Prof. Dr. Michael Weber

Institut für Medieninformatik
Fakultät für Ingenieurwissenschaften und Informatik

ulm university universität
uulm

vorgelegt von Stephan Kleber
Matrikelnummer: 493841

stephan.kleber@uni-ulm.de

Universität Ulm
Abgabe 17. September 2007

Gutachter Dr. Frank Kargl

Bachelorabschlußarbeit

Einsatz von RFID in der Materialverwaltung

Kurzfassung

Radio Frequency Identification (RFID) zeichnet sich als kontaktloser Kommunikationsweg zum Zugriff auf kleine, kostengünstige Datenträger aus. Durch das Anbringen solcher Datenträger an Gegenständen aller Art, können diese von einem Computersystem sowohl erkannt, als auch mit Informationen beschrieben werden. Solche Gegenstände werden als „smart“ bezeichnet, weil diese es ermöglichen intelligent reagierende Systeme zu entwerfen, die kontextbezogen auf die Anwesenheit eines Gegenstandes der realen Welt reagieren können. Neben anderen, ist dies eine Grundvoraussetzung für die Vision vom „Internet der Dinge“, die aus dem Bereich Ubiqutous Computing stammt. Diese Zusammenhänge und die grundlegenden Technologien, die hinter RFID stecken, müssen verstanden werden, um einen sinnvollen Einsatz von RFID in einem Materialverwaltungssystem bewerten zu können. Daneben soll anhand einer einfachen Umsetzung der gewonnenen Erkenntnisse in Software gezeigt werden, welche Grundfunktionen ein RFID-System mitbringen muss.

Inhalt

1 Einleitung

RFID steht für den Begriff *Radio Frequency IDentification*. Darunter versteht man die Identifizierung von Gegenständen oder Personen mittels Funkwellensignalen. Um Sinn und Funktion hinter diesem Begriff nachvollziehen zu können, muss zuallererst der Begriff der automatischen Identifizierung (Auto-ID) umrissen werden.

In vielen Bereichen des menschlichen Lebens, in denen Computer eine Rolle spielen, wird eine virtuelle Datenstruktur genutzt, um reale Situationen zu verwalten. Dazu ist es notwendig, die Daten der Repräsentation mit der abgebildeten Wirklichkeit in mehr oder weniger ständiger Übereinstimmung zu halten. Nur so kann Nutzen aus der Repräsentation gezogen und Entscheidungen sinnvoll darauf gegründet werden.

Zu Veranschaulichung soll folgendes Beispiel dienen: Die Volkssternwarte Laupheim e. V. habt einen gewissen Besitz, über den aus beliebigen Gründen Buch geführt werden muss. Dazu wird jedem Gegenstand ein Datenbankeintrag zugeordnet, der Informationen etwa über Art, Wert und Status des Gegenstandes enthält. Nun sollen Informationen zu einem Gegenstand betrachtet oder dessen Status in der Repräsentation verändert werden. Im einfachsten Fall muss ein Mensch die Beschriftung des Gegenstandes ablesen und diesen in die Suchmaske des Datenbanksystems eingeben. Diese menschliche Schnittstelle zwischen dem Identifikationsmerkmal eines Gegenstandes und dem virtuellen Verwaltungsgegenstück dieses Gegenstandes ist langsam, fehleranfällig und bedingt mühsame Arbeit von Menschen. Noch deutlicher wird dies, wenn im beschriebenen Szenario eine Inventur durchgeführt werden soll, wobei mehrere tausend Gegenstände an verschiedenen Lagerorten innerhalb eines Gebäudes identifiziert und deren korrekter Bestand, Lagerplatz oder gar Lagerbedingungen erfasst werden sollen.

All dies zu erleichtern, konkret die beschriebene Beziehung Identifikationsmerkmal-Mensch-Maschine durch eine direkte, schnelle und fehlerresistente Identifikationsmerkmal-Maschine-Brücke zu ersetzen, ist der Kern von Auto-ID [Fle]. Im erweiterten Sinne zählt dazu auch die Identifikation von Menschen beispielsweise zur Autorisation von Banktransaktionen (ec-Karte) oder für die Zutrittskontrolle zu beschränkten Bereichen.

RFID ist als Identifikationsmittel in diesem Zusammenhang in aller Munde. Mehrere Pilotprojekte verschiedener Unternehmen eine flächendeckende Nutzung dieser Technologie zu erreichen, haben einige Diskussionen in der breiten Öffentlichkeit angestoßen über die am Ende dieser Arbeit kurz gesprochen werden wird. Allerdings werden häufig mehrere Aspekte dieser Technologie missverstanden: Das physikalisch-technologische Potenzial der funkgestützten Identifikation ist weitaus eingeschränkter als viele Kritiker befürchten, aber auch als potentielle Nutzer erwarten. Dagegen sind die effizienten Anwendungsmöglichkeiten von RFID als Sensoren eines Information verarbeitenden Systems enorm.

1.1 Zielbestimmung

Beim heutigen Stand der Technik ist eine praktische Anwendung von RFID-Systemen zur Authentifizierung und in Produktion, Lagerhaltung und Logistik interessant. Die vorliegende Arbeit soll einen Überblick über diesen aktuellen Stand auf dem Gebiet der funkgestützten, automatisierten Identifikation bieten. Dies soll auch im Hinblick auf die Einsetzbarkeit in bestimmten Szenarien, insbesondere in der Materialverwaltung, geschehen.

Am Ende dieser Betrachtungen soll eine Empfehlung für adäquate Technologien zur Umsetzung eines RFID unterstützten Materialverwaltungssystems mit Ausleihe, einfa-

cher Inventur und Benutzerauthentifizierung stehen. Darüber hinaus soll ein Einblick in die physikalischen Grundlagen der verschiedenen RFID-Technologien geliefert werden, der ein Verständnis für die Möglichkeiten und Grenzen der RFID-Systeme schafft.

Im Licht all dieser gewonnenen Erkenntnisse soll – sozusagen als „Blick über den Tellerrand“ – eine allgemeine Einschätzung der technologischen Zukunft von RFID und dem Umgang der Gesellschaft mit einer Welt voller Identität funkender Gegenstände am Ende dieser Arbeit stehen.

1.2 Motivation und Abgrenzung

Aufgrund der vielfältigen Einsatzgebiete, die durch unterschiedliche RFID-Lösungen adressiert werden und häufig sehr stark spezialisiert sind, leidet die Übersichtlichkeit der zur Verfügung stehenden Hardwarepalette. Auf welche Weise welche Ausprägung von RFID-Hardware am besten geeignet ist, ist damit schwer auszumachen. Um eine sinnvolle Integration von RFID in ein Materialverwaltungssystem planen und vornehmen zu können, ist eine Klärung verschiedener Aspekte von RFID notwendig. Ausgehend von Alternativen, die auch noch heute eingesetzt werden und dadurch teilweise sogar in Konkurrenz zu RFID stehen, über physikalische, elektro- und informationstechnische Grundlagen, bis hin zum Überblick über verschiedene Einsatzgebiete und schließlich zum praktischen Einsatz, in Form einer exemplarischen Integration in ein Materialverwaltungssystem, soll diese Arbeit führen.

2 Identifikationsverfahren

2.1 Barcodes und andere Technologien zur Identifikation

Um die Fähigkeiten und Besonderheiten von RFID-Systemen und das adressierte Problem an sich bewerten zu können, soll im Folgenden eine Übersicht über verschiedene Identifikationsverfahren und deren Einsatzgebiete gegeben werden. Diese Verfahren werden in der einen oder anderen Weise auch noch heute genutzt und stehen damit in Konkurrenz zu RFID.

Eine der ersten automatisierten Identifikationsverfahren wurde in den sechziger Jahren des vorigen Jahrhunderts eingeführt. Als sowohl maschinen- als auch menschenlesbare Methode um Gegenstände erkennen zu können, wurde das OCR-Verfahren entwickelt. Die **Optische Zeichenerkennung** (*Optical Character Recognition*) basiert auf stilisierten lateinischen Buchstaben. Durch eindeutigere Unterschiede zwischen einzelnen Zeichen, als dies bei gängigen Schrifttypen der Fall ist, wird die Fehlerrate und Komplexität von Erkennungslogiken minimiert. Dennoch ist dieses Verfahren aufwändig, wodurch die benötigten Lesegeräte vergleichsweise teuer sind. [Fin 3f]

Bereits 1973 wurde der UPC (*Universal Product Code*) in den USA eingeführt. Dieser basiert auf dem sehr einfach maschinenlesbaren **Barcode-System**. Erweitert wurde dieser durch die 1976 in Europa eingeführte EAN (*European Article Number*) [Fin 3f]. Beide Systeme werden bis heute hauptsächlich in der Warenwirtschaft und den Kassensystemen des Einzelhandels verwendet. Auch viele Büchereien, Videotheken und ähnliche Einrichtungen identifizieren sowohl ihre Benutzer über Barcodes auf kreditkartenformatigen Trägern, als auch die entleihbaren Gegenstände über aufgeklebte Barcodes. Es können noch zahlreiche weitere Einsatzgebiete von Barcodes genannt werden, von Lagerhaltung und Logistik über Materialverfolgung und medizinische Anwendungen bis hin zur Personenidentifikation als Mittel der Zugangskontrolle oder Arbeitszeiterfassung. Hierzu werden meist andere Systeme als EAN/UPC verwendet, beispielsweise *Code 39* oder *Code 2/5*. Die verschiedenen Barcode-Systeme sind heute sehr weit verbreitet, da sie kostengünstig und einfach einzusetzen sind [Jes] [Han]. Um der begrenzten Speicherkapazität von klassischen Barcodes Abhilfe zu schaffen, wurden zweidimensionale Strichcodes entwickelt, die ganze Lieferscheininhalte auf einigen Zentimetern speichern können. Als Hauptvertreter von gestapelten Symbologien, die aus übereinander angeordneten Barcodezeilen bestehen, lässt sich *PDF 417* nennen. Daneben gibt es noch die so genannten Matrix-Codes, bei welchen die Information grafisch angeordnet ist und daher nur noch von CCD-Lesegeräten erfasst werden kann [Jes].

Biometrische Verfahren werden dazu genutzt Menschen aufgrund bestimmter, eindeutiger biologischer Merkmale automatisch zu identifizieren. Hierzu sind verschiedenste Eigenschaften eines Menschen geeignet, so etwa die Sprache, Fingerabdrücke, Merkmale des Auges wie die Netzhaut- oder Irisstruktur, oder die Anordnung und Form von Gesichtscharakteristika [Fin 4].

Karten mit **Magnetstreifen** wurden 1976 mit ISO[1] 3554 erstmals von der ISO standardisiert und bis heute weiterentwickelt. Der aktuelle Standard ist ISO 7810 in der Version von 2003. Diese Karten dienen der Identifikation von Personen. Am bekanntesten ist die Nutzung dieser Karten als Authentifizierungsmittel des *electronic cash* und verwandter Verfahren für bargeldlose Bezahlung im Einzelhandel.

[1] Alle Informationen über die erwähnten ISO-Standards sind, soweit nicht anders angegeben, implizit den öffentlich verfügbaren Abstracts aus dem Normenverzeichnis auf www.iso.org entnommen. Daher wird in diesen Fällen auf einen gesonderten Quellenverweis verzichtet.

Der letzte Schritt in dieser Entwicklung sind **Chipkarten**, die eher selten der reinen Personenidentifikation dienen, sondern meist Daten enthalten, aber auch komplexe Funktionen anbieten können. Sie sind mit einem integrierten Schaltkreis ausgestattet, der über elektrische Kontakte auf der Kartenoberfläche ausgelesen werden kann. Diese Karten können, gemäß ihrem Aufbau und ihrer Funktion, in Speicher- und Mikroprozessorkarten eingeteilt werden. Während die Speicherkarten, wie sie etwa bei der Krankenversichertenkarte genutzt werden [kvk 16ff], eine sequentielle Logik enthalten, über die auf einen Speicher zugegriffen wird, enthalten Mikroprozessorkarten eine komplette CPU mit Speicher für Anwendungsdaten und einem ROM für ein Betriebssystem [Fin 4ff]. Im Fall der *Java Card* kann eine Mikroprozessorkarte selbst Javaapplikationen ausführen, sobald die Karte in ein Lesegerät gesteckt und mit Energie versorgt wird [jaca]. Alle diese Karten basieren auf dem Standard ISO 7816.

2.2 RFID als kontaktloses Identifizierungsverfahren

Angesichts der zahl- und erfolgreichen Alternativen sollen hier die Vorteile von RFID gegenüber den vorgenannten Verfahren zur Identifikation kurz umrissen werden.

Während OCR und Barcodesysteme auf preisgünstigen, einfach herzustellenden Informationsträgern basieren, nämlich Aufkleber oder bedruckte Oberflächen, begrenzen die optischen Anforderungen merklich die Informationsdichte. Die Datenträger eines RFID-Systems, Transponder genannt, mit Größen von einigen Millimetern, verfügen über bis zu mehrere hundert kByte Speicherkapazität. Es gibt bereits Transponder mit Längen von 0,05 mm [hitachi], die noch 128 bit speichern. Demgegenüber bringen es klassische Barcodes beispielsweise mit 50 mm Breite auf zwischen 7 und 20 Nutzzeichen [Han]. Zweidimensionale Codes wie PDF 417 können etwas über 2000 Zeichen bei einer Fläche von mehreren Quadratzentimetern speichern [Jes]. Das entspricht einer maximalen Datendichte von unter 50 Byte/cm² bei niedrigster Fehlerkorrektureinstellung [wp PDF417]. Zudem bieten einige Transponder die Möglichkeit, Speicherinhalte zu verändern, was bei gedruckten Barcodes oder OCR-Texten nur durch Austausch oder Überkleben des kompletten Informationsträgers möglich ist.

Biometrie eignet sich per Definition ausschließlich zur Identifikation von Personen. Es können auch keine zusätzlichen Informationen gespeichert und gelesen werden, wenn man von Mimikerkennung absieht.

Karten mit Magnetstreifen als Datenträger sind anfällig für Magnetfelder in der Umgebung, die die gespeicherte Information zerstören können. Auch ist bedingt durch die Art des Lesens und Schreibens nur eine niedrige Datendichte von etwas über 200 Zeichen möglich [wp Magnetstreifen]. Zudem ist ein Magnetstreifen zur Identifikation von Gegenständen ungeeignet, da der Streifen in definierter Richtung direkt am Lesegerät vorbeigeführt werden muss. Dieser Aufwand ist im Hinblick auf andere Methoden wie Barcodes nicht vertretbar, bei denen aus einigen Zentimetern Entfernung und mit größerer Toleranz, was die Ausrichtung des Barcodes relativ zum Lesegerät angeht, erfasst werden kann.

Chipkarten, schließlich, sind RFID-Transpondern gegenüber den vorgenannten Technologien von daher am ähnlichsten, weil beide aus integrierten Schaltkreisen bestehen, deren Funktionen prinzipiell gleichartig sind. Bei beiden werden reine Speichermodule genutzt. Ebenso ist Rechenkapazität in kleinster Form durch beide Ansätze realisierbar. So können Metainformationen zum Träger des jeweiligen Schaltkreises direkt vor Ort gespeichert werden, sowie personen-, umgebungs- oder gegenstandsabhängig verarbeitet werden.

Der grundlegende Unterschied zwischen klassischen Chipkarten und RFID-Transpondern besteht in der Herstellung des Kon-

takts zum Lesegerät[1]. Während Chipkarten die physische Verbindung zum Lesegerät durch elektrische Kontaktstellen benötigen, um Energie für den Betrieb zu erhalten und Daten austauschen zu können, erfolgen diese beiden Vorgänge bei RFID-Systemen ohne direkten Kontakt. Energieversorgung und Datenaustausch werden hier durch elektrische, magnetische oder elektromagnetische Effekte ermöglicht, die später in dieser Arbeit näher betrachtet werden.

Letztendlich ist das namengebende, herausstehende Merkmal von Radio Frequency Identification, dass sowohl Daten als auch mindestens das Senden (*aktiver Transponder*), oft auch der Betrieb des Mikrocontrollers selbst (*passiver Transponder*), ohne eigene Energiequelle, sondern ausschließlich mit der vom Lesegerät erhaltenen Hochfrequenzenergie erfolgt. [Fin 1, 6f]

Diese Definition von RFID, die die funktionalen Eigenschaften umfasst, stammt aus [Lam]:

> „Die RFID-Technologie ist eine automatische Identifikationstechnologie, bei der eine Information, typischerweise eine Seriennummer, auf einem RFID Transponder gespeichert wird, der einen Mikrochip besitzt und als elektronischer Datenspeicher dient. Die Seriennummer kann mittels drahtloser Kommunikation, typischerweise über eine Distanz von einigen Metern, von einem Lesegerät ausgelesen werden. Die Stärken von RFID, speziell gegenüber dem Barcode, liegen in der vollautomatischen, gleichzeitigen Erkennung mehrerer RFID-Transponder, wobei keine Sichtverbindung zwischen Lesegerät und RFID-Transponder nötig ist. Dies erlaubt es, RFID-Transponder in Objekte einzubetten, ohne dass sie äußerlich sichtbar sind, um beispielsweise den Einsatz unter extremen Bedingungen wie Schmutz oder Hitze zu ermöglichen. Gegenüber Barcode-Scannern ist auch eine höhere Lesereichweite möglich; außerdem können Informationen auf einem RFID-Transponder mit Datenspeicher während des Einsatzes verändert werden, was bei einem Barcode nicht möglich ist.“

2.3 Ubiquitous Computing und „Das Internet der Dinge“

RFID zeichnet sich durch den kontaktlosen Informationsaustausch zwischen Transpondern, welche an allen Arten von Gegenständen angebracht sein können, und Lesegeräten, die diese Transponder unabhängig von Lage und Ausrichtung auslesen können, aus. Aus diesen Möglichkeiten ergeben sich völlig neue Perspektiven für Anwendungen von automatischen Identifizierungssystemen.

2.3.1 Ubiquitous Computing, Pervasive Computing, Ambient Intelligence

Dadurch, dass die *Tags*, wie die RFID-Transponder auch genannt werden, praktisch überall und in Verbindung mit fast jedem Gegenstand einsetzbar sind, wird RFID für das Ubiquitous Computing interessant. Um die Einsetzbarkeit von RFID in zukünftigen Szenarien bewerten zu können, soll im Folgenden ein Überblick über die Themenfelder *Ubiquitous* und *Pervasive Computing*, sowie *Ambient Intelligence* gege-

[1] Im Bezug auf RFID stellt ein Lesegerät fast immer auch eine Funktionalität zum Beschreiben von Tags zur Verfügung, die diese Funktion unterstützen. Im Folgenden ist ein Lesegerät immer auch ein potenzielles "Schreibgerät".

ben werden. Diese drei Begriffe werden häufig Synonym verwendet, besitzen aber ihre jeweils eigenen Konnotationen und Visionen für die Welt von Morgen.

Prägnant gefasst, ist das Ziel des **Ubiquitous Computing** (kurz: UbiComp) die Abschaffung von „Benutzerschnittstellen" (User Interfaces) in herkömmlichen Sinn. Durch Integration von Computern in Alltagsgegenstände, soll die bisher nötige Konzentration auf eine virtuelle Welt im Rechner – und damit auf Monitore, Tastaturen, etc. – abgelöst werden. Der Computer „enthält" nicht mehr eine Repräsentation der realen Welt, sondern ist selbst in dieser Welt vertreten und zwar in Form dezentralisierter Microcomputer. Der zentrale PC auf oder neben dem Schreibtisch sei an sich unangebracht, schreibt Mark Weiser, Visionär der ersten Stunde des UbiComp, 1991 in einem Artikel im „Scientific American" [Wei1]. Damit soll der natürliche und selbstverständliche Umgang des Menschen mit Informationstechnologie gefördert oder überhaupt erst ermöglicht werden. Allerdings bedingt dies, dass Gegenstände über ihren eigenen Standort oder über die Anwesenheit anderer Gegenstände oder Menschen „Bescheid wissen", so dass diese scheinbar intelligent reagieren können. Nur so brauchen deren Vorhandensein und deren kooperative Unterstützung für den Menschen nicht in dessen Bewusstsein zu dringen. Der Mensch kann sich auf seine eigentlichen Aufgaben und Ziele konzentrieren und sich in der immer größer werdenden Informationsflut mühelos zurechtfinden.

[Mat] ergänzt die vorige Aussage damit, dass heutige Bestrebungen, die in die vorgenannten visionären Ideen münden sollen, in zwei verschiedene Ansätze aufgeteilt werden können: Zum einen *embedded computing*, als in Alltagsgegenstände integrierte Halbleitertechnik, die den Umgang mit dem enthaltenden Gegenstand erleichtern soll. Zum anderen *Sensornetze*, welche aus miteinander interagierenden Mikrocontrollern bestehen, die mit einem System zur Erfassung einer oder mehrerer Umweltbedingungen ausgestattet sind.

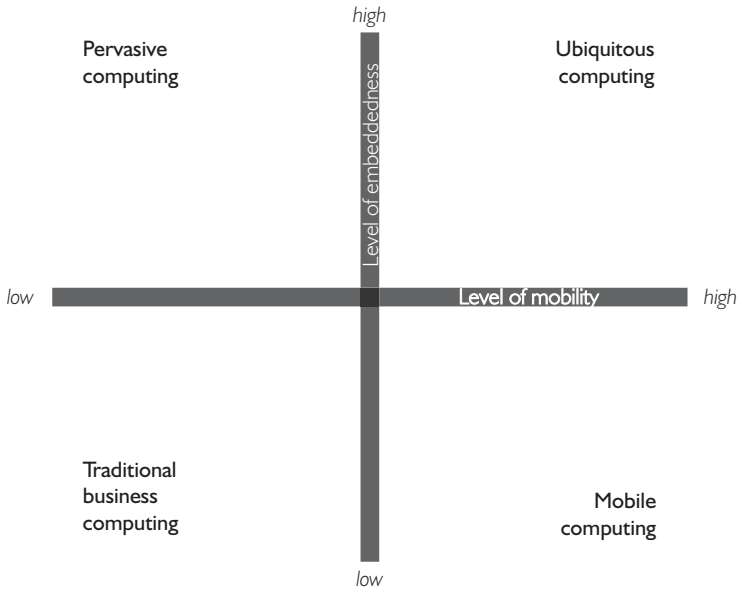

Abbildung 2.1 Dimensions of Ubiquitous Computing aus [Lyy]

Dahingegen ist die Zielsetzung des **Pervasive Computing** die Nutzung der momentan zu Verfügung stehenden technischen Möglichkeiten zur Optimierung von Prozessabläufen in Unternehmen. So ist der Begriff auch stark dadurch geprägt, dass er aus der Industrie stammt und die Betrachtungsweise des Pervasive Computing auf deren Bedürfnisse ausgerichtet ist. Stichworte sind hier *mobile commerce* und *webbasierte Geschäftsprozesse*. Mit dieser Betrachtungsweise sind implizit kommerzielle Hoffnungen verbunden [Mat 40].

Ambient Intelligence stammt im Gegensatz zu den anderen beiden Begriffen, die in den USA geprägt wurden, aus Europa [ist]. Hier geht es zunächst einmal darum, Konzepte und Architekturen zu entwickeln, die ultimativ eine Umwelt für den Menschen schaffen, die es diesem ermöglicht, auf beliebige informationstechnische Hilfestellungen überall und jederzeit im privaten und

beruflichen Alltag zurückgreifen. Die Hilfestellung soll allerdings so geartet sein, dass die eigentliche Natur der Hilfsquelle, ein Rechner, nicht spürbar wird, sondern die Umgebung scheinbar intelligent interagiert. Das bedeutet auch, dass zwar alle erdenklichen Alltagssituationen komfortabler, sicherer, effizienter und stressfreier ablaufen sollen, dass all dies aber in unaufdringlicher, intuitiver und an die jeweilige Situation der Umgebung und des Nutzers angepasste Art und Weise erfolgen soll. Das Ergebnis dieser Kombination von Anforderungen wäre eine intelligent wirkende Umgebung – die Ambient Intelligence [Mat 40f]. Monetäre und gesellschaftliche Probleme, die durch Einführung der Technologie entstehen könnten, werden als gelöst bzw. lösbar betrachtet [Biz 12].

Während verschiedene weitere Begriffe wie *mobile*, *calm* und *soft computing* [Biz 11ff], *embedded* sowie *wearable computing* und *context awareness* Teilbereiche oder Voraussetzungen der zuvor diskutierten Konzepte sind, lässt sich überblickend die in der Grafik illustrierte Einteilung geben. Diese erfolgt gemäß dem Grad der mobilen Verfügbarkeit und dem Grad der „Nahtlosigkeit“ der Einbettung – und in deren Folge der Unauffälligkeit und Selbstverständlichkeit, – der Dienste: Dabei stellt Pervasive Computing die Bestrebung zur besseren Einbettung von Rechnerunterstützung in alle Arten von Gegenständen dar. *Mobile computing* strebt gegen möglichst große Bewegungsfreiheit, während der Nutzung von Rechnerdiensten an. Die Kombination beider Bestrebungen mündet in Ubiquitous Computing. Ambient Intelligence ist die Erweiterung des Ubiquitous Computing um Aspekte alternativer Benutzerschnittstellen (Mensch-Maschine-Interaktion) und künstlicher Intelligenz.

Die drei Begriffe UbiComp, Pervasive Computing und Ambient Intelligence werden jedoch häufig synonym gebraucht, die vorangehende Unterscheidung ist also eher theoretischer Natur. Soweit in den folgenden Abschnitten des vorliegenden Textes Bezug auf dieses Themenfeld genommen wird, soll, der generellen Einsetzbarkeit von RFID in diesem Zusammenhang wegen, UbiComp als Überbegriff verwendet werden, der alle vorgenannten Aspekte einschließt [Mat 41] [Biz 12].

2.3.2 Smarte Gegenstände zur Vermeidung von Medienbrüchen

Die zentrale Voraussetzung für UbiComp ist das notwendige Kontextwissen, um algorithmisch und doch intelligent auf die Umwelt reagieren zu können. Am anderen Ende der Verarbeitungskette dieses Kontextwissens muss aber auch die Möglichkeit des Systems stehen, in die Umwelt einzugreifen und diese gemäß vorher definierten Bedingungen, abhängig von den erhobenen Umgebungsinformationen zu verändern. Im Folgenden wird zwar die Sensorik, also der erste Aspekt, adressiert, allerdings gilt analoges auch für die Aktuatorik, also Zweitgenanntes.

Im Sinne von UbiComp sollten Computersysteme bzw. Netzwerke von Minicomputern so zusammenarbeiten, dass ein Eingreifen des Menschen in einen automatisierbaren Prozess unnötig wird. Es soll beispielsweise vermieden werden, dass bei einer Inventur die zu prüfenden Inventargegenstände einzeln von einem Menschen aus dem Regal genommen werden müssen, der Bestand mit einem Soll-Wert verglichen und dieser dann in einem Inventarverwaltungssystem eingegeben werden muss. Der angestrebte Ablauf des Prozesses sollte die Brücke zwischen der realen Welt und deren Repräsentation nicht durch Menschen bilden. Stattdessen sollte der Prozess selbständig in der Lage sein, jederzeit jeden einzelnen Gegenstand zu erkennen und somit ohne Zeitversatz eine aktuelle Inventarliste zur Verfügung haben. Der Mensch ist also nicht mehr Teil des Systems, sondern reiner Nutzer der Endinformation, die das System für den Menschen ohne dessen Anstrengung und ohne dessen Fehleranfälligkeit bereitstellt.

Jedes Mal, wenn der Eingriff eines Menschen in ein solches System stattfinden muss, findet ein Medienbruch statt, der zu fehlenden, falschen oder wenig aktuellen Daten führen kann. So findet eine klassische Inventur eines Kaufhauses etwa ein bis zwei Mal im Jahr statt, da bei diesem Vorgang viel Arbeitskraft und Zeit benötigt wird und sich ein kürzeres Intervall wirtschaftlich nicht rechnet. Dies gilt, obwohl das Inventarsystem dann nur über Fortschreibungen der Daten den aktuellen Stand bestimmen kann, was durch Diebstahl, Schwund, durch fehlerhafte und beschädigte Ware zu ungenauen Angaben und schließlich zu Fehlkalkulationen in Nachbestellungen führen kann [Fle].

Durch Automation der Identifizierung von Gegenständen und der Bestimmung des Zustandes derselben, können Medienbrüche also verhindert werden. Mit geringem Aufwand können dann aktuelle und genaue Informationen über den Zustand der Teile einer definierten Umgebung und der Effizienz von Prozessen gewonnen werden. Dies führt wiederum zur Verbesserung von Folgeprozessen und zur Entlastung von Menschen. Prinzipiell kann es sich bei der angesprochenen Umgebung um ein Wohnhaus, ein Einkaufszentrum, eine Fertigungsstraße, allgemein alles, was auf Informationen über Zustände und Prozesse zurückgreift, handeln.

Voraussetzung dafür ist, dass die Teile einer solchen Umgebung in der Lage sind, zu „wissen“ wer oder was sie sind und in welchem Zustand sie sich befinden. Diese Information ist aber auch dann nur sinnvoll einsetzbar, wenn sie kommuniziert werden kann. Gegenstände, die Informationen über sich enthalten und diese auch weitergeben können, werden smarte Gegenstände genannt. „Smart“ bezieht sich dabei aber nicht darauf, dass diese Gegenstände über eine irgendwie geartete Intelligenz verfügten. „Smart“ bezieht sich darauf, dass sich die Umgebung durch Sensoren und Lesegeräte, die die im oder am Gegenstand gespeicherte Information auslesen können, so verhalten können, als ob sie ein Bewusstsein für ihre Teile hätte und damit *smartes* Verhalten simuliert [Mat 61ff].

2.3.3 Das Internet der Dinge

Smarte Umgebungen, die über das Vorhandensein und den Zustand von smarten Gegenständen in ihrem Einzugsbereich bescheid wissen, können auch untereinander kommunizieren. So entsteht ein Informationsfluss parallel zu den Bewegungen von Gegenständen in der realen Welt. Ähnlich wie beim Internet kann dann im Umkehrschluss ein „Routing“ von realen Gegenständen stattfinden. Von der Fertigungsstraße und dem Supermarktregal, über den Einkaufswagen und den Kühlschrank, bis hin zur Rechnungsstellung der Müllentsorgung und dem komponentengerechten Recycling kann in einer Welt der smarten Umgebungen ein Gegenstand selbständig den richtigen Weg für sich finden, ohne dass ein menschlicher Eingriff nötig wäre. Datenpakete des Internets sind das Vorbild für die Funktion des „Internet der Dinge“ [Bul]. Die Vision des Internet der Dinge ist allen angesprochenen Sparten des UbiComp gemein, die Schwerpunkte liegen aber unterschiedlich:

Beim Pervasive Computing stehen das Unternehmen und die Unterstützung der Geschäftsprozesse, Produktionsabläufe und Dienstleistungen im Vordergrund. Ziel ist das Echtzeitunternehmen, das

- auf zeitlich *feingranulare Informationen* zurückgreifen kann, um Entscheidungen immer aufgrund aktueller Daten fällen zu können,
- individuelle Informationen über den Verbleib von einzelnen Gegenständen erfasst und somit Daten zu *Instanzen*, nicht nur zu Klassen, von Gegenständen besitzt und damit beispielsweise besseres Qualitätsmanagement betreiben kann, in dem nach-

vollziehbar ist, an welcher Stelle das fehlerhafte Objekt seinen Fehler erhalten hat,
- Datenerfassung mit einem möglichst *feinen Lokalisationsgitter* dem Ort der Entstehung der Daten zuordnen kann, um Rückschlüsse auf einzelne Elemente eines Prozesses zu ermöglichen,
- jedem erfassten Objekt zumindest einen eindeutigen *Identifikator* zuordnet, je nach Objektart und Bedarf aber auch weitere *Informationen direkt am Objekt* sammeln kann, wie etwa Qualitätsdaten, nächste Produktionsschritte, Kundenname, Zielkonfiguration oder sogar Sensordaten wie Temperatur, Helligkeit und Feuchtigkeit an bestimmten Kontrollpunkten oder über die gesamte Objektlebenszeit hinweg.

So lassen sich in einem solchen Unternehmen die Kosten für die Integration der realen Welt reduzieren [Fle 13ff].

Eine interessante Anwendung von zeitnah verfügbaren Auto-ID Daten, wie RFID sie liefern kann, ist die Steuerung von Unternehmensprozessen durch einen geschlossenen digitalen Managementregelkreis [Fle]. Hierbei stellt die Sensorik, die durch Auto-ID-Systeme gebildet wird, die notwendigen Informationen zur Verfügung um daraus eine Regelgröße für einen Aktuator zu schaffen. So können beispielsweise nachfragesensitive Produktionsstätten, gesteuert werden, die auf Unregelmäßigkeiten im Prozess, wie etwa durch einen Maschinenausfall oder Lagerschwund, sofort reagieren können. Bei sinkenden Preisen für die Komponenten solcher Regelkreise, können diese auch in kleinerem Maßstab für Teilprozesse eingesetzt werden und so die Gesamteffizienz eines Unternehmens steigern.

Im Mittelpunkt der Betrachtungen zum Internet der Dinge steht bei Ambient Intelligence und Mobile Computing die ständige Verfügbarkeit von Informationen, die im Zusammenhang mit Alltagsaufgaben und -problemen für den einzelnen Menschen eine Erleichterung bedeuten. Als Kriterien solcher Systeme können gelten, dass immer und überall die Unterstützung durch Ubi-Comp Systeme verfügbar ist, dass die Mensch-Maschine-Schnittstellen unmerklich in der Umgebungsgestaltung verschwinden und ein Minimum an Aufmerksamkeit und gezielter Interaktion nötig ist, dass Nutzerpräferenzen und kontextuelle Bedingungen vom System automatisch bei der Ausführung von Funktionen beachtet werden und dass wiederkehrende, standardisierte Abläufe ohne Nutzereingriff durchgeführt werden können [Biz 12].

Welche Anforderungen und Ansprüche auch an das Internet der Dinge gestellt werden, welchen Nutzen man sich auch verspricht, so gilt in jedem Fall, dass eine technische und infrastrukturelle Möglichkeit gegeben sein muss, Objekte, Gegenstände und Personen eindeutig zu identifizieren. Um der Identifikation eine Bedeutung zu geben, indem diese um notwendige korres-

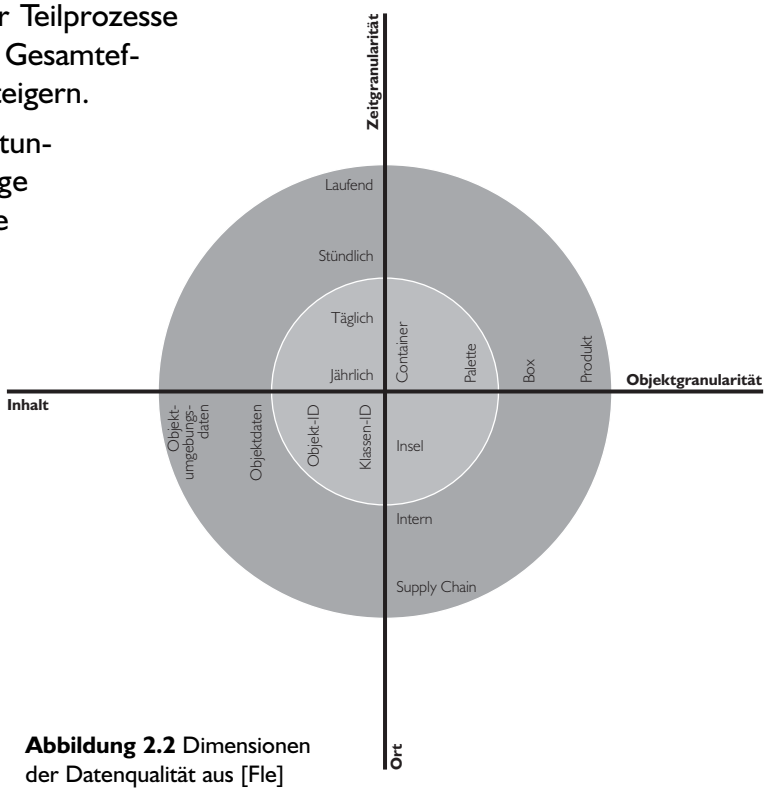

Abbildung 2.2 Dimensionen der Datenqualität aus [Fle]

pondierende Daten ergänzt wird, sind weitere Informationen eindeutig zuordenbar, sei es direkt am Gegenstand oder in einer zentralen Datenbank. Nur so kann ein Rechner auf die Anwesenheit oder das Fehlen eines Objekts in einer Umgebung und die damit verbundene Kontextänderung sinnvoll reagieren.

Um ein technologisches Rahmenwerk zu schaffen, das dies ermöglicht und von dem ausgehend eine breite Nutzung von RFID mit dem Ziel der Realisierung des Internets der Dinge initiiert werden kann, wurde 1999 am Massachusetts Institute of Technology (MIT) das Auto-ID Center gegründet. Auch andere Universitäten, Forschungseinrichtungen und Unternehmen beteiligten sich an diesem Projekt. Bis 2003 wurden in diesem Rahmen Grundlagen geschaffen, die eine breite Anwendung vorbereiten sollten. Seit 2003 wurde dieser nächste Schritt von EPCglobal übernommen, das als kommerzielle Nachfolgeorganisation gemeinsam von UCC (Uniform Code Council) und EAN International auf den Weg gebracht wurde. Beide Organisationen zeichnen für die internationalen Standards im Barcodebereich verantwortlich. Die an der Forschung im Rahmen des Auto-ID Centers beteiligten Universitäten arbeiten unter der Bezeichnung Auto-ID Labs parallel dazu weiter. Die entwickelten Schlüsseltechnologien dieser Initiativen werden im Folgenden kurz beschrieben.

Das zentrale Merkmal zur Identifizierung von Objekten mit Hilfe von RFID-Transpondern ist gemäß den Konzepten von EPCglobal, eine auf jedem der Siliziumchips vorhandene weltweit eindeutige Nummer. Was hierbei für das Internet die Internet-Protokoll-Nummer (IP-Adresse) ist, stellt im Internet der Dinge dieser Electronic Product Code (EPC) dar, über den in Datenbanken zugehörige Informationen zugeordnet werden können. Es ist nicht vorgesehen, dass weitere Informationen direkt auf dem Transponder gespeichert werden.

Der EPC selbst ist in der aktuellen Version des *Tag Data Standard* [tds] eine Nummer im Wertebereich zwischen 64 und 202 bit je nach Enkodierungsschema, wobei alle 64 bit-Schemata als veraltet deklariert wurden und ab einem noch zu nennenden Zeitpunkt in der Zukunft ungültig werden. Das Schema, von dem die weitere Interpretation des EPC abhängt, wird von einem 8 bit Headerfeld bestimmt. Abgesehen von den 64-bit-Schemata und reservierten Wertebereichen sind bisher Headerfeldwerte für folgende Schemata definiert:

- SGTIN (96 und 198 bit): EAN.UCC Global Trade Item Number, serialisierte Version
- SSCC (96 bit): EAN.UCC Serial Shipping Container Code
- SGLN (96 und 195 bit): EAN.UCC Global Location Number
- GRAI (96 und 170 bit): EAN.UCC Global Returnable Asset Identifier
- GIAI (96 und 202 bit): EAN.UCC Global Individual Asset Identifier
- GID (96 bit): General Identifier
- DoD (96 bit): Zulieferer-Produktnummer des US-Amerikanischen Department of Defense

Der GID ist darunter der einzige völlig von bisherigen Spezifikationen unabhängige Code, der eine allgemeine Identifikationsnummer zur Verfügung stellt. Eine Organisation, die Objekten GIDs zuweisen will, erhält von EPCglobal zu diesem Zweck eine *General Manager Number*, die unmittelbar nach dem *Header* des EPC genannt wird. Die folgende *Object Class*, die Arten von Objekten bestimmen soll, wird dann genauso von der per General Manager Number identifizierten Organisation vergeben, wie die abschließend folgende *Seriennummer*, die einzelne Instanzen der definierten Objektart ausweist.

Alle EAN.UCC-Nummern sind Adaptionen bestehender Nummernkonventionen für verschiedene Zwecke zur Nutzung in RFID-Tags. Der DoD-Identifikator wird vom Department of Defense der US-Amerikanischen Regierung verwaltet. Von der ursprünglich geplanten einheitlichen GID für alle Anwendungsbereiche musste aufgrund der Anforderung der Endnutzer abgerückt werden, da diese ihre bisherigen Nummernschemata nicht aufgeben wollten [Flö]. Es wurden aber auch zusätzliche Funktionen in die EPC-Spezifikation aufgenommen: Für alle bisherigen Codes, die nur Klassen von Objekten, jedoch keine Einzelinstanzen dieser Objektarten identifizieren konnten, wurde eine Seriennummer hinzugefügt. Bei der GTIN beispielsweise, die die bisherigen EAN/UPC-Barcodes repräsentiert, wurde ebendiese Seriennummer hinzugefügt, jedoch zusätzlich ein *Filter Value*-Feld, das ein Lesegerät in die Lage versetzt die Verpackungseinheit, die durch diese EPC bezeichnet wird, zu bestimmen. Vorgesehen sind „einzelverpackte Waren", „Standard Verkaufsgütergruppierung" (bspw. eine Palette), „Endkundenware" und ein Wert für bisher nicht spezifizierte Filterkriterien. So kann ein Lesegerät, falls gewünscht, selektiv nur bestimmte Verpackungseinheiten erfassen. Außerdem wurde ein *Partition*-Feld eingeführt, das angibt, wie lang das *Company Prefix* bzw. die *Item Reference* ist, die beide variabel viele, zusammen aber 13 Dezimalzahlen enthalten.

Standards für Transponder, Lesegeräte und Schnittstellen werden in den Abschnitten weiter unten näher betrachtet und daher hier nicht genauer beschrieben. Es ist aber der Erwähnung wert, dass seit dem Übergang vom Auto-ID Center zu EPCglobal der Trend besteht möglichst wenig normative Vorgaben zu machen und sich auf die notwendigsten zu beschränken. So wurden beispielsweise Pläne für die Referenzimplementierung einer Middlewarekomponente namens Savant aufgegeben und stattdessen die Definition einer Schnittstelle zwischen RFID-Middleware und Applikation angestrebt, die den Namen Application Level Events trägt (ALE) [Flö]. Im Fall der *Physical Markup Language* (PML) ist die Entwicklung beim Übergang zu EPCglobal eingestellt worden und durch eine analoge Spezifikation innerhalb des im Folgenden genannten EPCIS bzw. im *Reader Protocol* (vgl. Abschnitt 3.4) ersetzt worden. Diese Datenformate stellen XML-Schemata dar, wobei die EPCglobal-Ansätze nur einen Rahmen für hersteller- und produktspezifische Erweiterungen bietet [Flö 95] [arch 51] [epcis] [rp].

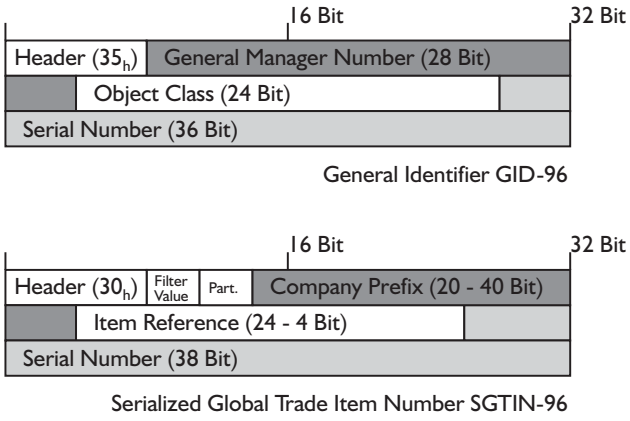

Abbildung 2.3 Beispiele für EPC-TDS-Bit-Level-Encodings

Dienste, die vom Auto-ID Center entwickelt und von EPCglobal weiter betreut werden, sind der *Object Naming Service* (ONS) und der *EPC Information Service*. Solche von EPCglobal unterhaltenen zentralen Dienste werden als *EPCglobal Core Services* beteichnet [arch 7]. Beim ONS handelt es sich um ein auf dem Domain Name Service (DNS) Protokoll basierendes System, um einzelnen EPC-Identifikatoren eine Datenquelle zuzuordnen. Zu diesem Zweck wird eine Anfrage an einen ONS-Server gestellt. Diese Anfrage enthält eine interpretierte Repräsentation des betreffenden EPCs in Form eines URNs. Der ONS-Server wiederum erzeugt eine Anfrage an einen DNS-Server für den URL, der Informationen zum angegebenen EPC enthält. Dieser URL könnte etwa ein EPC Information Service (EPCIS) Anbieter sein. Diese Auflösung eines EPC zu einem korrespondierenden URL führt nur zu Informationen über die Objektklasse, nicht jedoch eines einzelnen Objekts. Die Auflösung der Seriennummer

zu individuellen Daten betreffend einzelner Objekte muss unabhängig vom ONS durch den in der URL angegebenen Server der Anwendungsschicht auf eine nicht näher spezifizierte Art geleistet werden. Das Fehlen dieser Funktionalität in der ONS-Spezifikation soll in zukünftigen Versionen behoben werden [ons].

Der EPC Information Service ist eine Spezifikation, die es verschiedenen Applikationen erlauben soll, EPC-bezogene Daten auf semantisch sinnvoller Ebene auszutauschen. Dies kann innerhalb eines Unternehmens, aber auch organisationsübergreifend, in den durch das *EPCglobal Network* verbundenen Servern, geschehen. Erklärtes Fernziel dieses Dienstes ist es einen globalen Einblick in die Informationen der EPC tragenden Objekte, innerhalb des jeweils relevanten Kontexts, zu erhalten. Version 1.0 dieser Spezifikation wurde im April 2007 von EPCglobal verabschiedet [epcis].

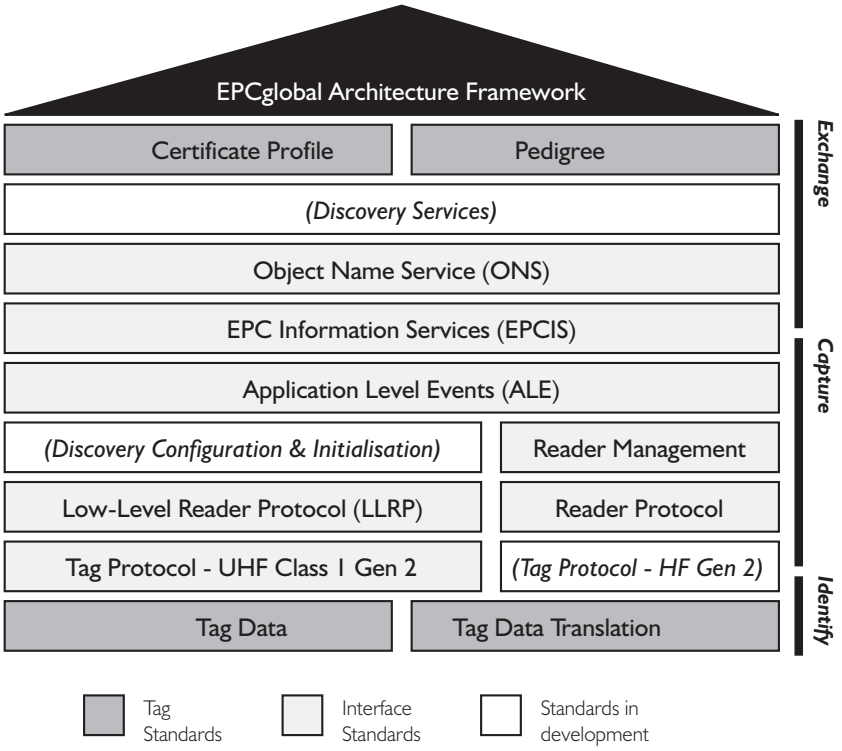

Abbildung 2.4 Übersicht über die EPCglobal Standards nach *http://www.epcglobalinc.org/standards*

Weitere Standardisierungsbemühungen unternimmt neben EPCglobal vor allem die *International Organisation for Standardisation* (ISO). Während beispielsweise ISO 15693 13,56 MHz-Transponderprotokolle definiert, befasst sich ISO 11784 mit Identifizierungscodes für Tiere und ISO 15963 nennt das Format für eine auf die Anforderungen der Waren- und Güterwirtschaft spezialisierten Identifikator. Diese und weitere ISO-Standards werden im Abschnitt 4.1 dieser Arbeit vorgestellt.

Weitere Ansätze im Bereich des UbiComp bezüglich des Internet der Dinge basieren in erster Linie auf anderen Technologien zur Identifikation als RFID. Beispielsweise setzt das *Cooltown*-Projekt der Firma HP auf Barcodes, Infrarotsensoren und ähnliche Technologien. Matrixcodes, die ursprünglich zum Einsatz in Industrie, Logistik und Verkauf von Denso in Japan entwickelt wurden, werden beispielsweise von einem Projekt der Firma Kaywa zum schnellen Zugriff auf Websites, SMS und ähnliche Dienste für das Handy genutzt [kaywa].

3 Technologische Basis

3.1 Physikalische Grundlagen

Es gibt verschiedene Systeme, die schon seit einiger Zeit in Deutschland annähernd flächendeckend zur Diebstahlsicherung eingesetzt werden. Diese Systeme verwenden 1-bit Transponder, die dem Lesegerät ihre Anwesenheit signalisieren. Alle Systeme beruhen darauf, das vom Lesegerät ausgesandte Signal so zu modifizieren, dass damit Information übertragen werden kann. Die erwähnten 1-bit Transponder entsprechen damit zwar der Definition eines RFID-Systems, die im folgenden Abschnitt gegeben wird, tragen aber außer ihrer Anwesenheit keine Information, so dass sie im Rahmen der Betrachtungen zu RFID-Systemen für die Materialverwaltung uninteressant sind. Informationen zur Funktionsweise enthält [Fin 32ff].

3.1.1 Energieversorgung

Bei den n-bit Transpondern gibt es grundsätzlich mehrere Möglichkeiten der Klassifizierung der Energieübertragungsverfahren. Das Hauptunterscheidungskriterium ist, ob der Transponder eine eigene Energieversorgung in Form einer Batterie besitzt oder nicht. Während aktive Transponder eine eigene Energiequelle besitzen, beziehen passive die Energie zum Betrieb des Mikrocontrollers aus ihrer Antenne, in der auf verschiedene Art Spannung entsteht. Diese Verfahren werden im Folgenden kurz erläutert.

Bevor auf die Unterschiede zwischen aktiven und passiven Transpondern eingegangen werden kann, muss noch die begriffliche Bedeutung eines aktiven Transponders im Bezug auf die Definition von RFID geklärt werden. *Aktive Transponder* werden in der Literatur auch als *semi-aktiv* oder *semi-passiv* bezeichnet, um auszudrücken, dass die Datenrückübertragung zum Lesegerät auf Grund einer Modifikation des magnetischen oder elektromagnetischen Feldes erfolgt, das von außen an den Transponder dringt. RFID-Transponder sind in diesem Sinne nie „aktiv“, denn es wird definitionsgemäß kein eigenes Hochfrequenzsignal (HF-Signal) erzeugt, sondern das durch das Lesegerät vorhandene genutzt. Transponder, die ein eignes HF-Signal aussenden, gehören zu den Telemetriesendern oder *short range devices* (SRD), auch wenn diese Begrifflichkeit von den Marketingabteilungen häufig komplett ignoriert wird [Fin 23ff]. Diese Arbeit beschäftigt sich mit RFID, nicht mit SRD, daher lassen sich die Begriffe „semi-aktiv“, „semi-passiv“ und „aktiv“ in diesem Zusammenhang der Einfachheit halber zu „aktiv“ zusammenlegen.

Aktive Transponder besitzen eine eigene Energiequelle, die aber ausschließlich der Versorgung des Mikrocontrollers dient und nicht zur Datenübertragung zum Lesegerät eingesetzt wird. Der primäre Einsatzzweck muss die hohen Kosten des Transponders, dessen große Bauform durch die zusätzliche Energiequelle und die gegebenenfalls nötige Wartung, die je nach Lebensdauer des Transponders einen regelmäßigen Batterie- oder Transponderaustausch umfasst, rechtfertigen können. Im Gegenzug steht eine im Vergleich große Kommunikationsreichweite zur Verfügung. Aktive Transponder können eine Reichweite bis zu 15 m besitzen, da aus der Antenne keine Energie für die Versorgung des Chips abgezogen werden muss [Fin 23ff]. Außerdem lässt sich mit der so verfügbaren Energie eine umfassende Bandbreite an Funktionalität für die Mikrocontroller erreichen. Daher wird dieser Typ auch für Sensoren aller Art verwendet, die durch entsprechende Kapselung in ein robustes Gehäuse auch widrigen Umständen standhalten können. Dazu gehören Temperatur-, Druck-, Feuchtigkeits- und Beschleunigungssensoren [Fin 388ff].

Aufgrund des deutlich geringeren Preises und der kleineren Bauform, die selbst eine Integration in Papier- bzw. Kunststofffolien-

aufkleber ermöglicht, sind passive Transponder dagegen für eine einfache und in hohen Stückzahlen durchgeführte Auszeichnung von Objekten geeignet. Die geringere Reichweite von wenigen Millimetern bis zu wenigen Metern, ist bei vielen Anwendungen problemlos zu verschmerzen, wenn nicht sogar aus Sicherheitsgründen oder um eine genauere Lokalisation zu ermöglichen, erwünscht [Fin 28f].

Da in vorliegender Arbeit der Einsatz als Massenauszeichnung von Gegenständen eines Inventars betrachtet wird, soll in den weiteren Ausführungen der Schwerpunkt auf den passiven Transpondern liegen. Diese können noch weiter klassifiziert werden. Ein Kriterium orientiert sich am physikalischen Effekt, der der kontaktlosen Energieversorgung zugrunde liegt. Die Energieübertragung kann hierbei, wie angedeutet, auf mehrere Arten erfolgen:

Zum einen durch die selten verwendete kapazitive Kopplung über elektrische Felder, wobei durch nahe beieinander liegende parallele Leiterplatten von Lesegerät und Transponder ein Kondensatoräquivalent geschaffen wird. Dieser elektrostatische Effekt ist in der Lage maximal einige Millimeter zu überbrücken. Für deutlich größere Reichweiten bis zu 8 m [inotec] sind elektromagnetisch gekoppelte Transponder geeignet. Diese entnehmen dem elektromagnetischen Feld des Lesegeräts die notwendige Energie durch Induktion in Dipolantennen. Die elektrodynamisch erzeugte Spannung auf den Antennenanschlüssen wird, wie bei allen anderen Verfahren, gleichgerichtet und für die Versorgungsspannung des Mikrocontrollers verwendet. Bei induktiver Kopplung über Magnetfelder, die nach Verkaufszahlen, die bei Weitem bedeutendste ist [Fin 65], bezieht der Mikrochip seine Energie aus dem magnetischen Feld des Lesegeräts. Damit entspricht die Funktionsweise der, eines Transformators zur galvanischen Trennung.

Größe und Form der Antennen bzw. Spulen bestimmen dabei die Energieausbeute im Transponder. Je größer beispielsweise die vom magnetischen Feld durchflossene Spulenfläche bzw. die Anzahl Spulenwindungen ist, desto mehr Energie kann aus dem magnetischen Feld entzogen werden und desto größer wird die Reichweite des Systems in der Folge.

Es existieren noch weitere Kriterien zur Klassifikation der Energieversorgung passiver RFID-Transponder. Hauptsächlich handelt es sich dabei um die Unterteilung in Halb- und Vollduplexverfahren in Kontrast zu den sequentiellen Systemen[1]. Bei den Duplexsystemen wird eine so genannte *continous wave* vom Lesegerät ausgesandt, die den Transponder ununterbrochen mit Energie versorgt. Daneben ist die Versorgungsenergie bei sequentiellen Systemen gepulst und die Datenrückantwort des Transponders an das Lesegerät erfolgt in dessen Sendepause.

Der Vorteil einer gepulsten Energieversorgung ist ganz allgemein, dass in der Sendepause des Lesegeräts nur der Transponder sendet und damit dessen Signal nicht vom Signal des Lesegeräts getrennt werden und damit auch weniger Signalrauschen unterdrückt werden muss, was auch zu einer höheren Reichweite führen kann. Um dies zu erreichen gibt es zwei Ansätze, induktiv gekoppelte und Oberflächenwellen-Transponder (OFW). Bei induktiv gekoppelten Systemen, wird die Energie für das Rücksignal des Transponders aus einem, während der Ladephase angeregten Schwingkreis, gewonnen. Der Chip wird während dieser Phase in einen Stromsparmodus versetzt, so dass praktisch die gesamte empfangene Energie in einem Kondensator gespeichert werden kann. So sind höhere Betriebsspannungen für den Chip möglich und die Leistungsaufnahme des Chips kann im Prinzip beliebig groß sein [Fin 42f, 58ff].

[1] Die Begriffe Halb-, Vollduplex und sequentiell, sind gemäß [Fin 42f] zu verstehen.

Transponder, die auf OFW (*surface acoustic wave devices* – SFW) beruhen, enthalten keinen Mikrocontroller wie die bisher betrachteten RFID-Geräte, sondern bestehen aus einem Material, auf dem durch den piezoelektrischen Effekt die Ausbreitung von Oberflächenwellen ausgelöst wird. Ein so genannter Interdigitalwandler übersetzt die HF-Signale in OFW-Signale. In Ausbreitungsrichtung der Wellen befinden sich in verschiedenen Abständen Reflektoren auf dem Trägermaterial, die Wellenanteile zurück zum Interdigitalwandler reflektieren. Dort von der OFW wieder zum HF-Signal konvertiert, wird dieses von der Antenne zum Lesegerät zurückgeschickt. Durch verschiedene Einflussgrößen wie Temperatur und Druck, kann sich die Ausbreitungsgeschwindigkeit der Wellen auf dem Trägermaterial verändern. Durch Messungen der Laufzeit zwischen den reflektierten Signalen, können diese Transponder als Sensoren dienen [Fin 61ff, 160ff].

3.1.2 Datenübertragung

Die vorgenannten Halb- und Vollduplex-Verfahren unterscheiden sich im Bezug auf die zeitliche Organisation der Datenübertragung. Während beim Halbduplex entweder Lesegerät oder Transponder sendet, können bei Vollduplex beide gleichzeitig senden. Da in jedem Fall zum Senden und Empfangen dieselbe Antenne verwendet wird, sowohl im Lesegerät als auch im Transponder, müssen die jeweils eigenen Signale von denen des Gegenübers unterschieden werden. Im Fall des Lesegeräts ist diese Detektion der Veränderungen, die der Transponder bewirkt hat, nicht trivial. Bei einer resonanzüberhöhten Antennenspannung von 100 V ist das besagte Nutzsignal als 10 mV-Schwankung zu erwarten (13,56 MHz-System, ungefähre Werte) [Fin 47].

Es gibt analog zu den Energieversorgungsverfahren drei korrespondierende Möglichkeiten zur Datenübertragung. Bei kapazitiver Kopplung wird derselbe Kondensator, den Lesegerät und Transponder zusammen bilden, zur Modulation eines elektrischen Feldes zwecks Kodierung von Signalen verwendet. Ebenso ist bei induktiver Kopplung die Veränderung des Energieabzugs in der Spule (Antenne) des Lesegerät messbar: Durch Zuschalten eines Lastwiderstandes im Transponder wird die Impedanz der Lesegerätantenne verändert. Erfolgt dies periodisch, entsprechend der zu übertragenen Daten, können diese vom Lesegerät erkannt werden. Dies wird Lastmodulation genannt.

Bei elektromagnetischer Kopplung ist keine direkte energetische Rückwirkung auf die Lesegerätantenne möglich. Die elektrischen und magnetischen Felder, die von der Antenne erzeugt wurden, haben sich in der Empfangsentfernung des Transponders bereits von der Antenne abgetrennt und existieren als unabhängige, sich mit Lichtgeschwindigkeit ausbreitende Felder bzw. Wellen, die energetisch nicht mehr mit ihrer Quelle verbunden sind. Das nötige Prinzip um Daten zurück an das Lesegerät übermitteln zu können, muss also ein anderes sein.

Elektromagnetische Wellen lassen sich reflektieren. Was vom sichtbaren Licht bekannt ist, gilt für das gesamte EM-Spektrum. Allerdings hängt die Fähigkeit eines Objektes, als Reflektor zu wirken, stark von dessen Größe, Form und Leitfähigkeit ab, vor allem aber vom Verhältnis der Objektgröße zur Wellenlänge [Fin 125f]. Idealerweise haben Transponder-Antennen eine Größe, die eine Resonanz bei der gewünschten Strahlungsfrequenz möglich macht, was dann geschieht, wenn Wellenlänge und Objekt vergleichbare Größen besitzen. So sind eine große Energieausbeute für den Chipbetrieb und ein möglichst hoher Rückstrahlquerschnitt, also eine gute Reflexion zum Lesegerät zurück, möglich. Besonders geeignet sind dafür Frequenzen mit Wellenlängen von einigen Zentimetern, da die Antennen in der Praxis in dieser Größe verwendet werden können. Die verwendeten Frequenzen von 868 MHz, 915 MHz und 2,45 GHz haben Wellenlängen von respektive etwa 35 cm, 33 cm und 12 cm.

Das Verfahren der Reflexion elektromagnetischer Wellen wird *backscatter* genannt. Um Daten auf das reflektierte Signal modulieren zu können, wird eine an der Antenne angeschlossene Last, also ein Widerstand, entsprechend der Datenenkodierung zugeschaltet. So wird dafür gesorgt, dass sich die Reflexionseigenschaften der Antenne ändern, was am Lesegerät, anhand der Stärke des von der Antenne abgegriffenen Rücksignals, gemessen werden kann. Dies stellt also eine Amplitudenmodulation dar und wird als modulierter Rückstrahlquerschnitt oder *modulated backscatter* bezeichnet [Fin 50ff].

Die Signalübertragung kann in Nahfeld[1] und Fernfeld eingeteilt werden. Dem Nahfeld gehören induktive und kapazitive Kopplung an. Beide arbeiten hauptsächlich mit Frequenzen um 135 kHz und 13,56 MHz und übertragen Daten vom Transponder zum Lesegerät durch Manipulation am magnetischen oder elektrischen Feld. Dies geschieht vor dessen Ablösung von der Lesegerätantenne per Rückwirkung auf deren Leistungsaufnahme. Dem Fernfeld gehört die Backscatterkopplung an, die die elektromagnetischen Wellen amplitudenmoduliert zum Lesegerät reflektiert. Diese arbeiten mit Frequenzen um 868/915 MHz und 2,45 GHz oder 5,8 GHz.

Die wichtigsten Frequenzen zum Einsatz bei RFID werden mit LF (*low frequency*, 100 – 135 kHz), HF (*high frequency*, 13,56 MHz), UHF (*ultra high frequency*, 868/915 MHz) und MW (*micro wave*, 2,45 GHz und 5,8 GHz) bezeichnet. Eine detaillierte Übersicht unter Berücksichtigung verschiedener Richtlinien zur Verwendung von Funksignalen gibt [Fin 169ff].

3.2 Hardware

Zur benötigten Hardware für ein RFID-System gehören grundsätzlich Lesegerät, Transponder und ein Rechner zur Weiterverarbeitung der gewonnenen Informationen. Insbesondere Transponder, aber auch Lesegeräte und deren grundlegende Funktionsweise werden im Verlauf dieses Abschnittes diskutiert.

Das Lesegerät besitzt wie der Transponder eine Antenne bzw. Spule je nach Art der Kopplung, also je nach Art der Energie- und Datenübertragung (vgl. voriger Abschnitt). An diese Antenne bzw. Spule ist zur Erzeugung des notwendigen magnetischen oder elektromagnetischen Feldes, zur Modulation und Demodulation der Informationen auf dieses Feld und zur Energieentnahme im Transponder ein HF-Interface im Lesegerät respektive Transponder angeschlossen. Die gewonnenen Signale werden an die dahinter liegende Verarbeitungseinheit weitergegeben. Im Falle des Lesegeräts ist diese Verarbeitungseinheit Software, zum Teil auch oder in spezialisierten und eingebetteten Systemen eine Hardwareimplemetierung derselben.

Die **Transponder**chips können gemäß ihrer Funktionsweise in elektronische oder physikalische Datenträger eingeteilt werden. Zu den physikalischen Datenträgern werden 1 bit-Transponder und Oberflächenwellensysteme gerechnet, die hier nicht weiter betrachtet werden sollen. Die elektronischen Datenträger, die durch integrierte Schaltungen (ICs) realisiert werden, können wiederum in reine Speichermedien auf Basis von Zustandsmaschinen sowie in gegebenenfalls programmierbare Mikroprozessoren eingeteilt werden [Fin 317].

Im Fall eines Transponders mit Zustandsmaschine werden die vom HF-Interface gewonnenen Daten dem IC übergeben, der den Automaten implementiert. Bei einfa-

[1] Der englische Begriff *Near Field Communication* (NFC) stellt eine spezielle Entwicklung und Standard (ISO/IEC 18092 und ISO/IEC 21481) dar, der auf 13,56 MHz-induktiver Kopplung beruht und ist daher nicht mit dem deutschen "Nahfeld" austauschbar [wp Near Field Communication] [Mat 49f].

chen read-only Transpondern bestehen diese Daten nur aus dem Trägersignal zur Energieversorgung, woraufhin der Transponder ununterbrochen seine Seriennummer sendet bis er den Ansprechbereich verlassen hat. Bei komplexeren Transpondern müssen erst ein selected Zustand und ein Sendekommando durch Signale des Lesegeräts ausgelöst werden, bevor ein Transponder beginnt zu senden. Mit diesem Verhalten kann ein Mehrfachzugriffsverfahren auf die Lesegerätfrequenz implementiert werden (vgl. nächster Abschnitt).

Neben diesen Zustandsmaschinen werden für komplexere Aufgaben, die ein Tag bewältigen soll, Varianten mit Mikroprozessor hergestellt. Ein Prozessor dieser Art wird durch ein Betriebssystem, das in einem ROM abgelegt ist, gesteuert (vgl. Java Card).

Beide Transpondertypen – sowohl Zustandsmaschinen als auch Mikroprozessoren – besitzen *read-only*- oder WORM[1]-Speicher, in dem der EPC oder eine andere Identifikationsnummer abgelegt ist. Tags mit benutzeränderbarem Speicher besitzen zudem ein Speicherinterface, über das bei einfachen Tags einige hundert Bit Speicher adressierbar sind. Bei weniger auf kleine und günstige Bauform spezialisierten Tags sind auch Speichergrößen von 8, 32 oder 64 kByte handelsüblich. HP gibt für Prototypen seiner so genannten *Memory Spots* in [ms] an, bis zu 4 Mbit in einem passiven Transponder auf wenigen Quadratmillimetern untergebracht zu haben.

Die Speicherbereiche von Prozessortags, immer mehr aber auch von Zustandsmaschinen mit kryptografischem Koprozessor [Fin 322f], sind durch Passwörter gegen unberechtigtes Auslesen und Überschreiben absicherbar. Häufig wird ein gestaffelter Zugriffsschutz verwendet, so dass Lesen und Schreiben unabhängig voneinander geschützt werden können. So kann beispielsweise ein ÖPNV-Betrieb die bereits bezahlten Fahrten bei Benutzung eines Verkehrsmittels entwerten, während der Fahrgast jederzeit seinen „Kontostand“ mit einem geeigneten Lesegerät auslesen kann. Der Speicher ist häufig so segmentiert, dass unterschiedliche Applikationen unabhängig voneinander geschützt und genutzt werden können. Ein Beispiel für solche Tags im Chipkartenformat stellt die Mifare-Reihe von Philips Semiconductors dar [Fin 331ff].

Als Speichertechnologie stehen verschiedene flüchtige und nicht-flüchtige Bauarten zur Verfügung, die je nach Anforderung, ihren Eigenschaften entsprechend, eingesetzt werden. Dazu gehört im Bereich der flüchtigen Zwischenspeicher etwa SRAM. Für die meisten Anforderungen mit nichtflüchtiger Speicherung, auch nach Energieverlust, werden EEPROMs verwendet, die aber Nachteile im Bezug auf Speichergeschwindigkeit und Energiebedarf während des Schreibens besitzen. FRAM – ferroelektrischer RAM – ist dem EEPROM diesbezüglich weit überlegen und besitzt weitere Vorteile, ist aber in Verbindung mit den anderen Komponenten eines Tags bisher nicht ausreichend kostengünstig für eine Massenproduktion herstellbar gewesen [Fin 12] [Fin 343ff], erlangt aber immer größere Verbreitung [sie].

Neben den weiter oben beschriebenen OFW-Transpondern existieren auch andere Bauarten von Sensoren, wobei dort eine Sensoreinheit an den Mikroprozessor angeschlossen ist, die von diesem genutzt werden kann. Häufig sind Informationen wie die genaue Position oder Lage eines Gegenstandes, der mit einem RFID-Transponder ausgestattet ist, von Interesse, was mit Sensoren und Zusatzfunktionen wie GPS-Positionsbestimmung erreicht werden kann. Das Problem solcher Ansätze ist jedoch zum Teil, dass für den Tag eine eigene Energiequelle notwendig ist, um diese Funktionseinheiten betreiben zu können. Zudem gehen weitere Vorteile, wie die geringe Baugröße und niedrige Kosten, verloren [Fin 348f].

[1] *Write once read multiple (times)*

Die vom **Lesegerät** gewonnenen Daten werden in der Regel über eine serielle Schnittstelle (RS-232 oder USB) von der Applikation bzw. *Middleware* ausgelesen [Fin 362f]. Das verwendete Protokoll zur Datenübertragung über diese Schnittstelle ist herstellerabhängig (ein solches Protokoll wird vom in Abschnitt 5 beschreibenen Lesegerät verwendet), es gibt aber Standardisierungsbemühungen. So hat etwa EPCglobal das *Reader Protocol* [rp] veröffentlicht. Ein Lesegerät kann auch in kompakter, mobiler Bauform mit einem integrierten Rechner in einem handlichen Gehäuse untergebracht sein, so dass es zur manuellen Erfassung von Transpondern vor Ort verwendet werden kann. Neben solchen Handgeräten werden auch Module zum Anschluss an einen PDA oder zum festen Einbau in ein Mobiltelefon vertrieben [Mon]. Lesegeräte, bei denen keine Möglichkeit zum direkten Anschluss an ein Computersystem besteht, können autark konstruiert sein, so dass die Erfassung und Speicherung von Daten direkt am Lesegerät erfolgen kann. Mit einem weiteren Kommunikationskanal wie etwa LAN, WLAN oder GSM ist dann die zeitnahe Weiterleitung an einen Server möglich. [Thi1 106ff]

3.3 Übertragungskontrolle, Sicherungsschicht

Einige RFID-Anwendungen erfordern, dass mehrere RFID-Tags innerhalb des Ansprechbereichs eines Lesegeräts, fehlerfrei annähernd gleichzeitig ausgelesen werden können. Für alle Tags muss sichergestellt sein, dass die übertragenen Daten korrekt sind. Um dies zu erreichen, werden, analog zu Diensten der Sicherungsschicht im OSI-Modell, geeignete Sicherungs- und Mehrfachzugriffsverfahren in RFID-Systeme implementiert. Daneben ist eine immer größere Zahl von Transpondern zur verschlüsselten Kommunikation mit dem Lesegerät in der Lage.

3.3.1 Fehlererkennung

Zur Sicherung der fehlerfreien Datenübertragung werden häufig *cyclic redundancy check* (CRC) Informationen mit den Nutzdaten übertragen. Daneben wird aber auch eine einfache *Paritätsprüfung* oder der *longitudinal redundancy check* (LRC) verwendet, die einfacher durchzuführen, allerdings auch weit weniger zuverlässig in der Fehlererkennung sind [Fin 209ff]. Der CRC-Wert ist bei fest programmierten Seriennummern – etwa dem EPC – im Speicher des Tags zusammen mit diesen Nutzdaten abgelegt [Col 13].

3.3.2 Mehrfachzugriffsverfahren

Einfache Transponder, die fortwährend ihre Seriennummer senden, sobald sie im Ansprechbereich eines Lesegeräts sind, können nur dann ausgelesen werden, wenn kein weiterer Transponder in diesem Bereich befindlich ist. Sobald zwei oder mehr Tags gleichzeitig senden, sind für das Lesegerät keine gültigen Daten mehr erkennbar. Die durch Signalkollision unbrauchbaren Übertragungsdaten werden durch die falschen CRC-Werte als solche erkannt. Bei günstiger Wahl der Bitkodierung ist es sogar möglich, den Fehler auf einzelne Bits einzugrenzen. Diese Eigenschaft, die etwa auf die Manchester-Kodierung zutrifft, machen sich bestimmte Antikollisions- bzw. Mehrfachzugriffsverfahren zu Nutze.

Im Folgenden wird eine Übersicht über die wichtigsten Antikollisionsverfahren geliefert, die in RFID-Systemen eingesetzt werden.

Von allen Mehrfachzugriffsverfahren ist TDMA, also die zeitliche Aufteilung des Übertragungsmediums unter konkurrierenden Sendern, für RFID am weitesten verbreitet. Hierbei kann das Lesegerät die Steuerung der Sendeberechtigung für mehrere Transponder im Ansprechbereich übernehmen. Dieses Verfahren wird *interrogator driven* [Fin 219] oder *interogator/reader-talks-first* (ITF/RTF) [uhfc1g2] [ism1356] genannt.

Daneben gibt es theoretisch auch die Möglichkeit, die Transponder selbständig senden zu lassen (*transponder driven*), was in Reinform durch ALOHA umgesetzt ist. Dieses komplett auf zufälligen Wartezeiten bis zum nächsten Sendeversuch eines Transponders aufbauende Verfahren wird allerdings praktisch nicht angewandt. Stattdessen werden RTF-Varianten verwendet, die in der Bandbreitenausnutzung etwas effizienter sind, wie beispielsweise *slotted ALOHA*. Der Nachteil dieses stochastischen Verfahrens ist, dass keine Garantie für das Erfassen aller erreichbarer Tags innerhalb einer definierten Zeit gegeben werden kann, da es innerhalb jeder beliebigen Zeitspanne immer eine Kollision geben kann [Lam 76f]. Zudem ist die maximale Bandbreitenausnutzung von slotted ALOHA bei vielen gleichzeitig sendebereiten Tags relativ gering und liegt bei 36,8%, beim reinen ALOHA jedoch nur bei 18,4% [Fin 220ff].

Weitere RTF-Verfahren sind etwa *polling*, das *adaptive round data collection protocol* und Baumtraversierung oder *binary search*.

Beim **polling** werden vom Lesegerät nacheinander eine Reihe bekannter Seriennummern abgefragt, bis sich ein Transponder daraufhin meldet. Dazu muss eine begrenzte Zahl möglicher Seriennummern beim Lesegerät bekannt sein, was nur für eine kleine Anzahl Tags sinnvoll ist. Zudem müssen die Nummern im Voraus bekannt sein [Fin 219].

Adaptive round data collection protocol ist eine in [Col] beschriebene Anwendung des STAC (*slotted terminating adaptive collection*) Protokolls. Hierbei wird den Tags vom Lesegerät eine Hashfunktion bereitgestellt. Auf deren Basis und in Verbindung mit seinem eigenen EPC, errechnet jeder Tag als Hashwert die Nummer eines von n Slots, der als Sendezeitraum des Tags verwendet wird. Meldet sich in einem dieser Slots kein Tag kann das Lesegerät den Slot vorzeitig schließen. Eventuelle Kollisionen werden vom Lesegerät erkannt und Zeitverlust durch unnötig übertragene Daten ebenfalls durch ein frühzeitiges Slotende verhindert. Die Wahrscheinlichkeit weiterer Kollisionen derselben Tags wird durch einen Wechsel der Hashfunktion beim Beginn der nächsten Abfragerunde minimiert. Damit ist dieses Verfahren wie ALOHA ein stochastisches RTF Protokoll. Durch ein select-Signal kann eine Gruppe von Tags anhand des EPC so ausgewählt werden, dass beim nächsten Sendezeitpunkt nur Mitglieder der Gruppe antworten, alle anderen Transponder sich dagegen still verhalten. Diese selektive Verringerung der Taganzahl auf für die Anwendung interessante Nummernbereiche wird auch bei der Baumtraversierung angewandt [Col 10ff].

Die **Baumtraversierung** nutzt, wie oben kurz erwähnt, die Fehlererkennungseigenschaften einer Bitkodierung wie etwa der Manchesterkodierung dahingehend aus, dass die Bit genaue Stelle einer Kollision bei mehreren gleichzeitig übertragenen Seriennummern festgestellt werden kann. So kann darauf rückgeschlossen werden, Tags welcher Nummernbereiche gesendet haben. Dadurch, dass der zur Kollision führende Nummernbereich in kleinere Subbereiche unterteilt wird, an welche einzeln Sendeaufforderungen des Lesegeräts verschickt werden, können letztendlich nach Iteration des Verfahrens einzelne Tags isoliert angesprochen werden. Dabei wird von einem geeigneten Wurzelwert eines binären Baums ausgehend iteriert. Solange in einem Wurzelknoten, der eine einzelne Abfrage darstellt, Kollisionen erkannt werden, wird in Subknoten abgestiegen. Dazu wird ein select-Kommando mit der Definition des gewünschten Nummernbereichs an die Transponder geschickt, auf das dann nur noch diejenigen Antworten, die der Definition entsprechen. Knoten, sind unbesetzt, wenn nach einer bestimmten Zeit nach dem select keine Antwort beim Lesegerät eingegangen ist [Fin 226ff] [Col 8ff].

Daneben werden neue Mehrfachzugriffsverfahren, wie etwa *tree slotted ALOHA*, das von Bonuccelli et al in [Bon] vorgestellt wird, diskutiert.

Protokolle mit weniger Wechseln des aktiven Kommunikationspartners werden bei niedrigeren Bandbreiten bevorzugt. Bei HF- oder gar LF-Transpondern wird eher eine ALOHA-Variante präferiert [ism1356 7]. Im UHF-Bereich wird stattdessen eine Lesegerät gesteuerte Baumtraversierungssuche genutzt, die mit vielen Senderwechseln verbunden ist, was bei deren höheren Bandbreiten gut verschmerzt werden kann.

Neben diesen Verfahren zum Auslesen mehrerer Tags durch ein Lesegerät, gibt es Lösungen für Szenarien mit einem Tag im Ansprechbereich mehrerer Lesegeräte zur gleichen Zeit. In diesem Fall kann durch Überlagerungen der HF-Felder der Lesegeräte die Energieversorgung oder Datenübertragung eines Tags teilweise oder komplett gestört sein [Bir 9ff]. Insbesondere durch stärkere Verbreitung mobiler Lesegeräte und flächendeckender Lesegerätinstallation etwa in einem Kaufhaus treten diese Szenarien vermehrt auf. Verschiedene Lösungsansätze sind auch in Standards für die Kommunikation zwischen Lesegerät und Tag eingeflossen. So etwa eine Kombination aus Frequenz- und Zeitmultiplexing in [uhfc1g2] oder eine CSMA-Methode mit Frequenzmultiplexing in [etsi]. Verschiedene Systeme basieren auch auf einer zentral gesteuerten Verteilung der Ressourcen wie Sendezeit oder Frequenz durch eine Serverhierarchie, die mit den Lesegeräten verbunden ist [Bir] [Leo].

3.3.3 Sicherheit

Wenn RFID-Systeme allgegenwärtig eingesetzt werden sollen, ist es unvermeidlich, dass die Tags der Allgemeinheit zugänglich sind. Selbst bei der heutigen Verbreitung von RFID-Systemen ist dies bereits der Fall. Durch diese unvermeidliche Zugänglichkeit von „Jedermann“ zu RFID-Tags, werden diese physikalischen Angriffen ausgesetzt, die das Ziel haben die Tags permanent zu zerstören oder deren Funktion temporär zu stören. Daneben gibt es auch Szenarien, die einen informationstechnischen Angriff auf ein RFID-System illustrieren. Es sind nicht-RFID-spezifische Angriffe auf Datenbanksysteme und Übertragungswege denkbar, die aber an anderer Stelle in der Literatur abgedeckt sind und hier nicht weiter betrachtet

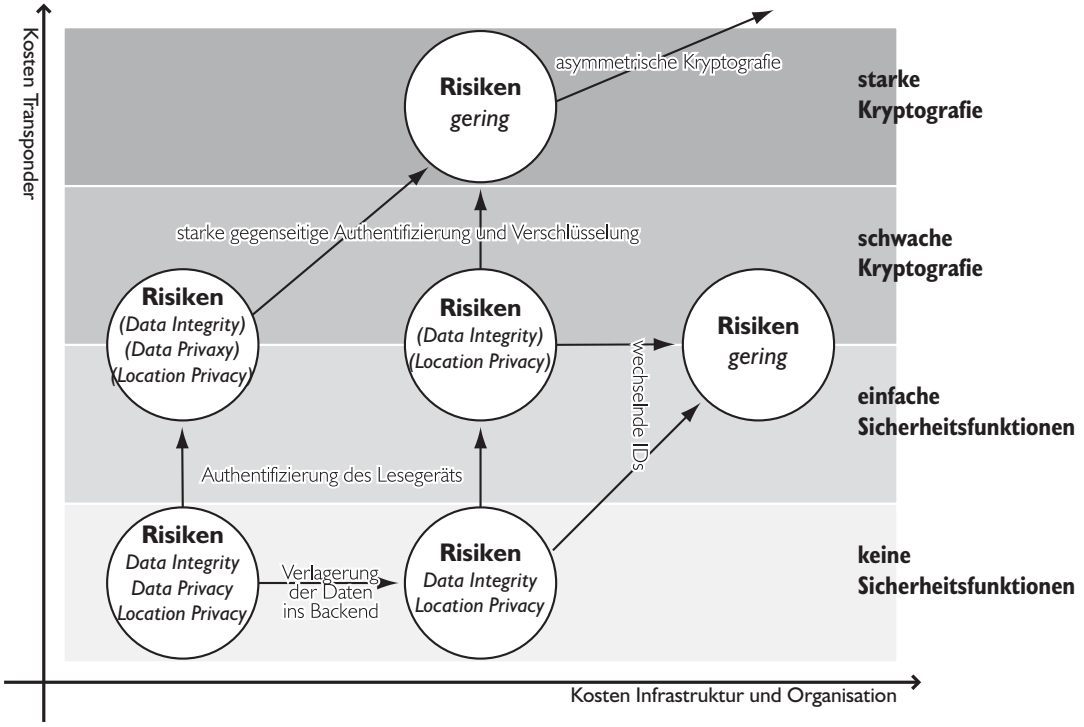

Abbildung 3.1 Kosten-Nutzen-Verhältnis in Bezug auf die Sicherheit aus [Hil]

werden. Vor allem aber stellt die Luftschnittstelle zwischen Tag und Lesegerät eine Schwachstelle unter Sicherheitskriterien dar. Die übertragenen Daten können von jedem Dritten, der in Reichweite des Signals ist, mitgehört oder sogar manipuliert werden.

Konkret lassen sich folgende Arten von Angriffen über die Luftschnittstelle nennen: Abhören des Signals und unbemerktes Auslesen durch manipulativ vergrößerte Lesereichweite, Stören des Signals, Blockieren eines Lesegeräts (DoS) oder eine *relay*- oder *man-in-the-middle*-Attacke. Keine der Angriffsarten lässt sich prinzipiell verhindern, zumindest ist es aber durch kryptographische Maßnahmen möglich, abgehörte Daten für Dritte unbrauchbar zu machen und die Identität des jeweiligen Senders zu verifizieren. Störungen des Signals, die an den physikalischen Grundlagen des Systems angreifen, können ebenfalls nicht verhindert werden, allerdings ist etwa der Betrieb eines Störsenders meist durch die jeweilige Gesetzgebung verboten [Fin 235ff].

Die Voraussetzungen für den Einsatz eines kryptographischen Verfahrens an der Luftschnittstelle des RFID-Systems ist zum einen die Möglichkeit der Energie und Platz sparenden Implementierung auf einem RFID-Chip. Zum anderen ist es für die Akzeptanz durch die Nutzer wichtig, die damit verbundenen Kosten für die Produktion eines Tags niedrig zu halten. Daneben ist noch zu beachten, dass kryptographische Verfahren immer auf Basis eines Geheimnisses arbeiten. Somit ist eine Infrastruktur zur sicheren Verteilung dieses Geheimnisses an die autorisierten Beteiligten notwendig. Nur so ist sichergestellt, dass alle betreffenden Lesegeräte immer aktuelle Schlüsselwerte besitzen. Insbesondere asymmetrische Verschlüsselungsverfahren wie RSA sind durch ihren hohen Rechenaufwand für einfache und kostengünstige RFID-Tags ungeeignet. Das *elliptic curve cryptosystem* (ECC), das aufgrund vergleichsweise geringerer Anforderungen an Speicher- und Rechenleistung auch in Smartcards eingesetzt wird, mindert diese Problematik etwas. Symmetrische Systeme eigenen sich aufgrund der einfacheren Implementierung besser für kostengünstige Systeme. Um ausreichend Sicherheit vor der mit der Verbreitung der Tags eines Systems steigenden Wahrscheinlichkeit der Aufdeckung des Schlüssels bieten zu können, muss jeder Tag einen eigenen Schlüssel besitzen, der in Abhängigkeit von der Seriennummer des Tags vom Lesegerät zugeordnet werden kann. Insbesondere hier ist die Infrastruktur zur Verbreitung neuer autorisierter Tags an die zugehörigen Lesegeräte von organisatorischer, sicherheitskritischer und finanzieller Bedeutung [Fin 252ff].

In [Rie] wird deutlich gemacht, dass nicht nur die Luftschnittstelle der RFID-Systeme Angriffsfläche für Attacken bieten, sondern dass auch bei den dahinter liegenden Verarbeitungseinheiten auf bedachten Umgang mit den gewonnenen Daten geachtet werden muss. Gerade auf der Verbindungsebene zwischen Tag und Lesegerät nicht gesicherte Übertragungen, müssen, vergleichbar mit der *best practice* im Segment Internetapplikationen, zunächst immer als möglicherweise manipuliert und damit „böse“ behandelt werden. Auch wenn der beschriebene RFID-Virus auf eine Situation im Backend angewiesen ist, die allgemein als Softwarefehler anerkannt ist, ist die zentrale Aussage des Textes von Rieback, et al. dass auch im RFID-Bereich bekannte Fehlerquellen nicht vernachlässigt behandelt werden dürfen, um das Gesamtsystem nicht zu gefährden.

3.4 Software: Applikationen und Middleware

Hand in Hand mit dem Einsatz von RFID geht die Konzeption des so genannten *Backends*, also der Infrastruktur, die die mit Hilfe von RFID gewonnenen Daten nutzt. Dabei ist, wie am Ende des vorigen Abschnitts klar wurde, auch die konsequente Fortsetzung von Sicherungsmaßnahmen gegen Angriffe auf diese Daten von ent-

scheidender Bedeutung. Zusammen genommen stellt die Backend-Infrastruktur in Verbindung mit RFID, die Mittel zur Verfügung UbiComp zu realisieren. Somit schließt sich mit diesem Absatz der Kreis, der seit der Darstellung des UbiComp gespannt wurde. Unter Berücksichtigung der diskutierten technischen Merkmale von RFID-Systemen muss dieses Backend implementiert werden.

Um die technischen Besonderheiten von RFID-Systemen von höher abstrahierten Applikationen zu entkoppeln und die Anwendung von der Obligation zu befreien sich selbst um die Ansteuerung des Lesegeräts und letztendlich des Tags kümmern zu müssen, wird **Middleware** eingesetzt. Die Middleware ist zwischen Betriebssystem und Applikationen einzuordnen und stellt letzteren gängige Funktionen zur Verfügung, die ansonsten von den einzelnen Applikationen redundant implementiert wären. Daneben hebt sie Basisfunktionen auf eine höhere Abstraktionsebene, so dass die Applikation sich nicht mehr mit Interna wiederkehrender Funktionen befassen muss, die viele kleinere oder einige aufwändige Aktionen auf Betriebssystemebene bedeuten können. Im Fall der verteilten Systeme stellt eine Middleware die transparente Verwendung von entfernten Ressourcen so zur Verfügung, dass die Applikation sich beispielsweise um den Verbindungsaufbau und die Verfügbarkeit unter einer bestimmten Adresse nicht kümmern muss.

Bei Middleware für UbiComp-Systeme handelt es sich um eine konsequente Fortsetzung des Konzepts für verteilte Systeme mit der Ergänzung um Aspekte des dynamischen bzw. mobilen Verhaltens von Objekten unter Einbeziehung des Zustandes der Umgebung, die durch diese Objekte geformt wird. Dazu ist eine geeignete Modellierung der physischen Umgebung zur Interpretation durch das UbiComp-System notwendig. Die weiteren Aspekte, wie implizite Benutzerinteraktion, ortsbasierte Dienste, geeignete Kommunikationswege zwischen den Objekten, Energieverwaltung und Integration, sowohl in die reale Welt als auch in bestehende Softwaresysteme, ergeben sich aus der Definition eines UbiComp-Systems oder sind technische Voraussetzung dafür [Sch].

In der von EPCglobal vorgesehenen Architektur für RFID-Systeme sind drei Ebenen zu unterscheiden: Bereits in den vorangegangenen Abschnitten wurde die Kommunikation zwischen Tag und Lesegerät thematisiert, welches die lokale Ebene der Architektur darstellt. Die zur unmittelbaren Weiterverarbeitung und auch zum Transport der Daten in eine Applikation oder Übertragung über eine Verbindung, wie etwa ein beliebiges Netzwerk an einen oder mehrere Server, notwendige lokale oder verteilte Middleware stellt die zweite Ebene dar. Die dritte ist die globale Struktur – namentlich die EPCglobal Core Services – insbesondere EPCIS, verteilter Informationsquellen im Internet, über die umfassende Daten zu den Einzelobjekten, mit anderen Worten den Tags, abrufbar sein sollen.

Neben dem im Abschnitt 2.3.3 bereits vorgestellten Diensten ONS und EPCIS von EPCglobal, verdienen insbesondere die Schnittstellen zwischen den verschiedenen Ebenen der Datenverarbeitung Beachtung. Standards für diese Schnittstellen wurden ebenfalls vom Auto-ID Center bzw. den Auto-ID Labs und EPCglobal vorgestellt. Durch die Beschränkung auf Schnittstellenprotokolle wird der Implementierung der einzelnen Systeme maximaler Freiraum gegeben. Bei der Betrachtung dieser Konzepte sind vor allem das Reader Protocol und die Application Level Events (ALE) von Interesse. Während das Reader Protocol die Datenübertragung von und zum Lesegerät bestimmt, beschreibt der ALE-Standard die Kommunikation zwischen verschiedenen Applikationen und Datenquellen. Die beiden Schnittstellen sind erklärterweise so konzipiert, dass nicht exklusiv RFID als Identifikationsverfahren dienen kann, sondern auch andere Systeme wie etwa Barcodes verwendbar sind und kombiniert werden können.

Der Standard zur Definition des Datenaustausches zwischen Lesegerät und der dahinter stehenden Software ist das **Reader Protocol** [rp], aufgrund des Gegenstandes der Definition auch als *Reader Interface Protocol* zitiert. Es soll für das Softwaresystem die Schnittstelle definieren, die nötig ist, um die Basiskonfiguration des Lesegeräts vornehmen zu können, ebenso wie das Lesen, Schreiben, Sperren und Zerstören von Tags [arch 36].

Der Standard ist in drei Ebenen organisiert: *Reader*, *Message* und *Transport Layer*. Der *Reader Layer* bietet Kommando- und Benachrichtigungsdefinitionen, die die eigentliche Kommunikation zwischen Lesegerät und Software darstellen. Dagegen werden im *Message* und *Transport Layer* Formate und Protokolle zur Kommunikation der Daten und Anweisungen aus dem Reader Layer beschreiben. Somit kann ein Datenaustausch von der Softwareapplikation mit unmittelbarer Verbindung zum Lesegerät zu anderen lokalen oder über das Netzwerk erreichbaren Anwendungen etabliert werden.

Message und Transport Layer treten immer in aufeinander angepassten Paaren auf und stellen Format und die Art der Paketisierung, sowie das eigentliche Transportprotokoll zusammen. Ein solches Definitionspaar nennt sich *Message/Transport Binding* (MTB). Beispiele für Transportprotokolle in diesem Sinne sind etwa TCP/IP, Bluetooth oder eine serielle Verbindung. Je nach Anwendung und Protokoll kann durch das MTB auch der Reader Layer beeinflusst werden, um etwa den Verbindungsaufbau zum Lesegerät zu initialisieren. Hauptaugenmerk des Standards liegt aber auf dem Datenaustausch zwischen Lesegerät und Software.

Für die Verbindung zwischen Lesegerät und Software sind zwei Kanäle vorgesehen, ein *Control* und ein *Notification Channel*. Der *Control Channel* transportiert Befehle von der Software zum Lesegerät und gemäß dem *request/response*-Schema auch die Antworten zurück zur Software. Der *Notification Channel* ist für Nachrichten vorgesehen, die die umgekehrte Initialisationsrichtung besitzen. Hier werden asynchrone Nachrichten des Lesegeräts an die Software gemeldet, um etwa das Eintreten eines Tags in den Lesebereich zu melden, ohne dass von Softwareseite eine regelmäßige Abfrage des Status (*polling*) nötig wäre.

Weder Lesegerät noch Software ist auf jeweils einen der Kanäle beschränkt. Ebenso wenig ist notwendigerweise der softwareseitige Endpunkt der beiden Kanäle bei einer 1:1-Verbindung dieselbe Applikation oder gar derselbe Rechner. So kann eine *Control Channel*-Nachricht von Rechner A im Netzwerk abgesandt werden, während Rechner B vom selben Lesegerät *Notification Channel*-Informationen bekommt. Daneben kann es auf einem Rechner A noch eine Applikation geben, die mit beiden Kanalarten wiederum zum selben Lesegerät verbunden ist. Die genaue Spezifikation, welche Konfiguration möglich bzw. notwendig ist, wird von einem MTB geleistet. So lassen sich verteilte Systeme zur Verarbeitung der gewonnenen Daten implementieren.

Eine weitere Softwarekomponente, die der Filterung und Sammlung von Tag-Informationen dient, steht zwischen der Lesegeräteschicht, die die Aufbereitung der Rohdaten erledigt und den Applikationen, die die gewonnenen Daten semantisch auswerten. Die standardisierte Schnittstelle für diese Komponente wird in der EPCglobal-Architektur **Application Level Events** (ALE) genannt. Diese Schnittstelle stellt die Mittel zur Verfügung, n Applikationen den Zugriff auf m Datenquellen für EPC-Informationen zu ermöglichen, wobei m und n beliebig sein

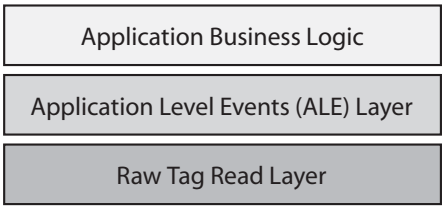

Abbildung 3.2
Einordnung von ALE und dem *Reader Protocol* aus [ale]

sollen. Daneben wird die Sicht der Applikationen von der physischen Struktur der Lesegeräte zu logischen Datenquellen abstrahiert. Die Funktionen, gewonnene Daten zu strukturieren, zu filtern und zu analysieren werden ebenfalls von ALE vorgegeben. Zugriff auf die Daten kann wahlweise synchron nach Bedarf erfolgen oder asynchron bei Auftreten eines Ereignisses, etwa dem Erscheinen eines Tags in einer logischen Datenquelle. Konkurrierende Zugriffe auf Lesegeräte werden durch den implementierenden Dienst transparent koordiniert. Anfragen und Daten erhalten eine standardisierte Repräsentation [arch 39f].

Ziel der Verarbeitung durch diese Softwareschicht ist, der Applikation höheren Abstraktionsgrades kompakt aufbereitete und nach Interesse für die Applikation gefilterte Daten zur Verfügung zu stellen, um die ansonsten großen zu erwartenden Datenmengen effizient handhabbar zu machen und die Flexibilität der Applikation sicherzustellen. Dazu werden aus erhaltenen Daten Ereignisse (Events) generiert. Die Verarbeitung erfolgt typischerweise in den drei Schritten: Daten empfangen, zusammentragen, filtern und strukturieren, sowie Darstellungen der Daten aufbereiten. Die vom Auto-ID Center entwickelte Referenzimplementierung einer Middleware namens *Savant*, ist der Vorläufer dieser Schnittstellendefinition. Savant selbst wurde von EPCglobal nicht weiterverfolgt.

Zufällige Tag-Leseereignisse oder Informationen die für eine Applikation interessant sind, führen bei anderen Applikationen zu einem „Hintergrundrauschen“ an Daten. Als Mittel zur Unterscheidung zwischen relevanten Daten und Rauschen können von den Applikationen in der ALE-Middleware Filter definiert werden. So ist es möglich, nur EPCs, die einem bestimmten Muster folgen, an die Applikation weiterzuleiten und das mehrfache Erfassen eines einzigen Tags in kurzer Zeit zu einem Ereignis zusammen zu fassen. Die Applikation selbst erhält nur gewünschte Informationen und kann sich auf deren Interpretation konzentrieren [ale 6f] [Flö 94].

Es hat sich gezeigt, dass der Begriff Middleware weiter unterteilt werden muss, um den Aufgaben eines Systems gerecht zu werden, das unternehmensweit oder wie in den UbiComp-Visionen weltweit agieren können soll. Bei entsprechend großer Skalierung sind tausende oder Millionen von Erfassungsereignissen pro Sekunde denkbar. Um einer solchen Datenflut Herr zu werden, ist es nötig auf jeder Abstraktionsebene geeignete Filtermöglichkeiten anzubieten, um überflüssige Daten erkennen und verwerfen zu können. Das von EPCglobal verfolgte Konzept sieht dazu drei Ebenen vor: Die Hardwarenahe Lesegeräteschicht, die die direkte Ansteuerung der einzelnen Geräte übernimmt. Hier wurde exemplarisch das Reader Protocol vorgestellt. Die zweite Schicht stellt die für Verteilung, inhaltliche Filterung und Aggregation zuständige Implementierung der ALE dar. Schließlich wird die endgültige Interpretation der Daten beispielsweise von der Unternehmenssoftware bzw. weltweiten Diensten wie EPCIS erledigt.

4 Einsatz in der Praxis

4.1 Standards

Um die weitere Verbreitung von RFID-Technologie zu unterstützen und die Kompatibilität der Hardware verschiedener Hersteller zu ermöglichen, wurden verschiedene Standards erstellt. Als erster ISO-Standard in diesem Bereich wurde 1991 ISO 10374 zur funkgestützten Identifikation von Frachtcontainern veröffentlicht. Diesem folgen bis heute weitere. Daneben wurden durch VDI 4470 Richtlinien für die Abnahme und Prüfung von Warensicherungssystemen (1-bit Transponder) gegeben. Von UCC und EAN wurde die GTAG Initiative ins Leben gerufen, die eine einfache Umsetzung des Prinzips der Barcodenummerierung in RFID-Tags anstrebt. Einige weitere Gremien wie das European Telecommunications Standards Institute (ETSI) haben ebenfalls Spezifikationen veröffentlicht [Fin 451ff]. Schließlich wurde und wird von EPCglobal eine in sich geschlossene RFID-Architektur entwickelt (vgl. Grafik in Abschnitt 2.3.3) [Fin 259ff].

Nachdem die wichtigsten Konzepte der EPCglobal-Architektur bereits angesprochen wurden, soll an dieser Stelle nur noch auf die Übersicht aller vom Auto-ID Center und von EPCglobal entwickelten Standards verwiesen werden, die im Anhang zu finden ist. Dort sind auch einige ISO-Standards aufgeführt, die sich thematisch mit RFID beschäftigen. Dieser Abschnitt gibt im Weiteren einen groben Überblick über jene ISO-Standards. Diese können grob eingeteilt werden in: Tagdaten-Definitionen, Luftschnittstellenbeschreibungen, Software- und Applikationsspezifikationen sowie „Meta-Standards“.

Die Tagdaten-Definitionen wie beispielsweise ISO/IEC 15459 enthalten Vereinbarungen von Nummernschemata und weiterer Speicherinhalte, die für die Funktion eines Auto-ID-Systems unverzichtbar sind. Es ist notwendig, dass solche Nummern so geartet sind, dass weltweit keine Dopplungen auftreten. Nur so ist die eindeutige Identifikation sichergestellt. Es werden auch Schemata für spezielle Nummernbereiche und Zusatzinformationen zur Speicherung im Tag definiert, wie etwa für Gaszylinder in ISO 21007.

Luftschnittstellenbeschreibungen geben physikalische und informationstechnische Betriebsparameter vor. Dazu zählen das zu nutzende Frequenzband sowie Signalstärken, Prüfsummen, Antikollisionsmethoden und das Datenübertragungsprotokoll zwischen Lesegerät und Tag. Wichtige Beispiele sind die Teile 2 bis 7 von ISO/IEC 18000, die für die Güter- und Warenwirtschaft (*item management*) entwickelt wurden.

Software- und Applikationsspezifikationen sind in Form von Interfacebeschreibungen (ISO/IEC 15961) und Datenmodellen (ISO/NP 28560) für verschiedene Anforderungen gegeben oder in der Entwicklung.

Unter dem Begriff „Meta-Standards“ können solche subsumiert werden, die sich mit übergeordneten Fragen beschäftigen, zu welchen Tests und Prüfrichtlinien (ISO/IEC 18046 und ISO/IEC 18047, ISO/IEC 10373), Referenzarchitekturen (ISO/IEC 18000-1), Architekturbeschreibungen für Spezialanwendungen wie das *real-time locating system* (RTLS) (ISO/IEC 24730-2) oder ein RFID-Vokabular (ISO/IEC 19762-3) zählen.

Neben Standards für die Güter- und Warenwirtschaft existieren auch stärker spezialisierte zum Beispiel für die Tieridentifikation (ISO 11784 und 11785) und solche Standards, die für einzelne Anwendungen sowohl logische als auch physikalische Parameter definieren, wie etwa die Spezifikationen für kontaktlose Chipkarten (ISO/IEC 10536, ISO/IEC 14443, ISO/IEC 15693). Gerade neu entwickelt werden Spezifikationen für supply chain Anwendungen (ISO/FDIS 17364, ISO/FDIS 17365, ISO/PRF 17366, ISO/PRF 17367). [iso] [Fin]

4.2 Praxisberichte aus der Literatur

Neben den Standardisierungsbemühungen, fördern die Anwendung von funkgestützter Auto-ID auch einige größere Pilotprojekte zu RFID in der Lieferkette (*supply chain*) und anderen Einsatzbereichen.

Dabei sind eine Reihe verschiedener Bauformen für die unterschiedlichsten Anwendungen entstanden. Dadurch, dass sowohl Energie- als auch Datenübertragung kontaktlos erfolgt, kann der RFID-Chip komplett vergossen oder in ein Kunststoff- oder Glasgehäuse eingebracht werden. Die so geschützte Elektronik kann auch in widrigen Umständen überdauern und sogar in Tiere und Menschen implantiert werden.

Daneben sind noch Chipkarten und Uhren zur einfachen Handhabung für die Personenauthentifizierung erhältlich. So genannte *smart labels* sind Transponder und Antenne in flacher Bauform auf einem Träger aus Folie oder Papier mit Klebefläche zum Aufbringen auf beliebigen Objekten. Objekte und Umgebungen die ganz oder teilweise aus Metallen oder Flüssigkeiten bestehen, stellen physikalisch eine Herausforderung für die Luftschnittstelle solcher Labels dar, jedoch sind auch spezielle Transponder mit Abschirmung erhältlich [Fin 14ff]. Daneben gibt es *coil-on-chip* Transponder, bei welchen die Antenne direkt mit dem Chip gefertigt wird. Diese Transponder sind bei einer Größe von nur einigen Millimetern inklusive Antenne bedeutend kleiner als die mehrere Zentimeter umfassenden *smart label*-Antennen, besitzen dadurch aber in Folge der geringeren Energieausbeute dementsprechend weniger Reichweite.

Einige Anwendungen und Pilotprojekte, die mit RFID-Technologie arbeiten, werden in Fleisch und Mattern (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis* (Springer 2005) sowie [Fin] ausführlich beschrieben. Neben Systemen zur Personenidentifikation für die Zugangkontrolle oder im ePass, sind Chip basierte Zahlungsverfahren, wie sie bereits durch electronic cash-, Kredit- und Geldkarte bekannt sind, ein mögliches Einsatzgebiet für RFID. Weiters werden Identifikationsszenarien beschrieben, die sich auf Supply Chains in Einzelhandel, Pharmaindustrie und Automobilindustrie beziehen. Der Verkauf von Artikeln an Endkunden im Supermarkt ist eine weitere Anwendung von RFID-gelabelten Gegenständen. Das Kassenförderband wird überflüssig, wenn alle Artikel direkt im Einkaufswagen erkannt und verbucht werden können. Auch die automatische Erfassung von Objektbewegungen im Logistikbereich ist für RFID-Systeme ein Paradebeispiel. Daneben ist die Nutzung von RFID für Inventarverwaltungssysteme zum Beispiel für das Werkzeugmanagement oder in einer Bibliothek interessant.

Da das Anforderungsprofil des Inventarsystems der vorliegenden Arbeit dem einer Bücherei ähnlich ist, hier ein kurzer Abriss von Thiesse [Thi2]: Eine steigende Anzahl Bibliotheken setzt RFID ein, um wiederkehrende Handgriffe des Personals zu vermeiden und die Dienstleistungsqualität zu steigern, während Kosten gesenkt werden können. Zu diesem Zweck muss jedes Buch mit einem RFID-Tag versehen sein, durch das ein schnelles Auffinden des zugehörigen Datensatzes für Ausleihe oder Rückgabe möglich ist. Daneben ist eine problemlose Inventur möglich, weil nicht jedes Buch aus dem Regal genommen werden muss, um z. B. von einem Barcodeleser erfasst werden zu können. Zudem bieten die verwendeten Tags wiederbeschreibbaren Speicher, so dass Informationen direkt am Objekt dezentral verfügbar sind. In Kombination mit EAS-Systemen (Diebstahlsicherung), die im Chip integriert sind, wird eine Selbstbedienungsausleihe und -rückgabe machbar. Neben weiteren Vorteilen für die Supply Chains im Buchhandel, ist der vergleichsweise hohe Anschaffungspreis der einzelnen Tags dadurch aufzufangen, dass eine stufenweise Einführung möglich ist, so dass bspw. Barcodes und Tags in einer Übergangsphase gleichzeitig verwendet werden können. Dass die Ansteuerung der entsprechenden Hardware durch Middleware transparent gestaltet werden kann, wurde bereits in Abschnitt 3.4 erwähnt.

5 Beispielimplementierung

5.1 Ziele

Für große Unternehmenssysteme, die die Verwaltung von Supply Chains, von Lagerbeständen und Transaktionen im Einzelhandel oder der Logistik übernehmen, existieren aufgrund der finanziellen Unterstützung durch die interessierten Firmen viele Pilotprojekte und bereits einige produktive Anwendungen. Durch die ständig sinkenden Preise für RFID-Tags werden jedoch auch Anwendungen im privaten Bereich und für kleine Unternehmen und Vereine erschwinglich. In diesem Abschnitt soll untersucht werden, wie eine minimalistische Referenzimplementierung für ein Inventarsystem aussehen könnte. Dazu soll eine Art Middleware in Form einer Treiberimplementierung für ein RFID-System erstellt werden. Diese soll als *Plugin* für ein bestehendes Inventarsystem dienen können. Im Rahmen dieser Arbeit soll als ein solches Inventarsystem ISIS (*Integrated an Simple Inventory and Lending Management System*) dienen, das als Praktikum für die Volkssternwarte Laupheim e.V. entstanden ist [isis].

Das System soll so konzipiert sein, dass einzelne, auf einem feststehenden Lesegerät platzierte Gegenstände, die mit einem RFID-Tag versehen sind, durch einen angeschlossenen Rechner erkannt werden können. Die Information soll an eine einzelne Applikation weitergeleitet werden, die auf Basis der gewonnen Information eine Aktion starten kann. Im konkreten Fall des ISIS-Systems soll es der Applikation möglich sein, eine erfasste RFID-Seriennummer einem Datensatz zuordnen zu können, so dass bei erneutem Erscheinen des Tags im Lesebereich der Datensatz geöffnet werden kann. So können auch weitere Aktionen unter diesem Kontext durchgeführt werden, wie beispielsweise die Ausleihe des Objekts.

Auch wenn für den angestrebten minimalistischen Ansatz eine direkte Umsetzung der EPCglobal-Standards für Softwareschnittstellen ungeeignet ist, da viel der Funktionalität nicht benötigt wird, sollen anwendbare Grundsätze der Middlewareentwicklung beachtet werden. Insbesondere sind dies:

Die Platzierung eines Objektes im Bereich des Lesegeräts kann als ortsbezogene Benutzerinteraktion aufgefasst werden, durch die implizite Aktionen ausgelöst werden sollen. Damit kann dem Benutzer eine explizite Anweisung zum Auslesen des Tags und teilweise nachfolgende Befehlseingaben abgenommen werden. Daraus folgt auch die Entscheidung für ein asynchrones Verhalten bei Auftreten eines Ereignisses. Alle vom Lesegerät erzeugten Eingaben werden nach Schema des *Listener-Event*-Prinzips, das aus Java bekannt ist, weitergereicht.

Im Zuge der Umsetzung des Plugins soll eine Trennung von Hardwareansteuerung und weiterverarbeitender Software verwirklicht werden. Dadurch soll insbesondere die eingesetzte Technologie zur Identifizierung austauschbar sein. So soll es möglich werden, verschiedene RFID-Lesegeräte oder auch Barcodescanner als Eingabegerät zu verwenden, ohne dass die stärker abstrahierende Interpretationsschicht in ihrer Funktion davon beeinflusst wird oder umgeschrieben werden muss.

Für das kleine betrachtete System ist eine zentrale Architektur die effizienteste Lösung, allerdings kann der Pluginansatz leicht dahingehend erweitert werden, dass mehrere Lesegeräte gleichzeitig an einem System betrieben werden können. Die Verbindung zwischen Datenbank und Tag wird durch die Seriennummer hergestellt. Diese wird zu jedem Datensatz abgelegt um die Zuordnung zu ermöglichen.

5.2 Anforderungen und Architektur

Der Aufbau der hier beschriebenen Testimplementierung orientiert sich am Zusammenspiel der beiden Komponenten Reader Protocol und ALE der Middleware-Architektur, das von EPCglobal vorgeschlagen wird. Während allerdings die Spezifikationen dieser beiden Standards sehr umfangreich ist und die Nutzung vergleichbarer ISO-Standards (ISO/IEC 15961, ISO/IEC 15962) mit zusätzlichen Kosten verbunden sind [iso], zeichnet sich die hier vorgestellt Referenzimplementierung durch ihre Einfachheit aus. Dieser soll allerdings nicht die flexible Erweiterbarkeit des Systems zum Opfer fallen. Die einfache Struktur der Implementierung ermöglicht es, auch mit einem kleinen Budget ein produktives System daraus aufzubauen. Für einfache Portierbarkeit wird hier als Realisierungssprache Java verwendet.

Die Kommunikationsebenen zwischen Tag und Applikation sind vom Tag ausgehend eingeteilt in:

- Luftschnittstelle zwischen Tag und Lesegerät
- Serielle Schnittstelle zur Kommunikation des Lesegeräts mit dem Rechner und umgekehrt
- Javaschnittstelle für die serielle Verbindung
- Verwaltung der logischen Verbindung
- Treiberebene, die Java-Methoden in Lesegerät-Befehle und Lesegerät-Antworten in Information kapselnde Event-Objekte übersetzt
- Filterebene mit Applikationsschnittstelle

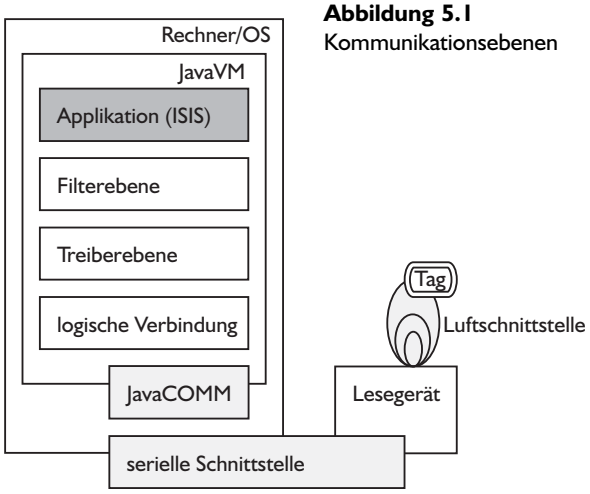

Abbildung 5.1
Kommunikationsebenen

Sowohl die Tag-Lesegerät-Verbindung als auch die serielle Schnittstelle sind durch die verwendete Hardware vorgegeben und stellen hier zunächst keinen Diskussionsgegenstand dar. Als Schnittstelle zwischen den Betriebssystemfunktionen für den seriellen Port und der Java-Virtual-Machine dient die Referenzimplementierung *SerialComm* von Sun, deren Windows-Version zwar nicht mehr weiterentwickelt wird, welche aber funktional ist. Versionen für Linux und Solaris und eine generische Implementierung werden weiterhin von Sun unterstützt [jaco].

Die Verbindungsverwaltung für die virtuelle serielle Schnittstelle wird von einer modifizierten Beispielimplementierung von Sun übernommen [seco]. Von dieser werden Eingangs- und Ausgangsdatenpuffer überwacht. Eingehende Daten werden an genau einen *ConnectionEventListener* weitergegeben und in der Treiberebene wiederum in *ReaderEvents* gekapselt. Ebenso ist vorgesehen, dass genau ein Objekt Kommandos für das Lesegerät an die Schnittstelle äußert. Der notwendige exklusive Besitz einer seriellen Schnittstelle ist der Grund für die 1:1-Zuordnung von Kommandoobjekt und Listener zwischen der Verbindungsverwaltung und der Treiberebene.

Auf der Treiberebene werden die Rohdaten interpretiert, die über die serielle Schnittstelle (*Strings*) als Kommandos versendet und als Antworten des Lesegeräts empfangen werden. Für das Senden von Kommandos an das Lesegerät existieren Objekt-Methoden, die dann die Lesegerätspezifischen Befehle in den Ausgangpuffer schreiben. In der Kommunikationsrichtung vom Tag zur Applikation wird der vom Eingangspuffer kommende Strom in einzelne Ereignisse gekapselt. Damit kann die Beschränkung auf eine 1:1-Zuordnung aufgehoben werden. Hier können beliebig viele *ReaderEventListener* registriert werden, an die ein auftretendes Ereignis verteilt wird. Damit entspricht die Treiberebene konzeptuell dem *Reader Layer* des Reader Protocol.

Schließlich stellt die Filterebene die Verbindung zwischen der Treiberebene und der Applikation dar. Diese stellt Funktionen zur Verfügung, mit denen eine Gruppierung mehrerer Ereignisse, die durch das Auslesen des immergleichen Tags in schneller Abfolge erzeugt wurden, möglich ist. Die Definition der Phrase „schnelle Abfolge“ geschieht durch einen Parameter zeitlicher Dimension, der der entsprechenden Methode übergeben wird. Die Auslösung des Ereignisses an die Applikation erfolgt beim ersten Auftreten des *ReaderEvents*. Weitere Ereignisse werden gemäß der Filterdefinition abgefangen und ein Zähler im betreffenden Applikations-Event wird inkrementiert. Wenn der Parameter nicht definiert wird, werden alle Ereignisse, die von einem Tag mit derselben Seriennummer ausgelöst werden zu einem zusammengefasst, bis ein anderes Tag erkannt wird. Das Wissen über vergangene Ereignisse wird verworfen, so dass ein erneutes Auftreten des vorigen Tags wieder zu einer Ereignisauslösung führt.

Beim Anspruch ein kostengünstiges System zu erstellen, kann vorausgesetzt werden, dass auch kostengünstige RFID-Hardware verwendet werden soll. Bei diesen Systemen ist im Tag nur eine Seriennummer gespeichert, die zwar ausgelesen, Daten aber nicht auf dem Tag gespeichert werden können. Die Schnittstelle zwischen Applikation und Treiberplugin kann sich also auf eine Methode zur Initialisierung des Lesegeräts mit der Arbeitskonfiguration beschränken. Daneben gibt es noch Methoden zur Registrierung von Listenern um Events weiterleiten zu können. Abgesehen hiervon sind keine Kommandos nötig. Tags, die sich in den Ansprechbereich des Lesegeräts begeben, lösen ausgehend vom Lesegerät eine Ereigniskette aus, die die Applikation mit den Seriennummern versorgt. So kann auf die Benutzerinteraktion „Tag im Lesebereich platziert“ kontextbezogen reagiert werden.

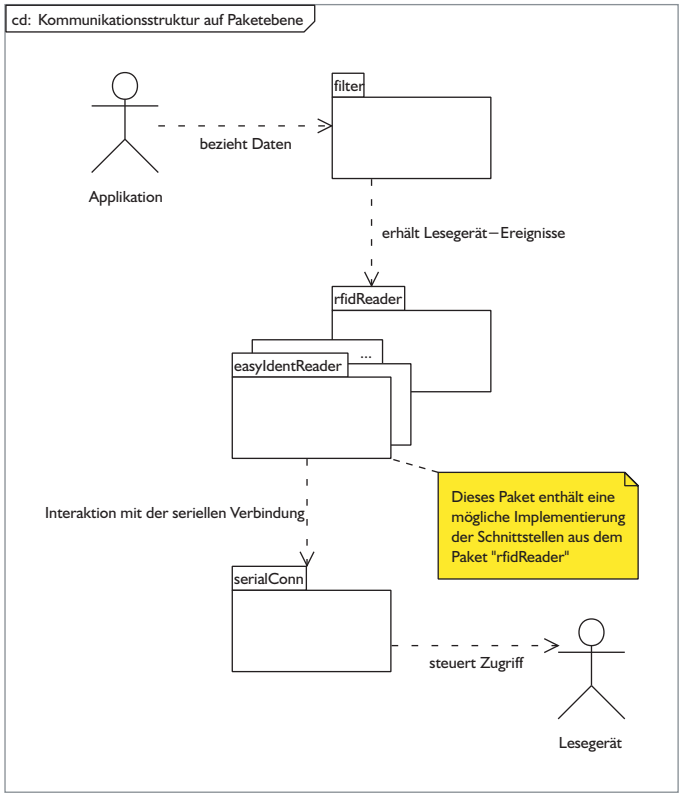

Abbildung 5.2 Paketdiagramm

Wie die Korrektheit der Daten anhand von Checksummen überprüft werden kann, ist hardwareabhängig. Die EM4102-Tags, die für Testzwecke zur Verfügung standen, übertragen eine 64-bit Zahl an das Lesegerät, die neben Header und Stoppbit 14 Paritätsbits zur Fehlererkennung für die 40-bit Seriennummer enthalten. Die Checksummenprüfung wird von der Lesegerätehardware übernommen [eirdr]. Zur Erkennung von Fehlern auf der seriellen Übertragungstrecke zwischen Lesegerät und Rechner – in diesem Fall eine USB-Verbindung – wird die Summe aller Stellen der Seriennummer in Hexadezimaldarstellung errechnet und deren vier LSBs (*least significant bits*) mit übertragen. Diese Sicherungsmaßnamen für die Übertragung sind, wie bereits in Abschnitt 3.3.1 diskutiert, nicht sehr zuverlässig in der Fehlererkennung dafür aber leicht umzusetzen.

Die verwendeten EM4102-Tags arbeiten im Frequenzbereich um 125 kHz und haben eine Reichweite von wenigen Zentimetern bei idealen Übertragungsbedingungen. Sie besitzen kein Antikollisionsverfahren und können daher nur einzeln ausgelesen werden [eitag] [em4102]. Da dies die einzige vorliegende Hardware zu diesem Zweck war, konnte hier leider nicht

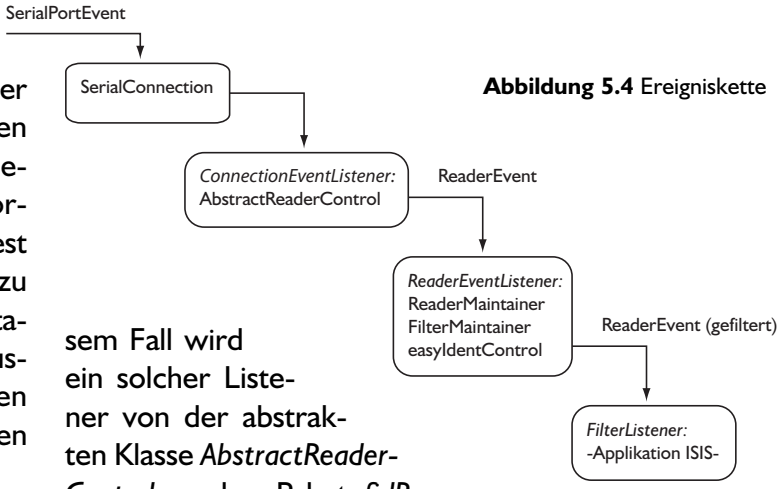

Abbildung 5.4 Ereigniskette

gezeigt werden, wie die Einbeziehung einer Antikollisionsfunktion mit ihren schnellen Ereignisfolgen in die Softwareimplementierung aussehen sollte. Allerdings ist das vorgestellte Ereignis basierte System zumindest prinzipiell in der Lage diese Funktion zu unterstützen, da die notwendige Interpretation der Daten innerhalb des leicht austauschbaren Treiberteils vorgenommen werden kann und geeignete Filterklassen schnell erstellt sind.

5.3 Implementierung

Gemäß der Strukturierung der Architektur wurden die Javapakete *serialConn*, *rfidReader*, *filter* und *easyIdentReader* zur Unterteilung der Klassenstruktur angelegt. *serialConn* entstammt einem Implementierungsbeispiel von Sun und wurde nur leicht modifiziert. Über die enthaltene Klasse *SerialConnection* können *ConnectionEventListener* registriert werden, an die Ereignisse der Verbindung weitergeleitet werden. In diesem Fall wird ein solcher Listener von der abstrakten Klasse *AbstractReaderControl* aus dem Paket *rfidReader* implementiert. Dieser delegiert die Interpretation der Rohdaten von der seriellen Verbindung, die als String vorliegen, an seine konkreten Subklassen mittels der abstrakten Methode *parseReply(String)*, die per Konvention von den Subklassen implementiert werden muss. Die Methode hat als Rückgabewert ein *ReaderEvent*, das dann in der Ereigniskette weitergereicht wird. Wie diese Methode implementiert wird, bleibt dem individuellen Treiber überlassen, der in der Lage sein muss,

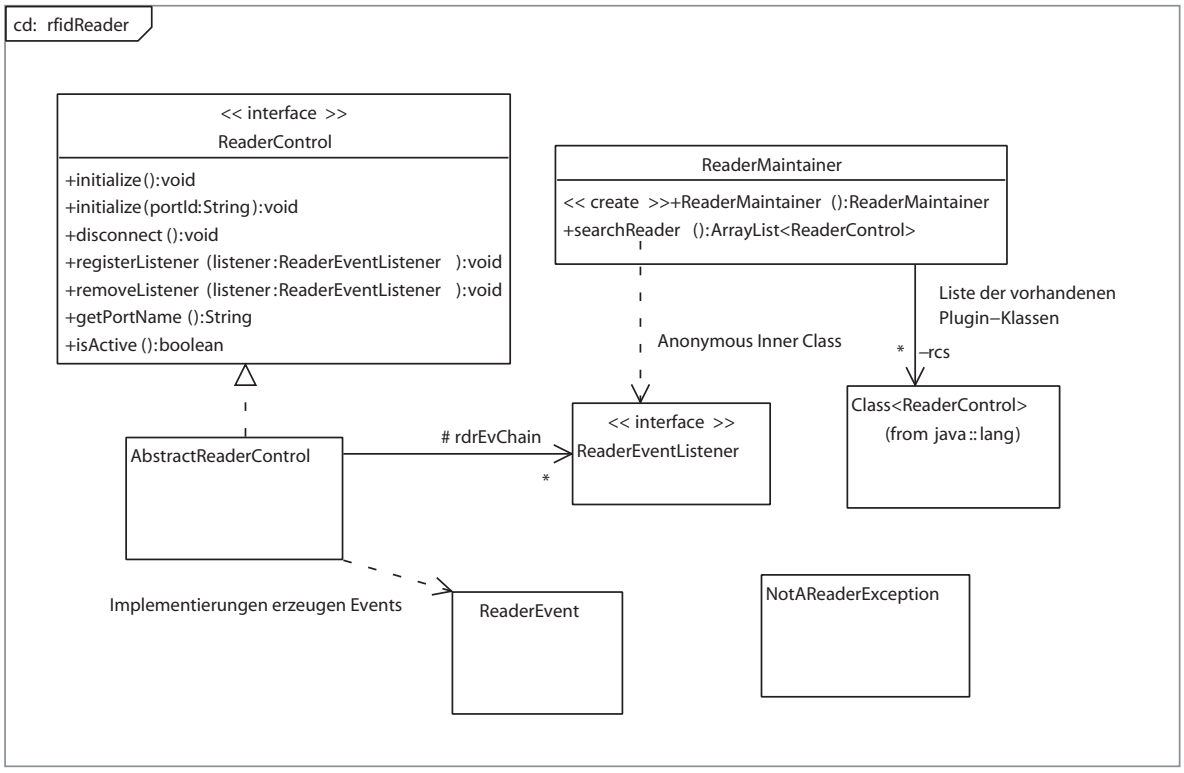

Abbildung 5.3 Klassendiagramm *rfidReader*

Anmerkung Zur Eingabe von Quellcode und zur Erzeugung des Compilats wurde eclipse, das Java Development Kit und die API-Dokumentation von Java und aus [seco] verwendet.

Befehle an das Lesegerät zu formulieren und dessen Antworten zu interpretieren. Zur vorliegenden Hardware von easyIdent [eirdr] wurde im Paket *easyIdentReader* eine passende Erweiterung der *AbstractReaderControl-Klasse* mit Namen *easyIdentControl* erstellt. Diese delegiert die Interpretation der Lesegerätdaten an eine Klasse *ReaderData*, welche die Daten kapselt und eine Methode zur Erzeugung des entsprechenden Events besitzt.

Damit es möglich ist, verschiedene Lesegerättreiber unabhängig zu entwickeln und dann einbinden zu können, existiert im Paket *rfidReader* eine Klasse *ReaderMaintainer*, die in ihrer Methode *searchReaders()* an allen verfügbaren seriellen Ports versucht, eine Verbindung zu einem bekannten Lesegerät herzustellen. Dazu wird für jeden Port *initialize(String port)* in jeder *ReaderControl*-Klasse aufgerufen, die in der Konfigurationsdatei *pluginClasses* angegeben ist. Da alle Antworten des Lesegeräts asynchron eintreffen, kann bereits mit dem nächsten Befehl, bzw. Port fortgefahren werden, während auf die Antwort des Lesegeräts gewartet wird. *ReaderMaintainer* behält solange einen Listener zu einem potentiellen Reader, bis eine definierte Zeit abgelaufen ist. Dann wird der Listener entfernt und angenommen, dass kein bekanntes Lesegerät an diesem Port verfügbar ist, wenn eine bestimmte Antwort innerhalb der Zeit ausbleibt.

Um nicht unnötig Lesegerät-Ereignisse an die top-level Applikation weiterzuleiten, welche keine Verwendung dafür hat, enthält das Paket *filter* eine *FilterMaintainer*-Klasse, an der *FilterListener* registriert werden können. An einen solchen Listener werden nur die *ReaderEvents* weitergeleitet, die eine bestimmte Bedingung erfüllen. Diese Bedingung wird durch eine Klasse geprüft, die das *interface Filter* implementiert. Die Methode *filterEvent(ReaderEvent)* dort liefert einen *boolean*-Wert zurück, der den *FilterMaintainer* entweder veranlasst das Ereignis an den Listener weiterzuleiten oder nicht.

Das *ReaderEvent* selbst, schließlich, das bei der Applikation ankommt, ist vom Typ *ReaderEvent.SNR_RECEIVED* und enthält eine *ArrayList* als Parameterliste. In dieser

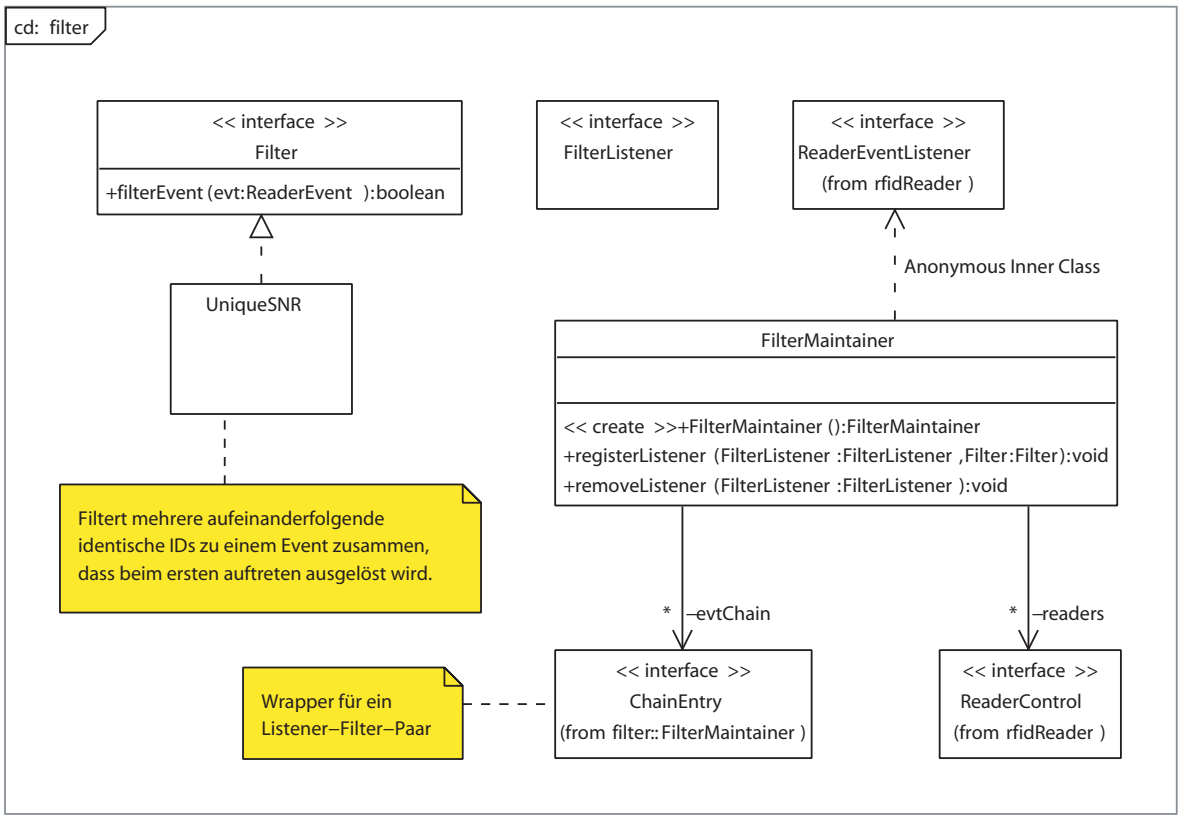

Abbildung 5.5 Klassendiagramm *filter*

Liste steht per Konvention an der Stelle 0 eine *Long*-Repräsentation der Seriennummer, an der Stelle 1 ein *String*, der eine Hexadezimalrepräsentation ebendieser enthält. Es existieren auch andere Eventtypen, die aber ausschließlich in den Verarbeitungsebenen unterhalb der Filterebene Bedeutung haben und daher gegenüber der toplevel Applikation nie in Erscheinung treten.

5.4 Bewertung der Funktionalität

Das vorgestellte System war erfolgreich in der Lage Seriennummern des vorliegenden Tag-Typs EM 4102 einzulesen und diese an [isis] als konkrete top-level-Applikation weiterzuleiten. Entsprechend den Anforderungen, die für diese Applikation definiert sind, werden die erhaltenen Daten weiterverarbeitet.

Der *FilterMaintainer* baut die Verbindung zum seriellen Port über *ReaderControl* automatisch auf und ab, in Abhängigkeit davon, ob momentan mindestens ein Listener registriert ist. Somit vereinfacht sich die Schnittstelle zwischen dem Paket *filter* und der Applikation darauf, Listener in Verbindung mit Filtern zu registrieren und diese zu entfernen. Alle weiteren Funktionen werden von den darunter liegenden Klassen, synchron bei der Listenerregistrierung oder asynchron bei der Ereignisweitergabe, durchgeführt.

Aufgrund der Checksummenprüfung ist es möglich, die meisten Übertragungsfehler schon früh in der Eventkette als solche zu erkennen. Es werden dann Ereignisse erzeugt, die Informationen über die fehlerhafte Übertragung enthalten. Ein passender Filter kann diese Informationen auswerten. Die Beispielimplementierung eines Filters mit Namen *UniqueSNR* hingegen leitet nur erfolgreich gelesene Seriennummern weiter. Über die Methode *setTimeout(int)* kann der Filter konfiguriert werden. Es kann festgelegt werden, ob alle Seriennummern gemeldet werden sollen (*int*-Parameter *0*) oder nur solche, die nicht bereits vor kurzem gelesen wurden. Wenn der Tag einige Zeit auf dem Lesegerät liegt und alle dadurch entstehenden Ereignisse gemeldet werden, wird die Applikation von Ereignissen bombardiert, die nicht von Interesse sind. Der Filter verhindert dies und lässt der Applikation dabei die Flexibilität zu bestimmen, wie entschieden werden soll, wann das Tag absichtlich erneut auf dem Lesegerät platziert wurde. Dazu gibt es folgende Möglichkeiten: Ist das Tag länger als eine bestimmte Zeit (*int*-Parameter in Millisekunden) nicht mehr gelesen worden, wird ein weiteres Auftreten eines Ereignisses weitergeleitet. Wird als Parameter ein beliebiger negativer Wert übergeben, werden folgende gleichartige Ereignisse jeweils solange zurückgehalten, bis eine andere Seriennummer erkannt wird. In jedem Fall wird dem bereits weitergeleiteten Event mitgeteilt, wie oft es wiederholt wurde. Dies kann von der Applikation bei Bedarf ausgewertet werden. Allerdings muss der vorliegende Filter für diese Funktionalität eine Referenz auf das letzte propagierte Ereignis halten und weitere Informationen zwischen dem Auftreten von Ereignissen speichern. In jedem Fall wird das erste Auftreten eines Ereignisses weitergeleitet, nicht das letzte.

Die so vorgestellte Implementierung erfüllt die geforderten Funktionen und ist somit in der Lage eine Applikation auf einfache Weise mit Daten eines RFID-Lesegeräts zu versorgen. Die notwendige Schnittstelle besteht ausschließlich aus der Eventverwaltung des Filterpakets und ist damit auf die kleinste denkbare reduziert. Dennoch ist das zugrunde liegende System aufgrund seiner Plugin-Bauweise leicht erweiterbar und selbst aus der Applikation heraus um Filter zu ergänzen, falls dies notwendig sein sollte. Leider konnten nicht alle beschriebenen Funktionen vollständig unter Produktionsbedingungen getestet werden, was im folgenden Abschnitt erläutert wird.

5.5 Anforderungsanalyse für ein produktives System

In den vorigen Abschnitten wurde an einigen Stellen deutlich, dass die Hardware des vorgestellten Testsystems nicht den Anforderungen an das geplante Inventarsystem entspricht. Im Folgenden soll aufgeführt werden, was am Aufbau des Testsystems unzureichend für einen produktiven Einsatz war und wie diese Mängel behoben werden können. Insbesondere müssen andere RFID-Tags verwendet werden.

Die Auswahl der Hardware hängt davon ab, welchen Zweck die Erfassung von Objekten haben soll. Im vorliegenden Fall soll bei der bewussten Platzierung eines Objektes im Ansprechbereich des Lesegeräts eine Aktion ausgelöst werden, die beispielsweise sein kann: Aufruf und Anzeige von Informationen zum Objekt, eine Ausleihe des betreffenden Objekts oder dessen Rückgabe sowie eine einfache Inventur. Dabei sollen Objekte in der Größe eines Buches durch Tags identifizierbar werden. Zu diesem Zweck sind Smart Labels geeignet, da sie sich problemlos auf vielen Gegenständen anbringen lassen und kostengünstig sind. Um Kontrolle darüber zu haben, welche Gegenstände erfasst werden, darf der Ansprechbereich nicht zu groß sein. Damit auf der anderen Seite nicht die genaue Position des Tags am Objekt bekannt sein muss, sollte die Reichweite allerdings etwas größer als die Ausdehnung des Gegenstandes sein. Für diese Parameter ergibt sich eine Lesereichweite von ca. 30 cm.

Um eine Inventur bequem durchführen zu können, sollte es möglich sein, einmal mit einem Lesegerät an einem Regal vorbeizufahren und dabei alle vorhandenen Gegenstände zu erfassen. Bei der veranschlagten Objektgröße eines Buches ist zu erwarten, dass sich mehrere dutzend Objekte gleichzeitig im Ansprechbereich befinden. Die gängigen Antikollisionsverfahren sind für mehrere hundert bis tausend Leseereignisse pro Sekunde ausgelegt, so dass dieses Szenario problemlos erfüllbar ist.

Beide Anforderungen erfüllt der EM 4102 nicht. Statt dessen eignet sich ein 13,56 MHz Transponder, wie er beispielsweise von EPCglobal [ism1356] oder ISO/IEC 18000-3 spezifiziert wird. Zu dieser Kategorie gehört etwa I.CODE und I.CODE SLI von NXP Semiconductors (Phillips) [nxp1] [nxp2]. I.CODE folgt bei der Luftschnittstelle dem EPCglobal-Standard, I.CODE SLI dagegen verwendet das Smart Card-Schnittstellenprotokoll aus ISO/IEC 15693. Ebendiesem Standard entspricht auch der my-d Chip von Infineon, der in [Thi2] beschrieben und vorhanden ist. Von Texas Instruments wird der Transponder Tag-it HF-I hergestellt, der ISO/IEC 18000-3 entspricht. Diese Aufzählung verfügbarer Transpondertypen ist nicht erschöpfend und stellt nur einen kleinen Ausschnitt aus dem marktverfügbaren Angebot dar.

Die in 5.2 und 5.3 beschriebene Softwarearchitektur und Implementierung ist so konzipiert, dass die benötigte Funktionalität bereitgestellt wird. Ob die Rechenleistung eines Handlesegerätes ausreicht um die Tags schnell genug zu erfassen und so dem Inventurszenario entsprechen zu können, gilt es noch zu prüfen.

Sollen in der Zielumgebung tragbare Lesegeräte eingesetzt werden, ist deren Integration von der Darstellung der Daten durch das entsprechende Lesegerät entscheidend: Ist das Lesegerät direkt beispielsweise über WLAN mit dem System verbunden und nimmt eine Live-Übertragung der gewonnenen Daten vor, ist eine Middleware mit größerem Funktionsumfang und Implementierungsaufwand nötig um diese Daten entgegenzunehmen und auszuwerten. Werden die Daten im Lesegerät offline gesammelt, ist eine Übertragung der Daten in die Applikation vom verwendeten Datenformat abhängig. Handelt es sich um Daten von einer seriellen Schnittstelle, kann ein Treiberplugin in hier vorgestellter Manier erstellt werden, das das Verhalten eines normalen Lesegeräts simuliert und die einzelnen erfassten Seriennummern jeweils als Event an die Applikation schickt.

6 Die soziotechnische Gesellschaft

Was der Einsatz von RFID für das tägliche Leben bedeutet ist augenscheinlich denkbar einfach beschrieben: Durch Computersysteme, die die Fähigkeit erhalten, ein akkurates und aktuelles Modell der Umwelt vorliegen zu haben, wird der Mensch von lästigen Routineaufgaben befreit. Diese Aufgaben reichen von den hier beschriebenen Inventarverwaltungsarbeiten über Zutrittskontrolle und Kassierertätigkeiten bis hin zur Erinnerung an Termine und Kontextinformationen zur aktuellen Umgebung. Während erstere bereits heute zunehmend umgesetzt werden, befinden sich letztere zum großen Teil noch in der Entwicklung. In jedem Fall jedoch entstehen dynamische Modelle durch die Sensorik von Computern. Durch die erreichte engere Verknüpfung von Modell und Realität rückt der Traum des UbiComp näher: Der Computer wird unsichtbar, die Funktion rückt in den Vordergrund. Dies hat jedoch nicht nur Konsequenzen für die physische Umgebung sondern auch für die soziale und kognitive. Lyytinen und Yoo [Lyy] nennen die entstehenden Systeme „sociotechnical“. Die Einbindung von allgegenwärtigen Computern in unser Leben wirkt sich auf eben dieses aus. Wissen ist schneller verfügbar, Kommunikation und Absprache sind durch ubiquitäre Medien flexibler, aber eventuell auch ein Eingriff in die Privatsphäre. Arbeitsabläufe sind mit Hilfe mobiler Rechenleistung nicht mehr an einen Schreibtisch gebunden. Neue Geschäftsfelder und Marketingmethoden können entstehen. All dies birgt die Gefahr unbeabsichtigter Nebenwirkungen und möglicherweise sogar kontraproduktiver Entwicklungen.

Neben dem Einsatz von RFID und WLAN zur Suche nach vermissten Kindern im Legoland, Dänemark beschreiben Angell und Kietzmann [Ang] auch beunruhigende Szenarien. Während sich die Kinder noch weniger über ihre Selbstbestimmungsrechte Gedanken machen, stellt sich die Frage, ob diese Rechte bei Soldaten immer gewahrt bleiben, die von den US-Streitkräften mit Armbändern ausgestattet werden, die zur Verfolgung von Verwundeten und Gefangenen verwendet werden sollen. Selbst wenn die Verantwortlichen sorgsam mit den Daten umgehen, könnte ein krimineller oder militärischer Angriff auf das System ungeahnte Folgen haben. Daneben stellen Angell und Kietzmann fest, dass es in einer Welt, in der Macht und Recht auf Information fußt, äußerst bedenklich ist, wenn der Grundsatz gelten sollte „Schuldig, bis zum Beweis der Unschuld, durch offen legen aller persönlichen und finanziellen Daten.“

UbiComp-Systeme zeichnen sich dadurch aus, dass sie alle Arten von Daten sammeln um ihre Aufgaben erfüllen zu können. Um sicherzustellen, dass dadurch nicht die informationelle Selbstbestimmung des Menschen verloren geht und dieser zum Objekt wird, müssen Verfahren entwickelt werden, um jedem Menschen Mittel zur Errichtung von Zugriffskontrollen auf seine Daten zu ermöglichen. Bereits Mark Weiser hat dies in [Wei2] erkannt.

Angst und Panik vor RFID zu verbreiten ist aber kein Weg zur Lösung des Problems. Die Vorteile von RFID-unterstützten Systemen haben ein breites Interesse an der Technologie geweckt. Ein ebenso verbreitetes Bewusstsein für die sicherheitskritischen und rechtlichen Implikationen muss dem folgen. Erste Schritte, wie der Verzicht auf das Senden fester Seriennummern beim elektronischen Pass [Fin 402ff] um Tracking zu verhindern sind gemacht. Verschlüsselungsfunktionen halten auch bei low-cost RFID-Tags Einzug.

All dies im Bewusstsein, darf aber nicht vergessen werden, dass UbiComp und RFID neue Technologien sind:

> „Researchers in this field are still 'dreaming' and 'creating problems' as much as they are solving problems and recording and theorizing about effects. Researchers need to find ways to maintain the rigor of scientific research without restraining their ability to imagine. […] Finally, research in ubiquitous computing requires transcending the traditional barriers between social and technical as well as levels of analysis – individual, team and organizational.“ [Lyy]

7 Literatur

[ale] EPCglobal: *The Application Level Events (ALE) Specification, Version 1.0*; 2005. abgerufen am 14.09.2007
http://www.epcglobalinc.org/standards/ale/ale_1_0-standard-20050915.pdf

[Ang] Angell, Ian; Kietzmann, Jan: *RFID and the End of Cash*; 2006. CACM 49,12 90 - 96

[arch] EPCglobal: *The EPCglobal Architecture Framework*; 2005. abgerufen am 14.09.2007
http://www.epcglobalinc.org/standards/architecture/architecture_1_0-standard-20050701.pdf

[Col] Cole, Peter H.: *Physics and Protocols in Radio Frequency Identification*; 2005. abgerufen am 14.09.2007
http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-HARDWARE-013.pdf

[Bir] Birari, Shailesh M.: *Mitigating the Reader Collision Problem in RFID Networks with Mobile Readers*, Master Thesis; 2005. abgerufen am 14.09.2007
http://www.it.iitb.ac.in/~sri/students/shailesh-thesis.pdf

[Bon] Bonuccelli, Maurizio A.; Lonetti, Francesca; Martelli, Francesca: *Tree Slotted Aloha: a New Protocol for Tag Identification in RFID Networks*; in *Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks*; 2006, International Workshop on Wireless Mobile Multimedia. IEEE Computer Society, Washington, DC. 603 - 608.

[Bul] Bullinger, Hans-Jörg; Hompel, Michael ten (Hrsg.): *Internet der Dinge*; 2007, VDI-Buch. Zitiert nach den Ausschnitten abgerufen am 14.09.2007 auf
http://www.internet-der-dinge.de/

[Mon] Monse, Kurt: *RFID und Handy - Hand in Hand*; 2006.
http://www.ecin.de/blog/node/244

[eitag] easyident: *4102 Transponder*, Datenblatt; 2004. abgerufen am 14.09.2007
http://www.easyident.de/PDF%20Files/Transponder%204102.PDF

[eirdr] easyident: *esyident-MU Mutireader mit USB*, Hardware Beschreibung; 2005. abgerufen am 14.09.2007
http://www.easyident.de/PDF%20Files/
FS-0022%20R2%20easyident-MU%20Hardware%20Beschreibung.pdf

[em4102] EM Microelectronic: *EM4102 - Read Only Contactless Identification Device*; 2005, Marin, Schweiz. abgerufen am 14.09.2007
http://www.emmicroelectronic.com/webfiles/Product/RFID/DS/EM4102_DS.pdf

[epcis] EPCglobal: *EPC Information Services (EPCIS) Version 1.0 Specification*; 2007. abgerufen am 14.09.2007
http://www.epcglobalinc.org/standards/epcis/epcis_1_0-standard-20070412.pdf

[etsi] ETSI: *EN 302 208 European Standard V1.2.1, Electromagnetic compatibility and Radio spectrum Matters (ERM); Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W; Part 1: Technical requirements and methods of measurement*; 2007. abgerufen am 14.09.2007
http://www.etsi.org/

[Fle] Fleisch, Elgar; Christ, Oliver; Dierkes, Markus: *Die betriebswirtschaftliche Vision des Internet der Dinge*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 3 - 37

[Flö] Flörkemeier, Christian: *EPC-Technologie - vom Auto-ID Center zu EPCglobal*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 87 - 100

[Fin] Finkenzeller, Klaus: *RFID Handbuch - Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten*; 4. Auflage 2006, Hanser München.

[Han] Hansen, Hans-Günter; Lenk, Bernhard: *Codiertechnik - Der Schlüssel zum Strichcode*; 3. Auflage 1990, Ident Neuss. 244ff

[Hil] Hilty, Lorenz: *Risiken der RFID-Technologie*; 2004, Eidgenössische Materialprüfungs- und Forschungsanstalt. abgerufen am 14.09.2007
http://www.m-lab.ch/rfid-workshop/empa_pres.pdf

[hitachi] Hitachi, Ltd., Pressemitteilung: *Operation verified on world's smallest 0.05 mm x 0.05 mm "contactless powder IC chip" One-ninth the size of previous prototype, enabling insertion in paper*; 2007. abgerufen am 14.09.2007 http://www.hitachi.com/New/cnews/070213.html

[inotec] inotec Barcode Security, Neumünster: Produktbeschreibung "*inotec Etiketten*" - "*RFID Etiketten und ihre Funktion*"; 2007.

[isis] Kleber, Stephan: Dokumentation zum Praktikum *Erstellung einer Inventardatenbank für das Planetarium Laupheim*; 2007, Universität Ulm.

[ism1356] Auto-ID Center: *Technical Report - 13.56 MHz ISM Band Class 1Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0*; 2003. abgerufen am 14.09.2007 http://www.epcglobalinc.org/standards/specs/13.56_MHz_ISM_Band_Class_1_RFID_Tag_Interface_Specification.pdf

[iso] International Organization for Standardization. abgerufen am 14.09.2007 http://www.iso.org/

[ist] European Commission, Directorate-General Information Society: *IST 2003: The Opportunities ahead*; 2003. abgerufen am 14.09.2007 ftp://ftp.cordis.europa.eu/pub/ist/docs/ist_2003_opportunities_ahead_en.pdf

[jaco] Sun Microsystems, Inc.: *Java(tm) Communication API*. abgerufen am 14.09.2007 http://www.sun.com/download/products.xml?id=43208d3d

[jaca] Sun Microsystems, Inc.: Java Card Platform Specification 2.2.2. abgerufen am 14.09.2007 http://java.sun.com/products/javacard/specs.html

[kaywa] KAYWA AG: *Kaywa Reader*. abgerufen am 14.09.2007 http://reader.kaywa.com/

[kvk] Spitzenverbände der Krankenkassen Kassenärztliche Bundesvereinigung und Kassenzahnärztlichen Bundesvereinigung: *Technische Spezifikation der Versichertenkarte*; 2006. abgerufen am 14.09.2007 http://www.vdak.de/vertragspartner/Telematik/download/techn_spezifik_vkarte_20061030_v2_07.pdf

[Lam] Lampe, Matthias; Flörkemeier, Christian; Haller, Stephan: *Einführung in die RFID-Technologie*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 69 - 86

[Leo] Leong, Kin Seong; Ng, Mun Leng; Grasso, Alfio R.; Cole, Peter H.: *Dense RFID Reader Deployment in Europe using Synchronization*. abgerufen am 14.09.2007 http://www.academypublisher.com/jcm/vol01/no07/jcm01070916.pdf

[Lyy] Lyytinen, Kalle; Yoo, Youngjin: *Issues and challenges in ubiquitous computing*; 2002. CACM 45,12 63ff

[Mat] Mattern, Friedemann: *Die technische Basis für das Internet der Dinge*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 39-66

[ms] Hewlett-Packard Development Company, Pressemeldung: *HP präsentiert "Memory Spot"*; 2006. abgerufen am 14.09.2007 http://h41131.www4.hp.com/de/de/pr/HP_prsentiert_Memory_Spot.html

[nxp1] Philips Semiconductors, Datenblatt: *SL2 ICS10 I-CODE EPC Smart Label IC Functional Specification*; Revision 3.0 2004. abgerufen am 14.09.2007 http://www.nxp.com/acrobat/other/identification/SL080530.pdf

[nxp2] Philips Semiconductors, Datenblatt: *I-CODE SLI Smart Label IC SL2 ICS20 Functional Specification*; Revision 3.0 2003. abgerufen am 14.09.2007 http://www.nxp.com/acrobat_download/other/identification/SL058030.pdf

[ons] EPCglobal: *Object Naming Service (ONS) Version 1.0*; 2005. abgerufen am 14.09.2007 http://www.epcglobalinc.org/standards/ons/ons_1_0-standard-20051004.pdf

[Rie] Rieback, Melanie R.; Crispo, Bruno; Tanenbaum, Andrew S.: *Is Your Cat Infected with a Computer Virus?*; 2006. abgerufen am 14.09.2007 http://www.rfidvirus.org/papers/percom.06.pdf

[Jes] Jesse, Ralf; Rosenbaum, Oliver: *Barcode - Theorie, Lexikon, Software*; Technik, 2000. 38ff, 130ff, 201

[rp] EPCglobal: *Reader Protocol Standard, Version 1.1*; 2006. abgerufen am 14.09.2007
http://www.epcglobalinc.org/standards/rp/rp_1_1-standard-20060621.pdf

[Sch] Schoch, Thomas: *Middleware für Ubiquitous-Computing-Anwendungen*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 119-140

[seco] Sun Microsystems, Inc., Quellcode: Auszug aus *Java(tm) Communications API*;
http://moon.felk.cvut.cz/~pjv/Jak/JavaComm/javacomm20-win32.zip
abgerufen am 14.09.2007
http://moon.felk.cvut.cz/~pjv/Jak/JavaComm/commapi/samples/SerialDemo/

[sie] Siemens A&D, Produktkatalog: *RFID systems 4*; 2007. abgerufen am 14.09.2007
http://www.automation.siemens.co.uk/main/Extra/literature/files/A&D%20Catalogues/Automation%20Catalogues/FS10%20Factory%20Automation%20Sensors/2007/e86060-k8310-a101-a3-7600_kap_4.pdf

[Biz] Bizer, Johann; Spiekermann, Sarah; Günter, Oliver: *TAUCIS - Technikfolgenabschätzung: Ubiquitäres Computing und Informationelle Selbstbestimmung. Studie im Auftrag des Bundesministeriums für Bildung und Forschung*; 2006. abgerufen am 14.09.2007
https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf

[tds] EPCglobal: *EPCglobal Tag Data Standards Version 1.3*; 2006. abgerufen am 14.09.2007
http://www.epcglobalinc.org/standards/tds/tds_1_3-standard-20060308.pdf

[Thi1] Thiesse, Frédéric: *Architektur und Integration von RFID-Systemen*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 101-117

[Thi2] Thiesse, Frédéric: *Das smarte Buch*; in Fleisch, Elgar; Mattern, Friedemann (Hrsg.): *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*; 2005, Springer Berlin. 291-299

[uhfc1g2] EPCglobal: *EPC™ Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz - 960 MHz Version 1.0.9*; 2004. abgerufen am 14.09.2007
http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_0_9-standard-20050126.pdf

[Wei1] Weiser, Mark: *The Computer for the 21st Century*; 1991. Scientific American 265,3 66 - 75

[Wei2] Weiser, Mark: *Some Computer Science Issues in Ubiquitous Computing*; 1993. CACM 36,7 75 - 84

[wp] Wikipedia - Die freie Enzyklopädie (deutsche Ausgabe, mit Angabe des Artikels in der Referenz). abgerufen am 14.09.2007
http://de.wikipedia.org/

8 Anhang

8.1 Normenübersicht

Status	Gremium/Nummer	Jahr	Titel
Ratified Standard	EPCglobal	2006	EPCglobal Tag Data Standards Version 1.3
Ratified Standard	EPCglobal	2006	EPCglobal Tag Data Translation (TDT) 1.0
Candidate Recommendation	Auto-ID Center	2003	13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0
Candidate Recommendation	Auto-ID Center	2002	860MHz -- 930 MHz Class 1 Radio Frequency (RF) Identification Tag Radio Frequency & Logical Communication Interface Specification
Incomplete	Auto-ID Center	2003	Draft protocol specification for a 900 MHz Class 0 Radio Frequency Identification Tag
in development	EPCglobal	--	HF Generation 2 Tag Protocol Standard
Ratified Standard	EPCglobal	2005	Class 1 Generation 2 UHF Air Interface Protocol Standard "Gen 2"
Ratified Standard	EPCglobal	2007	Low Level Reader Protocol (LLRP), Version 1.0.1
Ratified Standard	EPCglobal	2006	Reader Protocol Standard, Version 1.1
Ratified Standard	EPCglobal	2007	Reader Management 1.0.1
in development	EPCglobal	--	Discovery, Configuration & Initialization Standard for Reader Operations
Ratified Standard	EPCglobal	2005	The Application Level Events (ALE) Specification, Version 1.0
Ratified Standard	EPCglobal	2007	EPC Information Services (EPCIS) Version 1.0 Specification
Ratified Standard	EPCglobal	2005	Object Naming Service (ONS) Version 1.0
in development	EPCglobal	--	Discovery Services Standard
Ratified Standard	EPCglobal	2007	Pedigree
Ratified Standard	EPCglobal	2006	EPCglobal Certificate Profile
Ratified Standard	EPCglobal	2005	The EPCglobal Architecture Framework
Published standard	ISO/IEC 15459	06/07	Information technology -- Unique identifiers -- Part 1-6
Published standard	ISO/IEC 15963	2004	Information technology -- Radio frequency identification for item management -- Unique identification for RF tags
Published standard	ISO 21007	2005	Gas cylinders -- Identification and marking using radio frequency identification technology -- Part 1-2
Published standard	ISO 10374	91/95	Freight containers -- Automatic identification
Published standard	ISO 18185	06/07	Freight containers -- Electronic seals -- Part 1-5
Published standard	ISO 17363	2007	Supply chain applications of RFID -- Freight containers
Published standard	ISO/IEC TR 24710	2005	Information technology -- Radio frequency identification for item management -- Elementary tag licence plate functionality for ISO/IEC 18000 air interface definitions
Published standard	ISO/IEC 18000-1	2004	Information technology -- Radio frequency identification for item management -- Part 1: Reference architecture and definition of parameters to be standardized
Published standard	ISO/IEC 18000-2	2004	Information technology -- Radio frequency identification for item management -- Part 2: Parameters for air interface communications below 135 kHz
Published standard	ISO/IEC 18000-3	2004	Information technology -- Radio frequency identification for item management -- Part 3: Parameters for air interface communications at 13,56 MHz
Published standard	ISO/IEC 18000-4	2004	Information technology -- Radio frequency identification for item management -- Part 4: Parameters for air interface communications at 2,45 GHz
Published standard	ISO/IEC 18000-6	2004	Information technology -- Radio frequency identification for item management -- Part 6: Parameters for air interface communications at 860 MHz to 960 MHz
Published standard	ISO/IEC 18000-7	2004	Information technology -- Radio frequency identification for item management -- Part 7: Parameters for active air interface communications at 433 MHz
Published standard	ISO/IEC 15961	2004	Information technology -- Radio frequency identification (RFID) for item management -- Data protocol: application interface
Published standard	ISO/IEC 15962	2004	Information technology -- Radio frequency identification (RFID) for item management -- Data protocol: data encoding rules and logical memory functions
Published standard	ISO/IEC 15434	2006	Information technology -- Automatic identification and data capture techniques -- Syntax for high-capacity ADC media

Status	Gremium/Nummer	Jahr	Titel
Published standard	ISO/IEC 24730-1	2006	Information technology -- Real-time locating systems (RTLS) -- Part 1: Application program interface (API)
Published standard	ISO/IEC 24730-2	2006	Information technology -- Real-time locating systems (RTLS) -- Part 2: 2,4 GHz air interface protocol
Published standard	ISO/IEC TR 18001	2004	Information technology -- Radio frequency identification for item management -- Application requirements profiles
Published standard	ISO/IEC 18046	2006	Information technology -- Automatic identification and data capture techniques -- Radio frequency identification device performance test methods
Published standard	ISO/IEC TR 18047	04-06	Information technology -- Radio frequency identification device conformance test methods -- Part 2/4/6/7
Published standard	ISO/IEC 19762-3	2005	Information technology -- Automatic identification and data capture (AIDC) techniques -- Harmonized vocabulary -- Part 3: Radio frequency identification (RFID)
Published standard	ISO 11784	1996	Radio frequency identification of animals -- Code structure
Published standard	ISO 11785	1996	Radio frequency identification of animals -- Technical concept
Published standard	ISO 14223-1..-2	2003	Radiofrequency identification of animals -- Advanced transponders -- Part 1-2
Published standard	ISO/IEC 10536	95-00	Identification cards -- Contactless integrated circuit(s) cards -- Part 1-3
Published standard	ISO/IEC 14443	00-06	Identification cards -- Contactless integrated circuit(s) cards -- Proximity cards -- Part 1-4
Published standard	ISO/IEC 15693	00-06	Identification cards - Contactless integrated circuit(s) cards - Vicinity cards -- Part 1-3
Published standard	ISO/IEC 10373	01-07	Identification cards -- Test methods -- Part 1-3/5-7
Under development	ISO/IEC CD/NP 24791-1..-6	--	Information technology -- Automatic Identification and Data Capture Techniques -- Radio-Frequency Identification (RFID) for Item Management -- System Management Protocol -- Part 1-6
Under development	ISO/IEC DTR/NP TR 24729	--	Information technology -- Radio frequency identification for item management -- Implementation guidelines -- Part 1-3
Under development	ISO/IEC CD 24753	--	Automatic identification and data capture techniques -- Radio frequency identification (RFID) for item management -- Application protocol: encoding and processing rules for sensors and batteries
Under development	ISO/NP 28560	--	Information and documentation -- Data model for use of radio frequency identifier (RFID) in librairies
Under development	ISO/CD 24631	--	Radio frequency identification of animals -- Part 1-4
Under development	ISO/FDIS 17364	--	Supply chain applications of RFID -- Returnable transport items (RTIs)
Under development	ISO/FDIS 17365	--	Supply chain applications of RFID -- Transport units
Under development	ISO/PRF 17366	--	Supply chain applications of RFID -- Product packaging
Under development	ISO/PRF 17367	--	Supply chain applications of RFID -- Product tagging

Erklärung

Hiermit erkläre ich, die vorstehende Arbeit *selbständig* nach bestem Wissen und Gewissen erstellt zu haben. Ferner habe ich nur die in Text und Literaturhinweisen als solche *angegebenen Quellen und Hilfsmittel* verwendet.

Ulm, den 17.09.2007