bundesdatenschutzgesetz.
BNetzA	Bundesnetzagentur. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen. Deutsche Bundesbehörde (Regulierungsbehörde).
CD	Compact Disc. Digital und Audio/Video.
CDMA	Code Division Multiple Access. Codemultiplexverfahren.
CSMA	Carrier Sense Multiple Access. Verfahren zur Busarbitrierung.
CRC	Cyclic Redundancy Check. Bitorientierte Checksummen-Fehlerüberprüfung mit Polynomresterzeugung.
CMOS	Complementary Metal Oxide Semiconductor. S.a. MOS
CPU	Central Processing Unit. Prozessor eines Rechner.
DAC	Digital Analog Converter. Digital-Analog-Wandler
DIN	Deutsches Institut für Normung. Deutsche Normen oder DIN-Normen.
DIP	Dual Inline Package. Bauform mit zwei parallel angeordneten Anschlussreihen in 2.54 mm bzw. 1.27 mm Rastermaß.
DNA	DeoxyriboNucleic Acid. Träger des Erbguts, deutsch DNS .
DNS	Desoxy-Ribonuklein-Säure. Deutsche Bezeichnung für DNA , Träger des Erbguts.
DoD	Department of Defence. US-Verteidigungsministerium.
DRAM	Dynamic RAM . Flüchtiger Speicherbaustein.
EAS	Electronic Article Surveillance. Warenkontrolle.
EAN	European Article Numbering. Europäische Artikelnummer auf Barcodes (13 Zeichen), siehe auch UPC .
ETX	End of Text. ASCII -Steuerzeichen 0x03.
ECMA	European Computer Manufacturers Association.

EEPROM	Electrically Erasable Programmable Read-Only Memory. Elektrisch lösbarer programmierbarer Nur-Lese-Speicher.
EIRP	Equivalent/Effective Isotropic(ally) Radiated Power. Gibt als Rechnungsgröße die Leistung an einer isotrop – in alle Raumrichtungen gleichmäßig – strahlenden Antenne an, um ein gegebenes Fernfeld zu erreichen.
EMC	Electromagnetic Compatibility.
EMV	Elektromagnetische Verträglichkeit. Deutsche Bezeichnung für EMC .
EN	European Norm. Europäische Norm.
EPC	Electronic Product Code. Hersteller-, Produkt- und Seriennummer, vergeben von GS1 Global Standards. Siehe [GS1].
EPCIS	Electronic Product Code Information Service. Internetdienst der EPCglobal Network.
ERP	Effective Radiated Power. Rechnungsgröße wie EIRP , jedoch für $\lambda/2$ -Dipol mit 2.15 dB Gewinn, d.h einem Faktor 1.64.
ESD	ElectroStatic Discharge. Elektrostatische Entladung.
ETSI	European Telecommunications Standards Institute. Siehe [ETS].
F	Farad. SI -Einheit der Kapazität, As/V.
FDX	Full Duplex. Vollduplex.
FDMA	Frequency Division Multiple Access. Frequenzmultiplexverfahren.
FET	Field Effect Transistor. Feldeffekt Transistor.
FIFO	First In – First Out.
FM	Frequenzmodulation.
FSK	Frequency Shift Keying. Frequenzmodulation zur Signalisierung von Daten.
2-FSK	2-Frequency Shift Keying. FSK , wobei zur Signalisierung von Daten zwischen zwei Frequenzen geschaltet wird.
FSM	Finite State Machine. Zustandsautomat.
GDSN	Global Data Synchronisation Network.
GS1	Global Registry. Zentrale Netzwerkinstanz in GDSN .
GSM	Global System for Mobile communication. Technisches Committee der ETSI und europäischer Mobilfunkstandard. GSM is the new standard for digital cellular communication in Europe.
GPS	Global Positioning System. System zur Positionsbestimmung eines bewegten Objekts auf der Erde mittels Mikrowellen-Sender/Empfänger durch Empfang der Signale mehrerer geostationärer Satelliten.
h-da	Hochschule Darmstadt h_da .
H	Henry. SI -Einheit der Induktivität, Vs/A.
HDX	Half Duplex. Halbduplex.
HF	High Frequency. Kurzwellen. Frequenzen zwischen 3 MHz und 30 MHz.
Hz	Hertz. SI -Einheit für Frequenz, 1/s.
HITAG	Hitag®. RFID-Standard (125 kHz) der Firma NXP Semiconductors®(vormals Philips®)
IC	Integrated Circuit. Integrierter Schaltkreis.
I2C	Inter-Integrated Circuit. Serielle Schnittstelle für die Kommunikation zwischen verschiedenen Schaltungsteilen, entwickelt von NXP®.
I-Code	I-Code. RFID-Industrie-Standard (13.56 MHz). Kompatibel zu ISO 15693.
ICC	Integrated Circuit Card.
ID	Identifikation oder Identifikationsnummer.
IDE	Integrated Development Environment. Integrierte Entwicklungsumgebung.

IEC	International Electric/ Electrotechnical Commission. Internationale Elektrotechnische Kommission seit 1906, beschäftigt sich mit Ausarbeitung von Empfehlungen.
ISDN	Integrated Services Digital Network. Dienste integrierendes digitales Netz.
ISM	Industry, Scientific, Medical. Frequenzbereiche für Funkanwendungen in Industrie, Forschung und Medizin.
ISO	International Standard Organisation. [ISOa] .
ISP	In System Programmer. Schnittstelle zum Programmieren μControllern.
ITU	International Telecommunications Union.
JTAG	Joint Test Action Group. Schnittstelle zum Programmieren und Debuggen von μControllern.
LAN	Local Area Network. Lokales Netzwerk / Lokaler Rechnerverbund mit allgem. beschränkter Rechneranzahl und Netzausbreitung <20km.
LBT	Listen Before Talk.
LED	Light Emitting Diode. Leuchtdiode.
LF	Low Frequency. Langwellen. Frequenzen zwischen 30 kHz und 300 kHz.
LLCP	Logical Link Control Protocol. Spezifikation im Zusammenhang mit NFC .
LRC	Longitudinal Redundancy Check. Längssummenprüfung.
MIFARE	Mifare®. RFID-Industrie-Standard (13.56 MHz) der Firma NXP Semiconductors®. Kompatibel zu ISO 14443 A.
MOS	Metal Oxide Semiconductor.
MOSFET	Metal Oxide Semiconductor Field Effect Transistor. S.a. MOS u. FET
MRTD	Machine Readable Travel Document. Maschinenlesbares Reisedokument.
NCI	NFC Controller Interface.
NDA	Non-Disclosure Agreement. Vertrag, welcher das Stillschweigen über Verhandlungen, Verhandlungsergebnisse oder vertraulichen Unterlagen festschreibt [Wik] .
NDEF	NFC Data Exchange Format.
NFC	Near Field Communication. RF-Übertragungsverfahren mit 13.56 MHz auf max. 20 cm.
NFCIP	NFC Interface and Protocol. NFCIP-1: internationaler Standard ISO 18092 seit 2003, NFCIP-2: internationaler Standard ISO 21481 seit 2005.
NRZ	Non Return to Zero. Nicht selbsttaktende Darstellung eines Bits durch Rechteckimpulse.
ÖPNV	Öffentlicher Personen Nahverkehr.
OCR	Optical Character Recognition. Erkennung von geschriebenem Text.
OEM	Original Equipment Manufacturer. Hersteller fertiger Komponenten oder Produkte, der diese in seinen eigenen Fabriken produziert, sie aber nicht selbst in den Handel bringt [Wik] .
OFW	Oberflächenwellen. Deutsche Bezeichnung für SAW .
ONS	Object Naming Service. im Zusammenhang mit EPC .
OSI	Open System Interconnect(ion)/Intercommunication.
PC	Personal Computer.
PDA	Personal Digital Assistant. Sammelbezeichnung für Pocketcomputer, Organizer etc.
PCD	Proximity Coupling Device. Siehe z.B. ISO/IEC 14443-2.
PICC	Proximity Coupling Card. Siehe z.B. ISO/IEC 14443-2.
PM	Phasenmodulation.
PMR	Private Mobile Radio.
PSK	Phase Shift Keying. Phasenmodulation zur Signalisierung von Daten.
2-PSK	2-Phase Shift Keying. PSK , wobei zur Signalisierung von Daten zwischen 0° und 180° geschaltet wird.
QR	Quick Response. QR-Code als Markenbegriff der japanische Firma Denso Wave für einen

	zweidimensionalen Code [? , wiki-de]
RADAR	Radio Detection And Ranging. Funk-Erkennung und -Abstandsmessung.
RAM	Random Access Memory. Schreib-Lese-Speicher.
RegTP	Regulierungsbehörde für Post und Telekommunikation.
RFID	Radio Frequency Identification. Funkfrequenzkennzeichnung oder -identifikation.
ROM	Read Only Memory. Nur-Lese-Speicher.
RMS	Root Mean Square. Quadratischer Mittelwert.
RTD	Record Type Definition. Definiert die Struktur von NDEF -Nachrichten. Record kann weitere Records enthalten.
RTF	Reader Talks First.
RS232	Recommended Standard 232-D. Technische Festlegungen der EIA fuer eine V.24-Schnittstelle von 1986.
RX	Receive. Empfangen.
SAR	Specific Absorbtion Rate. Z.B. als Grenzwert bei der Strahlung von Funktelefonen.
SAW	Surface Acoustic Wave. Siehe OFW .
SIM	Subscriber Identification Module. Beispielsweise zur Identifikation des Nutzers im Mobilfunknetz.
SDMA	Space Division Multiple Access. Multiplex durch räumliche Trennung.
SGTIN	Serialised Global Trade Item Number.
SHF	Super High Frequency. Mikrowellen. Frequenzen zwischen 3 GHz und 30 GHz.
SI	Système International d'Unités. Internationaler Standard über (metrische) Einheiten im Messwesen, seit 02.07.1969 in Kraft.
SNEP	Simple NDEF Exchange Protocol.
RFC	Request For Comment. Informationen über Netzwerke und Protokolle als elektronische Dateien, siehe [RFC]
SBC	Single Board Computer. Einplatinencomputer, siehe [hyp] .
SMD	Surface Mounted Device. Platzsparende Fertigungstechnik durch miniaturisierte Bauelemente.
SRAM	Static RAM . Statischer Speicherbaustein.
SRD	Short Range device. Kurzstreckenfunkgerät, Telemetriesender.
STX	Start of Text. ASCII -Steuerzeichen 0x02.
TDMA	Time Division Multiple Access. Zeitmultiplex.
TDM	Time Division Multiplexing. Zeitmultiplexing.
TTF	Tag Talks First.
TTL	Transistor Transistor Logic. Bipolare Technologie bei IC 's.
TX	Transmit. Senden.
UCC	Universal Code Council.
UID	Unique Identifier. Globaler Identifier, siehe [hyp] , bei RFID auch für Antikollision verwendet.
UPC	Universal Product Code. Barcode Standard in USA und Kanada (12 Zeichen), vergleichbar mit EPC .
UART	Universal Asynchronous Receiver Transceiver. Chip für serielle Schnittstelle.
UHF	Ultra High Frequency. Ultrakurzwellen. Frequenzen zwischen 0.3 GHz und 3 GHz.
URL	Universal/Uniform Resource Location. definiert in RFC1738 .
USB	Universal Serial Bus. Serielles Bussystem zur Verbindung eines Computers mit Geräten.
V	Volt. SI -Einheit für Spannung.

-
- WLAN** Wireless [LAN](#).
- WORM** Write Once Read Many (Times). Einmal beschreiben, mehrmals lesen.
- ZFH** Zentralstelle für Fernstudien an Fachhochschulen. [[ZFH](#)].

Literatur

- [AIMa] AIM, Ident Jahrbuch 2007. <http://www.aim-d.de/Publikationen/>
- [AIMb] AIM, Management-Leitfaden RFID 2006. <http://www.aim-d.de/Publikationen/>
- [AIM06] RFID und Gesundheitsschutz – Gemeinsame Erklärung von GS1 Germany und AIM-Deutschland. <http://www.aim-d.de/Publikationen/>. Version: 2006
- [ARM] ARM - The Architecture for the Digital World. <http://www.arm.com/>
- [Aus] Bundesamt für Sicherheit in der Informationstechnik (BSI) - Der neue Personalausweis. <https://www.ausweisapp.bund.de/pweb/index.do>
- [BLSR] BOLIC, Miodrag ; LATTEUX, Michel ; SIMPLOT-RYL, David: *Framed Aloha Based Anti-collision Protocol for RFID tags*
- [BMI] BMI - Bundesministerium des Innern. <http://www.bmi.bund.de/>
- [BNS10] BEUTELSPACHER, Albrecht ; NEUMANN, Heike B. ; SCHWARZPAUL, Thomas: *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk.* 2. Aufl. Wiesbaden : Vieweg, 2010. – ISBN 9783834809773
- [BSI] Bundesamt für Sicherheit in der Informationstechnik. <http://www.bsi.bund.de>
- [Bun] Bundesdatenschutzgesetz. http://www.gesetze-im-internet.de/bdsg_1990/
- [Col04] COLEMAN, Christopher: *An Introduction to Radio Frequency Engineering.* Cambridge University Press, 2004. – ISBN 0521834813
- [DB96] DAVID, Klaus ; BENKNER, Thorsten: *Digitale Mobilfunksysteme.* Stuttgart : Teubner, 1996 (Informationstechnik). – ISBN 3-519-06181-3
- [Deu] Deutsche Bank Research. <http://www.dbresearch.de>
- [ebe] Isolde-Kurz-Gymnasium, Hertzscher Dipol. <http://www.ikg.rt.bw.schule.de/fh/eldy/hertz.html>

- [EH09] ERDMANN, Lorenz ; HILTY, Dr. L.: Einfluss von RFID-Tags auf die Abfallentsorgung - Prognose möglicher Auswirkungen eines massenhaften Einsatzes von RFID-Tags im Konsumgüterbereich auf die Umwelt und die Abfallentsorgung / Umweltbundesamt. 2009 (27 - UBAFBNr 001276). – Publikationen. – <http://www.umweltdaten.de/publikationen/fpdf-k/k3845.pdf>
- [EIC06] NIEDERMEIER, Robert (Hrsg.) EICAR e.V.: *Leitfaden: RFID und Datenschutz*. <http://www.eicar.org/rfid/infomaterial/RFID-Leitfaden-100406.pdf>. Version: 2006
- [ePa] *BMI - Bundesministerium des Innern - Pässe und Ausweise*. <http://www.epass.de/>
- [ETS] *The European Telecommunications Standards Institute*. <http://www.etsi.org/>
- [Fin06] FINKENZELLER, Klaus: *RFID-Handbuch*. Hanser Fachbuchverlag, 2006. – ISBN 3446403981
- [FL05a] FLOERKEMEIER, Christian ; LAMPE, Matthias: RFID middleware design - addressing application requirements and RFID constraints. In: *Proceedings of sOc-EUSAI 2005 (Smart Objects Conference)*. Grenoble, Oktober 2005, S. 6
- [Flö05b] FLÖRKEMEIER, Christian: EPC-Technologie – vom Auto-ID Center zu EPCglobal. In: FLEISCH, Elgar (Hrsg.) ; MATTERN, Friedemann (Hrsg.): *Das Internet der Dinge: Ubiquitous Computing und Rfid in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen* (Xpert.press). Springer, Berlin, 2005. – ISBN 3540240039, Kapitel B 3, S. 87–100
- [FM05] FLEISCH, Elgar ; MATTERN, Friedemann: *Das Internet der Dinge: Ubiquitous Computing und Rfid in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen* (Xpert.press). Springer, Berlin, 2005. – ISBN 3540240039
- [Fra06] FRAPORT AG: *Gepäckmanagement*. BITKOM Konferenz Raunheim, May 2006
- [GB06] GLOVER, Bill ; BHATT, Himanshu: *RFID Essentials*. Beijing : O'Reilly, 2006. – ISBN 9780596009441
- [GH06] GILLERT, Frank ; HANSEN, Wolf-Rüdiger: *RFID für die Optimierung von Geschäftsprozessen. Prozess-Strukturen, IT-Architekturen, RFID-Infrastruktur*. Hanser Fachbuchverlag, 2006. – ISBN 3446405070
- [GS1] GS1 - Germany. <http://www.gs1-germany.de/>
- [Her] Dipolantenne - Wikipedia de. <http://de.wikipedia.org/wiki/Dipolantenne/>

- [Hof06] Hof, Christian van't: RFID and Identity Management in Everyday Life / European Parliament. 2006 (IPOL/A/STOA/2006-22). – Forschungsbericht
- [hyp] Hypertext Glossar informatikbezogener Abkürzungen und ausgewählter Begriffe. www.surveyor.in-berlin.de/perls/cshg-suchen.cgi/
- [ICA] ICAO - Machine Readable Travel Documents. <http://mrtd.icao.int/>
- [ISOa] ISO - International Organization for Standardization - Homepage. <http://www.iso.ch>
- [ISOb] ISO - International Organization for Standardization. <http://www.iso.org/>
- [ITW] IT-Lexikon: Fachwissen für IT-Professionals - ITWissen.info. <http://www.itwissen.info/>
- [Kad95] KADERALI, Firoz: *Digitale Kommunikationstechnik*. Bd. 2: Übertragungstechnik, Vermittlungstechnik, Datenkommunikation, ISDN. Braunschweig [u.a.] : Vieweg, 1995. – ISBN 3-528-06485-4
- [Ker06] KERN, Christian: *Anwendung von RFID-Systemen (VDI-Buch)*. Springer, Berlin, 2006. – ISBN 3540444777
- [Kiz06] KIZILKAYA, Mesut: *Machbarkeitsstudie zur Umsetzbarkeit der Integration von Radio Frequency Identification (RFID)-Technologien im Gepäckmanagement von Airlines*. Darmstadt, Hochschule Darmstadt, Fachbereich Informatik, Diplomarbeit, Aug 2006. – unveröffentlicht
- [Kop05] KOPKA, Helmut: *LATEX, Bd. 1: Einführung*. Pearson Studium, 2005. – ISBN 3827370388
- [Kot07] KOTYNEK, Martin: Das Telefon-Ticket. In: *Süddeutsche Zeitung* (2007), Nr. 204, S. 18. – ISSN 0174–4917
- [KSW06] KORIES, Ralf ; SCHMIDT-WALTER, Heinz: *Taschenbuch der Elektrotechnik. Grundlagen und Elektronik*. Deutsch (Harri), 2006. – ISBN 3817117930
- [LFH05a] LAMPE, Matthias ; FLÖRKEMEIER, Christian ; HALLER, Stephan: *Einführung in die RFID-Technologie*. <http://www.vs.inf.ethz.ch/res/papers/mlampe-rfid-2005.pdf>. Version: 2005
- [LFH05b] LAMPE, Matthias ; FLÖRKEMEIER, Christian ; HALLER, Stephan: Einführung in die RFID-Technologie. In: FLEISCH, Elgar (Hrsg.) ; MATTERN, Friedemann (Hrsg.): *Das Internet der Dinge: Ubiquitous Computing und Rfid in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen (Xpert.press)*. Springer, Berlin, 2005. – ISBN 3540240039, Kapitel B 1, S. 69–85

- [lib] *libnfc.org - Public platform independent Near Field Communication (NFC) library.* <http://www.libnfc.org/documentation/introduction>. – zuletzt besucht am 28.11.2012
- [Lou10] LOUVAIN, Université catholique d.: *RFID Security & Privacy Lounge - reference of technical works related to security and privacy in RFID systems [...]*. <http://www.avoine.net/rfid/>. Version: 2010. – zuletzt besucht am 21.11.2010
- [LR10] LANGER, Josef ; ROLAND, Michael: *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin : Springer, 2010. – ISBN 9783642054969
- [Mai09] MAIN, Jonathan: NFC Technology Overview. In: *Spotlight for Developers Presentations at Oulu Member Meeting NFC Forum*, 2009. – http://members.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf
- [MG92] MEINKE, Hans H. ; GUNDLACH, Friedrich-Wilhelm: *Taschenbuch der Hochfrequenztechnik: Grundlagen, Komponenten, Systeme*. Springer, Berlin, 1992. – ISBN 3540547177
- [MG07] MEINKE, Hans H. ; GUNDLACH, Friedrich-Wilhelm: *Taschenbuch der Hochfrequenztechnik: 1. Band - Grundlagen*. Springer, Berlin, 2007. – ISBN 3540547142
- [MGB⁺05] MITTELBACH, Frank ; GOOSSENS, Michel ; BRAAMS, Johannes ; CARLISLE, David ; ROWLEY, Chris: *Der LaTeX-Begleiter*. Pearson Studium, 2005. – ISBN 382737166X
- [MK08] MÜLLER, Karl-Peter ; KURZ, Thomas: *EMF-Monitoring in Bayern 2006/2007 - Messungen von elektromagnetischen Feldern (EMF) in Wohngebieten*. Bürgermeister-Ulrich-Straße 160, 86179 Augsburg : Bayerisches Landesamt für Umwelt, 2008 (Broschüre). http://www.bestellen.bayern.de/application/stmug_app000018. ISSN 978-3-936385-32-8
- [Mül09] MÜLLER, Uwe: *NXP® Near Field Communication - Product Overview and Support Tools - Online Seminar*. http://www.nxp.com/technical_support/NFC_index.html. Version: Mar 2009. – NXP Semiconductors
- [MW04] MERRIAM-WEBSTER: *The Merriam-Webster Dictionary*. Merriam-Webster, 2004. – ISBN 087779930X
- [NFCa] *NFC Forum*. <http://www.nfc-forum.org/>
- [NFCb] *NFC Forum Presentations*. <http://members.nfc-forum.org/resources/presentations/>
- [Nyg12] NYGARD, Mathias: Orientierung im NFC-Labyrinth. In: *Design & Elektronik* (2012), Okt., Nr. 10, S. 30–31. – WEKA FACHMEDIEN GmbH, 85540 Haar

- [RFC] *RFC Editor Page*. <http://www.rfc-editor.org/>
- [RFI] *RFID Journal - Tim Kröner*. <http://www.rfid-journal.de/>
- [RFI06] *RFID/EPC und Sensorik - Einführung, Einsatzgebiete und Standardisierung*.
http://www.gs1-germany.de/content/e39/e466/e468/datei/epc_rfid/sensorik.pdf. Version: 2006
- [Rob04] ROBERTI, Mark: *RFID Journal - New ETSI RFID Rules Move Forward*. <http://www.rfidjournal.com/article/articleview/1229/1/1/>. Version: Nov 2004
- [Sch05] SCHOCH, Thomas: Middleware in Ubiquitous-Computing-Anwendungen. In: FLEISCH, Elgar (Hrsg.) ; MATTERN, Friedemann (Hrsg.): *Das Internet der Dinge: Ubiquitous Computing und Rfid in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen* (Xpert.press). Springer, Berlin, 2005. – ISBN 3540240039, Kapitel B 4, S. 121–140
- [Seg81] SEGELSTEIN, D.: *The Complex Refractive Index of Water*. Kansas City, University of Missouri, Diplomarbeit, 1981
- [SS05] SCHOBLICK, Robert ; SCHOBLICK, Gabriele: *RFID Radio Frequency Identification*. Franzis, 2005. – ISBN 3772359205
- [Stä02] STRÄHLER, Patrick: *Geschäftsmodelle in der digitalen Ökonomie: Merkmale, Strategien und Auswirkungen*. 2. Aufl. Lohmar : Eul, 2002. – ISBN 3899360133
- [ST05] SCHLAGER, Petra ; THIBUD, Manfred: *Wissenschaftlich mit LaTeX arbeiten*. Pearson Studium, 2005. – ISBN 3827370787
- [Swe06] SWEENEY, Patrick J.: *RFID für Dummies (Für Dummies)*. Wiley-VCH, 2006. – ISBN 3527702636
- [Syb] *RFID Software Applications - Radio Frequency Identification Systems & Solutions Supplier - Sybase Inc*. <http://www.sybase.com/products/rfidsoftware>
- [Thi05] THIESSE, Frédéric: Die Wahrnehmung von RFID als Risiko für die informationelle Selbstbestimmung. In: FLEISCH, Elgar (Hrsg.) ; MATTERN, Friedemann (Hrsg.): *Das Internet der Dinge: Ubiquitous Computing und Rfid in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen* (Xpert.press). Springer, Berlin, 2005. – ISBN 3540240039, Kapitel D 4, S. 363–378
- [TSG02] TIETZE, Ulrich ; SCHENK, Christoph ; GAMM, Eberhard: *Halbleiter - Schaltungstechnik. Neuer Teil: Nachrichtentechnische Schaltungen*. Springer, Berlin, 2002. – ISBN 3540428496

Literatur

- [TSI] *T-Systems Pressemitteilung* 09. Mar 2007: „RMV2Go“ - Das Handy wird zum Ticket und Fahrplan. <http://www.t-systems.de/tsi/de/142274/Startseite/PresseAnalysten/PresseCenter/PresseNewsArchiv/PressemeldungDetailseite/2007-03-09-PM-RMV2Go>
- [Ung88] UNGER, Hans G.: *Hochfrequenztechnik in Funk und Radar*. Teubner, Stuttgart, 1988.
– ISBN 3519100185
- [Wik] Wikipedia - deutsch. <http://de.wikipedia.org/>
- [ZFH] *Zentralstelle für Fernstudien an Fachhochschulen*. <http://www.zfh.de/>. – Konrad-Zuse-Straße 1, 56075 Koblenz
- [Zim00] ZIMMER, Gernot: *Hochfrequenztechnik. Lineare Modelle*. Springer, Berlin, 2000. – ISBN 3540667164

Literaturempfehlungen

Für das Grundstudium und die weiterführende Lektüre und Vertiefung einzelner Themen seien – in alphabetischer Reihenfolge – empfohlen:

- RFID, allgemeine Übersicht und Einführung
 - FINKENZELLER, Klaus: *RFID-Handbuch*. Hanser Fachbuchverlag, 2006. – ISBN 3446403981 ([Fin06])
 - GLOVER, Bill ; BHATT, Himanshu: *RFID Essentials*. Beijing : O'Reilly, 2006. – ISBN 9780596009441 ([GB06])
 - SCHOBLICK, Robert ; SCHOBLICK, Gabriele: *RFID Radio Frequency Identification*. Franzis, 2005. – ISBN 3772359205 ([SS05])
- RFID Anwendungen
 - FLEISCH, Elgar ; MATTERN, Friedemann: *Das Internet der Dinge: Ubiquitous Computing und Rfid in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen (Xpert.press)*. Springer, Berlin, 2005. – ISBN 3540240039 ([FM05])
 - GILLERT, Frank ; HANSEN, Wolf-Rüdiger: *RFID für die Optimierung von Geschäftsprozessen. Prozess-Strukturen, IT-Architekturen, RFID-Infrastruktur*. Hanser Fachbuchverlag, 2006. – ISBN 3446405070 ([GH06])
 - KERN, Christian: *Anwendung von RFID-Systemen (VDI-Buch)*. Springer, Berlin, 2006. – ISBN 3540444777 ([Ker06])
 - SWEENEY, Patrick J.: *RFID für Dummies (Fur Dummies)*. Wiley-VCH, 2006. – ISBN 3527702636 ([Swe06])
- RFID Sicherheit und Kryptografie
 - BEUTELSPACHER, Albrecht ; NEUMANN, Heike B. ; SCHWARZPAUL, Thomas: *Kryptografie in Theorie und Praxis: Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk*. 2. Aufl. Wiesbaden : Vieweg, 2010. – ISBN 9783834809773 ([BNS10])
 - ([Lou10])
- Near Field Communication

- NFC Forum Presentations. <http://members.nfc-forum.org/resources/presentations> ([NFCb])
 - LANGER, Josef ; ROLAND, Michael: *Anwendungen und Technik von Near Field Communication (NFC)*. Berlin : Springer, 2010. – ISBN 9783642054969 ([LR10])
 - MAIN, Jonathan: NFC Technology Overview. In: *Spotlight for Developers Presentations at Oulu Member Meeting NFC Forum*, 2009. – http://members.nfc-forum.org/events/oulu_spotlight/Technical_Architecture.pdf ([Mai09])
 - MÜLLER, Uwe: *NXP® Near Field Communication - Product Overview and Support Tools - Online Seminar*. http://www.nxp.com/technical_support/NFC/index.html. Version: Mar 2009. – NXP Semiconductors ([Mül09])
 - NYGARD, Mathias: Orientierung im NFC-Labyrinth. In: *Design & Elektronik* (2012), Okt., Nr. 10, S. 30–31. – WEKA FACHMEDIEN GmbH, 85540 Haar ([Nyg12])
 - libnfc.org - Public platform independent Near Field Communication (NFC) library. <http://www.libnfc.org/documentation/introduction>. – zuletzt besucht am 28.11.2012 ([lib])
- Elektronik und Elektrotechnik
 - KORIES, Ralf ; SCHMIDT-WALTER, Heinz: *Taschenbuch der Elektrotechnik. Grundlagen und Elektronik*. Deutsch (Harri), 2006. – ISBN 3817117930 ([KSW06])
 - TIETZE, Ulrich ; SCHENK, Christoph ; GAMM, Eberhard: *Halbleiter - Schaltungstechnik. Neuer Teil: Nachrichtentechnische Schaltungen*. Springer, Berlin, 2002. – ISBN 3540428496 ([TSG02])
 - Hochfrequenztechnik
 - COLEMAN, Christopher: *An Introduction to Radio Frequency Engineering*. Cambridge University Press, 2004. – ISBN 0521834813 ([Col04])
 - MEINKE, Hans H. ; GUNDLACH, Friedrich-Wilhelm: *Taschenbuch der Hochfrequenztechnik: 1. Band - Grundlagen*. Springer, Berlin, 2007. – ISBN 3540547142 ([MG07])
 - Digitale Ökonomie, e-Commerce
 - STÄHLER, Patrick: *Geschäftsmodelle in der digitalen Ökonomie: Merkmale, Strategien und Auswirkungen*. 2. Aufl. Lohmar : Eul, 2002. – ISBN 3899360133 ([Stä02])

Stichwortverzeichnis

Ω <i>siehe</i> Widerstand	
λ <i>siehe</i> Wellenlänge	
$\lambda/2$ -Dipol <i>siehe</i> Antenne	
ω <i>siehe</i> Kreisfrequenz	
A <i>siehe</i> Strom	
Abkürzungen 101	
Absorption 28, 34, 35, 38	
Absorptionskoeffizient 35	
Absorptionslänge 35	
Aggregation 88	
Aktenverwaltung 69	
ALOHA 55, 56, 58, 60	
dynamisches slotted 62	
slotted 55, 60	
dynamisches 55	
AM <i>siehe</i> Modulation	
Ampère <i>siehe</i> Strom	
Android 74	
Angriff	
Lausch- 94	
Antenne 25, 84	
Dipol- 29	
Ferrit- 29, 85	
Gewinn 30	
Mikrostrip- 29	
Patch- 29	
Schlitz- 29	
Antennenspule 20	
Antikollisionsverfahren 56	
lesergesteuert 60, 62	
transpondergesteuert 60	
Apple 73	
Artikelnummer 43	
Artikelüberwachung <i>siehe</i> EAS	
asynchron 55, 60, 89	
Ausweis	
elektronischer 10, 68	
Authentifizierung 66	
symmetrische 94	
Auto-ID 1	
Backscatter-Systeme 36, 38	
Bada 74	
Barcode 3, 70	
eindimensional 3	
zweidimensional 3	
BDSG 97	
Befehle <i>siehe</i> Transponder, <i>siehe</i> Transponder	
Betriebssystem 74	
Mobiltelefon 74	
Bezahlsysteme 68	
Bibliotheksverwaltung 69	
Binärbaum 56	
binäre Suche 56	
BlackBerry OS 74	
Block 91	
Bogenmaß 16	
Bolus 67, 80	
Broadcast 54	
C <i>siehe</i> Kapazität	
c <i>siehe</i> Lichtgeschwindigkeit	
Chipkarte	
kontaktbehaftet 4	

kontaktlos	5, 91
close coupling	46
Codierung	
Manchester-.....	46, 50, 54
Miller-.....	46, 50
modifizierte.....	50
NRZ-.....	46, 50, 54
Containeridentifikation	70
CRC	50, 54
Dämpfung	23
Daten	
-vermeidung	97
personenbezogene	97
Datenintegrität	49
Datenrate	33
maximale	33
Datenschutz.....	33, 37, 93, 97
Datenübertragung	19, 36, 38
verschlüsselt	95
dB	siehe Dezibel
Demodulator	32
deterministisch	89
Dezibel	24
Diebstahlsicherung	3, 10, 19, 66
Dipolantenne	29, 85
Downlink.....	46, 49
Durchsatz	59, 61
dynamisches S-ALOHA	62
EAN	43, 47
EAS	siehe Diebstahlsicherung
eBusiness	80
Echoquerschnitt	36
Echtzeit.....	89
ECMA	
340	78
352	78
356	78
Einwilligung	97
EIRP	30
EMV	95
Energie	13
Energierreichweite	siehe Reichweite
Energieversorgung	7, 18, 38, 79
ePass	43, 68, 69, 81
EPC	44, 47
EPCglobal Network	47
EPCIS	47, 87
ePerso	68, 69, 81
Ereignis	siehe Event
Ereignisrate	57
ERP	30
ETSI	
302-208	39, 53
Event	88
f	siehe Frequenz
Fälschungssicherheit	67–69
FDX	siehe Vollduplex, 67
Fehler	
Erkennung	49
Korrektur	49
Feld	12
elektrisches	12
elektromagnetisches	5
Fern-	34
magnetisches	5
Nah-	34
Wirbel-	18
Feldstärke	12
Fernfeld	34
Ferritkern	siehe Antenne
Filterung	88
Fingerabdruck	69
FM	siehe Modulation
Frequenz	27, 85
Arbeits-	33
Kreis-	16
Resonanz-	18
RFID-	28, 39
subharmonische	49

Träger-	33	10536	46
Frequenzbänder	39	11784	44, 67
Frequenzbereiche	9, 39	11785	44, 67
Gen2	46, 85	14223	44, 67
Generatorpolynom	50	14443	44, 69
Gepäckmanagement	70	Typ-A	44, 72
Geschäftsmodell	80	Typ-B	46, 72
Gesetz		15693	44
Bundesdatenschutz	97	15963	44
Lambert-Beer	35	18000	44
Maxwell	siehe Maxwell	-2	44
Gesundheit	95	18092	44, 78
Gewinn	siehe Antenne	21481	44, 78
Glaukom	79	24753	44, 48
Glossar	101–105	69873	70
Grenzwerte	96	isotrop	29
Güte	23	J	siehe Energie
Gütfaktor	23	Joule	siehe Energie
Halbduplex	44, 48, 49	Kapazität	14
HDX	siehe Halbduplex, 67	Kapazität	
Heimtiere	67	parasitäre	20
Herstellungskosten	85	Kodierung	33
Hertz	siehe Frequenz	Kollision	34, 53–56, 58
HF	85	Anti-	51, 54, 56
Hilfsträger	46, 49	Kollisionserkennung	50, 54, 58
HTC	73	Kollisionsvermeidung	58
Huawei Devices	73	Konfiguration	87
Hz	siehe Frequenz	Kopplung	
I	siehe Strom	elektromagnetische	37
ICC	4	induktive	18, 20, 70
IEC	siehe ISO	magnetische	18, 20
Impedanz	13	Kreisfrequenz	siehe Frequenz
Implantat	67, 80	Kryptografie	5, 33, 66, 94
Induktivität	15	Kryptologie	94
iOS	74	Kühlkette	70
ISM	9, 39	L	siehe Induktivität
ISO		Längssummenprüfung	49
3166	67	Lösungen	99
10373	44	Ländercode	67

Lastmodulation	7, 19, 49, 66	Last-	19, 46, 66
LBT	53	Phasen-	32, 46
Leistung	12	PSK-	46
Leistungsmaß	25	Motorola	73
Lenovo	73	Multiplex	
Lernziele	i	Code-	51
Lesegerät	34, 83	Frequenz-	51
Hand-	83, 84	Raum-	51
stationäres	84	Zeit-	51
Leser	34, 84	Nahfeld	34
lesergetrieben	55	NFC	71, 72, 74
LF	85	-Anwendungsarten	75
LG Electronics	73	Antenne	72
Lichtgeschwindigkeit	27	Architektur	78
Literatur	107–113	IP1	44, 78
Empfehlungen	113	IP2	44, 78
Logistik	1	Kommunikation	75
LRC	49	Logo	72
Luftschnittstelle	7, 20	Modus	
Manchestercode	50	card emulation	75, 76
Maxwell		card reader	75, 76
Durchflutungsgesetz	18	peer-to-peer	75, 76
Induktionsgesetz	18	NFC Forum	72
Medienbruch	1	NFC-Forum	78
Medizin	79	Nokia	72, 73
Micromax	73	Norm	43, 44, 46
Microsoft	73, 74	Normen	44
Phone	74	NRZ	50
Middleware	87	NXP	72
MIFare	72	NXP Semiconductor	siehe NXP, 72
Mikrostriptantenne	siehe Antenne	Oberflächenwellen	79
Millercode	50	Oberflächenwelle-Transponder	48
Mobilfunk	39	OCR	4
Mobiltelefon	72–74	OFW	79
Modulation	32, 36, 38	Ohm	siehe Widerstand
AM	32	Ohrmarke	67
Amplituden-	32	ONS	47, 87
ASK-	46	ÖPNV	3, 68, 77
FM	32	P	siehe Leistung
Frequenz-	32		

P2P	<i>siehe</i> NFC
Parität	54
gerade	49
ungerade	49
Passbild	69
Patchantenne	<i>siehe</i> Antenne
PDA	73
Periodendauer	28
Personalausweis	43
Phasenverschiebung	16
Poisson	57
-Statistik	57
-Verteilung	57
Polarisation	85
lineare	30
zirkulare	31
Portal	84
Potenzial	12
Potenzialdifferenz	12
Produkt	
-haftung	71
-sicherheit	70
Produktcode	47, 87
proximity coupling	44
Prozessor	5
Prüfbits	49
Pufferung	8
Pulsbetrieb	49
Quellen	107–112
R	<i>siehe</i> Widerstand
Radarquerschnitt	36
Reflexion	34, 35, 38
optischer Bereich	36
Resonanzbereich	36
Reichweite	34, 37, 85, 95
Energie-	34, 38
maximale	37
Reifendrucksensor	79
Reihenschwingkreis	<i>siehe</i>
Serienschwingkreis	
Reisepass	68, 69
Research In Motion	74
Resonanz	18
-breite	23
-frequenz	16, 17
-katastrophe	23
-kurve	22
RFID	5
Anwendungsszenario	80
Pass	69
Personalausweis	69
Symbol	69
Tag	<i>siehe</i> Tag
Transponder	<i>siehe</i> Transponder
Wachstum	1, 80
RIM	73, <i>siehe</i> Research In Motion, 74
Rückstrahlquerschnitt	36
Rückstreuquerschnitt	
moduliert	49
modulierter	38
Rückstreuung	36
modulierte	7, 37
S-ALOHA	55, 60
Samsung	73
SAR	95
Schlitzantenne	<i>siehe</i> Antenne
Schlüssel	
abgeleiteter	94
geheimer	94
Master-	94
Schwingkreis	
geöffneter	25
Serien-	20
Seitenband	33
Sektor	91
Sendeleistung	
äquivalente	30
Sensoren	48, 70, 80

sequenzielle Systeme	48, 49	Tracking	69
Seriennummer	48, 69, 91	Transponder	7, 61, 85
Serienschwingkreis	20	-Bauform	85
Sicherheit	33, 37, 93	-eigene Kennung	48
Sicherheitsabstand	96	1-Bit-	19
Smartcard	4	aktiv	7, 8, 53, 70
Smartphone	73, 74	Befehle	56, 61
Sony	72	Chipkarten-	85
Spannung	11	Glas-	80, 85
Spannungüberhöhung	22	Kommando	56, 61
Speicherkarte	5	passiv	7, 8
Spezifikation	44	semi-aktiv	8
Standard	43, 44	semi-passiv	8
Statistik	56	Seriennummer	48, 56, 61
Strahler		transpondergetrieben	55
isotroper	29	 U	<i>siehe</i> Spannung
Kugel-	29, 30	UCC	47
Strichcode	3	UHF	85
Strom	11	UPC	43
Stromversorgung . <i>siehe</i> Energieversorgung		Uplink	46, 49
Symbian	74	 V	<i>siehe</i> Spannung
synchron	52, 55, 60, 62	Verbraucherschutz	43, 66, 70
System		Verschlüsselung	<i>siehe</i> Kryptografie
gepulst	49	Verstärkungsmaß	25
geschlossen	43, 66, 67	vicinity coupling	44
offen	43, 67	Vielfachzugriff	55
 Tag	7, 85	Vollduplex	44, 48
aktiv	<i>siehe</i> Transponder	Volt	<i>siehe</i> Spannung
passiv	<i>siehe</i> Transponder	 W	<i>siehe</i> Leistung
Tastung	32	Wachstum	
Amplituden-	32	von RFID	1, 80
Frequenzum-	32	Waren Sicherung .. <i>siehe</i> Diebstahlsicherung	
Phasenum-	32	Warenwirtschaft	1
TCL Communication	73	Watt	<i>siehe</i> Leistung
Telemetrie	8, 9	Wegfahrsperrre	66
-sender	7	Wellenlänge ..	26, 28, 29, 34–36, 38, 39, 85
Telemetriesender	53	Werkzeugidentifikation	70
Texterkennung	4	Widerstand	13
Tieridentifikation	44, 66	komplexer	21
time slot	60, 62		

Wechselstrom-	21
Wirbelfeld	<i>siehe</i> Feld
wireless.....	72
Ws	<i>siehe</i> Energie
Xiaomi	73
ZTE	73
Zugangskontrolle.....	10, 67
Zugriffsschlüssel	91
Zugriffsverfahren	55
zyklischer Redundanzcheck.....	50

