

# RFID (Radio Frequency Identification)

Christian Böhm, Sebastian Sippl, Martin Tamme

VP Wissenschaftliche Arbeitstechniken und Präsentation  
Universität Salzburg

26. Januar 2006

# Inhalt

- 1 Einleitung
- 2 RFID Systeme
- 3 Übertragungsgarten
- 4 Anwendungen
- 5 Datenschutz

# Motivation

- Generelles Unwissen über die Existenz von RFID.
- Weitreichende Einsatzgebiete (hohes Zukunftspotential).
- Die damit verbundenen Gefahren (Datenschutz).

# Was ist RFID?

- Radio Frequency Identification.
- Oberbegriff für eine technische Infrastruktur.
- Ist über Funk auslesbar.

# Geschichte

- RFID ähnliche Systeme existieren bereits seit dem 2. Weltkrieg.
- 60er Jahre: EAS-Systeme (Electronic Article Surveillance).
- 70er Jahre: Anwendung bei der Tierkennzeichnung.
- 80er Jahre: Gefördert durch USA und Norwegen für Mautsysteme. Weitere Suche nach Einsatzgebieten.

# Geschichte

- 90er Jahre: In den USA setzen sich Mautsysteme durch. Zusätzliches Einsatzgebiet: Smart Card (Skipässe, Tankkarten, ...).
- 2000: Durch Massenproduktion starker Preisverfall (bis dato keine Standardisierung).
- 2003: Einige Standards vom Auto-ID Center entwickelt (EPC (Electronic Product Code), ...).

# Aufbau eines RFID Systems

Ein RFID System besteht aus:

- Transponder (RFID-Etikett, -Chip, -Lable, -Tag, ...).
- Sende/Empfangs Einheit (Reader).
- Server, Dienste, Integration mit Kassensystemen, Warenwirtschaftssystemen, Datenbanken, ...

# Tag-Klassen

In Abhängigkeit der Funktionalität wurden RFID-Tags in Klassen unterteilt.

Klasse	Speicher	Energieversorgung	Merkmale
0	kein	passiv	Artikelüberwachung
1	lese	beliebig	Identifikation
2	schreib-lese	beliebig	Datenerfassung
3	schreib-lese	semi-passiv oder aktiv	Umweltsensoren
4	schreib-lese	aktiv	Ad Hoc Netzwerk

# Übertragungsarten

Die zur Anwendung kommende Übertragungsart hängt davon ab, ob das RFID System im Nahfeld oder im Fernfeld operiert.

Dabei unterscheidet man zwischen:

- Induktive Kopplung: funktioniert im Nahfeld.
- Backscatter Verfahren: funktioniert im Fernfeld.

# Induktive Kopplung

- Arbeitet mit niedrigen Frequenzen.
- Lesegerät und Tag besitzen eine Antennenspule.
- Lesegerät erzeugt ein elektromagnetisches Feld mit einer bestimmten Resonanzfrequenz  $f_g$  (zum Datentransfer).
- Tag reagiert auf diese Frequenz(en).
- Durch das erzeugte Feld wird in der Spule vom Tag Induktionsstrom erzeugt (gleichgerichtet).
- Dadurch wird der Chip des Transponders mit Strom versorgt (Kondensator wird aufgeladen).

# Induktive Kopplung

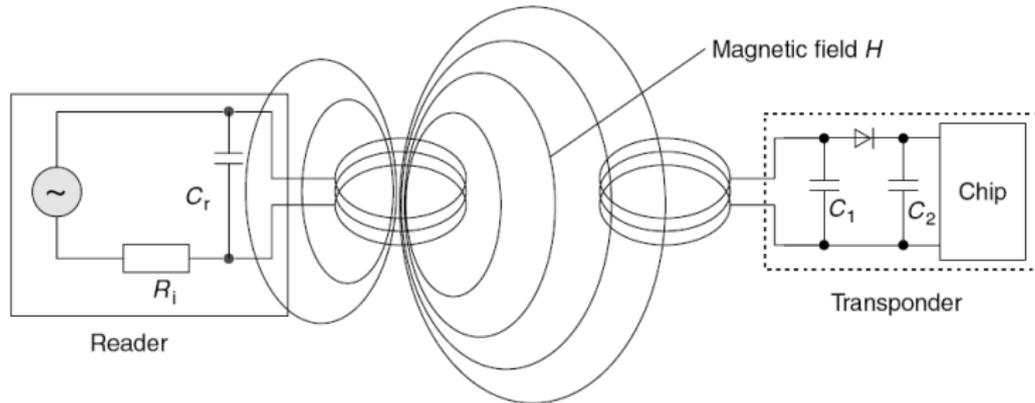


Abbildung: Induktive Kopplung

# Datentransfer duch Lastmodulation

- Funktioniert im Nahfeld:  $\frac{1}{2\pi} \lambda$
- Durch einen Lastwiderstand in der Antenne kann der Transponder die verbrauchte Energie regulieren.
- Der Energieabfall kann vom Reader exakt gemessen werden (hat Auswirkung auf die Amplitudenmodulation der Stromstärke in der Antenne des Readers).
- Wird das Ein/Ausschalten durch die Daten reguliert, können diese so am Reader wiedergewonnen werden (Demodulation).

# Lastmodulation in Seitenbändern

- Vermeidung der Überlagerung des Readersignals durch das Transpondersignal.
- Der Transponder sendet das Signal in einem Seitenband (radiotechnisch gesehen).
- Durch einen Bandpassfilter kann das Signal an der Antenne des Readers nun leicht demoduliert werden.
- Signalerzeugung im Seitenband benötigt einen zusätzlichen Lastwiderstand (teurer).

# Sequentieller Datentransfer

- Spezielle Art des Datentransfers.
- Reader sendet Signal, um den Kondensator am Tag zu laden.
- Feld des Readers wird abgeschaltet.
- Ende durch „End of Burst Detector“ festgestellt.
- Dadurch kann der Transponder mit der gespeicherten Energie ein Feld erzeugen und so antworten.
- Keine Überlagerung, daher größere Reichweite.

# Backscatter Verfahren

- Arbeitet mit hoher Frequenz.
- Durch größere Distanzen wird nicht genügend Strom im Transponder erzeugt.
- Daher benötigt der Mikrochip eine eigene Stromversorgung.
- Die elektromagnetischen Wellen werden vom Reader erzeugt und am Transponder reflektiert (Radar).
- Auch hier gibt es Resonanzwellenlängen.
- So kann der Tag erkennen, ob ein Reader in der Nähe ist und sich in den Power Up/Down Modus schalten.

# Modulated Reflection Cross Section

- Maßeinheit für Reflektionsstärke: RCS (Reflection Cross Section)
- Die RCS wird am Transponder durch einen Lastwiderstand reguliert.
- Dies wird wiederum von Daten gesteuert.
- Durch einen Directional Coupler wird das Signal am Reader gefiltert.
- Durch die Radargleichung kann die Signalstärke berechnet werden.

# Reichweiten

Passive Tags				
Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
6,75 MHz	-	44 Meter	1 Meter	Induktive Kopplung
13,56 MHz	Früher Supply-Chain-Management (Trend geht zu UHF)	3,5 Meter	1 Meter	Induktive Kopplung
UHF (865-928 MHz)	Supply-Chain-Management	unbegrenzt	7 Meter	Backscatter

Aktive Tags				
Frequenz	Hauptanwendung	Theoretische Reichweite	Berichtete/normale Reichweite	Übertragungsart
UHF (865-928 MHz)	Mautsystem (z.B. Österreich)	unbegrenzt	15-30 Meter	Backscatter

# 1-Bit Transponder

## 1-Bit Transponder als Diebstahlsicherung.

- Primitivster Tag.
- Datenspeicher von einem Bit (vorhanden/nicht vorhanden).
- Reader befindet sich am Ausgang des Geschäfts.
- Tag befindet sich auf den Waren.
- Beim Kauf der Ware wird der Tag durch ein starkes Magnetfeld zerstört.

# 1-Bit Transponder

## Problem

Da der Tag direkt auf der Ware angebracht ist, kann es bei gewissen Materialien (Metall, ...) vorkommen, daß der Tag nicht erfaßt werden kann.

## Lösung

Das Problem kann umgangen werden, indem bei der Abtastung des Readers nicht eine einzige Frequenz verwendet wird, sondern über einen Frequenzbereich gescannt wird.

# 1-Bit Transponder

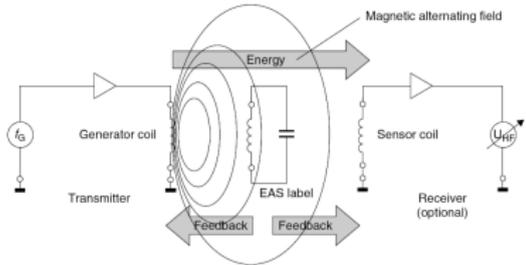


Abbildung: Funktionsweise

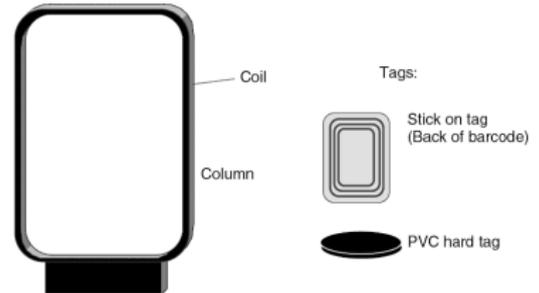


Abbildung: Komponenten

# Transponder mit ROM/RAM

Werden vorwiegend zur Kennzeichnung eingesetzt und besitzen einen kleinen ROM (16Byte – 8KB) bzw. RAM Speicher (256Byte – 64KB).

Einsatzgebiete:

- Produktkennzeichnung mittels EPC (Electronic Product Code).
- Tierkennzeichnung
- Logistische Erfassung

# Barcode vs. EPC

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



Abbildung: 96Bit EPC

Abbildung: Barcode

# Transponder mit Mikrochip

Die wesentlichen Bestandteile eines Transponders mit Mikrochip sind:

- Prozessor
- ROM (Betriebssystem)
- RAM (Arbeitsspeicher)
- EEPROM (Electrically Erasable Programmable Read Only Memory) beinhaltet anwendungsspezifische Daten.

# Transponder mit Mikrochip

- Größter Anwendungsbereich: Smart Cards.
- Als Übergangslösung existieren heute Hybridkarten.
- Anwendungen der Smart Cards: bargeldloses Zahlen, Bustickets, elektronische Ausweise, ...
- Smart Cards wurden nach ISO 7810 genormt.
- Weitere Anwendungen sind: Zugangssysteme, Autoschlüssel, österreichisches Mautsystem, ...

# Transponder mit Mikrochip

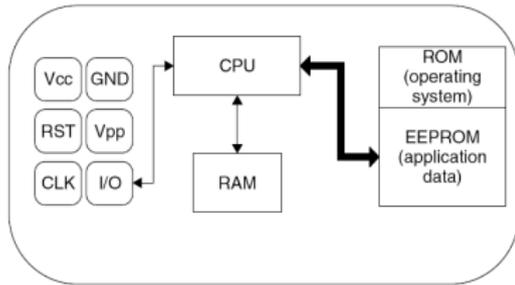


Abbildung: Aufbau



Abbildung: Smart Card

# Zukünftige Einsatzmöglichkeiten

- PSA (Personal Shopping Assistent)
- Intelligente Kühlschränke und Medikamentenschränke, welche gezielt auf ihren Inhalt reagieren.
- Geldscheine mit RFID-Tags.

# Einflüsse auf die Privatsphäre

- Unautorisiertes Auslesen von Eigentum.
- Durchführung von Verhaltensanalysen.
- Data-Mining (systematisches Extrahieren von zuvor unbekanntem Informationen aus großen Datenmengen).

# Vermeidung von Sicherheitsproblemen

- Zerstörung des RFID-Tags.
- Schutz durch Authentifizierung, Verschlüsselung.
- Kenntnis und Kontrolle des Besitzers über die gespeicherten (persönlichen) Informationen.
- Löschung aller objektbezogenen Daten nach einer gewisser Zeitspanne.

# Literatur

-  Klaus Finkenzeller (2003).  
*RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.*  
München: Giesecke & Devrient GmbH.
-  Holger Ziekow (2005).  
*RFID Technologie und Implikation.*  
Berlin: Berliner Forschungszentrum für Internetökonomie.

**Vielen Dank für die Aufmerksamkeit.**