Radio Frequency Identification

Der englische Begriff **Radio Frequency Identification** [ˈɹeɪdɪəʊ ˈfɹiːkwənsi aɪˌdɛntɪfɪˈkeɪʃn̩] (**RFID**) bedeutet im Deutschen *Identifizierung mit Hilfe von elektromagnetischen Wellen*. RFID ermöglicht die automatische Identifizierung und Lokalisierung von Gegenständen und Lebewesen und erleichtert damit erheblich die Erfassung und Speicherung von Daten.

Ein **RFID-System** besteht aus einem Transponder, der sich am oder im Gegenstand bzw. Lebewesen befindet und diese kennzeichnet sowie einem *Lesegerät* zum Auslesen der Transponder-Kennung.
Das Lesegerät enthält eine *Software* (ein Mikroprogramm), das den eigentlichen Leseprozess steuert und eine *RFID-Middleware* mit Schnittstellen zu weiteren EDV-Systemen und Datenbanken.

In der Regel erzeugt das Lesegerät ein elektromagnetisches Hochfrequenzfeld geringer Reichweite, vorzugsweise mit Induktionsspulen. Damit werden nicht nur Daten übertragen, sondern auch der Transponder mit Energie versorgt. Nur wenn größere Reichweiten erzielt werden sollen und die Kosten der Transponder nicht sehr kritisch sind, werden aktive Transponder mit eigener Stromversorgung eingesetzt. Meist wird die Frequenz 13,56 MHz benutzt, auf die auch Warnsysteme vor RFID-Einsatz ansprechen.

RFID-Transponder können so klein wie ein Reiskorn sein und implantiert werden, etwa bei Haustieren. Vorteile dieser Technik ergeben sich aus der Kombination von Kleinheit der Transponder, unauffälligen Auslesemöglichkeiten (z. B. neuer Pass) und geringem Preis der Transponder (teilweise im Cent-Bereich). Diese neue Technik verdrängt zunehmend den heute noch weit verbreiteten Barcode.

Verliehene Bücher mit RFID-Chips werden durch ein Lesegerät verbucht

Universelles RFID Handlesegeräte für 125 kHz/134 kHz und/oder 13,56 MHz; optional Barcode

Entwicklungsgeschichte

Die ersten RFID-Anwendungen wurden Ende des Zweiten Weltkrieges eingesetzt. Dort diente ein Sekundärradar zur Freund-Feind-Erkennung. In den Flugzeugen und Panzern waren Transponder und Leseeinheiten angebracht, um zu erkennen, ob die zu beschießende Stellung oder die anfliegenden Flugzeuge anzugreifen waren oder nicht. Bis heute werden Nachfolgesysteme in den Armeen eingesetzt. Harry Stockman gilt als die Person, der die Grundlagen von RFID mit seiner Veröffentlichung „Communication by Means of Reflected Power“ im Oktober 1948 gelegt hat.[1]

Ende der 1960er Jahre wurde als eine von vielen proprietären Lösungen die „Siemens Car Identification“, kurz SICARID, entwickelt. Damit war es möglich, zunächst Eisenbahnwagen und später Autoteile in der Lackiererei eindeutig zu identifizieren. Eingesetzt wurde es bis in die 1980er Jahre. Die Identifikationsträger waren Hohlraumresonatoren, die durch das Eindrehen von Schrauben einen Datenraum von 12 bit abdecken konnten. Abgefragt wurden sie durch eine lineare Frequenzrampe. Diese Hohlraumresonatoren können als erste rein passive und elektromagnetisch abfragbare Transponder betrachtet werden. Der erste passive Backscatter-Transponder der heute noch verwendeten Bauart mit eigener digitaler Logikschaltung wurde erst 1975 in einem IEEE-Aufsatz

vorgestellt.

In den 1970er wurden die ersten primitiven kommerziellen Vorläufer der RFID-Technik auf den Markt gebracht. Es handelte sich dabei um elektronische Warensicherungssysteme (engl. *Electronic Article Surveillance*, EAS) mit 1 Bit Speicherkapazität. Durch Prüfung der Markierung (vorhanden/fehlt) kann bei Diebstahl ein Alarm ausgelöst werden. Die Systeme basierten auf Hochfrequenztechnik bzw. niedrig- oder mittelfrequenter Induktionsübertragung.

Das Jahr 1979 brachte zahlreiche neue Entwicklungen und Einsatzmöglichkeiten für die RFID-Technik. Ein Schwerpunkt lag dabei auf Anwendungen für die Landwirtschaft, wie beispielsweise Tierkennzeichnung, z. B. für Brieftauben, Nutzvieh und andere Haustiere.

Gefördert wurde die Anwendung der RFID-Technik seit den 1980ern besonders durch die Entscheidung mehrerer amerikanischer Bundesstaaten sowie Norwegens, RFID-Transponder im Straßenverkehr für Mautsysteme einzusetzen. In den 1990er kam RFID-Technik in den USA verbreitet für Mautsysteme zum Einsatz.

Es folgten neue Systeme für elektronische Schlösser, Zutrittskontrollen, bargeldloses Zahlen, Skipässe, Tankkarten, elektronische Wegfahrsperren etc. [2] [3]

1999 wurde mit Gründung des Auto-ID-Centers am MIT die Entwicklung eines globalen Standards zur Warenidentifikation eingeläutet. Mit Abschluss der Arbeiten zum Electronic Product Code (EPC) wurde das Auto-ID Center[4]] 2003 geschlossen. Gleichzeitig wurden die Ergebnisse an die von Uniform Code Council (UCC) und EAN International (heute GS1 US und GS1) neu gegründete EPCglobal Inc. übergeben.

2006 ist es Forschern des Fraunhofer-Institut für Fertigungstechnik und Angewandte Materialforschung (IFAM) in Bremen erstmals gelungen, temperaturempfindliche RFID-Transponder in metallische Bauteile aus Leichtmetall einzugießen. Durch diese Verfahrensentwicklung ist es möglich, die herkömmlichen Methoden zur Produktkennzeichnung von Gussbauteilen durch die RFID-Technologie zu ersetzen und die RFID-Transponder direkt während der Bauteilherstellung im Druckgussverfahren in dem Bauteil zu integrieren.

Technik

Die RFID-Transponder unterscheiden sich zunächst je nach Übertragungsfrequenz, Hersteller und Verwendungszweck voneinander. Der Aufbau eines RFID-Transponders sieht prinzipiell eine Antenne, einen analogen Schaltkreis zum Empfangen und Senden (Transceiver), sowie einen digitalen Schaltkreis und einen permanenten Speicher vor. Der digitale Schaltkreis besitzt bei komplexeren Modellen eine Von-Neumann-Architektur.

RFID-Transponder verfügen mindestens über einen einmal beschreibbaren und oft lesbaren Speicher, der ihre unveränderliche Identität enthält. RFID-Transponder können über einen mehrfach beschreibbaren Speicher verfügen, in den während der Lebensdauer Informationen abgelegt werden können.

Nach Anwendungsgebiet unterscheiden sich auch die sonstigen Kennzahlen, wie z. B. Taktfrequenz, Übertragungsrate, Lebensdauer, Kosten pro Einheit, Speicherplatz, Lesereichweite und Funktionsumfang.

Prinzipiell funktioniert die RFID-Kommunikation folgendermaßen: Das Lesegerät (Reader) erzeugt ein hochfrequentes elektromagnetisches Wechselfeld, welches die Antenne des RFID-Transponders (RFID-Tag) beleuchtet. In der Antennenspule entsteht, sobald sie in das elektromagnetische Feld kommt, ein Induktionsstrom. Dieser Strom wird gleichgerichtet und damit ein Kondensator als Kurzzeitspeicher aufgeladen, welcher für den Lesevorgang die Stromversorgung des Chips besorgt. Diese Versorgung übernimmt bei aktiven Tags eine eingebaute Batterie. Bei halb-aktiven Tags übernimmt die Batterie lediglich die Versorgung des Mikrochips.

Der so aktivierte Mikrochip im RFID-Tag decodiert die vom Lesegerät gesendeten Befehle. Die Antwort codiert und moduliert dieser „Reader“ in das eingestrahlte elektromagnetische Feld durch Feldschwächung im kontaktfreien Kurzschluss oder gegenphasige Reflexion des vom Lesegerät ausgesendeten Feldes. Damit *sendet* das Tag seine eigene unveränderliche Seriennummer, weitere Nummern des gekennzeichneten Objekts oder andere vom Lesegerät abgefragte Daten. So sendet das Tag selbst kein Feld aus, sondern verändert nur das elektromagnetische Sendefeld

des Readers.

In der Betriebsfrequenz unterscheiden sich die HF-Tags mit Langwelle bei 128 kHz, mit Kurzwelle 13,56 MHz, mit UHF-Tags bei 865–869 MHz (Europäische Frequenzen) bis 950 MHz (US-Amerikanische und Asiatische Frequenzbänder) oder mit SHF-Tags bei 2,45 GHz oder 5,8 GHz: Regional (Asien, Europa, Amerika) unterscheiden sich die freigegebenen Frequenzen für LF-und UHF-Tags.

HF-Tags verwenden Lastmodulation, das heißt, sie verbrauchen durch Kurzschließen einen Teil der Energie des magnetischen Wechselfeldes. Dies kann das Lesegerät, theoretisch aber auch ein weiter entfernter Empfänger, detektieren. Die Antennen eines HF-Tags bilden eine Induktionsspule mit mehreren Windungen.

UHF-Tags hingegen arbeiten im elektromagnetischen Fernfeld zum Übermitteln der Antwort, das Verfahren nennt man Rückstreuung (engl. backscattering). Hier wird die elektromagnetische Welle entweder absorbiert (gegenphasiger Kurzschluss) oder mit möglichst großem gegenphasigen Rückstrahlquerschnitt reflektiert (Spiegel). Bei den UHF- oder SHF-Antennen handelt es sich meist um lineare, gefaltete oder spiralige Dipole, der Chip sitzt in der Mitte zwischen den linearen oder mehrfach gewinkelten Dipolarmen des RFID-Tags. Es gibt auch UHF-Tags ohne solche Antennen, deren Reichweite ist extrem kurz.

Damit ein Tag sowohl horizontal als auch vertikal gelesen werden kann, verwendet man häufig zirkulare Polarisation. Diese reduziert zwar das Signal-Rausch-Verhältnis, dafür ist jedoch beim Bekleben der Ware in zwei Achsen irrelevant, in welcher Orientierung das Tag aufgeklebt wurde. Da Wasser die UHF-Energie sehr stark absorbiert und Metall diese elektromagnetischen Wellen sehr stark reflektiert, beeinflussen diese Materialien die Ausbreitung der Antennenfelder. Weiterhin ‚verstimmen' dielektrische Untergrundmaterialien die Resonanzfrequenz der Antennen, daher ist es notwendig, UHF-Tags möglichst genau auf die Materialien der gekennzeichneten Objekte abzustimmen.

Die UHF- oder SHF-Technik sind erheblich komplexer ausgelegt als die LF- oder HF-Technik. Aufgrund ihrer Schnelligkeit können UHF- und SHF-Tags bei einer Passage erheblich längere Datensätze übertragen.

Da die Energieversorgung des Mikrochips bei passiven Tags durch die *Beleuchtung* gedeckt werden muss (ein handelsüblicher UHF-Tag mit NXP-Chip nach ISO/IEC 18000–6C benötigt für den Chip etwa 0,35 Mikroampere an Strom), muss der Reader während des Lesevorganges ein hinreichend starkes Feld erzeugen. Diese Betriebsweise der Trägerwelle nennt man in der Hochfrequenztechnik Dauerstrich (engl. continuous wave = Dauerwelle). Aufgrund der Tatsache, dass die Feldstärke quadratisch mit der Entfernung abnimmt und diese Entfernung in beide Richtungen – vom Lesegerät zum Tag und retour – zurückgelegt werden muss, wird diese *Dauerwelle* hinreichend leistungsstark gesendet. Üblicherweise verwendet man hier zwischen 0,5 und 2 Watt EIRP Sendeleistung. Semi-aktive Tags kommen für gleiche Reichweite mit einem Hundertstel dieser Sendeleistung aus.

Zum Auslesen der Tags stehen im UHF-Bereich zehn freie Kanäle zur Verfügung, zusätzlich oberhalb ein Kanal und unterhalb drei Kanäle, welche lediglich mit geringerer Leistung betrieben werden dürfen. Alle Kanäle erstrecken sich über eine Breite von 200 kHz. Die Funk-Antwort des UHF-Tags erfolgt durch Modulieren des Antwortsignals mit 200 kHz auf die Grundwelle. Dadurch entsteht ein Seitenband 200 kHz oberhalb und unterhalb dieser Mittenfrequenz, es belegt also außer dem Sendekanal auch einen Nachbarkanal.

Um in einer Nachbarschaft möglichst viele RFID-Lesegeräte gleichzeitig verwenden zu können, versucht man, möglichst die gesamte Anzahl der Kanäle auszunutzen. Eine häufig genutzte Variante ist es, den Readern in einer Umgebung die Kanäle 1, 4, 7 und 10 zuzuteilen. Für die Seitenbänder werden dann Kanal 0, 2, 3, 5, 6, 8, 9 und 11 belegt. Zusätzlich werden Anti-Kollisionsverfahren eingesetzt, damit die Tags nicht gleichzeitig senden (listen before talk etc.).

Für komplexere Anwendungen können auch Kryptographiemodule oder externe Sensoren wie z. B. GPS in den RFID-Transponder integriert sein. Die RFID-Sende-Empfangseinheiten unterscheiden sich in Reichweite, Funktionsumfang der Kontrollfunktionen und im Aussehen. So ist es möglich, sie direkt in Regale oder Personenschleusen (z. B. bei der Zugangssicherung und in Toreinfahrten) zu integrieren.

Die Vielzahl von unterschiedlichen Geräten und Etiketten ist im Rahmen der verschiedenen Normen (ISO/IEC-Standards ISO 18000-x) vollständig kompatibel. Es werden jedoch laufend neue proprietäre Lösungen vorgestellt, die von diesen Standards abweichen und zum Teil auch nicht gleichzeitig in einer Nachbarschaft verwendet werden können. Die Anwendung von standardisierten Tags empfiehlt sich, meist wird der Vorteil einer proprietären Lösung mit einem anderen Nachteil erkauft, und sei es auch nur der Stückpreis des in kleiner Stückzahl produzierten Tags oder die Einschränkung auf einen Hersteller der Lesegeräte.

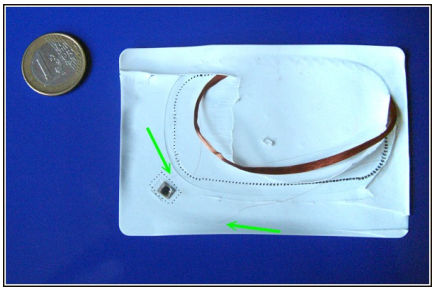
Auf verschiedenste Art kann es zu Problemen kommen, weil der RFID-Transponder direkt am Erzeugnis sitzt und dieses elektromagnetisch schlecht mit dem ausgewählten Tag verträglich ist. Um elektromagnetische Anpassungsprobleme zu umgehen, werden in der Logistik u. a. so genannte Flap- oder Flag-Tags eingesetzt, welche im rechten Winkel vom Produkt abstehen und so einen großen Abstand zum Produkt haben. Deren Verbreitung ist bisher nicht groß, jeder Anwender muss sich kritisch prüfen, ob er Liebhaberpreise für Tags durch kompetente Systemauslegung vermeiden kann.

Alleiniges Erfolgskriterium für eine RFID-Lösung ist schließlich der Leseerfolg (Lesequote) im Betriebsablauf. Darin zeigt sich das Können des beauftragten Systemanbieters. Wie bei jeder technischen Lösung muss auch bedacht werden, was im Fehlerfall passiert: Tag defekt, Leser defekt, Tag fehlt, Leser off-line, Bewegung in der falschen Richtung, zu schnell oder zu dicht nacheinander usw. Es gibt keine 100 %-Lösungen ohne Sicherungskonzept.

Baugröße & Bauformen

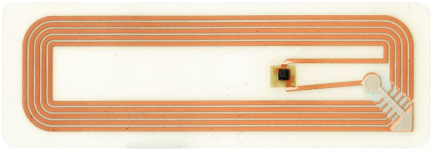
Transponder bestehen aus:

- Mikrochip
- Antenne
- Träger oder Gehäuse
- Energiequelle (bei aktiven Transpondern, siehe unten)



RFID-Chip mit Antenne

Maßgeblich für die Baugröße sind die Antenne, die Batterie und das Gehäuse. Die Form und Größe der Antenne ist abhängig von der Frequenz bzw. Wellenlänge. Je nach geforderter Anwendung werden Transponder in unterschiedlichen Bauformen, Größen und Schutzklassen angeboten.



13,56 MHz Transponder

Das Bild oben zeigt einen RFID-Chip in einer Scheckkarte. Vom Chip links unten führen zwei feine Drähte (grüne Pfeile) zu einer Spule. Sie besteht aus vielen Drahtwicklungen und füllt fast die gesamte Größe der Karte aus.

Aktive RFID-Transponder können, je nach Einsatzgebiet, durchaus die Größe von Büchern besitzen (z. B. in der Containerlogistik). Jedoch ist es mit heutiger Technik auch möglich, sehr kleine passive RFID-Transponder herzustellen, die sich in Geldscheinen oder Papier einsetzen lassen. So gab Hitachi am 16. Februar 2007 bekannt, staubkorngroße Chips mit einer Größe von 0,05 mm × 0,05 mm entwickelt zu haben.[5] Die Reichweite von passiven Transpondern ist neben der Frequenz auch maßgeblich von der Antennen- oder Spulengröße (Inlaygröße) abhängig. Die Reichweite sinkt sowohl bei UHF als auch bei HF mit kleineren Antennen rapide ab.

Transponder wurden ab Beginn des Einsatzes seit 1980 zunächst vorwiegend als LF 125 kHz passive produziert und eingesetzt. ISOCARD, CLAMSHELL Card-Bauformen aus dem LF-125-kHz-Bereich sind die weltweit am häufigsten verwendeten Bauformen im Bereich Zutrittskontrolle und Zeiterfassung. Genauso existieren auch Bauformen, die im Autoschlüssel eingebaut sind (Wegfahrsperre), bzw. als Implantate, Pansenboli oder Ohrmarken zur Identifikation von Tieren dienen. Weiterhin gibt es die Möglichkeit zur Integration in Nägel oder PU-Disk-TAGs zur Palettenidentifikation, in Chipcoins (Abrechnungssysteme z. B. in öffentlichen Bädern) oder in

Chipkarten (Zutrittskontrolle).

Im Bereich E-PURSE (elektronische Geldbörse und Ticketing) findet die 13,56-MHz-Mifare- bzw. I-Code-Technologie (Philips) Anwendung und wird weltweit in vielen Städten (Seoul, Moskau, London, Warschau etc.) in U-Bahnen, Bussen und als Universitäts- und Studentenausweis genutzt. Transponder in Form von Etiketten, die beispielsweise die Mediensicherung und Verbuchung in Bibliotheken erleichtern, werden erst seit dem Jahr 2000 in großen Stückzahlen hergestellt.

Energieversorgung

Das deutlichste Unterscheidungsmerkmal stellt die Art der Energieversorgung der RFID-Transponder dar.

Kleine batterielose RFID-Transponder besitzen keine eigene Energieversorgung und müssen ihre Versorgungsspannung durch Speisung aus den Funksignalen der Basisstationen gewinnen. Dies reduziert zwar die Kosten und das Gewicht der Chips, gleichzeitig verringert es aber auch die Reichweite. Diese Art von RFID-Transpondern wird z. B. für die Authentifizierung bzw. -auszeichnung von Produkten oder für Dokumentenverfolgung eingesetzt, da die Kosten pro Einheit hier ausschlaggebend sind.

RFID-Transponder mit eigener Energieversorgung erzielen eine erheblich höhere Reichweite und besitzen einen größeren Funktionsumfang, verursachen aber auch erheblich höhere Kosten pro Einheit. Deswegen werden sie dort eingesetzt, wo die zu identifizierenden oder zu verfolgenden Objekte eine lange Lebensdauer haben, z. B. bei wieder verwendbaren Behältern in der Containerlogistik (für See-Container bisher nur vereinzelte Einführung, noch keine weltweit wirksame Übereinkunft) oder bei Lastkraftwagen im Zusammenhang mit der Mauterfassung.

Zum Betrieb, insbesondere zur Signalmodulierung, muss der RFID-Mikrochip mit Energie versorgt werden. Hierbei werden zwei Arten von RFID-Transpondern unterschieden:

1. **Passive RFID-Transponder** beziehen ihre Energie zur Versorgung des Mikrochips aus den empfangenen Funkwellen, oft als „Continuous Wave“ (CW) bezeichnet. Mit einer Spule als Empfangsantenne wird durch Induktion ähnlich wie in einem Transformator ein Kondensator aufgeladen, welcher den Tag mit Energie versorgt. Die Continuous Wave muss aufgrund der geringen Kapazität des Kondensators durchgehend vom Lesegerät gesendet werden, während der Tag sich im Lesebereich befindet. Die Reichweite beträgt hier einige wenige Millimeter bis zu einigen Zentimetern.
2. **Aktive RFID-Transponder** sind batteriebetrieben, d. h. sie beziehen die Energie zur Versorgung des Mikrochips aus einer eingebauten Batterie. Normalerweise befinden sie sich im Ruhezustand bzw. senden keine Informationen aus, um die Lebensdauer der Energiequelle zu erhöhen. Nur wenn ein spezielles Aktivierungssignal empfangen wird, aktiviert sich der Sender. Nicht genutzt werden kann die Energie der Batterie für das Erzeugen des modulierten Rücksignals, dennoch erreicht man durch höheren Rückstrahlkoeffizienten beim Backscatteringverfahren aufgrund des geringeren Energieverbrauches an Feldenergie eine deutlich höhere Reichweite, die bis etwa 100 Meter betragen kann.

Frequenzbereiche

Für den Einsatz wurden bisher verschiedene ISM-Frequenzbänder vorgeschlagen und zum Teil europaweit oder international freigegeben:

- Niedrige Frequenzen (LF, 30–500 kHz). Diese Systeme weisen eine geringe Reichweite auf, arbeiten in der am häufigsten verwendeten 64-bit-read-only-Technologie einwandfrei und schnell genug für viele Anwendungen. Bei größeren Datenmengen ergeben sich längere Übertragungszeiten. LF-Transponder sind günstig in der Anschaffung, kommen mit hoher (Luft-)Feuchtigkeit und Metall zurecht und werden in vielfältigen Bauformen angeboten. Diese Eigenschaften begünstigen den Einsatz in rauen Industrieumgebungen, sie werden jedoch auch z. B. für Zugangskontrollen, Wegfahrsperren und Lagerverwaltung (häufig 125 kHz) verwendet. LF-Versionen eignen sich auch für den Einsatzfall in explosionsgefährdeten Bereichen. Hier können ATEX zertifizierte Versionen eingesetzt werden.

- Hohe Frequenzen (HF, 3–30 MHz). Kurze bis mittlere Reichweite, mittlere Übertragungsgeschwindigkeit, mittlere bis günstige Preisklasse der Lesegeräte. In diesem Frequenzbereich arbeiten die sog. Smart Tags (meist 13,56 MHz).
- Sehr hohe Frequenzen (UHF, 433 MHz (USA, DoD), 850–950 MHz (EPC und andere)). Hohe Reichweite (2–6 Meter für passive Transponder ISO/IEC 18000–6C; um 6 Meter und bis 100 m für semi-aktive Transponder) und hohe Lesegeschwindigkeit. Niedrige Preise für kurzlebige passive Transponder, höhere Preise für dauerhafte Transponder, tendenziell hohe Preise für aktive Transponder. Einsatz z. B. im Bereich der manuellen, halbautomatischen, automatisierten Warenverteilung mit Paletten und Container-Identifikation (Türsiegel, License-Plates) und zur Kontrolle von einzelnen Versand- und Handelseinheiten (EPC-Tags) sowie für Kfz-Kennzeichen (bisher nur in Großbritannien). Typische Frequenzen sind 433 MHz, 868 MHz (Europa), 915 MHz (USA), 950 MHz (Japan).
- Mikrowellen-Frequenzen (SHF, 2,4–2,5 GHz, 5,8 GHz und darüber). Kurze Reichweite für ausschließlich semi-aktive Transponder von 0,5 m bis 6 m bei rasanter Lesegeschwindigkeit wegen hoher Passagegeschwindigkeit für Fahrzeuganwendungen (PKW in Parkhäusern, Waggons in Bahnhöfen, LKW in Einfahrten, alle Fahrzeugtypen an Mautstationen).

Verschlüsselung

Die älteren Typen der RFID-Transponder senden ihre Informationen, wie in der Norm ISO 18000 vorgesehen, in Klartext. Neuere Modelle verfügen zusätzlich über die Möglichkeit, ihre Daten verschlüsselt zu übertragen oder Teile des Datenspeichers nicht jedem Zugriff zu öffnen.

Modulations- und Kodierungsverfahren

Keying/Modulation bezeichnet ein Verfahren um digitale Signale über analoge Leitungen übertragen zu können. Der Begriff Keying kommt aus den Anfangszeiten des Telegraphen. Die meist verwendeten Keying-/Modulationsverfahren sind:

- Amplitude Shift Keying (ASK): verwendet beim “proximity und vicinity coupling”
- Frequency Shift Keying (FSK, 2 FSK): verwendet beim “vicinity coupling”
- Phase Shift Keying (PSK, 2 PSK): verwendet beim “close coupling“

Die Leitungscodierung („encoding“) legt zwischen Sender und Empfänger fest wie die digitalen Daten so umcodiert werden, um bei der Übertragung möglichst optimal an die Eigenschaften des Übertragungskanals, in diesem Fall der Funkstrecke, angepasst zu sein. Die meist verwendeten Kanalcodierungsverfahren im RFID-Bereich sind:

- Biphase-Mark-Code und der dazu invertierte Biphase-Space-Code.
- Pulsphasenmodulationen in Kombination mit dem RZ-Code
- Manchester-Code
- Miller-Code

Einen Sonderfall stellen SAW-Tags dar, die SAW-Effekte nutzen. Dabei wird die Kennung in der Laufzeit der reflektierten Signale kodiert.

Pulk-Erkennung

Unter dem Begriff Pulk-Erkennung versteht man eine Nutzung bekannter Protokolle, in dem einzelne RFID-Tags unmittelbar nacheinander gelesen werden können, wobei dieser Prozess sich selbst organisiert. Das heißt, dass

- nicht alle Tags sich gleichzeitig bei dem gleichen Reader melden, und
- jedes Tag möglichst genau einmal gelesen wird, und
- ein einmal gelesenes Tag nach dem ersten erfolgreichen Lesen schweigt, bis es das Lesefeld verlässt oder das Lesefeld abgeschaltet wird,
- oder das einzelne dort bereits bekannte Tag vom Leser direkt erneut aktiviert wird.

Viele Anwendungen dieser auch „Singulation“ genannten funktechnischen Vereinzelung soll es dem Empfänger ermöglichen, die verschiedenen Identitäten der vorhandenen Tags streng nacheinander zu erkennen. Das Konzept ist in der Norm in verschiedener Ausprägung vorgesehen, aber bisher erkennbar nicht verbreitet. Weitere proprietäre Ausprägungen finden sich bei den verschiedenen Herstellern. An technischen Problemen mit passiven Tags ändert nichts, dass aktive Tags sich willkürlich bei einem Empfänger melden können.

Folgendes Problem wird allein durch RFID-Tags nicht gelöst: Zu erkennen,

- 1. wie viele Objekte,
- 2. wie viele Tags und
- 3. wie viele gelesene Kennzeichen

einen guten Leseerfolg ausmachen.

Bisher sind keine Einrichtungen der Pulk-Erkennung bekannt, die eine vollständige Erfassung sicherstellen (2008). Pulk-Erkennung ist für eine Inventarisierung oder eine Kontrolle der Vollständigkeit ungeeignet. Wenn kein Anti-Kollisionsverfahren und keine Stummschaltung wirken, ist die geometrische Vereinzelung außerhalb des Lesebereichs und die Beschränkung auf jeweils ein Tag im Lesebereich die Verfahrensweise mit generell besserer Erkennungsquote.

Antikollisions- oder Multi-Zugangsverfahren (Anti-collision)

Die Antikollision beschreibt eine Menge von Prozeduren, die den Tags ermöglichen, gleichzeitig zu kommunizieren, also das Überlagern mehrerer verschiedener Signale ausschließen soll. Das Antikollisionsverfahren regelt die Einhaltung der Reihenfolge bzw. Abstände der Antworten, beispielsweise durch zufällig verteiltes Senden dieser Responses, so dass der Empfänger jedes Tag einzeln auslesen kann. Die Leistung der Antikollisionsverfahren wird in der Einheit „Tags/s“ gemessen. Es gibt vier Grundarten für Antikollisions- oder Multi-Zugangsverfahren:

- Space Division Multiple Access (SDMA): Abstände, Reichweite, Antennenart und Positionierung werden eingestellt
- Time Division Multiple Access (TDMA): die Zugangszeit wird zwischen den Teilnehmern aufgeteilt
- Frequency Domain Multiple Access (FDMA): verschiedene Frequenzen werden verwendet
- Code Division Multiple Access (CDMA)

Typische Antikollisionsverfahren im RFID-Bereich sind:

- Slotted ALOHA: eine Variante des ALOHA-Verfahrens aus den 1970er (Aloha Networks, Hawaii). Aloha war die Inspiration für das Ethernet Protokoll und ist ein TDMA Verfahren. Die folgende Dramatisierung zeigt die Einfachheit und Effektivität dieses Verfahrens:
  - An der Wand eines leeren Zimmers hängt eine Uhr, die die Zeit in Millisekunden anzeigt.
  - Jetzt steht eine Person an der Wand und überblickt das Zimmer, sie repräsentiert den Leser.
  - Leser: ist jemand da? Die aktuelle Zeit ist „t“. Ich habe folgende Zeitschlitze: t + 10, t + 20, t + 30. Bitte antworten.
  - Tag 1 und 2 betreten den Raum.
  - Tag 1 würfelt und selektiert t + 30.

  - Tag 2 würfelt und selektiert t + 10.
  - Die Uhr zeigt t + 10.
  - Tag 2 sagt: zwei!
  - Leser: seid jetzt alle ruhig! Hiermit selektiere ich zwei.
  - Tag 2: das bin ich! Ich bin zwei!
  - Leser: hast du Daten mitzuteilen, zwei?
  - Tag 2: 12D25FB48C5A9E84, ich bin zwei!
  - Leser: ok, jetzt sei ruhig zwei… ist jemand da? Die aktuelle Zeit ist „t“. Ich habe folgende Zeitschlitze: t + 10, t + 20, t + 30. Bitte antworten.
- Adaptive Binary Tree: Dieses Verfahren verwendet eine binäre Suche um einen bestimmten Tag in einer Masse zu finden.
- Slotted Terminal Adaptive Collection (STAC): hat Ähnlichkeiten mit dem ALOHA-Verfahren, ist aber erheblich komplexer.
- EPC UHF Class I Gen 2: ist ein Singulationsverfahren.

Identität (Identity)

Alle RFID-Tags müssen eindeutig gekennzeichnet sein, damit der Empfänger Responses/Requests aller Tags erkennen kann:[6] RFID-Tags, in denen diese Kennzeichnung geändert werden kann, sind für eine sichere Prozessführung in einem offenen System ohne praktischen Wert (Beispiel: EPC Generation 1).

Unterscheidungsmerkmale von RFID-Systemen

Mindestmerkmale eines RFID-Systems sind

- ein Nummernsystem für RFID-Tags und für die zu kennzeichnenden Gegenstände:[7]
- Eine Verfahrensbeschreibung für das Kennzeichnen und für das Beschreiben und das Lesen der Kennzeichen:[8]
- ein an Gegenständen oder Lebewesen angebrachtes RFID-Tag, welches elektronisch und berührungslos eine seriell auszulesende Information bereitstellt.
- ein dazu passendes RFID-Lesegerät.

Zusatzfunktionen

Viele Tags unterstützen auch eine oder mehrere der folgenden Operationen:

- Die Tags können über einen sogenannten „kill code“ oder z. B. durch ein Magnetfeld permanent deaktiviert werden (engl. *kill, disable*).
- Die Tags erlauben ein einmaliges Schreiben von Daten (engl. *write once*).
- Die Tags können mehrmals mit Daten beschrieben werden (engl. *write many*).
- Antikollision: Die Tags wissen, wann sie warten oder Anfragen beantworten müssen.
- Sicherheit: Die Tags können (auch verschlüsselt) ein geheimes Passwort verlangen, bevor sie kommunizieren.

Datenstrom-Betriebsarten

RFID kann im Duplexbetrieb oder sequentiell Daten mit dem Lesegerät austauschen. Man unterscheidet:

- *full duplex system* (FDX) (Zuverlässig durch kontinuierlichem Datenstrom, geringe Reichweite)
- *half duplex system* (HDX) (gepulste Daten-Antwort, verbesserte Reichweite mittels in einem Kondensator integriert gesammelter Energie, Timing komplex)
- *sequential system* (SEQ)

Speicherkapazität

Die Kapazität des beschreibbaren Speichers eines RFID-Chips reicht von wenigen Bit bis zu mehreren KBytes. Die 1-Bit Transponder sind beispielsweise in Warensicherungsetiketten und lassen nur die Unterscheidung *da* oder *nicht da* zu.

Der Datensatz des Transponders wird bei dessen Herstellung fest in ihm als laufende eindeutige Zahl (inhärente Identität) oder bei dessen Applikation als nicht einmalige Daten (z. B. Chargennummer) abgelegt werden. Moderne Tags können auch später geändert oder mit weiteren Daten beschrieben werden.

Beschreibbarkeit

Beschreibbare Transponder verwenden derzeit meist folgende Speichertechnologien:

- nicht-flüchtige Speicher (Daten bleiben ohne Stromversorgung erhalten, daher geeignet für induktiv versorgte RFID):
  - EEPROM
  - FRAM
- flüchtige Speicher (benötigen eine ununterbrochene Stromversorgung um die Daten zu behalten):
  - SRAM

Energieversorgung

Passive Transponder entnehmen ihre Betriebsspannung dem (elektromagnetischen) Feld.

Semi-passive (auch genannt semi-aktive) Transponder besitzen eine (Stütz-)Batterie für den volatilen (flüchtigen) Speicher und zum Betrieb angeschlossener Sensoren, nicht jedoch für die Datenübertragung.

Aktive Transponder nutzen Batterien auch für den Datentransfer, sind mit einem eigenen Sender ausgestattet und erreichen so eine höhere Reichweite. In Deutschland werden sie auch als Telemetriegeräte (siehe unten) bezeichnet.

Baken-Transmitter mit Batterien, die andauernd senden und nicht auf eine Anregung reagieren.

Auch Telemetrie-SRD (Funkverbindungen über kurze Entfernungen, z. B. von Sensoren) werden teilweise als RFID bezeichnet, sie benutzen einen aktiven Sender, der z. B. mit Solarzellen oder der Bewegung des Gegenstandes (z. B. Reifendrucksensor) mit Energie versorgt wird. Bei warmblütigen Lebewesen ist auch die Versorgung aus einer Temperaturdifferenz in Entwicklung[9] .

Betriebsfrequenz

Frequenz	Bereich	Erlaubte Frequenzen (ISM-Band)
Langwellen-Frequenzen (LF)	30…300 kHz	9 kHz [sic]…135 kHz
Kurzwellen-Frequenzen (HF/RF)	3…30 MHz	6,78 MHz, 13,56 MHz, 27,125 MHz, 40,680 MHz [sic]
Dezimeterwellen (UHF)	300…3 GHz	433,920 MHz, 869 MHz, 915 MHz, 2,45 GHz [sic]
Mikrowellen	> 3 GHz	5,8 GHz, 24,125 GHz

Reichweiten und typische Anwendungen

Nach dem Englischen haben sich folgende Unterscheidungen im Sprachgebrauch etabliert:

- *Close coupling* – 0…1 cm
- *Remote coupling* (auch proximity coupling) – 0…1 m
- *Long range coupling* – > 1 m

Frequenz	Typische max. Reichweite für passive Tags	Typische Anwendungen
Langwellen-Frequenzen (LF)	50 cm	Tier-Identifizierung und Lesen von Gegenständen mit hohem Wasseranteil
Kurzwellen-Frequenzen (HF/RF)	1 m (sic)	Zugangskontrolle
Dezimeterwellen (UHF)	3-15 m	Lager und Logistikbereich (Paletten)
Mikrowellen	> 10 m	Fahrzeug-Identifizierung

Frequenzbeeinflussung

- Reflexion / gerichtete bzw. ungerichtete Streuung (*backscatter*): Frequenz der reflektierten Welle ist die Sendefrequenz des Lesegerätes
- Dämpfungsmodulation: durch den Transponder wird das Feld des Lesegerätes beeinflusst – Frequenzverhältnis 1:1)
- subharmonische Welle (Frequenzverhältnis 1:n)
- Erzeugung von Oberwellen (n-fache) im Transponder

Kopplungsmethoden

- elektrostatische Felder in kapazitiver Kopplung (für RFID eher die Ausnahme, kein Standard)
- magnetische Felder für induktive Kopplung oder Nahfeldkopplung: Datenübertragung und meist auch Energieversorgung erfolgen über das magnetische Nahfeld der Spulen im Lesegerät und im Tag.
- elektromagnetische Dipolfeldern für Fernfeldkopplung: Datenübertragung und oft auch Energieversorgung erfolgen mit Antennen (üblich sind Dipolantennen, Rahmenantennen, Ferritantennen oder Spiralantennen).

Einsatz

Generell ist die Logistik die Hauptüberschrift für das Einsatzgebiet. Logistische Problemstellungen gehen quer durch alle Branchen. Hier gibt es ein riesiges Rationalisierungspotential auszuschöpfen.

Manche Institutionen erhoffen sich darüber hinaus eine verbesserte Überwachung im Personen- und Warenverkehr. Der technische Aufwand und die Kosten auf der RFID-Seite sind überschaubar. Die zu erwartenden riesigen Datenmengen begrenzen die praktische Ausführung.

Der Begriff „fälschungssicher“ in diesem Zusammenhang wird sich nach kurzer Zeit relativieren.

Die folgende Aufzählung enthält nur einige, derzeit (2006) wichtige Gebiete:

- Fahrzeugidentifikation

  Electronic Road Pricing System in Singapur

  Die e-Plate-Nummernschilder identifizieren sich automatisch an Lesegeräten. Dadurch sind Zugangskontrollen, Innenstadtmautsysteme und auch Section-Control-Geschwindigkeitsmessungen möglich. Bei entsprechend dichtem Sensorennetz lassen sich auch Wegeprofile erstellen. In einem Großversuch hat das britische Verkehrsministerium im April/Mai 2006 ca. 50.000 Nummernschilder mit RFID-Funkchips ausstatten lassen. Ziel ist die Informationssammlung über die Fälschungsrate sowie die Gültigkeit von Zulassung und Versicherungsschutz. Bei erfolgreicher Erprobung ist eine flächendeckende Einführung geplant. Die Erfassung erfolgt im Abstand von weniger als zehn Metern. Eine Verwertung der Geschwindigkeitsmessung mit Hilfe dieser Technik ist durch die britische Rechtsprechung derzeit stark eingeschränkt.

- Banknoten

  Bereits im Jahr 2003 wurde bekannt, dass die Europäische Zentralbank mit dem japanischen Elektronikkonzern Hitachi über eine Integration von RFID-Transpondern in Euro-Banknoten verhandle.[10] Auf dem sogenannten *μ-Chip* (0,4 mm × 0,4 mm) ist eine eindeutige 38-stellige Zahlenfolge (128 Bit) gespeichert.[11] Mit einem solchen RFID-Chip gekennzeichnete Banknoten sollen besser gegen Geldfälscherei geschützt sein. Vorstellbar wäre aber auch eine lückenlose Dokumentation des Umlaufs. Aufgrund der mit der Implementierung verbundenen Kosten sowie datenschutzrechtlicher Probleme ist die Einführung bislang nicht vorgesehen.

- Identifizierung von Personen

  RFID-Chips sind in allen seit dem 1. November 2005 ausgestellten deutschen Reisepässen enthalten.

  Im November 2004 genehmigte die US-amerikanische Gesundheitsbehörde (FDA) den Einsatz des „VeriChip“ am Menschen.[12] Der Transponder der US-amerikanischen Firma Applied Digital Solutions wird unter der Haut eingepflanzt. Geworben wird mit einfacher Verfügbarkeit lebenswichtiger Informationen im Notfall. Andere Lösungen arbeiten dagegen mit Patientenarmbändern und koppeln diese Daten über den PDA des medizinischen Personals mit dem Patienteninformationssystem im Krankenhaus.[13]

- Echtheitsmerkmal für Medikamente

  Die US-Arzneimittelbehörde FDA empfiehlt den Einsatz von RFID-Technik im Kampf gegen gefälschte Medikamente. Bisher werden jedoch überwiegend optische Verfahren eingesetzt, da deren materieller Aufwand wirtschaftlich vertretbar ist. Für den Transport temperaturempfindlicher Medizinprodukte werden vielfach RFID-Tags mit Sensorfunktionen an den Transportbehältern eingesetzt. Die Aufzeichnung dokumentiert eine Verletzung von Transportbedingungen und unterstützt den Schutz der Patienten durch

qualifiziertes Verwerfen eines falsch transportierten Gutes.

- Kennzeichnung von Leiterplatten mit RFID-Tags

  RFID-Tags werden eingesetzt, um Leiterplatten oder andere Bauteile rückverfolgbar zu machen.[14] Leiterplatten wurden bislang häufig mit Barcodes gekennzeichnet.

- Bekleidungsindustrie

  In der Bekleidungsindustrie ist der Einsatz von RFID aufgrund der Verwendung von Hängeversandformen von besonderem Interesse. Als weltweit erstes Unternehmen hat Lemmi Fashion (Kindermode) die komplette Logistikkette auf RFID umgerüstet und eine weitreichende Integration mit der Warenwirtschaft (Microsoft Business Solutions) umgesetzt. Lemmi setzt hier Einwegtransponder mit 13,56 MHz ein (Philips ICode). Die Firma Levi Strauss & Co. hat vor kurzem ebenfalls begonnen ihre Jeans mit RFID-Etiketten auszustatten.[15]

- Container-Siegel

  Für See-Container sind spezielle mechanische Siegel mit zusätzlichen RFID-Tags entworfen worden, die in Einzelfällen bereits benutzt werden. Sie werden entweder wiederholt genutzt (semi-aktive RFID-Tags nach ISO/IEC 17363, ab 2007) oder einmalig eingesetzt (passive RFID-Tags nach ISO/IEC 18185, ab 2007). Bisher gibt es keine Verpflichtung zur Verwendung solcher elektronischen Siegel.

- Tieridentifikation

  Seit den 1970er Jahren kommen RFID-Transponder bei Nutztieren zum Einsatz. Außer der Kennzeichnung von Nutztieren mit Halsbändern, Ohrmarken und Boli werden Implantate bei Haustieren (EU-Heimtierausweis, ISO/IEC 11784 und ISO/IEC 11785) verwendet. Auch die Tiere im Zoo erhalten solche Implantate.

  * 125 kHz International Zootierhaltung, Nutztieridentifikation, Meeresschildkröten Erfassung, Forschung.

  * ISO 134,2 kHz (ursprünglich Europäischer) Internationaler Standard in der Nutztieridentifikation, Implantate bei Haustieren.[16]

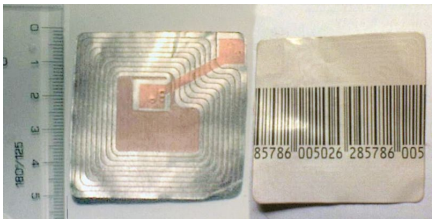
- Automobile Wegfahrsperre

  Als Bestandteil des Fahrzeugschlüssels bilden Transponder das Rückgrat der elektronischen Wegfahrsperren. Der Transponder wird dabei im eingesteckten Zustand über eine Zündschloss-Lesespule ausgelesen und stellt mit seinem abgespeicherten Code das ergänzende Schlüsselelement des Fahrzeugschlüssels dar. Für diesen Zweck werden üblicherweise Crypto-Transponder eingesetzt, deren Inhalt nicht ohne deren Zerstörung manipuliert werden kann.

- Kontaktlose Chipkarten

  In Asien sowie größeren Städten weit verbreitet sind berührungslose, wiederaufladbare Fahrkarten. Weltweiter Marktführer für das sogenannte **Ticketing** ist Philips mit seinem Mifare-System. In den USA und in Europa werden Systeme zur Zutrittskontrolle und Zeiterfassung bereits häufig mit RFID-Technik realisiert. Hier werden weltweit meist Mifare oder HiD bzw. iClass5 und in Europa hauptsächlich Legic, Mifare und teilweise unterschiedliche 125 kHz-Verfahren (Hitag, Miro etc.) eingesetzt. Manche Kreditkarten-Anbieter setzten RFID-Chips bereits als Nachfolger von Magnetstreifen bzw. Kontakt-Chips ein. 2006 kam die RFID-Technik in Deutschland bei den Eintrittskarten der Fußball-Weltmeisterschaft zum Einsatz. Ziel ist es, den Ticketschwarzhandel durch Bindung der Karte an den Käufer zu reduzieren. Beim VfL Wolfsburg und Alemannia Aachen kommt diese Technologie bereits bei Bundesliga-Spielen zum Einsatz. Fast alle größeren Skigebiete der Alpen verwenden heutzutage nur noch kontaktlose Skipässe.

- Waren- und Bestandsmanagement



RFID-Aufkleber mit EAN-Code

  In Bibliotheken jeder Größe und Typs wird RFID zur Medienverbuchung und Sicherung verwendet. Prominente Installationen sind die Münchner Stadtbibliothek, die großen Hamburger Stadtbibliotheken, die Wiener Hauptbücherei, die Stadtbücherei Stuttgart und die Hauptbibliothek der Technischen Universität Graz und der Universität Karlsruhe (TH). Die RFID-Lesegeräte sind in der Lage, spezielle RFID-Transponder stapelweise und berührungslos zu lesen. Dieses Leistungsmerkmal bezeichnet man mit Pulklesung. Das bedeutet bei der Entleihe und Rückgabe, dass die Bücher, Zeitschriften und audiovisuellen Medien nicht einzeln aufgelegt und gescannt werden müssen. Der Bibliotheksbenutzer kann auf diese Weise an RFID-Selbstverbuchungsterminals alle Medien selbständig ausleihen. Auch die Medienrückgabe kann automatisiert werden: Eigens entwickelte RFID-Rückgabeautomaten ermöglichen eine Rückgabe außerhalb der Öffnungszeiten. An den Türen und Aufgängen befinden sich Lesegeräte, die wie Sicherheitsschranken in den Kaufhäusern aussehen. Sie kontrollieren die korrekte Entleihe. Mit speziellen RFID-Lesegeräten wird die Inventarisierung des Bestandes und das Auffinden vermisster Medien spürbar einfacher und schneller.

  Große Einzelhandelsketten wie Metro, Rewe, Tesco und Wal-Mart sind an der Verwendung von RFID bei der Kontrolle des Warenflusses im Verkaufsraum interessiert. Dieser Einsatz hat in letzter Zeit zu Diskussionen geführt. Der Vereinfachung für den Kunden (z. B. Automatisierung des Bezahlvorganges) stehen Datenschutzbedenken gegenüber.

- Positionsidentifikation

  Im industriellen Einsatz in geschlossenen Arealen sind fahrerlose Transportsysteme (AGV), bei der die Position mit Hilfe von in geringen Abstand zueinander im Boden eingelassenen Transpondern bestimmt wird. Solche Systeme sind davon abhängig, dass lediglich zuvor bestimmte festgelegte Trassen und Routen befahren werden. Sobald ein Fahrzeug die Trasse verlässt, ist das System unwirksam.

- Zeiterfassung


Zeiterfassungsterminal mit RFID

  Transponder dienen am Schuh oder in der Startnummer eines Läufers bzw. im Rahmen eines Rennrades als digitales Identifikationsmerkmal in Sportwettkämpfen (Produktbeispiele: ChampionChip, Bibchip).

  An Terminals werden die Zeiten des Kommens und Gehens, evtl. auch der Pausenzeiten erfasst, wenn der Nutzer sein RFID-Medium (meist Chipkarte oder Schlüsselanhänger) in Lesereichweite bringt.

- Müllentsorgung

  In den Österreichischen Bezirken Kufstein und Kitzbühel wurde bereits im Jahr 1993 ein RFID basierendes („Veridat“) Müllmesssystem nach Liter entwickelt und flächendeckend eingeführt, sämtliche Transponder der Erstausgabe (AEGID Trovan ID200 125 kHz) aus dem Jahr 1993 sind dort trotz erneuerter Abfuhrfahrzeuge (und Reader-Einheiten) bis heute in der Originalbestückung unverändert im Einsatz. Eine Müllvorschreibung erfolgt bei diesem System nach tatsächlich gemessenen Litern (Laufende Abrechnung je

Quartal). Das System verknüpft über die Adresselemente Straße, Hausnummer, Türe und Top, automatisiert eine Personenanzahl (Datenabfrage aus dem zentralen Melderegister Österreichs) mit jedem Müllgefäß, und summiert unabhängig von einer tatsächlich abgeführten Müllmenge diese virtuell errechnete Mindestmüllmenge auf die Müllgefäßkonten. Zur Vermeidung eines sonst unweigerlichen Missbrauchs einer aufkommensgerechten Abfallvergebührung durch Littering vergleicht das System am Jahresende eine tatsächlich abgeführte Jahresmüllmenge je Gefäß mit einer virtuell aus der Personenanzahl errechneten Mindestmüllmenge (je Gemeinde 2-3 Liter je Woche und Person), und schreibt bei einer Unterschreitung der bemessenen Müllmenge eine Differenz am Jahresabschluss jedenfalls vor. Das beschriebene System befindet sich seit mehr als 14 Jahren ohne technisch bedingten Datenverlust, zudem konfliktfrei im Einsatz. Datenschutzrechliche Abläufe finden ausnahmslos innerhalb der kommunalen Gemeindeverwaltung statt, jeder Bürger kann auf Verlangen in seine Müllmessdaten in seiner Heimatgemeinde Einsicht nehmen.

In den deutschen Städten Bremen und Dresden werden Mülltonnen ebenfalls mit RFID-Transpondern versehen. Bei der Leerung erfassen die Abfuhrfahrzeuge mittels geeichter Waagen das Gewicht jeder einzelnen Tonne. Über RFID ist die Zuordnung des Abholgewichts jeder Tonne zu einem individuellen Haushalt möglich, die Bürger erhalten eine Abrechnung, die auf dem tatsächlich geleerten Gewicht (und nicht, wie sonst üblich, auf einer Volumenpauschale) basiert, bzw. in Bremen über die Anzahl der tatsächlichen Leerungen.

In Großbritannien wurden mehrere hunderttausend Mülltonnen ohne Wissen der Bürger mit RFID-Transpondern versehen.[17] Hintergrund soll die Absicht der britischen Kommunen sein, das Recyclingverhalten der Bürger zu erfassen.[18]

- Zutrittskontrolle

  Transponder am oder im Schlüssel dienen zur Zutrittskontrolle, wenn die Türen mit entsprechenden Lesegeräten oder mit entsprechenden Schließzylindern mit Leseoption ausgestattet sind.

Branche	**Kum. Anz. (in Mio.)**
Transport/Automotive	1000
Finanzen/Sicherheit	670
Handel/Konsumgüter	230
Freizeit	100
Wäschereien	75
Bibliotheken	70
Fertigung	50
Tiere/Landwirtschaft	45
Gesundheitswesen	40
Flugverkehr	25
Logistik/Post	10
Militär	2
Sonstige	80
Total	**2397**

Verbreitung und Kosten

Kumuliert wurden in den Jahren von 1944 bis 2005 insgesamt 2,397 Milliarden RFID-Chips verkauft.[19] Die genaue Verbreitung nach Anwendung sieht wie folgt aus:

Allein im Jahr 2005 wurden 565 Millionen Hochfrequenz-RFID-Tags (nach ISO/IEC 14443) abgesetzt, was insbesondere auf die erhöhte Nachfrage im Logistik-Bereich zurückzuführen ist.[20] Für das Jahr 2006 erwartet man einen weltweiten Absatz von 1,3 Milliarden RFID-Tags.[21] U. a. wegen der zunehmenden Vereinheitlichung von RFID-Lösungen sowie dem gewachsenen Austausch der Interessenten untereinander, mussten Marktforscher ihre Prognose für das Marktwachstum im Jahr 2007 um 15 % senken. So wird erwartet, dass im Jahr 2007 mit rund 3,7 Milliarden US-Dollar für RFID-Services und -Lösungen weniger Umsatz gemacht wird.[22]

Studienmöglichkeiten

Eine Reihe von Hochschulen bietet Kurse zum Thema RFID innerhalb bestehender Ausbildungen an. Seit dem Sommersemester 2009 besteht die Möglichkeit, ein Masterstudium an der Hochschule Magdeburg-Stendal(FH) [23] zu absolvieren.

Standards

- Müllentsorgung
  - Trovan
  - BDE VKI (Abwandlung ISO 11784 / 11785)[24]
- Tier-Identifizierung
  - ISO 11784
  - ISO 11785: FDX, HDX, SEQ
  - ISO 14223: advanced transponders
- Contactless Smartcards
  - ISO/IEC 10536: close coupling Smartcards (Reichweite bis 1 cm)
  - ISO/IEC 14443: proximity coupling Smartcards (Reichweite bis 10 cm)
  - ISO/IEC 15693: vicinity Smartcards (Reichweite bis 1 m)
  - ISO/IEC 10373: Testmethoden für Smartcards
- ISO 69873: für den Werkzeugbereich
- Container-Identifizierung (Logistikbereich)
  - ISO 10374: Container-Identifizierung (Logistikbereich)
  - ISO 10374.2: “Freight Container –Automatic Identification” das sog. licence plate
  - ISO 17363: „Supply Chain application of RFID – Freight Containers“ das sog. shipment tag
  - ISO 18185: „Freight Container – Electronic Seals“ das sog. eSeal (elektronische Siegel)
- VDI 4470: Diebstahlsicherung für Waren (EAS)
- VDI 4472: Anforderungen an Transpondersysteme zum Einsatz in der Supply Chain
  - Blatt 1: Einsatz der Transpondertechnologie (Allgemeiner Teil)
  - Blatt 2: Einsatz der Transpondertechnologie in der textilen Kette (HF-Systeme) (veröffentlicht 2006)
  - Blatt 5: Einsatz der Transpondertechnologie in der Mehrweglogistik (Bearbeitung abgeschlossen)
  - Blatt 8: Leitfaden für das Management von RFID-Projekten (Bearbeitung abgeschlossen)
  - Blatt 10: Abnahmeverfahren zur Überprüfung der Leistungsfähigkeit von RFID-Systemen (Bearbeitung abgeschlossen)
- Item Management (Verwaltung von Gegenständen)
  - ISO/IEC 18000 Information technology — Radio frequency identification for item management:

  - Part 1: Reference architecture and definition of parameters to be standardized
  - Part 2: Parameters for air interface communications below 135 kHz
  - Part 3: Parameters for air interface communications at 13,56 MHz
  - Part 4: Parameters for air interface communications at 2,45 GHz
  - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz
  - Part 7: Parameters for active air interface communications at 433 MHz
- Datenstrukturen und Reader-Kommunikationsprotokolle
  - EPCglobal (Electronic Product Code)
  - ISO/IEC 15961 AIDC RFID Data Protocol - Application interface
  - ISO/IEC 15962 AIDC RFID Data Protocol - Encoding Rules

Bedenken und Kritik

Technische Begrenzungen

Die Schwäche der RFID-Technik ist in der begrenzten Reichweite und in der Unschärfe der zu gewinnenden Information zu erkennen, da RFID-Chips keine direkte Information über die genaue Position und Bewegung liefern, sondern nur zur Identität. Ortsinformationen erhält man über den Umweg über die Kenntnis des Standorts des Lesegerätes. An Objekten angebrachte und von Personen mit sich geführte RFIDs könnten somit zu einer Gefahr für die Privatsphäre werden, da die unmerkbar gesendeten Daten potentiell personenbeziehbar sind (siehe unten). In dieser Hinsicht gleichen RFID einem eingeschalteten Mobiltelefon, dessen Standort anhand der nächstgelegenen Basisstation ermittelt werden kann.

Ungelöst ist derzeit noch das Problem der Entsorgung der Transponder als Elektronikschrott beim Masseneinsatz wie z. B. bei Supermarktartikeln. Unter anderem wird deshalb an neuen Materialien (z. B. auf Polymerbasis) geforscht, aber auch zur weiteren Senkung der Herstellungskosten sowie der Erschließung neuer Einsatzgebiete (z. B. in Geldscheinen und Kleidung eingearbeitete Transponder) [25] .

Gefahren des Verlustes der informationellen Selbstbestimmung

Die Gefahr der RFID-Technik liegt zum Beispiel im Verlust der informationellen Selbstbestimmung, d. h. die einzelne Person hat durch die „versteckten“ Sender keinen Einfluss mehr darauf, welche Informationen preisgegeben werden. Deshalb ist der bevorstehende massenhafte Einsatz von RFID-Transpondern unter Datenschutz-Gesichtspunkten problematisch. Um dem zu entgehen, schlagen manche Kritiker die Zerstörung der RFID-Transponder nach dem Kauf vor. Dies könnte (ähnlich wie bei der Deaktivierung der Diebstahlsicherung) an der Kasse geschehen. Ein Nachweis, dass ein Transponder wirklich zerstört bzw. sein Speicher wirklich gelöscht wurde, ist für den Verbraucher in der Regel nicht möglich. [26] .

Logo der StopRFID-Kampagne

Weiterhin ist die Integration zusätzlicher, nicht dokumentierter Speicherzellen oder Transponder denkbar. Für den Verbraucher wird ein RFID-Transponder so zur Black Box, weshalb manche eine lückenlose Überwachung des gesamten Produktionsprozesses fordern.

2003 hatte der Metro-Konzern einen Teil seiner Kundenkarten mit RFID-Transpondern ausgestattet ohne seine Kundinnen und Kunden darauf hinzuweisen. Der Konzern wurde daraufhin mit der Negativ-Auszeichnung Big Brother Award bedacht. Metro setzt seine RFID-Versuche in seinem Future Store zwar fort, tauschte die

betreffenden Kundenkarten jedoch um. Dies bewerten Datenschutz-Aktivisten als Folge ihrer Proteste. Generell kann sich ein Kunde gegen solche Praktiken erfolgreich wehren, wenn sie nicht heimlich geschehen. 2007 erhielt die Deutsche Bahn AG den genannten Big Brother Award, weil sie weiterhin – ohne die Kunden zu informieren – die BahnCard 100 mit RFID-Chips ausstattete.

Angriffs- bzw. Schutzszenarien

- Man kann versuchen, zu verhindern, dass die RFID-Transponder ihre Energie erhalten. Dazu kann man beispielsweise die Batterie herausnehmen oder die RFID-Transponder in einen Faradayschen Käfig stecken. Wenn RFID-Transponder induktiv auf *tiefen* Frequenzen um 100 kHz ankoppelt, sollte man eine Abschirmung aus magnetisierbaren Materialien wie Eisen oder MU-Metall verwenden. Bei hohen Frequenzen über 1 MHz genügt Umwickeln mit dünner Alufolie.
- Man kann einfach die Antenne beschädigen. Bei größeren RFID-Transpondern kann man im Röntgenbild die Spiralen der Antenne deutlich erkennen. Durchtrennt man sie an einer Stelle, funktioniert der RFID-Transponder nicht mehr.
- Die Induktivität einer Spulenantenne ist meist mit einem integrierten Kondensator auf die Arbeitsfrequenz abgestimmt (Schwingkreis). Durch Überkleben mit Alufolie wird die Resonanzfrequenz sehr deutlich erhöht und die Reichweite entsprechend verringert. Wenn dieser Schwingkreis die Sendefrequenz definiert, ist überhaupt kein Kontakt mehr möglich, weil das RFID auf viel zu hoher Frequenz sendet.
- Ein elektromagnetischer Impuls auf Transponder und Antenne zerstört diese ebenfalls und macht sie unbrauchbar. Als Beispiel dafür wurde auf dem Chaos Communication Congress 2005 der *RFID-Zapper* vorgestellt. Hierbei handelt es sich um ein Gerät, welches RFID-Transponder mittels eines elektromagnetischen Impulses deaktiviert. Einfacher ist es, den RFID einige Sekunden in den Mikrowellenherd zu legen. Die hohe Feldstärke zerstört die Elektronik. Dies birgt jedoch die Gefahr, dass nicht nur der Transponder, sondern auch das umgebende Trägermaterial (z. B. eine Kundenkarte) zerstört wird (beispielsweise durch Brandlöcher).
- Mit jedem handelsüblichen Elektroschocker kann man einen RFID Tag oder Chip einfach und effizient zerstören, indem man ihn nur kurz in die Funkenstrecke des Schockers bringt.
- Aufwändig: Durch Aussendung eines Störsignals – bevorzugt auf der Frequenz, auf der auch der RFID-Transponder sendet – können die recht schwachen Signale des RFID-Transponders nicht mehr empfangen werden. Dieser Störsender kann aber seinerseits geortet werden.
- Die Übertragung kann auch gestört werden, indem man eine große Zahl (mehrere hundert bis tausend) RFID-Transponder auf einen gemeinsamen Träger (Gehäuse) setzt. Wird das dadurch entstehende Gerät ("Jamming-Device") in den Lesebereich eines Lesegeräts gebracht, antworten die Tags alle gleichzeitig. Selbst wenn das Lesegerät mit Antikollisionsverfahren arbeitet, ist es bei einer derart großen Zahl von Transpondern doch überfordert und auch nicht mehr in der Lage, "echte" RFID-Tags (z. B. an Waren) zu erkennen. Solche Jamming-Vorrichtungen können als MP3-Player, Mobiltelefon, usw. getarnt sein.
- Kaum effektiv: Wie beim Telefon (per Draht oder drahtlos) kann man auch RFID-Signale ausspähen. Auf diese Weise kann man bestenfalls mitlesen, was der RFID gerade zurücksendet.
- Extrem aufwändig: RFID-Signale können manipuliert werden. Bei einem Speicherchip zur Authentifizierung werden daher auch Verschlüsselungsmethoden eingesetzt.
- Auf der IEEE Conference of Pervasive Computing 2006 (*Percom*) in Pisa stellten Wissenschaftler um Andrew S. Tanenbaum eine Methode vor, wie mit Hilfe von manipulierten RFID-Chips die Back-end-Datenbanken von RFID-Systemen kompromittiert werden können. Sie bezeichnen ihre Arbeit selbst als weltweit ersten RFID-Virus seiner Art. [27] . Diese Darstellung wird allerdings mittlerweile von verschiedenen Stellen als zu theoretisch konstruiert angesehen.[28]

Umwelt und Recycling

Auf Umverpackungen aufgebrachte RFID-Tags können nach derzeitigem Kenntnisstand nicht so gut recyclet werden wie Umverpackungen ohne RFID-Tags. Sortenreines Verpackungsmaterial wie Altglas, Altpapier oder Kunststoff kann durch die schwierig abzutrennenden RFID-Chips aus Kupfer und weiteren Metallen verunreinigt werden. Mögliche Risiken von Verunreinigungen des Recylingmaterials durch RFID-Chips können aufwendigeres Recycling oder mindere Qualität der entstehenden Rohstoffe bedeuten.[29] [30]

Störung der Medizintechnik durch RFID

Im Journal of the American Medical Association wurde im Juni 2008 eine Studie[31] veröffentlicht, die nachweist, dass zahlreiche diagnostische Messungen durch die zur Auslesung erforderlichen elektromagnetischen Wellen von RFID verfälscht werden (JAMA 2008; 299: 2884-2890). Geräte der Medizintechnik, die in jeder gut ausgestattenen Intensivmedizin-Station vorhanden sind, reagierten unterschiedlich empfindlich mit Messwert-Verzerrungen. „In einer Entfernung von einem Zentimeter bis sechs Metern kam es bei 34 von 123 Tests zu einer Fehlfunktion der medizinischen Geräte. In 22 Fällen wurden diese Störungen als gefährlich beurteilt, weil Beatmungsgeräte ausfielen oder selbsttätig die Atemfrequenz veränderten, weil Infusionspumpen stoppten oder externe Schrittmacher den Dienst versagten, weil ein Dialysegerät ausfiel oder der EKG-Monitor eine nicht vorhandene Rhythmusstörung anzeigte.“[32]

Siehe auch

- Auto-ID
- Chipkarte
- Data-Mining
- Polymerelektronik
- Near Field Communication
- Ubiquitous Computing
- Internet der Dinge

Literatur

Übersicht

- H. Bhatt, B. Glover: *RFID Essentials.* ISBN 0-596-00944-5
- Klaus Finkenzeller: *RFID-Handbuch.* ISBN 3-446-22071-2
- Patrick Sweeney: *RFID für Dummies (deutsch)* ISBN 3-527-70263-6

Monographien

- N. Bartneck, V. Klaas, H. Schönherr: "Prozesse optimieren mit RFID und Auto-ID" ISBN 978-3-89578-319-7
- Blecker, Thorsten / Huang George Q. (Hrsg.), *RFID in Operations and Supply Chain Management,* Erich Schmidt Verlag, Berlin 2008, ISBN 978-3-503-10088-0
- D.Dreher: *Der Einsatz von Radio Frequency Identification in der Logistik* ISBN 3-638-65794-9
- F. Gillert, W. Hansen: *RFID – für die Optimierung von Geschäftsprozessen.* ISBN 3-446-40507-0
- Markus Hansen, Sebastian Meissner: Identification and Tracking of Individuals and Social Networks using the Electronic Product Code on RFID Tags [33], IFIP Summer School, Karlstad, 2007, Folien [34]
- W. Franke, W. Dangelmaier: *RFID – Leitfaden für die Logistik.* ISBN 3-8349-0303-5
- C. Kern: *Anwendung von RFID-Systemen.* ISBN 3-540-27725-0 (2. Auflage, 2006)

- C. Köster: *Radio Frequency Identification. Einführung, Trends, gesellschaftliche Implikationen.* ISBN 3-8364-0162-2
- S. Kummer, M. Einbock, C. Westerheide: *RFID in der Logistik. Handbuch für die Praxis.* ISBN 3-901983-59-7
- Lietke, B., Boslau, M., Kraus, S.: *RFID-Technologie in der Wertschöpfungskette*, Wirtschaftswissenschaftliches Studium (WiSt) – Zeitschrift für Ausbildung und Hochschulkontakt (ISSN 0340–1650), Verlage C.H. Beck/Vahlen, 35. Jg., Nr. 12, S. 690–692
- Rosol, Christoph: *RFID. Vom Ursprung einer (all)gegenwärtigen Kulturtechnologie.* ISBN 978-3-86599-041-9
- R. Schoblick: *RFID.* ISBN 3-7723-5920-5
- E. Schuster, S. Allen, D. Brock: *Global RFID. The Value of the EPCglobal Network for Supply Chain Management.* ISBN 3-540-35654-1
- W. Seifert, J. Decker (Hrsg.): *RFID in der Logistik* ISBN 3-87154-322-5
- Finkenzeller, Klaus: *RFID-Handbuch : Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC*, München, 5., aktual. u. erw. Aufl., 2008 978-3-446-41200-2

Weblinks

- Literatur über *Radio Frequency Identification* in Bibliothekskatalogen: DNB [35], GBV [36]
- Verwendung von µ-Chips [37]
- Film über RFID – Auf Nummer sicher [38](avi 463 MB)
- Auto-ID Labs Forschungsverbund [39]
- EPCglobal Standardisierungsgremium für RFID und EPC [40]
- Die StopRFID-Seiten des FoeBuD e. V. [41]
- Die Spychip-Seiten der US-amerikanischen Verbraucherorganisation C.A.S.P.I.A.N. [42]
- Animation: So funktioniert RFID in der Logistik [43]
- Studie: Risiken und Chancen des Einsatzes von RFID-Systemen – Bundesamt für Sicherheit in der Informationstechnik [44] (PDF-Datei; 1,76 MB)
- BMBF Forschungszentrum zum Thema Kollaboration und RFID Humboldt-Universität zu Berlin [45]
- RFID-ATLAS: Anwendungsmöglichkeiten der RFID-Technologie - Fördermaßnahme des Bundesministeriums für Wirtschaft und Technologie (BMWi) [46]

Referenzen

[1] Rosol, Christoph: *RFID. Vom Ursprung einer (all)gegenwärtigen Kulturtechnologie.*

[2] Bundestag: *Funkchips – Die Radio Frequency Identification (RFID)* (http://www.bundestag.de/bic/analysen/2005/2005_03_21a.pdf) , 24. Mai 2007

[3] AIM Global: *AIM Shrouds of Time – The History of RFID* (https://www.aimglobal.org/estore/ProductDetails.aspx?ProductID=529) *oder AIM Shrouds of Time – The History of RFID* (http://www.rfidconsultation.eu/docs/ficheiros/shrouds_of_time.pdf)

[4] [http://www.autoidcenter.org Auto-ID Center

[5] heise online: *Hitachi treibt Miniaturisierung von RFID-Tags voran* (http://www.heise.de/newsticker/meldung/85432) , 16. Februar 2007

[6] ISO/IEC 18000-1:2008 Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46145)

[7] ISO/IEC 15459-3:2006 Information technology -- Unique identifiers -- Part 3: Common rules for unique identifiers (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43349)

[8] ISO/IEC 15459-4:2008 Information technology -- Unique identifiers -- Part 4: Individual items (http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51284)

[9] „Forschung aktuell“, Deutschlandfunk

[10] tecCHANNEL.de: *RFID-Chip soll Euro-Blüten verhindern* (http://www.tecchannel.de/news/themen/business/414589/), 23. Mai 2003

[11] Hitachi: *µ-Chip – The World's Smallest RFID IC* (http://www.hitachi.co.jp/Prod/mu-chip/), Stand: August 2006

[12] heise online: *Patientenidentifikation mit RFID-Chips* (http://www.heise.de/newsticker/meldung/77323/) , 27. August 2006

[13] RFID-Einsatz im Gesundheitswesen (http://ntcident.n-tier.de/DE/7_Publikationen/Publikationen/20040427 Praesentation RFID.pdf) (PDF; 634 KB)

[14] RFID Journal: http://www.rfidjournal.com/article/articleview/2032/1/1/"

[15] heise online: *Erste RFID-Markierungen auf Levi's Jeans* (http://www.heise.de/newsticker/meldung/72511), 28. April 2006
[16] http://www.banfield.net/about/article.asp?id=34 ISO 134,2 und der Proprietäre historische 125 kHz RFID Standard (engl.)
[17] Spiegel Online: *Briten empört: 500.000 Mülltonnen heimlich verwanzt* (http://www.spiegel.de/netzwelt/tech/0,1518,433800,00.html), 26. August 2006
[18] Mail on Sunday: *Germans plant bugs in our wheelie bins* (http://www.mailonsunday.co.uk/pages/live/articles/news/news.html?in_article_id=402439&in_page_id=1770), 26. August 2006
[19] IDTechEx: RFID tag sales in 2005 – how many and where (http://www.idtechex.com/products/en/articles/00000398.asp), 21. Dezember 2005
[20] CIO Online: *SCM – Es funkt im RFID-Markt* (http://www.cio.de/knowledgecenter/scm/827357/index.html), 25. September 2006
[21] Computerwoche: *Der RFID-Boom hat gerade erst begonnen* (http://www.computerwoche.de/nachrichten/579177/index.html), 24. Juli 2006
[22] silicon.de: *Marktforscher sieht 2007 weniger RFID-Wachstum* (http://www.silicon.de/enid/storage_network/21516), 11. August 2006
[23] http://de.wikipedia.org/wiki/Hochschule_Magdeburg-Stendal
[24] BDE Transponder (http://www.bde-berlin.de/01seiten/x4sitemap_set.htm)
[25] ZDNet.de: *Übersehene Gefahr: RFID-Chips verseuchen das Trinkwasser* (http://www.zdnet.de/itmanager/tech/0,39023442,39139086,00.htm), 5. Dezember 2005
[26] Kritik aus Sicht der Verbraucher: *Die StopRFID-Seiten des FoeBuD e. V.* (http://www.foebud.org/rfid/)
[27] *Is Your Cat Infected with a Computer Virus? (Paper)* (http://www.rfidvirus.org/papers/percom.06.pdf), Website des RFID-Virus (http://www.rfidvirus.org)
[28] *Roaming charges: Pet-embedded RFID chips bring down Las Vegas!* (http://www-128.ibm.com/developerworks/wireless/library/wi-roam45.html), Larry Loeb, 18. April 2006
[29] *Problem-Müll Funkchip* (http://www.wissenschaft.de/wissenschaft/hintergrund/287864.html), *wissenschaft.de, 5. Februar 2008*
[30] *Studie: Massenhafter RFID-Einsatz könnte Recycling verschlechtern* (http://www.heise.de/newsticker/Studie-Massenhafter-RFID-Einsatz-koennte-Recycling-verschlechtern--/meldung/98700), *heise.de, 9. November 2007*
[31] Abstract der JAMA-Studie (http://jama.ama-assn.org/cgi/content/short/299/24/2884)
[32] Deutsches Ärzteblatt: Studie: RFID-Etikette können medizinische Geräte empfindlich stören (http://www.aerzteblatt.de/v4/news/news.asp?id=32821), 25. Juni 2008
[33] https://tepin.aiki.de/blog/uploads/2007-hansen-meissner-tracking-epc-rfid-ifip.pdf
[34] https://tepin.aiki.de/blog/uploads/20070807-ifip-hansen-meissner-tracking-rfid-epc.pdf
[35] http://d-nb.info/gnd/954202376
[36] http://gso.gbv.de/DB=2.1/CMD?ACT=SRCHA&IKT=1016&SRT=YOP&TRM=954202376
[37] http://www.3sat.de/3sat.php?http://www.3sat.de/neues/dial/37123/index.html
[38] http://www.archive.org/download/AufNummersicher_546/AufNummersicher.avi
[39] http://www.autoidlabs.org/
[40] http://www.epcglobalinc.org/
[41] http://www.StopRFID.de/
[42] http://www.spychips.com/
[43] http://www.dp-dhl.de/rfid/
[44] http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf
[45] http://www.ko-rfid.de
[46] http://www.rfidatlas.de/

Quellen und Bearbeiter des Artikels

Radio Frequency Identification *Quelle*: http://de.wikipedia.org/w/index.php?oldid=65314472 *Bearbeiter*: .:bÄr, 08-15, 6BL-A504, AF666, Ahellwig, Aineias, Aka, Akl, Alblefter, Aleks-ger, Aloiswuest, Alpha dino, AngMo, Anton, Arbeo, ArtMechanic, Asdert, Authentic, AviationExpert, Avobert, BJ Axel, BLUcoder, Backwoods, Badenserbub, Bahnemann, Bananenfalter, Bdk, Belabls, Bernhard Wallisch, Bernhard55, Biberl, Bierdimpfl, Biezl, Bigbang, Bmr, Bpatgbibliothek, BravoOne, BunnyUsagi, Bye Bei, Büchsenöffner, C.Löser, Captaingrog, Casandro, Ce2, Cerno, Chaddy, Chipmeup, Cholo Aleman, Chrisfrenzel, ChristophDemmer, Clasen, Cleverboy, Coaster J, Coffeesandy, Colognese, Complex, Conny, D, DasBee, DerHexer, Diba, Donkelmann, Dontworry, Doudo, Drahtloser, Dugong, Ed.dunkel, Ejfis, ElRaki, Emgo, Ephraim33, EricPoehlsen, Ernesto, Esher, Euku, Euphoriceyes, Fab, FelixKaiser, Fipptehler, Forevermore, FriedhelmW, Frubi, Fujnky, Fusslkopp, G, GDK, GS, Garak76, Gerrit Tamm, Gnu1742, Goiken, Graukappe, Gregorgross1055, Grimsel, Grumml, Guenson, Guizza, Gunnar Eberlein, HAH, HaeB, Hafenbar, Hammertom, Hannes Röst, Harry20, Hedwig in Washington, HenrikHolke, Herbertweidner, Herrick, Historiograf, Horgner, Hubertl, Idler, IgorPodolskiy, Ilja Lorek, Itu, J. 'mach' wust, Jergen, JoePP, Jpkoester1, Justus Nussbaum, Jutta234, Kalinka, Kalinko, Karl Gruber, Karsten11, Katharina, Kdwnv, Kein Einstein, King, Kingruedi, Kku, Kmb, Kraete, Krawi, Kubrick, Kungfuman, Kunigunda, Kunobert, Kölscher Pitter, LKD, Liberaler Humanist, LimboDancer, Lipsianer, LogoX, Luiscantero, Lütke, MADE, Maprie, Mareikus, MartinWoelker, Maschinenjunge, Mathias Schindler, MauriceKA, Mbssch, Md-rfid, Mehrleisealslaut, Membeth, Micha99, MikeCGN-1, Miwu, Mjk, Mkaiser30, Mnh, MoLa, Modusvivendi, Mrilabs, Musik-chris, Mvb, Mwka, Nanahara, Ncornelius, Nerd, NetReaper, Nicor, Niemeyerstein, NoCultureIcons, Nolispanmo, Numbo3, Nuuk, Oehhar, Okfm, Okrumnow, Oms, OnlineT, Ot, P. Birken, PSS, Padeluun, Panama01, Patrickdu, Pblanc, PeeCee, Pendulin, Peter200, PhHertzog, Phantom, Philipendula, Pischdi, Plp, Polarlys, Polluks, Powerpille, Primus von Quack, Priwo, Prometeus, PsY.cHo, Pylon, Realfloasis, Regi51, Repat, Ri st, RiFID, Rissa, Rosa Schlagfertig, Rufus46, Ruppert, S.Didam, S.ludwig, STBR, Saehrimnir, Saemon, Saint Etienne, Satmap, SchorSch, Schwarzschilling, SeL, Shelmton, Shimba, Sina Eetezadi, Sinn, Sol1, Spaetabends, Spauli, Staro1, Staycoolandbegood, Stefan Kühn, Stefan h, StephanKetz, Stern, Stowasser, Supaari, Susanne und Stefanie, TdL, TheReincarnator, Thomas Schultz, Thomy pc, ThorstenS, Timekeeper, Tom md, Tomcat0815, Tomreplay, Tonk, Tuxo, Tzeh, Tönjes, UdoWDoege, Ulfbastel, UlrichAAB, Umherirrender, Walter Koch, Wdwd, Wernfried, Wesener, WikiBasti, WikiMax, WikipediaMaster, Wikipit, Xeph, YMS, Yoky, YourEyesOnly, ZDragon, Zaphiro, Zardoz28, Zaubermann, Zerberus, Zinnmann, Zum, ZweiBein, 738 anonyme Bearbeitungen

Quellen, Lizenzen und Autoren des Bildes

Datei:Rfid-reader(portal).JPG *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:Rfid-reader(portal).JPG *Lizenz*: Public Domain *Bearbeiter*: User:Wikipeder

Datei:HLG_H5.png *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:HLG_H5.png *Lizenz*: Public Domain *Bearbeiter*: User:Satmap

Datei:Rfidrp.jpg *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:Rfidrp.jpg *Lizenz*: GNU Free Documentation License *Bearbeiter*: Anton, Midnightcomm

Datei:transponder2.jpg *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:Transponder2.jpg *Lizenz*: unbekannt *Bearbeiter*: Original uploader was Kalinko at de.wikipedia

Datei:ERPBugis.JPG *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:ERPBugis.JPG *Lizenz*: Creative Commons Attribution-Sharealike 3.0 *Bearbeiter*: mailer_diablo

File:RFID-stick.jpg *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:RFID-stick.jpg *Lizenz*: Public Domain *Bearbeiter*: User:Kriplozoik

Datei:Zeiterfassungsterminal_mit_RFID.jpg *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:Zeiterfassungsterminal_mit_RFID.jpg *Lizenz*: Public Domain *Bearbeiter*: Shimba

Datei:Stoprfid-logo.svg *Quelle*: http://de.wikipedia.org/w/index.php?title=Datei:Stoprfid-logo.svg *Lizenz*: unbekannt *Bearbeiter*: Benutzer:Daniel 1992

Lizenz

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.
A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.
The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.
You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.
If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.
If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.
It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- **A.** Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- **B.** List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- **C.** State on the Title page the name of the publisher of the Modified Version, as the publisher.
- **D.** Preserve all the copyright notices of the Document.
- **E.** Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- **F.** Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- **G.** Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- **H.** Include an unaltered copy of this License.
- **I.** Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- **J.** Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- **K.** For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- **L.** Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- **M.** Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- **N.** Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- **O.** Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.
You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.
You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.
The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.
The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.
In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.
You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.
If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.
If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.
Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> Copyright (c) YEAR YOUR NAME.
>
> Permission is granted to copy, distribute and/or modify this document
>
> under the terms of the GNU Free Documentation License, Version 1.2
>
> or any later version published by the Free Software Foundation;
>
> with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
>
> A copy of the license is included in the section entitled
>
> "GNU Free Documentation License".

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

> with the Invariant Sections being LIST THEIR TITLES, with the
>
> Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.
If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.